Math. J. Okayama Univ. 36(1994), 1–21

FINITE p-GROUPS WITH CYCLIC SUBGROUPS OF INDEX p^2

Dedicated to Professor Manabu Harada on his 60th birthday

YASUSHI NINOMIYA

1. Intoduction. Let p be a prime number. It is trivial that a finite abelian p-group of order p^m and exponent p^{m-1} is of type $(m-1,1)$. A complete list of nonabelian such p-groups is contained in Burnside's book [1]. For convenience, we here restate it.

The finite nonabelian p-groups of order p^m and exponent p^{m-1} are of the following types:

(a) *p odd, $m \geq 3$*:
$M_m(p) = \langle a, b \mid a^{p^{m-1}} = 1, b^p = 1, b^{-1}ab = a^{1+p^{m-2}}\rangle$;

(b) $p = 2$, $m \geq 3$: *generalized quaternion group*
$Q_m = \langle a, b \mid a^{2^{m-1}} = 1, b^2 = a^{2^{m-2}}, b^{-1}ab = a^{-1}\rangle$;

(c) $p = 2$, $m \geq 3$: *dihedral group*
$D_m = \langle a, b \mid a^{2^{m-1}} = 1, b^2 = 1, b^{-1}ab = a^{-1}\rangle$;

(d) $p = 2$, $m \geq 4$: *quasi-dihedral group*
$M_m(2) = \langle a, b \mid a^{2^{m-1}} = 1, b^2 = 1, b^{-1}ab = a^{1+2^{m-2}}\rangle$;

(e) $p = 2$, $m \geq 4$: *semidihedral group*
$S_m = \langle a, b \mid a^{2^{m-1}} = 1, b^2 = 1, b^{-1}ab = a^{-1+2^{m-2}}\rangle$.

A finite abelian p-group of order p^m and exponent p^{m-2} is of type $(m-2, 2)$ or $(m-2, 1, 1)$. A complete list of finite nonabelian p-groups of order p^m which contain cyclic normal subgroups of order p^{m-2} is also given in [1], and defining relations for those groups are given explicitly. But it contains two clerical errors for the case $p = 2$ (see Remark 3 below). The classification of groups G of order p^m and exponent p^{m-2} which do not possess cyclic normal subgroups of order p^{m-2} has been discussed by Miller [2,3](see also [4]), to be more precise, the case where the centralizer $C_G(a)$ of an element a of G of order p^{m-2} properly contains $\langle a\rangle$ has been discussed in [2]; while the case where $C_G(a) = \langle a\rangle$ has been discussed in [3]. However it dose not seem to be easy to read defining relations for those groups. The object of the present paper is to provide the classification up to isomorphism of nonabelian p-groups of order p^m and exponent p^{m-2}

and to give one presentation by generators and defining relations for each isomorphism type of such groups. In what follows we denote by C_{p^k} the cyclic group of order p^k. Our result for the case p odd is as follows:

Theorem 1. *Let p be an odd prime. The finite nonabelian p-groups of order p^m and exponent p^{m-2} are of the following types:*

(a) $m \geq 3$:

$G_1 = \langle a,b,c \mid a^{p^{m-2}} = 1, b^p = 1, c^p = 1, ab = ba, c^{-1}ac = ab, bc = cb\rangle$;

(b) $m \geq 4$:

$G_2 = \langle a,b \mid a^{p^{m-2}} = 1, b^{p^2} = 1, b^{-1}ab = a^{1+p^{m-3}}\rangle$;

$G_3 = M_{m-1}(p) \times C_p$;

$G_4 = \langle a,b,c \mid a^{p^{m-2}} = 1, b^p = 1, c^p = 1, ab = ba, ac = ca, c^{-1}bc = a^{p^{m-3}}b\rangle$;

$G_5 = \langle a,b,c \mid a^{p^{m-2}} = 1, b^p = 1, c^p = 1, ab = ba, c^{-1}ac = ab, c^{-1}bc = a^{p^{m-3}}b\rangle$;

$G_6 = \langle a,b,c \mid a^{p^{m-2}} = 1, b^p = 1, c^p = 1, ab = ba, c^{-1}ac = ab, c^{-1}bc = a^{rp^{m-3}}b\rangle$,

where r is a quadratic nonresidue $\bmod p$;

$G_7 = \langle a,b,c \mid a^{p^{m-2}} = 1, b^p = 1, c^p = 1, b^{-1}ab = a^{1+p^{m-3}}, c^{-1}ac = ab, bc = cb\rangle$;

(c) $m \geq 5$:

$G_8 = \langle a,b \mid a^{p^{m-2}} = 1, b^{p^2} = 1, b^{-1}ab = a^{1+p^{m-4}}\rangle$;

$G_9 = \langle a,b \mid a^{p^{m-2}} = 1, b^{p^2} = 1, a^{-1}ba = b^{1+p}\rangle$;

(d) $m \geq 6$:

$G_{10} = \langle a,b \mid a^{p^{m-2}} = 1, a^{p^{m-3}} = b^{p^2}, a^{-1}ba = b^{1-p}\rangle$;

(e) $m = 4$; $p = 3$:

$G_{11} = \langle a,b,c \mid a^9 = 1, b^3 = 1, c^3 = a^3, ab = ba, c^{-1}ac = ab, c^{-1}bc = a^6b\rangle$.

Our result for finite nonabelian 2-groups is as follows:

Theorem 2. *The finite nonabelian 2-groups of order 2^m and exponent 2^{m-2} are of the following types:*

(a) $m \geq 4$:

$G_1 = \langle a,b \mid a^{2^{m-2}} = 1, b^4 = 1, b^{-1}ab = a^{1+2^{m-3}}\rangle$;

$G_2 = Q_{m-1} \times C_2$;

$G_3 = D_{m-1} \times C_2$;

$$G_4 = \langle a,b,c \mid a^{2^{m-2}} = 1, b^2 = 1, c^2 = 1, ab = ba, ac = ca, c^{-1}bc = a^{2^{m-3}}b\rangle;$$
$$G_5 = \langle a,b,c \mid a^{2^{m-2}} = 1, b^2 = 1, c^2 = 1, ab = ba, c^{-1}ac = ab, bc = cb\rangle;$$

(b) $m \geq 5$:

$$G_6 = \langle a,b \mid a^{2^{m-2}} = 1, b^4 = 1, b^{-1}ab = a^{-1}\rangle;$$
$$G_7 = \langle a,b \mid a^{2^{m-2}} = 1, b^4 = 1, b^{-1}ab = a^{-1+2^{m-3}}\rangle;$$
$$G_8 = \langle a,b \mid a^{2^{m-2}} = 1, b^4 = a^{2^{m-3}}, b^{-1}ab = a^{-1}\rangle;$$
$$G_9 = \langle a,b \mid a^{2^{m-2}} = 1, b^4 = 1, a^{-1}ba = b^{-1}\rangle;$$
$$G_{10} = M_{m-1}(2) \times C_2;$$
$$G_{11} = S_{m-1} \times C_2;$$
$$G_{12} = \langle a,b,c \mid a^{2^{m-2}} = 1, b^2 = 1, c^2 = 1, ab = ba, c^{-1}ac = a^{-1}, c^{-1}bc = a^{2^{m-3}}b\rangle;$$
$$G_{13} = \langle a,b,c \mid a^{2^{m-2}} = 1, b^2 = 1, c^2 = 1, ab = ba, c^{-1}ac = a^{-1}b, bc = cb\rangle;$$
$$G_{14} = \langle a,b,c \mid a^{2^{m-2}} = 1, b^2 = 1, c^2 = a^{2^{m-3}}, ab = ba, c^{-1}ac = a^{-1}b, bc = cb\rangle;$$
$$G_{15} = \langle a,b,c \mid a^{2^{m-2}} = 1, b^2 = 1, c^2 = 1, b^{-1}ab = a^{1+2^{m-3}}, c^{-1}ac = a^{-1+2^{m-3}}, bc = cb\rangle;$$
$$G_{16} = \langle a,b,c \mid a^{2^{m-2}} = 1, b^2 = 1, c^2 = 1, b^{-1}ab = a^{1+2^{m-3}}, c^{-1}ac = a^{-1+2^{m-3}}, c^{-1}bc = a^{2^{m-3}}b\rangle;$$
$$G_{17} = \langle a,b,c \mid a^{2^{m-2}} = 1, b^2 = 1, c^2 = 1, b^{-1}ab = a^{1+2^{m-3}}, c^{-1}ac = ab, bc = cb\rangle;$$
$$G_{18} = \langle a,b,c \mid a^{2^{m-2}} = 1, b^2 = 1, c^2 = b, b^{-1}ab = a^{1+2^{m-3}}, c^{-1}ac = a^{-1}b\rangle;$$

