

一类中心循环的有限 p -群的多项式自同构

徐涛, 张振辉

(河北工程大学数理学院, 河北邯郸 056038)

摘要: 本文研究了一类中心循环的有限 p -群的多项式自同构, 给出了这类有限 p -群的多项式自同构群的结构.

关键词: 多项式自同构; 有限 p -群; 内自同构

MR(2010) 主题分类号: 20D15; 20D45

中图分类号: O152

文献标识码: A

文章编号: 0255-7797(2025)02-0173-09

1 引言

本文涉及的群都是有限群, 采用的符号和术语都是标准的, 参照 [1].

设 α 是群 G 的自同构, 如果对于任意的 $x \in G$, 存在整数 $\epsilon_1, \epsilon_2, \dots, \epsilon_k$ 和 G 中元素 v_0, v_1, \dots, v_k , 使得

$$\alpha(x) = v_0 x^{\epsilon_1} v_1 \cdots v_{k-1} x^{\epsilon_k} v_k,$$

那么称 α 是 G 的多项式自同构. 因为 $\alpha(1) = 1$, 所以多项式自同构可以写成如下形式

$$\alpha(x) = (u_1^{-1} x^{\epsilon_1} u_1) \cdots (u_k^{-1} x^{\epsilon_k} u_k).$$

不难发现内自同构是多项式自同构. 有限群 G 的所有多项式自同构构成的集合记为 $\text{PAut}(G)$. 可以验证 $\text{PAut}(G)$ 是 G 的自同构群 $\text{Aut}(G)$ 的正规子群, 且有下列的正规群列

$$1 \trianglelefteq \text{Inn}(G) \trianglelefteq \text{PAut}(G) \trianglelefteq \text{Aut}(G).$$

群的多项式自同构的研究主要有两方面. 一方面, 研究多项式自同构与其它自同构的联系和区别. 如 Frohlich [2] 给出了非交换有限单群的自同构是多项式自同构, Endimioni [3] 指出了 n 次对称群 S_n 的自同构是多项式自同构; 另一方面, 确定给定群的 $\text{PAut}(G)$ 的结构. 如 Schweigert 在 [4] 中证明了如果 G 是有限可解群, 那么 $\text{PAut}(G)$ 是可解群.

众所周知, 如果群 G 的正规子群 G_1, G_2, \dots, G_n , 满足 i) $G = G_1 G_2 \cdots G_n$, ii) $[G_i, G_j] = 1$ ($i \neq j$), iii) $G_i \cap \prod_{j \neq i} G_j = \zeta G$ ($1 \leq i \leq n$), 那么称 G 是 G_1, G_2, \dots, G_n 的中心积, 记为

$$G = G_1 \circ G_2 \circ \cdots \circ G_n.$$

Bornand 在 [5] 里用中心积给出了一类中心循环的有限 p -群, 即

$$\underbrace{X_3(p^m) \circ X_3(p^m) \circ \cdots \circ X_3(p^m)}_n \circ \mathbb{Z}_{p^{m+r}},$$

*收稿日期: 2024-07-24

接收日期: 2024-10-09

基金项目: 国家自然科学基金资助 (11801129); 河北省自然科学基金资助 (A2022402002).

作者简介: 徐涛 (1983-), 男, 河北邢台, 教授, 主要研究方向: 群论, E-mail: gtxutao@163.com.

其中 $n \geq 1, m \geq 1, r \geq 0$ 且

$$X_3(p^m) = \langle x, y \mid x^{p^m} = y^{p^m} = 1, [x, y]^{p^m} = 1, [x, [x, y]] = [y, [x, y]] = 1 \rangle.$$

王玉雷等在 [6] 中确定了上述群的同构群. 本文研究了这类中心循环的有限 p - 群的多项式自同构, 得到了下面的结果.

定理 1.1 设 $G = \underbrace{X_3(p^m) \circ X_3(p^m) \circ \cdots \circ X_3(p^m)}_n \circ \mathbb{Z}_{p^{m+r}}$, 其中 p 是奇素数, $n \geq 1, m \geq 1, r \geq 0$, 则 $\text{PAut}(G)/\text{Inn}(G) \cong \mathbb{Z}_{p^r}$.

