FINITE $p$-GROUPS OF NILPOTENCY CLASS 3 WITH TWO CONJUGACY CLASS SIZES

BY

TUSHAR KANTA NAIK, RAHUL DATTATRAYA KITTURE AND MANOJ K. YADAV

Harish-Chandra Research Institute, HBNI
Chhatnag Road, Jhunsi, Allahabad-211 019, India
e-mail: mathematics67@gmail.com, rahul.kittle@gmail.com, myadav@hri.res.in

ABSTRACT

It is proved, for a prime $p > 2$ and an integer $n \geq 1$, that finite $p$-groups of nilpotency class 3 and having only two conjugacy class sizes, 1 and $p^n$, exist if and only if $n$ is even; moreover, for a given even positive integer $n$, such a group is unique up to isoclinism (in the sense of Philip Hall).

1. Introduction

A finite group $G$ is said to be of conjugate type $(1 = m_1, m_2, \ldots, m_r)$, $m_i < m_{i+1}$, if $m_i$'s are precisely the different sizes of conjugacy classes of $G$. In this paper we restrict our attention to finite groups of conjugate type $(1, m)$. Investigation on such groups $G$ was initiated by N. Ito [6] in 1953. He proved that groups of conjugate type $(1, m)$ are nilpotent, with $m$ a prime power, say $p^n$. In particular, $G$ is a direct product of its Sylow-$p$ subgroup and some abelian $p'$-subgroup. So, it is sufficient to study finite $p$-groups of conjugate type $(1, p^n)$ for $p$ a prime and $n \geq 1$ an integer. It was proved by K. Ishikawa [5] that the nilpotency class of such finite $p$-groups is either 2 or 3.

By a theorem of P. Hall (see Section 2), any two isoclinic groups are of the same conjugate type. The study of finite $p$-groups of conjugate type $(1, p^n)$, up to isoclinism, was initiated by Ishikawa [4]. He classified such groups for $n \leq 2$. 

Received January 1, 2019
As a consequence, it follows that there is no finite $p$-group of nilpotency class 3 and conjugate type $(1,p)$, and there is a unique finite $p$-group, up to isoclinism, of nilpotency class 3 and conjugate type $(1,p^2)$. The classification, up to isoclinism, of finite $p$-groups of conjugate type $(1,p^3)$ was recently done in [8], wherein, among other results, it was observed that there is no finite $p$-group of nilpotency class 3 and of conjugate type $(1,p^3)$.

The examples of $p$-groups of nilpotency class 3 and of conjugate type $(1,p^{2m})$ are known for all $m \geq 1$. These examples appeared in the construction of certain Camina $p$-groups of nilpotency class 3 by Dark and Scoppola [1, pp. 796–797]. It can be shown that for a given integer $m \geq 1$ and a prime $p > 2$, the $p$-group of conjugate type $(1,p^{2m})$ and nilpotency class 3, constructed by Dark and Scoppola, is isomorphic to $\mathcal{H}_m / Z(\mathcal{H}_m)$, where $\mathcal{H}_m$ is presented as follows (see Section 4 for more details):

$$
\mathcal{H}_m = \left\{ \begin{bmatrix}
1 & & & \\
a & 1 & & \\
c & b & 1 & \\
d & ab - c & a & 1 \\
f & e & c & b & 1
\end{bmatrix} : a, b, c, d, e, f \in \mathbb{F}_{p^m} \right\}.
$$

(1.1)

In view of these examples, the question asked in [8] reduces to the following: Does there exist a finite $p$-group of nilpotency class 3 and of conjugate type $(1,p^n)$, for an odd prime $p$ and odd integer $n \geq 5$?

We answer this question, by proving the following much more general result.

**Main Theorem:** Let $p > 2$ be a prime and $n \geq 1$ an integer. Then there exist finite $p$-groups of nilpotency class 3 and conjugate type $(1,p^n)$ if and only if $n$ is even. For each positive even integer $n = 2m$, every finite $p$-group of nilpotency class 3 and of conjugate type $(1,p^n)$ is isoclinic to the group $\mathcal{H}_m / Z(\mathcal{H}_m)$, where $\mathcal{H}_m$ is as in (1.1).

**Notations.** We set some notations for a multiplicatively written finite group $G$ which are mostly standard. We denote the commutator subgroup of $G$ by $G'$ and the center of $G$ by $Z(G)$. The third term of the lower central series of $G$ is denoted by $\gamma_3(G)$. To say that $H$ is a subgroup of $G$, we write $H \leq G$. For a subgroup $H$ of $G$, $[G : H]$ denotes the index of $H$ in $G$. For the elements $x, y, z \in G$, the commutator $[x,y]$ of $x$ and $y$ is defined by $x^{-1}y^{-1}xy$, and $[x,y,z] = [[x,y],z]$. For a subgroup $H$ of $G$ and an element $x \in G$, by $C_H(x)$
we denote the centralizer of $x$ in $H$. The exponent of $G$ is denoted by $\exp(G)$. If $N$ is a normal subgroup of $G$, then the fact that $xy^{-1} \in N$ will be denoted by $x \equiv y \pmod{N}$. By $\mathbb{F}_p$ we denote the field of integers modulo $p$. By $U_n(q)$ we denote the group of $n \times n$ lower unitriangular matrices over the finite field of order $q$.

2. Reductions

In 1940, P. Hall [2] introduced the concept of isoclinism among groups. Let $X$ be a finite group and $\overline{X} = X/Z(X)$. Then commutation in $X$ gives a well defined map $a_X : \overline{X} \times \overline{X} \to X'$ such that

$$a_X(xZ(X), yZ(X)) = [x, y]$$

for $(x, y) \in X \times X$. Two finite groups $G$ and $H$ are said to be \textit{isoclinic}, if there exists an isomorphism $\phi$ of the factor group $\overline{G} = G/Z(G)$ onto $\overline{H} = H/Z(H)$, and an isomorphism $\theta$ of the subgroup $G'$ onto $H'$ such that the following diagram is commutative:

$$
\begin{array}{ccc}
\overline{G} \times \overline{G} & \xrightarrow{a_G} & G' \\
\downarrow{\phi \times \phi} & & \downarrow{\theta} \\
\overline{H} \times \overline{H} & \xrightarrow{a_H} & H'.
\end{array}
$$

Note that isoclinism is an equivalence relation among groups. Equivalence classes under this relation are called \textit{isoclinism families}. We recall the following two results of Hall.

**Proposition 2.1** ([2, p. 136]): Any two finite isoclinic groups are of the same conjugate type.

**Proposition 2.2** ([2, p. 135]): Let $G$ be a finite group. Then there exists a finite group $H$ in the isoclinism family of $G$ such that $Z(H) \leq H'$.

The following interesting result is due to I. M. Isaacs.

**Theorem 2.3** ([3, p. 501]): Let $G$ be a finite group, which contains a proper normal subgroup $N$ such that all of the conjugacy classes of $G$ which lie outside of $N$ have the same sizes. Then either $G/N$ is cyclic or every non-identity element of $G/N$ has prime order.
As an immediate consequence of the preceding result, we get

**Corollary 2.4:** For a prime \( p \) and an integer \( n \geq 1 \), let \( G \) be a finite \( p \)-group of conjugate type \((1, p^n)\). Then \( \exp(G/\mathbb{Z}(G)) = p \). In particular, if \( G \) is of nilpotency class \( > 2 \), then \( p > 2 \).

The following result is due to K. Ishikawa.

**Theorem 2.5** ([5, Main Theorem]): For a prime \( p \) and an integer \( n \geq 1 \), let \( G \) be a finite \( p \)-group of conjugate type \((1, p^n)\). Then the nilpotency class of \( G \) is either \( 2 \) or \( 3 \). As a consequence, \( G' \) is elementary abelian.

The preceding results reduce our study to the groups \( G \) satisfying

**Hypothesis (A1):** \( G \) is a finite \( p \)-group such that:

1. \( G \) is of conjugate type \((1, p^n)\), \( n \geq 2 \).
2. Nilpotency class of \( G \) is \( 3 \).
3. \( Z(G) \leq G' \).
4. \( p > 2 \).

### 3. Key results

In this section we determine some important invariants associated to a finite \( p \)-group satisfying Hypothesis (A1).

**Lemma 3.1:** Let \( G \) satisfy Hypothesis (A1). Then \([G' : \mathbb{Z}(G)] < p^n\).

**Proof.** Since the nilpotency class of \( G \) is \( 3 \), \( G' \) is abelian; hence by the given hypothesis, we have \( p^n = [G : C_G(h)] \leq [G : G'] \), where \( h \in G' \setminus \mathbb{Z}(G) \). Thus, we can assume \([G : G'] = p^{n+k}\), for some integer \( k \geq 0 \).

We proceed by the way of contradiction. Let \([G' : \mathbb{Z}(G)] = p^m\) and contrarily suppose that \( m \geq n \). Our plan is to count the cardinality of the following set in two different ways:

\[ X = \{(xG', y\mathbb{Z}(G)) \mid x \in G \setminus G', y \in G' \setminus \mathbb{Z}(G), [x, y] = 1\} \]

Since \( G' \) is abelian, it is easy to see that \( X \) is well-defined. Fix \( y\mathbb{Z}(G) \) with \( y \in G' \setminus \mathbb{Z}(G) \). Note that \( C_G(y) \supseteq G' \) and \([C_G(y) : G'] = p^k\). Thus for each of \( p^m - 1 \) choices of \( y\mathbb{Z}(G) \), there are exactly \( p^k - 1 \) choices of \( xG' \) such that \((xG', y\mathbb{Z}(G)) \in X\). Thus

\[ |X| = (p^m - 1)(p^k - 1) \]
On the other hand, fix $xG'$ with $x \in G \setminus G'$. If $[G' : G' \cap C_G(x)] \geq p^n$, then

$$[G' : G' \cap C_G(x)] = [G' : G' \cap C_G(x)] \geq p^n = [G : C_G(x)],$$

which implies that $G' C_G(x) = G$; hence $G = C_G(x)$ (since $G' \leq \Phi(G)$), a contradiction, where $\Phi(G)$ denotes the Frattini subgroup of $G$. Thus

$$[G' : G' \cap C_G(x)] \leq p^{n-1},$$

and $[G' \cap C_G(x) : Z(G)] \geq p^{m-(n-1)}$. Hence, for each of $p^{n+k} - 1$ choices of $xG'$, there are at least $p^{m-(n-1)} - 1$ choices of $yZ(G)$ such that $(xG', yZ(G)) \in X$, and we get

$$|X| \geq (p^{n+k} - 1)(p^{m-(n-1)} - 1).$$

The comparison of two estimates of $|X|$ gives us

$$(p^{n+k} - 1)(p^{m-(n-1)} - 1) \leq (p^m - 1)(p^k - 1),$$

which on simplification gives

$$p + p^m + p^k \leq 1 + p^{1-n-k} + p^{n-m} < 3,$$

a contradiction to the choice of $p$. Hence $[G' : Z(G)] < p^n$. \hfill \blacksquare

Before proceeding further, we recall the notion of breadth in $p$-groups. Let $G$ be a finite $p$-group. For $x \in G$, the **breadth** $b(x)$ of $x$ in $G$ is defined as

$$p^{b(x)} := [G : C_G(x)].$$

The **breadth** $b_G$ of $G$ is defined as

$$b_G := \max\{b(x) \mid x \in G\}.$$ 

Let $A$ be an abelian normal subgroup of $G$. Then, following [9], we define

$$p^{b_A(x)} := [A : C_A(x)],$$

$$b_A(G) := \max\{b_A(x) \mid x \in G\},$$

$$B_A(G) := \{x \in G \mid b_A(x) = b_A(G)\}.$$ 

For the ease of notation, we denote $B_A(G)$ by $B_A$.

