

# 关于P-群的自同构群的阶

肖长城\*

(广西民族学院)

## 摘 要

若  $p$ -群  $G$  不循环且  $|G| > p^2$  时有  $|G| \mid |\text{Aut}(G)|$ , 则称  $G$  为  $LA$ -群. 本文证明若干类  $p$ -群为  $LA$ -群, 并引进  $DN$ -群的概念简化论题.

## 一、前 言

$p$ -群的自同构群之阶, 其上限已于 1933 年由  $G. Birkhoff$  与  $p. Hall$  解决<sup>[1]</sup>, 而其下限至今仍在探索之中. 近年来, 人们猜想: 任意一个阶大于  $p^2$  的非循环  $p$ -群  $G$  的阶  $|G|$  整除  $G$  的自同构群的阶  $|\text{Aut}(G)|$ . 文献 [2] 把适合这个猜想的  $p$ -群叫做  $LA$ -群.

$Otto$ <sup>[3]</sup> 首先证明交换  $p$ -群是  $LA$ -群, 又证明若  $p$ -群  $G$  为  $PN$ -群  $B$  与交换群  $p$  的直积, 且  $|B| \mid |\text{Aut}(B)|$ , 则  $|G| \mid |\text{Aut}(G)|$ . ( $PN$ -群是指没有非平凡交换直积因子的非交换  $p$ -群). 这一结果指出, 要证明猜想成立, 只要证明所有的  $PN$ -群是  $LA$ -群. 于是  $Otto$  接着证明若  $G$  是  $ECF(m, n, p)$  型  $PN$ -群, 其中  $n \geq m > 3$ , 则  $|G| \mid |\text{Aut}(G)|$ .  $G$  是  $ECF(m, n, p)$  型, 指  $G$  是  $p^n$  阶  $m-1$  类  $p$ -群,  $G/G_2$  初等交换, 且  $|G_i/G_{i+1}| = p$  ( $i = 2, 3, \dots, m-1$ ), 其中  $G_i$  是下中心列的第  $i$  项). 又证明猜想对中心  $Z$  为初等交换 (设  $|Z| = p^r$ ) 且满足下述任一条件的  $p^n$  阶  $PN$ -群  $G$  也成立: (1)  $r \geq n/2$ ; (2)  $p^r \geq |Z_2/Z|$ ; (3) 若  $G$  的幂零类  $m \geq 3$ , 则  $n+1-2r \leq m$ .

后来  $Faudree$ <sup>[4]</sup>、 $Davitt$ <sup>[5]</sup> 先后证明了幂零类  $2p$ -群与  $p$ -交换  $p$ -群都是  $LA$ -群.  $Davitt$  与  $Otto$ <sup>[6] [7] [8]</sup> 还陆续证明了具有非平凡亚循环中心商群的  $p$ -群 ( $p > 2$ ), 非交换模  $p$ -群 ( $p > 2$ ) 及满足  $|G:Z| \leq p^4$  的  $p$ -群都是  $LA$ -群.

$Exarchakos$ <sup>[2]</sup> 证明了下述几类  $p$ -群  $G$  是  $LA$ -群. (1)  $G$  的下中心列商因子  $L_i/L_{i+1} = p^r$  ( $r > 0, i = 1, \dots, C-1$ ), 且  $e \times pG/L_1 \leq |Z|$ ; (2)  $G$  中存在一个最大类的正规子群  $M$  满足 (i)  $G/M$  初等交换或 (ii)  $M$  在  $G$  中的指数为  $p^2$ ; (3)  $G$  的一个极大子群  $M$  含有阶为  $p$  的正规子群  $H$ , 而  $M/H$  有最大类. 并且证明了  $Frattini$  子群  $\Phi(G)$  循环的  $p$ -群  $G$  是上述第 1 类  $p$ -群因而是  $LA$ -群, 还推得最大类  $p$ -群是  $LA$ -群.

本文首先应用上述一部分结果证明, 含  $p^{n-1}$  阶元的  $p^n$  阶群与某些极大子群的中心循环的  $p$ -群是  $LA$ -群, 接着证明含较大交换直积因子的  $p$ -群、含较大初等交换中心的  $p$ -群及中

本文 1985 年 7 月 20 日收到.

\* 作者系本校数学系 62 级毕业生, 现为广西民族学院数学系讲师.

心商群的阶 $\leq p^{2(r+1)}$ 的某些  $p$ -群都是  $LA$ -群, 并引进  $DN$ -群的概念及给出  $DN$ -为  $LA$ -群的一些充分条件.

下文以  $H \leq G$  与  $H < G$  分别表示  $H$  是  $G$  的子群与真子群.  $\langle a, b, \dots \rangle$  表示由  $a, b, \dots$  生成的群,  $G = G_1 < G_2 < \dots < G_{c+1} = 1$  表示  $G$  的下中心列, 其中  $C$  为  $G$  的幂零类,  $C_c(A)$  表示  $A$  在  $G$  里的中心化子,  $G \cong H$  表示  $G$  与  $H$  同构,  $A_c(G)$  表示群  $G$  的中心自同构群, 还有一些符号用到时再说明.

