Far East Journal of Mathematical Sciences (FJMS)

http://www.pphmj.com
http://dx.doi.org/10.17654/MS103061077
Volume 103, Number 6, 2018, Pages 1077-1102 **ISSN: 0972-0871**

FINITE *p*-GROUPS IN WHICH THE UPPER CENTRAL FACTORS HAVE THE SAME EXPONENTS

Theodoros G. Exarchakos, George E. Baralis and George M. Exarchakos

Department of Mathematics and Informatics
Faculty of Primary Education
National and Kapodistrian University of Athens
20 Ippokratous Str., 10680 Athens
Greece

Abstract

By an E-group, we mean any p-group G in which the upper central factors have the same exponents.

For a long time, there exist two conjectures:

(I) "If G is a finite non-cyclic group of order p^n, p a prime and n an integer with $n > 2$, then the order of G divides the order of the group $A(G)$ of its automorphisms".

(II) "If G is a finite group, then there exists a function $g(h)$ for which $|A(G)|p \geq p^h$, whenever $|G| \geq p^{g(h)}$, where p is a prime number and h an integer with $h > 2$ ".

A p-group is an E-group, if it belongs to $E \cup C(p, n, c, k_1)$, where $E \cup C(p, n, c, k_1)$ is the collection of groups of order p^n, p a prime

Received: February 19, 2017; Accepted: April 10, 2017
2010 Mathematics Subject Classification: 20D15.
Keywords and phrases: p-groups, automorphisms, LA-groups.

and n, c, k_1 positive integers with $c > 2$, $n > 2$ and $\exp \frac{Z_{i+1}}{Z_i} = \exp Z = p^{k_1}$ for all $i = 0, 1, 2, ..., c-1$, where $G \geq Z_c \geq Z_{c-1} \cdots \geq Z_1 > Z_0 = 1$ is the upper central series of G and $Z_1 = Z$ is the center of G.

In this paper

(I) We prove that if G is an E-group, then the first conjecture is always true.

(II) By the proof of the first conjecture, we find a new value for the function $g(h)$ such that $g(h) \leq h$ for all integers h with $h > 2$. We believe that this value is the best possible for E-groups.

I. Proving the first conjecture

1.1. Historical overview

Since the 50's there exists the conjecture:

"If G is a finite non-cyclic group of order p^n, p a prime number and n an integer greater than 2, then the order $|G|$ of G divides the order $|A(G)|$ of the group $A(G)$ of its automorphism".

Groups which satisfy this conjecture are called *LA-groups*.

Many papers have been appeared upon this topic, but the conjecture remained open until now. For example:

Schenkman in 1955 proved that a finite non-abelian group of class two is an LA-group [27]. In this paper, some lemmas were incorrect. In 1968, Faudree proved by another way those lemmas and he proved that a finite non-abelian group of class two is an LA-group [15].

Ree in 1956 proved that any finite non-abelian group of order p^n and exponent p is an LA-group [25].

Otto in 1966 proved that any finite abelian group of order p^n is an LA-group [24].

Davitt and Otto in 1971 proved that a finite p-group with the central quotient metacyclic is an LA-group [6]. They also proved in 1972 that a finite modular p-group is an LA-group [7].

Davitt in 1970 proved that a metacyclic p-group of order p^n is an LA-group [5]. He also in 1972 proved that a non-abelian p-abelian finite group of order p^n is an LA-group [8]. He also in 1980 proved that if $\left|\frac{G}{Z}\right| \leq p^4$, then G is an LA-group [9].

Otto proved in [24, Theorem 1] that if G is a direct product $G = H \times K$, where H is abelian of order p^r and K is a PN-group, then $|A(G)| \geq p^r |A(K)|$.

The result of this type not only extends the number of groups to which the conjecture is known to be true, but also, and perhaps more importantly, shows that the truth of the overall conjecture depends only on being able to prove it for a smaller class of groups. Otto's result shows that it is sufficient to consider PN-groups, that is p-groups with no non-trivial abelian direct factors.

Also, Hummel proved in [21] that if the p-group G is a central product $H \cdot K$, where H is abelian and non-trivial and $|K|$ divides $|A(K)|$, then $|G|$ divides $|A(G)|$. Hummel's result shows that it is sufficient to consider p-groups which are not central product of no non-trivial groups $H \cdot K$, where H is abelian and $|K|$ divides $|A(K)|$. It may be noted here that if $Z \nleq \Phi(G)$, where Z is the center of G, then there exists a maximal subgroup M of G such that $Z \nleq M$. Then $G = Z \cdot M$ and G is a central product of Z and M, where Z is abelian. If $Z = \Phi(G)$, then G is of class two. Therefore, if G is of class $c > 2$, then Z is a proper subgroup of $\Phi(G)$. Therefore, in trying to prove the first conjecture, it is sufficient to prove it for p-groups for which $Z < \Phi(G)$.

Hence the truth of the overall conjecture depends only on being able to prove it for a class of groups which satisfy all the following Condition A:

Conditions A. (i) G has class $c > 2$.

(ii) G has more than two generators and so $t \geq 3$, where t is the number of invariants of $\frac{G}{L_2}$.

(iii) G is a PN-group

(iv) G is not a central product of $H \cdot K$, where H is abelian and $|K|$ divides $|A(K)|$.

(v) Z is a proper subgroup of $\Phi(G)$.

1.2. Notations and definitions

Throughout this paper, G will be a PN-group which satisfies Condition A. Also, we shall use the following notations:

G is a finite non-abelian group of order p^n, p a prime number, $G' = [G, G]$ is the commutator subgroup of G, $Z = Z(G)$ is the center of G and $\Phi(G)$ is the Frattini subgroup of G.

We denote the lower and the upper central series of G by:

$$G = L_1 \geq L_2 \geq L_3 \geq \cdots \geq L_{c-1} \geq L_c > L_{c+1} = 1,$$

where c is the class of G and $L_2 = G' = [G, G]$ is the commutator subgroup of G. Also, we denote the upper central series of G by

$$G = Z_c \geq Z_{c-1} \geq Z_{c-2} \geq \cdots \geq Z_1 > Z_0 = 1,$$

where $Z_1 = Z$ is the center of G.

