

文章编号: 1004-4353(2013)03-0192-03

特殊阶群的同构分类

钟艳林

(闽南理工学院 信息管理系, 福建 泉州 362700)

摘要: 运用有限交换群的基本定理、Sylow 定理等理论以及有限群阶数的素数分解, 研究了一些特殊阶群的基本构造, 并在同构意义下给出了它们的全部互不同构的类型.

关键词: 有限群; 阶数; 同构

中图分类号: O152

文献标识码: A

Isomorphism classification of groups of special orders

ZHONG Yanlin

(*Department of Information Management, Minnan University of Science
and Technology, Quanzhou 362700, China*)

Abstract: We study on some basic structures of groups of special order, by employing the famous theorems of finite Abelian group, Sylow in Algebra, and the prime factorization of order of finite groups. And the totally different types of them from the isomorphism point view are given.

Key words: finite groups; order number; isomorphism

群是抽象代数中最基本和最重要的概念之一, 它在现代科学技术的许多领域也有着广泛的应用. 在群论的众多分支中, 有限群论占据着重要的地位, 其中有限群的构造是有限群论研究的重要课题. 在研究有限群构造的诸多方法中, 利用子群对其进行研究是最有效的方法之一, 例如 Burside 定理、Hamilton 群等著名的结果都是通过子群来研究有限群结构得出来的. 文献[1-2]利用子群的换位子和群扩张理论得出了特定阶群的同构分类, 文献[3]通过对子群阶数的计算得出了一类群的同构分类. 本文通过对有限群阶数的素数分解, 再根据素数阶群一定为循环群等性质得出一些特殊阶群的同构分类, 证明了 p^2 阶、 p^3 阶及 $2p$ 阶群的同构分类, 最后给出了 12 阶和 15 阶群的具体同构分类.

1 预备知识

定义 1 设 G 是有限群, p 为素数, 如果 G 中元素 a 的阶 $o(a)$ 是 p 的方幂, 称元素 a 为 p 元素; 如果 G 的每个元素都是 p 元素, 称 G 为有限 p 群. 显然, 有限 p 群的阶为 p 的方幂.

引理 1 设 G 是有限 p 群, 则 $Z(G) > 1$.

证明 考虑 G 的共轭分类分解 $G = C_1 \cup C_2 \cup \cdots \cup C_s$, $C_1 = \{1\}$ 和类方程 $|G| = 1 + |C_2| + \cdots + |C_s|$. 因为 $|C_i| = |G : C_G(x_i)|^{[4]}$, 其中 $x_i \in C_i$, 由 $|G| = p^n$, 推知 $|C_i|$ 是 p 的方幂. 又由 $|C_1| = 1$ 推知至少还有某个 $|C_i| = 1^{[5]}$, 于是 $Z(G) > 1$.

引理 2^[6] 设 G 是 n 阶交换群, 其中 n 的标准分解式为 $n = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$, 其中 p_1, p_2, \dots, p_s 为不同的素数, $r_i > 0, i = 1, 2, \dots, s$. 每个 $p_i^{a_i} (i = 1, 2, \dots, s, \text{ 其中 } a_i \leq r_i)$ 称为群 G 的初等因子, $p_1^{a_1}, p_2^{a_2}, \dots, p_k^{a_k} (p_i \text{ 可能等于 } p_j, \text{ 但满足 } p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = n)$ 称为群 G 的初等因子组. 则 G 可唯一分解为素数幂阶循环群的直积 $G = \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_s \rangle$, 其中 $\langle a_i \rangle$ 是 $p_i^{a_i} (p_i \text{ 为素数}, i = 1, 2, \dots, s)$ 阶循环群.

2 主要结果及其证明

定理 1 阶数为 p^2 (p 为素数) 的群都是交换群, 它们只有两种同构分类, 分别是 C_{p^2} 和 $C_p \times C_p$, 其中 C_p 为 p 阶循环群.

