PACIFIC JOURNAL OF MATHEMATICS
Vol. 124, No. 2, 1986

MODULAR INVARIANT THEORY AND COHOMOLOGY ALGEBRAS OF EXTRA-SPECIAL p-GROUPS

PHAM ANH MINH

Let W_n be the group of all translations on the vector space $\mathbf{Z}_p^{n-1}$. Every element of W_n is considered as a linear transformation on $\mathbf{Z}_p^n$, i.e. W_n is identified to a subgroup of $\mathrm{GL}(n,\mathbf{Z}_p)$. We have then a natural action of W_n on $E(x_1,\ldots,x_n;1)\otimes P(y_1,\ldots,y_n;2)$. The purpose of this paper is to determine a full system of invariants of W_n in this algebra. Using this result, we determine the image $\operatorname{Im}\operatorname{Res}(A,G)$, for every maximal elementary abelian p-subgroup A of an extra-special p-group G.

Introduction. Let G be a finite group and $\mathbf{Z}_p$ be the prime field of p elements. Let us write $H^*(G)=H^*(G,\mathbf{Z}_p)$ (the mod p cohomology algebra of G).

If $p=2$, the cohomology algebras of all extra-special p-groups were determined by Quillen [7]. We are interested in the case $p>2$. So from now on, we shall assume this condition through the paper. For the extra-special p-groups of order p^3, their integral cohomology rings have been computed by Lewis in [3], and their mod p cohomology algebras are determined recently in Phạm Anh Minh-Huỳnh Mùi [4] and Huỳnh Mùi [6]. For an arbitrary extra-special p-group, Tezuka and Yagita had computed $H^*(G)/\sqrt{0}$ in [9]. As observed in [6], the ideal $\sqrt{0}$ of the nilpotents in this algebra is quite complicated, so it seems difficult to determine their nilpotent elements.

Let A be a maximal elementary abelian p-subgroup of an extra-special p-group G. The inclusion map $A\hookrightarrow G$ induces the restriction homomorphism $\operatorname{Res}(A,G)\colon\ H^*(G)\to H^*(A)^{W_G(A)}$, where $W_G(A)=N_G(A)/C_G(A)$, the quotient of the normalizer by the centralizer of A in G. The purpose of this paper is to determine the image $\operatorname{Im}\operatorname{Res}(A,G)$ for every A. We shall see that the nilideal of $\operatorname{Im}\operatorname{Res}(A,G)$ is complicated, so our results will be needed in the study of the ideal $\sqrt{0}$ of $H^*(G)$.

This paper contains 3 sections. In §1, we consider maximal elementary abelian p-subgroups of an extra-special p-group following Quillen [7] and Tezuka-Yagita [9]. By means of the modular invariant theory developed by Huỳnh Mùi [5], we determine in §2 a full system for the invariants of $W_G(A)$ in $H^*(A)$. Using the results in §2, we determine $\operatorname{Im}\operatorname{Res}(A, G)$ in §3. The main results of this paper are Theorem 2.4 and Theorem 3.1.

I would like to acknowledge my sincere gratitude to Prof. Huỳnh Mùi for his generous and inspiring guidance. I am also deeply grateful to Prof. Ngô Thê Phiệt for many valuable discussions.

1. Extra-special p-groups and maximal elementary abelian p-subgroups. Let G be a p-group. As usual, let $[G,G]$, $Z(G)$ $\Phi(G) = G^p \cdot [G,G]$ denote the commutator subgroup, the center and the Frattini group of G respectively. G is called an extra-special p-group if it satisfies the following condition

(1.1) $$[G,G] = \Phi(G) = Z(G) \cong \mathbf{Z}_p.$$

Equivalently, G is an extra-special p-group if we have the group extension

(1.2) $$0 \to \mathbf{Z}_p \xrightarrow{i} G \xrightarrow{\pi} V \to 0$$

where V is a vector space of finite dimension over $\mathbf{Z}_p$ and i is an isomorphism from $\mathbf{Z}_p$ onto the center of G. (For details or extra-special p-groups see D. Gorenstein, *Finite Groups*, Harper & Row, New York, 1968, especially §5.5.)

As well known, the dimension of $V \cong G/Z(G)$ is even. If $\dim V = 2$, G is isomorphic to one of the following groups

$$E = \langle a, b \mid a^p = b^p = [a,b]^p = [a,[a,b]] = [b,[a,b]] = 1\rangle,$$
$$M = \langle a, b \mid a^{p^2} = b^p = 1,\ b^{-1} \cdot ab = a^{1+p}\rangle.$$

Generally, if $\dim V = 2n - 2 (n \geq 2)$, then G is isomorphic to one of the following central products

(1.3) $$\begin{aligned} E_{n-1} &= E \cdot \cdots \cdot E \qquad (n-1 \text{ times}) \\ M_{n-1} &= E_{n-2} \cdot M. \end{aligned}$$

Let B: $G/Z(G) \times G/Z(G) \to [G,G]$ be the map defined by

$$B(u,v) = [u', v'] \quad \text{for } u, v \in G/Z(G)$$

where u', v' mean representatives of u and v respectively. One can easily see that B is well-defined. Identifying $G/Z(G) = V = \mathbf{Z}_p^{2n-2}$ and $[G,G] = \mathbf{Z}_p$, B becomes the alternating form $V \times V \to \mathbf{Z}_p$ defined by

(1.4) $$B(u,v) = \sum_{i=1}^{n-1} u_{2i-1} \cdot v_{2i} - u_{2i} \cdot v_{2i-1}$$

for

$$u = (u_1, \ldots, u_{2n-2}), \quad v = (v_1, \ldots, v_{2n-2}) \in V.$$

A subspace W of V is said to be B-isotropic if $B(u, v) = 0$ for all $u, v \in W$.

In Quillen [7; §4] and Tezuka-Yagita [9; 1.7 and 3.4], we have

LEMMA 1.5. *There is a* 1-1 *correspondence between maximal abelian p-subgroups A of G and maximal B-isotropic subspaces W of V. The dimension of any maximal B-isotropic subspaces W of V is just* $n - 1$.

From this lemma, we have

LEMMA 1.6. *Any maximal elementary abelian p-subgroup A of G is of rank n, i.e.* $A \cong \mathbf{Z}_p^n$.

Proof. It suffices to prove that A is also a maximal abelian subgroup of G, and the result is implied from (1.5). Assume that A is not a maximal abelian subgroup of G, then $A \not\subseteq A'$, where A' is a maximal abelian subgroup but not elementary of G. Let $a \in A'$ with $\text{ord}(a) = p^2$. Let $\Omega_1(G)$, $\mho_1(G)$ denote the subgroups of G defined by $\Omega_1(G) = \{x \in G/\text{ord}(x) \le p\}$ and $\mho_1(G) = \{y^p | y \in G\}$. Since $|\mho_1(G)| = p$, we have $|\Omega_1(G)| = p^{2n-2}$ and $\Omega_1(G)$ is not an extra-special p-group. Hence $Z(\Omega_1(G)) \not\supseteq Z(G)$. Let b be an element of $Z(\Omega_1(G)) \setminus Z(g)$, we have $[b, a] \neq 1$, hence $b \notin A$ and $\langle A, b \rangle$ is then an elementary abelian p-subgroup of G which contains strictly A, a contradiction. The lemma is proved.

