DOI:10.13718/j.cnki.xsxb.2018.12.004

具有最小元素同阶类类数的 $2qp$ 阶群的结构①

祁　娇，　曹洪平

西南大学 数学与统计学院，重庆 400715

摘要:在有限群中，群的阶和元素的阶对群的结构有很大影响. 通过研究群的阶和元素的阶可以得到群的结构、性质，甚至是部分群的分类. 群的元素的阶之集所含元素的个数，即同阶类类数，同样对群的结构有很大影响. 利用其阶所含素数的个数及群论基础知识，确定了所有阶为 $2qp$ 的群的同阶类类数的最小值为 5，其中 $q<p$ 是奇素数，并利用数论知识，确定出阶为 $2qp$ 的同阶类类数为 5 的群的分类及群的具体结构，详细给出了群的生成元及定义关系. 直接利用阶的分类结果，通过计算其元的阶的集合，同样给出了阶为 $2qp$ 的同阶类类数的最小值为 5，再利用阶为 $2qp$ 的群的分类，从中找出同阶类类数是 5 的群，其结构与通过理论方法确定出的群的结构是完全一致的.

关　键　词：有限群；可解群；元素同阶类

中图分类号：O152.1　　**文献标志码**：A　　**文章编号**：1000-5471(2018)12-0018-04

在群论研究中，群论工作者提出了同阶类的概念，即把阶相等的子群或元素视为一类，并利用这一概念对有限群进行研究. 由文献[1－6]可知，群的阶以及子群的性质与有限群的构造有关，也用元素阶的和刻画 $2qp$ 阶群. 在本文中，我们对 $2qp$ 阶群中元素的同阶类进行了讨论，并且通过文献[7－8]的数论知识，得出了阶为 $2qp$ 的群中元素的同阶类类数的最小值，并给出了当 $2qp$ 阶群 G 的元素的同阶类类数恰好取这一最小值时群 G 的结构.

设 G 是有限群，$|G|$ 为 G 的阶，$\pi(G)$ 表示 $|G|$ 的素因子集，$\pi_e(G)$ 表示 G 的元的阶之集. $\eta(G)$ 表示 G 的元素的同阶类类数，即 $\pi_e(G)$ 所含元的个数. 设 n 是一个给定的正整数，所有互不同构的 n 阶群设为 $G_1,G_2,\cdots,G_k$，称 $\eta(G_1),\eta(G_2),\cdots,\eta(G_k)$ 的最小者为 n 阶群的同阶类类数的最小值，记为 $\beta(n)$. 我们用 $\Gamma(G)$ 表示群 G 的素图，用 $t(G)$ 表示 $\Gamma(G)$ 的连通分支个数. $\pi_1,\pi_2,\cdots,\pi_{t(G)}$ 为 $\Gamma(G)$ 的连通分支. 若 $2\in\pi(G)$，我们总假设 $2\in\pi_1$. 其他符号都是标准的.

引理 1[9]　设 G 是有限群，则 $G\cong A_5$ 当且仅当 $\pi_e(G)=\{1,2,3,5\}$.

引理 2[10]　设 G 是有限群，G 的素图不连通，则 G 有如下 3 种结构：

(i) Frobenius 群；

(ii) 2-Frobenius 群；

(iii) G 有一正规群列 $1\trianglelefteq H\trianglelefteq K\trianglelefteq G$，其中 K/H 是非交换单群，H 和 G/K 是 π_1-群.

引理 3[10]　设 G 是偶阶 2-Frobenius 群，即 $G=ABC$，其中 $A\trianglelefteq G$，$AB\trianglelefteq G$，AB 是以 A 为核、B 为补的 Frobenius 群，BC 是以 B 为核、C 为补的 Frobenius 群，则：

$$t(G)=2 \qquad \pi(A)\cup\pi(C)=\pi_1 \qquad \pi(B)=\pi_2$$

且 G 是可解的.

引理 4[11]　n 阶循环群被 m 阶循环群的扩张是且只能是 $G=\langle a,b\rangle$，其中定义关系 $a^n=1$，$b^m=a^t$，

① 收稿日期：2018-03-27
基金项目：国家自然科学基金项目(11471266，11271301).
作者简介：祁　娇(1993-)，女，硕士研究生，主要从事有限群论的研究.
通信作者：曹洪平，副教授.

$a^b = a^r$，且整数 r,t 满足 $r^m \equiv 1 (\mathrm{mod}\ n)$ 与 $t(r-1) \equiv 0 (\mathrm{mod}\ n)$.

