Hokkaido Mathematical Journal Vol. 41 (2012) p. 185–208

Extensions of cyclic p-groups which preserve the irreducibilities of induced characters

Katsusuke Sekiguchi

(Received September 10, 2010; Revised October 22, 2011)

Abstract. For a prime p, we denote by B_n the cyclic group of order p^n. Let ϕ be a faithful irreducible character of B_n, where p is an odd prime. We study the p-group G containing B_n such that the induced character ϕ^G is also irreducible. Set $[N_G(B_n) : B_n] = p^m$ and $[G : B_n] = p^M$. The purpose of this paper is to determine the structure of G under the hypothesis $[N_G(B_n) : B_n]^{2d} \leq p^n$, where d is the smallest integer not less than M/m.

Key words: p-group, extension, irreducible induced character, faithful irreducible character.

1. Introduction

Let G be a finite group. We denote by $\mathrm{Irr}(G)$ the set of complex irreducible characters of G and by $\mathrm{FIrr}(G)$ ($\subset \mathrm{Irr}(G)$) the set of faithful irreducible characters of G.

Let p be a prime. For a non-negative integer n, we denote by B_n the cyclic group of order p^n. A finite group G is called an M-group, if every $\chi \in \mathrm{Irr}(G)$ is induced from a linear character of a subgroup of G.

It is well-known that every p-group is an M-group. Hence, when G is a p-group, for any $\chi \in \mathrm{Irr}(G)$, there exists a subgroup H of G and a linear character ϕ of H such that $\phi^G = \chi$. If we set $N = \mathrm{Ker}\,\phi$, then $N \lhd H$ and ϕ is a faithful irreducible character of $H/N \cong B_n$, for some non-negative integer n. In this paper, we will consider the case when $N = 1$, that is, ϕ is a faithful linear character of $H \cong B_n$.

We consider the following:

Problem 1 *Let p be an odd prime, and ϕ be a faithful irreducible character of B_n. Determine the p-group G such that $B_n \subset G$ and the induced character ϕ^G is also irreducible.*

Since all the faithful irreducible characters of B_n are algebraically conjugate to each other, the irreducibility of ϕ^G ($\phi \in \mathrm{FIrr}(B_n)$) is independent

---

2000 Mathematics Subject Classification : 20C15.

of the choice of ϕ, and depends only on n.

On the other hand, when $p = 2$, Iida and Yamada ([4]) proved the following interesting result:

Let $\mathbf{Q}$ denote the rational field. Let G be a 2-group and χ a complex irreducible character of G. Then there exist subgroups $H \rhd N$ in G and a complex irreducible character ϕ of H such that $\chi = \phi^G$, $\mathbf{Q}(\chi) = \mathbf{Q}(\phi)$, $N = \mathrm{Ker}\,\phi$ and

$$H/N \cong Q_n \ (n \geq 2), \text{ or } D_n \ (n \geq 2), \text{ or } SD_n \ (n \geq 3), \text{ or } B_n \ (n \geq 0).$$

Here, Q_n, D_n and SD_n denote the generalized quaternion group, the dihedral group of order 2^{n+1} $(n \geq 2)$ and the semidihedral group of order 2^{n+1} $(n \geq 3)$, respectively, and $\mathbf{Q}(\chi) = \mathbf{Q}(\chi(g), g \in G)$.

Further, they considered the following:

Problem 2 *Let ϕ be a faithful irreducible character of H, where $H = Q_n$ or D_n or SD_n. Determine the 2-group G such that $H \subset G$ and the induced character ϕ^G is also irreducible.*

Iida and Yamada ([3]) solved this problem in the case when $[G : H] = 2$ or 4 and we have solved Problem 2 completely ([6]). In the paper, we showed that

$$G = N_G(H) \quad \text{or} \quad N_G(N_G(H)),$$

for all $H = Q_n$ or D_n or SD_n, if G satisfies the conditions of Problem 2. Here, as usual, $N_G(H)$ and $N_G(N_G(H))$ are the normalizers of H and $N_G(H)$ in G, respectively. This means that, if we define subgroups of G by

$$M_1 = N_G(H), \quad \text{and} \quad M_{i+1} = N_G(M_i), \quad \text{for } i \geq 1,$$

then

$$H \subseteq M_1 \subseteq M_2 = M_3 = M_4 = \cdots = G,$$

for all $H = Q_n$ or D_n or SD_n.

In this paper, we consider Problem 1. We also define subgroups of G by

$$N_1 = N_G(B_n), \quad \text{and} \quad N_{i+1} = N_G(N_i), \quad \text{for } i \geq 1.$$

Concerning Problem 1, N_1 has been determined by Iida ([2]), and $N_2 = N_G(N_G(B_n))$ has also been determined under the hypothesis $[N_1 : B_n]^4 \leq p^n$ ([8]). For other results, see also [5] and [7].

The purpose of this article is to determine N_d, $d = 1, 2, \dots$ under the hypothesis $[N_1 : B_n]^{2d} \leq p^n$.

Remark 1 When $p = 2$, there are many possible 2-groups which satisfy the condition of Problem 1 (e.g. Q_n, D_n and SD_n), and it is difficult to determine them completely.

Remark 2 In this paper, we will say that "G is the extension group of N," when G contains N as a subgroup.

Throughout this paper, $\mathbf{Z}$ and $\mathbf{N}$ denote the set of rational integers and the natural numbers, respectively.

2. Statements of the results

For the rest of this paper, we assume that p is an odd prime.

First, we introduce the sequence of "extension groups":

(0) $G(n, m, 0) = \langle a \rangle = B_n$ with

$$a^{p^n} = 1.$$

(i) $G(n, m, 1) = \langle a, b_1 \rangle$ with

$$a^{p^n} = b_1^{p^m} = 1, \quad b_1 a b_1^{-1} = a^{1+p^{n-m}}, \quad (1 \leq m \leq n-1).$$

(ii) $G(n, m, 2) = \langle a,\ b_1,\ b_2 \rangle$ with

$$a^{p^n} = b_1^{p^m} = 1, \quad b_1 a b_1^{-1} = a^{1+p^{n-m}}, \quad b_2 a b_2^{-1} = a^{1+p^{n-2m}} b_1,$$
$$b_2^{p^m} = b_1, \quad b_2 b_1 b_2^{-1} = b_1 \quad (2m \leq n-1).$$

....

(d) $G(n, m, d) = \langle a, b_1, b_2, \dots b_{d-1}, b_d \rangle$ with

$$a^{p^n} = b_1^{p^m} = 1, \quad b_1 a b_1^{-1} = a^{1+p^{n-m}}, \quad b_i a b_i^{-1} = a^{1+p^{n-im}} b_{i-1},$$
$$b_i^{p^m} = b_{i-1}, \quad b_i b_{i-1} b_i^{-1} = b_{i-1}, \quad 2 \leq i \leq d, \quad (dm \leq n-1).$$

$(d-1,\,+t)$ $G(n,m,d-1,\,+t) = \langle a, b_1, b_2, \dots b_{d-1}, b\rangle$ with

$$a^{p^n} = b_1^{p^m} = 1, \quad b_1 a b_1^{-1} = a^{1+p^{n-m}}, \quad b_i a b_i^{-1} = a^{1+p^{n-im}} b_{i-1},$$
$$b_i^{p^m} = b_{i-1}, \quad b_i b_{i-1} b_i^{-1} = b_{i-1}, \quad 2 \le i \le d-1,$$
$$bab^{-1} = a^{1+p^{n-(d-1)m-t}} b_{d-1}^{p^{m-t}}, \quad bb_{d-1}b^{-1} = b_{d-1}, \quad b^{p^t} = b_{d-1},$$
$$(1 \le t \le m-1,\ (d-1)m+t \le n-1).$$