(c) $m \geq 6$:

$$G_{19} = \langle a,b \mid a^{2^{m-2}} = 1, b^4 = 1, b^{-1}ab = a^{1+2^{m-4}}\rangle;$$
$$G_{20} = \langle a,b \mid a^{2^{m-2}} = 1, b^4 = 1, b^{-1}ab = a^{-1+2^{m-4}}\rangle;$$
$$G_{21} = \langle a,b \mid a^{2^{m-2}} = 1, a^{2^{m-3}} = b^4, a^{-1}ba = b^{-1}\rangle;$$
$$G_{22} = \langle a,b,c \mid a^{2^{m-2}} = 1, b^2 = 1, c^2 = 1, ab = ba, c^{-1}ac = a^{1+2^{m-4}}b, c^{-1}bc = a^{2^{m-3}}b\rangle;$$
$$G_{23} = \langle a,b,c \mid a^{2^{m-2}} = 1, b^2 = 1, c^2 = 1, ab = ba, c^{-1}ac = a^{-1+2^{m-4}}b, c^{-1}bc = a^{2^{m-3}}b\rangle;$$
$$G_{24} = \langle a,b,c \mid a^{2^{m-2}} = 1, b^2 = 1, c^2 = 1, b^{-1}ab = a^{1+2^{m-3}}, c^{-1}ac = a^{-1+2^{m-4}}b, bc = cb\rangle;$$
$$G_{25} = \langle a,b,c \mid a^{2^{m-2}} = 1, b^2 = 1, c^2 = a^{2^{m-3}}, b^{-1}ab = a^{1+2^{m-3}}, c^{-1}ac = a^{-1+2^{m-4}}b, bc = cb\rangle;$$

(d) $m = 5$:

$$G_{26} = \langle a,b,c \mid a^8 = 1, b^2 = 1, c^2 = a^4, b^{-1}ab = a^5, c^{-1}ac = ab, bc = cb\rangle.$$

The proof of theorems 1 and 2 depends on Miller's idea on classifying the groups under consideration and Burnside's technique for choosing appropriate generators for each group, and it will be given in Sections 3 and 4.

2. Preliminaries. Let G be a finite nonabelian p-group of order p^m end exponent p^{m-2}. Choose an element $a \in G$ of order p^{m-2} and suppose $C_G(a) \neq \langle a\rangle$. Then G possesses an abelian subgroup H of type $(m-2,1)$ and has an element c such that $G = \langle H, c\rangle$ and $c^p \in H$. The action of c (by conjugation) on H follows the action of some element of order p lying in the automorphism group $A = \operatorname{Aut} H$ of H. Threrfore, in order to determine the group G, we need to find all the elements of order p lying in A.

Suppose $m \geq 4$ and choose an element b of H such that $H = \langle a\rangle \times \langle b\rangle$, $b^p = 1$. Then every automorphism of H maps a and b to $a^i b^k$ ($1 \leq i \leq p^{m-2}$, $p \nmid i$, $0 \leq k \leq p-1$) and $a^{p^{m-3}l} b^j$ ($1 \leq j \leq p-1$, $0 \leq l \leq p-1$) respectively. Hence denoting this automorphism by $\varphi(i,j;k,l)$, we have

$$A = \{\varphi(i,j;k,l) \mid 1 \leq i \leq p^{m-2},\ p \nmid i,\ 1 \leq j \leq p-1,\ 0 \leq k,l \leq p-1\}.$$

From this it follows that $|A| = p^{m-1}(p-1)^2$. To be explicit about the product of the antomorphisms of H, let $\varphi_1 = \varphi(i,j;k,l)$ and $\varphi_2 = \varphi(\alpha,\beta;\gamma,\delta)$ be two elements of A; then $\varphi_1\varphi_2$ is defined by putting $x(\varphi_1\varphi_2) = (x\varphi_1)\varphi_2$ for each element x of H. From this we have

$$(*) \quad \varphi(i,j;k,l)\,\varphi(\alpha,\beta;\gamma,\delta) = \varphi((i\alpha + p^{m-3}k\delta)^*, \overline{j\beta}; \overline{i\gamma + k\beta}, \overline{l\alpha + j\delta}\,),$$

where x^* (resp. $\bar{x}$) denotes the residue of x modulo p^{m-2} (resp. modulo p).

Suppose now p is odd. The center $Z(A)$ of A is given by

$$Z(A) = \{\varphi(i, \bar{i}; 0, 0 \mid 1 \leq i \leq p^{m-2},\ p \nmid i\}.$$

Hence $|Z(A)| = p^{m-3}(p-1)$ and a Sylow p-subgroup of $Z(A)$ is cyclic. Because $|A/Z(A)| = p^2(p-1)$, by Sylow's theorem $A/Z(A)$ is p-closed and hence A is p-closed. Now let P be a Sylow p-subgroup of A and set $Q = P \cap Z(A)$ $(= \langle \varphi(1+p, 1; 0, 0)\rangle)$. We choose the following three elements of order p from A:

$$\xi_1 = \varphi(1,1;0,1), \quad \xi_2 = \varphi(1+p^{m-3},1;0,0), \quad \xi_3 = \varphi(1,1;1,0),$$

and set $M = \langle \xi_1, \xi_2, \xi_3\rangle$. Then M is a nonabelian group of order p^3 and exponent p, and P is generated by M and Q. From this it follows that $M - \{1\}$ is the set of all the elements of order p in A.

We now find the conjugacy classes of the elements of order p lying in A.

Lemma 1. *$\langle \xi_1, \xi_2\rangle - \langle \xi_2\rangle$ is a conjugacy class in A.*

Proof. By making use of equation $(*)$, we see that the centralizer $C_A(\xi_1)$ of ξ_1 in A is given by

$$C_A(\xi_1) = \{\varphi(\alpha, \bar{\alpha}; 0, \delta) \mid 1 \le \alpha \le p^{m-2},\ p \nmid \alpha,\ 0 \le \delta \le p-1\}.$$

This shows that $|A : C_A(\xi_1)| = p(p-1)$. Further every element of $\langle \xi_1, \xi_2\rangle - \langle \xi_2\rangle$ is of the form $\xi_2^i\xi_1^j = \varphi(1+ip^{m-3},1;0,j)$ $(0 \le i \le p-1,\ 1 \le j \le p-1)$. Now let k, l be integers with $0 \le k \le p-1$, $1 \le l \le p-1$. Then $\varphi(l, j; \overline{i-k}, 0)$ transforms (by conjugation) $\xi_2^i\xi_1^j$ into $\xi_2^k\xi_1^l$. Hence the result follows.

Lemma 2. *$\langle \xi_2, \xi_3\rangle - \langle \xi_2\rangle$ is a conjugacy class in A.*

Proof. We have $|A : C_A(\xi_3)| = p(p-1)$ because $C_A(\xi_3)$ is given by

$$C_A(\xi_3) = \{\varphi(\alpha, \bar{\alpha}; \gamma, 0) \mid 1 \le \alpha \le p^{m-2},\ p \nmid \alpha,\ 0 \le \gamma \le p-1\}.$$

Every element of $\langle \xi_2, \xi_3\rangle - \langle \xi_2\rangle$ is of the form $\xi_2^i\xi_3^j = \varphi(1+ip^{m-3},1;j,0)$ $(0 \le i \le p-1,\ 1 \le j \le p-1)$, and the element $\varphi(j, l; 0, \overline{k-i})$ transforms $\xi_2^i\xi_3^j$ into $\xi_2^k\xi_3^l$. Hence the result follows.

Lemma 3. *For any i, j with $1 \le i, j \le p-1$, $\xi_1^i\xi_3^j$ is conjugate to every element of $\langle \xi_2\rangle\xi_1^i\xi_3^j$.*

Proof. Let i' be an integer with $1 \le i' \le p-1$, $ii' \equiv 1 \pmod p$. Then $\varphi(1, 1; \overline{-i'k}, 0)$ transforms $\xi_1^i\xi_3^j$ into $\xi_2^k\xi_1^i\xi_3^j$, and the result follows.