引理 5[12]　设素数 $r < q < p$，则 pqr 阶群 G 为可解群.

定理 1　设 G 为 $2qp$ 阶群，则 $\eta(G) \geqslant 5$，等号成立当且仅当 G 同构于下面两个群，其中 $q < p$ 是奇素数：

(i) $G_1 = \langle a, b \mid a^{qp} = 1, b^2 = 1, a^b = a^{-1} \rangle$；

(ii) $G_2 = \langle a, b, c \mid a^p = 1 = b^q = c^2, a^b = a^r, a^c = a^{-1}, b^c = b, r^q \equiv 1 (\mathrm{mod}\ p), r \not\equiv 1 (\mathrm{mod}\ p), q \mid (p-1) \rangle$.

特别地，$\beta(2qp) = 5$.

证　因为 $\mid G \mid = 2qp$，所以 $\pi_e(G) \supset \{1, 2, q, p\}$，从而 $\eta(G) \geqslant 4$. 若 $\eta(G) = 4$，则 $\pi_e(G) = \{1, 2, q, p\}$. 由文献[9]知 $G \cong A_5$，矛盾于 $\mid A_5 \mid = 60 = 2^2 \times 3 \times 5$. 故 $\eta(G) \geqslant 5$.

充分性：

由循环群的性质可知：当 $x \in \pi_e(G)$ 时，x 的所有因子在 $\pi_e(G)$ 中.

对 $G_1 = \langle a, b \mid a^{qp} = 1, b^2 = 1, a^b = a^{-1} \rangle$，由文献[11]知：$G_1$ 中有阶为 qp 的正规子群 A，且 $A = \langle a \rangle$ 为循环群. 于是 $G_1 = A + Ab$，$b^2 = 1$. 由关系式 $b^{-1}ab = a^{-1}$，知 $(a^ib)^2 = a^iba^ib = a^ia^{-i} = 1$，故 $\mid a^ib \mid = 2 (i = 0,1,2,\cdots,qp-1)$. 因此，$Ab$ 中元素全为 2 阶元，而其余各阶元均在 A 中，又因 A 循环，所以 $\pi_e(G_1) = \{1, 2, q, p, qp\}$，则 $\eta(G_1) = 5$.

对 $G_2 = \langle a, b, c \mid a^p = 1 = b^q = c^2, a^b = a^r, a^c = a^{-1}, b^c = b, r^q \equiv 1 (\mathrm{mod}\ p), r \not\equiv 1 (\mathrm{mod}\ p), q \mid (p-1) \rangle$. 由文献[11]知：$G_2$ 中有阶为 qp 的正规子群 A，且 $A = \langle a, b \mid a^p = 1 = b^q, a^b = a^r, r^q \equiv 1 (\mathrm{mod}\ p), r \not\equiv 1 (\mathrm{mod}\ p) \rangle$，于是 $G_2 = A + Ac$，其中 $c^2 = 1$. 由于 $q < p$，根据 Sylow 定理知 A 中 Sylow p-子群唯一. 故 A 中除了 p 阶元外，其余非单位元均为 q 阶元，由 a,b,c 之间的关系知，$(a^ic)^2 = a^ia^{-i} = 1$，故 $\mid a^ic \mid = 2 (i = 0,1,2,\cdots,p-1)$. 因为 $\mid b^jc \mid = 2q (j = 1,2,\cdots,q-1)$，而且 $(a^ib^jc)^2 = a^ib^jca^ib^jc = a^ib^jca^icb^j = a^ib^ja^{-i}b^j$，所以 $\mid a^ib^jc \mid = 2q (i = 1,2,\cdots,p-1;\ j = 1,2,\cdots,q-1)$. 于是 $\pi_e(G_2) = \{1, 2, q, p, 2q\}$. 进而 $\eta(G_2) = 5$.

必要性：

由 $\mid G \mid = 2qp = 2 \times q \times p$，$\eta(G) = 5$ 知 $\pi_e(G)$ 中只含一个合数，于是 $t(G) \geqslant 2$. 由引理 3 有以下情况：

(a) G 是 Frobenius 群.