By using Proposition 1 below ,we can show that $G(n,m,d)$ (respectively $G(n,m,d-1,\,+t)$) is an extension group of $G(n,m,d-1)$ for $d \ge 1$, when $2dm \le n$:

Proposition 1 *Let N be a finite group such that $G \triangleright N$ and $G/N = \langle uN\rangle$ is a cyclic group of order m. Then $u^m = c \in N$. If we put $\sigma(x) = uxu^{-1}$, $x \in N$, then $\sigma \in \mathrm{Aut}(N)$ and* (i) *$\sigma^m(x) = cxc^{-1}$, $(x \in N)$* (ii) *$\sigma(c) = c$.*

Conversely, if $\sigma \in \mathrm{Aut}(N)$ and $c \in N$ satisfy (i) *and* (ii)*, then there exists one and only one extension group G of N such that $G \triangleright N$ and $G/N = \langle uN\rangle$ is a cyclic group of order m and $\sigma(x) = uxu^{-1}$ $(x \in N)$ and $u^m = c$.*

Proof. For instance, see Zassenhaus ([9, III, Section 7]). □

The structure of N_1 and N_2 have been determined as follows:

(1) $N_1 = N_G(B_n) \cong G(n,m,1)$ for some $m \in \mathbf{N}$, $1 \le m \le n-1$ ([2]).
(2) $N_2 = N_G(N_G(B_n)) \cong G(n,m,2)$ for some $m \in \mathbf{N}$, when $4m \le n$ and $2m \le M$, where $[N_1 : B_n] = p^m$, and $[G : B_n] = p^M$ ([8]).

To state the theorem, we define the map $[\ ]_0 : \mathbf{Q} \longrightarrow \mathbf{Z}$, by the following: $[x]_0 = x$ if $x \in \mathbf{Z}$, and $[x]_0 = n+1$ if $n < x < n+1$, for some $n \in \mathbf{Z}$.

Our main theorem is the following:

Theorem *Let p be an odd prime, and G be a p-group which contains $B_n = \langle a\rangle$. Set $[N_1 : B_n] = p^m$, $[G : B_n] = p^M$ and $d = [M/m]_0$.*

Suppose that $\phi^G \in \mathrm{Irr}(G)$ for any $\phi \in \mathrm{FIrr}(B_n)$. Further, suppose that $2md \le n$. Then, $G = N_d$, and the following holds:

(1) *$G \cong G(n,m,d)$ if $M = md$.*
(2) *$G \cong G(n,m,d-1,+t)$ if $M < md$, where $t = M-(d-1)m$.*

To show the theorem, we prove Therem A,

Theorem A *Let p be an odd prime, and G be a p-group which contains $B_n = \langle a \rangle$. Suppose that $\phi^G \in \mathrm{Irr}(G)$ for any $\phi \in \mathrm{FIrr}(B_n)$.*

Set $[N_1 : B_n] = p^m$ and $[G : B_n] = p^M$. Then , for any positive integer d satisfying, $2md \leq n$, and $md \leq M$, we have $N_d \cong G(n, m, d)$.

More precisely, we can show the following

Theorem B *Under the same assumption and the notation as in Theorem A, we can find the elements $b_i \in G$, $1 \leq i \leq d$, and the integer s_d, $(p, s_d) = 1$, such that $a_d = a^{s_d}$ and b_i generate N_i, that is, $N_i = \langle a_d, b_1, b_2, \ldots, b_i \rangle = \langle a_d, b_i \rangle$ $(= \langle a, b_i \rangle)$, $1 \leq i \leq d$, and the following relations hold*

$$a_d^{p^n} = b_1^{p^m} = 1, \quad b_1 a_d b_1^{-1} = a_d^{1+p^{n-m}}, \quad b_i a_d b_i^{-1} = a_d^{1+p^{n-im}} b_{i-1},$$

$$b_i^{p^m} = b_{i-1}, \quad b_i b_{i-1} b_i^{-1} = b_{i-1}, \quad (2 \leq i \leq d).$$

Remark 3 Conversely, in Corollary 1, we will see that the groups $G(n, m, d)$ satisfy the condition (EX, B), which is defined in Section 3 of this paper. Hence these groups satisfy the conditions of Problem 1.

3. Some preleminary results

First, we state some results concerning the criterion for the irreducibilities of induced characters.

We denote by $\zeta = \zeta_{p^n}$ a primitive p^nth root of unity. It is known that, for $B_n = \langle a \rangle$, there are p^n irreducible characters ϕ_ν $(1 \leq \nu \leq p^n)$ of B_n:

$$\phi_\nu(a^i) = \zeta^{\nu i}, \quad (1 \leq i \leq p^n).$$

The irreducible character ϕ_ν is faithful if and only if $(\nu, p) = 1$.

It is well-known that

$$\mathrm{Aut}\langle a \rangle \cong \left(\mathbf{Z}/p^n\mathbf{Z}\right)^* \cong C_* \times B_{n-1}$$

where $(\mathbf{Z}/p^n\mathbf{Z})^*$ is the unit group of the factor ring $\mathbf{Z}/p^n\mathbf{Z}$ and C_* is the cyclic group of order $p-1$. Further, B_{n-1} is generated by the element $1+p$ in $\mathbf{Z}/p^n\mathbf{Z}$.

First, we state the following result of Shoda (cf. [1, p. 329]):

Proposition 2 *Let G be a group and H be a subgroup of G. Let ϕ be a linear character of H. Then the induced character ϕ^G of G is irreducible if and only if, for each $x \in G - H = \{g \in G \mid g \notin H\}$, there exists $h \in xHx^{-1} \cap H$ such that $\phi(h) \neq \phi(x^{-1}hx)$. (Note that, when ϕ is faithful, the condition $\phi(h) \neq \phi(x^{-1}hx)$ holds if and only if $h \neq x^{-1}hx$.)*

Using this result, we have the following:

Proposition 3 *Let $\langle a \rangle = B_n \subset G$, and ϕ be a faithful irreducible character of B_n. Then the following conditions are equivalent:*

(1) *ϕ^G is irreducible,*
(2) *For each $g \in G - B_n$, there exists $h \in \langle a \rangle \cap g\langle a \rangle g^{-1}$ such that $g^{-1}hg \neq h$.*

Definition 1 When the condition (2) of Proposition 3 holds, we say that G satisfies (EX, B).

Let H be a group. We denote by $|H|$ the order of H. For a normal subgroup N of H, and any $g,\ h \in H$, we write

$$g \equiv h \pmod N$$

when $g^{-1}h \in N$. For an element $g \in H$ we denote by $|g|$ the order of g.

For the rest of this section, we will show some equalities of the elements in $G(n, m, d)$.

In $G(n, m, 1)$, the following holds

Lemma 1 ([8, Lemma 1]) *Suppose that $n \geq 2m$, then the following equalities hold for any $i, j \in \mathbf{Z}$ and $l \in \mathbf{N}$.*

(i) $ab_1^{p^s} \equiv b_1^{p^s} a \pmod{\langle a^{p^{n-m+s}} \rangle}$, $(0 \leq s \leq m-1)$.
(ii) $b_1 a^{p^m} b_1^{-1} = a^{p^m}$.
(iii) $b_1^j a^i b_1^{-j} = a^{i(1+jp^{n-m})}$.
(iv) $(a^i b_1^j)^l = a^{il+ijp^{n-m}(l(l-1)/2)} b_1^{lj}$.
(v) $(a^i b_1^{jp^s})^{p^{m-s}} = a^{ip^{m-s}}$, $(0 \leq s \leq m-1)$.

