Can J. Math., Vol. XL, No. 6, 1988, pp. 1422–1435

THE MODULAR GROUP ALGEBRAS OF P-GROUPS OF MAXIMAL CLASS

C. BAGIŃSKI AND A. CARANTI

Introduction. The isomorphism problem for modular group algebras of finite p-groups appears to be still far from a solution (see [**7**] for a survey of the existing results). It is therefore of interest to investigate the problem for special classes of groups.

The groups we consider here are the p-groups of maximal class, which were extensively studied by Blackburn [**1**]. In this paper we solve the modular isomorphism problem for such groups of order not larger than p^{p+1}, having an abelian maximal subgroup, for odd primes p.

What we in fact do is to generalize methods used by Passman [**5**] to solve the isomorphism problem for groups of order p^4. In Passman's paper the case of groups of maximal class is actually the most difficult one.

In [**2**] the isomorphism problem is solved for 2-groups of maximal class. For odd primes the situation is not as manageable, and in fact the case of an arbitrary p-group of maximal class, even possessing an abelian maximal subgroup, appears to us to be quite difficult.

However, the results of Section 1 are fairly general, and do not apply only to p-groups of maximal class. It is also worth noting that almost everywhere we use the information provided not by the full group algebra, but by the factor algebra over the square of the ideal generated by the Lie commutators.

Notation. Our notation follows in general that of [**3**] and [**6**], except as specified below.

We write G_i for the i-th term of the lower central series of the group $G, i \geqq 2$. We denote by $[a,b] = ab - ba$ the (Lie) commutator of two elements a, b of an associative algebra, and by $(g,h) = g^{-1}h^{-1}gh$ the (group) commutator of two elements g, h of a group.

Our group algebras $\mathbf{F}G$ are always taken over the field $\mathbf{F}$ with p elements. We write $I(G)$ for the augmentation ideal of $\mathbf{F}G$, and $U(G) = 1 + I(G)$ for the group of normalized units of $\mathbf{F}G$.

We will use the following well-known formula

$$(*) \qquad [u, v^t] = \sum_{k=1}^{t} \binom{t}{k} v^{t-k}[u, v, \dots, v]$$

where v appears k times in the commutator.

Received December 1, 1987 and in revised form July 22, 1988. The research of the second author was partially supported by MPI, Italy.

By analogy with group theory we define, if A is an associative algebra, B, C are subalgebras of A, and D is an ideal of C, the centralizer in B of C/D as the following subalgebra of A

$$C_B(C/D) = \{b \in B | [b, c] \in D, \text{ for all } c \in C\}.$$

We refer to the original paper [**1**] and to III.14 of [**3**] for the theory of p-groups of maximal class. We refer to [**6**] for the theory of Jennings' basis, and the concept of weight of an element.

1. Let G be any finite p-group. We define a series of ideals of the group algebra $\mathbf{F}G$ by

$$\begin{aligned} J_2 &= \mathbf{F}G\,I(G_2), \text{ and} \\ J_k &= J_{k-1}I(G) + I(G)J_{k-1} \end{aligned}$$

for $k > 2$.

We show that

$$J_k = \sum_{i=2}^{k} I(G)^{k-i} I(G_i),$$

where $I(G)^0 = \mathbf{F}G$, so that

$$J_k = I(G)J_{k-1} + \mathbf{F}G\,I(G_k).$$

We first prove that, for all k,

$$(1) \qquad I(G)I(G_k) + I(G_k)I(G) = I(G)I(G_k) + \mathbf{F}G\,I(G_{k+1}).$$

To prove that the right hand side is contained in the left hand side, we note that by the modular analogue of Lemma 3.4.29 of [**9**], the map $g \longrightarrow g - 1$ induces an isomorphism

$$\frac{G_k}{G_{k+1}G_k^p} \cong \frac{\mathbf{F}G\,I(G_k)}{I(G)I(G_k) + I(G_k)I(G)}$$

so that in particular $I(G_{k+1})$ is contained in the left hand side of (1).