**Lemma 3.2**: Let $G$ satisfy Hypothesis (A1). Then

$$B_{G'} = \{x \in G \mid C_{G'}(x) = Z(G)\} \quad \text{and} \quad \langle B_{G'} \rangle = G.$$
Proof. As in the preceding lemma, we can assume \([G : G'] = p^{n+k}\) for some integer \(k \geq 0\). Let \([G' : Z(G)] = p^m\). Then, by Lemma 3.1, \(m \leq n - 1\). Define
\[
T := \{x \in G \mid x \text{ commutes with some element } y \in G' \setminus Z(G)\}.
\]
Note that \(T = \bigcup C_G(h)\), where the union is taken over \(h \in G' \setminus Z(G)\); in fact, it is easy to see that the union can be taken over the non-trivial coset representatives of \(Z(G)\) in \(G'\).

Since \(G'\) is abelian, for each \(h \in G' \setminus Z(G)\), \(G' \leq C_G(h)\) and \(|C_G(h)| = |G'| p^k\). Thus,
\[
|T| \leq (p^m - 1)|G'| p^k < |G'| p^{m+k} \leq |G'| p^{n+k-1} < |G|.
\]
Consequently, \(T\) is a proper subset of \(G\), and therefore there exists an element \(x \in G \setminus G'\) such that \(C_G(x) = Z(G)\). Thus
\[
B_{G'} = \{x \in G \mid C_G(x) = Z(G)\} = G \setminus T.
\]
Let \(\langle B_{G'} \rangle = H\). If \(H < G\), then \(|H| \leq |G|/p = |G'| p^{n+k-1}\), and we have
\[
|G| = |T \cup B_{G'}| < |G'| p^{n+k-1} + |G'| p^{n+k-1} < |G'| p^{n+k} = |G|,
\]
which is a contradiction. Hence \(\langle B_{G'} \rangle = G\), which completes the proof.

As a consequence of the Hall–Witt identity, we get

**Lemma 3.3:** Let \(G\) be a group of nilpotency class 3 and let \(x, y, z \in G\) be such that \([x, z], [y, z] \in Z(G)\). Then
\[
[x, y, z] = 1,
\]
that is, \([x, y] \in G' \cap C_G(z)\).

**Lemma 3.4:** If \(G\) satisfies Hypothesis A1, then for all \(h \in G' \setminus Z(G)\),
\[
C_G(h) = C_G(G').
\]

**Proof.** We can assume that \([G : G'] = p^{n+k}\) and \([G' : Z(G)] = p^m\), for some integer \(k \geq 0\). By Lemma 3.1 and Lemma 3.2, we have \(m < n\) and there exists \(x \in G\) such that \(C_G(x) \cap G' = Z(G)\). There exists \(y \in G\) such that \([y, x] \notin Z(G)\) (otherwise, by Lemma 3.3, \(G' \subseteq Z(G)\), a contradiction). For such \(y\) (fixed), define
\[
\varphi_y : C_G(x)/Z(G) \to G'/Z(G), \quad uZ(G) \mapsto [u, y]Z(G),
\]
where \(u \in C_G(x)\). It is easy to see that \(\varphi_y\) is a well-defined homomorphism.

Let
\[
\ker \varphi_y = L/Z(G).
\]
CLAIM: $L$ centralizes $G'$ and $L = C_G(x) \cap C_G(G')$.

Since $\text{Im}(\varphi_y) \leq G'/Z(G)$, for the first part of the claim, it suffices to prove that $L$ centralizes element-wise every coset of $Z(G)$ in $\text{Im}(\varphi_y)$ and $\varphi_y$ is surjective.

Note that

$$C_G(x)/L \cong \text{Im}(\varphi_y) \leq G'/Z(G)$$

and $[C_G(x) : Z(G)] = p^{m+k}$. Consider any $v \in L$ and any $u \in C_G(x)$. Then we have $[v, u] \in C_G(x) \cap G' = Z(G)$ (by Lemma 3.3) and $[v, y] \in Z(G)$ (by the definition of $L$). Again by Lemma 3.3, we get that $v$ centralizes $[u, y]$ and hence also centralizes $[u, y]Z(G)$ element-wise for every $u \in C_G(x)$. This being true for every $v \in L$, it follows that $L$ centralizes element-wise every coset of $Z(G)$ in $\text{Im}(\varphi_y)$.

In particular, for $u = x$, we get that $L \subseteq C_G([x, y])$. Since $G'$ is abelian,

$$LG' \leq C_G([x, y]).$$

Note that $|\text{Im}(\varphi_y)| \leq p^m$ and $[L : Z(G)] \geq p^k$. Indeed, $|\text{Im}(\varphi_y)| = p^n$ if and only if $[L : Z(G)] = p^k$. Suppose $[L : Z(G)] > p^k$. Since $C_G(x) \cap G' = Z(G)$, so $L \cap G' = Z(G)$; hence

$$[LG' : Z(G)] = [L : Z(G)] [G' : Z(G)] > p^{k+m}.$$  

Consequently $p^n > [G : LG'] \geq [G : C_G([x, y])] = p^n$, which is absurd. Hence

$$[L : Z(G)] = p^k,$$

and consequently $|\text{Im}(\varphi_y)| = p^m$, that is, $\varphi_y$ is surjective and

$$C_G([x, y]) = LG'.$$

It now follows that $L$ centralizes $G'$.

Since $G'$ is abelian, $LG' \leq C_G(G') \leq C_G([x, y]) = LG'$; hence $LG' = C_G(G')$.

Now

$$C_G(x) \cap C_G(G') = C_G(x) \cap LG' = L,$$

as $C_G(x) \cap G' = Z(G)$ and $Z(G) \leq L \leq C_G(x)$. The proof of the claim is now complete.

For any $h \in G' \setminus Z(G)$, $C_G(h) \supseteq C_G(G') = C_G([x, y])$; it follows (by the given hypothesis) that $C_G(h) = C_G(G')$, and the proof of the lemma is complete.

Lemma 3.5: If $G$ satisfies Hypothesis A1, then $C_G(G') = G'$, and $[G : G'] = p^n$. 

Proof. We can start assuming that $[G' : Z(G)] = p^m$ and $[G : G'] = p^{n+k}$. It follows from Lemma 3.1 and Lemma 3.4 that $m < n$ and $[C_G(G') : G'] = p^k$ respectively. Consequently, $[G : C_G(G')] = p^n$. We first prove that $C_G(G') = G'$. On the contrary, suppose that $G'$ is a proper subgroup of $C_G(G')$. Consider the set

$$S = \{(xZ(G), yZ(G)) \mid x \in G \setminus C_G(G'), y \in C_G(G') \setminus G', [x, y] = 1\}.$$ 

It is easy to see that $S$ is well defined. We count in two ways the cardinality of $S$ to arrive at a contradiction.

Note that $xZ(G)$ with $x \in G \setminus C_G(G')$ has

$$(p^n - 1)|C_G(G')/Z(G)| = (p^n - 1)p^{m+k}$$

choices. We now fix $xZ(G)$ with $x \in G \setminus C_G(G')$. Since $C_G(G') = C_G(h)$ for any $h \in G' \setminus Z(G)$, $C_G(x) \cap G' = Z(G)$. Let $L$ be as in the proof of Lemma 3.4. Recall that $L = C_G(G') \cap C_G(x)$ and $|L/Z(G)| = p^k$. Note that $(xZ(G), yZ(G)) \in S$ if and only if

$$y \in (C_G(G') \setminus G') \cap C_G(x) = (C_G(G') \cap C_G(x)) \setminus (G' \cap C_G(x)) = L \setminus Z(G).$$

It follows that the non-trivial cosets of $Z(G)$ in $L$ give all possible $yZ(G)$ such that $(xZ(G), yZ(G))$ lie in $S$, and they are $p^k - 1$ in number. Therefore

$$|S| = (p^n - 1)p^{m+k}(p^k - 1).$$

On the other hand, $yZ(G)$ with $y \in C_G(G') \setminus G'$ has $(p^{k-1} - 1)p^m$ choices. Now for a fixed $yZ(G)$ with $y \in C_G(G') \setminus G'$, we count $xZ(G)$ with $x \in C_G(y) \setminus C_G(G')$. Since $C_G(y) \cap C_G(G')$ contains $\langle y, G' \rangle$ and $[C_G(y) : G'] = p^k$, we have

$$[C_G(y) : C_G(y) \cap C_G(G')] \leq p^{k-1}.$$ 

Hence for each $yZ(G)$ with $y \in C_G(G') \setminus G'$, there are at most

$$(p^{k-1} - 1)|\langle y, G' \rangle/ Z(G)| = (p^{k-1} - 1)p^{m+1}$$

choices of $xZ(G)$ such that $(xZ(G), yZ(G)) \in S$. Thus

$$|S| \leq (p^{k-1} - 1)p^m(p^k - 1)p^{m+1}.$$

Comparing the two estimates of $|S|$ and simplifying it, we get

$$(p^n - 1)p^k \leq p^m(p^k - p),$$

which is absurd, since $(p^n - 1) \geq p^m$ (by Lemma 3.1) and $p^k > p^k - p$. Hence $C_G(G') = G'$. By Lemma 3.4 the proof is complete. \qed
The following important information about centralizers of elements in \( G \) is an immediate consequence of the preceding two lemmas; we use it frequently without any further reference.

**Corollary 3.6:** If \( G \) satisfies Hypothesis (A1), then, for all \( x \in G \setminus G' \), the following hold:

1. \( C_G(x) \cap G' = Z(G) \).
2. \([C_G(x) : Z(G)] = [G' : Z(G)]\).

**Theorem 3.7:** Let \( G \) satisfy Hypothesis (A1) and \([G' : Z(G)] = p^m\) with \( m \geq 1 \). Then \( n = 2m \).

**Proof.** Consider \( x, y \in G \) with \([x, y] \notin Z(G)\).

**Case 1.** \( n > 2m \).

Write \( \overline{G} = G / Z(G) \). Since \( \overline{G} \) is of nilpotency class 2 and \(|\overline{G}'| = p^m\), we have

\[
[\overline{G} : C_{\overline{G}}(\overline{x})] \leq p^m \quad \text{and} \quad [\overline{G} : C_{\overline{G}}(\overline{y})] \leq p^m.
\]

Since \([\overline{G} : \overline{G}'] = p^n > p^{2m}\), there exists \( \overline{w} \notin \overline{G}' \) such that \( \overline{w} \in C_{\overline{G}}(\overline{x}) \cap C_{\overline{G}}(\overline{y}) \), that is, \([x, w], [y, w] \in Z(G)\). Since \( w \notin G' \), it follows from Lemma 3.3 that \([x, y] \in C_G(w) \cap G' = Z(G)\), a contradiction to our supposition that \([x, y] \notin Z(G)\).