证明 设 G 是 p^2 阶有限群. 由引理 1 可得, $|Z(G)| > \{e\}$, 又由 $|Z(G)| \mid |G|$ 可知, $|Z(G)| = p^2$ 或 $|Z(G)| = p$. 当 $|Z(G)| = p^2$ 时, $|Z(G)| = |G|$, 此时 G 是交换群; 当 $|Z(G)| = p$ 时, 因 $|G/Z(G)| = p$, 故 $G/Z(G)$ 为 p 阶循环群, 从而 G 为交换群, 这与 $Z(G) \neq G$ 矛盾, 故此情形不成立. 所以 $|Z(G)| = p^2$, G 为交换群. 由引理 2 可知, $G \cong C_{p^2}$ 或 $G \cong C_p \times C_p$.

定理 2 p^3 阶交换群 G 的同构类型包括 $C_{p^3}, C_{p^2} \times C_p, C_p \times C_p \times C_p$.

证明 由引理 2 (有限交换群的基本定理) 可得证.

定理 3 p^3 阶非交换群 G 有以下类型: ① $G \cong \langle a, b \mid a^{p^2} = b^p = \{e\}, b^{-1}ab = a^{1+p} \rangle$; ② $G \cong \langle a, b \mid a^4 = \{e\}, b^2 = a^2, b^{-1}ab = a^3 \rangle$; ③ $G \cong \langle a, b, c \mid a^p = b^p = c^p = \{e\}, [a, b] = c, [a, c] = [b, c] = \{e\} \rangle$.

证明 由 Sylow 定理^[5] 可知, G 中一定存在 p 阶正规子群. 现从 G 中任取一个 p 阶正规子群, 记为 N , 则 $|G/N| = p^2$. 由定理 1 可知, G/N 是交换群, 所以 $G' \leq N$ ^[4]. 又因 $G' \neq \{e\}$, 故 $G' = N$, 并且 $G' \leq Z(G)$. 再由 G 是非交换, 所以 G 中没有 p^3 阶元. 现以两种情形讨论:

I) G 中有 p^2 阶元, 记为 a . 这时 $\langle a \rangle$ 是 G 的极大子群, 因此, $\langle a \rangle$ 是 G 的正规子群. 又因 $\langle a^p \rangle$ 是 $\langle a \rangle$ 的特征子群, 故 $\langle a^p \rangle$ 也是 G 的正规子群. 由以上可知 $G' = \langle a^p \rangle$. 在 $\langle a \rangle$ 外面任取一个元素 b_1 , 再分两种情况进行讨论: ① $o(b_1) = p$ 时, 因为 $G = \langle a, b_1 \rangle$, 换位子 $[a, b_1] \neq \{e\}$, 但又因 $G' = \langle a^p \rangle$, 故可设 $[a, b_1] = a^{kp}$, 这里 p 不整除 k . 取 i 满足 $ik \equiv 1 \pmod{p}$, 令 $b = b_1^i$, 则有 $[a, b] = [a, b_1^i] = [a, b_1]^i = a^{ikp} = a^p$, 于是 $G \cong \langle a, b \mid a^{p^2} = b^p = \{e\}, b^{-1}ab = a^{1+p} \rangle$. ② $o(b_1) = p^2$ 时, 因为 $b_1^p \in \langle a \rangle$, 比较阶可令 $b_1^p = a^{kp}$. 如果 $p \neq 2$, 则有 $(b_1 a^{-k})^p = b_1^p a^{-kp} [a^{-k}, b_1]^{C_p} = \{e\}$, 所以 $\langle a \rangle$ 外有 p 阶元 $b_1 a^{-k}$, 即第一种情况. 如果 $p = 2$, 则可能有 $b_1^2 = a^2, [a, b_1] = a^2$, 以 b 代替 b_1 得到 $G \cong \langle a, b \mid a^4 = \{e\}, b^2 = a^2, b^{-1}ab = a^3 \rangle$.