## 二、猜想成立的某些条件

本节命题 1 可用文献 [2] 的结果推出, 这里用另一方法证之.

**命题 1** 如果  $p^n$  阶群  $G (n > 2)$  含  $p^{n-1}$  阶元, 则  $G$  是  $LA$ -群.

**证** 因交换  $p$ -群是  $LA$ -群<sup>[3]</sup>, 以下只要证  $G$  非交换的情况.

(一)  $p > 2$  时,  $G = \langle a, b \rangle$ ,  $a^{p^{n-1}} = b^p = 1$ ,  $b^{-1}ab = a^{1+p^{n-2}}$ <sup>[9]</sup>.

取  $G$  中任意二元  $u = b^s a^t, v = b^r a^y$ , 可以算出其换位子

$$u^{-1}v^{-1}uv = a^{[(1+p^{n-2})^s - 1]t - [(1+p^{n-2})^r - 1]y},$$

而  $[(1+p^{n-2})^r - 1]t - [(1+p^{n-2})^s - 1]y = p^{n-2} \cdot k$ ,  $k$  为整数.

于是  $u^{-1}v^{-1}uv = (a^{p^{n-2}})^k$ ,

即  $G$  的任一换位子都是  $a^{p^{n-2}}$  的幂, 故  $G_2 \leq \langle a^{p^{n-2}} \rangle$ . 但  $G_3 < G_2$ , 而  $|(a^{p^{n-2}})| = p$ , 故  $G_3 = 1$ . 因此  $G$  为幂零类  $2p$ -群, 由文 [4] 有  $|G| \mid |Aut(G)|$ .

(二)  $p = 2$  时,  $G$  只能有以下四种类型<sup>[10]</sup>:

(I)  $G = \langle a, b \rangle$ ,  $a^{2^{n-1}} = b^2 = 1$ ,  $b^{-1}ab = a^{-1}$  (二面体群  $D_{2^n}$ ,  $n \geq 3$ );

(II)  $G = \langle a, b \rangle$ ,  $a^{2^{n-1}} = 1$ ,  $b^2 = a^{2^{n-2}}$ ,  $b^{-1}ab = a^{-1}$  (四元数群  $Q_{2^n}$ ,  $n \geq 3$ );

(III)  $G = \langle a, b \rangle$ ,  $a^{2^{n-1}} = b^2 = 1$ ,  $b^{-1}ab = a^{1+2^{n-2}}$  ( $n \geq 4$ );

(IV)  $G = \langle a, b \rangle$ ,  $a^{2^{n-1}} = b^2 = 1$ ,  $b^{-1}ab = a^{-1+2^{n-1}}$  ( $n \geq 4$ );

与(一)的证明同理, (III)型为幂零类 2 群, 因而有  $|G| \mid |Aut(G)|$ .

$G$  为 (I) 型时,  $|Aut(G)| = |D_8| = 2^n = |G|$  (当  $n = 3$ );  $|Aut(G)| = 2^{2^{n-3}} |G| = 2^{n-3} |G|$  (当  $n > 3$ );  $G$  为 (II) 型时,  $|Aut(G)| = |S_4| = 2^n \cdot 3 = 3 |G|$  (当  $n = 3$ );  $|Aut(G)| = 2^{2^{n-3}} = 2^{n-3} |G|$  (当  $n > 3$ )<sup>[10]</sup>.

因此,  $G$  为 (I)、(II) 型时都有  $|G| \mid |Aut(G)|$ .

$G$  为 (IV) 型时, 假定  $ba^t \in Z(G)$ , 则  $ba^t \cdot a = a \cdot ba^t = ba^{-1+2^{n-2}} a^t$ , 推得  $a = a^{-1+2^{n-2}}$ , 矛盾 (注意  $n \geq 4$ ), 因此  $Z(G)$  的元素只能为  $a$  的幂, 即  $Z(G) \leq \langle a \rangle$ , 因而  $Z(G)$  循环, 故  $G$  为  $PN$ -群. 又因  $a^{-1}b^{-1}ab = a^{-2+2^{n-2}}$ , 即  $a^{-2+2^{n-2}} \in G_2$ , 故

$$a^2 = a^2(a^{2^{n-1}})^{2^{n-4}-1} = (a^{-2+2^{n-2}})^{2^{(2^{n-4}-1)+1}} \in G_2,$$

因而  $\langle a^2 \rangle \leq G_2$ , 但  $\Phi(G) = \langle a^2 \rangle \langle b^2 \rangle = \langle a^2 \rangle$ , 即有  $\langle a^2 \rangle \leq G_2 \leq \Phi(G) = \langle a^2 \rangle$ ,