**Case 2.** \( n < 2m \).

Since \( x \notin G' \), we have

\[
[C_G(x)G' : G'] = [C_G(x) : C_G(x) \cap G'] = [C_G(x) : Z(G)] = p^m,
\]

and similarly

\[
[C_G(y)G' : G'] = p^m.
\]

Since \( n < 2m \), we have \([G : G'] = p^n < p^{2m}\); hence \( C_G(x)G' \cap C_G(y)G' \) contains \( G' \) properly. Consider \( w \in C_G(x)G' \cap C_G(y)G' \) with \( w \notin G' \). Since \( G \) is of nilpotency class 3, it is easy to see that \([w, x], [w, y] \in Z(G)\); hence it follows from Lemma 3.3 that \([x, y] \in C_G(w) \cap G' = Z(G)\), a contradiction again.

Thus, the only possibility is \( n = 2m \), and the proof is complete.

Before proceeding further, we strengthen Hypothesis (A1) as follows:

**Hypothesis (A2):** \( G \) is a finite \( p \)-group such that

1. \( G \) is of conjugate type \((1, p^{2m})\), \( m \geq 1 \).
2. Nilpotency class of \( G \) is 3.
3. \( Z(G) \leq G' \).
4. \( p > 2 \).
A group $G$ is said to be a Camina group if $xG'$ coincides with the conjugacy class of $x$ in $G$ for all $x \in G \setminus G'$. For determining the structure of $G/\text{Z}(G)$ when $G$ satisfies Hypothesis (A2), the following result of Verardi [10] (also see [7, Lemma 1.2]) is crucial.

**Theorem 3.8:** For an odd prime $p$ and a positive integer $k$, let $G$ be a Camina $p$-group of order $p^{3k}$, exponent $p$ and nilpotency class $2$. Let $[G : G'] = p^{2k}$ and there be two elementary abelian subgroups $A^*, B^*$ of $G$ such that $G = A^*B^*$, $A^* = A \times G'$, $B^* = B \times G'$, and thus $G = ABG'$. Then the following statements are equivalent:

1. $G$ is isomorphic to $U_3(p^k)$.
2. All the centralizers of non-central elements of $G$ are abelian.

**Theorem 3.9:** Let $G$ satisfy Hypothesis (A2). Write

$$\overline{G} = G/\text{Z}(G) \quad \text{and} \quad \overline{x} = x\text{Z}(G)$$

for $x \in G$. Then the following hold:

1. $C_G(x)\overline{G}' = C_{\overline{G}}(\overline{x})$ and $|C_G(x)| = p^{2m}$ for $\overline{x} \in \overline{G} \setminus \overline{G}'$.
2. $\overline{G}$ is a Camina $p$-group of order $p^{3m}$, exponent $p$, and $|\overline{G}'| = p^m$.
3. All the centralizers of non-central elements in $\overline{G}$ are elementary abelian in order $p^{2m}$.
4. If $A = C_{\overline{G}}(\overline{x})$ and $B = C_{\overline{G}}(\overline{y})$, for $\overline{x}, \overline{y} \in \overline{G} \setminus \overline{G}'$, are distinct centralizers in $\overline{G}$, then $A \cap B = \text{Z}(\overline{G})$ and $\overline{G} = AB$.
5. $\overline{G}$ is isomorphic to $U_3(p^m)$.

**Proof.** (1) By Lemma 3.4 and Theorem 3.7,

$$[G : G'] = p^{2m} \quad \text{and} \quad [G' : \text{Z}(G)] = p^m;$$

hence

$$|\overline{G}| = p^{3m} \quad \text{and} \quad |\overline{G}'| = p^m.$$

Further, for $h \in G' \setminus \text{Z}(G)$, $C_G(h) = G'$.

Since $\overline{G}$ is of nilpotency class 2, $\overline{G}'$ is contained in the centralizer of every element in $\overline{G}$. Hence $C_{\overline{G}}(\overline{x})\overline{G}' \leq C_{\overline{G}}(\overline{x})$ for any $x \in G \setminus G'$. Since

$$[C_G(x) : \text{Z}(G)] = [G' : \text{Z}(G)] = p^m$$

with $C_G(x) \cap G' = \text{Z}(G)$, we get

$$[C_G(x)G' : \text{Z}(G)] = p^{2m} \quad \text{and} \quad [G : C_G(x)G'] = p^m.$$ 

Hence $[\overline{G} : C_{\overline{G}}(\overline{x})] \leq p^m$ and $|C_{\overline{G}}(\overline{x})| \geq p^{2m}$. 
Fix \( x \in G \setminus G' \). If possible, suppose that \( |C_G(\overline{x})| > p^{2m} \), that is,
\[
|\overline{G} : C_G(\overline{x})| < p^m.
\]
Note that \( \overline{x} \not\in Z(\overline{G}) \). For, let \( \overline{x} \in Z(\overline{G}) \). For any minimal generating set \( \{ x_1, \ldots, x_{2m} \} \) of \( G \), \( \{ \overline{x}_1, \ldots, \overline{x}_{2m} \} \) is also a minimal generating set for \( \overline{G} \). Then \( [\overline{x}, \overline{x}_i] = 1 \), that is \( [x, x_i] \in Z(G) \) for \( 1 \leq i \leq 2m \). Then by Lemma 3.3, for \( 1 \leq i \leq 2m \), \( [x_i, x_j] \in C_G(x) \cap G' = Z(G) \) (since \( x \notin G' \)); hence \( G' \subseteq Z(G) \), a contradiction. Thus, there exists \( t \in G \) such that \([t, x] \notin Z(G)\).

Since \( |\overline{G}| = p^m \), we have \( |\overline{G} : C_G(\overline{t})| \leq p^m \), and therefore it follows that \( C_G(\overline{x}) \cap C_G(\overline{t}) \) contains \( \overline{G} \) properly. Take \( \overline{w} \in (C_G(\overline{x}) \cap C_G(\overline{t})) \setminus \overline{G} \). Then \( [w, x], [w, t] \in Z(G) \) with \( w \notin G' \). By Lemma 3.3, \( [x, t] \in C_G(w) \cap G' = Z(G) \), a contradiction. Thus
\[
|C_G(\overline{x})| = p^{2m} = |C_G(x)G'|.
\]
This proves assertion (1).

(2) By Corollary 2.4, \( \exp(\overline{G}) = p \). Now the assertion (2) follows from assertion (1).

(3) Consider any \( x \in G \setminus G' \). For \( y_1, y_2 \in C_G(x) \), by Lemma 3.3,
\[
[y_1, y_2] \in C_G(x) \cap G' = Z(G).
\]
Hence \( [C_G(x), C_G(x)] \leq Z(G) \). Since \( G \) is of nilpotency class 3, we have
\[
[C_G(x)G', C_G(x)G'] = [C_G(x), C_G(x)] [C_G(x), G'] [G', G'] \leq Z(G),
\]
i.e., \( C_G(x) = C_G(x)G' \) is abelian. Since \( \overline{G} \) is of exponent \( p \), then so is \( C_G(\overline{x}) \).

(4) It is given that \( A = C_G(\overline{x}) \) and \( B = C_G(\overline{y}) \) are distinct proper subgroups of \( \overline{G} \), and are abelian by assertion (3). Thus for any element \( \overline{w} \in A \cap B \), it follows that
\[
|C_G(\overline{w})| \geq |AB| > p^{2m}.
\]
Hence, by (3), \( \overline{w} \in Z(\overline{G}) \). Since \( |\overline{G}| = p^{3m} \), \( |Z(\overline{G})| = p^m \) and \( |A| = |B| = p^{2m} \), we have \( \overline{G} = AB \).

(5) The assertion follows by (2)–(4) along with Theorem 3.8.

Using Theorem 3.9(1), the following result is an easy exercise.

**Corollary 3.10:** Let \( G \) satisfy Hypothesis (A2) and \( u, v \in G \setminus G' \) such that \( [u, v] \in Z(G) \). Then there exists an element \( h \in G' \) such that \( [u, vh] = 1 \). In particular, \( [u, v] \in \gamma_3(G) \).
As a consequence of the Hall–Witt identity, in a $p$-group $G$ of nilpotency class 3, we get

(3.11) If $[a, b] \in Z(G)$ then $[[a, t], b] = [[b, t], a]$ \hspace{1cm} (a, b, t \in G).

So far, we have shown that if $G$ satisfies Hypothesis (A2), then $[G : G'] = p^{2m}$ and $[G' : Z(G)] = p^m$. We conclude this section with the following interesting result on the order of $Z(G)$.

**PROPOSITION 3.12:** Let $G$ satisfy Hypothesis (A2). Then $Z(G) = \gamma_3(G)$, and is elementary abelian of order $p^{2m}$.

**Proof.** Since $G'$ is elementary abelian (by Theorem 2.5), so are $\gamma_3(G)$ and $Z(G)$. Consider $x_1 \in G \setminus G'$. Recall that

$C_G(x_1) \cap G' = Z(G), \quad [C_G(x_1) : Z(G)] = [G' : Z(G)] = p^m \quad \text{and} \quad [G : G'] = p^{2m}$.

Let

$$C_G(x_1) = \langle x_1, \ldots, x_m, Z(G) \rangle.$$  

Consider $y_1 \in G \setminus C_G(x_1)G'$. Let

$$C_G(y_1) = \langle y_1, \ldots, y_m, Z(G) \rangle.$$  

Then $C_G(y_1) = \langle y_1, \ldots, y_m, G' \rangle$ and $C_{G'}(y_1) = \langle \bar{y}_1, \ldots, \bar{y}_m, \bar{G'} \rangle$ are distinct proper centralizers of $\bar{G}$; hence, by Theorem 3.9(4), they generate $\bar{G}$. It follows that $\{x_1, \ldots, x_m, y_1, \ldots, y_m\}$ is a (minimal) generating set for $G$. Define

$$[x_1, y_i] = h_i \quad (1 \leq i \leq m).$$

By Theorem 3.9(2), $h_1, \ldots, h_m$ are independent modulo $Z(G)$, and

$$G' = \langle h_1, \ldots, h_m, Z(G) \rangle.$$  

Next define

$$[h_1, x_i] = z_i, \quad \text{and} \quad [h_1, y_i] = z_{m+i} \quad (1 \leq i \leq m).$$

Since $x_1, \ldots, x_m, y_1, \ldots, y_m$ are independent modulo $G' = C_G(h_1)$, it follows that

$$[h_1, x_1], \ldots, [h_1, x_m], [h_1, y_1], \ldots, [h_1, y_m]$$

are independent, and they generate a subgroup $K$ of order $p^{2m}$ in $\gamma_3(G)$.
We now proceed to show that $K = \gamma_3(G)$. It is sufficient to show that for any $h \in G' \setminus Z(G)$, $[h, x_i], [h, y_i] \in K$ for $1 \leq i \leq m$. For any $h \in G' \setminus Z(G)$ and fixed $i$ with $1 \leq i \leq m$, consider $[h, x_i]$. Let

$$A = \langle x_1, \ldots, x_m, Z(G) \rangle \quad \text{and} \quad B = \langle y_1, \ldots, y_m, Z(G) \rangle.$$ 

Since $\langle [x_1, y_1], \ldots, [x_1, y_m], Z(G) \rangle = G'$, there exists $y \in B$ such that

$$h \equiv [x_1, y] \pmod{Z(G)}.$$

Then, by (3.11),

$$[h, x_i] = [[x_1, y], x_i] = [[x_i, y], x_1].$$

Again, since $\langle [x_1, y_1], \ldots, [x_1, y_m], Z(G) \rangle = G'$, there exists $x \in A$ such that

$$[x_i, y] \equiv [x, y_1] \pmod{Z(G)}.$$

Therefore, again by (3.11), we get

$$[h, x_i] = [[x_i, y], x_1] = [[x_1, y_1], x_1] = [[x_1, y_1], x] = [h_1, x] \in K.$$

Similarly we can show that $[h, y_i] \in K$, $1 \leq i \leq m$; hence

$$K = \gamma_3(G)$$

and is of order $p^{2m}$.