We also denote by $m_1 \geq m_2 \geq \cdots \geq m_t \geq 1$ and $k_1 \geq k_2 \geq \cdots \geq k_s \geq 1$ the invariants of $\frac{G}{L_2}$ and Z, respectively, where t and s are the numbers of invariants of $\frac{G}{L_2}$ and Z, respectively. If $|G/L_2| = p^m$ and $|Z| = p^k$, then $m = m_1 + m_2 + \cdots + m_t$ and $k = k_1 + k_2 + \cdots + k_s$. Also, $\exp \frac{G}{L_2} = p^{m_1}$ and $\exp Z = p^{k_1}$.

$A(G)$, $I(G)$ and $A_c(G)$ are the groups of automorphisms, inner automorphisms and central automorphisms of G, respectively. $Hom(G, Z)$ is the set of all homomorphisms of G into Z.

A p-group G is called *p-abelian* if $(ab)^p = a^p b^p$ for every two elements a and b of G.

The p-group G is called *metacyclic* if it has a normal subgroup H such that both H and G/H are cyclic.

We say that the p-group G has *exponent p* if $a^p = 1$ for every $a \in G$.

The p-group G is called *PN-group* if it has no non-trivial abelian direct factor.

As we have mentioned in the abstract, a p-group is an E-group, if it belongs to $E \cup C(p, n, c, k_1)$, where $E \cup C(p, n, c, k_1)$ is the collection of groups of order p^n, p a prime and n, c, k_1 positive integers with $c > 2$, $n > 2$ and

$$\exp \frac{Z_{i+1}}{Z_i} = \exp Z = p^{k_1} \text{ for all } i = 0, 1, 2, \ldots, c-1, \tag{1}$$

where $G \geq Z_c \geq Z_{c-1} \cdots \geq Z_1 > Z_0 = 1$ is the upper central series of G and $Z_1 = Z$ is the center of G.

All groups G which belong to $E \cup C(p, n, c, k_1)$ are called *E-groups*.

All p-groups of maximal class are E-groups. If a p-group G has a maximal subgroup which is abelian, then G is an E-group. Also, all finite non-abelian p-groups with cyclic upper central factors are E-groups. Therefore, the class $E \cup C(p, n, c, k_1)$ is not empty.

We have proved in [14, Lemma 1] that the relation (1) holds for all finite non-abelian p-groups. That is all p-groups which satisfy Condition A are E-groups. However, later on we found two examples of p-group G for which the relation (1) is not valid. These two examples are groups which do not satisfy Condition A. The first example is a group of class two. The second is a group which is a central product of groups $G = H \cdot K$, where H is abelian and $|K|$ divides $|A(K)|$. So we tried persistently, however, unsuccessfully, to find a p-group satisfying Condition A, but in this particular group, the relation (1) is not valid. However, if in the future one could find a p-group that satisfies Condition A and in which the relation (1) is not valid, then it must be proved that this particular group is an LA-group.

If such a group does not exist, then in this paper, we prove that the first conjecture is always true.

Also, by proving the first conjecture, we find a new value for the function $g(h)$ such that $g(h) \leq h$ for all integers h with $h > 2$.

1.3. Preliminaries-elementary results

The number of automorphisms of a finite group has been an interesting subject of research for a long time. Here by $A(G)$, $I(G)$ and $A_c(G)$, we denote the groups of automorphisms, inner automorphisms and central automorphisms of G, respectively.

The group $I(G)$ of inner automorphisms of G is a normal subgroup of $A(G)$ and $I(G)$ is isomorphism to $\frac{G}{Z}$. Hence $|I(G)| = \left|\frac{G}{Z}\right|$ and so $I(G)$ is a p-group.

The group $A_c(G)$ of central automorphisms of G is a normal subgroup of $A(G)$ and it is the centralizer of $I(G)$ in $A(G)$. Also, $A_c(G)$ contains $I(G)$ if and only if $I(G)$ is abelian. That is $A_c(G)$ contains $I(G)$ if and only if G has class $c \leq 2$. Also, it always holds that $A_c(G) \cap I(G) = Z(I(G))$. Then $|A_c(G) \cap I(G)| = |Z(I(G))| = \left| Z\left|\frac{G}{Z}\right|\right| = \left|\frac{Z_2}{Z}\right|$.

For PN-groups G, it has been proved in [11, Lemma 1] that $A_c(G) = p^a$, with $a = \sum_{m_i k_1}^{t,s} \min(m_i, k_j)$, where $m_1 \geq m_2 \geq \cdots \geq m_t \geq 1$ and $k_1 \geq k_2 \geq \cdots \geq k_s \geq 1$ are the invariants of the abelian groups $\frac{G}{L_2}$ and Z, respectively. Therefore, if G is a PN-group, then $A_c(C)$ is also a p-group.

Let $|A(G)|_p = p^A$ be the greatest power of p which divides $|A(G)|$. In order to prove that the p-group G is an LA-group, it is enough to prove that $A \geq n$, where $|G| = p^n$.

Since for PN-groups both $I(G)$ and $A_c(G)$ are p-groups, we get

$$p^A = |A(G)|_p \geq |A_c(G) \cdot I(G)| = \frac{|A_c(G)| \cdot |I(G)|}{|A_c(G) \cap I(G)|} = \frac{|A_c(G)| \cdot \left|\frac{G}{Z}\right|}{\frac{Z_2}{Z}}$$

$$= |A_c(G)| \cdot \left|\frac{G}{Z_2}\right| = p^a \cdot p^b,$$

where $\left|\frac{G}{Z_2}\right| = p^b$. Then we get

$$A = a + b, \text{ where } |A(G)|_p = p^A, |A_c(G)| = p^a \text{ and } \left|\frac{G}{Z_2}\right| = p^b.$$

Let G be a PN-group of order p^n. In order to prove that G is an LA-group, it is enough to prove that $a + b \geq n$.

