PHAM ANH MINH
KODAI MATH. J.
17 (1994), 571—584

A COHOMOLOGICAL APPROACH TO THEORY OF GROUPS OF PRIME POWER ORDER

BY PHAM ANH MINH

§0. Introduction

Let G be a finite group and A a G-module. Consider the set of group extensions

$$(\Gamma) \qquad 0 \to A \to \Gamma \to G \to 1$$

in which the G-module of A defined via conjugation of G coincides with the one already given in A. Two extensions (Γ) and (Γ') are said to be equivalent if there exists a homomorphism $f : \Gamma \to \Gamma'$ such that the diagram

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "i"] \arrow[d, equal] & \Gamma \arrow[r, "j"] \arrow[d, "f"'] & G \arrow[r] \arrow[d, equal] & 1 \\ 0 \arrow[r] & A \arrow[r, "i'"] & \Gamma' \arrow[r, "j'"] & G \arrow[r] & 1 \end{tikzcd}$$

is commutative.

Let $\mathcal{E}(\mathcal{G}, \mathcal{A})$ be the set of equivalence classes of such extensions. It is well-known that there exists a natural 1-1 correspondence

$$H^2(G, A) \overset{\theta}{\longleftrightarrow} \mathcal{E}(G, A)$$

with $\theta[\Gamma]$ the factor set of the extension (Γ). Good description of $H^2(G, A)$ is then an effective tool to the study of group extensions of A by G. This material has been used by several authors: Babakhanian [1], Baer [2], Beyl [4], Evens [7], Gruenberg [9], Schreier [20] [21], Stammbach [22] ... to obtain group theoretical results.

In this work, we restrict ourselves to the case where G is a group of prime power order (i.e. a p-group); in such a case, A can be chosen to be central and elementary. Our method is focussed on the Hochschild-Serre spectral sequence of a central extension: by studying the relation between the Hochschild-Serre filtration of $H^2(G, A)$ and the Frattini class of Γ, we obtain cohomological proofs of results concerning the Frattini subgroup of a p-group. Most of these results were already proved by other group theorists (Berger-Kovaćs-Newman [3], Blackburn [5], Kahn [13] [14], Hobby [10], Thompson [23] ...).

This note is organized as follows. In §1, we consider the central extension by an elementary abelian p-group and the term $E_\infty^{i,j}$, $(i+j=2)$ of the Hochschild-Serre spectral sequence for it. §2 is devoted to the study of the relation between the Hochschild-Serre filtration of $H^2(G, A)$ and the Frattini class of Γ; the main results of this section are Theorems 2.1 and 2.3. They are applied to the study of p-groups with cyclic Frattini

Received May 14, 1993.

subgroup and d-maximal p-groups in §3; some of these results were appeared in our earlier papers, we can refer to [6], [16].

From now on, for every p-group G, $H^*(G), Z(G), \Phi(G)$ denote respectively the mod$p$ cohomology algebra of G with coefficients in the prime field Z_p, the center and Frattini subgroup of G.

§1. Central extension by an elementary abelian p-group:

Let G be a p-group and A a central and elementary abelian subgroup of G of rank n. Consider the central extension

$$\text{(G)} \qquad 0 \to A \to G \to K \to 1$$

with $K = G/A$. We denote by z the factor set of the extension (G). So z is of form

$$z = (z_1, \dots, z_n) \in H^2(K, A) = \bigoplus_{n \text{ times}} H^2(K)$$

with $z_i \in H^2(K)$.

Let $\{u_1, \dots, u_n\}$ be a base of $H^1(A)$ and $v_i = \beta u_i$ with β the Bockstein homomorphism. Then

$$H^*(A) = \begin{cases} Z_2[u_1, \dots, u_n], & \text{if } p = 2 \\ E[u_1, \dots, u_n] \otimes Z_p[v_1, \dots, v_n], & \text{if } p > 2 \end{cases}$$

with $E[x, y, \dots]$ (resp. $Z_p[x, y, \dots]$) the exterior (resp. polynomial) algebra with generators $x, y, \dots$ over Z_p.

We denote by $\{E_r(G), d_r\}$ the Hochschild-Serre spectral sequence (HSss, in short) for the extension (G). So

$$E_2(G) = H^*(K) \otimes H^*(A) \Rightarrow H^*(G).$$

The base $\{u_1, \dots, u_n\}$ of $H^1(A)$ can be chosen such that $d_2(u_i) = z_i$. Note that u_i, v_i are transgressive and $d_3(v_i) = \beta z_i$. Generalizing [17, Prop. 1.5] and [18, Prop. 2.1], we have

PROPOSITION 1.1. (a) $E_\infty^{2,0}(G) = E_3^{2,0}(G) = H^2(K)/(z_1, \dots, z_n)$;
(b) $E_\infty^{1,1}(G) = E_3^{1,1}(G) = \{\sum \lambda_{ij} x_i \otimes u_j | \lambda_{ij} \in Z_p, x_i \in H^1(K), \sum \lambda_{ij} x_i . z_j = 0\}$;
(c) *If $z_1, \dots, z_n$ are linearly independent in $H^2(K)$, then*

$$E_3^{0,2}(G) = Z_p\{v_1, \dots, v_n\}$$

the vector space over Z_p generated by $v_1, \dots, v_n$, and $E_\infty^{0,2}(G) = E_4^{0,2}(G)$. Furthermore, $v_i \in E_\infty^{0,2}(G)$ iff $\beta z_i = 0$ mod$(z_1, \dots, z_n)$ in $H^*(K)$.

Proof. We need to prove that $E_3^{0,2}(G) = Z_p\{v_1, \dots, v_n\}$ if $z_1, \dots, z_n$ are linearly independent in $H^2(K)$. The remaining parts of the proposition are obvious by noting that d_r is of bidegree $(r, 1-r)$.