假设 G 是以 A 为核、B 为补的 Frobenius 群. 由 Frobenius 群的性质，有：

$$(\mid A \mid, \mid B \mid) = 1 \qquad \mid B \mid \Big| (\mid A \mid - 1)$$

则存在以下情况：

(a_1) $\mid A \mid = 2q$，$\mid B \mid = p$，且 $p = 2q-1$；(a_2) $\mid A \mid = 2p$，$\mid B \mid = q$，且 $q \mid (2p-1)$；

(a_3) $\mid A \mid = qp$，$\mid B \mid = 2$，且 $2 \mid (qp-1)$；(a_4) $\mid A \mid = p$，$\mid B \mid = 2q$，且 $2q \mid (p-1)$；

(a_5) $\mid A \mid = q$，$\mid B \mid = 2p$，且 $2p \mid (q-1)$；(a_6) $\mid A \mid = 2$，$\mid B \mid = qp$，且 $qp \mid (2-1)$.

已知 $q < p$，可排除(a_5),(a_6). 下面分别讨论其它情况：

对(a_1)，$\mid A \mid = 2q$，$\mid B \mid = p$，且 $p = 2q-1$. 由 $\mid A \mid = 2q$，知 A 的 Sylow q-子群 Q char A，从而 $Q \trianglelefteq G$. 于是 QB 也是 Frobenius 群，从而 $p \mid (q-1)$，这与 $q < p$ 矛盾.

对(a_2)，$\mid A \mid = 2p$，$\mid B \mid = q$，且 $q \mid (2p-1)$. 由 $\mid A \mid = 2p$，知 A 的 Sylow p-子群 P char A，从而 $P \trianglelefteq G$. 于是 PB 也是 Frobenius 群，从而 $q \mid (p-1)$. 又因为 $q \mid (2p-1)$，所以 $q \mid p$. 这与 $q < p$ 为奇素数矛盾.

对(a_3)，$\mid A \mid = qp$，$\mid B \mid = 2$，且 $2 \mid (qp-1)$. 由于 A 是 G 的核，所以 A 是幂零群，故 A 为循环群. 设 $A = \langle a \rangle$，$a^{qp} = 1$. 由于 $\mid B \mid = 2$，所以可取 b 为 B 的 2 阶元，则 $b^{-1}ab = a^r$. 从而由 $b^2 = 1$ 有 $a^{r^2} = a$，所以 $r^2 \equiv 1 (\mathrm{mod}\ qp)$. 据文献[7-8]中数论知识，$r^2 \equiv 1 (\mathrm{mod}\ qp)$ 有 4 个解：$1, -1, pp' - qq', qq' - pp' (\mathrm{mod}\ qp)$，其中 p' 与 q' 分别满足 $pp' \equiv 1 (\mathrm{mod}\ q)$，$qq' \equiv 1 (\mathrm{mod}\ p)$.

若 $r \equiv 1 (\mathrm{mod}\ qp)$，则 $ab = ba$，G 中有 $2qp$ 阶元，与 $\pi_e(G)$ 中只有一个合数矛盾.

若 $r \equiv pp' - qq' (\mathrm{mod}\ qp)$，则 $ab = ba^{pp'-qq'}$. 由 $qq' \equiv 1 (\mathrm{mod}\ p)$，有 $qq' = 1 + k_1p$，其中 k_1 为整数.

故$(ab)^{2q}=a^{(pp'-qq'+1)q}=a^{-q^2q'+q}=a^{-k_1qp}=1$，即$|ab|=2q$. 于是$G$中有$2q$阶元. 这与$\pi_e(G)$中只有一个合数矛盾.

若$r\equiv qq'-pp'(\mathrm{mod}\ qp)$，则$ab=ba^{qq'-pp'}$. 由$pp'\equiv 1(\mathrm{mod}\ q)$，有$pp'=1+k_2q$，其中$k_2$为整数，故$(ab)^{2p}=a^{(qq'-pp'+1)q}=a^{-p^2p'+p}=a^{-k_2qp}=1$，即$|ab|=2p$. 于是$G$中有$2p$阶元. 这与$\pi_e(G)$中只有一个合数矛盾.

若$r\equiv -1(\mathrm{mod}\ qp)$，则$ab=ba^{-1}$. 从而$a^ib$均2为阶元$(i=0,1,\cdots,qp-1)$. 故$\pi_e(G)=\{1,2,q,p,qp\}$，满足条件，所以$G=\langle a,b\mid a^{qp}=1,b^2=1,a^b=a^{-1}\rangle\cong G_1$.

对(a_4)，$|A|=p$，$|B|=2q$，且$2q\mid p-1$. 由$|B|=2q$为偶数及B为Frobenius补知，B的中心$Z(B)$的阶为偶数，所以B为循环群. 令$A=\langle a\rangle$，$a^p=1$，$B=\langle b,c\rangle$，$b^q=1=c^2$，$c^{-1}bc=b$. 由引理4可知$G=\langle a,b,c\mid a^p=1=b^q=c^2,a^b=a^r,a^c=a^{-1},b^c=b,r^q\equiv 1(\mathrm{mod}\ p),r\not\equiv 1(\mathrm{mod}\ p),q\mid(p-1)\rangle\cong G_2$.

