MARTA MORIGI

On $p$-groups with abelian automorphism group


<http://www.numdam.org/item?id=RSMUP_1994__92__47_0>
On $p$-Groups with Abelian Automorphism Group.

MARTA MORIGI (*)

Introduction.

In this paper we give an answer to the following question: «Which is the smallest order of a non cyclic $p$-group whose automorphism group is abelian?» (here $p$ is a prime number). For $p = 2$ the answer is already well known; namely in 1913 G. Miller explicitly constructed a group of order $2^6$ with the property stated above [5]. For $p \neq 2$ the problem was investigated mainly by B. Earnley who proved that no non-cyclic $p$-groups of order less or equal to $p^5$ have abelian automorphism groups ([1], p.30). In a previous paper Jonah and Konvisser had stated that there exist some groups of order $p^8$, $p \neq 2$, whose automorphism groups are abelian of order $p^{16}$ [4] and afterwards B. Earnley generalized this result by constructing a family of groups of order $p^2 + 3n$ with the given property, for each natural number $n \geq 2$ [1].

After these achievements, the unsolved problem was actually whether there existed a non-cyclic group $G$ whose automorphism group is abelian and such that $p^6 \leq |G| \leq p^7$. In this paper the answer is obtained in two steps:

— in the first section we prove that there exist no groups of order $p^6$ whose automorphism groups are abelian,

— in the second section we give the example of a group of order $p^7$ whose automorphism group is abelian. This group is special, is generated by 4 elements and is the smallest of an infinite family of groups of order $p^{n^2 + 3n + 3}$, where $n$ is a natural number.

(*) Indirizzo dell'A.: Dipartimento di Matematica Pura e Applicata, Università di Padova, via Belzoni 7, 35131 Padova.
Notation and preliminary results.

The notation used is standard. In the whole paper if $G$ is a group $Z = Z(G)$ will denote its center, if no ambiguity can arise.

$\text{Aut}_C G = \{ \alpha \in \text{Aut} G | \alpha \text{ induces the identity on } G/Z(G) \}$ is the group of central automorphisms of $G$.

$C_G(S)$ is the centralizer of $S$ in $G$, if $S$ is a subset of $G$.

$\Omega_1(G) = \langle y \in G | y^p = 1 \rangle$, if $G$ is a $p$-group.

A PN group is a group with no non-trivial abelian direct factors.

$\mathbb{Z}/p\mathbb{Z}$ is the field with $p$ elements and if $r \in \mathbb{Z}/p\mathbb{Z}$, $r \neq 0$ then $1/r$ will denote its inverse.

In the whole paper, we shall often represent the automorphisms of an elementary abelian $p$-group by matrices. In fact such a group is a vector space over the field $\mathbb{Z}/p\mathbb{Z}$ so that, once we have fixed a basis $\{ x_i \ | \ i = 1, \ldots, n \}$, we can associate to each $\alpha \in \text{Aut} G$ the matrix $A = (a_{ij})_{i,j = 1, \ldots, n}$ with entries in $\mathbb{Z}/p\mathbb{Z}$ satisfying $x_i^\alpha = \prod_{j=1}^n x_j^{a_{ij}}$.

We collect in the following lemmas some known results which will be used in the sequel.

**Lemma 0.1.** Let $G$ be a group of class 2. For all $x, y, w \in G$, $m \in \mathbb{Z}$ and $n \in \mathbb{N}$ we have:

(i) $[x, yw] = [x, y][x, w],$

(ii) $[xy, w] = [x, w][y, w],$

(iii) $[x, y^m] = [x^m, y] = [x, y]^m,$

(iv) $(xy)^n = x^n y^n [y, x]^{n(n - 1)/2}$.

**Proof.** See [3], p. 253.

**Lemma.** 0.2. If $G$ is a PN group

$$|\text{Aut}_C G| = \prod_{i=1}^k |\Omega_i(Z)|^{r_i}$$

where $p^k$ is the exponent of $G/G'$ and $r_i$ factors of order $p^i$ occur in the decomposition of $G/G'$ as direct product of cyclic groups.