Lemma 4. *Given an integer k with $1 \le k \le p-1$, let k' be an integer with $1 \le k' \le p-1$, $kk' \equiv 1 \pmod p$. Then for i, j with $1 \le i$, $j \le p-1$, $\xi_1^i\xi_3^j$ is conjugate to $\xi_1^{ki}\xi_3^{k'j}$.*

Proof. Noting that $\varphi(1,k;0,0)^{-1} = \varphi(1,k';0,0)$, we obtain

$$\varphi(1,k;0,0)\cdot\xi_1^i\xi_3^j\cdot\varphi(1,k;0,0)^{-1} = \xi_1^{ki}\xi_3^{k'j}\ ,$$

and the result follows.

From Lemma 4, it follows that $\xi_1\xi_3$ is conjugate to $\xi_1^k\xi_3^{k'}$. But because $\xi_1^k\xi_3^{k'} \equiv (\xi_1^{k^2}\xi_3)^{k'} \bmod \langle\xi_2\rangle$, by Lemma 3 $\xi_1\xi_3$ is conjugate to $(\xi_1^{k^2}\xi_3)^{k'}$. Now let r be a quadratic nonresidue mod p. Then $\xi_1^r\xi_3$ is conjugate to $(\xi_1^{k^2r}\xi_3)^{k'}$. This shows that for an integer z, $1 \le z \le p-1$, if z is a quadratic residue mod p then the cyclic group $\langle\xi_1^z\xi_3\rangle$ contains an element which is conjugate to $\xi_1\xi_3$; and if z is a quadratic nonresidue mod p then the cyclic group $\langle\xi_1^z\xi_3\rangle$ contains an element which is conjugate to $\xi_1^r\xi_3$.

As stated before, G contains an element c such that $G = \langle H, c\rangle$ and $c^p \in H$, and the action of c on H follows that of some element φ of order p in A. Now let G' be another p-group of order p^m which contains $H = \langle a, b\rangle$. Choose an element c' of G' so that $G' = \langle H, c'\rangle$ and $c'^p \in H$. Assume that the action of c' on H follows that of φ' in A. Then it is easy to see that if either φ' is conjugate to φ or φ' is contained in $\langle\varphi\rangle$, G' is isomorphic to G. Summarizing above, we have the following:

Proposition 1. *Under the above notation, we can assume that the action of c on H is given by one of the following elements in A:*

$$\xi_1 = \varphi(1,1;0,1),\qquad \xi_2 = \varphi(1+p^{m-3},1;0,0),\qquad \xi_3 = \varphi(1,1;1,0),$$
$$\xi_1\xi_3 = \varphi(1,1;1,1),\qquad \xi_1^r\xi_3 = \varphi(1,1;1,r),$$

where r is a quadratic nonresidue mod p.

We next consider the case $p = 2$. In this case, A is given by

$$A = \{\varphi(i,1;k,l) \mid 1 \le i \le 2^{m-2},\ 2 \nmid i,\ 0 \le k, l \le 1\},$$

and so $|A| = 2^{m-1}$. We now find all the involutions in A. By $(*)$, we see that $\varphi(i,1;k,l)$ is an involution if and only if $i^2 + 2^{m-3}kl \equiv 1 \pmod{2^{m-2}}$. From this we obtain the following:

Lemma 5. *When $p = 2$, all the involutions in A are as follows:*
(1) $m = 4$: $\varphi(1,1;0,1)$, $\varphi(1,1;1,0)$, $\varphi(3,1;k,l)$;
(2) $m = 5$: $\varphi(1,1;0,1)$, $\varphi(1,1;1,0)$, $\varphi(3,1;k,l)$, $\varphi(5,1;k,l)$,
$\varphi(7,1;k,l)$;

(3) $m \geq 6$: $\varphi(1,1;0,1)$, $\varphi(1,1;1,0)$, $\varphi(\pm 1 + 2^{m-3}, 1; k, l)$,
$\varphi(-1 + 2^{m-2}, 1; k, l)$, $\varphi(\pm 1 + 2^{m-4}, 1; 1, 1)$,
$\varphi(\pm 1 + 3 \cdot 2^{m-4}, 1; 1, 1)$;

where $(k,l) = (0,0)$, $(0,1)$ *or* $(1,0)$.

Since $Z(A) = \{\varphi(i,1;0,0) \mid 1 \leq i \leq 2^{m-2}, 2 \nmid i\}$ is of order 2^{m-3}, $|A{:}Z(A)| = 2^2$. Hence the conjugacy class of each noncentral involution consists of two elements. One can see that for $(k,l) = (0,1)$, $(1,0)$, $\varphi(1 + 2^{m-3}, 1; k, l)$ is conjugate to $\varphi(1,1;k,l)$ $(m \geq 4)$ and $\varphi(-1 + 2^{m-3}, 1; k, l)$ is conjugate to $\varphi(-1 + 2^{m-2}, 1; k, l)$ $(m \geq 5)$ and $\varphi(\pm 1 + 3 \cdot 2^{m-4}, 1; 1, 1)$ is conjugate to $\varphi(\pm 1 + 2^{m-4}, 1; 1, 1)$ $(m \geq 6)$. Therefore we obtain the following result corresponding to Proposition 1.

Proposition 2. *When* $p = 2$, *we can assume that the action of* c *on* H *is given by one of the following elements in* A:

(1) $m = 4$: $\varphi(3,1;0,0)$, $\varphi(1,1;k,l)$;
(2) $m = 5$: $\varphi(i,1;0,0)$, $(i = 3,5,7)$, $\varphi(1,1;k,l)$, $\varphi(7,1;k,l)$;
(3) $m \geq 6$: $\varphi(i,1;0,0)$, $(i = \pm 1 + 2^{m-3}, -1 + 2^{m-2})$, $\varphi(1,1;k,l)$,
$\varphi(-1 + 2^{m-2}, 1; k, l)$, $\varphi(\pm 1 + 2^{m-4}, 1; 1, 1)$;

where $(k,l) = (0,1)$ *or* $(1,0)$.

3. Proof of Theorem 1. This section will be devoted to the proof of Theorem 1. Throughout this section, let p be an odd prime and G a finite nonabelian p-group of order p^m and exponent p^{m-2}. If $m = 3$, as G is of exponent p, by [1, §112] we have

Proposition 3. *If* $m = 3$ *then* G *is isomorphic to* G_1.

Suppose $m \geq 4$ and let a be an element of G of order p^{m-2}. We first consider the case that $C_G(a) \neq \langle a \rangle$.

Proposition 4. *Suppose* $C_G(a) \neq \langle a \rangle$. *Then* G *is isomorphic to one of the groups*: $G_1, G_2, G_3, G_4, G_5, G_6, G_9$ *and* G_{11}.

Proof. Let b be an element of order p such that $H = \langle a, b \rangle$ is an abelian subgroup of G of type $(m-2, 1)$, and choose $c \in G$ so that $G = \langle H, c \rangle$. Then the action of c on H follows the action of one of the automorphisms listed in Proposition 1. We consider four separate cases, depending on the action of c.

Case 1. Suppose that the action of c on H is given by ξ_1. Then $C_G(a) = G$ and $c^{-1}bc = a^{p^{m-3}}b$. As $G/\langle a\rangle$ is not a cyclic group, $\langle a, c\rangle$ is an abelian group of type $(m-2,1)$. Hence we can assume $c^p = 1$. This shows that $G \simeq G_4$.

Case 2. Suppose that the action of c on H is given by ξ_2. We show that $G \simeq G_2$ or G_3. By our assumption, we have

$$c^{-1}ac = a^{1+p^{m-3}}, \quad c^{-1}bc = b.$$

Assume first that $G/\langle a\rangle$ is not cyclic. Then $\langle a, c\rangle$ is a nonabelian p-group of order p^{m-1} and exponent p^{m-2}. Hence $\langle a, c\rangle \simeq M_{m-1}(p)$, and consequently $G \simeq G_3$. We next assume that $G/\langle a\rangle$ is a cyclic group. Then we can choose c so that $c^{p^2} \in \langle a\rangle$ and $c^p \notin \langle a\rangle$. Then $c^{p^2} = a^{\alpha p^2}$ for some α, and consequently $a^{-\alpha}c$ is of order p^2. Hence by choosing $\{a, a^{-\alpha}c\}$ as a generator of G, we have $G \simeq G_2$.