定理 1.2 设 $G = \underbrace{X_3(2^m) \circ X_3(2^m) \circ \cdots \circ X_3(2^m)}_n \circ \mathbb{Z}_{2^{m+r}}$, 其中 $n \geq 1, m \geq 1, r \geq 0$, 则

- (i) 当 $r = 0$ 或 1 时, $\text{PAut}(G) = \text{Inn}(G)$.
- (ii) 当 $r \geq 2$ 时, $\text{PAut}(G)/\text{Inn}(G) \cong \mathbb{Z}_{2^{r-1}}$.

2 预备知识

由 [1] 的定理 5.3.5 容易得到下面的引理 2.1.

引理 2.1 设 G 是幂零类 ≤ 2 的幂零群, 则对于 $x, y \in G$, 有 $(xy)^n = x^n y^n [y, x]^{\frac{n(n-1)}{2}}$, 其中 n 是整数.

引理 2.2 设 $G = \underbrace{X_3(p^m) \circ X_3(p^m) \circ \cdots \circ X_3(p^m)}_n \circ \mathbb{Z}_{p^{m+r}}$, 其中 $n \geq 1, m \geq 1, r \geq 0$ 且

$$X_3(p^m) = \langle x, y \mid x^{p^m} = y^{p^m} = 1, [x, y]^{p^m} = 1, [x, [x, y]] = [y, [x, y]] = 1 \rangle.$$

如果 α 是 G 的一个如下形式的多项式自同构

$$\alpha(x) = (u_1^{-1} x^{\epsilon_1} u_1)(u_2^{-1} x^{\epsilon_2} u_2) \cdots (u_k^{-1} x^{\epsilon_k} u_k),$$

那么

- (i) 当 p 是奇素数时, $\epsilon_1 + \epsilon_2 + \cdots + \epsilon_k \equiv 1 \pmod{p^m}$.
- (ii) 当 $p = 2$ 时, $\epsilon_1 + \epsilon_2 + \cdots + \epsilon_k \equiv 1 \pmod{2^{m+1}}$.

证 因为 G 的幂零类是 2, 所以对于 $x \in G$, 有

$$\begin{aligned} \alpha(x) &= (u_1^{-1} x^{\epsilon_1} u_1)(u_2^{-1} x^{\epsilon_2} u_2) \cdots (u_k^{-1} x^{\epsilon_k} u_k) \\ &= x^{\epsilon_1} [x^{\epsilon_1}, u_1] x^{\epsilon_2} [x^{\epsilon_2}, u_2] \cdots x^{\epsilon_k} [x^{\epsilon_k}, u_k] \\ &= x^{\epsilon_1 + \epsilon_2 + \cdots + \epsilon_k} [x^{\epsilon_1}, u_1] [x^{\epsilon_2}, u_2] \cdots [x^{\epsilon_k}, u_k] \\ &= x^{\epsilon_1 + \epsilon_2 + \cdots + \epsilon_k} [x, u_1^{\epsilon_1} u_2^{\epsilon_2} \cdots u_k^{\epsilon_k}]. \end{aligned}$$

因此 $\alpha(x) = x^\epsilon [x, u]$, 其中 $\epsilon = \epsilon_1 + \epsilon_2 + \cdots + \epsilon_k, u = u_1^{\epsilon_1} u_2^{\epsilon_2} \cdots u_k^{\epsilon_k}$.

注意到 $\alpha(xy) = \alpha(x)\alpha(y)$, 我们有 $(xy)^\epsilon = x^\epsilon y^\epsilon$. 再根据引理 2.1 可知

$$x^\epsilon y^\epsilon [y, x]^{\frac{\epsilon(\epsilon-1)}{2}} = x^\epsilon y^\epsilon.$$

从而

$$y^{-\epsilon} x^{-\epsilon} x^\epsilon y^\epsilon [y, x]^{\frac{\epsilon(\epsilon-1)}{2}} = 1.$$

进而

$$[y, x]^{\frac{\epsilon(\epsilon-1)}{2}} = 1.$$

因为 $G' = \langle y^{p^r} \rangle$ 的阶数是 p^m , 所以

$$\frac{\epsilon(\epsilon-1)}{2} \equiv 0 \pmod{p^m}.$$

当 p 是奇素数时, $\epsilon \equiv 1 \pmod{p^m}$ 或者 $\epsilon \equiv 0 \pmod{p^m}$. 如果 $\epsilon \equiv 0 \pmod{p^m}$, 那么对于任意的 $1 \neq g \in G' \leq \zeta G$,

$$\alpha(g) = g^\epsilon [g, u] = [g, u] = 1,$$

矛盾于 α 的核是 1. 因此 $\epsilon \equiv 1 \pmod{p^m}$.