**Proof.** See [6].

**Lemma 0.3.** Let $G$ be a finite non-abelian PN group such that $G' = Z(G)$. Then $\text{Aut}_C G$ is abelian. Moreover if $\varphi \in \text{Aut} G$ the function $f$ given by: $g^f = g^{-1}g^\varphi$ is a homomorphism of $G$ in $Z$ and we have $g^g = g(g^f)^g$. 

LEMMA 0.4. The group of central automorphisms of a p-group, when \( p \) is odd, is a p-group if and only if \( G \) is a PN group.

PROOF. See [6].

LEMMA 0.5. Consider the extension: \( 1 \to \mathbb{Z} \to G \to G / \mathbb{Z} \to 1 \) where \( G \) is a p-group and \( G / \mathbb{Z} \) is a direct product of \( n \geq 2 \) cyclic groups all of the same order \( p^t \). Let \( T: G / \mathbb{Z} \to Z / Z^p \) be the homomorphism given by: \( \bar{x}^T = x^p \bar{Z}^p \), where \( x \mathbb{Z} = \bar{x} \), and let \( [\cdot, \cdot]: G / \mathbb{Z} \times G / \mathbb{Z} \to Z \) be defined by: \( [\bar{x}, \bar{y}] = [x, y] \), where \( x \mathbb{Z} = \bar{x} \) and \( y \mathbb{Z} = \bar{y} \) (note that neither map depend on the choice of representatives in \( G \)). Now let \( (\alpha, \beta) \in \text{Aut } G / \mathbb{Z} \times \text{Aut } \mathbb{Z} \). Then there exists an automorphism of \( G \) which induces \( \alpha \) on \( G / \mathbb{Z} \) and \( \beta \) on \( \mathbb{Z} \) if and only if the following two diagrams commute:

\[
\begin{array}{ccc}
G / \mathbb{Z} \times G / \mathbb{Z} & \xrightarrow{[\cdot, \cdot]} & Z \\
\downarrow{\alpha \times \alpha} & & \downarrow{\beta} \\
G / \mathbb{Z} \times G / \mathbb{Z} & \xrightarrow{[\cdot, \cdot]} & Z \\
\end{array}
\]

\[
\begin{array}{ccc}
G / \mathbb{Z} \to Z / Z^p \to 1 \\
\downarrow{\alpha} & & \downarrow{\beta} \\
G / \mathbb{Z} \to Z / Z^p \to 1 \\
\end{array}
\]

where \( (zZ^p)^\beta = z^{\beta}Z^p \).

PROOF. See [1], p. 19.

1. – We show that there exists no non-abelian group of order \( p^6 \) whose automorphism group is abelian. (Here, and in the whole paper, \( p \) is an odd prime.) The outline of the proof is the following: we first analyze the structure which such a group should have and then we come to a contradiction. We start with the following

OBSERVATION 1.0. If \( G \) is a group such that \( \text{Aut } G \) is abelian then every automorphism of \( G \) is central; so in order to prove that the automorphism group of a given group \( G \) is not abelian it suffices to show that there exists a non-central automorphism.

The proof follows immediately from the fact that the group of central automorphisms is the centralizer of \( \text{Inn } G \) in \( \text{Aut } G \).

We also need the following result, proved by B. Earnley.

LEMMA 1.1. If \( G \) is a non-cyclic p-group such that \( \text{Aut } G \) is abelian then:
(i) $Z(G)$ and the Frattini subgroup $\Phi(G)$ of $G$ cannot have cyclic intersection.

(ii) If $|G| = p^6$ then $G/Z$ is elementary abelian of rank 4.

PROOF. See [2], pp. 16 and 48.

PROPOSITION 1.2. Let $G$ be a non-abelian $p$-group of order $p^6$ such that $\text{Aut } G$ is abelian. Then $Z$ and $G/Z$ are elementary abelian of rank 2 and 4 respectively and $Z = \Phi(G)$. Furthermore, a maximal abelian subgroup of $G$ has order $p^4$.