Since v_i is transgressive, we have $v_i \in E_3^{0,2}(G)$. Let $u = \sum \lambda u_i u_j$ be an element of Kerd_2, with $\lambda_{ij} \in Z_p$. By a change of base of A, we can assume that $u = \sum \lambda_{2k-12k} u_{2k-1} u_{2k}$. So $0 = \sum \lambda_{2k-12k}(z_{2k-1} u_{2k} - u_{2k-1} z_{2k})$. Since $z_1, \dots, z_n$ are linearly independent, we have $\lambda_{2k-12k} = 0$. The proposition follows. []

Let $\{F^iH^*(G)\}$ be the Hochschild-Serre filtration on $H^*(G)$. Following [11], we have

$$E_\infty^{i,j}(G) = F^iH^{i+j}(G)/F^{i+1}H^{i+j}(G).$$

We have then an isomorphism between vector spaces over Z_p:

$$H^2(G)] \xrightarrow{\eta} E_\infty^{2,0}(G) \oplus E_\infty^{1,1}(G) \oplus E_\infty^{0,2}(G). \tag{1.2}$$

The map η is defined as follows: if $x \in F^iH^2(G)$ $(o \le i \le 2)$, then $\eta x =$pr x, with pr the projection map from $F^iH^2(G)$ onto $E_\infty^{i,2-i}(G)$.

Note that the extensions (G) is obtained from successive central extensions by Z_p. In fact, let $\{a_1,\dots,a_n\}$ be the base of A, dual to $\{u_1,\dots,u_n\}$. Set $G^{(i)} = G/<a_i,a_{i+1},\dots,a_n>$. So $G^{(1)} = K$ and $G^{(n)} = G$. We get then a sequence of central extensions

$$0 \to <a_i> \to G^{(i+1)} \to G^{(i)} \to 1 \tag{$G^{(i)}$}$$

with factor set $z_i \in \operatorname{Im} \operatorname{Inf}(G^{(i)}, K)$.

(1.3) We now consider the simplest case where $n = 1$ and $z \neq 0$. Set $A =<a>$, u the dual of a and $v = \beta u$. Let X be an arbitrary element of $H^2(G)$ and Γ the central extension

$$0 \to Z_p \xrightarrow{i} \Gamma \to G \to 1 \tag{Γ}$$

with factor set X. Set $Z = iZ_p$. Note that Γ is isomorphic to the group whose underlying set is $Z_p \times G$, and the multiplication is given by

$$(a,g).(b,h) = (a+b+X(g,h), g.h)$$

with $a, b \in Z_p, g, h \in G$. We have

PROPOSITION 1.4. (a) $Z \subset \Phi(\Gamma)$ *iff* $X \neq 0$ *in* $H^2(G)$. *Furthermore, if* $X \neq 0$, *then* $\Phi(\Gamma)/Z = \Phi(G)$;

(b) *If* $\eta X = v$, *then* $(0,a)^p = (1,0)$;

(c) *If* $\eta X = x \otimes u$, *with* $x \in H^1(G)$, *and* g *an element of* G *with* $x(g) = 1$, *then* $[(0,g),(0,a)] = (1,0)$.

Proof. (a) It is obvious that $X = 0$ implies that $\Gamma = G\times Z$, so $Z \not\subset \Phi(\Gamma)$. Conversely, assume that $Z \not\subset \Phi(\Gamma)$, then there exists a maximal subgroup H of Γ such that $Z \not\subset H$. Hence $\Gamma = H.Z = H \times Z$, so the extension (Γ) splits. This implies $X = 0$.

For $X \neq 0$, since $\Gamma/\Phi(\Gamma)$ is elementary abelian and $\Gamma/\Phi(\Gamma) \cong \Gamma/Z/\Phi(\Gamma)/Z = G/\Phi(\Gamma)/Z$, we have $\Phi(G) \subset \Phi(\Gamma)/Z$. On the other hand, let L be normal in Γ with $L/Z = \Phi(G)$, then $\Gamma/L \cong \Gamma/Z/L/Z = G/\Phi(G)$. Since $G/\Phi(G)$ is elementary abelian, we have $\Phi(\Gamma) \subset L$. Hence $\Phi(\Gamma) = L$, so $\Phi(\Gamma)/Z = \Phi(G)$.

(b) Let B be the subgroup of Γ with $B/Z = A$, we have the central extension $0 \to Z \to B \to A \to 1$ with factor set $\operatorname{Res}(A,G)X = v \in H^2(A)$. So $B = C_{p^2}$, the cyclic group of order p^2. Hence $(0,a)^p = (1,0)$.

(c) Let C be the subgroup of Γ with $C/Z =<a,g>$, we have the central extension $0 \to Z_p \to C \to <a,g> \to 1$ with factor set $\operatorname{Res}(<a,g>,G)X = x.u \in H^2(<a,g>)$. So $[(0,g),(0,a)] = (1,0)$. ▯

We complete this section by some remark concerning the map η defined in (1.2).

Remark 1.5. (a) The map η is closely related to the Genea one in [8], and especially to the comodule structure of $H^*(G)$ over $H^*(A)$, defined by Stammbach in [22], as follows : since A is central, the map $m : A \times G \to G, (a,g) \mapsto a.g$ is a homomorphism. One gets then a map $\mu : H^*(G) \to H^*(G) \otimes H^*(A)$ (the Genea map is just the restriction of μ to $H^1(G) \to H^1(G) \otimes H^1(A)$). Hence, we have the map

$$\mu_2 : H^2(G) \to H^2(A) \oplus (H^1(G) \otimes H^1(A)) \oplus H^2(G).$$

One can check that μ_2 is nothing but

$$\begin{aligned} H^2(G) \xrightarrow{\ \eta\ } E_\infty^{2,0}(G) \oplus E_\infty^{1,1}(G) \oplus E_\infty^{0,2}(G) \hookrightarrow \\ H^2(K)/(z) \oplus (H^1(K) \otimes H^1(A)) \oplus H^2(A) \\ \xrightarrow{\ \text{Inf}\ } H^2(G) \oplus (H^1(G) \otimes H^1(A)) \oplus H^2(A). \end{aligned}$$

(b) As Im $\text{Inf}(H^2(K) \to H^2(G)) = E_\infty^{2,0}$, the sequence

$$\begin{aligned} 0 \to H^1(K) \xrightarrow{\ \text{Inf}\ } H^1(G) \xrightarrow{\ \text{Res}\ } H^1(A) \xrightarrow{\ \text{Inf}\ } H^2(G)_A \\ \xrightarrow{\ \eta'\ } H^2(A) \oplus (H^1(K) \otimes H^(A)) \xrightarrow{\ d_2\ } H^3(K) \end{aligned}$$

is exact, with η' the restriction of η to $E_\infty^{1,1}(G) \oplus E_\infty^{0,2}(G)$ and $H^2(G)_A = \text{KerRes}(H^2(G) \to H^2(A))$. We have then the extending Hochschild-Serre exact sequence, which has been given in [15] and [24].