Blackburn proved in [1, Theorem 1.5] that if $m_1 \geq m_2 \geq \cdots \geq m_t \geq 1$ are the invariants of $\frac{G}{L_2}$, then

$$p^{m_2} \geq \exp \frac{L_2}{L_3} \geq \exp \frac{L_3}{L_4} \geq \cdots \geq \exp \frac{L_{c-1}}{L_c} \geq \exp \frac{L_c}{L_{c+1}}.$$

Let $\exp \frac{L_{c-1}}{L_c} = p^r$. Then

$$m_2 \geq r. \tag{1}$$

Take $a \in G$, $b \in L_{c-1}$. Then $[a, b] \in L_c \leq Z$ and so $[a, b]$ commutes with both a and b. Hence $[a^n, b] = [a, b^n] = [a, b]^n$ for any positive integer n. Then $[a, b^{p^r}] = [a, b]^{p^r} = 1$. This gives $[a, b]^{p^r} = 1$ for $[a, b] \in Z$. Thus $b^{p^r} \in Z$ for every $b \in L_{c-1}$ and so

$$r \geq k_1. \tag{2}$$

By (1) and (2), we get

$$m_2 \geq k_1.$$

Since $m_2 \geq k_1$ by [11, Lemma 1], we get $a \geq 2k + 1(t-2)s$ as $t \geq 3$. Hence we have

$$a \geq 2k + s.$$

Let $G = Z_c \geq Z_{c-1} \geq \cdots \geq Z_1 > Z_0 = 1$ be the upper central series of G. Since it is an E-group, we have $\exp \frac{Z_{i+1}}{Z_i} = \exp Z = p^{k_1}$ for all $i = 0, 1, 2, \ldots, c-1$. Therefore, we have $p^b = \left| \frac{G}{Z_2} \right| = \left| \frac{G}{Z_{c-1}} \right| \cdot \left| \frac{Z_{c-1}}{Z_2} \right|$. Since $\frac{G}{Z_{c-1}}$ cannot be cyclic, we have $\left| \frac{G}{Z_{c-1}} \right| \geq p^{k_1+1}$.

Hence

$$p^b = \left|\frac{G}{Z_2}\right| = \left|\frac{G}{Z_{c-1}}\right| \cdot \left|\frac{Z_{c-1}}{Z_2}\right| \geq p^{k_1+1} \cdot p^{k_1(c-3)} = p^{k_1c-2k_1+1}.$$

Therefore, it is always valid

$$b \geq k_1c - 2k_1 + 1.$$

By these results, we get $A \geq a + b \geq 2k + s + b$ with $b \geq k_1c - 2k_1 + 1.$

We could summarize all the results above in the following Lemma 1 and we shall use this lemma without any further references:

Lemma 1. *Let G be a group of order* p^n *which satisfies Condition A. Then all the following conditions hold*:

(i) $A = a + b,$ *where* $|A(G)|_p = p^A, |A_c(G)| = p^a$ *and* $\left|\frac{G}{Z_2}\right| = p^b.$

(ii) $a \geq 2k + s,$ *where s is the number of invariants of Z.*

(iii) $b \geq k_1c - 2k_1 + 1 \geq c - 1 \geq 2.$

Now we are going to state some known results without proofs. There proofs could be found in [12], [14] and [19].

First we will state with a minor modification some results which have been proved in [14, Lemma 2].

For example, in case (v), it is stated that “if $k > m_1 \geq k_1 \geq m_t,$ then $a \geq k + m + s - m_1 - 1$”. That case (v) we change to “if $k \geq m_1 \geq k_1 \geq m_t,$ then $a \geq k + m + s - m_1 - 1$”. The proof is exactly the same.

Note that by this result, since $k \geq m_1,$ we get $a \geq m + s - 1$ and therefore case (iv) can be written as follows: “If $k \geq m_1,$ then $a \geq m + s - 1$”.

Lemma 2. *Let G be a group of order* p^n *and class c. Also, let* $G = L_1 \geq L_2 \geq L_3 \geq \cdots \geq L_{c-1} \geq L_c > L_{c+1} = 1$ *and* $G = Z_c \geq Z_{c-1} \geq Z_{c-2} \geq \cdots \geq Z_1 > Z_0 = 1$ *be the lower and the upper central series of G, where*

$L_2 = G' = [G, G]$ *is the commutator subgroup of* G *and* $Z_1 = Z$ *is the center of* G. *Let* $\left|\frac{G}{L_2}\right| = p^m, |Z| = p^k$ *and* $m_1 \geq m_2 \geq \cdots \geq m_t \geq 1$ *and* $k_1 \geq k_2 \geq \cdots \geq k_s \geq 1$ *be the invariants of* $\frac{G}{L_2}$ *and* Z, *where* t *and* s *are the numbers of invariants of* $\frac{G}{L_2}$ *and* Z, *respectively*, $\exp \frac{G}{L_2} = p^{m_1}$, $\exp Z = p^{k_1}$. *In such a group, all the following conditions hold*:

(i) $|A_c(G)| = p^a$, *where* $a = \sum_{i, j}^{t, s} \min(m_i, k_j)$.

(ii) *If* $m_i \geq k_1$ *for some* i *with* $1 \leq i \leq t$, *then* $a \geq ik + (t - i)s$.

(iii) *If* $k \geq m_1 \geq k_1 \geq m_t$, *then* $a \geq k + m + s - m_1 - 1$.

(iv) *If* $m_1 \leq k$, *then* $a \geq m + s - 1$, *where* $\left|\frac{G}{L_2}\right| = p^m$.

Lemma 3. *Let* G *be a group of order* p^n *and class* c. *If* G *has more than one maximal subgroup which is abelian, then*:

(i) G *has class two and* $\left|\frac{G}{Z}\right| = p^2$.

(ii) G' *is cyclic of order* p.

(iii) G *has two generators if and only if all maximal subgroups of* G *are abelian*.

Proof. As in [12, Theorem 1.24, p. 14].