PROOF. By the Lemma above $G/Z$ is elementary abelian of rank 4 and $Z$ is not cyclic, so it must be elementary abelian of rank 2. Then we have: $\Phi(G) \leq Z$, as $G/Z$ is elementary abelian, and it cannot be a proper inclusion because otherwise $\Phi(G) \cap Z$ would be cyclic, contradicting the Lemma above. Let $A$ be a maximal abelian subgroup of $G$; $Z$ is contained in $A$ and the inclusion is proper because $\langle g, Z \rangle$ is abelian for all $g \in G \setminus Z$; hence $|A| \geq p^3$. Assume $|A| = p^3$ and take $a \in A \setminus Z$, so that $A = \langle a, Z \rangle$. Since $G' \leq Z$, we have $|[a, G]| \leq p^2$, $|G: C_G(a)| \leq p^2$ and there exists $x \in G \setminus A$ such that $[x, a] = 1$. Then $\langle a, x, Z \rangle$ is abelian and $A$ is properly contained in it, contrary to the assumptions. Thus $|A| \geq p^4$. Assume $|A| = p^5$. Hence $G = A(y)$ for some $y \in G \setminus A$ and as we have $|G: C_G(y)| \leq p^2$ it follows that $|A \cap C_G(y)| \geq p^3$ and there exists an element $x \in (A \cap C_G(y)) \setminus Z$. Anyway $A$ is abelian and if $x \in A$ centralizes $y$ it centralizes every element of $G$, hence $x \in Z$, contrary to the assumption. Since $G$ is not abelian we have $|A| \neq p^6$; hence $|A| = p^4$, as we wanted to prove.

PROPOSITION 1.3. Let $G$ be a group of order $p^6$ such that $Z$ and $G/Z$ are elementary abelian of rank 2 and 4 respectively and assume $Z = \Phi(G)$. If there exists an elementary abelian subgroup $A$ of $G$ of order $p^4$, then $\text{Aut } G$ is not abelian.

PROOF. By Proposition 1.2 $G$ cannot have abelian subgroups of order $p^5$, thus $Z \leq A$. As $|G'| \leq p^2$ we have $|[A, g]| \leq p^2$ for all $g \in G$; moreover $[A, g] \neq 1$ for all $g \in G \setminus A$ because $A$ is maximal abelian. There are two cases:

(i) There exists $b_1 \in G \setminus A$ such that $|[A, b_1]| = p$.

Hence $|[A: C_A(b_1)]| = p$ and there is $a_1 \in A \setminus Z$ such that $[a_1, b_1] = 1$. Put $A = \langle a_1, a_2, Z \rangle$ and $G = \langle a_1, a_2, b_1, b_2 \rangle$. 

Let \( a \) be the automorphism of \( G/Z \) associated to the matrix

\[
\begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
1 & 0 & 0 & 1
\end{pmatrix}
\]

referring to the basis \( \{a_1 Z, a_2 Z, b_1 Z, b_2 Z\} \) and let \( \beta \) be the identity of \( Z \). Then by Lemma 0.5 \( G \) has an automorphism \( \gamma \) which induces \( a \) on \( G/Z \) and \( \beta \) on \( Z \); \( \gamma \) is not central and by the observation 1.0 \( \text{Aut} \, G \) is not abelian.

(ii) For all \( b \in G \setminus A \) we have \([A, b] = Z\).

Consider \( b_1 \in G \setminus A \); hence \( C_G(b_1) \cap A = Z \) and \(|G: C_G(b_1)| = p^2\).

Put \( C_G(b_1) = \langle b_1, b_2, Z \rangle \); thus \( G = \langle A, b_1, b_2 \rangle \) and \([A, b_1] = [A, b_2] = Z\). Consider \( a_1 \in A \setminus Z \); as \([A, b_1] = Z\), there exists \( a_2 \in A \) such that \([a_2, b_1] = [a_1, b_2]\).

We now prove that \( a_2 \notin \langle a_1, Z \rangle \).

Deny this statement and assume \( a_2 = a_1 z \), with \( z \in Z \); by Lemma 0.1 we have \([a_2, b_1] = [a_1 z, b_1] = [a_1, b_1]\), hence \([a_1, b_1][a_1, b_2]^{-1} = 1\), that is \([a_1, b_1 b_2^{-1}] = 1\).

It follows that \(|[A, b_1 b_2^{-1}]| \leq p\), contrary to the assumptions.

Hence \( G = \langle a_1, a_2, b_1, b_2 \rangle \).