§2. Frattini filtration of a p-group and HSss

Let G be a p-group. Set $\Phi^o G = G, \Phi^1 G = G^p.[G,G]$ (the Frattini subgroup of G), $\ldots, \Phi^{i+1}G = ((\Phi^i G)^p.[\Phi^i G, G], \ldots$. We have then the following descending sequence of subgroups of G

$$G = \Phi^o G \supset \Phi^1 G \supset \cdots \supset \Phi^i G \supset \Phi^{i+1} G \supset \ldots.$$

It is called the Frattini filtration of G. The Frattini class of G, denoted by $cl_\Phi(G)$, is defined to be the smallest integer m such that $\Phi^m(G) = \{1\}$. For example, $cl_\Phi(G) = 0$ iff $G = \{1\}$, $cl_\Phi(G) = 1$ iff G is elementary abelian, $cl_\Phi(G) = 2$ iff G is almost-special (i.e. a central extension of an elementary abelian p-group by an another). It is clear that $G/\Phi^i G$ is of Frattini class i.

By setting $A_i G = \Phi^{i-1}G/\Phi^i G$, $A_i G$ is then a vector space over Z_p.

In the remaining of this section, we suppose that $cl_\Phi G = m+1$. So $A_{m+1}G = \Phi^m G$ is central and elementary abelian. Furthermore, there exists quotients G_i of G given by the central extensions

(G_2) $$1 \to A_2 G \to G_2 \to A_1 G \to 0$$

(G_3) $$1 \to A_3 G \to G_3 \to G_2 \to 1$$

$$\ldots$$

(G_{m+1}) $$1 \to A_{m+1} G \to G_{m+1} \to G_m \to 1$$

with $G_{m+1} = G, G_{i-1} = G_i/A_i G$ and $G_1 = A_1 G$.

Let n_i =dim $_{Z_p} A_i G$ and $z^{(i)} = (z_1^{(i)}, \ldots, z_{n_{i+1}}^{(i)}) \in H^2(G_i, A_{i+1}G) = \bigoplus_{n_{i+1} \text{ times}} H^2(G_i)$ be the factor set of central extension (G_{i+1}). G is then determined by the sets $\{A_i G\}_{1 \le i \le m+1}$ and $\{z^{(i)}\}_{1 \le i \le m}$. The groups G_i, together with the maps $\text{Inf}(G_j, G_i)$ $(j \ge i)$ form a direct system. For simplicity, we denote by $\text{Inf}_2(G_i)$ the image of the map $\text{Inf}(H^2(G_i) \to H^2(G))$.

We now consider a central extension

$$(\Gamma) \qquad 0 \to Z_p \to \Gamma \to G \to 1$$

with factor set $X \in H^2(G)$. We want to know the Frattini class of Γ. It is clear that $m+2 \geq cl_\Phi\Gamma \geq m+1$. The following is obvious from Proposition 1.4 and its proof.

THEOREM 2.1. (a) *If $X \notin \mathrm{Inf}_2(G_m)$, then $cl_\Phi\Gamma = m+2$;*
(b) *If $X \in \mathrm{Inf}_2(G_i)$, then $cl_\Phi\Gamma = m+1$ and*

$$-A_{i+1}\Gamma = n_{i+1}+1 \text{ if } X, z_1^{(i)}, \dots, z_{n_{i+1}}^{(i)} \text{ are linearly independent,}$$
$$-A_1\Gamma = n_1+1 \text{ if } X, z_1^{(i)}, \dots, z_{n_{i+1}}^{(i)} \text{ are linearly dependent.}$$

We have then

COROLLARY 2.2. *$z_1^{(i)}, \dots, z_{n_{i+1}}^{(i)}$ are linearly independent in $H^2(G_i)/\mathrm{Inf}_2(G_i, G_{i-1})$.*

Let G and Γ be given as in (1.3). Assume furthermore that $z \neq 0$ and $X \neq 0$. We have

THEOREM 2.3. (a) *If $\eta X \in E_3^{1,1}(G)$, then $E_\infty^{0,2}(\Gamma) = 0$;*
(b) *If $\eta X \in E_3^{0,2}(G)$, then $E_\infty^{1,1}(\Gamma) = 0$;*

Proof. (a) If $\eta X \in E_3^{1,1}(G)$, then ηX is of form $x \otimes u$, with $x \in H^1(K)$. Let g be an element of K such that $x(g) \neq 0$ and (D) the central extension $0 \to Z_p \to D \to < g > \to 1$. Then $\mathrm{Res}(D,G)X \mapsto x \otimes u \in E_\infty^{1,1}(D)$. Hence $\beta X \mapsto x \otimes \beta u \in E_\infty^{1,2}(D)$ which is non-zero. Since $x \otimes \beta u$ is not of form $y.x \otimes \beta u$ with $y \in H^1(< g >)$, it follows that $\beta X = d_3(\beta u) \neq 0(\mathrm{mod}\ X)$. This implies $E_\infty^{0,2}(\Gamma) = 0$.

(b) Obvious by noting that v is algebraically independent in $E_\infty(G)$. □

From this, we obtain the following, which has been proved by Kahn in [14]

COROLLARY 2.4. *Let $i \geq 1$ be an integer. The following assertions are equivalent:*
(a) *$(\Phi^i G)^p = \Phi^{i+1}G$;*
(b) *$(\Phi^k G)^p = \Phi^{k+1}G$, $\forall \quad k \geq i$;*
(c) *$E_\infty^{1,1}(G_i) = 0$;*
(d) *$E_\infty^{1,1}(G_k) = 0$, $\forall \quad k \geq i$,*
with (G_i) the extension $1 \to A_iG \to G_i \to G_{i-1} \to 1$.

§3. Some applications

We are now going to apply our results to obtain cohomoligical proofs of some group theoretical one. We are interested in p-groups with cyclic Frattini subgroup and d-maximal p-groups.

a. p-groups with cyclic Frattini subgroup. We give here cohomological proofs of Hobby's theorem [10] (III 7.8 c in [12]), which asserts that $\Phi(G)$ is cyclic if $Z(\Phi(G))$ is cyclic, and of Berger, Kovaćs and Newman's result [3] on the classification of p-groups with cyclic Frattini subgroup.