当 $p = 2$ 时, $\epsilon \equiv 1 \pmod{2^{m+1}}$ 或者 $\epsilon \equiv 0 \pmod{2^{m+1}}$. 如果 $\epsilon \equiv 0 \pmod{2^{m+1}}$, 不妨设 $\epsilon = 2^{m+1}k$, 其中 k 是整数, 则对于任意的 $1 \neq h \in G'$,

$$\alpha(h) = h^\epsilon [h, u] = h^{2^{m+1}k} [h, u] = (h^{2^m})^{2k} [h, u] = [h, u] = 1.$$

矛盾, 舍去 $\epsilon \equiv 0 \pmod{2^{m+1}}$. 因此 $\epsilon \equiv 1 \pmod{2^{m+1}}$.

3 定理 1.1 的证明

由 [6] 可知 G 有生成元 $x_1, x_2, \dots, x_{2n}, y$, 且 $x_i^{p^m} = 1 (1 \leq i \leq 2n)$, $y^{p^{m+r}} = 1$, 并满足

$$[x_{2i-1}, x_{2i}] = y^{p^r}, \quad 1 \leq i \leq n$$

$$[x_{2i-1}, x_j] = 1, \quad j \neq 2i$$

$$[x_{2i}, x_l] = 1, \quad l \neq 2i - 1$$

任取 $\alpha \in \text{PAut}(G)$, 存在整数 $\epsilon_1, \epsilon_2, \dots, \epsilon_k$ 和 G 中元素 $u_t = (\prod_{j=1}^{2n} x_j^{a_{t,j}}) y^{b_t} (1 \leq t \leq k, 0 \leq a_{t,j} < p^m, 0 \leq b_t < p^{m+r})$, 使得

$$\begin{aligned} \alpha(x_{2i-1}) &= (u_1^{-1} x_{2i-1}^{\epsilon_1} u_1) (u_2^{-1} x_{2i-1}^{\epsilon_2} u_2) \cdots (u_k^{-1} x_{2i-1}^{\epsilon_k} u_k) \\ &= x_{2i-1}^{\epsilon_1} [x_{2i-1}^{\epsilon_1}, u_1] x_{2i-1}^{\epsilon_2} [x_{2i-1}^{\epsilon_2}, u_2] \cdots x_{2i-1}^{\epsilon_k} [x_{2i-1}^{\epsilon_k}, u_k] \\ &= x_{2i-1}^{\epsilon_1} [x_{2i-1}^{\epsilon_1}, (\prod_{j=1}^{2n} x_j^{a_{1,j}}) y^{b_1}] \cdots x_{2i-1}^{\epsilon_k} [x_{2i-1}^{\epsilon_k}, (\prod_{j=1}^{2n} x_j^{a_{k,j}}) y^{b_k}] \\ &= x_{2i-1}^{\epsilon_1} [x_{2i-1}^{\epsilon_1}, \prod_{j=1}^{2n} x_j^{a_{1,j}}] \cdots x_{2i-1}^{\epsilon_k} [x_{2i-1}^{\epsilon_k}, \prod_{j=1}^{2n} x_j^{a_{k,j}}] \\ &= x_{2i-1}^{\epsilon_1} [x_{2i-1}^{\epsilon_1}, x_{2i}^{a_{1,2i}}] \cdots x_{2i-1}^{\epsilon_k} [x_{2i-1}^{\epsilon_k}, x_{2i}^{a_{k,2i}}] \\ &= x_{2i-1}^{\epsilon_1} y^{\epsilon_1 a_{1,2i} p^r} x_{2i-1}^{\epsilon_2} y^{\epsilon_2 a_{2,2i} p^r} \cdots x_{2i-1}^{\epsilon_k} y^{\epsilon_k a_{k,2i} p^r} \\ &= x_{2i-1}^{\epsilon_1 + \epsilon_2 + \cdots + \epsilon_k} y^{(\epsilon_1 a_{1,2i} + \epsilon_2 a_{2,2i} + \cdots + \epsilon_k a_{k,2i}) p^r}, \end{aligned}$$