Let \( a \) be the automorphism of \( G/Z \) associated to the matrix

\[
\begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 \\
0 & 1 & 0 & 1
\end{pmatrix}
\]

referring to the basis \( \{a_1 Z, a_2 Z, b_1 Z, b_2 Z\} \) and let \( \beta \) be the identity of \( Z \). By the same argument as before the result follows.

**Proposition 1.4.** Let \( G \) be a group of order \( p^6 \) such that \( Z \) and \( G/Z \) are elementary abelian of rank 2 and 4 respectively and assume \( Z = \Phi(G) \). If \( G \) has no elementary abelian subgroups of order \( p^4 \) then \( \text{Aut} \, G \) is non-abelian.

**Proof.** \( G^P \) is contained in \( Z \), so it has order at most \( p^2 \) and we have \(|\Omega_1(G)| \geq p^4\). From the assumptions it also follows that for all \( x, y \in \Omega_1(G) \setminus Z \) such that \( xZ \neq yZ \) we have \([x, y] \neq 1\). If \( A = \langle x, y, Z \rangle \) we have \( A = E \times \langle z \rangle \), where \( z \in Z \) and \( E = \langle a_1, a_2, u | [a_1, a_2] = u, [a_1, u] = [a_2, u] = 1, a_1^p = a_2^p = 1 \rangle \).
There are two cases:

(i) There exists $b_1 \in G \setminus A$ such that $[A, b_1] = 1$.

Put $G = \langle A, b_1, b_2 \rangle$; then there are $r_1, r_2, s_1, s_2 \in \mathbb{Z}/p\mathbb{Z}$ such that $a_1^{b_2} = a_1 u^{r_1} z^{s_1}$ and $a_2^{b_2} = a_2 u^{r_2} z^{s_2}$.

If $s_1 \neq 0$ we may assume that $s_2 = 0$ (take $k \in \mathbb{Z}/p\mathbb{Z}$ such that $s_2 = s_1 k$ and replace $a_1, a_2, u$ with $a'_1 = a_1, a'_2 = a_1^{-k} a_2$ and $u' = [a'_1, a'_2]$).

Let $\alpha$ the automorphism of $G/Z$ associated to the matrix
\[
\begin{pmatrix}
1 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & -r_2 & 0 & 1
\end{pmatrix}
\]
referring to the basis $\{a_1 Z, a_2 Z, b_1 Z, b_2 Z\}$ and let $\beta$ be the identity of $Z$. Then by Lemma 0.5 there is a non-central automorphism $\gamma$ of $G$ which induces $\alpha$ on $G/Z$ and $\beta$ on $Z$ and the result follows from the observation 1.0.

If $s_1 = 0$ we come to the same conclusions by replacing the preceding matrix with
\[
\begin{pmatrix}
1 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
r_1 & 0 & 0 & 1
\end{pmatrix}
\]

(ii) For all $b \in G \setminus A$ we have $[A, b] \neq 1$, that is $C_G(A) = Z$.

We shall now show that in this case $\Omega_1(G) = A$. $A$ is contained in $\Omega_1(G)$ by definition of $A$ and assume that the inclusion is proper. Hence there is $b \in \Omega_1(G) \setminus A$ and by the same argument as in the preceding case there is $a \in A \setminus Z$ such that $a^b = a u^r, r \in \mathbb{Z}/p\mathbb{Z}$. Take $c \in A$ such that $[a, c] = u^r$ and put $b' = b c^{-1}$; we have $[a, b'] = 1, b' \in G \setminus A$ and $(b')^p = (b c^{-1})^p = b^p = 1$ (Lemma 0.7), but this contradicts the fact that $G$ has no elementary abelian subgroups of order $p^4$. Hence $A = \Omega_1(G)$ and $A$ is characteristic in $G$.