于是  $G_2 = \Phi(G)$ , 所以  $G/G_2$  初等交换. 其次  $(a^2)^{-1}b^{-1}a^2b = a^{-2^2}$ , 即  $a^{2^2} \in [G_2, G] = G_3$  因此

$\langle a^{2^2} \rangle \leq G_3$ , 但  $G_3 < G_2$  且  $\langle a^{2^2} \rangle$  为  $G_2 = \langle a^2 \rangle$  的极大子群, 故  $G_3 = \langle a^{2^2} \rangle$ ,

因而  $|G_2/G_3| = |\langle a^2 \rangle / \langle a^{2^2} \rangle| = 2$ . 归纳假设  $G_k = \langle a^{2^{k-1}} \rangle (2 < k \leq n-1)$ ,

则因  $\langle a^{2^{k-1}} \rangle^{-1} b^{-1} a^{2^{k-1}} b = a^{-2^k}$ , 即  $a^{2^k} \in [G_k, G] = G_{k+1}$ ,

因此  $\langle a^{2^k} \rangle \leq G_{k+1}$ . 但  $G_{k+1} < G_k$  且  $\langle a^{2^k} \rangle$  为  $G_k = \langle a^{2^{k-1}} \rangle$  的极大子群,

故  $G_{k+1} = \langle a^{2^k} \rangle$ , 因而  $|G_k/G_{k+1}| = |\langle a^{2^{k-1}} \rangle / \langle a^{2^k} \rangle| = 2$ .

因此 (IV) 型为  $ECF(m, n, p)$  型  $PN$ -群,  $n = m > 3$ , 故  $|G| \mid |Aut(G)|^{[3]}$ .

**命题 2** 若  $p$ -群  $G$  中含  $Z(G)$  的极大子群的中心都循环, 则  $G$  是  $LA$ -群.

**证** 同命题 1 的证明, 我们只须考虑  $G$  非交换的情况. 在此情况下  $Z(G)$  必含于  $G$  的某一极大子群  $H$ , 因而  $Z(G) \leq Z(H)$ . 由命题条件推得  $Z(G)$  循环.

假定  $\Phi(G)$  不循环, 则存在  $(p, p)$  型正规子群  $A \leq \Phi(G)^{[10]}$ . 而  $G$  的元素在  $A$  上导出的内自同构群的阶为  $|G/C_G(A)|$ . 但  $|Aut(A)| = (p^2 - 1)(p^2 - p)$ , 故  $|G/C_G(A)| \leq p$ , 因此  $G_C(A)$  或为  $G$  或为  $G$  的极大子群, 若  $C_G(A) = G$ , 则  $A \leq Z(G)$ , 循环, 不可能, 若  $C_G(A)$  为  $G$  的极大子群, 则因  $C_G(A)$  含  $Z(G)$ , 根据命题条件  $Z(C_G(A))$  循环, 但  $A \leq Z(C_G(A))$ , 亦矛盾. 所以  $\Phi(G)$  循环, 由 [2] 知  $G$  是  $LA$ -群.

### 三、非 $PN$ -群的 $P$ -群

自从文 [3] 证明了某些  $PN$ -群是  $LA$ -群以后, 至今未见有人再继续讨论还有哪些  $PN$ -群是  $LA$ -群. 因此, 我们有必要同时考虑不是  $PN$ -群的  $p$ -群, 本节就是借助文 [11] 的结果给出非  $PN$ -群的  $p$ -群是  $LA$ -群的充分条件.

**定理 1** 设  $p^n$  阶群  $G = H \times K$ , 其中  $K$  交换, 则  $|Aut(K)| \mid |I(G)| \mid |Aut(G)|$ .

**证**  $Aut(K)$  的每一个元  $\tau$  都可以延拓为  $Aut(G)$  的一个元  $\sigma$ :  $hk \rightarrow hk\tau$  ( $h \in H, k \in K$ ), 且易证  $Aut(K)$  的所有元经如此延拓作成与  $Aut(K)$  同构的  $Aut(G)$  的一个正规子群, 它与  $G$  的自同构群  $I(G)$  的直积作成  $Aut(G)$  的一个子群. 因此  $|Aut(K)| \mid |I(G)| \mid |Aut(G)|$ .