$$\begin{aligned}
\alpha(x_{2i}) &= (u_1^{-1}x_{2i}^{\epsilon_1}u_1)(u_2^{-1}x_{2i}^{\epsilon_2}u_2)\cdots(u_k^{-1}x_{2i}^{\epsilon_k}u_k) \\
&= x_{2i}^{\epsilon_1}[x_{2i}^{\epsilon_1}, u_1]x_{2i}^{\epsilon_2}[x_{2i}^{\epsilon_2}, u_2]\cdots x_{2i}^{\epsilon_k}[x_{2i}^{\epsilon_k}, u_k] \\
&= x_{2i}^{\epsilon_1}[x_{2i}^{\epsilon_1}, (\prod_{j=1}^{2n}x_j^{a_{1,j}})y^{b_1}]\cdots x_{2i}^{\epsilon_k}[x_{2i}^{\epsilon_k}, (\prod_{j=1}^{2n}x_j^{a_{k,j}})y^{b_k}] \\
&= x_{2i}^{\epsilon_1}[x_{2i}^{\epsilon_1}, \prod_{j=1}^{2n}x_j^{a_{1,j}}]\cdots x_{2i}^{\epsilon_k}[x_{2i}^{\epsilon_k}, \prod_{j=1}^{2n}x_j^{a_{k,j}}] \\
&= x_{2i}^{\epsilon_1}[x_{2i}^{\epsilon_1}, x_{2i-1}^{a_{1,2i-1}}]\cdots x_{2i}^{\epsilon_k}[x_{2i}^{\epsilon_k}, x_{2i-1}^{a_{k,2i-1}}] \\
&= x_{2i}^{\epsilon_1}y^{-\epsilon_1 a_{1,2i-1}p^r}x_{2i}^{\epsilon_2}y^{-\epsilon_2 a_{2,2i-1}p^r}\cdots x_{2i}^{\epsilon_k}y^{-\epsilon_k a_{k,2i-1}p^r} \\
&= x_{2i}^{\epsilon_1+\epsilon_2+\cdots+\epsilon_k}y^{-(\epsilon_1 a_{1,2i-1}+\epsilon_2 a_{2,2i-1}+\cdots+\epsilon_k a_{k,2i-1})p^r},
\end{aligned}$$

和

$$\alpha(y) = (u_1^{-1}y^{\epsilon_1}u_1)(u_2^{-1}y^{\epsilon_2}u_2)\cdots(u_k^{-1}y^{\epsilon_k}u_k) = y^{\epsilon_1+\epsilon_2+\cdots+\epsilon_k}.$$

根据引理 2.2 得到

$$\begin{aligned}
\alpha(x_{2i-1}) &= x_{2i-1}y^{(\epsilon_1 a_{1,2i}+\epsilon_2 a_{2,2i}+\cdots+\epsilon_k a_{k,2i})p^r}, \\
\alpha(x_{2i}) &= x_{2i}y^{-(\epsilon_1 a_{1,2i-1}+\epsilon_2 a_{2,2i-1}+\cdots+\epsilon_k a_{k,2i-1})p^r}, \\
\alpha(y) &= y^\mu,
\end{aligned}$$

其中 $1 \leq \mu \leq (p^r - 1)p^m + 1$. 又 ζG 的阶数是 p^{m+r} , 故

$$\begin{aligned}
\alpha(x_{2i-1}) &= x_{2i-1}y^{\mu_{2i-1}p^r}, \\
\alpha(x_{2i}) &= x_{2i}y^{\mu_{2i}p^r}, \\
\alpha(y) &= y^\mu,
\end{aligned}$$

其中 $0 \leq \mu_{2i-1}, \mu_{2i} < p^m, 1 \leq \mu \leq (p^r - 1)p^m + 1$.

设集合

$$A = \left\{ \left(\begin{array}{cccccc} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ a_1 & a_2 & \cdots & a_{2n} & a \end{array} \right) \middle| 0 \leq a_i < p^m, a \in \langle p^m + 1 \rangle \text{ 且 } a \in \mathbb{Z}_{p^{m+r}} \right\}.$$

下证 $A \cong \underbrace{(\mathbb{Z}_{p^m} \oplus \mathbb{Z}_{p^m} \oplus \cdots \oplus \mathbb{Z}_{p^m})}_{2n} \rtimes \mathbb{Z}_{p^r}$. 记

$$A_1 = \left\{ \left(\begin{array}{cccccc} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ a_1 & a_2 & \cdots & a_{2n} & 1 \end{array} \right) \middle| 0 \leq a_i < p^m \right\},$$