Lemma 4. *Let* G *be a group of order* p^n *and class* c. *Let* H *be a normal proper subgroup of* G. *Then there exists a normal subgroup* K *of* G *containing* H *such that* $\left|\frac{K}{H}\right| = p$.

Proof. Assume that $H \neq 1$. Then $H \cap Z \neq 1$. Let K be a normal subgroup of G containing H. Then $\frac{K}{H} \cap Z\left(\frac{K}{H}\right) \neq 1$. Hence there exists $x \in \frac{K}{H} \cap Z\left(\frac{K}{H}\right)$ with $x \neq 1$. Choose $x \in \frac{K}{H} \cap Z\left(\frac{K}{H}\right)$ such that $x \neq 1$ and $x^p \in H$. Then $K = \langle x, H\rangle$ and K is a normal subgroup of G.

Lemma 5. *Let G be a finite p-group with* $\left|\frac{G}{Z}\right| = p^r$. *If* $\frac{G}{Z}$ *has class less than p, then it has defined type which is the partition of r. Moreover, the two largest type invariants of* $\frac{G}{Z}$ *are the same.*

Proof. This has been proved by Hall in [19, p. 137].

Theorem 1[*]. *Let G be a group of order* p^n *and class* $c > 2$, *where p is a prime and n is an integer greater than* 2. *Let*

$$G = L_1 \geq L_2 \geq L_3 \geq \cdots \geq L_{c-1} \geq L_c > L_{c+1} = 1$$

and

$$G = Z_c \geq Z_{c-1} \geq Z_{c-2} \geq \cdots \geq Z_t > Z_0 = 1$$

be the lower and the upper central series of G, where $L_2 = G' = [G, G]$ *is the commutator subgroup of G and* $Z_1 = Z$ *is the center of G.*

We denote by $m_1 \geq m_2 \geq \cdots \geq m_t \geq 1$ and $k_1 \geq k_2 \geq \cdots \geq k_s \geq 1$ the invariants of $\frac{G}{L_2}$ and Z, respectively, where t and s are the numbers of invariants of $\frac{G}{L_2}$ and Z, respectively. Since G has more than two generators, $t \geq 3$.

---

[*]This theorem has been proved in [14, Theorem 2]. But in that proof, there exist some points which maybe need more explanations. To overcome these ambiguous points, we give here a new proof of that theorem.

Let $\left|\frac{G}{L_2}\right| = p^m$ and $|Z| = p^k$. Then we have $m = m_1 + m_2 + \cdots + m_t$ and $k = k_1 + k_2 + \cdots + k_s$. Also, $\exp \frac{G}{L_2} = p^{m_1}$ and $\exp Z = p^{k_1}$.

In such a group, if the center Z of G is elementary abelian, then G is an LA-group.

Proof. By Lemma 1,

$$b \geq k_1 c - 2k_1 + 1 \geq c - 1 \geq 2. \tag{1}$$

If $|Z| = p^k$ and $k = 1$, then $|A(G)| \geq p|I(G)| = p\left|\frac{G}{Z}\right| = |G|$. Therefore, we may assume that

$$k \geq 2. \tag{2}$$

Since Z is elementary abelian, $k_i = 1$ for all $i = 1, 2, \ldots, s$.

Then

$$a \geq kt \geq 3k. \tag{3}$$

Let $|A(G)|_p = p^A$. Then $A \geq a + b$ (Lemma 1), where $|A_c(G)| = p^a$. By (1), (2) and (3), we have $A \geq a + b \geq 3k + c - 1 \geq 8$. Since $k \geq 2$, $a \geq 3k \geq 2k + 2$ and so $A \geq 2k + c + 1 \geq n$ for $k \geq \frac{n-4}{2}$.

Hence,

$$\text{if } n \leq 8 \text{ or } k \geq \frac{n-4}{2}, \text{ then } G \text{ is an LA-group.} \tag{4}$$

Therefore, we may assume that

$$n \geq 9 \tag{5}$$

and

$$k < \frac{n-4}{2}. \tag{6}$$

Since $k < \frac{n-4}{2}$, there exists some integer $\varphi > 0$, such that $k = \frac{n-4-\varphi}{2}$. Since $k \geq 2$, we get $\frac{n-4-\varphi}{2} \geq 2$, which gives $\varphi \leq n-8$. By (5), $n-8 \geq 1$, for all $n \geq 9$ and so $\varphi \leq 1$. But $\varphi > 0$. Hence $\varphi = 1$ and so

$$k = \frac{n-5}{2}. \tag{7}$$

Then

$$a \geq 3k \geq \frac{3n-15}{2} \tag{8}$$

and so $A \geq a + b \geq \frac{3n+15}{2} + b$.

If $b \geq 3$, then we get $A \geq a + b \geq \frac{3n-15}{2} + 3 = \frac{3n-9}{2} \geq n$ as $n \geq 9$. Hence we may assume that $b = 2$.

Since $A \geq a + b$ and $b = 2$, by (8), we get $A \geq \frac{3n-15}{2} + 2 = \frac{3n-11}{2} \geq n$ for $n \geq 11$.

By (4), $A > n$ for $n \leq 8$. Therefore, to complete the proof of the theorem, we have to prove that $A \geq n$ for $n = 10$ and $n = 9$.

For $n = 10$, $k = \frac{n-5}{2} > 2$ and so $k \geq 3$. Then $A \geq 2k + 4 \geq 10$.