PROPOSITION 1.7. *Let A be a maximal elementary abelian p-subgroup of G. Then there exist the elements* $a_1, \ldots, a_n$, $b_1, \ldots, b_{n-1}$ *of G such that*

(a) $A = \langle a_1, \ldots, a_n \rangle$ *and* $a_n = c$ *is a generator of* $Z(G)$

(b) $W_G(A) = \langle \underline{b}_1, \ldots, \underline{b}_{n-1} \rangle$ *where* $\underline{b}_i = b_i A$, $1 \le i \le n - 1$

(c) $a_i^{b_j} = a_i$ *if* $i \neq j$, $a_i \cdot a_n$ *if* $i = j$ *for* $1 \le i, j \le n - 1$.

Proof. It suffices to prove that: (*) there exist the elements $a_1, \ldots, a_n$, $b_1, \ldots, b_{n-1}$ of G satisfying the conditions:

(a′) $A = \langle a_1, \ldots, a_n \rangle$, where $a_n = c$,

(b′) for each i, $1 \le i \le n - 1$, $\langle a_i, b_i \rangle$ is an extra-special p-subgroup of G of order p^3,

(c′) $[b_i, a_j] = 1$ if $i \neq j$, and the proposition can be obtained by noting that $W_G(A) = G/A$ and $a_i \in C_G(\langle a_j, b_j \rangle)$ if $i \neq j$.

First, let $c_1, \ldots, c_{n-1}$, $c_n = c$, be a basis of A. Clearly, for $1 \le i \le n - 1$, $c_i \in G \setminus Z(G)$, so there exists an element d_i of G such that $[c_i, d_i] \neq 1$. Hence $E_i = \langle c_i, d_i \rangle \supset Z(G) = \Phi(G)$ and $\langle c_i \Phi(G), d_i \Phi(G) \rangle$ is a subgroup of $G/\Phi(G)$ of order less than p^2. Then $|E_i| \le p^3$. Since E_i is not abelian, we have $|E_i| = p^3$. Thus E_i is an extra-special p-group of order p^3. By [**8**, 4.17 Chap. 4], we have $G = E_i \cdot C_G(E_i)$.

Since $G = E_1 \cdot C_G(E_1)$, each c_i $(i \neq n)$ has the form

$$c_i = c_1^{r_i} \cdot d_1^{s_i} \cdot a_i^{(1)}$$

with $0 \le r_i$, $s_i \le p - 1$ and $a_i^{(1)} \in C_G(E_1)$. Since $[c_i, c_1] = 1$, s_i is then equal zero. Set $a_1^{(1)} = c_1$, $b_1^{(1)} = d_1$. We have $A = \langle a_1^{(1)}, \ldots, a_{n-1}^{(1)}, c \rangle$ and there exist the elements $b_2^{(1)}, \ldots, b_{n-1}^{(1)}$ of G such that $\langle a_i^{(1)}, b_i^{(1)} \rangle$ is an extra special p-group of order p^3, and $[b_1^{(1)}, a_i^{(1)}] = 1$ for $i \neq 1$.

Assume that there exists the elements $a_1^{(k)}, \ldots, a_{n-1}^{(k)}, b_1^{(k)}, \ldots, b_{n-1}^{(k)}$ $(1 \le k < n - 1)$ of G such that

(i) $A = \langle a_1^{(k)}, \ldots, a_{n-1}^{(k)}, c \rangle$,

(ii) $\langle a_i^{(k)}, b_i^{(k)} \rangle$ is an extra-special p-group of order p^3,

(iii) $[b_j^{(k)}, a_i^{(k)}] = 1$ for $i \neq j$ and $j \le k$.

For $i \neq k + 1$, $a_i^{(k)}$ has the form $a_i^{(k)} = a_{k+1}^{(k)m_i} \cdot a_i^{(k+1)}$ with $0 \le m_i < p$ and $a_i^{(k+1)} \in C_G(\langle a_{k+1}^{(k)}, b_{k+1}^{(k)} \rangle)$. Set $a_{k+1}^{(k+1)} = a_{k+1}^{(k)}$, $b_j^{(k+1)} = b_j^{(k)}$ for $j \le k + 1$. Let $b_i^{(k+1)}$ $(k - 2 \le i \le n - 1)$ be the elements of G such that $\langle a_i^{(k+1)}, b_i^{(k+1)} \rangle$ is an extra-special p-group of order p^3. We have then

(i) $A = \langle a_1^{(k+1)}, \ldots, a_{n-1}^{(k+1)}, c \rangle$,

(ii) $\langle a_i^{(k+1)}, b_i^{(k+1)} \rangle$ is an extra-special p-group of order p^3, for $i \neq n$,

(iii) $[b_j^{(k+1)}, a_i^{(k+1)}] = 1$ for $j \neq i$ and $j \le k + 1$. Finally, put $a_i = a_i^{(n-1)}$, $b_i = b_i^{(n-1)}$, $1 \le i \le n - 1$. We obtain (*). The proposition is then proved.

(1.8) From now on, suppose that we are given a maximal elementary abelian p-subgroup A of G. Let us identify A with the vector space $\mathbf{Z}_p^n$ by the correspondence

$$a_i \mapsto e_i = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix} < i,$$

where $a_1, \ldots, a_n$ satisfy (1.7a). Then $W_G(a)$ is the group

$$W_G(A) = \left\{ \begin{bmatrix} 1 & & & \\ & 1 & & 0 \\ 0 & & \ddots & \\ * & * & \cdots \; * & 1 \end{bmatrix} \in \mathrm{GL}(n, \mathbf{Z}_p) \right\}.$$

Let $x_1,\dots,x_n \in H^1(A) = \mathrm{Hom}(A,\mathbf{Z}_p)$ be the duals of $c_1,\dots,c_n$. Let $y_i = \beta x_i$, where β denotes the Bockstein operator. As it is well known, we have

$$H^*(A) = E(x_1,\dots,x_n;\ 1) \otimes P(y_1,\dots,y_n;\ 2)$$

where $E(x_1,\dots,x_n;\ 1)$ (resp. $P(y_1,\dots,y_n;\ 2)$) denotes the exterior (resp. polynomial) algebra of n generators $x_1,\dots,x_n$ (resp. $y_1,\dots,y_n$) of order 1 (resp. 2) over $\mathbf{Z}_p$.

As in Huỳnh Mùi [3, Chap. 2, §1], we have

$$(1.9)\qquad (H^*(A))^{W_G(A)} = (E(x_1,\dots,x_n;\ 1) \otimes P(y_1,\dots,y_n;\ 2))^{W_n}$$

where W_n is the subgroup of $\mathrm{GL}(n,\mathbf{Z}_p)$ given by

$$W_n = \left\{ \begin{bmatrix} 1 & & & & * \\ & 1 & & 0 & * \\ & & \ddots & & \vdots \\ & 0 & & 1 & * \\ & & & & 1 \end{bmatrix} \in \mathrm{GL}(n,\mathbf{Z}_p) \right\}$$

and $(E(x_1,\dots,x_n;\ 1) \otimes P(y_1,\dots,y_n;\ 2))^{W_n}$ denotes the invariants of W_n in $E(x_1,\dots,x_n;\ 1) \otimes P(y_1,\dots,y_n;\ 2)$.