**定理 1** 设  $p^n$  阶群  $G = H \times K$ , 其中  $K$  交换,  $|K| = p^{n_1}$ ,  $|Z(G)| = p^{n_2}$ ,  $K$  的极大循环子群的阶为  $p^{n_1-1}$ . 则  $K$  满足下述条件时,  $G$  为  $LA$ -群:

(I)  $K$  的型长  $t \neq 1$  时,  $n_1 + 2(i-1) \geq n_2$

(II)  $K$  的型长  $t = 1$  时,

$n_1 + 2i - 3 \geq n_2$  (当  $K$  不是  $p^3$  或  $p^4$  阶初等交换群)

$n_1 + 2(i-2) \geq n_2$  (当  $K$  是  $p^3$  或  $p^4$  阶初等交换群)

**证** (I) 根据文 [11],  $t \neq 1$  时,  $|K| p^{2(i-1)} \mid |Aut(K)|$ . 故若  $n_1 + 2(i-1) \geq n_2$ , 则有  $p^{n_2} \mid p^{n_1+2(i-1)} \mid |Aut(K)|$ . 由引理 1,  $p^n = p^{n_2} p^{n-n_2} \mid |Aut(K)| \mid |I(G)| \mid |Aut(G)|$ . 即  $G$  是  $LA$ -群.

(II) 与 (I) 同理可由 [11] 证得.

当定理 1 中的  $K$  初等交换时,  $p^{\frac{n_1(n_1-1)}{2}} \mid |Aut(K)|$ . 运用引理 1 我们可以得到更强的结果, 即

**定理 2** 设  $p^n$  阶群  $G = H \times K$ ,  $K$  初等交换,  $|K| = p^n$ ,  $|Z(G)| = p^{n/2}$ , 且  $\frac{n_1(n_1-1)}{2} \geq n_2$ , 则  $G$  为  $LA$ -群.

例如  $|Z(G)| = p^{20}$  时, 由定理 1, 当  $K$  为阶大于等于  $p^9$  的初等交换群时,  $G = H \times K$  为  $LA$ -群; 而由定理 2, 只要  $K$  为阶大于等于  $p^7$  的初等交换群时,  $G = H \times K$  为  $LA$ -群.

#### 四、中心初等交换的 $P$ -群

远用上一节及文 [3] 的一些结果, 可以得到一般  $p$ -群 (即非专指  $PN$ -群) 为  $LA$ -群的一些充分条件. 特别当  $p$ -群的中心初等交换时.

先把文 [3] 的 Cor. 4.3 稍加改进成

**定理 2** 设  $p^n$  阶  $PN$ -群  $G$  的中心  $Z$  是阶为  $p^r$  的初等交换群, 且  $r \geq \frac{n-2}{2}$ ; 则  $G$  为  $LA$ -群.

**证** 若  $G$  的幂零类  $m \leq 2$ , 由 [3] 与 [4]  $G$  为  $LA$ -群. 若  $m \geq 3$ , 则由引理条件得  $n+1-2r \leq 3$ , 因而  $n+1-2r \leq m$ , 根据 [3],  $G$  也为  $LA$ -群.

**定理 3** 设  $p^n$  阶群  $G$  的中心是阶为  $p^r$  的初等交换群, 且  $r \geq \frac{n-1+\sqrt{n-1}}{2}$ , 则  $G$  是  $LA$ -群.

**证** 只要证明  $G$  非交换的情况

由定理条件显然有  $r \geq \frac{n}{2}$ , 故若  $G$  为  $PN$ -群, 根据 [3] 定理真. 若  $G$  不是  $PN$ -群, 可设  $G = B \times P$ , 其中  $B$  是  $PN$ -群,  $P$  是  $p^{n_1}$  阶交换群 ( $n_1 \geq 1$ ).

由  $Z(G) = Z(B) \times P$  及定理条件知  $Z(B)$  与  $P$  都初等交换且  $|Z(B)| = p^{r-n_1}$ .

又因  $|B| = p^{n-n_1}$ , 故若  $r-n_1 \geq \frac{n-n_1-2}{2}$ , 则由引理 2 有  $|B| \mid |Aut(B)|$  但是根据 [3]

$$p^{n_1} |Aut(B)| \nmid p \mid |Aut(G)|, \text{ 故 } |G| = p^{n_1} |B| \nmid |Aut(G)|; \text{ 若 } r-n_1 < \frac{n-n_1-2}{2},$$

$$\text{即 } n > 2r - n_1 + 2, \text{ 则由定理条件 } r \geq \frac{n-1+\sqrt{n-1}}{2} > \frac{2r-n_1+1+\sqrt{2r-n_1+1}}{2},$$

推算出  $\frac{n_1(n_1-1)}{2} > r$ . 于是由定理 2,  $G$  为  $KA$ -群.

定理 3 是在  $p$ -群的中心初等交换的条件下发展了文 [8] 的结果, 即指出中心较大的  $p^n$  阶群是  $LA$ -群. 例如若  $G$  是  $p^{30}$  阶群, 则由 [8] 得,  $|Z(G)| \geq p^{20}$  时  $G$  为  $LA$ -群. 而当  $Z(G)$  初等交换时由定理 3 得, 只要  $|Z(G)| \geq p^{10}$  时  $G$  就为  $LA$ -群.