For $d \geq 2$, we can see the following

Lemma 2 *Suppose that $2dm \leq n$, then the following assertions hold for any $i, j, s \in \mathbf{Z}$ and $d \in \mathbf{N}$, $0 \leq s \leq m-1$, $2 \leq d$:*

(i) $\langle a^{p^{n-tm+s}}\rangle \times \langle b_{t-1}^{p^s}\rangle$ $(1 \leq t \leq d)$ *and* $\langle a^{p^{n-(d+1)m+s}}\rangle \cdot \langle b_d^{p^s}\rangle$ *(the semidirect product of* $\langle a^{p^{n-(d+1)m+s}}\rangle$ *by* $\langle b_d^{p^s}\rangle$*) are the normal subgroups of* $G(n,m,d)$*, where* $b_0 = 1$.

(ii) $(a^i b_d^j)^l \equiv a^{il} b_d^{jl} \pmod{\langle a^{p^{n-dm}}\rangle \times \langle b_{d-1}\rangle}$*, for any* $l \in \mathbf{N}$.

(iii) $(a^i b_d^{jp^s})^{p^{km}} \equiv a^{ip^{km}} b_d^{jp^{km+s}} = a^{ip^{km}} b_{d-k}^{jp^s} \pmod{\langle a^{p^{n-(d-k)m+s}}\rangle \times \langle b_{d-k-1}^{p^s}\rangle}$*, for any* $k \in \mathbf{Z}$, $1 \leq k \leq d-1$*, where* $b_0 = 1$.

(iv) $(a^i b_d^{jp^s})^{p^{dm-s}} = a^{ip^{dm-s}}$,

(v) $b_d a^{p^{dm}} b_d^{-1} = a^{p^{dm}}$,

Proof. We show the lemma by the induction on d.

First, we show the case when $d = 2$.

(i) Note that

$$b_1 a^{p^{n-2m}} b_1^{-1} = a^{p^{n-2m}} \tag{1}$$

by Lemma 1 (ii), and by our assumption that $4m \leq n$. Further, since $b_2 a^{p^m} b_2^{-1} = (a^{1+p^{n-2m}} b_1)^{p^m} = a^{(1+p^{n-2m})p^m}$, by Lemma 1 (v), we have

$$b_2 a^{p^{n-lm}} b_2^{-1} \in \left\langle a^{p^{n-lm}} \right\rangle \quad (l = 1, 2, 3), \tag{2}$$

and

$$b_2 a^{p^{n-2m}} b_2^{-1} = a^{(1+p^{n-2m})p^{n-2m}} = a^{p^{n-2m}}, \tag{3}$$

because $4m \leq n$.

Using (1) and (3), we get,

$$b_2^l a b_2^{-l} = a^{1+lp^{n-2m}} b_1^l \tag{4}$$

for any $l \in \mathbf{N}$. So,

$$b_2^{jp^s} a^i b_2^{-jp^s} = \left(a^{1+jp^{n-2m+s}} b_1^{jp^s}\right)^i \equiv a^{i(1+jp^{n-2m+s})} b_1^{ijp^s} \pmod{\langle a^{p^{n-m+s}}\rangle}, \tag{5}$$

for any $s \in \mathbf{Z}$, $0 \le s \le m-1$, by Lemma 1 (i). Using (2) and (5), we can show (i).

(ii) follows from the fact that $b_2 a b_2^{-1} \equiv a \pmod{\langle a^{p^{n-2m}} \rangle \times \langle b_1 \rangle}$.

(iii) Using (5) repeatedly, we have

$$\begin{aligned}\left(a^i b_2^{jp^s}\right)^l &\equiv a^{il+ijp^{n-2m+s}\{1+2+\cdots+(l-1)\}} b_1^{ijp^s\{1+2+\cdots+(l-1)\}} b_2^{ljp^s} \\ &\equiv a^{il+ijp^{n-2m+s}(l(l-1)/2)} b_1^{ijp^s(l(l-1)/2)} b_2^{ljp^s} \pmod{\langle a^{p^{n-m+s}} \rangle},\end{aligned}$$

for any $l \in \mathbf{N}$, $s \in \mathbf{Z}$, $0 \le s \le m-1$.

In particular, we get

$$\left(a^i b_2^{jp^s}\right)^{p^m} \equiv a^{ip^m} b_2^{jp^{m+s}} = a^{ip^m} b_1^{jp^s} \pmod{\langle a^{p^{n-m+s}} \rangle}. \tag{6}$$

This completes the proof of (iii).

(iv) By (6), we can write

$$\left(a^i b_2^{jp^s}\right)^{p^m} = a^{ip^m + xp^{n-m+s}} b_1^{jp^s},$$

for some $x \in \mathbf{Z}$. So, we have $(a^i b_2^{jp^s})^{p^{2m-s}} = a^{ip^{2m-s}}$, by Lemma 1 (v).

(v) follows from (iv). This completes the proof of the case when $d = 2$.

Suppose that the assertions of the lemma hold for any e, $2 \le e \le d-1$.

(i) By the induction hypothesis, we have

$$b_d a^{p^l} b_d^{-1} = \left(a^{1+p^{n-dm}} b_{d-1}\right)^{p^l} = a^{(1+p^{n-dm})p^l},$$

for any l, $(d-1)m \le l$. Since $2dm \le n$, by our hypothesis, we have

$$b_d a^{p^{n-tm+s}} b_d^{-1} \in \left\langle a^{p^{n-tm+s}} \right\rangle, \tag{7}$$

for any $t \in \mathbf{N}$, $1 \le t \le d+1$, and

$$b_d a^{p^{n-dm}} b_d^{-1} = a^{(1+p^{n-dm})p^{n-dm}} = a^{p^{n-dm}}.$$

By the same calculations as in (4), we get

$$b_d^l a b_d^{-l} = a^{1+lp^{n-dm}} b_{d-1}^l.$$

for any $l \in \mathbf{N}$.
In particular, we kave

$$b_d^{jp^s} a b_d^{-jp^s} = a^{1+jp^{n-dm+s}} b_{d-1}^{jp^s}.$$

Since

$$b_{d-1}^{jp^s} a b_{d-1}^{-jp^s} = a^{1+jp^{n-(d-1)m+s}} b_{d-2}^{jp^s} \equiv a \pmod{\langle a^{p^{n-(d-1)m+s}}\rangle \times \langle b_{d-2}^{p^s}\rangle},$$

for $s, j \in \mathbf{Z}$, $0 \leq s \leq m-1$, by the induction hypothesis, we have

$$b_d^{jp^s} a^i b_d^{-jp^s} = \left(a^{1+jp^{n-dm+s}} b_{d-1}^{jp^s}\right)^i \equiv a^{i(1+jp^{n-dm+s})} b_{d-1}^{ijp^s} \pmod{\langle a^{p^{n-(d-1)m+s}}\rangle \times \langle b_{d-2}^{p^s}\rangle}. \quad (8)$$

Therefore, we can write

$$b_d^{jp^s} a^i b_d^{-jp^s} = a^{i(1+jp^{n-dm+s})+xp^{n-(d-1)m+s}} b_{d-1}^{ijp^s} b_{d-2}^{yp^s},$$

for some $x, y \in \mathbf{Z}$, and so, we have

$$a^{-i} b_d^{jp^s} a^i \in \left\langle a^{p^{n-(d+1)m+s}}\right\rangle \cdot \left\langle b_d^{p^s}\right\rangle. \quad (9)$$

By using (7) and (9), we can see that $\langle a^{p^{n-(d+1)m+s}}\rangle \cdot \langle b_d^{p^s}\rangle$ is the normal subgroup of $G(n, m, d)$. For $t \leq d$, (i) can be shown by the induction hypothesis and (7).