2. A full system for the invariants of W_n in $E(x_1,\dots,x_n;\ 1) \otimes P(y_1,\dots,y_n;\ 2)$. We shall determine a full system for the invariants $(E(x_1,\dots,x_n;\ 1) \otimes P(y_1,\dots,y_n;\ 2))^{W_n}$ by use of Huỳnh Mùi's invariants in [5].

Let $1 \le k \le n$ be an integer. Following Huỳnh Mùi [5], we let

$$(2.1)\qquad V_k = \prod_{\lambda_i \in \mathbf{Z}_p} (\lambda_1 y_1 + \lambda_2 y_2 + \cdots + \lambda_{k-1} y_{k-1} + y_k).$$

Let $(s_1,\dots,s_k)$ be a sequence of integers with $0 \le s_1 < \cdots < s_k < n$. For $1 \le i \le k$, define

$$(2.2)\qquad M_{n,s_i} = \begin{vmatrix} x_1 & x_2 & \cdots & x_n \\ y_1 & y_2 & \cdots & y_n \\ \cdots & \cdots & \cdots & \cdots \\ y_1^{p^{s_i-1}} & y_2^{p^{s_i-1}} & \cdots & y_n^{p^{s_i-1}} \\ y_1^{p^{s_i+1}} & y_2^{p^{s_i+1}} & \cdots & y_n^{p^{s_i+1}} \\ \cdots & \cdots & \cdots & \cdots \\ y_1^{p^{n-1}} & y_2^{p^{n-1}} & \cdots & y_n^{p^{n-1}} \end{vmatrix}.$$

As in [5, Prop. I4.5], the product $M_{n,s_1} \cdot M_{n,s_2} \cdots M_{n,s_k}$ has the factor L_n^{k-1}. Here

$$L_n = V_1 \cdot V_2 \cdot \cdots \cdot V_n$$

is Dickson's invariant (see e.g. [5]). Hence we have Huỳmh Mùi's invariants

$$(2.3)\qquad M_{n,s_1,s_2,\ldots,s_k} = M_{n,s_1,\ldots,s_k}(x_1,\ldots,x_n,y_1,\ldots,y_n) = (-1)^{k(k-1)/2} M_{n,s_1}\cdots M_{n,s_k}/L_n^{k-1}.$$

We have the following theorem

THEOREM 2.4. *There is a direct sum decomposition of modules*

$$\begin{aligned}(E(x_1,\ldots,x_n;1)\otimes P(y_1,\ldots,y_n;2))^{W_n} &= E(x_1,\ldots,x_{n-1})\otimes P(y_1,\ldots,y_{n-1},V_n)\\ &\oplus \sum_{k=1}^{n}\oplus \sum_{0\le s_1<\cdots<s_k=n-1} \oplus M_{n,s_1,\ldots,s_k}P(y_1,\ldots,y_{n-1},V_n).\end{aligned}$$

Therefore the invariants $x_1,\ldots,x_{n-1},y_1,\ldots,y_{n-1},V_n\quad M_{n,s_1,\ldots,s_k}, 1\le k\le n, 0\le s_1<\cdots s_k=n-1$ *form a full system for the invariants of* W_n *in*

$$E(x_1,x_2,\ldots,x_n;1)\otimes P(y_1,\ldots,y_n;2).$$

Let $1\le k\le n$ and let $W_{n,k}$ denote the subgroup of $\mathrm{GL}(n,\mathbf{Z}_p)$ consisting of all elements

$$\left[\begin{array}{cc} \boxed{\begin{matrix} 1 & & 0\\ & \ddots & \\ 0 & & 1\end{matrix}} & \\ 0 & \begin{matrix} 1 & & \\ & \ddots & \\ & & 1\end{matrix}\end{array}\right]\begin{matrix}\}\,k \text{ lines}\\ \\ \\ \end{matrix} \in \mathrm{GL}(n,\mathbf{Z}_p).$$

Particularly, $W_{n,n-1}=W_n$ and $W_{n,1}=\mathrm{GL}_{n,p}$.

As a corollary of Theorem 2.4, we have

COROLLARY 2.6.

$$\begin{aligned}(E(x_1,\ldots,x_n;1)\otimes P(y_1,\ldots,y_n;2))W_{n,k} &= E(x_1,\ldots,x_k)\otimes P(y_1,\ldots,y_k,V_{k+1},\ldots,V_n)\\ &\oplus \sum_{l=1}^{n}\oplus \sum_{s=k+1}^{n}\oplus \sum_{0\le s_1<\cdots s_l=s-1}\\ &\qquad \oplus M_{s,s_1,\ldots,s_l}P(y_1,\ldots,y_k,V_{k+1},\ldots,V_n).\end{aligned}$$

Note that $W_{n,1} = \mathrm{GL}_{n,p}$, *so Theorem* 2.4 *provides a proof of* [5,Th. I5.6].

Proof. For $k + 1 \leq i \leq n$, let

$$W_{n,k}^{(i)} = \left\{ \begin{bmatrix} \boxed{\begin{matrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{matrix}} & 0 \quad * \quad 0 \\ & \ddots \quad * \\ 0 & \quad 1 \\ & \qquad \ddots \\ & \qquad\qquad 1 \end{bmatrix} \in W_{n,k} \right\}.$$

$\hat{i}$th-column

Since

$$\left(E(x_1,\dots,x_n;1) \otimes P(y_1,\dots,y_n;2)\right)^{W_{n,k}}$$
$$= \bigcap_{i=k+1}^{n} \left(E(x_1,\dots,x_n;1) \otimes P(y_1,\dots,y_n,2)\right)^{W_{n,k}^{(i)}}$$

the assertion follows from Theorem 2.4.

We shall prove Theorem 2.4 by induction on n. If $n = 2$, $W_2 = \mathrm{GL}_{2,p}$ and the theorem follows from [5, Th. I5.6].

LEMMA 2.7. $P(y_1,\dots,y_n)^{W_n} = P(y_1, y_2,\dots, y_{n-1}, V_n)$.

Proof. Let $f \in P(y_1,\dots,y_n)$ be an invariant of W_n having the factor y_n, then f has the factor

$$\omega y_n = \omega_{1n} y_2 + \cdots + \omega_{n-1n} y_{n-1} + y_n \quad \text{for } \omega = (\omega_{ij}) \in W_n.$$

Consequently f contains $\prod_{\omega \in W_n} \omega y_n = V_n$ as a factor (refer to [5, I3.3]).

Assume that f' is another invariant of W_n. Let f_0 be the sum of all terms of f' free of y_n. Then f_0 is an invariant of W_n, hence so is $f' - f_0$. Since $f' - f_0$ has the factor y_n, it has also the factor V_n. We have $f' - f_0 = V_n^n \cdot f''$, where f'' is a polynomial not having y_n as factor. Repeating the above process on f'', we conclude that $y_1,\dots,y_{n-1}$, V_n generate the algebra $P(y_1,\dots,y_n)^{W_n}$.

Clearly $y_1,\dots,y_{n-1}$, V_n are algebraically independent. The lemma follows.