First, we prove

THEOREM 3.1 (Hobby [10]). *If $Z(\Phi(G))$ is cyclic, then so is $\Phi(G)$.*

We need

LEMMA 3.2. *Let G and Γ be given as in (1.3). Assume that $X \neq 0$, then:*
(a) *Every extension of a subgroup of $\Phi(G) \cap Z(G)$ by Z is contained in $Z(\Phi(\Gamma))$;*
(b) *If $\eta X \in E_3^{2,0}(G)$, then $A \times Z$ is a subgroup of $\Phi(\Gamma) \cap Z(\Gamma)$.*

Proof. (a) Let $a \in \Phi(G) \cap Z(G)$ and $b \in \Gamma$ such that $bG = a$. For $g, h \in \Gamma$, since $[g, b]$ and $[h, b]$ belong to Z, we have $[g^p, b] = 1$ and $[[g, h], b] = 1$ in Z. (a) is then proved.

(b) Obvious from the definition of the Hochschild-Serre filtration on Bar cochains. □

From this and Proposition 1.4, we obtain

LEMMA 3.3. *With the assumption of Lemma 3.2, assume that $Z(\Phi(\Gamma))$ is cyclic, then $\Phi(G) \cap Z(G)$ is cyclic and $\eta X \in E_\infty^{0,2}(G)$.*

LEMMA 3.4. *With the assumption of Lemma 3.2, assume that $\Phi(\Gamma) \cap Z(\Gamma)$ is cyclic and $E_\infty^{0,2}(\Gamma) \neq 0$, then $\Phi(G) \cap Z(G)$ is cyclic and $\eta X \in E_\infty^{0,2}(G)$.*

Proof. Consider the extension (G), with A an arbitrary subgroup of $\Phi(G) \cap Z(G)$ of order p. Since $\Phi(\Gamma) \cap Z(\Gamma)$ and $E_\infty^{0,2}(\Gamma) \neq 0$, it follows from Lemma 3.3 that $\eta X \in E_\infty^{0,2}(G)$. So $\mathrm{Res}(A, G)X = v$. Since A is an arbitrary normal subgroup of G of order p, $\Phi(G) \cap Z(G)$ is cyclic. The lemma follows. □

Proof of Theorem 3.5. Let $|G| = p^{n+l}$ and $|\Phi(G)| = p^l$. By Lemmas 3.3 and 3.4, we get a sequence of central extensions $(G_i) 0 \to Z_p \to G_i \to G_{i+1} \to 1, 1 \leq i \leq l$, with $G_1 = G, G_{l+1} = C_p^n$, and the factor set z_i of (G_i) satisfies $z_i \in E_\infty^{0,2}(G_{i+1})$, $\beta z_l = 0$. Hence $\Phi(G_l)$, $\Phi(G_{l-1})$, ..., $\Phi(G_1)$ are cyclic. The theorem is proved.

The classification of p-groups with cyclic Frattini subgroup has been done by Berger, Kovaćs and Newmann [3]. These groups can be constructed cohomologically as follows. First, we recall some basic facts of cohomology of groups. Let b be a generator of the cyclic group C_{p^l} and u_b , v_b be respectively the 1- and 2-cocycles of C_{p^l} given by

$$u_b(b) = 1, \quad v_b(b^i, b^j) = \begin{cases} 0, & \text{if } i + j < p^l \\ 1, & \text{otherwise.} \end{cases}$$

So $v_b = \beta u_b$, for $l = 1$. It is well-known that

$$H^*(C_{p^l}) = \begin{cases} Z_2[u_b], & \text{if } l = 1 \text{ and } p = 2 \\ E[u_b] \otimes Z_p[v_b; 2], & \text{otherwise.} \end{cases} \tag{3.6}$$

Hence, if k is an integer and $C_{p^l} \times C_p^{k-1} =< b_1, ..., b_k/b_1^{p^l} = b_i^p = [b_j, b_i] = 1, 2 \leqq i \leqq k, 1 \leqq j \leqq k >$, by setting $u_i = u_{b_i}, v_i = v_{b_i}$, we get

$$H^*(C_{p^l} \times C_p^{k-1}) = \begin{cases} Z_2[u_1, ..., u_k], & \text{if } l = 1 \text{ and } p = 2 \\ E[u_1] \otimes Z_2[v_1] \otimes Z_2[u_2, ..., u_k], & \text{if } l > 1 \text{ and } p = 2 \\ E[u_1, ..., u_k; 1] \otimes Z_p[v_1, ..., v_k; 2], & \text{if } p > 2 \end{cases}$$

The following is then obvious.

LEMMA 3.7. *Let $0 \neq X \in H^2(C_{p^l} \times C_p^{k-1})$. Assume furthermore that* $\mathrm{Res}(< b_1^{p^{l-1}} >, C_{p^l} \times C_p^{k-1})X = v_{b_1^{p^{l-1}}}$ *if $l > 1$. Then X can be reduced by an automorphism of $C_{p^l} \times C_p^{k-1}$ to one of the canonical forms*

i) $\sum_{i=1}^m u_{2i-1}.u_{2i}$, $u_1^2 + \sum_{i=2}^m u_{2i-1}.u_{2i}$, $u_1^2 + u_2^2 + u_1.u_2 + \sum_{i=2}^m u_{2i-1}.u_{2i}$ *if $p = 2$ $l = 1$;*

ii) $\lambda v_1 + \mu u_1.u_2 + \sum_{i=2}^m u_{2i-1}.u_{2i}$ *if $l > 1$ or $p > 2$,*

with $\mu =$ 0 or 1, and

$$\lambda = \begin{cases} 1, & \text{if } l > 1 \\ 0 \quad \text{or} \quad 1, & \text{otherwise.} \end{cases}$$

Let

$$E = \begin{cases} < a, b/a^p = b^p = [a, b]^p = [a, [a, b]] = [b, [a, b]] = 1 >, & \text{if } p > 2 \\ D_8, & \text{if } p = 2. \end{cases}$$

and M be an extra-special p-group of order p^{l+2} or one of the groups given by

(1) $M(p^{l+2}) =< a, b/a^{p^{l+1}} = b^p = 1, a^b = a^{1+p^l} >$ for $p > 2$,

(2) $M(2^{l+2})$,
$D(2^{l+2}) =< a, b/a^{2^{l+1}} = b^2 = 1, b^{-1}ab = a^{-1} >$,
$Q(2^{l+2}) =< a, b/a^{2^{l+1}} = b^2, b^{-1}ab = a^{-1} >$,
$S(2^{l+2}) =< a, b/a^{2^{l+1}} = b^2 = 1, b^{-1}ab = a^{-1+2^{n-2}} >$ (especially, $D(8) = M(8)$, $S(8) = C_4 \times C_2$). We have