则 A_1 是 $GL(2n+1, \mathbb{Z}_{p^m})$ 的一个子群. 通过定义

$$\Upsilon\left(\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ a_1 & a_2 & \cdots & a_{2n} & 1 \end{pmatrix}\right) = (a_1, a_2, \cdots, a_{2n}),$$

构造 A_1 到 $\underbrace{\mathbb{Z}_{p^m} \oplus \mathbb{Z}_{p^m} \oplus \cdots \oplus \mathbb{Z}_{p^m}}_{2n}$ 的群同态 Υ , 可知 $A_1 \cong \underbrace{\mathbb{Z}_{p^m} \oplus \mathbb{Z}_{p^m} \oplus \cdots \oplus \mathbb{Z}_{p^m}}_{2n}$. 记

$$A_2 = \left\{ \left(\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & a \end{pmatrix} \right) \middle| a \in \langle p^m + 1 \rangle \text{ 且 } a \in \mathbb{Z}_{p^{m+r}} \right\}.$$

容易验证 $A_2 \cong \mathbb{Z}_{p^r}$. 又因为 $A = A_1 A_2$, $A_1 \trianglelefteq A$, $A_1 \cap A_2 = 1$, 所以 $A = A_1 \rtimes A_2$, 即

$$A \cong \underbrace{(\mathbb{Z}_{p^m} \oplus \mathbb{Z}_{p^m} \oplus \cdots \oplus \mathbb{Z}_{p^m})}_{2n} \rtimes \mathbb{Z}_{p^r}.$$

注意到多项式自同构 α 在基 $\{x_1, x_2, \cdots, x_{2n}, y\}$ 下的 $2n+1$ 阶方阵是

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ \mu_1 & \mu_2 & \cdots & \mu_{2n} & \mu \end{pmatrix},$$

显然此方阵属于 A . 因此考虑群同态

$$\Psi: \text{PAut}(G) \rightarrow A$$

$$\sigma \mapsto \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ \varepsilon_1 & \varepsilon_2 & \cdots & \varepsilon_{2n} & \varepsilon \end{pmatrix}$$

其中 $\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ \varepsilon_1 & \varepsilon_2 & \cdots & \varepsilon_{2n} & \varepsilon \end{pmatrix}$ 是 σ 在基 $\{x_1, x_2, \cdots, x_{2n}, y\}$ 下的方阵. 由同态定理可得

$$\text{PAut}(G) \cong A,$$

进而 $\text{PAut}(G)/\text{Inn}(G) \cong \mathbb{Z}_p^r$.

4 定理 1.2 的证明

由 [6] 可设 G 有生成元 $x_1, x_2, \dots, x_{2n}, y$, 且 $x_i^{2^m} = 1 (1 \leq i \leq 2n)$, $y^{2^{m+r}} = 1$, 同时有

$$[x_{2i-1}, x_{2i}] = y^{2^r}, \quad 1 \leq i \leq n$$

$$[x_{2i-1}, x_j] = 1, \quad j \neq 2i$$

$$[x_{2i}, x_l] = 1, \quad l \neq 2i - 1$$

任取 $\alpha \in \text{PAut}(G)$, 存在整数 $\epsilon_1, \epsilon_2, \dots, \epsilon_k$ 和 G 中元素 $u_t = (\prod_{j=1}^{2n} x_j^{a_{t,j}}) y^{b_t} (1 \leq t \leq k, 0 \leq a_{t,j} < 2^m, 0 \leq b_t < 2^{m+r})$, 使得

$$\begin{aligned} \alpha(x_{2i-1}) &= (u_1^{-1} x_{2i-1}^{\epsilon_1} u_1) (u_2^{-1} x_{2i-1}^{\epsilon_2} u_2) \cdots (u_k^{-1} x_{2i-1}^{\epsilon_k} u_k) \\ &= x_{2i-1}^{\epsilon_1} [x_{2i-1}^{\epsilon_1}, x_{2i}^{a_{1,2i}}] \cdots x_{2i-1}^{\epsilon_k} [x_{2i-1}^{\epsilon_k}, x_{2i}^{a_{k,2i}}] \\ &= x_{2i-1}^{\epsilon_1 + \epsilon_2 + \cdots + \epsilon_k} y^{(\epsilon_1 a_{1,2i} + \epsilon_2 a_{2,2i} + \cdots + \epsilon_k a_{k,2i}) 2^r}, \end{aligned}$$