Let $n = 9$. Then $k = \frac{n-5}{2} = 2$. Let $H = \frac{G}{Z}$. Then $Z(H) = Z\left(\frac{G}{Z}\right) = \frac{Z_2}{Z}$. Hence $\left|\frac{H}{Z(H)}\right| \simeq \left|\frac{G}{Z_2}\right|$ and so $\left|\frac{H}{Z(H)}\right| = p^2$ and $\exp \frac{H}{Z(H)} = p$. Then there exist elements $a, b \in H$ such that $a \neq b$ and $a, b \notin Z(H)$ and $a^p \in Z(H)$, $b^p \in Z(H)$. Take $A = \langle a, Z(H)\rangle$ and $B = \langle b, Z(H)\rangle$. Then A and B are maximal abelian subgroups of H. By Lemma 3, H is of class two and $L_2(H)$ is cyclic of order p. Then we have: G is of class 3 and so

$L_2 \leq Z_2, \ L_3 \leq Z$. Also, $L_2(H) = L_2\left(\frac{G}{Z}\right) = \frac{L_2(G)Z}{Z}$. Then $\left|\frac{L_2 Z}{Z}\right| = p$. This gives $\left|\frac{L_2}{L_2 \cap Z}\right| = p$. Since $L_3 \leq L_2 \cap Z$, $|L_2 \cap Z| \geq p$ and since $L_2 \cap Z \leq Z$ and $|Z| = p^2$, we get $|L_2 \cap Z| \leq p^2$. Therefore, $|L_2| \leq p^3$. If $|L_2| \leq p^2$, then $\left|\frac{L_2}{L_3}\right| = |L_3| = p$ and G has homocyclic lower central factors. Then by [14, Theorem 1], G is an LA-group. Therefore, we may assume that $|L_2| = p^3$. Then $L_2 \cap Z = Z$ and so $Z \leq L_2$. Hence $Z \leq L_2 \leq Z_2$. Since $\exp\frac{Z_2}{Z} = p$, we get $\exp\frac{Z_2}{L_2} = p$. Since $\exp\frac{G}{Z_2} = p$, we have $\exp\frac{G}{L_2} \leq p^2$. Then $m_1 \leq 2 \leq k$ and Lemma 2 gives $a \geq m + s - 1 \geq m + 1$, as $s = 2$. For $|L_2| = p^3$, we have $m = n - 3 = 6$ as $n = 9$. Therefore, $a \geq m + 1 \geq 7$. Thus $A \geq a + b \geq 9$.

This proves Theorem 1.

Corollary 1. *Let G be a group as in Theorem* 1. *Then G is an LA-group under any one of the following conditions*:

1.1. *If* $b \leq 3$.

1.2. *If* $\exp\frac{G}{Z} = p$.

1.3. *If G is regular and* $\exp G' = p$.

Proof. 1.1. If $b = 2$, then $\left|\frac{G}{Z_2}\right| = p^2$ and since $\frac{G}{Z_2}$ cannot be cyclic, we have $\exp\frac{G}{Z_2} = p$ and so $\exp Z = p$ and by Theorem 1, G is an LA-group.

If $b = 3$, then $\left|\frac{G}{Z_2}\right| = p^3$ and so $\exp\frac{G}{Z_2} \leq p^2$.

If $\exp \frac{G}{Z_2} = p^2$, then $\exp Z = p^2$ and so $k_1 \geq 2$. This gives $b \geq k_1 c - 2k_1 + 1 \geq 2c - 3$. For $b = 3$, we get $c = 3$. Then $H = \frac{G}{Z}$ has class 2 and since $Z(H) = Z\left(\frac{G}{Z}\right) = \frac{Z_2}{Z}$, we get $\frac{H}{Z(H)} \simeq \frac{G}{Z_2}$. Since H has class 2, we have $\frac{H}{Z(H)}$ is abelian and by Lemma 5, $\frac{H}{Z(H)}$ has type (p, p, p). Then $\exp \frac{G}{Z_2} = \exp \frac{H}{Z(H)} = p$, a contradiction. Therefore, $\exp \frac{G}{Z_2} = p$ and so $\exp Z = p$ and by Theorem 1, G is an LA-group.

1.2. If $\exp \frac{G}{Z} = p$, then we get $\exp Z\left(\frac{G}{Z}\right) = p$ and so $\exp \frac{Z_2}{Z} = p$ and the result follows by Theorem 1.

1.3. For any regular p-group, we have $\exp \frac{G}{Z} = \exp G'$ and so $\exp \frac{G}{Z} = p$, and the result follows by Corollary 1.2.

Theorem 2. *Let G be a group as in Theorem* 1. *If G has class* $c = 3$, *then G is an LA-group*.

Proof. By Theorem 1, we may assume that Z is not elementary abelian. Then $k_1 \geq 2$. So

$$k \geq 2. \tag{1}$$

By Lemma 1,

$$a \geq 2k + (t-2)s \geq 2k + s \tag{2}$$

as $t \geq 3$.

Hence

$$a \geq 2k + 1. \tag{3}$$

Let $|A(G)|_p = p^A$. Then

$$A \geq a + b. \tag{4}$$

By Corollary 1.1, we may assume that

$$b \geq 4. \tag{5}$$

By (3), (4) and (5), we get

$$A \geq a + b \geq 2k + 5. \tag{6}$$

Since $k \geq 2$, for $c = 3$, we have $A \geq 2k + 5 \geq 9$. Also, $A \geq 2k + 5 \geq n$ for $k \geq \frac{n-5}{2}$. Therefore,

$$\text{if } n \leq 9 \text{ or } k \geq \frac{n-5}{2}, \; G \text{ is an LA-group.} \tag{7}$$

Hence we may assume that

$$n \geq 10 \tag{8}$$

and $k < \frac{n-5}{2}$.

Since $k < \frac{n-5}{2}$, there exists some integer $x > 0$ such that $k = \frac{n-5-x}{2}$. But $k \geq 2$ and so $\frac{n-5-x}{2} \geq 2$, which gives $x \leq n - 9$. By (8), $n - 9 \geq 1$. So $x \leq 1$ and since $x > 0$, we have $x = 1$. Then

$$k = \frac{n-5-x}{2} = \frac{n-6}{2}. \tag{9}$$

By (3), we have

$$a \geq 2k + 1 = n - 5. \tag{10}$$

Since $b \geq 4$, we first prove Claim 1.

Claim 1. We claim that if $b = 4$, then G is an LA-group.