LEMMA 3.8. *Let $0 \to Z_p \to G \to C_{p^l} \times C_p^{k-1} \to 1$ be a central extension with factor set $0 \neq z \in H^2(C_{p^l} \times C_p^{k-1})$ having one of the forms given in Lemma 3.7. Then G is isomorphic to one of the following groups*

$$C_{p^{l+1}} \cdot \underbrace{E \cdot ... \cdot E}_{m-1 \text{ times}} \times C_p^{k-2m+1}, \quad M \cdot \underbrace{E \cdot ... \cdot E}_{m-1 \text{ times}} \times C_p^{k-2m}.$$

Here and in what follows, $A \cdot B$ means the central product of A and B with $|A \cap B| = p$.

Proof. Obvious from the fact that the factor sets of the central extensions

$$0 \to Z_p \to C_{p^{l+1}} \to C_{p^l} \to 1,$$
$$0 \to Z_p \to G \to C_{p^l} \times C_p \to 1$$

with $G = E, Q_8$ (for $l = 1$), $M_{p^{l+2}}$ are respectively v_1, $u_1.u_2$, $u_1^2 + u_2^2 + u_1.u_2$, $v_1 + u_1.u_2$. □

Analogous results can be stated if we replace C_{p^l} by $D(2^l)$. Recall that

$$D(2^l) =< a, b/a^{2^{l-1}} = b^2 = 1, a^b = a^{-1} > .$$

Let u_a, u_b be elements of $H^1(D(2^l))$ given by $u_a(a^ib^j) = i, u_b(a^ib^j) = j$ for $0 \leqq i < 2^{l-1}, 0 \leqq j < 2$ and $Z_l \in H^2(D(2^l))$ the factor set of the central extension $0 \to Z_2 \to D(2^{l+1}) \to D(2^l) \to 1$. The following is due to Quillen [19] and Mui [18].

LEMMA 3.9. *$H^*(D(2^l)) = P[u_a, u_b, Z_l]/(u_a^2 + u_a.u_b)$. Furthermore, we have:*
(i) *$\beta Z_l = u_b.Z_l$.*
(ii) *if $A =< a^{2^{l-2}}, a^ib >$ is a maximal elementary abelian subgroup of $D(2^l)$, with $0 \leq i < 2^{l-1}$, then $\mathrm{Res}(A, D(2^l))Z_l = u^2_{a^{2^{l-2}}} + u_{a^{2^{l-2}}}.u_{a^ib}$.*

Let c be a generator of C_2. Set $\Gamma = D(2^l) \times C_2$, we have

LEMMA 3.10. *Let $X \in H^2(\Gamma)$ with $\mathrm{Res}(< a^{2^{l-2}} >, \Gamma)X = u^2_{a^{2^{l-2}}}$. Then X can be reduced by an automorphism of Γ to one of the canonical forms*

$$Z_l + \mu u_c^2, \quad Z_l + u_a^2 + \mu u_c^2, \quad Z_l + u_b^2, \quad Z_l + u_a^2 + u_a.u_c + \mu u_c^2$$

with $\mu \in Z_2$.

Proof. The proof follows by appropriate change of generators of Γ (for details, see [16]). □

Let k be an integer and $\{b_1, ..., b_{k-1}\}$ a base of C_2^{k-1}. Set $\Psi_l = D(2^l) \times C_2^{k-1}$, then

$$H^*(\Psi_l) = P[u_a, u_b, u_1, ..., u_{k-1}, Z_l]/(u_a^2 + u_a.u_b).$$

By appropriate change of generators of Ψ_l, we get

LEMMA 3.11. *Let $X \in H^2(\Psi_l)$ with $\mathrm{Res}(< a^{2^{l-2}} >, \Psi_l)X = u^2_{a^{2^{l-2}}}$. Then X can be reduced by an automorphism of Ψ_l to one of the canonical forms*

$$Z_l + \mu u_a^2 + \nu(1-\mu)u_b^2 + \sum_{i=1}^{m-1} u_{2i-1}.u_{2i},$$

$$Z_l + u_a^2 + u_a.u_1 + \mu u_1^2 + \sum_{i=2}^{m-1} u_{2i-1}.u_{2i},$$

$$Z_l + u_a^2 + u_a.u_1 + u_2^2 + \sum_{i=2}^{m-1} u_{2i-1}.u_{2i},$$

with $\mu, \nu \in Z_2$.

Let $H = D^+(2^{l+2})$ (resp. $Q^+(2^{l+2})$) be the central extension

$$0 \to Z_2 \to H \to \Gamma \to 1$$

with factor set $Z_l + u_a^2 + u_a.u_1$ (resp. $Z_l + u_a^2 + u_a.u_1 + u_1^2$). Since the factor sets of the extensions

$$0 \to Z_2 \to G \to D(2^l) \to 1,$$

with $G = D(2^{l+1})$, $S(2^{l+1})$, $Q(2^{l+1})$ are respectively Z_l, $Z_l + u_a^2$, $Z_l + u_b^2$, (see e.g. Mui[18]), we have

LEMMA 3.12. *Let* $0 \to Z_2 \to G \to \Psi_{l+1} \to 1$ *be a central extension with factor set* $0 \neq z \in H^2(\Psi_{l+1})$ *having one of the forms given in Lemma* 3.11, *then* G *is isomorphic to one of the following groups*

$$M \cdot \underbrace{E \cdot \ldots \cdot E}_{m-1\text{times}} \times C_2^{k-2m+1}, \quad N \cdot \underbrace{E \cdot \ldots \cdot E}_{m-2\text{times}} \times C_2^{k-2m+2},$$

$$D^+(2^{l+3}) \cdot C_4 \cdot \underbrace{E \cdot \ldots \cdot E}_{m-2\text{times}} \times C_2^{k-2m+1}$$

where N *is either* $D^+(2^{l+2})$, $Q^+(2^{l+2})$, $D(2^{l+2}) \cdot C_4$ *or* $S(2^{l+2}) \cdot C_4$.