要用到两个引理:

下面再讨论中心最小的  $p^n$  阶群, 即中心的阶为  $p$  的  $p$ -群

**定理 3** 设  $p$ -群  $G$  的中心  $Z$  初等交换, 则  $Z_2/Z$  也初等交换.

**定理 4**  $I(G) \cap A_c(G) \cong Z_2/Z$

其中  $Z_2/Z$  是  $G/Z$  的中心

引理 3 的证明: 设  $gZ \in Z_2/Z$ , 则对任意  $X \in G$ ,  $gZ$  与  $xZ$  的换位子  $[gZ, xZ] = Z$ , 即有

$[g, x] \in Z$ , 由换位子的性质  $[g', x] = [g, x]'$ . 但  $Z$  初等交换, 故  $[g, x]' = 1$ . 推得  $g' \in Z$ , 可见  $Z_2/Z$  中非单位元都是  $p$  阶元, 因而初等交换.

引理 4 在文 [3] 中已在几处用到, 故其证明省略.

**定理 4** 中心的阶为  $p$  的  $p^n$  阶群  $G (n > 2)$  若满足下述条件之一时必为  $LA$ -群.

(1)  $|Z_2/Z| = p$

(2)  $Z_2/Z$  循环

(3) 设  $G/G_2$  为  $(n_1, n_2, \dots, n_k)$  型,  $|Z_2/Z| = P^r$ , 则  $k \geq r+1$ .

**证** 中心的阶为  $p$  的  $p^n$  阶群  $G (n > 2)$  是  $PN$ -群, 故由 [3] 知,  $|Z_2/Z| = P$  时定理成立. 又由引理 3 知,  $Z_2/Z$  循环必有  $|Z_2/Z| = P$ , 因而条件 (1) 或 (2) 满足时  $G$  为  $LA$ -群.

再由 [3],  $|A_c(G)| \geq p^c$ , 其中  $c = 1 \cdot \sum_{x \geq 1} b_x$ , 而由定理条件 (3) 得  $\sum_{x \geq 1} b_x = k$ . 另一方面, 由引理 4  $|A_c(G) I(G)| = |A_c(G)| |I(G)| / |Z_2/Z| = p^{k+n-1-r}$ . 又由条件 (3) 有  $p^n |p^{k+n-1-r}| |Aut(G)|$ . 故条件 (3) 满足时  $G$  也为  $LA$ -群.

## 五、猜想证明的简化与 $DN$ -群

*Hummel* 在文 [12] 中证明: 若  $p$ -群  $G$  可分解成两个真子群  $H$  与  $A$  的中心积 (即  $G = HA$ ,  $H$  中元与  $A$  中元可交换),  $A$  交换且  $|H| \mid |Aut(H)|$ , 则  $|G| \mid |Aut(G)|$  有了这一结果就可以把证明所有  $p$ -群都是  $LA$ -群, 简化成只要证明所有无交换中心积因子 (指非平凡的, 下同) 的非交换  $p$ -群都是  $LA$ -群. 由于无交换中心积因子的非交换  $p$ -群必为  $PN$ -群, 而  $PN$ -群不必为无交换中心积因子的  $p$ -群. 因此 *Hummel* 这一结果比 *Otto* 的前述结果 (见前言) 更进一步. *Hummel* 还指出对  $p$ -群  $G$  来说,  $G$  无交换中心积因子与  $G$  满足  $Z(G) \leq \Phi(G)$  这两个条件等价.

*Hummel* 的结果还可以再推进一步.

**引理 5** 若  $G = B_1 \times B_2 \times \dots \times B_r$ , 则  $|Aut(B_1)| |Aut(B_2)| \dots |Aut(B_r)| \mid |Aut(G)|$ .

只要仿引理 1 把  $Aut(B_i)$  ( $i = 1, \dots, r$ ) 延拓后, 可以推得  $Aut(B_1) \times Aut(B_2) \times \dots \times Aut(B_r)$  与  $Aut(G)$  的一个子群同构, 因而证得本引理.

**引理 6** 若  $G = B_1 \times B_2 \times \dots \times B_r$ , 且  $G$  满足极大条件,  $Z(G) \leq \Phi(G)$ , 则  $Z(B_i) \leq \Phi(B_i)$  ( $i = 1, \dots, r$ ).

**证** 由

$$G = B_1 \times B_2 \times \dots \times B_r \quad (I)$$

得  $Z(G) = Z(B_1) \times Z(B_2) \times \dots \times Z(B_r)$  与

$$\Phi(G) = \Phi(B_1) \times \Phi(B_2) \times \dots \times \Phi(B_r) \quad (II)$$

若某一  $Z(B_i) \not\leq \Phi(B_i)$ , 不妨设  $Z(B_1) \not\leq \Phi(B_1)$ , 则  $Z(B_1)$  中存在一元  $z \in \Phi(B_1)$ . 但  $Z(B_1) \leq Z(G) \leq \Phi(G)$ , 故  $z \in \Phi(G)$ , 由 (II)  $z = z_1 z_2 \dots z_r$ , 其中  $z_i \in \Phi(B_i)$ , 因而  $z_i \in B_i$ . 但  $z \in Z(B_1) \leq B_1$ , 故由 (I) 不得不有  $z_2 = z_3 = \dots = z_r = 1$ , 而  $z_1 = z \in \Phi(B_1)$ , 矛盾. 故  $Z(B_i) \leq \Phi(B_i)$  ( $i = 1, \dots, r$ ).