Put $G = \langle A, b_1, b_2 \rangle$ and assume $b_1^p = b_2^p$. By Lemma 0.1 we have $(b_1 b_2^{-r})^p = 1$ and so $b_1 b_2^{-r} \in (G \setminus A) \cap \Omega_1(G)$, which contradicts the fact that $A = \Omega_1(G)$. Hence $\langle b_1^p \rangle \neq \langle b_2^p \rangle$. 
We claim that it is possible to choose the generators of $G$ in order to have:

$$G = AB, \quad A = \langle a_1, a_2, u \mid [a_1, u] = [a_2, u] = 1, \quad a_1^p = a_2^p = 1, [a_1, a_2] = u \rangle \times \langle z \rangle;$$

$$B = \langle b_1, b_2 \rangle; \quad b_1^p = u^k; \quad b_2^p = z; \quad [a_1, b_1] = [a_2, b_2] = z; \quad [a_1, b_2] = [a_2, b_1] = 1; \quad [b_1, b_2] = u^\xi z^\eta; \quad \xi, \eta \in \mathbb{Z}/p\mathbb{Z};$$

$$G/Z = \langle a_1 Z \rangle \times \langle a_2 Z \rangle \times \langle b_1 Z \rangle \times \langle b_2 Z \rangle; \quad Z = \langle u \rangle \times \langle z \rangle.$$ 

Up to now the situation is the following:

$$A = \langle E \rangle \times \langle z \rangle \triangleleft G; \quad A' = \langle u \rangle; \quad G = \langle A, b_1, b_2 \rangle; \quad Z = \langle b_1^p \rangle \times \langle b_2^p \rangle; \quad B = \langle b_1, b_2 \rangle; \quad B \cap A = Z.$$

Take $b \in B$; $b$ induces an automorphism of the elementary abelian group $A/A'$ which in turn determines a matrix of the type:

$$\begin{bmatrix}
1 & 0 & s \\
0 & 1 & r \\
0 & 0 & 1
\end{bmatrix}$$

referring to the basis $\{a_1 A', a_2 A', zA'\}$. In this way we produce a homomorphism

$$\phi: B \to S = \left\{ \begin{bmatrix} 1 & 0 & s \\ 0 & 1 & r \\ 0 & 0 & 1 \end{bmatrix} \mid r, s \in \mathbb{Z}/p\mathbb{Z} \right\}.$$ 

If $b \in \text{Ker} \phi$ we have $a_1^b = a_1 u^s$, $a_2^b = a_2 u^r$ for some $r, s \in \mathbb{Z}/p\mathbb{Z}$, hence $a_i^{a_i a_j} = a_i^b$ with $i = 1, 2$; $a_1^{-r} a_2^{-1} b^{-1} \in C_G(A) = Z$ and $b \in A \cap B = Z$. Since $Z \leq \text{Ker} \phi$ trivially, we have $\text{Ker} \phi = Z$, $|B^s| = |B/\text{Ker} \phi| = p^2 = |S|$ and $\phi$ is surjective.

So we can assume $b_1 \in \phi^{-} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ and $b_2 \in \phi^{-} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$.

We have $a_1^{b_1} = a_1 zu^{r_1}$; $a_2^{b_1} = a_2 u^{r_2}$; $a_1^{b_2} = a_1 u^{r_3}$; $a_2^{b_2} = a_2 zu^{r_4}$, with $r_i \in \mathbb{Z}/p\mathbb{Z}$ for $i = 1, \ldots, 4$. Multiplying $b_1$ and $b_2$ for suitable elements of $A$ we can arrange things in order to have $[a_1, b_i] = [a_2, b_i] = z$ and $[a_i, b_j] = 1$ if $i \neq j$. Hence $[A, B] = \langle z \rangle$. Since $Z = \langle u \rangle \times \langle z \rangle = B^p$ there are $c_1, c_2 \in B$ such that $c_1^p = u$; $c_2^p = z$ and $B = \langle c_1, c_2 \rangle$. 
Consider $R = \{ \alpha \in \text{Aut}_B(b^x b^{-1} \in \langle z \rangle) \forall b \in B \}$ and let $\psi : A \to R$ be the homomorphism which associates to each $\alpha \in A$ the inner automorphism induced by $\alpha$ on $B$. $\text{Ker } \psi = C_A(B) = Z$, hence $|A^\psi| = |A/Z| = p^2$.

There is also a bijection $R \to \text{Hom}(B, \langle z \rangle)$ which associates to each $\alpha \in R$ the homomorphism $f$ defined by $x^f = x^\alpha x^{-1}$.

Thus $|R| = |\text{Hom}(B, \langle z \rangle)| = p^2$ and $\psi$ is surjective, that is the automorphisms of $B$ which induce the identity on $B/\langle z \rangle$ are the restrictions to $B$ of the inner automorphisms induced by the elements of $A$.