Berger-Kovaćs-Newman's result can be stated as follows.

THEOREM 3.13 (Berger, Kovaćs, Newman [3]). *Let* G *be a* p*-group with cyclic Frattini subgroup of order* p^l. *If* $|G| = p^{n+l}$, *then* G *is isomorphic to one of the groups given in Lemmas 3.8 and 3.12.*

To prove it, we need

LEMMA 3.14. *Let* (G) *be the central extension given in* (1.3). *If* K *is not elementary abelian, then* $\Phi(G)$ *is cyclic iff* $\Phi(K)$ *is cyclic and* $z \mapsto \alpha v \in E_\infty^{0,2}(G)$ *with* $0 \neq \alpha \in Z_p$.

Proof. By Proposition 1.4 a), we have the central extension $0 \to A \to \Phi(G) \to \Phi(K) \to 1$. So $\Phi(G)$ is cyclic iff $\Phi(K)$ is cyclic and $\mathrm{Res}(\Phi(K), K)z \neq 0$. The lemma follows. []

LEMMA 3.15. *Let* $K = C_{p^l} \times C_p^{k-1}$ *or* $D(2^l) \times C_2^{k-1}$ *and* G *be one of the groups given in Lemmas* 3.8 *and* 3.12. *Then* $E_\infty^{0,2}(G) \neq 0$ *iff* $G = C_{p^{l+1}} \times C_p^{k-1}$ *or* $D(2^{l+1}) \times C_2^{k-1}$

Proof. It is obvious that $E_\infty^{0,2}(G) \neq 0$ iff $\beta z = 0(\mathrm{mod}\ z)$ in $H^*(K)$. This fact is equivalent to $z = v_1$ or $z = Z_l$. The lemma follows. []

Proof of Theorem 3.16. We proceed by induction on l. The theorem is clearly true for $l = 1$. Assume that it holds for $l - 1$ $(l \geq 2)$. Let Z be the subgroup of $\Phi(G)$ of order p. By Lemmas 3.14 and 3.15, $\Phi(G/Z)$ is cyclic, $G/Z \cong C_{p^l} \times C_p^{n-1}$ or $D(2^l) \times C_2^{n-1}$ and the factor set for the central extension $1 \to Z \to G \to G/Z \to 1$ is of one of the forms given in Lemmas 3.7 and 3.11. The theorem follows from Lemmas 3.8 and 3.12.

b. <u>d-maximal p-groups.</u>

For every p-group G, let $d(G) = \dim H^1(G)$ the minimal number of generators of G. Following Kahn [13],, G is said to be d-maximal if $d(K) < d(G)$ for every proper subgroup K of G. These groups have been studied by Blackburn [5], Kahn [13][14] and Thompson[23]. The following is due to Blackburn (for $d(G) \leq 3$) and Thompson (for $p > 2$ and $d(G)$ replaced by $|G/[G,G]|$) and reproved by Kahn in [13].

THEOREM 3.17 (Blackburn-Thompson). *Let G be a d-maximal p-group, then G is of (nilpotence) class ≤ 2 provided that $p > 2$, or $p = 2$ and $d(G) \leq 3$.*

It is reasonable to ask whether the conclusion remains true for $p = 2$ and $d(G) \geq 4$. In [13], Kahn claimed that it is valid for $d(G) = 4$, but this claim is not true. We prove

THEOREM 3.18. *Let G be a d-maximal p-group, then G is of class 2 and* Inf *$(H^2(G/\Phi(G)) \to H^2(G))$ is surjective, provided that one of the following conditions is satisfied:*

(a) $p > 2$.
(b) $p = 2$ *and* $|\Phi(G)| = 2^m$ *with* $m \leq 2$.

COROLLARY 3.19. *If G is d-maximal, G is of class 2 provided that one of the following conditions is satisfied:*

(a) $p > 2$.
(b) $p = 2$ *and* $|\Phi(G)| \leqq 2^3$.
(c) $p = 2$ *and* $d(G) \leqq 3$.
(d) $\Phi(G)$ *is elementary abelian.*

THEOREM 3.20. *For every $n \geq 4$, there exists a d-maximal 2-group $\mathcal{G}_\backslash$ of class ≥ 3 with $d(\mathcal{G}_\backslash) = \backslash$.*

From those, we obtain another proof of Theorem 3.17, and the fact that any d-maximal p-group G is of class 2 iff $\Phi(G)$ is elementary abelian. Besides, Theorem 3.20 shows that the mentioned conclusion is false for $p = 2$ and $d(G) \geq 4$.

We need the following lemmas. The first one is due to Kahn [13].

LEMMA 3.21. *If G is d-maximal and N is normal in $G, N \subset \Phi(G)$, then G/N is d-maximal.*

A d-maximal p-group of class ≤ 2 is almost special, according to the following.

LEMMA 3.22. *If G is d-maximal, then $\Phi(G) = [G, G]$(the commutator subgroup of G). Hence, if G is of class 2, $\Phi(G)$ is elementary abelian.*

Proof. By Lemma 3.2, $G/[G, G]$ is d-maximal. Since $G/[G, G]$ is abelian, it is elementary abelian. So $\Phi(G) = [G, G]$. If G is of class 2 , we have $[x, y]^p = [x^p, y] = 1$ for every $x, y \in G$. So $\Phi(G)$ is elementary abelian. $\square$

LEMMA 3.23. *Let*

$$0 \to Z_p \xrightarrow{i} G \to K \to 1$$

be a central extension with factor set $z \in H^2(K)$. Set $Z = iZ_p$. Then:

(a) $d(K) \leq d(G) \leq d(K) + 1$. *Moreover,* $d(G) = d(K) + 1$ *iff the extension splits, i.e.* $z = O$ *in* $H^2(K)$.
(b) *if* $z \neq 0$ *in* $H^2(K)$, *then G is not d-maximal provided that z is decomposable (i.e.*

$z = x.y$ with $x, y \in H^1(K)$), or $z = \beta x$ with $x \in H^1(K)$.

(c) *for every subgroup L of G, we have $d(L) \leq d(L.Z)$, and $d(L) = d(L.Z)$ iff $Z \subset L$.*

Proof. (a) It is clear that $d(K) \leq d(G)$. By Prop. 1.4. we have $d(G) \leq d(K) + 1$, and $d(G) = d(K)$ iff $Z \not\subset \Phi(G)$, or equivalently, $z = 0$.