Let $b = 4$. Then $\left|\frac{G}{Z_2}\right| = p^4$. Let $H = \frac{G}{Z}$. Then $\frac{H}{Z(H)} = \frac{\frac{G}{Z}}{\frac{Z_2}{Z}} \simeq \frac{G}{Z_2}$ and so $p^4 = \left|\frac{G}{Z_2}\right| = \left|\frac{H}{Z(H)}\right|$. In that case, since G has class $c = 3$, $H = \frac{G}{Z}$ has class 2. Hence $\frac{H}{Z(H)}$ is abelian. Then by Lemma 5, $\frac{H}{Z(H)}$ has either type (p^2, p^2) or (p, p, p, p). We shall assume then $\frac{H}{Z(H)}$ has type (p^2, p^2) and get a contradiction.

Let $\frac{H}{Z(H)}$ has type (p^2, p^2). Then there exist elements a, b of H such that $a \neq b$, $a \notin Z(H)$, $a^p \notin Z(H)$ and $a^{p^2} \in Z(H)$. Also, $b \notin Z(H), b^p \notin Z(H)$ and $b^{p^2} \in Z(H)$. Take the groups $A = \langle a_1 Z(H)\rangle$ and $B = \langle b_1 Z(H)\rangle$. Then A and B are normal abelian subgroups of H and $\left|\frac{A}{Z(H)}\right| = \left|\frac{B}{Z(H)}\right| = p^2$. Applying Lemma 4 to subgroups A and B, we can find subgroups M and N of H such that $\left|\frac{M}{A}\right| = \left|\frac{N}{B}\right| = p$.

Take $x \in \frac{M}{A} \cap Z\left(\frac{M}{A}\right)$ such that $x \neq 1$ and $x^p \in A$. Then $M = \langle x, A\rangle$.

Take $w \in \frac{N}{B} \cap Z\left(\frac{N}{B}\right)$ with $w \neq 1$ and $w^p \in B$. Then $N = \langle w, B\rangle$. Then $\left|\frac{M}{A}\right| = \left|\frac{N}{B}\right| = p$ and so M and N are maximal subgroups of H and they are both abelian. Then by Lemma 3, it should be $\left|\frac{H}{Z(H)}\right| = p^2$, a contradiction.

Therefore, $\frac{H}{Z(H)}$ has type (p, p, p, p). Then $\exp\frac{G}{Z_2} = \exp\frac{H}{Z(H)} = p$, which gives $\exp Z = p$ and by Theorem 1, G is an LA-group. This proves our claim. Therefore we may assume that

$$b \geq 5. \tag{11}$$

By (10) and (11), we get $A \geq a + b \geq n$. This proves Theorem 2.

Corollary 2. *If* $b \leq 4$, *then G is an LA-group.*

Proof. If $b = 4$, then by the claim, we have proved in Theorem 2, G is an LA-group.

If $b \leq 3$, then the result follows from Corollary 1.1.

Theorem 3. *Let G be a group as in Theorem* 1. *If* $k_1 \leq 2$, *then G is an LA-group.*

Proof. By Theorem 1, we may assume that $k_1 \geq 2$. Then $k_1 = 2$ and so

$$k \geq 2. \tag{1}$$

By Corollary 2, we may assume that

$$b \geq 5. \tag{2}$$

By Lemma 1, we get $a \geq 2k + (t-2)s \geq 2k + s$, as $t \geq 3$. Thus

$$a \geq 2k + 1. \tag{3}$$

Let $|A(G)|_p = p^A$. Then $A \geq a + b$ and so $A \geq 2k + 6 \geq 10$. Also, $A \geq 2k + 6 \leq n$ for $k \geq \frac{n-6}{2}$. Hence

$$\text{for } n \leq 10 \text{ or for } k \geq \frac{n-6}{2},\ G \text{ is an LA-group.} \tag{4}$$

Therefore, we may assume that

$$n \geq 11 \tag{5}$$

and $k < \frac{n-6}{2}$. Since $k < \frac{n-6}{2}$, there exists some integer $x > 0$ such that $k = \frac{n-6-x}{2}$. But $k \geq 2$ and so $\frac{n-6-x}{2} \geq 2$, which gives $x \leq n - 10$. By (5), $n - 10 \geq 1$ for all n with $n \geq 11$. This gives $x \leq 1$ and so $x = 1$. Then

$$k = \frac{n-7}{2}. \tag{6}$$

By (3) and (6), we get

$$a \geq 2k + 1 = n - 6. \tag{7}$$

Claim. By Corollary 2, we may assume that $b \geq 5$. We claim that if $b = 5$, then G is an LA-group.

By Theorem 4 in [14], we may assume that $b \geq 2c - 2$. If $b = 5$, then we get $2c - 2 \leq 5$, which gives $c \leq \frac{7}{2} < 4$. Therefore $c \leq 3$, as by Theorem 2, G is an LA-group. This proves our claim.

By this claim and Corollary 2, we may assume that

$$b \geq 6. \tag{8}$$

By (7) and (8), we get $A \geq a + b \geq n - 6 + 6 = n$. This proves Theorem 3.

Corollary 3. *If* $b \leq 5$, *then G is an LA-group.*

Proof. With $b = 5$, we have proved in Claim 2 that G is an LA-group. If $b \leq 4$, then the result follows by Corollary 2.

Theorem 4. *Let G be a group as in Theorem* 1. *If the center Z of G is cyclic, then G is an LA-group.*

Proof. By Theorem 3, we may assume that $k_1 \geq 3$. Then

$$k \geq 3. \tag{1}$$

Also, by Corollary 3, we may assume that

$$b \geq 6. \tag{2}$$

By Lemma 1, we get $a \geq 2k + (t-2)s \geq 2k + s.$ Hence

$$a \geq 2k + 1. \tag{3}$$

Let $|A(G)|_p = p^A.$ Then $A \geq a + b \geq 2k + 7 \geq 13.$ Also, $A \geq 2k + 7 \geq n$ for $k \geq \frac{n-7}{2}.$ Thus, for $n \leq 13$ or for $k \geq \frac{n-7}{2},$ G is an LA-group. Therefore we may assume that

$$n \geq 14 \tag{4}$$

and $k < \frac{n-7}{2}.$ Since $k < \frac{n-7}{2},$ there exists some integer $x > 0$ such that $k = \frac{n-7-x}{2}.$ But $k \geq 3$ and so $\frac{n-7-x}{2} \geq 3,$ which gives $x \leq n - 13.$ By (4), $n - 13 \geq 1$ for all $n \geq 14.$ Then $x \leq 1$ and so $x = 1.$ Then

$$k = \frac{n-8}{2}. \tag{5}$$

Since Z is cyclic, we have $k = k_1.$ Also, $b \geq k_1 c - 2k_1 + 1$ gives $b \geq kc - 2k + 1 = k(c-2) + 1 \geq 2k + 1,$ as

$$c \geq 4. \tag{6}$$

By (3) and (6), we get $A \geq a + b \geq 4k + 2$ and so by (5), we get $A \geq a + b \geq 4k + 2 = 4\frac{n-8}{2} + 2 = 2n - 14.$ But $n \geq 14$ and so $A \geq 2n - 14 \geq n.$ This proves Theorem 4.