(2.8) For later use, we need some notations. Consider $V_n = V_n(y_1, \ldots, y_n)$, we set

$$V'_n = V_n(y_2, \ldots, y_n, y_1)$$
$$V''_{n-1} = V_{n-1}(y_2, \ldots, y_{n-1}, y_n).$$

Let $0 \leq s \leq n$ be an integer. Then we have inductively the Dickson invariants

$$Q_{n,0} = (V_1 \cdot \cdots \cdot V_n)^{p-1}$$
$$Q_{n,s} = Q_{n-1,s} \cdot V_n^{p-1} + Q_{n-1,s-1}^p, \qquad 0 < s \leq n$$

where $Q_{s,s} = 1$. By a similar way as in 2.8, we set

$$Q'_{n-1,s} = Q_{n-1,s}(y_2, \ldots, y_n)$$

and

$$M'_{n-1,s_1,\ldots,s_k} = M_{m-1,s_1,\ldots,s_k}(x_2, \ldots, x_n;\ y_2, \ldots, y_n).$$

Let $I = \{i_1, \ldots, i_k\}$ with $i_1 < \cdots < i_k$ be a subset of $\{1, \ldots, n\}$. We set

$$x_1 = x_{i_1} \cdot x_{i_2} \cdots x_{i_k}.$$

Further, we denote

$$W'_{n-1} = \left\{ \begin{bmatrix} 1 & & & & 0 \\ & 1 & & 0 & * \\ & & \ddots & & \vdots \\ & 0 & & 1 & * \\ & & & & 1 \end{bmatrix} \in \mathrm{GL}(n, \mathbf{Z}_p) \right\}.$$

LEMMA 2.9. *Let $1 \leq k \leq n$ and let f be an element of*

$$E(x_1, \ldots, x_n; 1) \otimes P(y_1, \ldots, y_n; 2)$$

having the form

$$f = \sum_I x_I f_I(y_1, \ldots, y_n)$$

where I runs over the subsets of order k in $\{1, \ldots, n\}$. If f is an invariant of W_n, then

(a) *$f_{\dot I}$ is an invariant of W_n, for all $\dot I$ such that $n \in \dot I$. Furthermore, if $k = 1$, then $f_{\{n\}}$ contains L_{n-1} as a factor.*

(b) *If $f_{\dot I} = 0$ for all $\dot I$ such that $n \in \dot I$, then f_I is an invariant of W_n, for all I.*

Proof. Let $\omega = (\omega_{ij})$ be an element of W_n, we have

$$\omega x_i = \begin{cases} x_i & 1 \le i < n, \\ \omega_{1n}x_1 + \cdots + \omega_{n-1n}x_{n-1} + x_n, & i = n. \end{cases}$$

Then f has the form

$$f = \sum_{I \neq \hat{I}} x_I(\omega f_I) + x_{\hat{I}}(\omega f_{\hat{I}}).$$

This implies that $\omega f_{\hat{I}} = f_{\hat{I}}$, hence $f_{\hat{I}}$ is an invariant of W_n.

For the case $k = 1$, let $1 \le m \le n-1$ be an integer and $\omega = 1 + \lambda_1\varepsilon_{1n} + \cdots + \lambda_{m-1}\varepsilon_{m-1n} + \varepsilon_m$ be an element of W_n, where $\lambda_i \in \mathbf{Z}_p$ and ε_{ij} denote the matrix with 1 in the (i, j)-position and 0 elsewhere. By comparing the coefficients of x_m, we have

$$\begin{aligned} &f_m(y_1, \dots, y_{n-1}, y_n + \lambda_1 y_1 + \cdots + \lambda_{m-1}y_{m-1} + y_m) \\ &\qquad + f_n(y_1, \dots, y_{n-1}, y_n + \lambda_1 y_1 + \cdots + \lambda_{m-1}y_{m-1} + y_m) \\ &\quad = f_m(y_1, \dots, y_{n-1}, y_n). \end{aligned}$$

Put $y_m = -(\lambda_1 y_1 + \cdots + \lambda_{m-1}y_{m-1})$, we have

$$f_n(y_1, \dots, y_{m-1}, -(\lambda_1 y_1 + \cdots + \lambda_{m-1}y_{m-1}), y_{m+1}, \dots, y_n) = 0$$

hence f_n contains $y_m + \lambda_1 y_1 + \cdots + \lambda_{m-1}y_{m-1}$ as a factor. Consequently f_n contains L_{n-1} as a factor. The lemma is proved.

LEMMA 2.10. *If* $0 \le s_1 < \cdots < s_k \le n-2$, *we have*

$$M_{n-1, s_1, \dots, s_k} \cdot V_n = M_{n, s_1, \dots, s_k} - \sum_{i=1}^{k} (-1)^{k+i} M_{n, s_1, \dots, \hat{s}_i, \dots, s_k, n-1} \cdot Q_{n-1, s_i}$$

and

$$M'_{n-1, s_1, \dots, s_k} \cdot V'_n = M_{n, s_1, \dots, s_k} - \sum_{i=1}^{k} (-1)^{k+i} M_{n, s_1, \dots, \hat{s}_i, \dots, s_k, n-1} \cdot Q'_{n-1, s_i}$$

up to a sign.

Proof. The first relation was proved in [5, Lemma I 4.12]. The second is a direct consequence of the first by permuting 1 and n.

LEMMA 2.11. *If* $0 \le s_1 < \cdots < s_k \le n-2$, *we have*

$$M'_{n-1, s_1, \dots, s_k} \cdot V'_{n-1} = \sum_{0 \le t_1 < \cdots < t_k = n-1} M_{n, t_1, \dots, t_k} \cdot F_{(t_1, \dots, t_k)+h}$$

where $F_{(t_1,\ldots,t_k)}$ *are elements of* $P(y_1,\ldots,y_n)$ *and* $h \in E(x_1,\ldots,x_{n-1}) \otimes P(y_1,\ldots,y_n)$.

Proof. Put

$$U = \prod_{\substack{\lambda_i \in \mathbf{Z}_p \\ \lambda_n \neq 0}} (\lambda_2 y_2 + \cdots + \lambda_{n-1} y_{n-1} + \lambda_n y_n + y_1)$$

then $V'_n = V'_{n-1} \cdot U$. By Lemma 2.10, we have

$$\begin{aligned} M'_{n-1,s_1,\ldots,s_k} \cdot V'_{n-1} \cdot U &= M_{n,s_1,\ldots,s_k} \\ &\quad - \sum_{i=1}^{k} (-1)^{k+i} M_{n,s_1,\ldots,\hat{s}_i,\ldots,s_k,n-1} \cdot Q'_{n-1,s_i} \\ &= M_{n,s_1,\ldots,s_k} \cdot V_n \\ &\quad + \sum_{i=1}^{k} (-1)^{k+i} M_{n,s_1,\ldots,\hat{s}_i,\ldots,s_k,n-1} \left(Q_{n-1,s_i} - Q'_{n-1,s_i}\right) \end{aligned}$$

up to a sign.

Since V_n contains U as a factor, it remains to prove that $Q_{n-1,s_i} - Q'_{n-1,s_i}$ has U as a factor. This is the fact by noting that

$$Q_{n-1,s_i}(\lambda_2 y_2 + \cdots + \lambda_n y_n, y_2, \ldots, y_{n-1}) = Q'_{n-1,s_i}(y_2, \ldots, y_n)$$

for any $\lambda_i \in \mathbf{Z}_p$, $\lambda_n \neq 0$. The lemma is proved.