It only remains to show that $Z(G) = \gamma_3(G)$. For this, since

$$[x_1, y_1], \ldots, [x_1, y_m]$$

are independent modulo $Z(G)$ and

$$G' = \langle [x_1, y_1], \ldots, [x_1, y_m], Z(G) \rangle,$$

it suffices to prove that

(3.13) \quad $G' = \langle [x_1, y_1], \ldots, [x_1, y_m], \gamma_3(G) \rangle$.

Note that $\gamma_3(G) \subseteq Z(G)$ and $\gamma_3(G) = \langle z_1, \ldots, z_{2m} \rangle$. Also

$$A = \langle x_1, \ldots, x_m, Z(G) \rangle = C_G(x_1) \quad \text{and} \quad B = \langle y_1, \ldots, y_m, Z(G) \rangle = C_G(y_1).$$

If (3.13) does not hold, then there exist $z \in Z(G) \setminus \gamma_3(G)$ and a commutator $[x_i, y_j]$ for some $i, j$ with $1 \leq i, j \leq m$, such that

$$[x_i, y_j] = [x_1, y_1]^{e_1} \cdots [x_1, y_m]^{e_m} z,$$
where \( e_i \in \mathbb{F}_p \) for \( 1 \leq i \leq m \). Let \( y = y_1^{e_1} \cdots y_m^{e_m} \). Then the preceding equation implies
\[
[x_i, y_j] \equiv [x_1, y]z \quad \text{(mod } \gamma_3(G))\).
\]
Now \([x_i, x_1] = 1\) and so
\[
[x_i y, x_1 y] \equiv [x_i, x_1][x_i, y_j][y, x_1][y, y_j] \equiv z[y, y_j] \quad \text{(mod } \gamma_3(G))\).
\]
Since \([y, y_j]\) and \([x_i y, x_1 y]\) lie in \(Z(G)\), by Corollary 3.10 both \([y, y_j]\) and \([x_i y, x_1 y]\) lie in \(\gamma_3(G)\). Consequently \(z \in \gamma_3(G)\), a contradiction.

This proves that (3.13) holds. Hence
\[
\gamma_3(G) = Z(G),
\]
and the proof is complete. \(\blacksquare\)

4. Examples

In this section, we describe the examples of \(p\)-groups of nilpotency class 3 and conjugate type \((1, p^{2m})\) from the construction by Dark and Scoppola [1].

Let \(\mathbb{F}_q\) denote the field of order \(q = p^m\) for \(p\) an odd prime and \(m \geq 1\). On the set \(G\) of quintuples \((a, b, c, d, e)\) over \(\mathbb{F}_q\), define an operation \(\cdot\) as follows. For any two quintuples \((a, b, c, d, e)\) and \((x, y, z, u, v)\), define \((a, b, c, d, e) \cdot (x, y, z, u, v)\) to be the quintuple
\[
(a + x, b + y, c + z + bx, d + u + az + (ab - c)x, e + v + cy + b(xy - z)).
\]
A routine check shows that \(G\) is a group under this operation, in which \((0, 0, 0, 0, 0)\) is the identity element and we denote it by \(0\), and
\[
(a, b, c, d, e)^{-1} = (-a, -b, -c + ab, -d, -e).
\]
Then \((a, b, c, d, e) \cdot (x, y, z, u, v) \cdot (a, b, c, d, e)^{-1} \cdot (x, y, z, u, v)^{-1}\) is the quintuple
\[
(0, 0, bx - ay, 2az - 2cx + a^2y - bx^2, 2(c - ab)y - 2b(z - xy) - ay^2 + b^2x).
\]
It is easy to see that:

1. \(G' = \{(0, 0, c, d, e) \mid c, d, e \in \mathbb{F}_q\}\).
2. \(\gamma_3(G) = \{(0, 0, 0, d, e) \mid d, e \in \mathbb{F}_q\} = Z(G)\).

Consider \((0, 0, c, d, e) \in G' \setminus Z(G)\). Then \(c \neq 0\). If
\[
[(0, 0, c, d, e), (x, y, z, u, v)] = 0,
\]
then by the commutator formula above, $-2cx = 2cy = 0$. Since the characteristic of $\mathbb{F}_q$ is odd and $c \neq 0$, we get $x = y = 0$. Noting that $G'$ is abelian, it follows that the centralizer of any element of $G' \setminus Z(G)$ is $G'$, which has index $q^2 = p^{2m}$ in $G$.

Next fix $g = (a, b, c, d, e)$ with $(a, b) \neq (0, 0)$. Then $(x, y, z, u, v)$ centralizes $g$ if and only if

\begin{align*}
(4.1) & \quad bx - ay = 0, \\
(4.2) & \quad 2az - 2cx + a^2y - bx^2 = 0, \\
(4.3) & \quad 2(c - ab)y - 2b(z - xy) - ay^2 + b^2x = 0.
\end{align*}

Suppose $a \neq 0$. For arbitrary $x, u, v \in \mathbb{F}_q$, we see that $y$ is uniquely determined from (4.1), and then $z$ is uniquely determined from (4.2). Further, it is easy to see that the unique values of $y$ and $z$ satisfy (4.3). Hence the centralizer of $(a, b, c, d, e)$ has order $q^3 = p^{3m}$, and therefore has index $p^{2m}$ in $G$. Similarly, if $a = 0$ and $b \neq 0$, then it follows that the centralizer of $(a, b, c, d, e)$ in $G$ has index $p^{2m}$. Hence $G$ is of conjugate type $(1, p^{2m})$.

We show that the group $G$ has a nice description in terms of a matrix group over $\mathbb{F}_q$. Consider the following collection of unitriangular matrices over $\mathbb{F}_q$:

\[
H_m = \left\{ \begin{bmatrix} 1 \\ a \\ c \\ d \\ f \\ \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ a \\ f \\ \end{bmatrix} : a, b, c, d, e, f \in \mathbb{F}_q \right\}.
\]

It is easy to see that $H_m$ is a subgroup of $U_5(q)$. Denote the general element of $H_m$ by $(a, b, c, d, e, f)$. An easy computation shows that

\[
Z(H_m) = \{(0, 0, 0, 0, 0, f) \mid f \in \mathbb{F}_q\}.
\]

Therefore, we have a natural homomorphism $H_m \to H_m/Z(H_m)$, in which we identify

\[
(a, b, c, d, e, f)Z(H_m) \longleftrightarrow (a, b, c, d, e).
\]

Then one can check that the product $(a, b, c, d, e)(x, y, z, u, v)$ in $H_m/Z(H_m)$ is the same as $(a, b, c, d, e)(x, y, z, u, v)$ in $G$. Hence $H_m/Z(H_m)$ is isomorphic to $G$, and therefore is of nilpotency class 3 and conjugate type $(1, p^{2m})$. 
As a conclusion of the preceding discussion, we obtain

**Theorem 4.4:** For any even integer \( n \geq 1 \) and an odd prime \( p \), there exists a finite \( p \)-group of nilpotency class 3 and conjugate type \((1, p^n)\).

**5. Proof of Main Theorem**

Let \( G \) be a \( p \)-group of nilpotency class 3 such that \( G/Z(G) \) is isomorphic to the group \( U_3(p^m) \). Our strategy for proving Main Theorem is to obtain presentations of groups \( G \) satisfying Hypothesis (A2) from a presentation of \( U_3(p^m) \); then we proceed to show that the groups, given by the presentations obtained, belong to the same isoclinism family.

We start with finding some structure constants of \( U_3(p^m) \). Let \( \mathbb{F}_{p^m} \) denote the field of order \( p^m \). Then

\[
\mathbb{F}_{p^m} = \mathbb{F}_p(\alpha),
\]

where \( \alpha \) satisfies a monic irreducible polynomial of degree \( m \) over \( \mathbb{F}_p \). Consider the following matrices in \( U_3(p^m) \) for any integer \( i \geq 1 \):

\[
X_i = \begin{bmatrix} 1 & 1 \\ 0 & \alpha^i \end{bmatrix}, \quad Y_i = \begin{bmatrix} 1 & \alpha^{i-1} \\ 0 & 0 \end{bmatrix}, \quad H_i = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.
\]

Then it is easy to see that

\[
\{X_1, \ldots, X_m, Y_1, \ldots, Y_m\}
\]

is a minimal generating set for \( U_3(p^m) \) and \( \{H_1, \ldots, H_m\} \) is a minimal generating set for the center (as well as the commutator subgroup) of \( U_3(p^m) \). Further, these matrices satisfy the following relations:

\[
(5.1) \quad X_i^p = Y_i^p = H_i^p = 1,
\]

\[
(5.2) \quad [X_i, X_j] = [Y_i, Y_j] = 1,
\]

\[
(5.3) \quad [H_i, X_j] = [H_i, Y_j] = 1,
\]

\[
(5.4) \quad [X_i, Y_j] = H_{i+j-1} \quad \text{for all } i, j \geq 1.
\]

Since \( \mathbb{F}_p(\alpha) \) is a vector space over \( \mathbb{F}_p \) with basis

\[
(1, \alpha, \ldots, \alpha^{m-1}),
\]
for $\alpha^{i+j-2} \in \mathbb{F}_p(\alpha)$, there exist unique $\kappa_{i,j,1}, \ldots, \kappa_{i,j,m} \in \mathbb{F}_p$ such that

$$\alpha^{i+j-2} = \kappa_{i,j,1} + \kappa_{i,j,2} \alpha + \cdots + \kappa_{i,j,m} \alpha^{m-1}.$$ 

Then, by (5.4), we have

$$H_{i+j-1} = H_1^{\kappa_{i,j,1}} H_2^{\kappa_{i,j,2}} \cdots H_m^{\kappa_{i,j,m}} = [X_1, Y_1^{\kappa_{i,j,1}} Y_2^{\kappa_{i,j,2}} \cdots Y_m^{\kappa_{i,j,m}}],$$

which in turn implies that

$$(5.5) \quad [X_i, Y_j] = [X_1, Y_1^{\kappa_{i,j,1}} Y_2^{\kappa_{i,j,2}} \cdots Y_m^{\kappa_{i,j,m}}] \quad (1 \leq i, j \leq m).$$

The constants $\kappa_{i,j,l}$ for $1 \leq i, j, l \leq m$, which we call the structure constants of $U_3(p^m)$, will be frequently used in the remaining part of the paper. Since the irreducible polynomial of $\alpha$ depends on both $p$ and $m$, so do the structure constants $\kappa_{i,j,l}$ for $1 \leq i, j, l \leq m$.