(ii) follows from the fact that $b_d a b_d^{-1} \equiv a \pmod{\langle a^{p^{n-dm}}\rangle \times \langle b_{d-1}\rangle}$.

(iii) Using the equality (8) repeatedly, we have

$$\left(a^i b_d^{jp^s}\right)^l \equiv a^{il+ijp^{n-dm+s}(l(l-1)/2)} b_{d-1}^{ijp^s(l(l-1)/2)} b_d^{ljp^s} \pmod{\langle a^{p^{n-(d-1)m+s}}\rangle \times \langle b_{d-2}^{p^s}\rangle},$$

for any $l \in \mathbf{N}$.
In particular, we have

$$\left(a^i b_d^{jp^s}\right)^{p^m} \equiv a^{ip^m} b_d^{jp^{m+s}} = a^{ip^m} b_{d-1}^{jp^s} \pmod{\langle a^{p^{n-(d-1)m+s}}\rangle \times \langle b_{d-2}^{p^s}\rangle}.$$

So, we can write

$$\begin{aligned}\left(a^i b_d^{jp^s}\right)^{p^m} &= a^{ip^m + xp^{n-(d-1)m+s}} b_{d-1}^{jp^s} b_{d-2}^{yp^s} \\ &= a^{ip^m + xp^{n-(d-1)m+s}} b_{d-1}^{jp^s + yp^{m+s}},\end{aligned}$$

for some $x, y \in \mathbf{Z}$.

Then, by the induction hypothesis, we have

$$\begin{aligned}\left(a^i b_d^{jp^s}\right)^{p^{km}} &= \left(a^{ip^m + xp^{n-(d-1)m+s}} b_{d-1}^{jp^s + yp^{m+s}}\right)^{p^{(k-1)m}} \\ &\equiv a^{ip^{km} + xp^{n-(d-k)m+s}} b_{d-k}^{jp^s + yp^{m+s}} \\ &\equiv a^{ip^{km}} b_{d-k}^{jp^s} \qquad \pmod{\langle a^{p^{n-(d-k)m+s}}\rangle \times \langle b_{d-k-1}^{p^s}\rangle},\end{aligned}$$

for $k \in \mathbf{Z}$, $2 \le k \le d-1$. This completes the proof of (iii).

(iv) In particular, we have

$$\left(a^i b_d^{jp^s}\right)^{p^{(d-1)m}} \equiv a^{ip^{(d-1)m}} b_1^{jp^s} \pmod{\langle a^{p^{n-m+s}}\rangle}.$$

So, we can write

$$\left(a^i b_d^{jp^s}\right)^{p^{(d-1)m}} = a^{ip^{(d-1)m} + xp^{n-m+s}} b_1^{jp^s},$$

for some $x \in \mathbf{Z}$. Therefore we have

$$\left(a^i b_d^{jp^s}\right)^{p^{dm-s}} = a^{ip^{dm-s}},$$

by Lemma 1 (v).

(v) follows from (iv). □

Corollary 1 *Suppose that $2dm \le n$, then $G(n,m,d)$ satisfies (EX, B).*

Proof. Let $g \in G(n,m,d)$. Write $g = a^i b_k^{jp^s}$, $1 \le k \le d$, $0 \le s \le m-1$, $(j,p) = 1$.

Then

$$
\begin{aligned}
gag^{-1} &= \left(a^i b_k^{jp^s}\right) a \left(a^i b_k^{jp^s}\right)^{-1} = a^i \left(a^{1+jp^{n-km+s}} b_{k-1}^{jp^s}\right) a^{-i} \\
&\equiv a^{1+jp^{n-km+s}} b_{k-1}^{jp^s} \qquad \pmod{\langle a^{p^{n-(k-1)m+s}} \rangle \times \langle b_{k-2}^{p^s} \rangle}.
\end{aligned}
$$

So, we can write

$$
\begin{aligned}
gag^{-1} &= a^{1+jp^{n-km+s}+x_0 p^{n-(k-1)m+s}} b_{k-1}^{jp^s} b_{k-2}^{y_0 p^s} \\
&= a^{1+p^{n-km+s}(j+x_0 p^m)} b_{k-1}^{p^s(j+y_0 p^m)}
\end{aligned}
$$

for some x_0, $y_0 \in \mathbf{Z}$. If we set $x_1 = j + x_0 p^m$, and $y_1 = j + y_0 p^m$, then

$$
gag^{-1} = a^{1+x_1 p^{n-km+s}} b_{k-1}^{y_1 p^s},
$$

and $(x_1, p) = (y_1, p) = 1$. So, $ga^{p^l} g^{-1} = (a^{1+x_1 p^{n-km+s}} b_{k-1}^{y_1 p^s})^{p^l} \in \langle a \rangle$ if and only if $l \geq (k-1)m - s$, by Lemma 2 (iii), (iv). Therefore we have

$$
g\langle a \rangle g^{-1} \cap \langle a \rangle = \left\langle a^{p^{(k-1)m-s}} \right\rangle.
$$

Since

$$
\begin{aligned}
ga^{p^{(k-1)m-s}} g^{-1} &= a^{(1+x_1 p^{n-km+s}) p^{(k-1)m-s}} \\
&= a^{p^{(k-1)m-s} + x_1 p^{n-m}} \neq a^{p^{(k-1)m-s}},
\end{aligned}
$$

the proof of Corollary 1 is completed. □

4. Proof of Theorem B

We show Theorem B by the induction on d. For $d = 1$, we can show the assertion by the direct calculations, and for $d = 2$, we have already shown it in [8].

Suppose that the assertion hold for any e, $(1 \leq e \leq d-1)$.

We use the same notations as in Theorem A, that is, s_{d-1} is the integer and b_i $(1 \leq i \leq d-1)$ are the elements in G such that $a_{d-1} = a^{s_{d-1}}$ and $b_1, \ldots, b_{d-1}$ generate N_{d-1}, $N_{d-1} = \langle a_{d-1}, b_1, b_2, \ldots, b_{d-1} \rangle = \langle a_d, b_{d-1} \rangle$ $(= \langle a, b_{d-1} \rangle)$, and the following relations hold

$$a_{d-1}^{p^n} = 1, \quad b_i a_{d-1} b_i^{-1} = a_{d-1}^{1+p^{n-im}} b_{i-1},$$
$$b_i^{p^m} = b_{i-1}, \quad b_i b_{i-1} b_i^{-1} = b_{i-1}, \quad (1 \le i \le d-1).$$

Let $f : N_d \longrightarrow N_d/N_{d-1}$ be the natural epimorphism of groups. For $g \in N_d$, we write $\mathrm{o}(g)$ for the order of $f(g)$ in N_d/N_{d-1}.

Define $p^{t_0} = \max\{\mathrm{o}(g) \mid g \in N_d\}$, and take an element $g_0 \in N_d$ such that $\mathrm{o}(g_0) = p^{t_0}$. Hereafter we fix the element g_0.

Without loss of generality, we may assume that $a_{d-1} = a^{s_{d-1}} = a$.

We can show the following:

Claim I

(i) *For any $g \in N_d$, there exist integers r_i, $1 \le i \le d-1$, such that the following equalities hold*:

$$(a^{r_i} g) b_i (a^{r_i} g)^{-1} = b_i, \quad 1 \le i \le d-1 \tag{I}$$

Further, we can write

$$(a^{r_{d-1}} g) a (a^{r_{d-1}} g)^{-1} = a^{1+k_d p^{n-(d-1)m-t}} b_{d-1}^{l_d p^{m-t}}, \tag{II}$$

where k_d, l_d are the integers such that $(k_d, p) = (l_d, p) = 1$ and $\mathrm{o}(g) = p^t$.

(ii) $t_0 \le m$.