(b) G是2-Frobenius群.

假设G是2-Frobenius群，则由引理5知G是可解群，$t(G)=2$，$G=ABC$，其中$A\lhd G$，$AB\lhd G$，AB是以A为核、B为补的Frobenius群，BC是以B为核、C为补的Frobenius群. 于是存在以下情况：

(b_1) $|A|=p$，$|B|=q$，$|C|=2$；(b_2) $|A|=q$，$|B|=p$，$|C|=2$；

(b_3) $|A|=p$，$|B|=2$，$|C|=q$；(b_4) $|A|=q$，$|B|=2$，$|C|=p$；

(b_5) $|A|=2$，$|B|=p$，$|C|=q$；(b_6) $|A|=2$，$|B|=q$，$|C|=p$.

由引理5可知，$\pi(A)\cup\pi(C)=\pi_1$，$2\in\pi_1$，故可排除(b_3)，(b_4). 因为G是2-Frobenius群，所以$|B|\big|(|A|-1)$，$|C|\big|(|B|-1)$，但是$q<p$为奇素数，故排除(b_2)，(b_5)，(b_6).

对(b_1)，$|A|=p$，$|B|=q$，$|C|=2$. 设$A=\langle a\rangle$，$a^p=1$，$B=\langle b\rangle$，$b^q=1$，$C=\langle c\rangle$，$c^2=1$. 由于$A\lhd G$，所以$a^c=a^r$，从而$a=a^{c^2}=(a^c)^c=a^{r^2}$，于是$r^2\equiv 1(\mathrm{mod}\ p)$. 因而$r\equiv 1,-1(\mathrm{mod}\ p)$，进而$a^c=a$或$a^c=a^{-1}$. 由于$BC$为Frobenius群，所以$b^c=b^{-1}$. 又因$AB$为Frobenius群，所以$a^b=a^s$，$s^q\equiv 1(\mathrm{mod}\ p)$.

若$a^c=a$，则$(b^c)^{-1}a^cb^c=(b^{-1}ab)^c=(a^c)^s=a^s=b^{-1}ab$，且$(b^c)^{-1}a^cb^c=bab^{-1}$. 于是$b^{-1}ab=bab^{-1}$，从而$b^{-2}ab^2=a$. 但$b^{-2}ab^2=a^{s^2}$，所以$s^2\equiv 1(\mathrm{mod}\ p)$. 由于$s^q\equiv 1(\mathrm{mod}\ p)$，其中$q$是奇数，所以$s\equiv 1(\mathrm{mod}\ p)$，于是$a^b=a$，这与$AB$为Frobenius群矛盾.

若$a^c=a^{-1}$，则由$b^{-1}ab=a^s$有$(b^c)^{-1}a^cb^c=(a^c)^s$，即$ba^{-1}b^{-1}=a^{-s}$. 取s'使得$s's\equiv 1(\mathrm{mod}\ p)$，由$b^{-1}ab=a^s$，可得$b^{-1}a^{s'}b=a$，于是$a^{s'}=bab^{-1}$. 从而$a^{-s'}=ba^{-1}b^{-1}$，所以$a^{-s'}=a^{-s}$，所以$s\equiv s'(\mathrm{mod}\ p)$，$s^2\equiv ss'\equiv 1(\mathrm{mod}\ p)$. 又因$s^q\equiv 1(\mathrm{mod}\ p)$，其中$q$是奇数，所以$s\equiv 1(\mathrm{mod}\ p)$，于是$a^b=a$，这与$AB$为Frobenius群矛盾.

(c) G有一正规群列$1\lhd H\lhd K\lhd G$，其中K/H是非交换单群，H和G/K是π_1-群.

若G是(c)中群，则G是不可解的，这与引理2矛盾.

定理1得证.