The generators $X_i, Y_i, H_i, 1 \leq i \leq m$, the constants $\kappa_{i,j,l}$, and the relations (5.1)–(5.5) give a presentation of the group $U_3(p^m)$. From (5.4), it follows that

$$[X_i, Y_j] = [X_j, Y_i]$$

for all $i, j \geq 1$, and so

$$(5.6) \quad \kappa_{i,j,l} = \kappa_{j,i,l}.$$ 

Also, combining (5.5) with the relation

$$[X_i, Y_j] = [X_j, Y_i],$$

we obtain

$$(5.7) \quad [X_j, Y_i] = [X_1^{\kappa_{i,j,1}} X_2^{\kappa_{i,j,2}} \cdots X_m^{\kappa_{i,j,m}}, Y_1] \quad (1 \leq i, j \leq m).$$

We now build up a presentation of a finite $p$-group $G$ such that

$$G/\text{Z}(G) \cong U_3(p^m).$$

**Lemma 5.8**: Fix a prime $p > 2$ and an integer $m \geq 2$. Let $H$ be a $p$-group of nilpotency class 3 and of conjugate type $(1, p^2m)$. Then there exist

$$\alpha_{i,j,l}, \beta_{i,j,l}, \gamma_{i,j,l}, \delta_{i,j,l}, \lambda_{i,j,l}, \mu_{i,j,l}, \epsilon_{i,l}, \nu_{i,l} \in \mathbb{F}_p \quad (1 \leq i, j \leq m, 1 \leq l \leq 2m),$$
such that $H$ is isoclinic to the group $G$ admitting the following presentation:

$$G = \langle x_1, \ldots, x_m, y_1, \ldots, y_m, h_1, h_2, \ldots, h_m, z_1, z_2, \ldots, z_{2m} \rangle$$

(R0) \quad x_i^p = \prod_{l=1}^{2m} z_{i,l}^{\kappa_{i,l}}, \quad y_i^p = \prod_{l=1}^{2m} z_{i,l}^{\nu_{i,l}}, \quad h_i^p = 1 (1 \leq i \leq m), \quad z_i^p = 1 (1 \leq i \leq 2m),

(R1) \quad [z_k, z_r] = [z_k, x_i] = [z_k, y_i] = [z_k, h_i] = 1 (1 \leq k, r, \leq 2m, 1 \leq i \leq m),

(R2) \quad [h_i, h_j] = 1 (1 \leq i, j \leq m),

(R3) \quad [h_i, x_j] = \prod_{l=1}^{2m} z_{i,j,l}^{\gamma_{i,j,l}} (1 \leq i, j \leq m),

(R4) \quad [h_i, y_j] = \prod_{l=1}^{2m} z_{i,j,l}^{\delta_{i,j,l}} (1 \leq i, j \leq m),

(R5) \quad [x_i, x_j] = \prod_{l=1}^{2m} z_{i,j,l}^{\alpha_{i,j,l}} (1 \leq i, j \leq m),

(R6) \quad [y_i, y_j] = \prod_{l=1}^{2m} z_{i,j,l}^{\beta_{i,j,l}} (1 \leq i, j \leq m),

(R7) \quad [x_i, y_j] = [x_1, y_1^{\kappa_{i,j,1}} y_2^{\kappa_{i,j,2}} \cdots y_m^{\kappa_{i,j,m}}] \prod_{l=1}^{2m} z_{i,j,l}^{\lambda_{i,j,l}} (1 \leq i, j \leq m),

(R8) \quad [x_j, y_i] = [x_1^{\kappa_{i,j,1}} x_2^{\kappa_{i,j,2}} \cdots x_m^{\kappa_{i,j,m}}, y_i] \prod_{l=1}^{2m} z_{i,j,l}^{\mu_{i,j,l}} (1 \leq i, j \leq m),

(R9) \quad [x_1, y_i] = h_i, \quad [h_1, x_i] = z_i, \quad [h_1, y_i] = z_{m+i} (1 \leq i \leq m),

where $\kappa_{i,j,l}, 1 \leq i, j, l \leq m$, are the structure constants of $U_3(p^m)$.

**Proof.** By Propositions 2.1 and 2.2, $H$ is isoclinic to a group $G$ satisfying hypothesis (A1). Then by Lemma 3.4, Theorem 3.7 and Proposition 3.12,

$$[G : G'] = p^{2m}, \quad [G' : Z(G)] = p^m, \quad |Z(G)| = p^{2m}.$$

The desired presentation of $G$ is obtained from the presentation of $G/Z(G)$ ($\cong U_3(p^m)$), described just before the lemma. Note, by Theorem 2.5, that $G'$ is elementary abelian.
Since $|Z(G)| = p^{2m}$ and $Z(G)$ is of exponent $p$, $Z(G)$ is minimally generated by $2m$ elements $z_1, z_2, \ldots, z_{2m}$ (say). Let $\varphi : G \to U_3(p^m)$ denote a surjective homomorphism with $\ker \varphi = Z(G)$. Note that $X_i$’s, $Y_i$’s and $H_i$’s are the generators of $U_3(p^m)$.

Choose $x_1, \ldots, x_m, y_1, \ldots, y_m, h_1, \ldots, h_m$ in $G$ such that
\[
\varphi(x_i) = X_i, \quad \varphi(y_i) = Y_i \quad \text{and} \quad \varphi(h_i) = H_i \quad (1 \leq i \leq m).
\]
It follows that the set
\[
\{x_1, \ldots, x_m, y_1, \ldots, y_m, h_1, h_2, \ldots, h_m, z_1, z_2, \ldots, z_{2m}\}
\]
generates $G$, and the set
\[
\{h_1, h_2, \ldots, h_m, z_1, z_2, \ldots, z_{2m}\}
\]
generates $G'$.

Since $\varphi(x_i^p) = 1$, $1 \leq i \leq m$, there exist some $\epsilon_{i,l} \in \mathbb{F}_p$, $1 \leq l \leq 2m$, such that
\[
x_i^p = \prod_l z_i^{\epsilon_{i,l}}.
\]
Similarly there exist some $\nu_{i,l} \in \mathbb{F}_p$, $1 \leq l \leq 2m$, such that
\[
y_i^p = \prod_l z_i^{\nu_{i,l}}
\]
for $1 \leq i \leq m$. Since $G'$ is elementary abelian, we get $h_i^p = 1$, $[h_i, h_j] = 1$, $1 \leq i, j \leq m$ and $z_i^p = 1$, $1 \leq i \leq 2m$. This gives all the relations in (R0) and (R2). Since $z_i \in Z(G)$, the relations (R1) are the obvious commutator relations of $z_i$’s with the other generators of $G$. The relations (5.2), (5.3), (5.5) and (5.7) of $U_3(p^m)$ give the relations (R3)–(R8) for some $\alpha$’s, $\beta$’s, $\gamma$’s, $\delta$’s, $\lambda$’s and $\mu$’s in $\mathbb{F}_p$.

It remains to obtain relations (R9). Since, for $1 \leq i \leq m$, $[X_1, Y_i] = H_i$, by the choice of $x_1$, $y_i$ and $h_i$, we have
\[
[x_1, y_i] \equiv h_i \pmod{Z(G)}.
\]
Thus $[x_1, y_i] = h_iw_i$ for some $w_i \in Z(G)$. Replacing $h_i$ by $h_iw_i$, which do not violate any of the preceding relations, we can assume, without loss of generality, that
\[
(5.9) \quad [x_1, y_i] = h_i \quad (1 \leq i \leq m).
\]
Finally, we have $h_1 \in G' \setminus \mathbb{Z}(G)$. Further, $G$ is of conjugate type $(1, p^{2m})$, and $[G : G'] = p^{2m}$ with $G'$ abelian. Therefore 

$$C_G(h_1) = G'.$$

Since $x_1, \ldots, x_m, y_1, \ldots, y_m$ are independent modulo $C_G(h_1) = G'$, it follows that the $2m$ commutators

$$[h_1, x_1], \ldots, [h_1, x_m], [h_1, y_1], \ldots, [h_1, y_m]$$

are independent, and they belong to $\gamma_3(G) = \mathbb{Z}(G)$, which is elementary abelian of order $p^{2m}$. Thus, without loss of generality, we can take $[h_1, x_i] = z_i$ and $[h_1, y_i] = z_{m+i}$ for $1 \leq i \leq m$. This, along with (5.9), gives relations (R9).

**Theorem 5.10:** Given an even integer $2m \geq 2$ and an odd prime $p$, there is a unique finite $p$-group satisfying Hypothesis (A2), up to isoclinism. In particular, such a group is isoclinic to the group $\mathcal{H}_m/\mathbb{Z}(\mathcal{H}_m)$.

Assuming the preceding theorem, we are now ready to present

**Proof of Main Theorem.** For an integer $n \geq 1$ and a prime $p$, let $G$ be a finite $p$-group of nilpotency class 3 and of conjugate type $(1, p^n)$. In view of Propositions 2.1 and 2.2, we can assume that $\mathbb{Z}(G) \leq G'$. Then, by Theorem 3.7, $n$ is even. Conversely, if $n \geq 1$ is an even integer and $p$ is an odd prime, then, that there exists a finite $p$-group of nilpotency class 3 and of conjugate type $(1, p^n)$, follows from Theorem 4.4. This proves the first assertion of Main Theorem. The second one is Theorem 5.10.

The rest of this section is devoted to the proof of Theorem 5.10.

**Notation:** Throughout, for a prime $p$, and integer $m \geq 1$, $G$, which depends on $\alpha, \beta, \gamma, \delta, \lambda, \mu, \epsilon, \nu \in \mathbb{F}_p$, always denotes a group of conjugate type $(1, p^{2m})$, admitting the presentation as in Lemma 5.8.

For $m = 1$, Theorem 5.10 has been proved by Ishikawa in [4, Theorem 4.2]. Thus, assume that $m \geq 2$. Further, let the homomorphism $\varphi : G \rightarrow U_3(p^m)$,

$$x_i \mapsto X_i, \quad y_i \mapsto Y_i, \quad \text{and} \quad h_i \mapsto H_i$$

be as in the proof of Lemma 5.8.

First, we proceed to show that there is a unique choice for $\alpha$’s, $\beta$’s, $\gamma$’s, $\delta$’s, $\lambda$’s and $\mu$’s for which the group $G$ considered in Lemma 5.8 is of conjugate type $(1, p^{2m})$. We start with simplifying the relations of $G$ without any loss of generality.
**Lemma 5.11:** We can choose generators $x_j$'s and $y_j$'s of $G$ such that

$$ [x_1, x_j] = [y_1, y_j] = 1 \quad (2 \leq j \leq m). $$

**Proof.** Fix $j$ with $2 \leq j \leq m$. Since $x_1, x_j \notin G'$ and $[x_1, x_j] \in Z(G)$, by Corollary 3.10, there exists $h_j \in G'$ such that $[x_1, x_j h_j] = 1$. Thus replacing $x_j$ by $x_j h_j$, if necessary, we can assume that $[x_1, x_j] = 1$. Similarly, we can choose $y_j$'s such that $[y_1, y_j] = 1$.