(b) Let $L = \mathrm{Ker} x \subset G$. Then $d(L/Z) = d(G/Z) - 1 = d(G) - 1$. Since $\mathrm{Res}(L/Z, K)z = 0$, the extension $0 \to Z_p \to L \to L/Z \to 1$ splits. Hence $d(L) = d(L/Z) + 1 = d(G)$. So G is not d-maximal.

(c) If $Z \not\subset L$, then $L.Z = L \times Z$, so $d(L.Z) = d(L) + 1$. Hence $d(L) \leq d(L.Z)$ and $d(L) = d(L.Z)$ iff $Z \subset L$. []

(3.24) Let G be an almost special p-group given by the central extension

$$0 \to W \to G \to V \to 0$$

with factor set $z \in H^2(V, W)$, where W and V are respectively vector spaces of dimension m, n over Z_p. Let $\{e_1, ..., e_m\}$ be a fixed base of W. The factor set z is then of form $z = (z_1, ..., z_m)$ with $z_i = p_i^*(z) \in H^2(V)$. If $f \in GL(W)$, it is obvious that G is isomorphic to the extension of W by V with factor set $f^* z$.

Set $r(z) = \mathrm{rank}(z_1, ..., z_m)$ in $H^2(V)$. By Theorem 2.1 and the fact that KerInf $(H^2(V) \to H^2(G)) = (z_1, ..., z_m)$, we have

LEMMA 3.25. *With the notations of (3.24), then $\Phi(G) = W$ iff $r(z) = m$.*

Let $\{u_1, ..., u_n\}$ be a base of $H^1(V)$. Each u_i is consedered as element of $H^1(G)$ via the inflation map. From Lemmas 3.23 c) and 3.25, we get the following lemma, which has been proved by Kahn in [13].

LEMMA 3.26. *With the notations of (3.24), let $1 \leq k \leq n$ be an integer and $L = \bigcap_{i=1}^k \mathrm{Ker} u_i \subset G$. Then $d(L) = d(G) - k + m - r(z|_L)$ with $z|L = \mathrm{Res}(L/W, V)z$. Hence G is d-maximal iff $m < k + r(z|_L)$ for every $1 \leq k \leq n$.*

(3.27) For convenience, with a given subgroup $L = \bigcap_{i=1}^k \mathrm{Ker} u_i$ of G as in Lemma 3.26 and $X \in H^*(V)$, we write $X' = X|_L = \mathrm{Res}(L/W, V)X$. With this notation, z' is then obtained from z by setting $u_1 = ... = u_k = 0$, $\beta u_1 = ... = \beta u_k = 0$.

In the following three lemmas , G is assumed to be given as in (3.24) with $r(z) = m$.

LEMMA 3.28. *If there exist $x_1, ..., x_m \in H^1(V)$ not all equal to 0 such that $x_1 z_1 + ... + x_m z_m = 0$ or $x_1 z_1 + \beta z_1 = 0$, then G is not d-maximal.*

Proof. If $x_1 z_1 + ... + x_m z_m = 0$, we can suppose that $x_1, ..., x_m$ are linearly independent. So, for every i, we have $z_i \in (x_1, ..., x_m, \beta x_1, ..., \beta x_m)$, the ideal generated by $x_1, ..., x_m, \beta x_1, ..., \beta x_m$ Hence $r(z') = 0$ with $L = \bigcap_{i=1}^m \mathrm{Ker} x_i$. By Lemma 3.26, G is not d-maximal.

If $x_1 z_1 + \beta z_1 = 0$, z_1 is then of form $z_1 = \beta u + x_1.v$ with $u, v \in H^1(V)$. We have then $\beta z_1 + x_1 z_1 = 0$. For $p > 2$, this implies $\beta x_1.v - x_1.\beta v + x_1.\beta u = 0$, so $v = \lambda x_1$, with $\lambda \in Z_p$. For $p = 2$, $x_1[z_1 + (x_1 + v)v] = 0$, so $z_1 = v(x_1 + v)$. By Lemma 3.23 b), G

is not d-maximal. ▯

LEMMA 3.29. *If there exist $x_1, \ldots, x_m \in H^1(V)$ not all equal to 0 such that $X = x_1z_1 + \ldots + x_mx_m + \beta z_m = 0$, then G is not d-maximal provided that $p > 2$, or $p = 2$ and $m = 2$.*

Proof. By Lemma 3.28, we can assume that $m \geq 2$. Since $X = 0, z_m$ is of form $z_m = \beta u + v_1x_1 + \ldots + v_mx_m$ with $u, v_i \in H^1(V)$. Hence $Y = \sum_{i=1}^m [\beta(v_i) + z_i]x_i - \beta x_i.v_i = 0$. Consider the following cases:

(a) $p > 2$: for every $1 \leq k \leq m$, set $H = \bigcap_{i \neq k} \mathrm{Ker} v_i$, then $0 = Y|_H = [\beta(u_k) + z_k]x_k - \beta(x_k).v_k$. Hence $v_k \in (x_1, \ldots, x_m)$ and $z_k \in (x_1, \ldots, x_m, \beta x_1, \ldots, \beta x_m)$. We have then $r(z') = 0$ with $L = \bigcap_{i=1}^m \mathrm{Ker} x_i$. By Lemma 3.26, G is not d-maximal.

(b) $p = 2$ and $m = 2$: since $0 = Y = x_1[v_1(x_1 + v_1) + z_1] + x_2[v_2(x_2 + v_2) + z_2]$, we obtain $z_1 = v_1(v_1 + x_1) + k.x_2, z_2 = k.x_1 + v_2(v_2 + x_2)$ with $k \in H^1(V)$. So $k(k + x_1) = v_1(v_1 + x_1)$. This implies $k = v_1$ or $v_1 + x_1$. Hence z_2 is decomposable and G is not d-maximal by Lemma 3.23 b). ▯

LEMMA 3.30. *If G is d-maximal, then* $\mathrm{Inf}(H^2(V) \to H^2(G))$ *is surjective, provided that $p > 2$ or $p = 2$ and $m \leq 2$.*

Proof. Obvious from Lemmas 3.28, 3.29 and (1.2).

Proof of Theorem 3.31. The proof is evident from Lemma 3.30 and Theorem 2.1.

Proof of Theorem 3.32. The proof follows from Theorem 3.18, Theorem 2.1 and Proposition 1.4.

