J. Math. Soc. Japan
Vol. 33, No. 2, 1981

LA-groups

By Theodoros EXARCHAKOS

(Received Jan. 9, 1979)

The number of automorphisms of a finite p-group G has been an interesting subject of research for a long time. It has been conjectured that, if G is a non-cyclic finite p-group of order p^n, $n>2$, then the order of G divides the order of the group of automorphisms of G. This has been established for abelian p-groups and for certain classes of finite p-groups. In this paper we show that the conjecture is also true for some other classes of non-abelian p-groups.

A finite p-group G, which satisfies the above conjecture, is called an LA-group.

Throughout this paper G stands for a finite non-abelian group of order p^n (p a prime number), commutator subgroup G' and center Z. We denote the order of any group H by $|H|$. Also we take the lower and the upper central series of a finite p-group G to be:

$$G=L_0>L_1=G'>\cdots>L_c=1$$

and

$$1=Z_0<Z_1=Z<\cdots<Z_c=G,$$

where c is the class of G. For $c=2$, G is an LA-group ([3]). So we shall assume that $c>2$. The invariants of G/L_1 are taken to be $m_1\geqq m_2\geqq\cdots\geqq m_t\geqq 1$ and $|G/L_1|=p^m$. Similarly we take the invariants of Z to be $k_1\geqq k_2\geqq\cdots\geqq k_s\geqq 1$ and $|Z|=p^k$. We denote by $A(G)$, $I(G)$, $A_c(G)$ the groups of automorphisms, inner automorphisms, central automorphisms of G respectively. $\mathrm{Hom}(G, Z)$ is the group of homomorphisms of G into Z. Finally $P(G)=\langle x^p \mid x\in G\rangle$ and $E(G)=\langle x\in G \mid x^p=1\rangle$.

G is called a PN-group, if G has no non-trivial abelian direct factor.

We begin with:

LEMMA 1. (i) *If G is a PN-group, $|A_c(G)|=p^a$, where*

$$a=\sum \min(m_j, k_i).$$

(ii) *If $G=H\times K$, where H is abelian and non-trivial and K is a PN-group, then*

$$|A_c(G)|=|A(H)|\,|A_c(K)|\,|\mathrm{Hom}(K, H)|\,|\mathrm{Hom}(H, Z(K))|.$$

PROOF. (i) Since G is a PN-group $|A_c(G)|=|\mathrm{Hom}(G, Z)|$ ([1]). Hence $|A_c(G)|=|\mathrm{Hom}(G/L_1, Z)|=|\mathrm{Hom}(\prod_j C(p^{m_j}), \prod_i C(p^{k_i}))|=\prod_{j,i}|\mathrm{Hom}(C(p^{m_j}), C(p^{k_i}))|$ $=p^a$, where

$$a=\sum \min(m_j, k_i).$$

(ii) Let $g\in A_c(G)$. Then for $x\in G$, $x^{-1}g(x)\in Z$. So $g(x)=xf(x)$ for some $f\in\mathrm{Hom}(G, Z)$. Consider the mapping $g\to f_g$. This is a one-to-one mapping of $A_c(G)$ into $\mathrm{Hom}(G, Z)$. Furthermore, given $f\in\mathrm{Hom}(G, Z)$, $g(x)=xf(x)$ is an endomorphism of G which is an automorphism if and only if $f(x)\neq x^{-1}$ for every $x\in G$, $x\neq 1$. If G is a PN-group, then for $f\in\mathrm{Hom}(G, Z)$ the mapping $g(x)=xf(x)$ is always an automorphism of G. Let

$$A=\{\hat{g}\mid \hat{g}(h, k)=(h, g(k)),\ h\in H,\ k\in K,\ g\in A_c(K)\},$$

$$B=\{\hat{y}\mid \hat{y}(h, k)=(hy(k), k),\ h\in H,\ k\in K,\ y\in\mathrm{Hom}(K, H)\},$$

$$C=\{\hat{f}\mid \hat{f}(h, k)=(f(h), k),\ h\in H,\ k\in K,\ f\in A(H)\},$$

$$D=\{\hat{x}\mid \hat{x}(h, k)=(h, kx(h)),\ h\in H,\ k\in K,\ x\in\mathrm{Hom}(H, Z(K))\}.$$

We shall prove that $A_c(G)=ABCD$ and $|A_c(G)|=|A||B||C||D|$.