**Theorem 5.12:** In the group $G$ in Lemma 5.8, for $1 \leq i, j \leq m$, we have

$$ [h_i, x_j] = [h_j, x_i] = z_1^{K_{i,j,1}} z_2^{K_{i,j,2}} \cdots z_m^{K_{i,j,m}} $$

and

$$ [h_i, y_j] = [h_j, y_i] = z_{m+1}^{K_{i,j,1}} z_{m+2}^{K_{i,j,2}} \cdots z_{2m}^{K_{i,j,m}}. $$

In particular, $\gamma$'s and $\delta$'s (in the relations (R3) and (R4)) are uniquely determined by the structure constants $\kappa_{i,j,l}$ of $U_3(p^m)$.

**Proof.** Since $H_i = [X_1, Y_i]$ in $U_3(p^m)$ for $1 \leq i \leq m$, we get $h_i \equiv [x_1, y_i] \pmod{Z(G)}$ in $G$. Therefore

$$ [h_i, x_j] = [[x_1, y_i], x_j]. $$

As $[x_1, x_j] = 1 \in Z(G)$, by (3.11), we get

$$ [h_i, x_j] = [[x_1, y_i], x_j] = [[x_j, y_i], x_1]. $$

From the relation (R8),

$$ [x_j, y_i] \equiv [x_1^{K_{i,j,1}} x_2^{K_{i,j,2}} \cdots x_m^{K_{i,j,m}}, y_1] \pmod{Z(G)}. $$

Consequently, using the fact that $[x_1, x_1^{K_{i,j,1}} x_2^{K_{i,j,2}} \cdots x_m^{K_{i,j,m}}] = 1 \in Z(G)$, again by (3.11), we get

$$ [h_i, x_j] = [x_j, y_i, x_1] = [x_1^{K_{i,j,1}} x_2^{K_{i,j,2}} \cdots x_m^{K_{i,j,m}}, y_1, x_1] $$

$$ = [x_1, y_1, x_1^{K_{i,j,1}} x_2^{K_{i,j,2}} \cdots x_m^{K_{i,j,m}}] $$

$$ = [h_1, x_1^{K_{i,j,1}} x_2^{K_{i,j,2}} \cdots x_m^{K_{i,j,m}}] $$

$$ = z_1^{K_{i,j,1}} z_2^{K_{i,j,2}} \cdots z_m^{K_{i,j,m}}. $$

Since the structure constants $\kappa_{i,j,l}$ are symmetric in $i, j$ (see (5.6)), $[h_i, x_j] = [h_j, x_i]$. This proves the first assertion of the Lemma, and the second one goes on the same lines. $lacksquare$

As an immediate consequence of the preceding result, we have
Corollary 5.13: Consider the elements
\[ x = x_1^{a_1} \cdots x_m^{a_m}, \quad x' = x_1^{b_1} \cdots x_m^{b_m}, \quad y = y_1^{c_1} \cdots y_m^{c_m} \quad \text{and} \quad y' = y_1^{d_1} \cdots y_m^{d_m} \]
in the group \( G \) in Lemma 5.8. If
\[ [x, y, x'] = 2^m \prod_{l=1}^{2m} z_l^{r_l} \quad \text{and} \quad [y, x, y'] = 2^m \prod_{l=1}^{2m} z_l^{s_l}, \]
for some \( r_l, s_l \in \mathbb{F}_p \), then the values of \( r_l \) and \( s_l \) are uniquely determined by the structure constants of \( U_3(p^m) \) and, respectively, by \( a_i \)'s, \( b_i \)'s, \( c_i \)'s and \( a_i \)'s, \( c_i \)'s, \( d_i \)'s.

Next we show the uniqueness of \( \lambda \)'s and \( \mu \)'s.

Lemma 5.14: In the group \( G \), for \( 1 \leq i, j \leq m \), we have
\[ [x_i, x_j] \in \langle z_1, \ldots, z_m \rangle \quad \text{and} \quad [y_i, y_j] \in \langle z_{m+1}, \ldots, z_{2m} \rangle. \]

Proof. Fix \( i, j \) with \( 1 \leq i, j \leq m \). Since \([x_i, x_j] \in Z(G)\), by Corollary 3.10, there exists \( h \in G' \) (depending on \( x_i, x_j \)) such that \([x_i, x_j, h] = 1\). Then
\[ [x_i, x_j] = [x_i, h]^{-1} = [h, x_i]. \]

Since \( G' = \langle h_1, h_2, \ldots, h_m, Z(G) \rangle \), by Theorem 5.12, \([h, x_i] \in \langle z_1, \ldots, z_m \rangle\), proving the first assertion. The second assertion follows on the same lines. \( \blacksquare \)

Before proceeding further, we recall the following commutator identities in a finite \( p \)-group \( G \) of nilpotency class 3 with \( p \) odd, which will be used in the computations without any further reference. Noting that \( G' \) is abelian, the ordering of commutators is immaterial. For \( a, b, c \in G \),

\begin{enumerate}
  \item \([a, b, c] = [a, c][b, c][a, c, b] \quad \text{and} \quad [a, bc] = [a, b][a, c][a, b, c], \]
  \item \([a^i, b^j, c^k] = [a, b, c]^{ijk} \quad \text{(since} \ G \ \text{is of nilpotency class} \ 3), \]
  \item \([a^s, b] = [a, b]^s[a, b, a]^\frac{s(s-1)}{2} \quad \text{and} \quad [a, b^s] = [a, b]^s[a, b, b]^\frac{s(s-1)}{2} \quad (s \in \mathbb{F}_p),\]
\end{enumerate}
where \( \left( \frac{s}{2} \right) = \frac{s(s-1)}{2} \) in \( \mathbb{F}_p, p > 2 \).

Lemma 5.15: For \( x = x_1^{a_1} \cdots x_m^{a_m} \) and \( y = y_1^{a_1} \cdots y_m^{a_m} \) in \( G \), the following hold:

\begin{enumerate}
  \item \([x_1, y] \equiv [x, y_1] \pmod{Z(G)} \).
  \item If \([x_1, y] = [x, y_1] \prod_{l=1}^{2m} z_l^{c_l} \), then \( c_l \)'s are uniquely determined by \( a_i \)'s and the structure constants of \( U_3(p^m) \).
\end{enumerate}
Proof. If $a_i = 0$ for all $i$, then $x = y = 1$, and so $c_i = 0$ for all $i$; there is nothing to prove. Thus, assume that not all $a_i$’s are 0. In $U_3(p^n)$, consider $X = X_1^{a_1} \cdots X_m^{a_m}$ and $Y = Y_1^{a_1} Y_2^{a_2} \cdots Y_m^{a_m}$. Since $[X_i, Y_j] = [X_j, Y_i]$ for all $i, j$ (by (5.4)), we have $[X_1, Y] = [X, Y_1]$; hence $[x_1, y] \equiv [x, y_1] \pmod{Z(G)}$ in $G$. This proves assertion (1).

We prove assertion (2) in two steps, as the arguments of Step 1 will be used further.

**Step 1.** For $m + 1 \leq l \leq 2m$, $c_l$ is uniquely determined by the structure constants of $U_3(p^m)$.

With $X, Y$ as in the proof of assertion (1), we have $[X_1, Y] = [X, Y_1]$, which implies that $[X_1 Y_1^r, XY^r] = 1$ for any $r \in \mathbb{F}_p$; hence, in $G$, we get

$$[x_1 y_1^r, xy^r] \equiv 1 \pmod{Z(G)}.$$

By Corollary 3.10, there exists an element $h(r)$, depending on $r$, in $G'$ such that

$$[x_1 y_1^r, xy^r h(r)] = 1.$$

Since $[x_1, x] = [y_1, y] = 1$ (see Lemma 5.11), we have

$$1 = [x_1 y_1^r, xy^r h(r)]$$

$$= [x_1, y]^r [x_1, y, y_1]^{(2)} [x_1, y_1]^{r^2} [x_1, h(r)] [y_1, x]^{r^2} [y_1, x, y_1]^{(2)} [y_1, y]^{r^2} [y_1, h(r)].$$

Consequently, by the given hypothesis, we get

$$\left( \prod_{l=1}^{2m} z_l^{c_l} \right)^{-r}$$

$$= ([x_1, y]^{r^2} [y_1, x]^{r^2} [y_1, x, y_1]^{(2)} [y_1, y]^{r^2} [y_1, h(r)])^r.$$

By Theorem 5.12, $[G', y], [G', y_1]$ are subgroups of $\langle z_{m+1}, \ldots, z_{2m} \rangle$ and

$$[x_1, h(r)] \in \langle z_1, \ldots, z_m \rangle;$$

hence all commutators on the right side of (5.16), except $[x_1, h(r)]$, belong to $\langle z_{m+1}, \ldots, z_{2m} \rangle$. Thus

$$\left( \prod_{l=1}^{m} z_l^{-c_l} \right)^r = [x_1, h(r)].$$
and
\[
\left( \prod_{l=m+1}^{2m} z_l^{-c_l} \right)^r = [x_1, y, y]^{(2)}[x_1, y, y_1]^{r^2} [y_1, x, y_1]^{(2)} [y_1, x, y]^{r^2} [y_1, h(r)]^r.
\]

Since, by Theorem 5.12, \( z_i = [h_1, x_i] = [h_i, x_1] \) for \( 1 \leq i \leq m \), we have
\[
\prod_{l=1}^{m} z_l^{-c_l} = \prod_{l=1}^{m} [x_1, h_l]^{c_l} = [x_1, h_1^{c_1} \cdots h_m^{c_m}] = [x_1, \tilde{h}],
\]
where \( \tilde{h} = h_1^{c_1} \cdots h_m^{c_m} \), which is independent of \( r \). Then from (5.17) we get
\[
[x_1, h(r)] = [x_1, \tilde{h}]^r,
\]
which implies that \( \tilde{h}^r h(r)^{-1} \in C_G(x_1) \cap G' = Z(G) \). Hence
\[
h(r) \equiv \tilde{h}^r \pmod{Z(G)}.
\]

Using this in (5.18), we get
\[
\left( \prod_{l=m+1}^{2m} z_l^{-c_l} \right)^r = [x_1, y, y]^{(2)}[x_1, y, y_1]^{r^2} [y_1, x, y_1]^{(2)} [y_1, x, y]^{r^2} [y_1, \tilde{h}]^{r^2}.
\]

Since this equation holds for all \( r \in \mathbb{F}_p \), for \( r = 1 \) and \( r = -1 \), we, respectively, get
\[
\prod_{l=m+1}^{2m} z_l^{-c_l} = [x_1, y, y_1][y_1, x, y][y_1, \tilde{h}]
\]
and
\[
\prod_{l=m+1}^{2m} z_l^{c_l} = [x_1, y, y][x_1, y, y_1][y_1, x, y_1][y_1, x, y][y_1, \tilde{h}].
\]

From these equations, we obtain
\[
\prod_{l=m+1}^{2m} z_l^{2c_l} = [x_1, y, y][y_1, x, y_1].
\]

By Corollary 5.13, the right hand side of the preceding equation is uniquely determined by \( a_i \)'s and the structure constants of \( U_3(p^m) \), so are \( c_l \) for \( m + 1 \leq l \leq 2m \).
Step 2. For \(1 \leq l \leq m\), \(c_l\) is uniquely determined by the structure constants of \(U_3(p^m)\).