任意一个  $p$ -群  $G$  都可以分解成为无直积因子的诸  $p$ -群的直积, 且由引理 6 若  $G$  满足

$Z(G) \leq \Phi(G)$ , 则分解出来的直积因子也满足. 因此只要能证明满足  $Z(G) \leq \Phi(G)$  且无直积因子的  $p$ -群  $G$  为  $LA$ -群, 则由引理 5 及引理 6, 满足  $Z(G) \leq \Phi(G)$  的  $p$ -群  $G$  都是  $LA$ -群, 因而所有  $p$ -群都是  $LA$ -群<sup>[12]</sup>.

为叙述方便, 作如下定义:

**定义**  $G$  称为  $DN$ -群, 如果  $G$  是满足  $Z(G) \leq \Phi(G)$  且无直积因子的  $p$ -群.

于是上述结果可以写成

**定理 5** 若  $DN$ -群是  $LA$ -群, 则  $p$ -群都是  $LA$ -群(即前言所述的猜想成立).

容易证明, 中心循环且满足  $Z(G) \leq \Phi(G)$  的  $p$ -群  $G$  是  $DN$ -群. 但是,  $DN$ -群不必为中心循环的  $p$ -群, 如下例

$$G = \langle a, b \rangle, \quad a^{3^3} = b^{3^3} = 1, \quad b^{-1}ab = a^{4^{13}}.$$

先证明:  $Z(G) = \langle a^{3^2} \rangle \times \langle b^{3^2} \rangle$

对任意  $b^s a^t \in G$ , 若  $s = 0$ , 则有  $b^s a^t \cdot a^{3^2} = a^{3^2} \cdot b^s a^t$ . 若  $1 \leq s < 3^3$ , 则  $4^s - 1 = (4 - 1)(4^{s-1} + 4^{s-2} + \cdots + 4 + 1) = 3k$ ,  $k = 4^{s-1} + 4^{s-2} + \cdots + 1$ , 即  $a^{4^s - 1} = a^{3k}$ , 因此  $a^{4^s - 1} a^{-3^2} = a^{3^2}$  ( $4^s - 1 = a^{3^2} = 1$ ), 即  $a^{4^s - 1} = a^{3^2}$ , 故  $a^{3^2} \cdot b^s a^t = b^s a^{4^s - 1} a^t = b^s a^{3^2} a^t$ , 因此  $a^{3^2} \in Z(G)$ .

又对任意  $b^s a^t \in G$ , 因  $4^{3^2} - 1 = (3 + 1)^9 - 1 = 3^3 k$ ,  $k$  为整数,

故  $a^{4^{3^2} - 1} = a^{(4^{3^2} - 1)a^t} = a^{3^3 k} a^t = a^t$ . 因此  $b^s a^t \cdot b^{3^2} = b^s b^{3^2} a^{4^{3^2} - 1} = b^{3^2} \cdot b^s a^t$ , 于是  $b^{3^2} \in Z(G)$ .

所以  $Z(G) \geq \langle a^{3^2} \rangle \langle b^{3^2} \rangle = \langle a^{3^2} \rangle \times \langle b^{3^2} \rangle$ .

其次, 对任意  $a^u b^v \in G$ , 若  $u$  无  $3^2$  因子, 则  $a^{4^{v+1}u} a^{-4^v u} = a^{3^2 u} \neq 1$ , 因而  $a^{4^{v+1}u} \neq a^{4^v u}$ . 故  $a^u b^v \cdot b = b^{v+1} a^{4^{v+1}u} \neq b b^v a^{4^v u} = b \cdot a^u b^v$ , 因此  $a^u b^v \notin Z(G)$ . 若  $v$  无  $3^2$  因子, 则由  $4^v - 1 = (3 + 1)^v - 1 = 3^v + v \cdot 3^{v-1} + \cdots + \frac{v(v-1)}{2} 3^2 + v \cdot 3$  易证  $4^v - 1$  无  $3^3$  因子, 故  $a^{4^v - 1} \neq 1$ ,

即  $a^{4^v} \neq a$ , 故  $a \cdot a^u b^v = b^v a^{4^v(u+1)} \neq b^v a^{4^v u} a = a^u b^v \cdot a$ , 因此  $a^u b^v \notin Z(G)$ .