Theorem 5. *Let G be a group as in Theorem* 1. *If G has class* $c \leq 4,$ *then G is an LA-group.*

Proof. If G has class $c \leq 3,$ then G is an LA-group (Theorem 2). Hence we may assume that $c = 4.$

Also, by Theorems 1 and 4, we may assume that Z is not elementary abelian and not cyclic. Then $k_1 \geq 2,$ $k > k_1$ and $s \geq 2.$ Thus

$$k \geq 3. \tag{1}$$

By Lemma 1, $a \geq 2k + (t-2)s \geq 2k + s$, as $t \geq 3$. So

$$a \geq 2k + 2. \tag{2}$$

Let $|A(G)|_p = p^A$. By Lemma 1, we have

$$A \geq a + b. \tag{3}$$

By Corollary 3, we may assume that

$$b \geq 6. \tag{4}$$

Also, $A \geq a + b \geq 2k + 8 \geq 14$. Also, $A \geq 2k + 8 \geq n$ for $k \geq \frac{n-8}{2}$. Thus, for either $n \leq 14$ or $k \geq \frac{n-8}{2}$, G is an LA-group.

Hence we may assume that

$$n \geq 15 \tag{5}$$

and $k < \frac{n-8}{2}$.

Since $k < \frac{n-8}{2}$, there exists some integer $x > 0$ such that $k = \frac{n-8-x}{2}$. But $k \geq 3$ and so $k = \frac{n-8-x}{2} \geq 3$, which gives $x \leq n - 14$. By (5), $n - 14 \geq 1$ for all $n \geq 15$ and so $x \leq 1$. But $x > 0$ and so $x = 1$ and

$$k = \frac{n-9}{2}. \tag{6}$$

By (2) and (6), we get

$$a \geq 2k + 2 = n - 7. \tag{7}$$

By Theorem 3, we may assume that $k_1 \geq 3$. Then $b \geq k_1 c - 2k_1 + 1 \geq 3c - 5$. Since $c = 4$, we get

$$b \geq 3c - 5 \geq 7. \tag{8}$$

By (7) and (8), we get $A \geq a + b \geq n.$

This proves Theorem 5.

Corollary 5. *If* $b \leq 7,$ *then G is an LA-group.*

Proof. By Theorem 4 in [14], we may assume that $b \geq 2c - 2.$ So we have $2c - 2 \leq b \leq 7$ which gives $c \leq \frac{9}{2} < 5.$ Hence $c \leq 4$ and by Theorem 5, G is an LA-group.

Theorem 6 (The first conjecture)**.** *Let G be a non-cyclic group of order* p^n *and class c, where p is a prime number and n is an integer greater than two. Then the order of G divides the order of the group* $A(G)$ *of its automorphisms.*

Proof. By Theorem 5, we may assume that G has class $c \geq 5.$ Also, by Theorems 1 and 4, we may assume that the center Z of G is not elementary abelian and not cyclic. By Theorem 3, we may assume that $k_1 \geq 3.$

Hence

$$k \geq 4. \tag{1}$$

By Lemma 1, $a \geq 2k + (t - 2)s \geq 2k + s,$ as $t \geq 3.$ This gives

$$a \geq 2k + s \geq 2k + 2. \tag{2}$$

Let $|A(G)|_p = p^A.$ By Lemma 1, we have

$$A \geq a + b. \tag{3}$$

By Corollary 5, we may assume that

$$b \geq 8 \tag{4}$$

By (2), (3) and (4), we have $A \geq a + b \geq 2k + 10.$ Since $k \geq 4,$ we have $A \geq 2k + 10 \geq 18.$ Also, $A \geq 2k + 10 \geq n$ for $k \geq \frac{n - 10}{2}.$

Thus, for either $n \leq 18$ or $k \geq \frac{n-10}{2}$, G is an LA-group.

Therefore, we may assume that

$$n \geq 19 \tag{5}$$

and $k < \frac{n-10}{2}$.

Since $k < \frac{n-10}{2}$, there exists some integer $x > 0$ such that $k = \frac{n-10-x}{2}$. But $k \geq 4$ and so $k = \frac{n-10-x}{2} \geq 4$, which gives $x \leq n-18$. By (5), $n-18 \geq 1$ and so $x \leq 1$. Then $x = 1$, as $x > 0$. Thus

$$k = \frac{n-11}{2}. \tag{6}$$

By (2) and (6), we get

$$a \geq 2k + 2 = n - 9. \tag{7}$$

Since $c \geq 5, k_1 \geq 3$ and $b \geq k_1c - 2k_1 + 1$, we get

$$b \geq 3c - 5 \geq 10 \text{ as } k_1 \geq 3. \tag{8}$$

By (7) and (8), we get $A \geq a + b > n$. This proves Theorem 6 and the first conjecture.

II. Proving the second conjecture

As we mentioned in the beginning of this paper, the second conjecture has as following:

"*If G is a finite group, then there exists a function $g(h)$ for which $|A(G)|_p \geq p^h$, whenever $|G| \geq p^{g(h)}$, where p is a prime number and h an integer with $h > 2$*".