LEMMA 2.12. *Let* $1 \leq k \leq n$ *and* f *be an element of*

$$E(x_1,\ldots,x_n;1) \otimes P(y_1,\ldots,y_n;2)$$

given by

$$f = \sum_{0 \leq s_1 < \cdots < s_k = n-1} M_{n,s_1,\ldots,s_k} f_{(s_1,\ldots,s_k)}(y_1,\ldots,y_k)$$

then f *contains* V_n *as a vector if and only if so does every* $f_{(s_1,\ldots,s_k)}$.

Proof. By definition of $M_{n,s_1,\ldots,s_k}$, we have

$$\begin{aligned} f = (-1)^{n-1} x_n &\sum_{0 \leq s_1 < \cdots < s_k = n-1} M_{n-1,s_1,\ldots,s_{k-1}} f_{s_1,\ldots,s_k} \\ &+ \sum_I x_I f_I(y_1,\ldots,y_n) \end{aligned}$$

where Σ_I denotes the summation over the subsets I of order k in $\{1,\ldots,n-1\}$. Put $y_n = \lambda_1 y_1 + \cdots + \lambda_{n-1}y_{n-1}$. For each I, $f_I(y_1,\ldots,y_{n-1},\lambda_1 y_1 + \cdots + \lambda_{n-1}y_{n-1})$ must be equal zero. Then f_I has V_n as a factor. Consequently

$$F = \sum_{0\le s_1<\cdots<s_k} M_{n-1,s_1,\ldots,s_{k-1}} f_{s_1,\ldots,s_k}$$

also contains V_n as a factor.

Let $0 \le s_1 < \cdots < s_k = n-1$ and $s_{k+1} < \cdots < s_{n-1}$ be its complement in $\{0,\ldots,n-2\}$, we have

$$F \cdot M_{n-1,s_{k+1},\ldots,s_{n-1}} = \pm x_1 \cdot x_2 \cdots x_{n-1} I_{n-1} f_{s_1,\ldots,s_k}$$

by (2.3). Since the left side is equal zero for $y_n = \lambda_1 y_1 + \cdots + \lambda_{n-1}y_{n-1}$, so is $f_{s_1,\ldots,s_k}$. Hence $f_{s_1,\ldots,s_k}$ contains V_n as a factor. The lemma is proved.

LEMMA 2.13. *Let* $1 \le k \le n$ *and*

$$f = \sum_{0\le s_1<\cdots<s_k=n-1} M_{n,s_1,\ldots,s_k} f_{s_1,\ldots,s_k}(y_1,\ldots,y_k) + g$$

be an element of $E(x_1,\ldots,x_n;1)\otimes P(y_1,\ldots,y_n;2)$, *where* g *is an element of* $E(x_1,\ldots,x_{n-1})\otimes P(y_1,\ldots,y_n)$. *If* $f=0$ *then* $g=0$ *and* $f_{s_1,\ldots,s_k}=0$ *for each* $0\le s_1 \cdots s_k = n-1$.

Proof. Let $g = \Sigma_I x_I g_I(y_1,\ldots,y_n)$, where I runs over the subsets of order k of $\{1,\ldots,n-1\}$. We have

$$f\cdot M_{n,n-1} = 0 = g \cdot M_{n,n-1}.$$

For each I, the coefficient of $x_I \cdot x_n$ in $g\cdot M_{n,n-1}$ is $(-1)^{n-1} g_I \cdot L_{n-1}$. Hence $g_I = 0$. Then $g=0$ and

$$f = \sum_{0\le s_1<\cdots<s_k=n-1} M_{n,s_1,\ldots,s_k} f_{s_1,\ldots,s_k} = 0.$$

For $0\le s_1 < \cdots < s_k = n-1$, let $s_{k+1} < \cdots < s_n$ be its complement in $\{0,\ldots,n-1\}$, we have

$$f\cdot M_{n,s_{k+1},\ldots,s_n} = \pm x_1\cdot x_2 \cdots x_n \cdot L_n \cdot f_{s_1,\ldots,s_k}$$

then $f_{s_I,\ldots,s_k}=0$. The lemma is proved.

Let k be an integer with $2\le k\le n$ and let f be an invariant of W_n having the form

$$f = \sum_I x_I f_I(y_1,\ldots,y_n)$$

where I runs over the subsets of order k in $\{1, \dots, n\}$. We write

(2.14) $$f = x_1\left(\sum{}' x_J f_I\right) + \sum{}'' x_I f_I$$

where Σ' (resp. Σ'') denotes the summation over the subsets of order $k-1$ (resp. k) in $\{2, \dots, n-1, n\}$, and in the first summation J is given by $I = J \cup \{1\}$ for each I containing 1. We set

$$G = \sum{}' x_J f_I$$

then G is an invariant of W'_{n-1}.

Now, we suppose that Theorem 2.4 is true for W_{n-1}. We have then

(2.15) $$G = \sum_{0 \le s_1 < \cdots < s_{k-1} = n-2} M'_{n-1, s_1, \dots, s_{k-1}} g_{s_1, \dots, s_{k-1}} + \sum_J x_J g_J$$

where $g_{s_1, \dots, s_{k-1}}$ and g_J are the invariants of W'_{n-1} in $P(y_1, \dots, y_n)$ and Σ_J denotes the summation over the subsets of order $k-1$ in $\{2, \dots, n-1\}$.

LEMMA 2.16. *All* $g_{s_1, \dots, s_{k-1}}$ *in* (2.15) *are invariants of* W_n.

Proof. Clearly all $g_{s_1, \dots, s_{k-1}}$ are invariants of W'_{n-1}. We need only prove that $g_{s_1, \dots, s_{k-1}} = \alpha_1 g_{s_1, \dots, s_{k-1}}$ with $\omega_1 = 1 + \varepsilon_{1n}$. We have

$$\begin{aligned} f &= x_1 G + \sum{}'' x_I f_I \\ &= \sum_{0 \le s_1 < \cdots < s_{k-1} = n-2} x_1 M'_{n-1, s_1, \dots, s_{k-1}} g_{s_1, \dots, s_{k-1}} \\ &\quad + \sum{}^{(1)} x_I h_I(y_1, \dots, y_n) + \sum{}^{(2)} x_I 1_I(y_1, \dots, y_n) \end{aligned}$$

where $\Sigma^{(1)}$ (resp. $\Sigma^{(2)}$) denotes the summation over the subsets of order k in $\{1, \dots, n-1\}$ (resp. $\{2, \dots, n-1, n\}$ such that $n \in I$). By Lemma 2.9, each 1_I with I in $\Sigma^{(2)}$ is an invariant of W_n. Hence

$$\begin{aligned} \omega_1 f = \sum_{0 \le s_1 < \cdots < s_{k-1} = n-2} &\Big(x_1 M'_{n-1, s_1, \dots, s_{k-1}} \omega_1 g_{(s_1, \dots, s_{k-1})} \\ &\pm x_1 M_{n-1, s_1, \dots, s_{k-1}} \omega_1 g_{(s_1, \dots, s_{k-1})} \Big) \\ &+ \sum{}^{(1)} x_1 \omega_1 h_I \pm \sum{}^{(2)} x_1 \cdot x_{I \setminus \{n\}} \cdot 1_I + \sum{}^{(2)} x_I 1_I. \end{aligned}$$