Case 3. Suppose that the action of c on H is given by ξ_3. We show that $G \simeq G_1$ or G_9. Because

$$c^{-1}ac = ab, \quad c^{-1}bc = b,$$

$G/\langle b\rangle$ is an abelian group of type $(m-2,1)$, and so we can assume that $c^p \in \langle b\rangle$. If $c^p = 1$, $G \simeq G_1$. On the other hand, if $c^p = b^\beta \neq 1$, by choosing $\{a^\beta b, b^\beta, c\}$ as a generator of G, we see that G has a presentation

$$\langle a, b, c \mid a^{p^{m-2}} = b^p = 1, c^p = b, ab = ba, c^{-1}ac = ab\rangle.$$

This shows that G is generated by $A = a^{-1}$ and $B = c$. Because A and B satisfy the relation:

$$A^{p^{m-2}} = B^{p^2} = 1, \quad A^{-1}BA = B^{1+p},$$

we have $G \simeq G_9$ in this case. Further if $m = 4$ then clearly $G_9 \simeq G_2$.

Case 4. Suppose that the action of c on H is given by $\xi_1\xi_3$ or $\xi_1^r\xi_3$. We show that $G \simeq G_5$ for the former case and $G \simeq G_6$ or G_{11} for the latter case. By our assumption,

$$c^{-1}ac = ab, \quad c^{-1}bc = a^{\delta p^{m-3}}b,$$

where

$$\delta = \begin{cases} 1 & \text{if the action of } c \text{ is given by } \xi_1\xi_3, \\ r & \text{if the action of } c \text{ is given by } \xi_1^r\xi_3. \end{cases}$$

From this it follows that $c^p \in Z(G) = \langle a^p \rangle$. Furthermore, because $G/\langle a^{p^{m-3}}, b\rangle$ is an abelian group of type $(m-3, 1)$, we can asssume that $c^p \equiv 1 \pmod{\langle a^{p^{m-3}}, b\rangle}$, and so $c^p = 1$ or $a^{\alpha p^{m-3}}$ for some α, $0 < \alpha < p$. If $c^p = 1$ then $G \simeq G_5$ or G_6. So we assume that there is no element of order p outside $\langle a, b\rangle$. Then noting that $c^{-k}a^x c^k = a^y b^{xk}$, where

$$y = x\Big(1 + \frac{\delta k(k-1)}{2}p^{m-3}\Big),$$

we obtain $(a^x c)^p = a^z$, where

$$z = \alpha p^{m-3} + x\Big(p + \frac{\delta(p+1)(p-1)}{6}p^{m-2}\Big).$$

Hence, if $p > 3$ then $(a^x c)^p = a^{\alpha p^{m-3} + xp}$, and so $(a^{-\alpha p^{m-4}}c)^p = 1$, which contradicts our assumption. This contradiction shows that $p = 3$. We then have $(a^x c)^3 = a^z$, where

$$z = 3^{m-3}\alpha + (3 + 3^{m-3}\delta)x.$$

Hence if $m > 4$, $(a^{-3^{m-4}\alpha}c)^3 = 1$, which contradicts our assumption again. Therefore only the case $p = 3$, $m = 4$ is remained. In this case, $c^3 = a^3$ or a^6 and $c^{-1}bc = a^3 b$ or $a^6 b$. But if $c^{-1}bc = a^3 b$, $(a^i c)^3 = 1$, where

$$i = \begin{cases} 1 & \text{if } c^3 = a^3, \\ 2 & \text{if } c^3 = a^6. \end{cases}$$

This is not the case. Hence $c^{-1}bc = a^6 b$, and so if $c^3 = a^3$, $G \simeq G_{11}$; and if $c^3 = a^6$, by choosing $\{a^2, b^2, c\}$ as a generator of G, we get $G \simeq G_{11}$ again. Thus we complete the proof of Proposition 4.

We next consider the case where G has no element of order p^{m-2} whose centralizer is of order greater than p^{m-2}.

Proposition 5. *Suppose that G has no element of order p^{m-2} whose centralizer is of order greater than p^{m-2}. If $\langle a\rangle$ is normal in G then G is isomorphic to G_8; while if G has no normal cyclic subgroup of order p^{m-2} then G is isomorphic to G_7 or G_{10}.*

Proof. Suppose first that $\langle a\rangle$ is normal in G. Since $C_G(a) = \langle a\rangle$, $G/\langle a\rangle$ is contained isomorphically in $\mathrm{Aut}\langle a\rangle$. Hence $G/\langle a\rangle$ is cyclic and $|\mathrm{Aut}\langle a\rangle|$ is divisible by $|G/\langle a\rangle| = p^2$, which implies that $m \geq 5$. Let b be an element of G such that $G = \langle a, b \rangle$. Then we may assume that the action of b on $\langle a \rangle$ is given by $b^{-1}ab = a^{1+p^{m-4}}$ (see [1, §100]). As $b^{p^2} \in Z(G) = \langle a^{p^2} \rangle$ we may set $b^{p^2} = a^{\alpha p^2}$. But then $(a^{-\alpha}b)^{p^2} = 1$. Therefore, by choosing $\{a, a^{-\alpha}b\}$ as a generator of G, we have $G \simeq G_8$.

Suppose next that G has no normal cyclic subgroup of order p^{m-2}. Let H be a maximal subgroup of G containing a. Then H is a nonabelian group of order p^{m-1} and exponent p^{m-2}. Therefore $H \simeq M_{m-1}(p)$. We choose c in $G - H$ so that $G = \langle H, c \rangle$. Now set

$$H = \langle a, b \mid a^{p^{m-2}} = 1, b^p = 1, b^{-1}ab = a^{1+p^{m-3}} \rangle.$$

We first consider the case $m \geq 5$ and set $\bar{G} = G/\langle a^{p^{m-3}} \rangle$. Then $\bar{H} = \langle \bar{a} \rangle \times \langle \bar{b} \rangle$ is an abelian group of type $(m-3, 1)$ and the action of $\bar{c}$ on $\bar{H}$ is given by an automorphism of $\bar{H}$ of order p. Such an automorphism is already given in the paragraph preceding Lemma 1. But because $\langle a \rangle$ is not normal, the automorphism is given by $\varphi(1 + ip^{m-4}, 1; j, k)$ with $j \neq 0$. Further we claim that k must be 0. Indeed, as $c^{-1}bc \equiv a^{kp^{m-4}}b$ $(\operatorname{mod} \langle a^{p^{m-3}} \rangle)$, if $k \neq 0$ we would have $|c^{-1}bc| > p$, which is impossible. Therefore the automorphism is given by $\varphi(1 + ip^{m-4}, 1; j, 0)$ with $j \neq 0$. We distinguish two cases.

Case 1. Suppose that the action of $\bar{c}$ on $\bar{H}$ is given by $\varphi(1, 1; j, 0)$. We show that $G \simeq G_7$ in this case. By our assumption we have

$$c^{-1}ac = a^{1+\alpha p^{m-3}}b^j, \quad c^{-1}bc = a^{\beta p^{m-3}}b,$$

where $0 \leq \alpha, \beta \leq p-1$. We first note that we can assume $\beta = 0$. Indeed, by setting $u = a^{\beta}c$, we have $u^{-1}bu = b$. We therefore have the following possibilities:

(i) $c^{-1}ac = ab$, $\quad c^{-1}bc = b$,
(ii) $c^{-1}ac = ab^j$, $\quad c^{-1}bc = b$,
(iii) $c^{-1}ac = a^{1+\alpha p^{m-3}}b$, $\quad c^{-1}bc = b$,
(iv) $c^{-1}ac = a^{1+\alpha p^{m-3}}b^j$, $\quad c^{-1}bc = b$,

where $1 \leq \alpha \leq p-1$, $1 < j \leq p-1$. We now set

$$v = \begin{cases} c^{j'} & \text{for case (ii)}, \\ b^{-\alpha}c & \text{for case (iii)}, \\ b^{-j'\alpha}c^{j'} & \text{for case (iv)}, \end{cases}$$

where $jj' \equiv 1 \pmod p$. We then have $v^{-1}av = ab$. This shows that we can assume that the action of c on H is given by (i). Then $c^p \in Z(G) = \langle a^p \rangle$.

As $C_G(c) \neq \langle c \rangle$, our assumption forces c to be of order at most p^{m-3}. Hence $c^p = a^{\gamma p^2}$ for some γ, and consequently $(a^{-\gamma p}c)^p = 1$. Therefore by choosing $\{a, b, a^{-\gamma p}c\}$ as a generator of G, we have $G \simeq G_7$ $(m \geq 5)$.