Obviously A, C are subgroups of $A_c(G)$. Also $\hat{y}$ is multiplicative and $\ker\hat{y}=1$. Since $(h, k)^{-1}\hat{y}(h, k)\in Z$, $\hat{y}\in A_c(G)$ and so $B\leqq A_c(G)$. Similarly $D\leqq A_c(G)$. Therefore $A_c(G)\supseteqq ABCD$.

Let $\hat{a}\in A_c(G)$. Then $\hat{a}(h, k)=(h, k)\cdot a(h, k)$ for some $a\in\mathrm{Hom}(G, Z)$. So $\hat{a}(1, k)=(1, k)(a_1(k), a_2(k))=(a_1(k), ka_2(k))$, where $a_1\in\mathrm{Hom}(K, H)$, $a_2\in\mathrm{Hom}(K, Z(K))$. Let $b(k)=ka_2(k)$. Since K is a PN-group, $b\in A_c(K)$. Therefore if $\hat{g}(h, k)=(h, b^{-1}(k))$, $\hat{g}\hat{a}(1, k)=(a_1(k), k)$. Taking $\hat{y}(h, k)=(hy(k), k)$, where $y(k)=(a_1(k))^{-1}$, $y\in\mathrm{Hom}(K, H)$, we get $\hat{c}(1, k)=\hat{y}\hat{g}\hat{a}(1, k)=(1, k)$. Let $\hat{c}(h, 1)=(c_1(h), c_2(h))$, $c_1\in\mathrm{Hom}(H, H)$, $c_2\in\mathrm{Hom}(H, Z(K))$. Then $\hat{c}(h, k)=(c_1(h), kc_2(h))$. Here c_1 is an automorphism of H, since for $c_1(h)=1$, $h\neq 1$, we get $\hat{c}(h, (c_2(h))^{-1})=(1, 1)$. Taking $\hat{f}(h, k)=(c_1^{-1}(h), k)$ we then get $\hat{f}\hat{c}(h, k)=(h, kc_2(h))=\hat{x}(h, k)$ for some $\hat{x}\in D$. Hence $\hat{x}=\hat{f}\hat{c}=\hat{f}\hat{y}\hat{g}\hat{a}$, so that $\hat{a}=\hat{g}^{-1}\hat{y}^{-1}\hat{f}^{-1}\hat{x}\in ABCD$. Therefore $A_c(G)\subseteqq ABCD$ and so $A_c(G)=ABCD$.

Since $\hat{y}\hat{g}(h, k)=\hat{y}(h, g(k))=(hy(g(k)), g(k))=\hat{g}\hat{y}_1(h, k)$, where $\hat{y}_1(h, k)=(hy(g(k)), k)$, we have $BA\leqq AB$. So $M=AB$ is a group. Similarly $\hat{x}\hat{f}(h, k)=\hat{f}\hat{x}_1(h, k)$ for a suitable $\hat{x}_1\in D$. Hence $N=CD$ is also a group. Clearly $A\cap B=C\cap D=1$. Moreover $M\cap N=1$. For let $\hat{g}\hat{y}(h, k)=(hy(k), g(k))=\hat{f}\hat{x}(h, k)=(f(h), kx(h))$. Setting $k=1$, we get $f(h)=h$, $x(h)=1$; setting $h=1$, we get $g(k)=k$, $y(k)=1$. Therefore

$$|A_c(G)|=|MN|=|M||N|=|AB|\cdot|CD|=|A||B||C||D|.$$

We now prove the following lemma, which is of some interest in its own right.