Then

(1) $$\begin{aligned} 0 &= f - \omega_1 f \\ &= \sum_{0 \le s_1 < \cdots < s_{k-1} = n-2} x_1 M'_{n-1, s_1, \dots, s_{k-1}} \left(g_{s_1, \dots, s_{k-1}} - \omega_1 g_{s_1, \dots, s_{k-1}} \right) \\ &\quad \times \sum_K x_K f'_K(y_1, \dots, y_n) \end{aligned}$$

where Σ_K denotes the summation over the subsets of order k in $\{1, \ldots, n-1\}$. By multiplying (1) by $M'_{n-1,n-2}$, we obtain $f'_K = 0$ for each K, by (2.3). Let $0 \le s_1 < \cdots < s_{k-1} = n-2$ and $s_k < s_{k+1} < \cdots < s_{n-1}$ be the ordered complement in $\{0, 1, \ldots, n-2\}$. By multiplying (1) by $M'_{n-1, s_k, \ldots, s_{n-1}}$, according to (2.3), we obtain

$$g_{s_1, \ldots, s_{k-1}} - \omega_1 g_{s_1, \ldots, s_{k-1}} = 0.$$

The lemma is proved.

Lemmata 2.7–2.13 are obtained by a similar way as in [5]. The following is crucial in the determination of the invariants of W_n.

LEMMA 2.17. *Let k be an integer with $2 \le k \le n$ and f be an element of $E(x_1, \ldots, x_n; 1) \otimes P(y_1, \ldots, y_n; 2)$ given by*

$$f = \sum_I x_I f_I(y_1, \ldots, y_n)$$

where I runs over the subsets of order k in $\{1, \ldots, n\}$ such that $\{1, n\} \not\subset I$. If f is an invariant of W_n, then f can be decomposed into the form

$$f = \sum_{0 \le s_1 < \cdots < s_k = n-1} M_{n, s_1, \ldots, s_k} f_{s_1, \ldots, s_k} + h$$

where all $f_{s_1, \ldots, s_k}$ are invariants of W_n in $P(y_1, \ldots, y_n)$ and h is an element of $E(x_1, \ldots, x_{n-1}) \otimes P(y_1, \ldots, y_{n-1}, V_n)$.

Proof. We write

$$f = \sum{}'' x_I f_I + x_1\Big(\sum{}' x_J f_I\Big)$$

as in (2.14). Set $F = \Sigma'' x_I f_I$, then F is an invariant of W'_{n-1}, and we have the decomposition

$$F = \sum_{0 \le s_1 < \cdots < s_k = n-2} M'_{n-1, s_1, \ldots, s_k} F_{s_1, \ldots, s_k}(y_1, \ldots, y_n)$$
$$+ \sum_I x_I F_I(y_1, \ldots, y_n)$$

where $F_{s_1, \ldots, s_k}$ and F_I are invariants of W'_{n-1}, and Σ_I denotes the summation over the subsets of order k in $\{2, \ldots, n-1\}$. As in the proof of Lemma 2.16, one can see that all $F_{s_1, \ldots, s_k}$ are invariants of W_n. Furthermore, we can assume that all F_I, where I occurs in Σ_I, and all f_I, with $1 \in I$, have y_n as a factor. Hence they obtain V''_{n-1} as a factor.

Let $\omega_1 = 1 + \varepsilon_{1n}$. We have

$$\omega_1 f = \sum_{0 \le s_1 < \cdots < s_k = n-2} M'_{n-1,s_1,\ldots,s_k} F_{s_1,\ldots,s_k}$$
$$\pm \sum_{0 \le s_1 < \cdots < s_k = n-2} M_{n-1,s_1,\ldots,s_k} F_{s_1,\ldots,s_k}$$
$$+ \sum_I x_I \omega_1 F_I + x_1\left(\sum{}' x_J \omega_1 f_I\right).$$

Hence

$$0 = f - \omega_1 f = \pm \sum_{0 \le s_1 < \cdots < s_k = n-2} M_{n-1,s_1,\ldots,s_k} F_{s_1,\ldots,s_k}$$
$$+ \sum_I x_I (F_I - \omega_1 F_I) + x_1\left(\sum{}' x_J (f_I - \omega_1 f_I)\right).$$

Since F_I and f_I have V''_{n-1} as a factor, $F_I - \omega_1 F_I$ and $f_I - \omega_1 f_I$ contain V'_{n-1} as a factor. By Lemma 2.12, $F_{s_1,\ldots,s_k}$ also contains V'_{n-1} as a factor. Then we have

$$f = \sum_{0 \le s_1 < \cdots < s_k = n-2} M'_{n-1,s_1,\ldots,s_k} V'_{n-1} F'_{s_1,\ldots,s_k}$$
$$+ \sum_I x_I F_I + x_1\left(\sum{}' x_J f_I\right).$$

By Lemma 2.11, f has then the form

$$f = \sum_{0 \le s_1 < \cdots < s_k = n-1} M_{n,s_1,\ldots,s_k} f_{s_1,\ldots,s_k}(y_1 2, y_n) + \sum{}''' x_I h_I$$

where Σ''' denotes the summation over the subsets of order k in $\{1,\ldots, n-1\}$.

Let ω be an element of W_n. We have

$$0 = f - \omega f = \sum{}''' x_I (h_I - \omega h_I)$$
$$+ \sum_{0 \le s_1 < \cdots < s_k = n-1} M_{n,s_1,\ldots,s_k}\left(f_{s_1,\ldots,s_k} - \omega f_{s_1,\ldots,s_k}\right).$$

By Lemma 2.13, we have $f_{s_1,\ldots,s_k} - \omega f_{s_1,\ldots,s_k} = 0$ and $h_I - \omega h_I = 0$. Hence $f_{s_1,\ldots,s_k}$ and h_I are invariants of W_n. The lemma is proved.

The proof of Theorem 2.4 will be completed by the following

LEMMA 2.18. *Let k be an integer with $1 \le k \le n$ and f be an element of $E(x_1,\ldots,x_n; 1) \otimes P(y_1,\ldots,y_n; 2)$ given by*

$$f = \sum_I x_I f_I(y_1,\ldots,y_n)$$

where I runs over the subsets of order k in $\{1, \dots, n\}$. If f is an invariant of W_n, then f can be decomposed into the form

$$f = \sum_{0 \le s_1 < \cdots < s_k = n-1} M_{n,s_1,\dots,s_k} f_{s_1,\dots,s_k}(y_1, \dots, y_n) + h$$

where all $f_{s_1,\dots,s_k}$ are invariants of W_n, and h is an element of $E(x_1, \dots, x_{n-1}) \otimes P(y_1, \dots, y_{n-1}, V_n)$.

Proof. If $k = 1$, we have $f = x_1 f_1 + \cdots + x_n f_n$. By Lemma 2.9, f_n contains L_{n-1} as a factor

$$f_n = L_{n-1} g$$

with some invariant g of W_n in $P(y_1, \dots, y_n)$. Then

$$f = x_1 f_1 + \cdots + x_{n-1} f_{n-1} + x_n L_{n-1} g$$

$$= (-1)^{n-1} M_{n,n-1} g + h.$$

Hence the lemma is proved for the case $k = 1$.