Case 2. Suppose that the action of $\bar{c}$ on $\overline{H}$ is given by $\varphi(1 + ip^{m-4}, 1; j, 0)$, $i \neq 0$. We show that $G \simeq G_{10}$. By our assumption,

$$c^{-1}ac = a^{1+(i+kp)p^{m-4}}b^j, \quad c^{-1}bc = a^{lp^{m-3}}b,$$

where $0 \leq k, l \leq p-1$. Setting $u = a^l c$, we get $u^{-1}bu = b$, and so we can assume $l = 0$. We therefore have the following possibilities:

(i) $c^{-1}ac = a^{1+p^{m-4}}b$, $\quad c^{-1}bc = b$,
(ii) $c^{-1}ac = a^{1+p^{m-4}}b^j$, $\quad c^{-1}bc = b$,
(iii) $c^{-1}ac = a^{1+\alpha p^{m-4}}b$, $\quad c^{-1}bc = b$,
(iv) $c^{-1}ac = a^{1+\alpha p^{m-4}}b^j$, $c^{-1}bc = b$,

where $1 < \alpha \leq p^2 - 1$, $p \nmid \alpha$, $1 < j \leq p-1$. Let α' be an integer with $\alpha\alpha' \equiv 1 \pmod{p^2}$ and $2'$ an integer with $22' \equiv 1 \pmod{p}$. Set

$$v = \begin{cases} b^{2'(\alpha-1)}c^{\alpha'} & \text{if } m = 5, \\ c^{\alpha'} & \text{if } m \geq 6. \end{cases}$$

Then

$$v^{-1}av = \begin{cases} a^{1+p^{m-4}}b^{\alpha'} & \text{for case (iii)}, \\ a^{1+p^{m-4}}b^{\alpha' j} & \text{for case (iv)}. \end{cases}$$

This shows that we can assume that the action of c on H is given by (i) or (ii). Suppose that case (ii) holds and let j' be an integer with $jj' \equiv 1 \pmod{p}$. Then setting

$$A = a^{j'}, \quad B = a^x b,$$

where $x = 2'(3j' + 1)p^{m-3}$, we get

$$B^{-1}AB = A^{1+p^{m-3}}, \quad c^{-1}Ac = A^{1+p^{m-4}}B, \quad c^{-1}Bc = B.$$

This shows that the group given by (ii) is isomorphic to the group given by (i), and consequently we can assume that the action of c on H is given by (i). We then have

$$c^{-p}ac^p = a^{1+p^{m-3}} = b^{-1}ab,$$

which implies that $c^p \equiv b \pmod{Z(G)}$. But $Z(G) = \langle a^{p^2} \rangle$, and hence we may set $c^p = a^{\gamma p^2}b$. Then $(a^{-\gamma p}c)^p = b$. Thus, by choosing $\{a, b, a^{-\gamma p}c\}$ as a generator of G, we see that G has a presentation

$$\langle a, b, c \rangle, \ a^{p^{m-2}} = b^p = 1, \ c^p = b, \ b^{-1}ab = a^{1+p^{m-3}}, \ c^{-1}ac = a^{1+p^{m-4}}b.$$

This shows that G is generated by $A = a$ and $B = a^{p^{m-5}}c$. But, because B^p is a generator of the commutator subgroup of G, $\langle B\rangle$ is normal in G. Therefore, if $m = 5$, G has a cyclic normal subgroup of order p^3 $(= p^{m-2})$, which contradicts our assumption. Thus we have $m \geq 6$. Because A and B satisfy the relation:

$$A^{p^{m-2}} = 1, \quad A^{p^{m-3}} = B^{p^2}, \quad A^{-1}BA = B^{1-p},$$

we get $G \simeq G_{10}$.

In final, we show that if $m = 4$ then $G \simeq G_7$. Since c^p is of order at most p, we may set $c^p = a^{\alpha p}b^{\beta}$. If $\beta \neq 0$ then a^p is not contained in $\langle c\rangle$. But, because $\langle a^p\rangle$ is the center of $\langle a, b\rangle$ and its order is p, a^p is a central element of G. Therefore it is contained in $C_G(c)$. Because c is of order p^2, this contradicts our assumption. Thus we have $\beta = 0$. Set $\overline{G} = G/\langle a^p\rangle$. Then, because $\langle a\rangle$ is not normal in G, we see that $\overline{G}$ is a nonabelian group of order p^3 and exponent p. Hence by [1, §112], we can assume that

$$ac \equiv cab, \quad bc \equiv cb, \quad (\mathrm{mod}\, \langle a^p\rangle).$$

Then the action of c on $\langle a, b\rangle$ is given by

$$c^{-1}ac = a^{1+\gamma p}b, \quad c^{-1}bc = a^{\delta p}b.$$

Hence, setting $u = a^{\delta}b^{-\gamma}c$, we have $u^{-1}bu = b$. This shows that $C_G(u) \neq \langle u\rangle$. Therefore by our assumption u is of order p. Then, because $u^{-1}au = ab$, by choosing $\{a, b, u\}$ as a generator of G, we have $G \simeq G_7$. Thus we complete the proof of Proposition 5, and so Theorem 1 is proved.

Remark 1. We show that none of the groups listed in Theorem 1 are isomorphic. We use the following notation: Given a finite p-group G, $\Phi(G)$ is a Frattini subgroup of G. We set $p^{d(G)} = |G/\Phi(G)|$. $\gamma_2(G)$ is the commutator subgroup of G and $\overline{G} = G/\gamma_2(G)$. The group generated by $\{x^p \mid x \in G\}$ is denoted by G^p.

(1) $d(G_3) = d(G_4) = 3$ and $d(G_i) = 2$ for $i \neq 3, 4$.

(2) $Z(G_3) \simeq C_{p^{m-3}} \times C_p$ and $Z(G_4) \simeq C_{p^{m-2}}$.

(3) $[G_1 : G_1^p] = p^3$ and $\gamma_2(G_5) \simeq \gamma_2(G_6) \simeq \gamma_2(G_7) \simeq \gamma_2(G_{11}) \simeq C_p \times C_p$. This implies that the groups G_i $(i = 1, 5, 6, 7, 11)$ are nonmetacyclic. While, evidently G_2, G_8, G_9 and G_{10} are metacyclic.

(4) $\overline{G}_2 \simeq C_{p^{m-3}} \times C_{p^2}$, $\overline{G}_8 \simeq C_{p^{m-4}} \times C_{p^2}$, $\overline{G}_9 \simeq C_{p^{m-2}} \times C_p$ and $\overline{G}_{10} \simeq C_{p^{m-3}} \times C_p$.

(5) $\overline{G}_1 \simeq C_{p^{m-2}} \times C_p$ and $\overline{G}_5 \simeq \overline{G}_6 \simeq \overline{G}_7 \simeq C_{p^{m-3}} \times C_p$.

(6) $C_{G_5}(\gamma_2(G_5)) = C_{G_6}(\gamma_2(G_6)) = \langle a, b\rangle$ and $C_{G_7}(\gamma_2(G_7)) = \langle a^p, b, c\rangle$.

(7) For any $u \in C_{G_5}(\Phi(G_5)) - \Phi(G_5) = \langle a, b\rangle - \langle a^p, b\rangle$ and $x \in G_5 - C_{G_5}(\Phi(G_5)) = G_5 - \langle a, b\rangle$, $[[u, x], x] = u^{qp^{m-3}}$, where q is some quadratic residue mod p. On the other hand, for $a \in C_{G_6}(\Phi(G_6)) - \Phi(G_6) = \langle a, b\rangle - \langle a^p, b\rangle$ and $c \in G_6 - C_{G_6}(\Phi(G_6)) = G_6 - \langle a, b\rangle$, $[[a, c], c] = a^{rp^{m-3}}$.

These seven claims imply that none of the groups $G_1, \dots, G_{10}$ are isomorphic. Because $\gamma_2(G_1) \simeq C_p$, by (1) and (3) it suffices to show that none of the groups G_5, G_6, G_7 with $p = 3$, $m = 4$ are isomorphic to G_{11}. Because $C_{G_{11}}(\gamma_2(G_{11})) = \langle a, b\rangle$, (6) implies that G_7 is not isomorphic to G_{11}. Further $G_{11} - C_{G_{11}}(\gamma_2(G_{11}))$ contains no element of order 3, but for $i = 5, 6$, $G_i - C_{G_i}(\gamma_2(G_i))$ contains an element of order p for any prime p. Hence neither G_5 nor G_6 is isomorphic to G_{11}.

4. Proof of Theorem 2. This section will be devoted to the proof of Theorem 2. Throughout this section, let G be a nonabelian 2-group of order 2^m and exponent 2^{m-2}, and let a be an element of G of order 2^{m-2}.