LEMMA 2. *If* $\exp(G/L_1)\leqq|Z|$, *then* $|A_c(G)|\geqq p^m$.

PROOF. Let G be a PN-group. For fixed j Lemma 1 (i) gives $\sum_{i=1}^{s}\min(m_j, k_i)\geqq m_j$. In fact, this is obvious if $m_j\leqq k_i$ for some i. If $m_j>k_i$ for all i, then $\sum_{i=1}^{s}\min(m_j, k_i)=k\geqq m_j$ by assumption. Hence $a\geqq\sum_{j=1}^{t}m_j=m$. Therefore we may assume that $G=H\times K$, where H is abelian and K is a PN-group. Let $|H|=p^r$ $(r>0)$. Since $G/G'=H\times K/K'$ and $Z=H\times Z(K)$, we get $|K/K'|=p^{m-r}$ and $|Z(K)|=p^{k-r}$. Let $a_1\geqq a_2\geqq\cdots\geqq a_d\geqq 1$ be the invariants of K/K', $\exp Z(K)=p^u$ and $p^v=|A_c(K)|=|\mathrm{Hom}(K/K', Z(K))|$. For $u\geqq a_1$, $v\geqq\sum a_i$ and for $a_i>u$ with $a_{i+1}\not> u$, $v\geqq(k-r)i+a_{i+1}+\cdots+a_d$. Similarly, let $\exp H=p^b$ and $p^l=|\mathrm{Hom}(K, H)|=|\mathrm{Hom}(K/K', H)|$. Then, as above, $l\geqq\sum a_i$ for $b\geqq a_1$ and $l\geqq rj+a_{j+1}+\cdots+a_d$ for $a_j>b$ with $a_{j+1}\not> b$. Since $k\geqq a_1$, we get, in all cases, that $v+l\geqq\sum a_i=m-r$. Since $|A(H)|\geqq p^{r-1}$ and $|\mathrm{Hom}(H, Z(K))|\geqq p$, by Lemma 1 (ii) we get

$$|A_c(G)|\geqq p^{r-1+v+l+1}\geqq p^m .$$

A.D. Otto proved in ([7]) that if L_i/L_{i+1} has order p for all $i=1, \cdots, c-1$ and $\exp G/L_1=p$ then G is an LA-group. The following theorem is a generalization of Otto's result. First we need the following lemma.

LEMMA 3. $\mathrm{Exp}\, L_{i+1}\leqq[L_i: L_i\cap Z]$ *for all* $i\geqq 0$.

PROOF. Let τ be the transfer homomorphism of L_i into $L_i\cap Z$ and let $[L_i: L_i\cap Z]=p^r$ and $x\in L_i$. Then $\tau(x)=\prod_i a_i x^{p^{r_i}}a_i^{-1}$, where $a_i x^{p^{r_i}}a_i^{-1}\in L_i\cap Z$ and $\sum_i p^{r_i}=p^r$. Hence, $a_i x^{p^{r_i}}a_i^{-1}=x^{p^{r_i}}$ and so $\tau(x)=x^{p^r}$. Let $y\in G$. Since $x^{p^r}\in L_i\cap Z\leqq Z$, x^{p^r} commutes with y for every $y\in G$. So $[x, y]^{p^r}=\tau([x, y])=\tau(x^{-1}y^{-1}xy)=\tau(x^{-1})\tau(y^{-1}xy)=x^{-p^r}(y^{-1}xy)^{p^r}=1$. Thus, $\exp L_{i+1}\leqq p^r$.

THEOREM 1. *If* L_i/L_{i+1} *is cyclic of order* p^r $(r>0)$ *for all* $i=1, \cdots, c-1$ *and* $\exp G/L_1\leqq|Z|$, *then* G *is an* LA-*group*.