Next we consider the case $2 \le k \le n$. As in the proof of Lemma 2.16, f has the form

$$f = x_1 \sum_{0 \le s_1 < \cdots < s_{k-1} = n-2} M'_{n-1,s_1,\dots,s_{k-1}} g_{s_1,\dots,s_{k-1}}$$

$$+ \sum{}^{(1)} x_I h_I(y_1, \dots, y_n) + \sum{}^{(2)} x_I g_I(y_1, \dots, y_n)$$

and all $g_{s_1,\dots,s_{k-1}}$ are invariants of W_n by Lemma 2.16. Let $0 \le s_1 < \cdots < s_{k-1} = n-2$. By definition of $M_{n,s_1,\dots,s_{k-1},n-1}$ we have

$$x_1 M'_{n-1,s_1,\dots,s_{k-1}} = M_{n,s_1,\dots,s_{k-1},n-1} + \sum_I x_I h'_I(y_1, \dots, y_n)$$

where Σ_I denotes the summation over the subsets of order k in $\{2, \dots, n\}$. Then f has the form

$$f = \sum_{0 \le s_1 < \cdots < s_{k-1} = n-2} M_{n,s_1,\dots,s_{k-1},n-1} g_{s_1,\dots,s_{k-1}}$$

$$+ \sum{}^{(3)} x_I f'_I(y_1, \dots, y_n)$$

where $\Sigma^{(3)} x_I f'_I$ satisfies the conditions of Lemma 2.17. The lemma is proved.

3. The restriction homomorphism. Let G be an extra-special p-group of order p^{2n-1} $(n \ge 2)$. Let A be a maximal elementary abelian

p-subgroup of G as in (1.8). We are going to apply the invariants of W_n to prove the main theorem of this paper as follows.

THEOREM 3.1. (a) *If* $G = E_{n-1}$, *then*

$$\begin{aligned}\operatorname{Im}\operatorname{Res}(A,G) &= H^*(A)^{W_G(A)}\\ &= E(x_1,\dots,x_{n-1}) \otimes P(y_1,\dots,y_{n-1},V_n)\\ &\quad \oplus \sum_{k=1}^{n} \oplus \sum_{0\le s_1<\cdots<s_k=n-1} \oplus M_{n,s_1,\dots,s_k} P(y_1,\dots,y_{n-1},V_n).\end{aligned}$$

(b) *IF* $G = M_{n-1}$, *then*

$$\operatorname{Im}\operatorname{Res}(A,G) = E(x_1,\dots,x_{n-1}) \otimes P(y_1,\dots,y_{n-1},V_n).$$

LEMMA 3.2. *The elements* x_i, y_i, $1 \le i < n$, *and* V_n *are in* $\operatorname{Im}\operatorname{Res}(A,G)$.

Proof. This lemma has been proved by Tezuka-Yagita in [**9**]. For V_n, Tezuka and Yagita had used the Chern class of a complex representation of G. Here we give another proof by use of the norm map in Evens [**1**]. Let $\mathcal{N} = \mathcal{N}_{Z(G)\to G}$ be the norm map. By [**1**, Th. 2], we have

$$\operatorname{Res}(A,G)\mathcal{N}(y_n) = V_n.$$

LEMMA 3.3. *For* $0 \le s_1 < \cdots < s_k = n-1$, *there exist* $\varepsilon_i = 0,1$; $t_i = 1,2,3,\dots$ *such that*

$$M_{n,s_1,\dots,s_k} = \beta^{\varepsilon_0}\mathcal{P}^{t_1}\beta^{\varepsilon_1}\cdot\,\cdots\,\cdot\mathcal{P}^{t_l}\beta^{\varepsilon_l}M_{n,0,1,\dots,n-1}$$

up to a sign, where $\mathcal{P}^i$ *are the Steenrod operations.*

Proof. Let $\{i_1,\dots,i_k\}$, $\{i'_1,\dots,i'_{k'}\}$ be respectively two subsets of order k and k' in $\{0,1,\dots,n-1\}$ with $i_1 < \cdots < i_k$, $i'_1 < \cdots < i'_{k'}$. Let us define the relation

$$\{i_1,\dots,i_k\} \le \{i'_1,\dots,i'_{k'}\}$$

if one of the following conditions is satisfied:

—$k < k'$,

—if $k = k'$, then there exists an integer $1 \le m \le k$ such that $i_m < i'_m$ and $i_s = i'_s$ for $m+1 \le s \le k$, unless $\{i_1,\dots,i_k\} = \{i'_1,\dots,i'_k\}$.

The set $\mathcal{P}(\{0,1,\dots,n-1\})$ is then totally ordered. The lemma will be proved by descending induction on $\{s_1,\dots,s_k\}$.

First, we have $M_{n,1,2,\dots,n-1} = \pm\beta M_{n,0,1,\dots,n-1}$ up to a sign. Assume inductively that the lemma holds with $\{s_1,\dots,s_k\}$. Let $s'_1,\dots,s'_{k'}$ be the preceding element of $\{s_1, \ldots, s_k\}$. We have

—if $k' < k$, the $M_{n,s'_1,\ldots,s'_{k'}} = \beta M_{n,0,s'_1,\ldots,s'_{k'}}$,

—if $k' = k$, then there exists $0 \leq m \leq k$ such that $s'_m < s_m$ and $s'_t = s_t$ for $m + 1 \leq t \leq k$. Hence

$$M_{n,s'_1,\ldots,s'_k} = \pm \mathscr{P}^{p^{s_m}} M_{n,s_1,\ldots,s_k}.$$

The lemma is proved.

Let $Z = Z(G)$. We have the following commutative diagram of group extensions

$$\begin{array}{llllllllll}
(3.4) & 1 & \rightarrow & Z & \rightarrow & G & \rightarrow & G/Z & \rightarrow & 1 \\
 & & & \| & & \cup & & \cup & & \\
(3.5) & 1 & \rightarrow & Z & \rightarrow & A & \rightarrow & A/Z & \rightarrow & 1
\end{array}$$

Let $A' = A/Z$ be identified with the subgroup $\mathbf{Z}_p^{n-1}$ of A. The central group extension (3.5) becomes

$$(3.5)' \qquad 1 \rightarrow Z \rightarrow A \rightarrow A' \rightarrow 1$$

corresponding to the trivial cohomology class.

Let $a_1, \ldots, a_n, b_1, \ldots, b_{n-}$ be the elements of G satisfying Prop. 1.7, such that $a_1, \ldots, a_n$ correspond to the canonical basis of A as in (1.8). Then $\{a_1Z, \ldots, a_{n-1}Z, b_1Z, \ldots, b_{n-1}Z\}$ form a basis of G/Z. Let us identify G/Z with $\mathbf{Z}_p^{2n-2}$ by the correspondence

$$a_i \mapsto e_i = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix} < i, \qquad b_i \mapsto e_{n+i-1} \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix} < n + i - 1.$$

For $i \geq n$, let x_{i+1} be the dual of e_i over $\mathbf{Z}_p$ and $y_{i+1} = \beta x_{i+1}$. For $i < n$ (resp. $i = n$), the element $x_i \in H^1(A)$ can be identified with the dual of e_i (resp. $c \in Z$) over $\mathbf{Z}_p$. We have then

$$H^*(G/Z) = E(x_1, \ldots, x_{n-1}, x_{n+1}, \ldots, x_{2n-1}; 1)$$
$$\otimes P(y_1, \ldots, y_{n-1}, y_{n+1}, \ldots, y_{2n-1}; 2)$$

and $H^*(Z) = E(x_n; 1) \otimes P(y_n; 2)$.