Proposition 6. *Suppose $C_G(a) \neq \langle a\rangle$. Then G is isomorphic to one of the groups $G_1, G_2, \dots, G_{14}, G_{22}$ and G_{23}.*

Proof. Let b be an element of order 2 such that $H = \langle a, b\rangle$ is an abelian subgroup of G of type $(m-2, 1)$ and choose $c \in G$ so that $G = \langle H, c\rangle$. Then the action of c on H follows the action of one of the automorphisms listed in Proposition 2. We consider nine separate cases, depending on the action of c.

Case 1. Suppose that the action of c on H is given by $\varphi(1, 1; 0, 1)$. Then by making use of a similar argument as in Case 1 of the proof of Proposition 4, we have $G \simeq G_4$.

Case 2. Suppose that the action of c on H is given by $\varphi(1 + 2^{m-3}, 1; 0, 0)$. We show that G is isomorphic to $G_2 (m = 4)$ or $G_3 (m = 4)$ or G_1 or G_{10}. By our assumption, we have

$$c^{-1}ac = a^{1+2^{m-3}}, \quad c^{-1}bc = b.$$

Suppose first that $G/\langle a\rangle$ is not cyclic. Then $\langle a, c\rangle$ is a nonabelian 2-group of order 2^{m-1} and exponent 2^{m-2}. Hence if $m \geq 5$, $\langle a, c\rangle \simeq M_{m-1}(2)$, and if $m = 4$, $\langle a, c\rangle \simeq Q_3$ or D_3, and correspondingly $G \simeq G_{10}$ or $G \simeq G_2$

$(m = 4)$ or $G \simeq G_3$ $(m = 4)$. On other hand, if $G/\langle a\rangle$ is cyclic then we may set $c^4 = a^{4\alpha}$. But then, because $(a^{-\alpha}c)^4 = 1$, by choosing $\{a, a^{-\alpha}c\}$ as a generator of G, we have $G \simeq G_1$.

Case 3. Suppose that the action of c on H is given by $\varphi(1,1;1,0)$. Then by making use of a similar argument as in Case 3 of the proof of Proposition 4, we have $G \simeq G_5$ or G_9; and $G_9 \simeq G_1$ provided $m = 4$.

Case 4. Suppose that $m \geq 5$ and the action of c on H is given by $\varphi(-1+2^{m-2},1;0,0)$. Then

$$c^{-1}ac = a^{-1}, \quad c^{-1}bc = b.$$

From this we have $Z(G) = \langle a^{2^{m-3}}, b\rangle$. As $c^2 \in Z(G)$, $c^2 = 1$, $a^{2^{m-3}}$, b or $a^{2^{m-3}}b$. If $c^2 = 1$ (resp. $a^{2^{m-3}}$), then $G \simeq G_3$ (resp. G_2). On the other hand, if $c^2 = b$ or $a^{2^{m-2}}b$ then by choosing $\{a, c\}$ as a generator of G, we have $G \simeq G_6$.

Case 5. Suppose that $m \geq 5$ and the action of c on H is given by $\varphi(-1+2^{m-2},1;0,0)$. Then

$$c^{-1}ac = a^{-1+2^{m-3}}, \quad c^{-1}bc = b.$$

From this it follows that $G/\langle b\rangle \simeq S_{m-1}$, and so we can assume that $c^2 = 1$ or b. We therefore have $G \simeq G_{11}$ or G_7.

Case 6. Suppose that $m \geq 5$ and the action of c on H is given by $\varphi(-1+2^{m-2},1;0,1)$. Because

$$c^{-1}ac = a^{-1}, \quad c^{-1}bc = a^{2^{m-3}}b,$$

$c^2 \in Z(G) = \langle a^{2^{m-4}}b\rangle$ and consequently $c^2 = 1$, $a^{2^{m-3}}$, $a^{2^{m-4}}b$ or $a^{3\cdot 2^{m-4}}b$. If $c^2 = a^{2^{m-3}}$ then $(abc)^2 = 1$. This shows that if $c^2 = 1$ or $a^{2^{m-3}}$ then $G \simeq G_{12}$. On the other hand, if $c^2 = a^{2^{m-4}}b$ or $a^{3\cdot 2^{m-4}}b$ then by choosing $\{a, c\}$ as a generator of G, we have $G \simeq G_8$.

Case 7. Suppose that $m \geq 5$ and the action of c on H is given by $\varphi(-1+2^{m-2},1;1,0)$. Then

$$c^{-1}ac = a^{-1}b, \quad c^{-1}bc = b.$$

Since $c^2 \in Z(G)$, $c^2 = 1$, $a^{2^{m-3}}$, b or $a^{2^{m-3}}b$. If $c^2 = b$ (resp. $a^{2^{m-3}}b$), $(ac)^2 = 1$ (resp. $a^{2^{m-3}}$). Hence we can assume that $c^2 = 1$ or $a^{2^{m-3}}$, and consequently we have $G \simeq G_{13}$ or G_{14}.

Case 8. Suppose that $m \geq 6$ and the action of c on H is given by $\varphi(1+2^{m-4}, 1; 1, 1)$. Because

$$c^{-1}ac = a^{1+2^{m-4}}b, \quad c^{-1}bc = a^{2^{m-3}}b,$$

$G/\langle a^{2^{m-4}}b\rangle$ is an abelian group of type $(m-3, 1)$, and so we can assume that $c^2 \in \langle a^{2^{m-4}}b\rangle$. Therefore, noting that $c^2 \in Z(G) = \langle a^2 b\rangle$, we obtain $c^2 = 1$ or $a^{2^{m-3}}$. If $c^2 = a^{2^{m-3}}$ then $(bc)^2 = 1$. This shows that we can assume $c^2 = 1$, and consequently we have $G \simeq G_{22}$.

Case 9. Suppose that $m \geq 6$ and the action of c on H is given by $\varphi(-1+2^{m-4}, 1; 1, 1)$. Then

$$c^{-1}ac = a^{-1+2^{m-4}}b, \quad c^{-1}bc = a^{2^{m-3}}b.$$

From this we have $Z(G) = \langle a^{2^{m-4}}b\rangle$. As $c^2 \in Z(G)$, it holds that $c^2 = 1$, $a^{2^{m-3}}$, $a^{2^{m-4}}b$ or $a^{3\cdot 2^{m-4}}b$. But then $(a^k c)^2 = 1$, where

$$k = \begin{cases} 2 & \text{if } c^2 = a^{2^{m-3}}, \\ 3 & \text{if } c^2 = a^{2^{m-4}}b, \\ 1 & \text{if } c^2 = a^{3\cdot 2^{m-4}}b, \end{cases}$$

and consequently we can assume that $c^2 = 1$, and so $G \simeq G_{23}$.

We next consider the case where G has no element of order 2^{m-2} whose centralizer is of order greater than 2^{m-2}.

Proposition 7. *Suppose that G has no element of order 2^{m-2} whose centralizer is of order greater than 2^{m-2}. If $\langle a\rangle$ is normal in G then G is isomorphic to one of the groups G_{15}, G_{16}, G_{19} and G_{20}; while if G has no normal cyclic subgroup of order 2^{m-2} then G is isomorphic to one of the groups $G_{17}, G_{18}, G_{21}, G_{24}, G_{25}$ and G_{26}.*

Proof. Suppose first that $\langle a\rangle$ is normal in G. We distinguish two cases.

Case 1. $G/\langle a\rangle$ is cyclic. We show that $G \simeq G_{19}$ or G_{20}. Since $G/\langle a\rangle$ is contained isomorphically in $\mathrm{Aut}\langle a\rangle$, we have $m \geq 6$. We can choose an element b of G so that $G = \langle a, b\rangle$, $b^4 \in \langle a\rangle$, and we can assume that the action of b on $\langle a\rangle$ is given by $b^{-1}ab = a^{1+2^{m-4}}$ or $a^{-1+2^{m-4}}$ (see [1, §100]). Suppose first $b^{-1}ab = a^{1+2^{m-4}}$. We may set $b^4 = a^{4\alpha}$. Then for an integer k with $\alpha + (1+2^{m-5})k \equiv 0 \pmod{2^{m-4}}$, we have $(a^k b)^4 = 1$. Suppose next $b^{-1}ab = a^{-1+2^{m-4}}$. Then $b^4 \in Z(G) = \langle a^{2^{m-3}} \rangle$. If $b^4 = a^{2^{m-3}}$ then $(ab)^4 = 1$. Therefore we can assume that $b^4 = 1$ in either case. Thus we have $G \simeq G_{19}$ or G_{20}.