注1 定理1的证明没有使用$2qp$阶群的分类，实际上由参考文献[11]给出的$2qp$阶群的分类知，设p,q是两个互异的奇素数，且$q<p$，则$2qp$阶群有以下6种类型：

(i) $G=\langle a\mid a^{2qp}=1\rangle$；

(ii) $G=\langle a,b\mid a^{qp}=1,b^2=1,b^{-1}ab=a^{-1}\rangle$；

(iii) $G=\langle a,b\mid a^{qp}=1,b^2=1,b^{-1}ab=a^r\rangle$，其中$r\equiv pp'-qq'(\mathrm{mod}\ pq)$，$pp'\equiv 1(\mathrm{mod}\ q)$，$qq'\equiv 1(\mathrm{mod}\ p)$；

(iv) $G=\langle a,b\mid a^{qp}=1,b^2=1,b^{-1}ab=a^{-r}\rangle$，其中$r\equiv pp'-qq'(\mathrm{mod}\ pq)$，$pp'\equiv 1(\mathrm{mod}\ q)$，$qq'\equiv 1(\mathrm{mod}\ p)$；

(v) $G=\langle a,b,c\mid a^p=1=b^q=c^2,b^{-1}ab=a^r,c^{-1}ac=a,c^{-1}bc=b,r^q\equiv 1(\mathrm{mod}\ p),r\not\equiv 1(\mathrm{mod}\ p)\rangle$；

(vi) $G=\langle a,b,c\mid a^p=1=b^q=c^2,b^{-1}ab=a^r,c^{-1}ac=a^{-1},c^{-1}bc=b,r^q\equiv 1(\mathrm{mod}\ p),r\not\equiv 1(\mathrm{mod}\ p)\rangle$.

其中情形(v)，(vi)仅在$q\mid(p-1)$时才出现.

我们也可以直接计算这 6 个群的元的阶之集，即可得到元素的同阶类类数，从而得到定理 1 的证明.

参考文献：

[1] 赵永刚，郭继东. 子群的阶之集对有限群结构的影响 [J]. 伊犁师范学院学报(自然科学版)，2011(4)：8－10.
[2] 李　月，曹洪平. 交错群 A_5，A_6，A_7 的新刻画 [J]. 西南大学学报(自然科学版)，2016，38(2)：47－50.
[3] 申　虹，曹洪平. 阶对有限群的刻画 [J]. 重庆师范大学学报(自然科学版)，2010，27(5)：54－56.
[4] 李方方，曹洪平. 子群的性质对有限群结构的影响 [J]. 西南大学学报(自然科学版)，2008，30(8)：5－8.
[5] 孙宗明. 群的元素的阶与群的构造 [J]. 泰安师专学报，2002，24(3)：1－6.
[6] 薛海波，吕　恒. 非交换子群具有极小中心化子的有限 p-群 [J]. 西南师范大学学报(自然科学版)，2016，41(8)：12－15.
[7] 王杰官. 数论基础 [M]. 福建：科学技术出版社，1987.
[8] 闵嗣鹤，严士健. 初等数论 [M]. 北京：高等教育出版社，1982.
[9] 施武杰，杨文泽. A_5 的一个新刻划与有限质元群 [J]. 西南师范学院学报，1984(1)：36－40.
[10] 陈贵云. Frobenius 群与 2－Frobenius 群的构造 [J]. 西南师范大学学报(自然科学版)，1995，20(5)：485－487.
[11] 张远达. 有限群构造（上册）[M]. 北京：科学出版社，1982：288－291.
[12] 徐明曜. 有限群初步 [M]. 北京：科学出版社，2001.

The Structure of Groups of Order $2qp$ with the Minimum Class Number of Same Element Order

QI　Jiao，　CAO Hong-ping

School of Mathematics and Statistics，Southwest University，Chongqing 400715，China

Abstract：In finite groups，group order and element order have great influence on the structure of the group. We can get the structure of a group and its property，and even the classification of some groups by researching group order and element order. The number of elements contained in the set of element orders of the group，that is，the number of classes of the same order，also has a great influence on the structure of the group. $q<p$ in groups of order $2qp$ are odd primes. Using the number of prime numbers contained in its set of orders and the basic knowledge of group theory，it can be determined that the minimum value of the same order class number of all groups with order $2qp$ is 5. After defining the minimum value of the same order class number of groups with an order of $2qp$，the possible situation of the prime graph and the relationship between the prime graph and the structure of the group are determined by using the knowledge of number theory. The classification and structure of group with order $2qp$ are given. On the other hand，by directly using the classification results of the order，and calculating the set of the order of its elements，the minimum value of the number of the same class with the order of $2qp$ is also 5. Using the classification of groups with order $2qp$ ，we find out the groups with 5 classes of the same order. The group structure is completely consistent with that determined by theoretical methods.

Key words：finite group；solvable group；the class of same element order

责任编辑　廖　坤　崔玉洁