In Phạm Anh Minh–Huỳnh Mùi [**4**; Lemma 2.2], we have proved

LEMMA 3.6. *Let $f \in H^2(\mathbf{Z}_p^n)$ be represented by a 2-cocycle $f\colon \mathbf{Z}_p^n \otimes \mathbf{Z}_p^n \rightarrow \mathbf{Z}_p$. Then we have*

$$f = \sum_{i=1}^{n} \alpha_i y_i + \sum_{1 \leq i < j \leq n} \beta_{ij} x_i x_j$$

where

$$\alpha_i = \sum_{k=1}^{p-1} f(e_i, e_i^k) \quad \text{and} \quad \beta_{ij} = f(e_i, e_j) - f(e_j, e_i).$$

From this lemma, one can see that the cohomology class z corresponding to the extension (3.4) is

$$(3.7) \quad \begin{array}{ll} y_1 + x_1 x_{n+1} + x_2 x_{n+2} + \cdots + x_{n-1} x_{2n-1} & \text{if } G = M_{n-1} \\ x_1 x_{n+1} + x_2 x_{n+2} + \cdots + x_{n-1} x_{2n-1} & \text{if } G = E_{n-1} \end{array}$$

via the isomorphism $(x_n)^*$: $H^2(G/Z, Z) \cong H^2(G/Z, \mathbf{Z}_p)$.

Consider the Hochschild-Serre spectral sequences of the central extensions (3.4) and (3.5)′. Let τ: $H^*(Z) \to H^{*+1}(G/Z)$ denote the transgression as usual. From [**2**; Chap. III, 3], we have

$$\tau x_n = z \in H^2(G/Z).$$

LEMMA 3.8. *If* $G = M_{n-1}$, *then*

$$\operatorname{Im}\operatorname{Res}(A, G) = E(x_1, \ldots, x_{n-1}) \otimes P(y_1, \ldots, y_{n-1}, V_n).$$

Proof. Since $\operatorname{Ann}_{H^*(X/G)}(\tau x_n) = 0$, we have

$$E_3(Z, G) = H^*(G/Z)|_{(\tau x_n, \beta\tau x_n)} \otimes \mathbf{Z}_p[y_n]$$

(see e.g. Phạm Anh Minh–Huỳnh Mùi [**4**]).

The inclusion map $A \hookrightarrow G$ gives us the corresponding map

$$E_\infty(Z, G) \to E_\infty(Z, A) = E_2(Z, A) = H^*(A) \otimes H^*(Z)$$

with image in $H^x(A') \otimes \mathbf{Z}_p[y_n]$. Then

$$\begin{aligned} \operatorname{Im}\operatorname{Res}(A, G) &\subset \left(H^*(A') \otimes \mathbf{Z}_p[y_n]\right)^{W_n} \\ &\subset E(x_1, \ldots, x_{n-1}) \otimes P(y_1, \ldots, y_{n-1}, V_n) \end{aligned}$$

by Theorem 2.4. The lemma is proved.

The above lemma concludes the part (b) of Theorem 3.1. The following completes the proof of 3.1(a).

LEMMA 3.9. *If* $G = E_{n-1}$, *then* $M_{n,0,1,\ldots,n-1} = x_1, \ldots, x_n$ *is an element of* $\operatorname{Im}\operatorname{Res}(A, G)$, *hence so are the elements* $M_{n,s_1,\ldots,s_k}$, $0 \le s_1 < \cdots < s_k = n - 1$.

Proof. Since $x_1 \cdot x_2 \cdot \cdots \cdot x_{n-1} \in \mathrm{Ann}_{H^*(G/Z)}(\tau x_n)$, we have

$$x_1 \cdot x_2 \cdots x_{n-1} \otimes x_n \in E_\infty^{n-1,1}(Z,G)$$

(see e.g. Phạm Anh Minh–Huỳnh Mùi [4]).

Consider the morphism of spectral sequences induced by the inclusion map $(A,G) \hookrightarrow (G,Z)$. We have the commutative diagram

$$\begin{array}{ccc} F^{n-1}H^n(G) & \to & E_\infty^{n-1,1}(Z,G) \\ \downarrow & & \downarrow f \\ F^{n-1}H^n(A) & \to & E_\infty^{n-1,1}(Z,A). \end{array} \tag{3.10}$$

Here $F^iH^*(G)$ and $F^iH^*(A)$ are Hochschild-Serre filtrations corresponding to (3.4) and (3.5)′.

Let m be an element of $F^{n-1}H^n(G)$ such that

$$M \in F^{n-1}H^n(G) \mapsto x_1 \cdot x_2 \cdot \cdots \cdot x_{n-1} \otimes x_n \in E_\infty^{n-1,1}(Z,G).$$

From the diagram (3.10), we have

$$\mathrm{Res}(A,G)M = x_1 \cdot x_2 \cdots x_n + F^nH^n(A).$$

Since $F^nH^n(A) = H^n(A') \subset \mathrm{Im}\,\mathrm{Res}(A,G)$ by Lemma 3.2, the element $x_1 \cdot x_2 \cdots x_n$ lies to $\mathrm{Im}\,\mathrm{Res}(A,G)$.

By Lemma 3.3, all $M_{n,s_1,\ldots,s_k}$ are elements of $\mathrm{Im}\,\mathrm{Res}(A,G)$. The lemma is proved.

REFERENCES

[1] L. Evens, *A generalization of the transfer map in cohomology of groups*, Trans. Amer. Math. Soc., **108** (1963), 54–65.

[2] G. P. Hochschild and J. P. Serre, *Cohomology of group extensions*, Trans. Amer. Math. Soc., **74** (1953), 110–135.

[3] G. Lewis, *The integral cohomology rings of groups of order* p^3, Trans. Amer. Math. Soc., **132** (1968), 501–529.

[4] Phạm Anh Minh and Huỳnh Mùi, *The* mod p *algebra of the group* $M(p^n)$, to appear.

[5] Huỳnh Mùi, *Modular invariant theory and cohomology algebras of symmetric groups*, J. Fac. Sci. Tokyo Univ., **22** (1975), 319–369.

[6] ______, *The* mod p *cohomology algebra of the extra-special group* $E(p^3)$, to appear.

[7] D. Quillen, *The* mod 2 *cohomology rings of extra-special 2-groups and the Spiner groups*, Math. Ann., **194** (1971), 197–223.

[8] Michie Suzuki, *Theory of groups*, Iwanami shoten, 1977 (in Japanese).

[9] M. Tezuka and N. Yagita, *The varieties of* mod p *cohomology rings of extra-special p-groups for an odd prime*, to appear.

Received July 7, 1983.

C/O NEAL KOBLITZ
UNIVERSITY OF WASHINGTON
SEATTLE, WA 98195