Case 2. $G/\langle a \rangle$ is not cyclic. We show that $G \simeq G_{15}$ or G_{16}. Since $G/\langle a \rangle$ is an abelian group of type $(1,1)$ we have $m \geq 5$ and we can choose elements b and c of G so that

$$G = \langle a, b, c \rangle, \quad b^2, c^2 \in \langle a \rangle, \quad bc \equiv cb \pmod{\langle a \rangle}.$$

Now set $b^{-1}ab = a^i$, $c^{-1}ac = a^j$. If $i = j$ then $bc^{-1} \in C_G(a) = \langle a \rangle$, which contradicts our assumption. Hence $i \neq j$. Assume $i = -1$. Then $j = 1 + 2^{m-3}$ or $-1 + 2^{m-3}$, and

$$(bc)^{-1}a(bc) = \begin{cases} a^{-1+2^{m-3}} & \text{if } j = 1 + 2^{m-3}, \\ a^{1+2^{m-3}} & \text{if } j = -1 + 2^{m-3}. \end{cases}$$

The above implies that by replacing b and c with suitable elements of G if necessary, we can assume that $i = 1 + 2^{m-3}$, $j = -1 + 2^{m-3}$ and $b^2 = c^2 = 1$. We then have $(bc)^{-1}a(bc) = a^{-1}$, and so $\langle a, bc \rangle \simeq D_{m-1}$ or Q_{m-1}. Therefore $(bc)^2 = 1$ or $a^{2^{m-3}}$, which implies that $c^{-1}bc = b$ or $a^{2^{m-3}}b$. Thus $G \simeq G_{15}$ or G_{16} in this case.

Suppose next that G has no normal cyclic subgroup of order 2^{m-2}. Let H be a maximal subgroup of G containing a. Then H is a nonabelian group of order 2^{m-1} and exponent 2^{m-2}. We first show that $m \geq 5$. So suppose $m = 4$. Then $H \simeq Q_3$ or D_3. But, because $\langle a \rangle$ is not normal in G, H is isomorphic to Q_3 and $G/\langle a^2 \rangle$ is nonabelian. Therefore we can choose an element u of G so that $u^2 \in H - \langle a^2 \rangle$. But then u is of order 8, which contradicts our assumption. This contradiction shows that $m \geq 5$. If $H \simeq Q_{m-1}$, D_{m-1} or S_{m-1} then $\langle a \rangle$ is a characteristic subgroup of H, and so $\langle a \rangle$ is normal in G, which is not the case. Hence $H \simeq M_{m-1}(2)$. Set

$$H = \langle a, b \mid a^{2^{m-2}} = 1, b^2 = 1, b^{-1}ab = a^{1+2^{m-3}} \rangle,$$
$$G = \langle H, c \rangle, \quad \overline{G} = G/\langle a^{2^{m-3}} \rangle.$$

Then $\overline{H} = H/\langle a^{2^{m-3}} \rangle$ is an abelian group of type $(m-3, 1)$ and $\overline{G} = \langle \overline{H}, \overline{c} \rangle$. Therefore the action of $\overline{c}$ on $\overline{H}$ is given by an automorphism of $\overline{H}$ of order 2. Such an automorphism is already given in Lemma 5. But, because $\langle a \rangle$ is not normal, the automorphism is given by $\varphi(i, 1; 1, l)$. Further $\overline{b}$ must be transformed into $\bar{b}$ by this automorphism, and so $l = 0$. Therefore the automorphisms are as follows:

$$m = 5: \quad \varphi(1,1;1,0),\ \varphi(3,1;1,0);$$
$$m \geq 6: \quad \varphi(1,1;1,0),\ \varphi(-1+2^{m-3},1;1,0),\ \varphi(\pm 1+2^{m-4},1;1,0).$$

We consider four separate cases, depending on the action of $\bar{c}$.

Case 1. Suppose that $m \geq 5$ and the action of $\bar{c}$ on $\bar{H}$ is given by $\varphi(1,1;1,0)$. We show that $G \simeq G_{17}$ or G_{26}. By our assumptoin we have the following possibilities:

(i) $c^{-1}ac = ab,\quad c^{-1}bc = b,$
(ii) $c^{-1}ac = a^{1+2^{m-3}}b, c^{-1}bc = b,$
(iii) $c^{-1}ac = ab,\quad c^{-1}bc = a^{2^{m-3}}b,$
(iv) $c^{-1}ac = a^{1+2^{m-3}}b, c^{-1}bc = a^{2^{m-3}}b.$

If $c^{-1}bc = a^{2^{m-3}}b$, setting $u = ac$, we have $u^{-1}bu = b$. This shows that it will suffice to consider cases (i) and (ii). But if (ii) holds then, setting $v = bc$, we have $v^{-1}av = ab$, and consequently we can assume that the action of c on H is given by (i). Then as $c^2 \in Z(G) = \langle a^4 \rangle$, we may set $c^2 = a^{4\alpha}$. If $m \geq 6$, $(a^{-(2+2^{m-4})\alpha}c)^2 = 1$. Hence, by choosing $\{a, b, a^{-(2+2^{m-4})\alpha}c\}$ as a generator of G, we have $G \simeq G_{17}$ in this case. On the other hand, if $m = 5$, $c^2 = 1$ or a^4, and so $G \simeq G_{17}$ or G_{26}.

Case 2. Suppose that $m \geq 5$ and the action of $\bar{c}$ on $\bar{H}$ is given by $\varphi(-1+2^{m-3},1;1,0)$. Then by a similar argument as in case 1, we can assume that the action of c on H is given by

$$c^{-1}ac = a^{-1}b, \quad c^{-1}bc = b.$$

Then $c^{-2}ac^2 = b^{-1}ab$, which implies that $c^2 \equiv b \,(\mathrm{mod} Z(G))$. But, because $Z(G) = \langle a^{2^{m-3}} \rangle$, we have $c^2 = b$ or $a^{2^{m-3}}b$. If $c^2 = a^{2^{m-3}}b$ then $(a^2c)^2 = b$. This shows that we can assume $c^2 = b$, and hence $G \simeq G_{18}$.

Case 3. Suppose that $m \geq 6$ and the action of $\bar{c}$ on $\bar{H}$ is given by $\varphi(1+2^{m-4},1;1,0)$. Then by a similar argument as in Case 1, we can assume that the action of c on H is given by

$$c^{-1}ac = a^{1+2^{m-4}}b, \quad c^{-1}bc = b.$$

Then $c^{-2}ac^2 = b^{-1}ab$, which implies that $c^2 \equiv b \,(\mathrm{mod}\, Z(G))$. But, because $Z(G) = \langle a^2 \rangle$, we may set $c^2 = a^{2\alpha}b$. If α is odd then c is of order 2^{m-2}

and $C_G(c) \neq \langle c \rangle$. This is not the case. Hence α is even. We then have $(a^{-\alpha}c)^2 = b$, which shows that we can assume $c^2 = b$. Thus G has a presentation

$$\langle a, b, c \rangle,\ a^{2^{m-2}} = b^2 = 1,\ c^2 = b,\ b^{-1}ab = a^{1+2^{m-3}},\ c^{-1}ac = a^{1+2^{m-4}}b.$$

Now set $B = a^{2^{m-5}}c$. Then G is generated by a and B, and these elements satisfy the relation:

$$a^{2^{m-3}} = B^4, \quad a^{-1}Ba = B^{-1}.$$

Thus we get $G \simeq G_{21}$.

Case 4. Suppose that $m \geq 6$ and the action of $\bar{c}$ on $\bar{H}$ is given by $\varphi(-1+2^{m-4}, 1; 1, 0)$. By a similar argument as in Case 1, we can assume that the action of c on H is given by

$$c^{-1}ac = a^{-1+2^{m-4}}b, \quad c^{-1}bc = b.$$

Then $c^2 \in Z(G) = \langle a^{2^{m-3}} \rangle$, and so $c^2 = 1$ or $a^{2^{m-3}}$. Hence $G \simeq G_{24}$ or G_{25}. This completes the proof of Proposition 7, and so Theorem 2 is proved.

Remark 2. We show that none of the groups listed in Theorem 2 are isomorphic. Given a finite 2-group G, we denote by $I(G)$ the set of all the involutions in G, and by $i(G)$ the number of elements in $I(G)$. The class of G is denoted by $\mathrm{cl}(G)$. The other notation we use here is given in Remark 1.