于是, 又有  $Z(G) \leq \langle a^{3^2} \rangle \times \langle b^{3^2} \rangle$ , 所以  $Z(G) = \langle a^{3^2} \rangle \times \langle b^{3^2} \rangle$ .

但是  $\Phi(G) = \langle a^3 \rangle \langle b^3 \rangle$ , 故  $Z(G) \leq \Phi(G)$ .

下面证  $G$  无直积因子:

假定  $G = B_1 \times B_2$ , 其中  $B_1, B_2$  非平凡. 分两种情况考虑:

1.  $|B_1| = |B_2| = 3^3$ . 若  $B_i \cap \langle a \rangle = 1$  ( $i = 1$  或  $2$ ), 则  $G = B_i \times \langle a \rangle$ , 推得  $Z(G) \geq \langle a \rangle$ , 与  $Z(G) = \langle a^{3^2} \rangle \times \langle b^{3^2} \rangle$  矛盾, 于是  $B_i \cap \langle a \rangle \neq 1$  ( $i = 1, 2$ ), 但又因此推得  $B_1 \cap B_2 \geq \langle a^{3^2} \rangle \neq 1$ , 也不可能.

2.  $|B_1| > |B_2|$ . 则有  $|B_2| < 3^3$ , 因而  $B_2$  交换, 即  $G$  有交换直积因子, 与  $Z(G) \leq \Phi(G)$  矛盾. 同理  $|B_1| < |B_2|$  也不可能.

故  $G$  是中心不循环的  $DN$ -群.

上例说明中心循环的  $DN$ -群是特殊类型的  $DN$ -群, 命题 2 与定理 4 证明的  $LA$ -群都是中心循环的  $PN$ -群与  $DN$ -群, 而下面两个定理证明的  $LA$ -群则包括中心不循环的一些  $DN$ -群.

**定理 6** 设  $p^n$  阶  $DN$ -群  $G$  的中心是  $p^r$  阶的初等交换群,  $|\Phi(G): Z(G)| \leq p^{n-r-\frac{n-2}{r}}$ ,

且满足下述两个条件之一, 则  $G$  为  $LA$ -群.

$$(I) \Phi(G) = G_2$$

$$(II) G/G_2 \text{ 初等交换.}$$

证 由引理 4,  $|A_c(G) \cdot I(G)| = |A_c(G)| \cdot |I(G)| / |Z_2/Z|$ . 若  $|Z_2/Z| = |G/Z|$ , 则  $G$  为幂零类 2 群, 因而是  $LA$ -群<sup>[4]</sup>. 以下设  $|Z_2/Z| < |G/Z|$ , 即有  $|Z_2/Z| \leq p^{n-r-2}$ . 于是

$$|A_c(G)I(G)| \geq |A_c(G)| p^{n-r}/p^{n-r-2} = p^2 |A_c(G)| \quad (I)$$

(I) 若  $\Phi(G) = G_2$ , 则  $G/G_2$  初等交换, 且  $|G/G_2| = |G/\Phi(G)| = |G/Z(G)| / |\Phi(G)/Z(G)|$ . 但由定理条件  $|\Phi(Z)/Z(G)| \leq p^{n-r-\frac{n-2}{2}}$ , 故  $|G/G_2| \geq p^{n-r-(n-r-\frac{n-2}{2})} = p^{\frac{n-2}{2}}$ . 根据

据 [3],  $|A_c(G)| = p^4 = p^r \sum_{x \geq 1} bx \geq p^r \frac{p^{n-2}}{r} = p^{n-2}$ . 于是由 (I)  $|A_c(G)I(G)| \geq p^2 p^{n-2} = p^n$ ;

推得  $|G| \mid |A_c(G)I(G)| \mid |Aut(G)|$ .

(II) 根据  $p$ -群的性质  $\Phi(G) \geq G_2$ , 但  $G/G_2$  初等交换, 故又有  $\Phi(G) \leq G_2$ . 因此  $\Phi(G) = G_2$ , 同 (I) 得证.

**定理 7** 设  $G$  为  $p^n$  阶  $DN$ -群,  $|Z_2| \leq |G/G_2|$  且  $e \times pG/G_2 \leq |Z|$ , 则  $G$  为  $LA$ -群.

证 设  $|Z| = p^r$ ,  $|G_2| = p^t$ .

由定理条件  $|Z_2| \leq |G/G_2|$  得  $|Z_2/Z| \leq |G/G_2|/|Z| = p^{n-r-t}$ . 由引理 4,  $|A_c(G)I(G)| = |A_c(G)| \cdot |I(G)| / |Z_2/Z| \geq |A_c(G)| p^{n-r}/p^{n-r-t} = p^t |A_c(G)|$ . 又因  $e \times pG/G_2 \leq p^r$ , 根据 [3],

$|A_c(G)| \geq p^c = p \sum_{k=1}^r kb_k = p^{n-t}$ . 故有  $|A_c(G)I(G)| \geq p^t p^{n-t} = p^n$ , 因此  $G$  是  $LA$ -群.