It is easy to check that the functions $\alpha_1, \alpha_2$ defined by: $c_1^{\alpha_1} = c_1 z^{-1}, c_2^{\alpha_1} = c_2, c_1^{\alpha_2} = c_1, c_2^{\alpha_2} = c_2 z^{-1}$ extend by linearity to automorphisms of $B$ which belong to $R$; hence there are $a_1', a_2' \in A$ such that $c_1^{a_1'} = c_1 z^{-1}; c_2^{a_2'} = c_2 z^{-1}; c_i^{a_i} = c_i$ if $i \neq j; i, j = 1, 2$. Moreover $A = \langle a_1', a_2', Z \rangle$. Putting $u' = [a_1', a_2']$ we obtain $c_i^p = (u')^k$ with $k \in Z/pZ, k \neq 0$; $c_2^p = z, [a_1', c_1] = [a_2', c_2] = z$ and $[a_i', c_j] = 1$ if $i \neq j; i, j = 1, 2$. This establishes our claim.

Consider the matrices

$$M = \begin{pmatrix} -1 & \gamma/k & 0 & 0 \\ 0 & 1 & 0 & O \\ 0 & \gamma & -1 & 0 \\ \gamma & -\gamma^2/k & \gamma/k & 1 \end{pmatrix}, \quad N = \begin{pmatrix} -1 & 0 \\ \gamma & 1 \end{pmatrix}$$

and let $\alpha$ and $\beta$ be the automorphisms of $G/Z$ and $Z$ respectively associated to $M$ and $N$, referring to the basis $\{a_1Z, a_2Z, b_1Z, b_2Z\}$ and $\{u, v\}$. (We remind that $\gamma$ and $k$ are defined by the relations written before.)

By Lemma 0.5 there is a non-central automorphism $\gamma$ of $G$ which induces $\alpha$ on $G/Z$ and $\beta$ on $Z$ and we can conclude that $\text{Aut } G$ is not abelian.

**Proposition 1.4.** There is no group $G$ of order $p^6$ whose automorphism group is an abelian $p$-group.

**Proof.** Deny the statement and assume that there is a group $G$ with the given properties. Then by Lemma 0.4 $G$ is a PN group and the result follows from Propositions 1.3, 1.1 and 1.4.

From the proofs of Propositions 1.3 and 1.4 and from [3] we can also obtain the following

**Proposition 1.5.** Every non abelian group of order $p^6$ has a non central automorphism.
2. - In this section we describe a family of $p$-groups whose automorphism groups are abelian. Among them, the one with smallest order has $p^7$ elements and it is the smallest non abelian $p$-group with the property stated above.

**Proposition 2.1.** For each natural number $n$ there exists a group $G(n)$ of order $p^{n^2 + 3n + 3}$ whose automorphism group is an elementary abelian $p$-group of order $p^{(n^2 + n + 1)(2n + 2)}$.

**Proof.** Let $n$ be a natural number and let $G = G(n)$ be the group of class two generated by the set $\{a_1, a_2, b_1, \ldots, b_{2n}\}$ and satisfying the following further relations:

$$[a_1, b_{2i + 1}] = [a_2, b_{2i + 2}] = [b_{2i + 1}, b_{2i + 2}] =$$

$$=[b_{2i + 2}, b_{2j + 2}] = [b_{2i + 1}, b_{2j + 1}] = 1; \quad \text{for } i, j = 0, \ldots, n - 1;$$

$$a_1^p = a_2^p = 1;$$

$$[a_1, a_2]^p = [a_1, b_{2i + 2}]^p = [a_2, b_{2i + 1}]^p = [b_{2i + 1}, b_{2j + 2}]^p = 1;$$

$$\quad \text{for } i, j = 0, \ldots, n - 1; i \neq j;$$

$b_1^p$ is the product of the elements of the set

$$X = \{[a_1, a_2], [a_1, b_{2i + 2}], [a_2, b_{2i + 1}], [b_{2i + 1}, b_{2j + 2}]\};$$

$$i, j = 0, \ldots, n - 1; i \neq j;$$

$$b_2^p = b_1^p [a_1, b_2]^{-1}, b_{2i + 1}^p = b_{2i}^p [a_2, b_{2i + 1}]^{-1}, b_{2i + 2}^p = b_{2i + 1}^p [a_1, b_{2i + 2}]^{-1},$$

$$\quad \text{for } i = 1, \ldots, n - 1.$$

By a standard construction we can see that $G$ is a group of order $p^{n^2 + 3n + 3}$; $G'$ is elementary abelian of rank $n^2 + n + 1$ and basis $X$, and $\Omega_2(G) = \{a_1, a_2, G'\}$.