(iii) *N_d is generated by a, b_{d-1} and g_0, that is, $N_d = \langle a, b_{d-1}, g_0 \rangle$.*

Proof. (i) (I). We show (i) (I) by the induction on i. When $i = 1$, the proof is essentially the same as that of Claim I of [8], so we omit it.

Suppose that there exists an integer r_{i-1} such that

$$(a^{r_{i-1}} g) b_{i-1} (a^{r_{i-1}} g)^{-1} = b_{i-1}.$$

Without loss of generality, we can assume that $g b_{i-1} g^{-1} = b_{i-1}$.

Write $gag^{-1} = a^{x_1} b_{d-1}^{y_1}$, then $(x_1, p) = 1$, because $(a^{x_1} b_{d-1}^{y_1})^{p^{(d-1)m}} = a^{x_1 p^{(d-1)m}}$ and the order of gag^{-1} is p^n.

Since the order of $g b_i g^{-1}$ is p^{im}, by Lemma 2 (iii), (iv), we can write $g b_i g^{-1} = a^k b_i^l$, for some $k, l \in \mathbf{Z}$.

Then

$$b_{i-1} = gb_{i-1}g^{-1} = gb_i^{p^m}g^{-1} = (a^k b_i^l)^{p^m} \equiv a^{kp^m} b_{i-1}^l$$
$$(\text{mod } \langle a^{p^{n-(i-1)m}} \rangle \times \langle b_{i-2} \rangle),$$

by Lemma 2 (iii).

Therefore we have

$$l \equiv 1 \pmod{p^m} \quad \text{and} \quad kp^m \equiv 0 \pmod{p^{n-(i-1)m}}.$$

So, we can write $l = 1 + l_1 p^m$, $k = k_1 p^{n-im}$ and

$$gb_ig^{-1} = a^{k_1 p^{n-im}} b_i^{1+l_1 p^m} = a^{k_1 p^{n-im}} b_{i-1}^{l_1} b_i,$$

for some k_1, $l_1 \in \mathbf{Z}$.

Since

$$b_i a^{p^{n-im}} b_i^{-1} = \left(a^{1+p^{n-im}} b_{i-1}\right)^{p^{n-im}} = a^{p^{n-im}},$$

by our assumption $n \geq 2dm$ and Lemma 2 (iv), we have

$$\begin{aligned} b_{i-1} = gb_{i-1}g^{-1} = gb_i^{p^m} g^{-1} &= \left(a^{k_1 p^{n-im}} b_i^{1+l_1 p^m}\right)^{p^m} \\ = a^{k_1 p^{n-(i-1)m}} b_{i-1}^{1+l_1 p^m} &= a^{k_1 p^{n-(i-1)m}} b_{i-2}^{l_1} b_{i-1}. \end{aligned}$$

Therefore we get

$$k_1 \equiv 0 \pmod{p^{(i-1)m}}, \quad l_1 \equiv 0 \pmod{p^{(i-2)m}}.$$

So, we can write $l_1 = l_2 p^{(i-2)m}$, $k_1 = k_2 p^{(i-1)m}$ and

$$gb_ig^{-1} = a^{k_2 p^{n-m}} b_1^{l_2} b_i,$$

for some k_2, $l_2 \in \mathbf{Z}$.

Taking the conjugate of both sides of the equality, $b_i a b_i^{-1} = a^{1+p^{n-im}} b_{i-1}$ by g, we get

$$\left(a^{k_2 p^{n-m}} b_1^{l_2} b_i\right)\left(a^{x_1} b_{d-1}^{y_1}\right)\left(a^{k_2 p^{n-m}} b_1^{l_2} b_i\right)^{-1} = \left(a^{x_1} b_{d-1}^{y_1}\right)^{1+p^{n-im}} b_{i-1}.$$

Since $(a^{x_1}b_{d-1}^{y_1})^{1+p^{n-im}}b_{i-1} = a^{x_1p^{n-im}}(a^{x_1}b_{d-1}^{y_1})b_{i-1} = a^{x_1(1+p^{n-im})}b_{d-1}^{y_1} \cdot b_{i-1}$, and

$$\begin{aligned}&\left(a^{k_2p^{n-m}}b_1^{l_2}b_i\right)\left(a^{x_1}b_{d-1}^{y_1}\right)\left(a^{k_2p^{n-m}}b_1^{l_2}b_i\right)^{-1}\\ &= b_1^{l_2}\left\{(a^{1+p^{n-im}}b_{i-1})^{x_1}b_{d-1}^{y_1}\right\}b_1^{-l_2}\\ &= \left\{a^{(1+l_2p^{n-m})(1+p^{n-im})}b_{i-1}\right\}^{x_1}b_{d-1}^{y_1},\end{aligned}$$

we have

$$\left\{a^{(1+l_2p^{n-m})(1+p^{n-im})}b_{i-1}\right\}^{x_1} = a^{x_1(1+p^{n-im})}b_{i-1}. \tag{10}$$

So, we get

$$\begin{aligned}&\left\{a^{(1+l_2p^{n-m})(1+p^{n-im})}b_{i-1}\right\}^{x_1-1}\\ &\quad = a^{x_1(1+p^{n-im})}b_{i-1}\left\{a^{(1+l_2p^{n-m})(1+p^{n-im})}b_{i-1}\right\}^{-1} \in \langle a\rangle.\end{aligned}$$

But $(a^{(1+l_2p^{n-m})(1+p^{n-im})}b_{i-1})^{p^l} \in \langle a\rangle$ if and only if $l \geq (i-1)m$, by Lemma 2 (iii), (iv).

Therefore we must have $x_1 - 1 \equiv 0 \pmod{p^{(i-1)m}}$.

Write $x_1 = 1 + x_2p^{(i-1)m}$ for some $x_2 \in \mathbf{Z}$. Then we have

$$\begin{aligned}&\left\{a^{(1+l_2p^{n-m})(1+p^{n-im})}b_{i-1}\right\}^{x_1}\\ &= \left\{a^{(1+l_2p^{n-m})(1+p^{n-im})}b_{i-1}\right\}^{x_2p^{(i-1)m}}\left\{a^{(1+l_2p^{n-m})(1+p^{n-im})}b_{i-1}\right\}\\ &= a^{x_2p^{(i-1)m}(1+l_2p^{n-m})(1+p^{n-im})}\left\{a^{(1+l_2p^{n-m})(1+p^{n-im})}b_{i-1}\right\}\\ &= a^{x_1(1+l_2p^{n-m})(1+p^{n-im})}b_{i-1}.\end{aligned} \tag{11}$$

By (10) and (11), we have $l_2 \equiv 0 \pmod{p^m}$, and so

$$gb_ig^{-1} = a^{k_2p^{n-m}}b_1^{l_2}b_i = a^{k_2p^{n-m}}b_i.$$

Note that

$$b_ia^{p^{(i-1)m}}b_i^{-1} = \left(a^{1+p^{n-im}}b_{i-1}\right)^{p^{(i-1)m}} = a^{(1+p^{n-im})p^{(i-1)m}} = a^{p^{(i-1)m}+p^{n-m}}.$$

So, if we take $r_i = k_2 p^{(i-1)m}$, then

$$(a^{r_i}g)b_i(a^{r_i}g)^{-1} = a^{k_2 p^{(i-1)m}} g b_i g^{-1} a^{-k_2 p^{(i-1)m}} = b_i.$$

This completes the proof of (i) (I).

(ii) Let g be an arbitrary element in N_d, and write $\mathrm{o}(g) = p^t$. If we set $g_1 = a^{r_{d-1}}g$, then $g_1 b_{d-1} g_1^{-1} = b_{d-1}$ and $\mathrm{o}(g_1) = \mathrm{o}(g) = p^t$. To prove (ii), we show that $t \le m$.