The existence of the function $g(h)$ was first conjectured in 1954 by Scott [28], who proved that $g(2) = 3$. In 1956, Ledermann and Neumann

[23] proved that in the general case of finite groups $g(h) \leq (h-1)^3 \cdot p^{h-1} + h$. Also, Green [17] and Howarth [20] reduced this bound. In 1970, Hyde [22] proved that if G is a p-group, then $g(h) = h + 1$ for $h \leq 4$ and $g(h) = \frac{1}{2}h(h-3)$ for $h \geq 5$. In 1980, we reduced this bound to $g(h) = h$ for $h \leq 5$ and $g(h) = \frac{1}{6}h^2$ for $h \geq 12$ [12]. Also, for $7 \leq h \leq 11$, we gave some other expression for $g(h)$. In 1988, Burmester and Exarchakos [3] proved that $g(h) = h$ for $h \leq 6$ and $g(h) = \frac{1}{7}h^2$ for $h \geq 42$ and for $7 \leq h \leq 41$, they gave the following expressions for $g(h)$. They proved that for $7 \leq h \leq 12$, $g(h) = 3h - 13$, for $13 \leq h \leq 22$, $g(h) = 3h - 31$, for $23 \leq h \leq 31$, $g(h) = 7h - 81$ and for $32 \leq h \leq 41$, $g(h) = 9h - 142$. In 2012, Exarchakos et al. in [13] reduced all the above bounds considerably. For the first time up to the present day, the function $g(h)$ takes a linear expression for all integers h with $h > 2$. They proved that $g(h) = h$ for $h \leq 13$ and $g(h) = 2h - 11$ for $h \geq 14$.

By Theorem 6, as we have proved it in this paper, we get that $g(h) = h$ for all integers h with $h > 2$. Note that if $|G| \geq p^{g(h)=h}$, then $|A(G)| \geq p^h$.

We believe that the function $g(h) \leq h$ is the best possible for p-groups. Therefore, Theorem 6, which has contributed to the proof of the first conjecture gives the best (least) function $g(h)$ and also proves the second conjecture for p-groups G.

References

[1] N. Blackburn, On a special class of *p*-groups, Acta Math. 100 (1958), 45-92.

[2] Gilbert Baumslag and Norman Blackburn, Groups with upper central factors, Proc. London Math. Soc. (3) 10 (1960), 531-544.

[3] M. V. D. Burmester and Th. Exarchakos, The function $g(h)$ for which $|A(G)|_p \geq p^h$ whenever $|G| \geq p^{g(h)}$, G a finite p-group, Bull. Greek Math. Soc. 29 (1988), 27-44.

[4] W. Burnside, On some properties of groups whose orders are powers of primes, Proc. Lond. Math. Soc. (2) 11 (1912), 225-245.

[5] R. M. Davitt, The automorphisms group of finite metacyclic p-group, Proc. Amer. Math. Soc. 25 (1970), 876-879.

[6] R. M. Davitt and A. D. Otto, On the automorphism group of a finite p-group with the central quotient metacyclic, Proc. Amer. Math. Soc. 30(3) (1971), 467-472.

[7] M. Davitt and A. D. Otto, On the automorphism group of a finite modular p-group, Proc. Amer. Math. Soc. 35(2) (1972), 399-404.

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

[9] R. N. Davitt, On the automorphism group of a finite p-group with a small central quotient, Canad. J. Math. 32(5) (1980), 1168-1176.

[10] Th. Exarchakos, LA-groups, J. Math. Soc. Japan 33 (1981), 185-190.

[11] Th. Exarchakos, On the number of automorphisms of a finite p-group, Canad. J. Math. 32(6) (1980), 1448-1458.

[12] Th. Exarchakos, The order of the group of automorphisms of a finite p-group, Ph.D. Thesis, Department of Mathematics, Royal Holloway College, University of London, July 1977.

[13] Th. G. Exarchakos, G. M. Dimakos and G. E. Baralis, The function $g(h)$ for which $|A(G)|_p \geq p^h$ whenever $|G|_p \geq p^{g(h)}$, G is a finite p-group, Far East J. Math. Sci. (FJMS) 62(2) (2012), 161-175.

[14] Th. Exarchakos, G. Dimakos and G Baralis, On the automorphisms of finite p-groups, Far East J. Math. Sci. (FJMS) 87(1) (2014), 1-21.

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

[16] J. A. Gallian, Finite p-groups with homocyclic central factors, Canad. J. Math. 26 (1974), 636-643.

[17] J. A. Green, On the number of automorphisms of a finite group, Proc. Roy. Soc. (London) Ser. A 237 (1956), 574-581.

[18] M. Hall, Jr., The Theory of Groups, Macmillan Company, 1959.

[19] P. Hall, The classification of prime powers group, J. Reine Angew. Math. 182 (1940), 130-141.

[20] J. C. Howarth, On the power of a prime dividing the order of the automorphism group of a finite group, Proc. Glasgow Math. Assoc. 4 (1960), 163-170.

[21] K. G. Hummel, The order of the automorphisms group of a central product, Proc. Amer. Math. Soc. 47(1) (1975), 37-40.

[22] K. H. Hyde, On the order of the Sylow-subgroups of the automorphism group of a finite group, Glasgow Math. J. 11 (1970), 88-96.

[23] N. Ledermann and B. Neumann, On the order of the automorphism group of a finite group, II, Proc. Roy. Soc. Ser. A 235 (1956), 235-246.

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

[25] R. Ree, The existence of outer automorphisms of some groups, Proc. Amer. Math. Soc. 7 (1956), 962-964.

[26] R. Ree, The existence of outer automorphisms of some groups II, Proc. Amer. Math. Soc. 9 (1958), 105-109.

[27] Eugene Schenkman, The existence of outer automorphisms of some nilpotent groups of class 2, Proc. Amer. Math. Soc. 6 (1955), 6-11.

[28] W. R. Scott, On the number of the automorphisms group of a group, Proc. Amer. Math. Soc. 5 (1954), 23-24.

[29] H. Zassenhaus, The theory of groups, Translated from the German, Chelsea Publishing Company, 1949.