With \(X, Y\) as in the proof of assertion (1), we have \([Y, X_1] = [Y_1, X]\), which implies that \([Y_1X_r, YX^r] = 1\) for any \(r \in \mathbb{F}_p\); hence, in \(G\), we get
\[
[y_1x_1^r, yx^r] \equiv 1 \pmod{Z(G)}.
\]
By Corollary 3.10, there exists an element \(k(r)\), depending on \(r\), in \(G'\) such that
\[
[y_1x_1^r, yx^r k(r)] = 1.
\]
With appropriate modifications in Step (1), it follows that \(c_l\) for \(1 \leq l \leq m\) are uniquely determined by \(a_i\)’s and the structure constants of \(U_3(p^m)\).

Finally by Step 1 and Step 2, \(c_l\) for \(1 \leq l \leq 2m\) are uniquely determined by the \(a_i\)’s and the structure constants of \(U_3(p^m)\).

Lemma 5.19: In the relations (R7), namely, for \(1 \leq i, j \leq m\),
\[
\left[x_i, y_j\right] = \left[x_1, y_1^{\lambda_{i,j,1}}y_2^{\lambda_{i,j,2}} \cdots y_m^{\lambda_{i,j,m}}\right] \prod_{l=1}^{2m} z_{l}^{\lambda_{i,j,l}},
\]
\(\lambda_{i,j,l}, m + 1 \leq l \leq 2m,\) are uniquely determined by the structure constants of \(U_3(p^m)\).

Proof. For simplicity, we fix \(i, j \leq m\) and write
\[
y_1^{\lambda_{i,j,1}}y_2^{\lambda_{i,j,2}} \cdots y_m^{\lambda_{i,j,m}} = y.
\]
Since \([x_i, y_j] \equiv [x_1, y] \pmod{Z(G)}\), we have \([x_1y_j^r, x_1y^r] \equiv 1 \pmod{Z(G)}\) for any \(r \in \mathbb{F}_p\).

That \(\lambda_{i,j,l}, m + 1 \leq l \leq 2m,\) are uniquely determined by the structure constants of \(U_3(p^m)\), follows on the lines (without any extra work) of Step 1 of Lemma 5.15.

By the symmetry of \(x_i\)’s and \(y_i\)’s, the following lemma is dual of the preceding one.

Lemma 5.21: In the relations (R8), namely, for \(1 \leq i, j \leq m\),
\[
\left[x_j, y_i\right] = \left[x_1^{\mu_{i,j,1}}x_2^{\mu_{i,j,2}} \cdots x_m^{\mu_{i,j,m}}, y_1\right] \prod_{l=1}^{2m} z_{l}^{\mu_{i,j,l}},
\]
\(\mu_{i,j,l}, 1 \leq l \leq m,\) are uniquely determined by the structure constants of \(U_3(p^m)\).
We are now ready to prove the uniqueness of $\lambda$’s and $\mu$’s.

**Theorem 5.23:** In the relations (R7) and (R8), $\lambda_{i,j,l}$ and $\mu_{i,j,l}$, $1 \leq i, j \leq m$, $1 \leq l \leq 2m$, are uniquely determined by the structure constants of $U_3(p^m)$.

**Proof.** The proof involves a careful application of Lemmas 5.15, 5.19 and 5.21.

Interchanging $i$ and $j$ in (5.22), and noting that $\kappa_{i,j,l} = \kappa_{j,i,l}$, we get

\[
[x_i, y_j] = [x_1^{\kappa_{i,j,1}} \cdots x_m^{\kappa_{i,j,m}}, y_1] \prod_{l=1}^{2m} z_l^{\mu_{i,j,l}}.
\]

By Lemma 5.21, $\mu_{i,j,l}$, $1 \leq i, j, l \leq m$, are uniquely determined by the structure constants of $U_3(p^m)$.

By (5.20) and (5.24), we get

\[
[x_1, y] = [x, y] \prod_{l=1}^{2m} z_l^{\mu_{i,j,l} - \lambda_{i,j,l}},
\]

where

\[
x = x_1^{\kappa_{i,j,1}} \cdots x_m^{\kappa_{i,j,m}} \quad \text{and} \quad y = y_1^{\kappa_{i,j,1}} \cdots y_m^{\kappa_{i,j,m}}.
\]

By Lemma 5.15, $\mu_{i,j,l} - \lambda_{i,j,l}$, $1 \leq i, j, l \leq m$, $1 \leq l \leq 2m$, are uniquely determined by the structure constants of $U_3(p^m)$.

Hence $\lambda_{i,j,l}$, $1 \leq i, j, l \leq m$, $1 \leq l \leq m$, are uniquely determined by the structure constants of $U_3(p^m)$. This, together with Lemma 5.19, completes the uniqueness of $\lambda$’s.

Similarly, $\mu_{i,j,l}$, $1 \leq i, j \leq m$, $1 \leq l \leq 2m$, are uniquely determined by the structure constants of $U_3(p^m)$.

Finally we prove the uniqueness of $\alpha$’s and $\beta$’s in the relations (R5) and (R6). Although the proofs are almost similar to the proofs of the previous cases, these do not go verbatim. Thus, we give a complete proof of uniqueness of $\alpha$’s and $\beta$’s.

We need the following preliminary lemma.

**Lemma 5.25:** For any $i$ with $1 \leq i \leq m$ and $c_j, c'_j, d_j, d'_j \in \mathbb{F}_p$ for $1 \leq j \leq m$, assume that the commutator equations

\[
[h_1^{c_1} \cdots h_m^{c_m}, x_i] = z_1^{d_1} \cdots z_m^{d_m} \quad \text{and} \quad [h_1^{c'_1} \cdots h_m^{c'_m}, y_i] = z_{m+1}^{d'_1} \cdots z_{2m}^{d'_m}
\]

hold in the group $G$. Then there exists an $m \times m$ invertible matrix $A$, whose entries are the structure constants $\kappa_{i,j,l}$ of $U_3(p^m)$, such that

\[
[c_1 \cdots c_m]A = [d_1 \cdots d_m] \quad \text{and} \quad [c'_1 \cdots c'_m]A = [d'_1 \cdots d'_m].
\]
Proof. Since \(h_1, h_2, \ldots, h_m\) are independent modulo \(C_G(x_i)\), it follows that 
\([h_1, x_i], [h_2, x_i], \ldots, [h_m, x_i]\) are independent, and lie in \(\langle z_1, z_2, \ldots, z_m \rangle\) (by Theorem 5.12). In other words, 
\([h_1, x_i], [h_2, x_i], \ldots, [h_m, x_i]\) is also a basis for the vector space \(\langle z_1, z_2, \ldots, z_m \rangle\) over \(\mathbb{F}_p\). From Theorem 5.12,

\[
[h_j, x_i] = z_{1}^{\kappa_{j,i,1}} z_{2}^{\kappa_{j,i,2}} \cdots z_{m}^{\kappa_{j,i,m}}.
\]

The desired matrix \(A\) is the matrix of change of basis from \(\{z_1, \ldots, z_m\}\) to 
\([h_1, x_i], [h_2, x_i], \ldots, [h_m, x_i]\), which is given by \(A = (a_{r,s})\), where \(a_{r,s} = \kappa_{r,i,s}\) for \(1 \leq r, s \leq m\).

Changing \(x_i\) by \(y_i\) and \(z_i\) by \(z_{m+i}\); similarly, we get the second assertion. \(\blacksquare\)

**Theorem 5.26:** In the relations (R5) and (R6), \(\alpha_{i,j,l}\) and \(\beta_{i,j,l}\), \(1 \leq i, j \leq m, 1 \leq l \leq 2m\), are uniquely determined by the structure constants of \(U_3(p^m)\).

**Proof.** Fix \(i, j\) with \(1 \leq i, j \leq m\). Consider the relations (R7):

\[
[x_i, y_j] = [x_1, y_1^{\kappa_{i,j,1}} y_2^{\kappa_{i,j,2}} \cdots y_m^{\kappa_{i,j,m}}] \prod_{l=1}^{2m} z_l^{\lambda_{j,i,l}}.
\]

Since \(\kappa_{i,j,l} = \kappa_{j,i,l}\), interchanging \(i\) and \(j\), we get

\[
[x_j, y_i] = [x_1, y_1^{\kappa_{i,j,1}} y_2^{\kappa_{i,j,2}} \cdots y_m^{\kappa_{i,j,m}}] \prod_{l=1}^{2m} z_l^{\lambda_{j,i,l}}.
\]

From the preceding two equations, we obtain

\[(5.27) \quad [x_i, y_j] = [x_j, y_i] \prod_{l=1}^{2m} z_l^{\lambda_{i,j,l} - \lambda_{j,i,l}};\]

hence \([x_i, y_j] \equiv [x_j, y_i] \pmod{Z(G)}\). Since \([x_i, x_j] \equiv [y_i, y_j] \equiv 1 \pmod{Z(G)}\), it follows that \([x_i y_i^r, x_j y_j^r] \equiv 1 \pmod{Z(G)}\) for all \(r \in \mathbb{F}_p\). By Corollary (3.10), there exists an element \(k(r)\), depending on \(r\), in \(G'\) such that

\([x_i y_i^r, x_j y_j^r k(r)] = 1\).

Then

\[
1 = [x_i y_i^r, x_j y_j^r k(r)]
= [x_i, x_j] [x_i, y_j]^r [x_i, y_j, y_j]^{(r)} [x_i, y_j, y_j]^r [x_i, k(r)]
= [y_i, x_j]^r [y_i, x_j, y_i]^{(r)} [y_i, x_j, y_j]^r [y_i, y_j]^r [y_i, k(r)]^r.
\]
Using (5.27), we get
\[
\left( \prod_{l=1}^{2m} z_l^{\lambda_{i,j,l} - \lambda_{j,i,l}} \right)^{-r} = ([x_i, x_j][x_i, k(r)]) ([x_i, y_j, y_j]^{(2)} [x_i, y_j, y_i] r^2 [y_i, x_j, y_j] r^2 [y_i, k(r)] r^2).
\]

Using Theorem 5.12 and Lemma 5.14, it follows that
\[
[x_i, x_j][x_i, k(r)] \in \langle z_1, \ldots, z_m \rangle
\]
and the rest of the terms in the right side of the preceding equation belong to \langle z_{m+1}, \ldots, z_{2m} \rangle. Thus
\[
(5.28) \quad \left( \prod_{l=1}^{m} z_l^{\lambda_{j,i,l} - \lambda_{i,j,l}} \right)^{r} = [x_i, x_j][x_i, k(r)]
\]
and
\[
(5.29) \quad \left( \prod_{l=m+1}^{2m} z_l^{\lambda_{j,i,l} - \lambda_{i,j,l}} \right)^{r} = [x_i, y_j, y_j]^{(2)} [x_i, y_j, y_i] r^2 [y_i, x_j, y_j] r^2 [y_i, y_j] r^2 [y_i, k(r)] r^2.
\]