Write $g_1 a g_1^{-1} = a^x b_{d-1}^y$, for some $x, y \in \mathbf{Z}$.

It is easy to see that

$$g_1\big(\langle a^{p^{n-(d-1)m}}\rangle \times \langle b_{d-2}\rangle\big)g_1^{-1} = \big\langle a^{p^{n-(d-1)m}}\big\rangle \times \langle b_{d-2}\rangle.$$

Since

$$b_{d-1} a b_{d-1}^{-1} \equiv a \pmod{\langle a^{p^{n-(d-1)m}}\rangle \times \langle b_{d-2}\rangle},$$

we have

$$g_1 a^j g_1^{-1} = \big(a^x b_{d-1}^y\big)^j \equiv a^{xj} b_{d-1}^{yj} \pmod{\langle a^{p^{n-(d-1)m}}\rangle \times \langle b_{d-2}\rangle},$$

for any $j \in \mathbf{N}$. Therefore we get

$$g_1^l a g_1^{-l} \equiv a^{x^l} b_{d-1}^{y(x^{l-1}+\cdots+x+1)} \pmod{\langle a^{p^{n-(d-1)m}}\rangle \times \langle b_{d-2}\rangle},$$

for any $l \in \mathbf{N}$.

In particular,

$$g_1^{p^t} a g_1^{-p^t} \equiv a^{x^{p^t}} b_{d-1}^{y(x^{p^t-1}+\cdots+x+1)} \pmod{\langle a^{p^{n-(d-1)m}}\rangle \times \langle b_{d-2}\rangle}. \tag{12}$$

Since $g_1^{p^t} \in N_{d-1}$, we must have

$$g_1^{p^t} a g_1^{-p^t} \equiv a \pmod{\langle a^{p^{n-(d-1)m}}\rangle \times \langle b_{d-2}\rangle}.$$

Therefore

$$x^{p^t} \equiv 1 \pmod{p^{n-(d-1)m}}, \tag{13}$$

and

$$y\big(x^{p^t-1}+\cdots+x+1\big)\equiv 0 \pmod{p^m}.$$

By (13), we can write $x=1+x_0p^{n-(d-1)m-t}$, for some $x_0\in\mathbf{Z}$.

So,

$$y\big(x^{p^t-1}+\cdots+x+1\big)=y\left(\frac{x^{p^t}-1}{x-1}\right)=yp^tv, \tag{14}$$

for some $v\in\mathbf{Z}$, $(p,v)=1$.

Suppose that $t\geq m+1$, then

$$y\big(x^{p^{t-1}-1}+\cdots+x+1\big)=yp^{t-1}v_1\equiv 0 \pmod{p^m}.$$

for some $v_1\in\mathbf{Z}$, $(p,v_1)=1$.

This means that $g_1^{p^{t-1}}ag_1^{-p^{t-1}}\in N_{d-2}$ and $g_1^{p^{t-1}}\in N_{d-1}$, which contradicts our hypothesis that $\mathrm{o}(g)=p^t$. Therefore we must have $t\leq m$, and the proof of (ii) is completed.

(i) (II) By (12) and (14), we can write $y=y_0p^{m-t}$ and

$$g_1ag_1^{-1}=a^{1+x_0p^{n-(d-1)m-t}}b_{d-1}^{y_0p^{m-t}}$$

for some $y_0\in\mathbf{Z}$.

Since

$$g_1a^{p^{n-(d-1)m-t}}g_1^{-1}=\big(a^{1+x_0p^{n-(d-1)m-t}}b_{d-1}^{y_0p^{m-t}}\big)^{p^{n-(d-1)m-t}}=a^{p^{n-(d-1)m-t}}$$

by Lemma 2 (iv) and by our assumption $n\geq 2dm$, we have

$$g_1^{p^{t-1}}ag_1^{-p^{t-1}}=a^{1+x_0p^{n-(d-1)m-1}}b_{d-1}^{y_0p^{m-1}}.$$

But $g_1^{p^{t-1}}\notin N_{d-1}$, we must have $(p,y_0)=1$.

Suppose that $(p,x_0)=p$, then we can write $x_0=x_3p$, for some $x_3\in \mathrm{Z}$, and

$$g_1^{p^{t-1}}ag_1^{-p^{t-1}}=a^{1+x_3p^{n-(d-1)m}}b_{d-1}^{y_0p^{m-1}}.$$

If we put $g_2 = b_{d-1}^{-x_3} g_1^{p^{t-1}}$, then $g_2 \notin N_{d-1}$.
Since $b_{d-1} a^{p^{n-(d-1)m}} b_{d-1}^{-1} = a^{p^{n-(d-1)m}}$, we have

$$\begin{aligned} g_2 a g_2^{-1} &= b_{d-1}^{-x_3} a^{1+x_3 p^{n-(d-1)m}} b_{d-1}^{y_0 p^{m-1}} b_{d-1}^{x_3} \\ &= \left(a^{1-x_3 p^{n-(d-1)m}} b_{d-2}^{-x_3}\right)\left(a^{x_3 p^{n-(d-1)m}}\right)\left(b_{d-1}^{y_0 p^{m-1}}\right) \\ &= a b_{d-2}^{-x_3} b_{d-1}^{y_0 p^{m-1}} = a b_{d-1}^{(y_0 - x_3 p) p^{m-1}}. \end{aligned}$$

By Lemma 2 (iii), (iv), we have

$$\left(g_2 a g_2^{-1}\right)^{p^l} = \left(a b_{d-1}^{(y_0 - x_3 p) p^{m-1}}\right)^{p^l} \in \langle a \rangle,$$

if and only if $l \geq (d-2)m + 1$.

Therefore we have

$$g_2 \langle a \rangle g_2^{-1} \cap \langle a \rangle = \left\langle a^{p^{(d-2)m+1}} \right\rangle.$$

Further,

$$g_2 a^{p^{(d-2)m+1}} g_2^{-1} = \left(a b_{d-1}^{(y_0 - x_3 p) p^{m-1}}\right)^{p^{(d-2)m+1}} = a^{p^{(d-2)m+1}},$$

by Lemma 2 (iv).

This contradicts our hypothesis that G satisfies (EX, B). So, we must have $(x_0, p) = 1$. If we set $k_d = x_0$ and $l_d = y_0$, we complete the proof of (i) (II).

(iii) Take an arbitrary element $u \in N_d$. Let $\mathrm{o}(u) = p^{t_1}$. Then, by (i), we may assume that

$$u a u^{-1} = a^{1+h_1 p^{n-(d-1)m-t_1}} b_{d-1}^{h_2 p^{m-t_1}},$$

and

$$u b_i u^{-1} = b_i, \qquad 1 \leq i \leq d-1,$$

where $(p, h_1) = (p, h_2) = 1$. Since $t_1 \leq t_0$, we can take an element $w \in \langle a, b_{d-1}, g_0^{p^{t_0 - t_1}} \rangle$ such that

$$w^{-1}aw = a^{1+l_1p^{n-(d-1)m-t_1}} b_{d-1}^{l_2p^{m-t_1}},$$

and

$$w^{-1}b_iw = b_i, \qquad 1 \le i \le d-1,$$

where $(p, l_1) = (p, l_2) = 1$. Let c be the integer satisfying $l_2c \equiv -h_2 \pmod{p^{(d-2)m+t_1}}$, and set $w_1 = w^c$. Then $(p, c) = 1$,

$$w_1^{-1}aw_1 = a^{1+l_1cp^{n-(d-1)m-t_1}} b_{d-1}^{l_2cp^{m-t_1}} = a^{1+l_1cp^{n-(d-1)m-t_1}} b_{d-1}^{-h_2p^{m-t_1}},$$

and

$$w_1^{-1}b_{d-1}w_1 = b_{d-1}.$$

Therefore we have

$$\begin{aligned} w_1^{-1}(uau^{-1})w_1 &= w_1^{-1}\big(a^{1+h_1p^{n-(d-1)m-t_1}} b_{d-1}^{h_2p^{m-t_1}}\big)w_1 \\ &= a^{1+(l_1c+h_1)p^{n-(d-1)m-t_1}} \in \langle a \rangle. \end{aligned}$$

This means that $w_1^{-1}u \in N_1$, so we must have $u \in \langle a, b_{d-1}, g_0 \rangle$. This completes the proof of (iii).