PROOF. Since $|L_i/L_{i+1}|=p^r$ for $i=1, \cdots, c-1$,

$$n=m+(c-1)r . \tag{1}$$

Also we have

$$|Z_{i+1}/Z_i|\geqq|L_{c-i-1}Z_i/Z_i|=|L_{c-i-1}/L_{c-i-1}\cap Z_i|. \tag{2}$$

We shall show that $L_{c-i-1}\cap Z_i=L_{c-i}$. This is trivial for $i=0$, and for $i=1$ by Lemma 3, $p^r=\exp L_{c-1}\leqq[L_{c-2}: L_{c-2}\cap Z]\leqq[L_{c-2}: L_{c-1}]=p^r$, as $L_{c-1}\leqq L_{c-2}\cap Z$. Hence $L_{c-1}=L_{c-2}\cap Z$. Assuming $L_{c-i-1}\cap Z_i=L_{c-i}$, then $[G, Z_{i+1}\cap L_{c-i-2}]\leqq Z_i\cap L_{c-i-1}=L_{c-i}$ and so modulo L_{c-i} we have $Z_{i+1}(G/L_{c-i})\cap L_{c-i-2}(G/L_{c-i})\leqq Z(G/L_{c-i})\cap L_{c-i-2}(G/L_{c-i})=L_{c-i-1}(G/L_{c-i})$. Therefore $Z_{i+1}\cap L_{c-i-2}\leqq L_{c-i-1}$. Since $L_{c-i-1}\leqq Z_{i+1}\cap L_{c-i-2}$ we get $L_{c-i-1}=Z_{i+1}\cap L_{c-i-2}$. Thus $L_{c-i-1}\cap Z_i=L_{c-i}$

for $i=1, \cdots, c-2$. From (2) we get

$$|Z_{i+1}/Z_i| \geqq |L_{c-i-1}/L_{c-i}| = p^r. \tag{3}$$

Let K/L_3 be the centralizer of L_1/L_3 in G/L_3. Then by ([2], Lemma 2.5) G/K has order p^r. It is easily seen that theorems 2.6, 2.7 and corollary in ([2]) hold for p-groups with homocyclic lower central factors. Hence $|K/Z_{c-1}| = p^r$ and so

$$|G/Z_{c-1}| = p^{2r}. \tag{4}$$

From (1), (3), (4) we get $m+(c-1)r \geqq 2r+(c-3)r+v+k$, where $|Z_2/Z| = p^v$. Then $m \geqq v+k$ and Lemma 2 gives $|A_c(G)|_p \geqq p^{v+k}$. Therefore

$$|A(G)|_p \geqq |I(G)\cdot A_c(G)|_p = |I(G)|\cdot|A_c(G)|_p/|Z_2/Z| \geqq p^{n-k+v+k-v} = p^n.$$

COROLLARY 1.1. *If the Frattini subgroup $\Phi(G)$ of G is cyclic, then G is an LA-group.*

PROOF. Let $p \neq 2$. Since $G' \leqq \Phi(G)$, G' is cyclic and so G is regular. Then $|E(G/E(G))| = |E_2(G)/E(G)| = |P(G)/P_2(G)|$. But $P(G) \leqq \Phi(G)$ gives that $P(G)$ is cyclic and $|P(G)/P_2(G)| \leqq p$. Hence $|E(G/E(G))| \leqq p$ and $G/E(G)$ has at most one subgroup of order p. Then $G/E(G)$ is cyclic and so $G' \leqq E(G)$. Since G is regular, $\exp E(G) = p$ which gives $\exp G' = p$. Since G' is cyclic, $|G'| = p$ and G has class two. Let $p=2$. Then $P(G) = \Phi(G)$. So there exists $a \in G$ such that $\Phi(G) = \langle a^2 \rangle$. Let S be the set of all subgroups H of G containing a such that $\langle a \rangle$ has index p in H for every H in S. For $x \in G$, $x^2 \in \Phi(G)$, so $G = \langle H | H \in S \rangle$. Let $H \in S$. Then H has a maximal subgroup which is cyclic so that H is either (i) abelian, (ii) class two with $H/Z(H)$ elementary abelian of order 4 or (iii) of maximal class. If there exists no element in S of maximal class, then $a^2 \in Z(H)$ for every $H \in S$ and so $\Phi(G) = \langle a^2 \rangle \leqq Z$ and G is of class two. If H is of maximal class for some H in S, then $|H/H'| = 4 = |H/\Phi(G)|$ so that $G' = \Phi(G)$ as $H' \leqq G' \leqq \Phi(G)$. Thus $\exp G/G' = p$ and L_i/L_{i+1} is cyclic of order p for all $i = 1, \cdots, c-1$. Then by Theorem 1, G is an LA-group.