Proof of Theorem 3.33. Let G be the almost special 2-group given by the central extension

$$0 \to Z_2^3 \to G \to Z_2^4 \to 0$$

with factor set $z = (z_1, z_2, z_3)$ in which

$$z_1 = x^2 + b(y + b),$$
$$z_2 = xy + a(a + x),$$
$$z_3 = y^2 + a^2 + b^2 + ax + by,$$

with $\{x, y, a, b\}$ a fixed base of $H^1(Z_2^4)$.

By Lemma 3.26 and by a direct verification, we can show that G is d-maximal. Clearly $d(G) = 4$ and $|\Phi(G)| = 2^3$. Since $\beta z_3 = yz_1 + xz_2$, following Proposition 1.1, there exists a non-zero element $V \in H^2(G)$ such that $V|_Z = u^2 \neq 0$, so $V|_{\Phi(G)} \neq 0$. Let Γ be the central extension

$$0 \to Z_2 \xrightarrow{j} \Gamma \to G \to 1$$

with factor set V, then $d(\Gamma) = 4$. Assume that there exists a subgroup L of Γ such that $d(L) \geq 4$. By Lemma 3.23 c), we can suppose that $Z' = jZ_2 \subset L$. Since L/Z' is a subgroup of G and G is d-maximal, $d(L/Z') \leq 3$. By Lemma 3.23 a), $d(L) \geq 4$ implies the splitting of the extension

$$1 \to Z' \to L \to L/Z' \to 1$$

and $d(L/Z') = 3, Z \subset L/Z'$. We have then $V|_{L/Z'} = 0$. This contradicts the fact that $V|_Z \neq 0$. So Γ is d-maximal.

Since $V|_{\Phi(G)} \neq 0$, $\Phi(\Gamma)$ is not elementary abelian. By Lemma 3.2, $\Phi(\Gamma) \not\subset Z(\Gamma)$. Hence Γ is of class ≥ 3. For every $n \geq 4$, set $\mathcal{G}_\backslash = - \times \mathcal{Z}_\epsilon^{\backslash-\Delta}$. It is clear that $\mathcal{G}_\backslash$ is d-maximal of class ≥ 3 and $d(\mathcal{G}_\backslash) = \backslash$. The theorem follows.

The following is straighforward from Corollary 2.4, Lemma 3.28 and 3.33.

COROLLARY 3.34. *For every p-group G, G is d-maximal iff $G/\Phi^i G$ is d-maximal, for any $i \geq 2$. Furthermore, if G is d-maximal, then $(\Phi^i G)^p = \Phi^{i+1} G$.*

Remark 3.35. In [13], Kahn claimed that every d-maximal 2-group H with $d(H) = 4$ is of class ≤ 2, by proving that if $cl(H) = 3, [\Phi(H), H] = Z_2$, then there exists an element $x \in H - \Phi(H)$ such that $x^2 \in \Phi(H)^2$. This proof is not correct. In fact, if H has such a property, then so does $G = H/Z$, with $Z = [\Phi(H), H]$. Our group G defined in 3.33 is a counterexample of it.

REFERENCE

[1] A. Babakhanian, *Cohomological wethods in group theory*, Marcel Dekker Inc., 1972.

[2] R. Baer, *Erweiterung von Gruppen und ihren Isomorphismen*, Math. Z. **38** (1934), 375–416.

[3] T.R. Berger, L.C. Kovaćs, M.F. Newman, *Groups of prime order with cyclic Frattini subgroup*, Nederl. Akad. Wetensch. Proc. Ser. A.83(1) = Indag. Math (1980), 13–18.

[4] R. Beyl, *The classification of metacyclic p-groups, and other applications of homological algebra to group theory*, Dissertation, Cornell (1972).

[5] N. Blackburn, *Generalizations of certain elementary theorems on p-groups*, Proc. London Math. Soc. **11** (1961), 1–22.

[6] N.V. Duc-P.A. Minh, *p-Groups with cyclic Frattini subgroup*, Preprint (1992).

[7] L. Evens, *Terminal p-groups*, J. Math. **12** (1968), 682–699.

[8] T. Ganea, *Homologie et extensions centrales de groupes*, C. R. Acad. Sc. Paris **266** (1968), 556–558.

[9] K.W. Gruenberg, *Cohomological Topics in group theory*, Lecture Notes in Math. 143, Springer, (1970).

[10] C. Hobby, *The Frattini subgroup of a p-group*, Pac. J. Math. **10** (1960), 209–212.

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

[12] B. Huppert, *Endliche Gruppen I*, Die Grundlehren der mathematischen wissenschaften, 134. Springer-Verlag, Berlin, Heidelberg, New York, (1967).

[13] B. Kahn, *The total Stiefel-Whitney class of a regular representation*, J. Alg. **144** (1991), 214–247.

[14] B. Kahn, *Sur une propriété de certains p-groupes*, Preprint, (1992).

[15] N. Iwahori - M. Matsumoto, *Several remarks on projective representations of finite groups*, J. Fac. Sci. Univ. Tokyo **10** (1963/64), 129–146.

[16] P.A. Minh, *d-maximal p-groups*, Preprint, (1992).

[17] P.A. Minh and H. Mui, *The mod p cohomology algebra of the group $M(p^n)$*, Act. Math. Viet. **7** (1982), 17–26.

[18] H. Mui, *The mod 2 cohomology algebras of the groups of order 2^4*, Preprint (1982).

[19] D. Quillen, *The Adams conjecture*, Topology **10** (1971), 67–80.

[20] O. Schreier, *Ueber die Eiwerterung von Gruppen, I.*, Monatah. Math. und Phys. **34** (1926), 165–180.

[21] O. Schreier, *Ueber die Eiwerterung von Gruppen, II*, Abh. Math. Sem, Hamburg **4** (1926), 321–346.

[22] Urs. Stammbach, *Homology in group theory*, Lecture Notes in Math. 359, Springer, 1973.

[23] J.G. Thompson, *A replacement theorem for p-groups and a conjecture*, J. Alg **13** (1969), 149–151.

[24] N.Q.D. Thong, *Sur le module des relations d'un p-groupe et la suite exacte d'inflation-restriction*, J. Reine Angew. Math. (1980).

Department of Mathematics
University of Hue
DAI HOC TONG HOP, Hue
Vietnam