(1) $d(G_i) = 2$ or 3; and $d(G_i) = 3$ only when $i = 2, 3, 4, 10, 11, 12, 15$ or 16.

(2) $\mathrm{cl}(G_4) = \mathrm{cl}(G_{10}) = 2$; and $\mathrm{cl}(G_i) = m - 2$ for $i = 2, 3, 11, 12, 15$ and 16.

(3) $Z(G_4) \simeq C_{2^{m-2}}$ and $Z(G_{10}) \simeq C_{2^{m-3}} \times C_2$.

(4) $Z(G_2) \simeq Z(G_3) \simeq Z(G_{11}) \simeq C_2 \times C_2$; $Z(G_{12}) \simeq C_4$ and $Z(G_{15}) \simeq Z(G_{16}) \simeq C_2$.

(5) $\langle I(G_2) \rangle = Z(G_2)$, $\langle I(G_3) \rangle = G_3$ and $\langle I(G_{11}) \rangle \simeq D_{m-2} \times C_2$.

(6) $i(G_{15}) = 2^{m-2} + 2^{m-3} + 3$ and $i(G_{16}) = 2^{m-3} + 3$.

The above implies that when $m \neq 4$ none of the groups generated by exactly three elements are isomorphic. Let $m = 4$. Then G_2, G_3 and G_4

are the groups generated by exactly three elements and all of them are of class 2. But by (3), (4) and (5) none of them are isomorphic.

(7) $\gamma_2(G_{17}) \simeq \gamma_2(G_{26}) \simeq C_2 \times C_2$; and for each $i \in \{5, 13, 14, 18, 22, 23, 24, 25\}$, $\gamma_2(G_i)$ is a cyclic group whose generator is not the square of an element of G. This implies that the groups G_i ($i = 5, 13, 14, 17, 18, 22, 23, 24, 25, 26$) are nonmetacyclic. While evidently G_i ($i = 1, 6, 7, 8, 9, 19, 20, 21$) are metacyclic.

(8) $\mathrm{cl}(G_1) = \mathrm{cl}(G_9) = \mathrm{cl}(G_{19}) = 2$; $\mathrm{cl}(G_{21}) = 3$; and $\mathrm{cl}(G_6) = \mathrm{cl}(G_7) = \mathrm{cl}(G_8) = \mathrm{cl}(G_{20}) = m - 2$ (≥ 3).

(9) $\gamma_2(G_1) \simeq \gamma_2(G_9) \simeq C_2$ and $\gamma_2(G_{19}) \simeq C_4$; $\bar{G}_1 \simeq C_{2^{m-3}} \times C_4$ and $\bar{G}_9 \simeq C_{2^{m-2}} \times C_2$.

(10) $Z(G_6) \simeq Z(G_7) \simeq C_2 \times C_2$, $Z(G_8) \simeq C_4$ and $Z(G_{20}) \simeq C_2$;

$$\langle x^2 \mid x \in G_6 - C_{G_6}(\gamma_2(G_6))\rangle = \langle b^2 \rangle \simeq C_2,$$
$$\langle x^2 \mid x \in G_7 - C_{G_7}(\gamma_2(G_7))\rangle = \langle a^{2^{m-3}}, b^2 \rangle \simeq C_2 \times C_2.$$

(11) $\mathrm{cl}(G_5) = 2$, $\mathrm{cl}(G_{17}) = \mathrm{cl}(G_{22}) = \mathrm{cl}(G_{26}) = 3$ and $\mathrm{cl}(G_i) = m - 2$ (≥ 3) for $i = 13, 14, 18, 23, 24$ and 25.

(12) $\gamma_2(G_{17}) \simeq C_2 \times C_2$ and $\gamma_2(G_{22}) \simeq C_4$.

(13) $Z(G_{13}) \simeq Z(G_{14}) \simeq C_2 \times C_2$, $Z(G_{18}) \simeq Z(G_{24}) \simeq Z(G_{25}) \simeq C_2$ and $Z(G_{23}) \simeq C_4$.

(14) $i(G_{13}) = i(G_{24}) = 2^{m-2} + 3$; $i(G_{14}) = i(G_{25}) = 3$ and $i(G_{18}) = 2^{m-3} + 3$.

(7) through (14) imply that when $m \neq 5$ none of the groups generated by exactly two elements are isomorphic. Now let $m = 5$. Then G_i ($i = 6, 7, 8, 13, 14, 17, 18, 26$) are the groups of order 2^5 which are genenrated by exactly two elements and of class 3. But $\gamma_2(G_{17}) \simeq \gamma_2(G_{26}) \simeq C_2 \times C_2$ and $\gamma_2(G_i) \simeq C_{2^{m-3}}$ for the other i. Hence by (7), (10), (13) and (14) it suffices to show that G_{17} with $m = 5$ is not isomorphic to G_{26}. This follows at once from the fact that $i(G_{26}) = 3$ and $i(G_{17}) = 11$ provided $m = 5$.

Remark 3. Burnside [1] has given all the types of the groups of exponent p^{m-2} under the assumption that the groups have cyclic normal subgroups of order p^{m-2}. But, when $p = 2$ there are two clerical errors: one group is omitted and two groups which are isomorphic are listed as distinct groups.

(1) Suppose that $m > 5$, $C_G(a) \neq \langle a \rangle$ and $G/\langle a \rangle$ is cyclic. As for such

groups, the following five distinct types are given in pp.138–139:

$$\langle a, b \mid a^{2^{m-2}} = 1,\ b^4 = 1,\ b^{-1}ab = a^{\alpha} \rangle,$$

where $\alpha = -1$, $\pm 1 + 2^{m-3}$, $\pm 1 + 2^{m-4}$. But there is one more type, that is, the group G_8 in Theorem 2 should be added in the list.

(2) The groups of type (xi) and (xii) in p.139 are isomorphic. These groups are given by

$$\begin{aligned} G_{\mathrm{xi}} = \langle a, b, c \mid a^{2^{m-2}} = 1,\ b^2 = 1,\ c^2 = 1,\ ab = ba,& \\ c^{-1}ac = a^{-1},\ c^{-1}bc = a^{2^{m-3}}b \rangle;& \\ G_{\mathrm{xii}} = \langle a, b, c \mid a^{2^{m-2}} = 1,\ b^2 = 1,\ c^2 = 1,\ ab = ba,& \\ c^{-1}ac = a^{-1+2^{m-3}},\ c^{-1}bc = a^{2^{m-3}}b \rangle.& \end{aligned}$$

G_{xii} is generated by $A = ab$, b and c; and these elements satisfy the following relation:

$$c^{-1}Ac = A^{-1}, \quad c^{-1}bc = A^{2^{m-3}}b.$$

This shows that $G_{\mathrm{xii}} \simeq G_{\mathrm{xi}}$.

Remark 4. By using our results, we can calculate the nilpotency indices of the radicals $J(kG)$ of the group algebras kG over a field k of characteristic p for p-groups G with cyclic subgroups of index p^2, and consequently we can characterize the p-groups G of order p^m such that the nilpotency indices of $J(kG)$ are greater than or equal to p^{m-2} (see [5]).

REFERENCES

[1] W. BURNSIDE: Theory of Groups of Finite Order, 2nd edition, Cambridge Univ. Press, Cambridge, 1911.

[2] G. A. MILLER: Determination of all the groups of order p^m which contain the abelian group of type $(m-2, 1)$, p being any prime, Trans. Amer. Math. Soc. **2** (1901), 259–272.

[3] G. A. MILLER: On the groups of order p^m which contain operators of order p^{m-2}, Trans. Amer. Math. Soc. **3** (1902), 383–387.

[4] G. A. MILLER: Notes and errata, Trans. Amer. Math. Soc. **3** (1902), 499–500.

[5] Y. NINOMIYA: Nilpotency indices of the radicals of p-group algebras, Proc. Edinburgh Math. Soc. **37** (1994), to appear.

DEPARTMENT OF MATHEMATICS
FACULTY OF LIBERAL ARTS
SHINSHU UNIVERSITY
MATSUMOTO 390, JAPAN

(*Received November 11, 1992*)

CURRENT ADDRESS:
DEPARTMENT OF MATHEMATICAL SCIENCES
FACULTY OF SCIENCE
SHINSHU UNIVERSITY
MATSUMOTO 390, JAPAN

E-mail address: ysninom@gipac.shinshu-u.ac.jp