$$\begin{aligned} \alpha(x_{2i}) &= (u_1^{-1} x_{2i}^{\epsilon_1} u_1) (u_2^{-1} x_{2i}^{\epsilon_2} u_2) \cdots (u_k^{-1} x_{2i}^{\epsilon_k} u_k) \\ &= x_{2i}^{\epsilon_1} [x_{2i}^{\epsilon_1}, x_{2i-1}^{a_{1,2i-1}}] \cdots x_{2i}^{\epsilon_k} [x_{2i}^{\epsilon_k}, x_{2i-1}^{a_{k,2i-1}}] \\ &= x_{2i}^{\epsilon_1 + \epsilon_2 + \cdots + \epsilon_k} y^{-(\epsilon_1 a_{1,2i-1} + \epsilon_2 a_{2,2i-1} + \cdots + \epsilon_k a_{k,2i-1}) 2^r}, \end{aligned}$$

和

$$\alpha(y) = (u_1^{-1} y^{\epsilon_1} u_1) (u_2^{-1} y^{\epsilon_2} u_2) \cdots (u_k^{-1} y^{\epsilon_k} u_k) = y^{\epsilon_1 + \epsilon_2 + \cdots + \epsilon_k}.$$

当 $r = 0$ 时, 由引理 2.2 知

$$\begin{aligned} \alpha(x_{2i-1}) &= x_{2i-1} y^{(\epsilon_1 a_{1,2i} + \epsilon_2 a_{2,2i} + \cdots + \epsilon_k a_{k,2i})}, \\ \alpha(x_{2i}) &= x_{2i} y^{-(\epsilon_1 a_{1,2i-1} + \epsilon_2 a_{2,2i-1} + \cdots + \epsilon_k a_{k,2i-1})}, \\ \alpha(y) &= y. \end{aligned}$$

又 ζG 的阶数是 2^m , 故

$$\begin{aligned} \alpha(x_{2i-1}) &= x_{2i-1} y^{\eta_{2i-1}}, \\ \alpha(x_{2i}) &= x_{2i} y^{\eta_{2i}}, \\ \alpha(y) &= y, \end{aligned}$$

其中 $0 \leq \eta_{2i-1}, \eta_{2i} < 2^m$.

考虑 $\text{GL}(2n+1, \mathbb{Z}_{2^m})$ 的一个子群

$$B = \left\{ \left(\begin{array}{cccc|c} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ b_1 & b_2 & \cdots & b_{2n} & 1 \end{array} \right) \mid 0 \leq b_i < 2^m \right\}.$$

不难证明 $B \cong \underbrace{\mathbb{Z}_{2^m} \oplus \mathbb{Z}_{2^m} \oplus \cdots \oplus \mathbb{Z}_{2^m}}_{2n}$. 因为多项式自同构 α 在基 $\{x_1, x_2, \cdots, x_{2n}, y\}$ 下的方阵属于 B , 所以构造群同态

$$\Gamma: \text{PAut}(G) \rightarrow B$$

$$\tau \mapsto \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ \lambda_1 & \lambda_2 & \cdots & \lambda_{2n} & 1 \end{pmatrix}$$

其中 $\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ \lambda_1 & \lambda_2 & \cdots & \lambda_{2n} & 1 \end{pmatrix}$ 是 τ 在基 $\{x_1, x_2, \cdots, x_{2n}, y\}$ 下的方阵. 由同态定理可得

$$\text{PAut}(G) \cong B \cong \text{Inn}(G).$$

当 $r \geq 1$ 时, 根据引理 2.2 可得

$$\begin{aligned} \alpha(x_{2i-1}) &= x_{2i-1}y^{(\epsilon_1 a_{1,2i} + \epsilon_2 a_{2,2i} + \cdots + \epsilon_k a_{k,2i})2^r}, \\ \alpha(x_{2i}) &= x_{2i}y^{-(\epsilon_1 a_{1,2i-1} + \epsilon_2 a_{2,2i-1} + \cdots + \epsilon_k a_{k,2i-1})2^r}, \\ \alpha(y) &= y^\vartheta, \end{aligned}$$

其中 $1 \leq \vartheta \leq (2^{r-1} - 1)2^{m+1} + 1$. 又 ζG 的阶数是 2^{m+r} , 故

$$\begin{aligned} \alpha(x_{2i-1}) &= x_{2i-1}y^{\vartheta_{2i-1}2^r}, \\ \alpha(x_{2i}) &= x_{2i}y^{\vartheta_{2i}2^r}, \\ \alpha(y) &= y^\vartheta, \end{aligned}$$