We now determine $C_G(a)$, where $a$ is any element of $\Omega_2(G) \setminus G'$.

If $a = a_1^{x_1} a_2^{x_2} z, g = a_1^{y_1} a_2^{y_2} b_1^{y_1} b_2^{x_2} u$, with $z, u \in G'; x_i, y_i, w_i \in \mathbb{Z}; i = 1, 2; j = 1, \ldots, n$; we have:

$$[a, g] = [a_1, a_2]^{x_1 y_2 - x_2 y_1} \prod_{i = 0}^{n - 1} ([a_1, b_{2i + 2}]^{x_1 y_2 + x_2} [a_2, b_{2i + 1}]^{x_2 y_2 + 1}).$$

If $x_1 \equiv 0 \pmod{p}$, we have $[a, g] = 1$ if and only if $w_{2j + 1} \equiv 0 \pmod{p}$ for all $j = 0, \ldots, n - 1$ and $y_1 \equiv 0 \pmod{p}$.

If $x_2 \equiv 0 \pmod{p}$, we have $[a, g] = 1$ if and only if $w_{2j + 2} \equiv 0 \pmod{p}$ for all $j = 0, \ldots, n - 1$ and $y_2 \equiv 0 \pmod{p}$.
If $x_1 \neq 0 \neq x_2 \pmod{p}$ we have $[a, g] = 1$ if and only if
$w_{2i+1} \equiv w_{2j+2} \equiv 0 \pmod{p}$ for all $i, j = 1, \ldots, n$ and $y_1 \equiv kx_1, y_2 \equiv kx_2 \pmod{p}$ with $k \in \mathbb{Z}$.
Thus:

$$C_G(a_1) = \langle a_1, b_{2i+1}, G' \mid i = 0, \ldots, n-1 \rangle,$$

$$C_G(a_2) = \langle a_2, b_{2i+2}, G' \mid i = 0, \ldots, n-1 \rangle,$$

$$C_G(a) = \langle a, G' \rangle \quad \text{if } a \in \Omega_1(G) \setminus (G' \langle a_1 \rangle \cup G' \langle a_2 \rangle).$$

$C_G(a_i)/G'$ is elementary abelian of rank $n+1$, for $i = 1, 2$, and $C_G(a)/G'$ is cyclic of order $p$ for all $a \in \Omega_1(G) \setminus (G' \langle a_1 \rangle \cup G' \langle a_2 \rangle)$. This also shows that $Z(G) = G'$.

Let $\varphi \in \text{Aut } G$; hence $C_G(a_i)^\varphi = C_G(a_i^\varphi)$ and we have $a_i^\varphi \in \langle a_1, G' \rangle$ or $a_i^\varphi \in \langle a_2, G' \rangle$.

We shall say that $\varphi$ is of type 1 if it fixes $C_G(a_1)$ and $C_G(a_2)$, of type 2 if it interchanges them.

Assume that $\varphi$ is of type 1 and consider $r \in \{0, \ldots, n-1\}$.

It must be $b_{2r+1}^\varphi \in C_G(a_1); b_{2r+2}^\varphi \in C_G(a_2)$ and $[b_{2r+1}^\varphi, b_{2r+2}^\varphi] = 1$.