**推论** 设  $G$  为  $p^n$  阶  $DN$ -群,  $|G_2| \leq p^2$  且  $e \times pG/G_2 \leq |Z|$ , 则  $G$  为  $LA$ -群.

证 因  $DN$ -群非交换, 故  $|G_2| \neq 1$ . 若  $|G_2| = p$ , 则  $G$  为幂零类 2 群, 推论真<sup>[4]</sup>. 下面考虑  $|G_2| = p^2$  的情况: 当  $|Z_2/Z| = |G/Z|$  时,  $G$  也为幂零类 2 群, 推论真; 当  $|Z_2/Z| < |G/Z|$  时, 则有  $|Z_2| \leq p^{n-2}$ , 因而  $|Z_2| \leq |G/G_2|$ , 由定理 7, 推论成立.

定理 7 与推论中的条件  $G$  为  $DN$ -群减弱为  $G$  为  $PN$ -群时也成立.

还有哪些  $DN$ -群是  $LA$ -群, 有待于继续探讨. 与此同时也可以考虑非  $DN$ -群, 我们有

**定理 8** 如果满足  $Z(G) \leq \Phi(G)$  的  $p$ -群  $G$  可以分解成  $r$  个 ( $r \geq 2$ )  $p$ -群的直积, 且  $|G/Z(G)| \leq p^{2(r+1)}$ , 则  $G$  为  $LA$ -群.

证 设  $G = B_1 \times B_2 \times \cdots \times B_r$ , 则  $Z(G) = Z(B_1) \times Z(B_2) \times \cdots \times Z(B_r)$ , 因而  $|B_1/Z(B_1)| \cdot |B_2/Z(B_2)| \cdots |B_r/Z(B_r)| = |G/Z(G)| \leq p^{2(r+1)}$ .

若某一  $|B_i/Z(B_i)| > p^4$ , 则  $\prod_{i=1}^r |B_i/Z(B_i)| < p^{2(r-1)}$ . 于是必有某一  $|B_j/Z(B_j)| < p^2$ ,

由  $p$ -群的性质知,  $B_j$  交换. 但由定理条件与引理 6 有  $Z(B_j) \leq \Phi(B_j)$ , 矛盾. 故  $|B_i/Z(B_i)| \leq p^4$  ( $i = 1, 2, \dots, r$ ), 由 [8],  $B_1, B_2, \dots, B_r$  都是  $LA$ -群, 因而由引理 5,  $G$  是  $LA$ -群.

本文承李世余、俞曙霞老师和曹锡华、陈重穆教授的帮助, 作者谨此表示感谢.

## 参 考 文 献

- [1] G. Birkhoff and P. Hall, On the order of group of automorphism, Trans. Amer. Math. Soc., 39(1936)496—499.
- [2] T. Exarchakos, LA-groups, J. Math. Soc. Japan, 33, 2(1981), 185—190.
- [3] A. D. Otto, Central automorphism of a finite p-group, Trans. Amer. Math. Soc., 125(1966), 280—287.
- [4] R. Faudree, A note on the automorphism group of a p-group, Proc. Amer. Math. Soc., 19(1968), 1379—1382.
- [5] R. M. Davitt, The automorphism group of finite p-abelian p-groups, Illinois J. Math., 16(1972), 76—85.
- [6] R. M. Davitt and A. D. Otto, On the automorphism group of a finite p-group with the central quotient meta-cyclic, Proc. Amer. Math. Soc., 30(1971), 467—472.
- [7] R. M. Davitt and A. D. Otto, On the automorphism group of a finite modular p-group, Proc. Amer. Math. Soc., 35(1972), 399—404.
- [8] R. M. Davitt, On the automorphism group of a finite p-group with a small central quotient, Can. J. Math., 32(1980)1168—1176.
- [9] 张远达, 有限群构造, 科学出版社, 北京, (1982).
- [10] 徐明耀, 有限群讲义, 北京大学, (1982).
- [11] 俞曙霞, 有限交换P-群的自同构群的阶的几点注记, 数学杂志, 32(1983), 189—191.
- [12] K. Hummel, The order of the automorphism group of a central product, Proc. Amer. Math. Soc., 47(1975), 37—40.
- [13] 徐明耀, 杨燕昌, 有限p-群的半p-交换性和正则性, 数学学报, 19, 4(1976), 281—285.

## The Order of Automorphism of P-Group

Xiao Changcheng

## Abstract

P-group  $G$  is called LA-group if  $|G| \mid |\text{Aut}(G)|$  when  $G$  is non-cyclic and  $|G| > p^2$ . This paper shows that several classes of p-group are LA-groups and introduces the concept of MN-group to simplify the problem.