.

. .

For any finite p-group G of class $c>2$, G/Z_{c-1} is non-cyclic and $|Z_i/Z_{i-1}| \geqq p$ for $i=1, \cdots, c-1$. Hence $|G/Z_2| \geqq p^{c-1}$ and $|A(G)| \geqq |I(G)\cdot A_c(G)| = |A_c(G)| \cdot |G/Z_2| \geqq |A_c(G)| \cdot p^{c-1}$. Also Lemma 1 gives $|A_c(G)|_p \geqq p^{2s}$. Hence,

LEMMA 4. *If G has class $c>2$, $|A(G)|_p \geqq |A_c(G)|_p \cdot p^{c-1} \geqq p^{2s+c-1}$.*

By this result, any p-group of maximal class is an LA-group. Below we consider the case in which G has certain normal subgroups of maximal class.

THEOREM 2. *Let G have a normal subgroup M which has maximal class. Then G is an LA-group, if either,*

(i) *G/M is elementary abelian, or*

(ii) *M has index p^2 in G.*

PROOF. Let $|G/M|=p^a$ and $M=\bar{L}_0>\bar{L}_1>\cdots>\bar{L}_{c'}=1$ be the lower central series of M, where $c'=n-a-1$ is the class of M. Then $c\geqq c'$. Since any non-abelian finite p-group has an outer automorphism of order p^r, $r\geqq 1$ ([4]), we may assume that $|Z|>p$, otherwise $|A(G)|_p\geqq p|I(G)|=|G|$.

(i) $L_1\leqq \Phi(G)\leqq M$, as G/M is elementary abelian. Also $\Phi(G)\neq M$, as $\Phi(G)$ cannot be of maximal class. Hence $L_1<M$ and so $m\geqq a+1$. On the other hand $|L_i/L_{i+1}|\geqq p$ for $i=1,\cdots,c-1$ so that $|L_1|\geqq p^{c-1}$ which gives $m\leqq a+2$. Therefore either $m=a+1$, or $m=a+2$. Since $p=\exp(G/\Phi(G))=\exp(G/L_1/\Phi(G)/L_1)$ and $|\Phi(G)/L_1|\leqq p$, we get $\exp(G/L_1)\leqq p^2\leqq |Z|$.

Then Lemma 2 gives $|A_c(G)|_p\geqq p^m$. By Lemma 4, it is enough to show that $m+c-1\geqq n$. This is true for $m=a+2$ as $c\geqq n-a-1$.