Since \([h_1, x_i], [h_2, x_i], \ldots, [h_m, x_i]\) are independent and belong to \langle z_1, z_2, \ldots, z_m \rangle (see Theorem 5.12), we get
\[
\langle z_1, z_2, \ldots, z_m \rangle = \langle [h_1, x_i], [h_2, x_i], \ldots, [h_m, x_i] \rangle,
\]
Hence there exists \(\tilde{k} \in G'\), independent of \(r\), such that
\[
\prod_{l=1}^{m} z_l^{-\lambda_{i,j,l} + \lambda_{j,i,l}} = [x_i, \tilde{k}].
\]
Similarly there exists \(\hat{k} \in G'\), independent of \(r\), such that
\[
(5.30) \quad [x_i, x_j] = [x_i, \hat{k}^{-1}].
\]
Therefore, from (5.28), we get \([x_i, \tilde{k}]^r = [x_i, \hat{k}^{-1}] [x_i, k(r)]\), which implies that \(\tilde{k}^r \hat{k} k(r)^{-1} \in C_G(x_i) \cap G' = Z(G)\). Hence
\[
k(r) \equiv \tilde{k}^r \hat{k} \pmod{Z(G)}.
\]
Using this in (5.29), we get
\[
\prod_{l=m+1}^{2m} z_l^{r(\lambda_{j,i,l}-\lambda_{i,j,l})} = [x_i, y_j, y_j]^{(r)}[x_i, y_j, y_i]^{(r)}[y_i, x_j, y_j]^{(r)}[y_i, \hat{k}]^{r} [y_i, y_j]^{r} [y_i, \hat{k}]^{r}.
\]

Writing this equation for \( r = 1 \) and \( r = -1 \), we get
\[
\prod_{l=m+1}^{2m} z_l^{\lambda_{j,i,l}-\lambda_{i,j,l}} = [x_i, y_j, y_j][y_i, x_j, y_j][y_i, \hat{k}][y_i, y_j][y_i, \hat{k}]^{-1}.
\]

The preceding two equations give
\[
\prod_{l=m+1}^{2m} z_l^{2(\lambda_{j,i,l}-\lambda_{i,j,l})} = [x_i, y_j, y_j]^{-1}[y_i, x_j, y_j]^{-1}[y_i, \hat{k}]^{2}.
\]

Rearranging the terms, we get
\[
\prod_{l=m+1}^{2m} z_l^{(\lambda_{j,i,l}-\lambda_{i,j,l})} [x_i, y_j, y_j]^{1/2}[y_i, x_j, y_j]^{1/2} = [y_i, \hat{k}]^{2}.
\]

Note that the left side of the preceding equation is of the form \( z_{m+1}^{d_1} \cdots z_{2m}^{d_m} \). By Corollary 5.13 and Theorem 5.23, \( d_i \)'s are uniquely determined by the structure constants of \( U_3(p^m) \). Let \( \hat{k} = h_1^{c_1} \cdots h_m^{c_m} \) (mod \( Z(G) \)). Thus, we have the commutator equation
\[
z_{m+1}^{d_1} \cdots z_{2m}^{d_m} = [y_i, h_1^{c_1} \cdots h_m^{c_m}]^{\hat{k}}.
\]

By Lemma 5.25, it follows that \( c_i \)'s are uniquely determined by the structure constants of \( U_3(p^m) \).

By Lemma 5.14, \( \alpha_{i,j,l} = 0 \) for \( l > m \). Then by (5.30), we have
\[
\prod_{l=1}^{m} z_l^{\alpha_{i,j,l}} = [x_i, x_j] = [\hat{k}, x_i] = [h_1^{c_1} \cdots h_m^{c_m}, x_i].
\]

Again, by Lemma 5.25, it follows that \( \alpha_{i,j,l}, 1 \leq i, j \leq m, 1 \leq l \leq 2m, \) are uniquely determined by the structure constants of \( U_3(p^m) \).

That \( \beta_{i,j,l}, 1 \leq i, j \leq m, 1 \leq l \leq 2m, \) are uniquely determined by the structure constants of \( U_3(p^m) \), follows on the same lines. ■
Before proceeding to the proof of Theorem 5.10, we summarize the preceding discussion of this section. For simplicity, fix a prime \( p > 2 \), an integer \( m \geq 2 \), and a finite \( p \)-group \( H \) of nilpotency class 3 and of conjugate type \((1, p^{2m})\). Then, there exist \( \alpha_{i,j,l}, \beta_{i,j,l}, \gamma_{i,j,l}, \delta_{i,j,l}, \lambda_{i,j,l}, \mu_{i,j,l}, \epsilon_{i,l}, \nu_{i,l} \in \mathbb{F}_p \) \((1 \leq i, j \leq m, 1 \leq l \leq 2m)\), such that \( H \) is isoclinic to the group \( G \) with presentation as in Lemma 5.8. By Theorems 5.12, 5.23 and 5.26, all of these coefficients, except \( \epsilon_{i,l} \) and \( \nu_{i,l} \), are uniquely determined. In particular, the isoclinism type of the group \( H \) depends only on \( \epsilon_{i,l} \) and \( \nu_{i,l} \), \( 1 \leq i \leq m, 1 \leq l \leq 2m \).

Thus, for the proof of Theorem 5.10, we fix those unique \( \alpha_{i,j,l}, \beta_{i,j,l}, \gamma_{i,j,l}, \delta_{i,j,l}, \lambda_{i,j,l}, \mu_{i,j,l}, \epsilon_{i,l}, \nu_{i,l} \in \mathbb{F}_p \), \( 1 \leq i, j \leq m, 1 \leq l \leq 2m \), for which a group given by the presentation as in Lemma 5.8 is of conjugate type \((1, p^{2m})\), for some \( \epsilon \)'s and \( \nu \)'s in \( \mathbb{F}_p \). Then we denote the resulting group with presentation as in Lemma 5.8 by \( G(\epsilon, \nu) \).

**Lemma 5.31:** For any choice of \( \epsilon_{i,l}, \nu_{i,l}, \epsilon'_{i,l}, \nu'_{i,l} \in \mathbb{F}_p \), \( 1 \leq i \leq m, 1 \leq l \leq 2m \), the groups \( G(\epsilon, \nu) \) and \( G(\epsilon', \nu') \) are isoclinic.

**Proof.** Consider the presentation of \( G(\epsilon, \nu) \) as in Lemma 5.8. To distinguish the generators of \( G(\epsilon, \nu) \) and \( G(\epsilon', \nu') \), we write the presentation of \( G(\epsilon', \nu') \) as in Lemma 5.8, where we replace \( x_i \) by \( \hat{x}_i \), \( y_i \) by \( \hat{y}_i \), \( h_i \) by \( \hat{h}_i \), and \( z_l \) by \( \hat{z}_l \) for \( 1 \leq i \leq m, 1 \leq l \leq 2m \). For simplicity, we denote the groups \( G(\epsilon, \nu) \) and \( G(\epsilon', \nu') \) by \( G_1 \) and \( G_2 \) respectively.

It follows, from the construction of \( G_1 \) and \( G_2 \), that the map \( x_i Z(G_1) \mapsto \hat{x}_i Z(G_2) \), \( y_i Z(G_1) \mapsto \hat{y}_i Z(G_2) \), \( h_i Z(G_1) \mapsto \hat{h}_i Z(G_2) \) extends to an isomorphism \( \phi : \frac{G_1}{Z(G_1)} \to \frac{G_2}{Z(G_2)} \). Since \( G_1' \) and \( G_2' \) are elementary abelian, it is clear that the map \( h_i \mapsto \hat{h}_i \), \( z_l \mapsto \hat{z}_l \) extends to an isomorphism \( \theta : G_1' \to G_2' \). Consider the diagram

\[
\begin{array}{ccc}
\overline{G}_1 \times \overline{G}_1 & \overset{a_{G_1}}{\longrightarrow} & \overline{G}_1' \\
\phi \times \phi \downarrow & & \downarrow \theta \\
\overline{G}_2 \times \overline{G}_2 & \overset{a_{G_2}}{\longrightarrow} & \overline{G}_2'
\end{array}
\]

where \( a_{G_1} \) and \( a_{G_2} \) are the commutation maps as defined in Section 2.
From the commutator relations of $G_1$ and $G_2$ (that is, the relations $(R1)$–$(R9)$ of $G_1$, and correspondingly those of $G_2$), it follows that the above diagram commutes for the generators of $G_1$ and $G_2$ taken in their presentation. A routine calculation now shows that the diagram commutes.

Stitching all the above pieces together, we get

**Proof of Theorem 5.10.** For a prime $p > 2$ and integer $n = 2m \geq 2$, let $H$ be a finite $p$-group of nilpotency class 3 and of conjugate type $(1, p^n)$. If $m = 1$, then the result follows from [4, Theorem 4.2]. Thus, we can assume that $m \geq 2$.

By Lemma 5.8, there exist $\alpha$’s, $\beta$’s, $\gamma$’s, $\delta$’s, $\lambda$’s, $\mu$’s, $\epsilon$’s and $\nu$’s in $\mathbb{F}_p$ such that $H$ is isoclinic to a group $G$ with the presentation as in Lemma 5.8. By Theorems 5.12, 5.23 and 5.26, $\alpha$’s, $\beta$’s, $\gamma$’s, $\delta$’s, $\lambda$’s, and $\mu$’s are uniquely determined by the structure constants of $\text{U}_3(p^m)$. By Lemma 5.31, the isoclinism type of $G$ is independent of the choice of $\epsilon$’s and $\nu$’s in $\mathbb{F}_p$.

Thus, for any $m \geq 1$, $H$ is uniquely determined up to isoclinism, and hence is isoclinic to the group $H_m/Z(H_m)$ (see Section 4).

**ACKNOWLEDGEMENT.** We thank Prof. C. M. Scoppola for bringing to our attention the examples of finite $p$-groups of nilpotency class 3 and conjugate type $(1, p^{2m})$ constructed in [1]. We thank the referee for various important suggestions for simplifying some proofs, e.g., Lemma 3.4, Lemma 3.5, Proposition 3.12.

**References**

[1] R. Dark and C. M. Scoppola, *On Camina groups of prime power order*, Journal of Algebra **181** (1996), 787–802.

[2] P. Hall, *The classification of prime-power groups*, Journal für die Reine und Angewandte Mathematik **182** (1940), 130–141.

[3] I. M. Isaacs, *Groups with many equal classes*, Duke Mathematical Journal **37**(3) (1970), 501–506.

[4] K. Ishikawa, *Finite $p$-groups up to isoclinism, which have only two conjugacy lengths*, Journal of Algebra **220** (1999), 333–345.

[5] K. Ishikawa, *On finite $p$-groups which have only two conjugacy lengths*, Israel Journal of Mathematics **129** (2002), 119–123.

[6] N. Ito, *On finite groups with given conjugate types I*, Nayoga Mathematical Journal **6** (1953), 17–28.

[7] A. Mann and C. M. Scoppola, *On $p$-groups of Frobenius type*, Archiv der Mathematik **56** (1991), 320–332.
[8] T. K. Naik and M. K. Yadav, *Finite p-groups of conjugate type \{1, p^3\},* Journal of Group Theory 21 (2018), 65–82.

[9] G. Parmeggiani and B. Stellmacher, *p-groups of small breadth,* Journal of Algebra 213 (1999), 52–68.

[10] L. Verardi, *Gruppi semieextraspeciali di esponente p,* Annali di Matematica Pura ed Applicata 148 (1987), 131–171.