II) G 中无 p^2 阶元, 分 $p = 2$ 和 $p \neq 2$ 两种情况: $p = 2$ 时, $\exp G = 2$ 推出 G 交换^[7], 即非交换群不会发生此类情况. $p \neq 2$ 时, 假定 $G/G' = \langle aG', bG' \rangle$, 于是 $G = \langle a, b, G' \rangle$, 但由 G 非交换, 必有 $[a, b] \neq \{e\}$, 于是 $G' = \langle [a, b] \rangle$, 并且还有 $G = \langle a, b \rangle$. 令 $c = \langle a, b \rangle$, 则 $G \cong \langle a, b, c \mid a^p = b^p = c^p = \{e\}, [a, b] = c, [a, c] = [b, c] = \{e\} \rangle$.

定理 4 阶数为 $2p$ (p 为大于 2 的素数) 的群有两种同构分类, 分别是 C_{2p} 和 D_p .

证明 由 Sylow 第三定理^[5] 可知, G 有 1 个 Sylow- p 子群. 因为 p 为素数, 故该子群为循环群, 不妨记为 $H = \langle a \rangle$, 其中 a 是 p 阶元. 另外, G 有 1 个或 p 个 Sylow 2 子群^[1].

1) 当 G 有 1 个 Sylow- p 子群 $H (H = \langle a \rangle)$, 也只有 1 个 Sylow 2 子群 (记为 $K, K = \langle b \rangle$, 其中 b 是 2 阶元) 时, 由 Sylow 第二定理^[5] 的推论可知, H 和 K 都是 G 的正规子群, 因此 HK 也是 G 的子群. 由此易知 $H \cap K = \{e\}$, $|H \cap K| = 1$, 因此 $|HK| = 2p = |G|$, 故 $G = HK$, 并且 $aba^{-1}b^{-1} \in H$, $aba^{-1}b^{-1} \in K$, 所以 $aba^{-1}b^{-1} \in H \cap K = \{e\}$, 故 $aba^{-1}b^{-1} = e$, 即 $ab = ba$, 所以 $o(ab) = 2p, G = \langle ab \rangle$, 即 G 是由 ab 生成的 $2p$ 阶循环群.

2) 当 G 有 1 个 Sylow- p 子群 $H (H = \langle a \rangle)$ 和 p 个 Sylow 2 子群时, G 有 p 个 2 阶元, 记其中一个 2 阶元为 b . 由群的定义可知, $ba \in G$. 由此易知 $ba \neq b$ 且 $ba = a^i (i = 0, 1, \dots, p-1)$, 否则 $b = a^i$. 此时 b

要么是 e , 要么是 p 阶元, 这与 b 是 2 阶元矛盾, 因此 ba 是 G 的新元素. 同理, $ba^i (i=0, 1, \dots, p-1)$ 都是 G 的新元素, 于是 $G = \{e, a, \dots, a^{p-1}, b, ba, \dots, ba^{p-1}\}$, 其中 $ba^i (i=0, 1, \dots, p-1)$ 都是 2 阶元.

下面讨论 G 的乘法运算. 易知 $ab \neq a^i (i=0, 1, \dots, p-1)$, 否则 $b = a^{i-1} (i=0, 1, \dots, p-1)$, 这与 b 是 2 阶元矛盾. 同样, $ab \neq ba^i (i=0, 1, \dots, p-1)$, 否则 $ab \cdot ba^i = ba^i \cdot ba^i = e$, 由 $b^2 = e$ 得 $a^{i+1} = e (i+1 \leq p-1)$. 这与 a 是 p 阶元矛盾, 因此 $ab = ba^{p-1} = ba^{-1}$. 此时, $G = \{e, a, \dots, a^{p-1}, b, ba, \dots, ba^{p-1}\}$, 其中 $a^p = e, b^2 = e, ab = ba^{-1}$. 这个 G 就是二面体群, 用符号 D_p 来表示. 综上所述, 阶数为 $2p$ 的群只有两种同构分类, 分别是 C_{2p} 和 D_p .

下面根据以上定理给出阶数 12 和阶数 15 的群的所有同构分类.