Therefore we may assume that $m=a+1$. Then $|L_1/\bar{L}_1|=p$. Since $\bar{L}_1\lhd G$, $L_1/\bar{L}_1\leqq Z(G/\bar{L}_1)$ which gives $L_2=[G, L_1]\leqq \bar{L}_1$. Since M/L_1 is cyclic, $\bar{L}_1=[M, L_1]$ ([2], Lemma 2.1) and so $L_2=[L_1, G]\geqq[L_1, M]=\bar{L}_1$. Thus $L_2=\bar{L}_1$. Assuming by induction that $L_{i+1}=\bar{L}_i$ we get $\bar{L}_i=L_{i+1}>L_{i+2}=[L_{i+1}, G]\geqq[\bar{L}_i, M]=\bar{L}_{i+1}$. Since M is of maximal class, $|\bar{L}_i/\bar{L}_{i+1}|=p$ and so $L_{i+2}=\bar{L}_{i+1}$. Therefore $L_{i+1}=\bar{L}_i$ for all i. So $L_{c'+1}=\bar{L}_{c'}=1$ and $L_{c'}=\bar{L}_{c'-1}\neq 1$. Thus G has class $c=c'+1=n-a$ and $m+c-1=a+1+n-a-1=n$.

(ii) From (i) we may assume that G/M is cyclic of order p^2 and $c\geqq c'=n-3$.

Since G/L_1 cannot be cyclic, $L_1<M$ and $m\geqq 3$. Also $|L_1|\geqq p^{c-1}$ gives $m\leqq 4$ so that either $m=3$ or $m=4$. Let $m=3$. Proceeding as in (i) we get $c=c'+1=n-2$, and so Lemmas 2 and 4 give $|A(G)|_p=p^3\cdot p^{c-1}=p^n$, as $\exp(G/L_1)\leqq p^2\leqq|Z|$. Let $m=4$. Then $|L_i/L_{i+1}|=p$ for all $i\geqq 1$ and $c=n-3$. Since $|G/L_1|=p^4=|G/M||M/\bar{L}_1|=|G/\bar{L}_1|$ we get $L_1=\bar{L}_1$ and by ([5]) G cannot be generated by two elements. Therefore G/L_1 has more than two invariants and $\exp(G/L_1)\leqq p^2\leqq|Z|$. Again Lemmas 2 and 4 give $|A(G)|_p\geqq p^4\cdot p^{c-1}=p^n$.

THEOREM 3. *Let M be a maximal subgroup of G. If M contains a normal subgroup H of order p such that M/H is of maximal class, then G is an LA-group.*

PROOF. Since $|M/H|=p^{n-2}$, M/H has class $n-3$ and so M has class $c'\geqq n-3$. For $c'=n-2$ the result follows from the previous theorem.

Take $c'=n-3$. Since $H\lhd M$ and $|H|=p$, $H\leqq Z(M)$. Let $Z(M)$ be cyclic. Since M has order p^{n-1} and class $n-3$, $p^2\leqq|M/M'|\leqq p^3$ so that M/M' has either type (p, p), (p, p^2) or (p, p, p). In all cases $\exp L_{c'-1}(M)=p$. Since $L_{c'-1}(M)\leqq Z(M)$ and $Z(M)$ is cyclic, $L_{c'-1}(M)$ is cyclic of order p. As $Z(M)$ has only one subgroup H of order p, $H=L_{c'-1}(M)$ and so $L_{c'-1}(M/H)=1$ a contradiction. Hence $Z(M)$ is elementary abelian of order p^2. By Lemma 4, $|A(M)|_p$

$\geqq p^{c'+3}=p^n$. If $Z\nleqq M$, $G=ZM$ and by ([6]), $|A(G)|_p\geqq|G|$. Let $Z\leqq M$. Then $Z\leqq Z(M)$. As in Theorem 2, we may assume that $|Z|>p$ so that Z is elementary abelian of order p^2. Then Lemma 4 gives $|A(G)|_p\geqq p^{c+3}\geqq p^n$.

References

[1] J.E. Adney and Ti. Yen, Automorphisms of a p-group, Illinois J. Math., **9** (1965), 137-143.

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

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

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

[5] C. Hobby and C.R.B. Wright, A generalization of a theorem of N. Itô on p-groups, Proc. Amer. Math. Soc., **11** (1960), 707-709.

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

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

Theodoros EXARCHAKOS
41, Kuduriotu Street
Korydallos, Athens
Greece