其中 $0 \leq \vartheta_{2i-1}, \vartheta_{2i} < 2^m, 1 \leq \vartheta \leq (2^{r-1} - 1)2^{m+1} + 1$. 由此可以看到当 $r = 1$ 时, $\vartheta = 1$, 这与 $r = 0$ 的情形一样. 因此 $r = 1$ 时, $\text{PAut}(G) = \text{Inn}(G)$. 下面只需考虑 $r \geq 2$ 的情形即可.

记 $\text{GL}(2n+1, \mathbb{Z}_{2^m})$ 的一个子群

$$C_1 = \left\{ \left(\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ c_1 & c_2 & \cdots & c_{2n} & 1 \end{pmatrix} \middle| 0 \leq c_i < 2^m \right\}.$$

可知 $C_1 \cong \underbrace{\mathbb{Z}_{2^m} \oplus \mathbb{Z}_{2^m} \oplus \cdots \oplus \mathbb{Z}_{2^m}}_{2n}$. 再考虑集合

$$C_2 = \left\{ \left(\begin{array}{ccccc} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & c \end{array} \right) \middle| c \in \langle 2^{m+1} + 1 \rangle \text{ 且 } c \in \mathbb{Z}_{2^{m+r}} \right\}.$$

易证 $C_2 \cong \mathbb{Z}_{2^{r-1}}$. 记

$$C = \left\{ \left(\begin{array}{ccccc} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ c_1 & c_2 & \cdots & c_{2n} & c \end{array} \right) \middle| 0 \leq c_i < 2^m, c \in \langle 2^{m+1} + 1 \rangle \text{ 且 } c \in \mathbb{Z}_{2^{m+r}} \right\},$$

则 $C = C_1 \rtimes C_2$, 从而 $C \cong \underbrace{(\mathbb{Z}_{2^m} \oplus \mathbb{Z}_{2^m} \oplus \cdots \oplus \mathbb{Z}_{2^m})}_{2n} \rtimes \mathbb{Z}_{2^{r-1}}$.

构造群同态

$$\Phi: \text{PAut}(G) \rightarrow C$$

$$\theta \mapsto \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ \xi_1 & \xi_2 & \cdots & \xi_{2n} & \xi \end{pmatrix}$$

其中 $\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ \xi_1 & \xi_2 & \cdots & \xi_{2n} & \xi \end{pmatrix}$ 是 θ 在基 $\{x_1, x_2, \cdots, x_{2n}, y\}$ 下的方阵. 由同态定理可得

$$\text{PAut}(G) \cong C,$$

从而 $\text{PAut}(G)/\text{Inn}(G) \cong \mathbb{Z}_{2^{r-1}}$.

参 考 文 献

- [1] Robinson D J S. A course in the theory of groups (2nd ed.)[M]. New York: Springer-Verlag, 1996.
- [2] Frohlich A. The near-ring generated by the inner automorphisms of a finite simple group [J]. Journal of The London Mathematical Society, 1958, 33: 95-107.

- [3] Endimioni G. Polynomial automorphisms of soluble groups [J]. *Communications in Algebra*, 2009, 37: 3388–3400.
- [4] Schweigert D. Polynomautomorphismen auf endlichen Gruppen [J]. *Archiv Der Mathematik*, 1977, 29: 34–38.
- [5] Bornand D. Elementary abelian subgroups in p -groups of class 2 [D]. Lausanne: Ecole Polytechnique Federale de Lausanne, 2009.
- [6] 王玉雷, 刘合国, 吴佐慧. 一类中心循环的有限 p - 群的自同构群的研究 [J]. *数学杂志*, 2016, 36(6): 1273–1282.

POLYNOMIAL AUTOMORPHISMS OF A CLASS OF FINITE P -GROUPS WITH A CYCLIC CENTER

XU Tao, ZHANG Zhen-hui

(School of Science, Hebei University of Engineering, Handan 056038, China)

Abstract: In this paper, the polynomial automorphisms of a class of finite p -groups with a cyclic center are studied. The structure of the group of polynomial automorphisms of these finite p -groups is determined.

Keywords: polynomial automorphism; finite p -group; inner automorphism

2010 MR Subject Classification: 20D15; 20D45