阶数为 12 的群: 当 G 是交换群时, 可得 G 有两种同构分类: $G \cong C_3 \times C_4$ 和 $G \cong C_3 \times C_2 \times C_2^{[7]}$. 当 G 是非交换时, G 的 Sylow 2 子群和 Sylow 3 子群不能同时是 G 的正规子群. 下面分两种情况讨论:

1) 若 G 的 Sylow 3 子群(记为 H) 非正规, 则 H 的核 $H_G = \{e\}$, 于是 G 在 H 上的置换表示是 G 的忠实表示. 由 $|G:H|=4$ 得 G 同构于 S_4 的子群. 又因为 S_4 只有一个 12 阶子群 A_4 , 所以 $G \cong A_4$.

2) 若 G 的 Sylow 3 子群(记为 H) 在 G 中正规, 则 G 的 Sylow 2 子群(记为 K) 非正规, 此时 $G = HK$. 对 H 运用 N/C 定理得 $G/C_G(H)$ 同构于 $Aut(H)$ 的子群. 而 $Aut(H) \cong C_2$, 又由 G 是非交换得 $G/C_G(H) \cong C_2$, $|C_G(H)| = 6$, 于是 $C_G(H) \cong C_6$. 由此知 G 是 C_6 被 C_2 的扩张. 由循环群的扩张定理可知, G 满足以下定义关系: $a^6 = e, b^2 = a^t, ab = ba^r, r \not\equiv 1 \pmod{6}, r^2 \equiv 1 \pmod{6}, t(r-1) \equiv 0 \pmod{6}$. 解得 $r \equiv -1 \pmod{6}, t \equiv 3$ 或 $0 \pmod{6}$. 当 $r = -1, t = 0$ 时, $G = \langle a, b \mid a^6 = b^2 = e, ab = ba^{-1} \rangle$; 当 $r = -1, t = 3$ 时, $G = \langle a, b \mid a^6 = e, b^2 = a^3, ab = ba^{-1} \rangle$.

综上所述, 12 阶群的所有同构分类共有 5 种, 分别是: $G \cong C_3 \times C_4; G \cong C_3 \times C_2 \times C_2; G \cong A_4; G = \langle a, b \mid a^6 = b^2 = e, ab = ba^{-1} \rangle; G = \langle a, b \mid a^6 = e, b^2 = a^3, ab = ba^{-1} \rangle$.

阶数为 15 的群: 由 Sylow 第三定理^[5] 可知, G 有且只有 1 个 Sylow 3 子群(记为 $H, H = \langle a \rangle, a$ 是 3 阶元) 和 1 个 Sylow 5 子群(记为 $K, K = \langle b \rangle, b$ 是 5 阶元). 又由 Sylow 第二定理^[5] 推论可得 H 和 K 都是 G 的正规子群, 于是 HK 是 G 的子群. 易知 $H \cap K = \{e\}, |H \cap K| = 1$, 又因 $|H \cap K| = 3 \times 5 = |G|$, 所以 $G = HK = \langle a, b \rangle$, 且 $aba^{-1}b^{-1} \in H, aba^{-1}b^{-1} \in K$, 故 $aba^{-1}b^{-1} \in H \cap K = \{e\}, aba^{-1}b^{-1} = e$, 即 $ab = ba$, 由此知 G 是交换群. 由引理 2 可得 $G \cong C_3 \times C_5$.

综上所述, 15 阶群只有一种同构分类: $G \cong C_3 \times C_5$.

参考文献:

- [1] 杨晓萍. 给定阶的有限群同构分类问题的研究[D]. 青岛: 青岛大学, 2008.
- [2] 李志秀. 阶为 24 的有限群的分类[J]. 晋中学院学报, 2011, 30(3): 11-13.
- [3] 钱国华. 能表示成四个真子群并的有限群[J]. 数学杂志, 2011, 31(5): 891-892.
- [4] 徐明曜. 有限群导引[M]. 2 版. 北京: 科学出版社, 1999: 53-58.
- [5] 聂灵沼, 丁石孙. 代数学引论[M]. 北京: 高等教育出版社, 2000: 79-83.
- [6] 张远达. 有限群构造[M]. 北京: 科学出版社, 1982: 126-135.
- [7] 逊宗明. 有限阿贝尔群同构的一个判定算法[J]. 商丘师范学院学报, 2004, 20(2): 53-54.