If $b_{2r+1}^\varphi = a_{i_1}^{y_1} \cdot a_{i_2}^{y_2} \cdots b_{2n-1}^{y_{2n-1}}$ and $b_{2r+2}^\varphi = a_{i_2}^{y_2} \cdot b_{2}^{y_2} \cdots b_{2n}^{y_{2n}}$; with $x_i, y_i \in \mathbb{Z}$; $i = 1, 2; j = 1, \ldots, n$ we have:

$$[b_{2r+1}^\varphi, b_{2r+2}^\varphi] = [a_1, a_2]^{y_1x_1 \prod_{i,j=0}^{n-1}}.$$
We must have

\[(b_{2i+1}^p)^p = (b_{2i+1}^p)^p\]

hence \(b_{2i+1}^p + 1 \in \langle (b_{2i+1}^p) \rangle\) and as in the representation of \(b_{2i+1}^p\) there are exactly \(n^2 + n - 1 - 2i\) elements of \(X\) with non-zero exponent we must have \(n^2 + n - 1 - 2i = n^2 + n - 1 - 2\sigma(i)\), that is \(\sigma\) must be the identity. In the same way, if \(\varphi \in Aut\ G\) is of type 2, we have \(b_{2i+1}^\varphi \in \langle b_{2\varphi(i)+1}, G' \rangle\) and \(b_{2i+2}^\varphi \in \langle b_{2\varphi(i)+1}, G' \rangle\), with \(\tau \in S_n\); and the condition (\(\ast\)) leads to a contradiction.

Hence every \(\varphi \in Aut\ G\) is of type 1 and induces on \(G/G'\) an automorphism associated to a diagonal matrix \(M\) with entries in \(\mathbb{Z}/p\mathbb{Z}\) of the type

\[
M = \begin{pmatrix}
\alpha_1 \\
\alpha_2 \\
\beta_1 \\
\beta_2 \\
\vdots \\
\beta_{2n}
\end{pmatrix}
\]

where the basis of \(G/G'\) is \(\{a_1 G', a_2 G', b_1 G', \ldots, b_{2n} G'\}\). We have:

\[
[a_1, a_2]^p = [a_1, a_2]^{x_1 x_2}, \quad [a_1, b_{2i+2}]^p = [a_1, b_{2i+2}]^{x_1 \beta_{2i+2}},
\]

\[
[a_2, b_{2i+1}]^p = [a_2, b_{2i+1}]^{x_2 \beta_{2i+1}},
\]

\[
[b_{2i+1}, b_{2j+2}]^p = [b_{2i+1}, b_{2j+2}]^{\beta_{2i+1} \beta_{2j+2}},
\]

with \(0 \leq i \neq j \leq n - 1\).

From the conditions \((b_1^\varphi)^p = (b_1^p)^p\) and \((b_2^\varphi)^p = (b_2^p)^p\) we obtain:

\[\alpha_1 \alpha_2 = \beta_1 = \alpha_2 \beta_{2i+1} = \alpha_1 \beta_{2i+2}\]

for all \(i = 0, \ldots, n - 1\) and \(\beta_2 = \alpha_1 \alpha_2\);

and it follows that \(M\) is the identity.

Hence we have proved that every automorphism of \(G\) is central and by Lemma 0.2 we have \(|Aut\ G| = |Aut\ C_G| = p^{(n^2 + n + 1)(2n + 2)}\). From the fact that \(Z\) has exponent \(p\) it follows that \((g^f)^p = 1\) for all \(f \in Hom\ (G, Z(G))\) and for all \(g \in G\), thus \(\varphi^p = 1\) for all \(\varphi \in Aut\ G\). Moreover \(Z(G) = G'\), so by Lemma 0.3 \(Aut\ G\) is an elementary abelian \(p\)-group, as we wanted to prove.
Observation. For \( n = 1 \) we obtain that \( G = G(1) \) has order \( p^7 \), it is generated by 4 elements \( \{a_1, a_2, b_1, b_2\} \), it has class 2, it satisfies the relations

\[
a_1^p = a_2^p = 1; \quad [a_1, b_1] = [a_2, b_2] = [b_1, b_2]^p = 1;
\]

\[
[a_1, a_2]^p = [a_1, b_2]^p = [a_2, b_1]^p = 1;
\]

\[
b_1^p = [a_1, a_2][a_1, b_2][a_2, b_1]; \quad b_2^p = [a_1, a_2][a_2, b_1]
\]

and its automorphism group is elementary abelian of order \( p^{12} \).

From this facts and Proposition 1.5 we obtain the following

**Proposition 2.2.** Let \( p \) be an odd prime. The smallest order of a \( p \)-group whose automorphism group is abelian is \( p^7 \).

**References**