Next, we show the following:

Claim II *Let a, b_i, $(1 \le i \le d-1)$ and g_0 be the elements as in Claim I. Then there exist integers z_1, z_2, and the element $w \in N_{d-1}$ such that $(z_1, p) = (z_2, p) = 1$, and $a_1 = a^{z_1}$, b_i, $(1 \le i \le d-1)$ and $b = wg_0^{z_2}$ satisfy the following relations*:

$$a_1^{p^n} = 1, \quad b_ia_1b_i^{-1} = a_1^{1+p^{n-im}} b_{i-1}, \quad b_ib_{i-1}b_i^{-1} = b_{i-1},$$
$$b_i^{p^m} = b_{i-1} \ (1 \le i \le d-1)$$
$$ba_1b^{-1} = a_1^{1+p^{n-(d-1)m-t_0}} b_{d-1}^{p^{m-t_0}}, \quad bb_{d-1}b^{-1} = b_{d-1}, \quad b^{p^{t_0}} = b_{d-1},$$

where, $b_0 = 1$.

Proof. In this proof, we use the notations t and g instead of t_0 and g_0, respectively. First we consider the element $g^{p^t} (\in N_{d-1})$.

By Claim I, we may assume that

$$gag^{-1} = a^{1+k_d p^{n-(d-1)m-t}} b_{d-1}^{l_d p^{m-t}}, \tag{15}$$

and

$$gb_i g^{-1} = b_i, \qquad 1 \leq i \leq d-1,$$

for some k_d, $l_d \in \mathbf{Z}$, $(k_d, p) = (l_d, p) = 1$.

By Lemma 2 (iii), (iv), we see that

$$ga^{p^l} g^{-1} \notin \langle a \rangle,$$

for any $l \in \mathbf{N}$, $1 \leq l \leq (d-2)m + t - 1$, and

$$ga^{p^l} g^{-1} = a^{(1+k_d p^{n-(d-1)m-t})p^l},$$

for any $l \in \mathbf{N}$, $(d-2)m + t \leq l$. So,

$$ga^{p^l} g^{-1} = a^{p^l},$$

if and only if $(d-1)m + t \leq l$.

Since $g^{p^t} \in N_{d-1}$, we can write $g^{p^t} = a^{r_1} b_{d-1}^s$, for some r_1, $s \in \mathbf{Z}$. Since $gb_{d-1}g^{-1} = b_{d-1}$, we have $ga^{r_1}g^{-1} = a^{r_1}$. So we can write

$$g^{p^t} = a^{r_2 p^{(d-1)m+t}} b_{d-1}^s,$$

for some $r_2 \in \mathbf{Z}$. Therefore we have

$$\begin{aligned} g^{p^t} a g^{-p^t} &= \left(a^{r_2 p^{(d-1)m+t}} b_{d-1}^s\right) a \left(a^{r_2 p^{(d-1)m+t}} b_{d-1}^s\right)^{-1} \\ &= a^{1+sp^{n-(d-1)m}} b_{d-2}^s. \end{aligned} \tag{16}$$

On the other hand, by (15), we have

$$g^{p^t} a g^{-p^t} = a^{1+k_d p^{n-(d-1)m}} b_{d-2}^{l_d}. \tag{17}$$

Comparing (16) and (17), we get

$$k_d \equiv s \pmod{p^{(d-1)m}} \quad \text{and} \quad l_d \equiv s \pmod{p^{(d-2)m}}.$$

So, we can write

$$k_d = s + f_1 p^{(d-1)m} \quad \text{and} \quad l_d = s + f_2 p^{(d-2)m}, \tag{18}$$

for some $f_1,\ f_2 \in \mathbf{Z}$.

Thus we can write

$$g^{p^t} = a^{r_2 p^{(d-1)m+t}} b_{d-1}^{k_d}.$$

By (18), we have

$$l_d = k_d - f_1 p^{(d-1)m} + f_2 p^{(d-2)m},$$

and

$$\begin{aligned} gag^{-1} &= a^{1+k_d p^{n-(d-1)m-t}} b_{d-1}^{l_d p^{m-t}} \\ &= a^{1+k_d p^{n-(d-1)m-t}} b_{d-1}^{\{k_d - f_1 p^{(d-1)m} + f_2 p^{(d-2)m}\} p^{m-t}} \\ &= a^{1+k_d p^{n-(d-1)m-t}} b_{d-1}^{k_d p^{m-t}} b_1^{f_2 p^{m-t}}. \end{aligned}$$

So, we have

$$g a^{p^{(d-1)m}} g^{-1} = a^{p^{(d-1)m}\{1+k_d p^{n-(d-1)m-t}\}},$$

and

$$\begin{aligned} g^l a^{rp^{(d-1)m}} g^{-l} &= a^{rp^{(d-1)m}\{1+k_d p^{n-(d-1)m-t}\}^l} \\ &= a^{rp^{(d-1)m}\{1+lk_d p^{n-(d-1)m-t}\}}, \end{aligned} \tag{19}$$

for any $r \in \mathbf{Z}$ and $l \in \mathbf{N}$. By using (19), we get

$$\left(a^{rp^{(d-1)m}} g\right)^l = a^{lrp^{(d-1)m}} a^{rk_d p^{n-t}(l(l-1)/2)} g^l, \tag{20}$$

for any $r \in \mathbf{Z}$ and $l \in \mathbf{N}$. In particular, we have

$$\left(a^{rp^{(d-1)m}}g\right)^{p^t} = a^{rp^{(d-1)m+t}}g^{p^t} = a^{rp^{(d-1)m+t}}a^{r_2p^{(d-1)m+t}}b_{d-1}^{k_d}.$$

So, if we put $g_2 = a^{-r_2p^{(d-1)m}}g$, we get

$$g_2^{p^t} = b_{d-1}^{k_d}, \quad g_2ag_2^{-1} = a^{1+k_dp^{n-(d-1)m-t}}b_{d-1}^{k_dp^{m-t}}b_1^{f_2p^{m-t}},$$
$$g_2b_ig_2^{-1} = b_i, \quad 1 \le i \le d-1.$$

Let v_1 be the integer such that $k_dv_1 \equiv 1 \pmod{p^{(d-1)m+t}}$, and set $g_3 = g_2^{v_1}$.
Then the following equalities hold:

$$g_3^{p^t} = g_2^{v_1p^t} = b_{d-1}^{k_dv_1} = b_{d-1}, \quad g_3b_ig_3^{-1} = b_i, \quad 1 \le i \le d-1,$$
$$\begin{aligned} g_3ag_3^{-1} &= a^{1+k_dv_1p^{n-(d-1)m-t}}b_{d-1}^{k_dv_1p^{m-t}}b_1^{f_2v_1p^{m-t}} \\ &= a^{1+p^{n-(d-1)m-t}}b_{d-1}^{p^{m-t}}b_1^{f_2v_1p^{m-t}}. \end{aligned}$$

Further, let $a_1 = a^{1-f_2v_1p^{(d-2)m}}$. Then $a_1^{p^{n-t}} = a^{p^{n-t}}$, and

$$\begin{aligned} g_3a_1g_3^{-1} &= \left(g_3a^{-f_2v_1p^{(d-2)m}}g_3^{-1}\right)\left(g_3ag_3^{-1}\right) \\ &= \left(a^{1+p^{n-(d-1)m-t}}b_{d-1}^{p^{m-t}}b_1^{f_2v_1p^{m-t}}\right)^{-f_2v_1p^{(d-2)m}} \\ &\quad\cdot\left(a^{1+p^{n-(d-1)m-t}}b_{d-1}^{p^{m-t}}b_1^{f_2v_1p^{m-t}}\right) \\ &\equiv \left\{a^{(1+p^{n-(d-1)m-t})(-f_2v_1p^{(d-2)m})}b_1^{-f_2v_1p^{m-t}}\right\} \\ &\quad\cdot\left(a^{1+p^{n-(d-1)m-t}}b_{d-1}^{p^{m-t}}b_1^{f_2v_1p^{m-t}}\right) \pmod{\langle a^{p^{n-t}}\rangle} \\ &\equiv a^{(1+p^{n-(d-1)m-t})(1-f_2v_1p^{(d-2)m})}b_{d-1}^{p^{m-t}} \pmod{\langle a^{p^{n-t}}\rangle} \\ &\equiv a_1^{1+p^{n-(d-1)m-t}}b_{d-1}^{p^{m-t}} \pmod{\langle a^{p^{n-t}}\rangle} \\ &\equiv a_1^{1+p^{n-(d-1)m-t}}b_{d-1}^{p^{m-t}} \pmod{\langle a_1^{p^{n-t}}\rangle}. \end{aligned}$$

So, we can write

$$g_3 a_1 g_3^{-1} = a_1^{1+p^{n-(d-1)m-t}+yp^{n-t}} b_{d-1}^{p^{m-t}},$$

for some $y \in \mathbf{Z}$. It is easy to see that

$$a_1^{p^n} = 1 \quad \text{and} \quad b_i a_1 b_i^{-1} = a_1^{1+p^{n-im}} b_{i-1}, \quad 1 \leq i \leq d-1.$$

Finally, if we set $b = b_1^{-yp^{m-t}} g_3$, then we have

$$ba_1 b^{-1} = b_1^{-yp^{m-t}} \big(a_1^{1+p^{n-(d-1)m-t}+yp^{n-t}} b_{d-1}^{p^{m-t}}\big) b_1^{yp^{m-t}} = a_1^{1+p^{n-(d-1)m-t}} b_{d-1}^{p^{m-t}},$$

and

$$b^{p^t} = \big(b_1^{-yp^{m-t}} g_3\big)^{p^t} = g_3^{p^t} = b_{d-1}, \quad bb_i b^{-1} = b_i \quad 1 \leq i \leq d-1.$$

Thus the proof of Claim II is completed. □

We can easily see that

$$\langle a_1 \rangle = \langle a \rangle \quad \text{and} \quad \langle a_1, b_1, \ldots, b_{d-1}, b \rangle = \langle a, b_1, \ldots, b_{d-1}, g_0 \rangle = N_d.$$

We will complete the proof of the Theorem B, by showing the following:

Claim III $t_0 = m$ *when* $[G : N_{d-1}] \geq p^m$.

Proof. We use the same notations as in Claim II, that is, $N_d = \langle a_1, b_1, \ldots, b_{d-1}, b \rangle$, and $|N_d/N_{d-1}| = p^{t_0}$. For simplicity, we write t and a instead of t_0 and a_1. Suppose that $t \leq m-1$. Take an element $u \in N_G(N_d) - N_d$ such that $u^p \in N_d$. By the same way as in the proof of Claim I, we can assume that $ubu^{-1} = b$, $ub_i u^{-1} = b_i$, $1 \leq i \leq d-1$.

Further we can see that

$$u\big(\langle a^{p^{n-(d-1)m-t}} \rangle \times \langle b_{d-1}^{p^{m-t}} \rangle\big) u^{-1} = \big\langle a^{p^{n-(d-1)m-t}} \big\rangle \times \big\langle b_{d-1}^{p^{m-t}} \big\rangle,$$

by using Lemma 2 (iii), (iv).

Let $uau^{-1} = a^x b^y$, $x, y \in \mathbf{Z}$. Then we have

$$u^p a u^{-p} \equiv a^{x^p} b^{y(x^{p-1}+\cdots+x+1)} \equiv a^{x^p} b^{y((x^p-1)/(x-1))} \pmod{\langle a^{p^{n-(d-1)m-t}} \rangle \times \langle b_{d-1}^{p^{m-t}} \rangle}.$$

Since $u^p \in N_d$, we must have

$$x^p \equiv 1 \pmod{p^{n-(d-1)m-t}},$$

and

$$y\left(\frac{x^p - 1}{x - 1}\right) \equiv 0 \pmod{p^m}.$$

So, we can write $x = 1 + x_1 p^{n-(d-1)m-t-1}$ for some $x_1 \in \mathbf{Z}$. In this case, we can write $\frac{x^p-1}{x-1} = pz$ for some $z \in \mathbf{Z}$, $(z, p) = 1$. Therefore we must have $y \equiv 0 \pmod{p^{m-1}}$. But this fact means $uau^{-1} = a^x b^y \in N_{d-1}$. On the other hand, $ub_i u^{-1} = b_i$ $1 \leq i \leq d-1$, so we have $u \in N_d$, which contradicts our hypothesis that $u \notin N_d$. This completes the proof of Claim III. □

5. Proof of Theorem

If $M = md$, then, by Theorem A, we have $N_d \cong G(n, m, d)$. But $[G : B_n] = [G(n, m, d) : B_n]$. So, $G = N_d \cong G(n, m, d)$.

When $M < md$, we have $N_{d-1} \cong G(n, m, d-1)$, by Theorem A. By Claim I (iii) and Claim II, we can see that $N_d \cong G(n, m, d-1, +t)$, for some $t, 1 \leq t \leq m-1$. But, by the same argument as in Claim III, we must have $G = N_d$. Comparing $[G : B_n]$ and $[N_d : B_n]$, we have $t = M - (d-1)m$. □

Acknowledgments The author would like to express his gratitude to the referee for his careful reading and pertinent suggestions.

References

[1] Curtis C. and Reiner I., Representation theory of finite groups and associative algebras (Interscience, New York, 1962).

[2] Iida Y., *Normal extensions of a cyclic p-group.* Comm. Algebra **30**(4) (2002), 1801–1805.

[3] Iida Y. and Yamada T., *Extensions and induced characters of quaternion, dihedral and semidihedral groups.* SUT J. Math. **27** (1991), 237–262.

[4] Iida Y. and Yamada T., *Types of faithful metacyclic 2-groups.* SUT J. Math. **28** (1992), 23–46.

[5] Sekiguchi K., *Irreducibilities of the induced characters of cyclic p-groups.* Math. J. of Okayama Univ. **41** (1999), 27–36.

[6] Sekiguchi K., *Extensions and the irreducibilities of induced characters of some 2-groups*. Hokkaido Math. J. **31** (2002), 79–96.
[7] Sekiguchi K., *Extensions and the irreducibilities of the induced characters of cyclic p-groups*. Hiroshima Math. J. **32** (2002), 165–178.
[8] Sekiguchi K., *Extensions and the induced characters of cyclic p-groups*. Comm. Algebra **35** (2007), 3611–3623.
[9] Zassenhaus H., The theory of groups (Chelsea, New York, 1949).

Department of Mathematics and Science
School of Science and Engineering
Kokushikan University
4-28-1 Setagaya Setagaya-Ku,
Tokyo 154-8515 , Japan
E-mail: sekiguch@kokushikan.ac.jp