To prove the opposite inclusion, we first record the formula, for subgroups H, K of the group G,

$$(2) \qquad [I(H), I(K)] \subseteq \mathbf{F}G\,I((H, K)).$$

Thus if $a \in I(G_k), b \in I(G)$,

$$ab \in I(G)I(G_k) + [I(G_k), I(G)] \subseteq I(G)I(G_k) + \mathbf{F}G\,I(G_{k+1}),$$

and this proves (1).

Now assume by induction

$$J_{k-1} = I(G)^{k-3}I(G_2) + \cdots + I(G)^{k-i-1}I(G_i) + \cdots + \mathbf{F}G\, I(G_{k-1}).$$

We get

$$(3) \qquad \begin{aligned} J_k &= I(G)^{k-2}I(G_2) + \cdots + I(G)^{k-i}I(G_i) + \cdots + I(G)I(G_{k-1}) \\ &\quad + I(G)^{k-3}I(G_2)I(G) + \cdots + I(G)^{k-i-1}I(G_i)I(G) + \cdots + I(G_{k-1})I(G). \end{aligned}$$

Now since, using (1),

$$\begin{aligned} &I(G)^{k-i}I(G_i) + I(G)^{k-i-1}I(G_i)I(G) \\ &\qquad = I(G)^{k-i-1}(I(G)I(G_i) + I(G_i)I(G)) \\ &\qquad = I(G)^{k-i-1}(I(G)I(G_i) + \mathbf{F}G\, I(G_{i+1})) \\ &\qquad = I(G)^{k-i}I(G_i) + I(G)^{k-i-1}I(G_{i+1}), \end{aligned}$$

all the terms in the second row of (3) are superfluous, except the last one. For this we have, by (1),

$$I(G)I(G_{k-1}) + I(G_{k-1})I(G) = I(G)I(G_{k-1}) + \mathbf{F}G\, I(G_k).$$

LEMMA 1.1. *Let* $\alpha_1, \ldots, \alpha_n \in U(G), n \geqq 2$. *Then*

$[\alpha_1, \ldots, \alpha_n] \in J_n$, *and*

$(\alpha_1, \ldots, \alpha_n) - 1 \equiv [\alpha_1, \ldots, \alpha_n] \bmod J_{n+1}$.

Proof. The first formula follows immediately by induction from the definition of J_n.

We prove the second one also by induction. For $n = 2$ we have

$$\begin{aligned} (\alpha_1, \alpha_2) - 1 &= \alpha_1^{-1}\alpha_2^{-1}[\alpha_1, \alpha_2] = [\alpha_1, \alpha_2] + (\alpha_1^{-1}\alpha_2^{-1} - 1)[\alpha_1, \alpha_2] \\ &\equiv [\alpha_1, \alpha_2] \bmod J_3. \end{aligned}$$

Assume

$$(\alpha_1, \ldots, \alpha_{n-1}) - 1 \equiv [\alpha_1, \ldots, \alpha_{n-1}] \bmod J_n,$$

that is,

$$(\alpha_1, \ldots, \alpha_{n-1}) = 1 + [\alpha_1, \ldots, \alpha_{n-1}] + \beta, \text{ for some } \beta \in J_n.$$

https://doi.org/10.4153/CJM-1988-065-2 Published online by Cambridge University Press

We have

$$\begin{aligned}(\alpha_1, \dots, \alpha_n) - 1 &= (\alpha_1, \dots, \alpha_{n-1})^{-1}\alpha_n^{-1}[(\alpha_1, \dots, \alpha_{n-1}), \alpha_n] \\ &= [\alpha_1, \dots, \alpha_{n-1}, \alpha_n] + [\beta, \alpha_n] \\ &+ ((\alpha_1, \dots, \alpha_{n-1})^{-1}\alpha_n^{-1} - 1) \\ &\cdot ([\alpha_1, \dots, \alpha_{n-1}, \alpha_n] + [\beta, \alpha_n]) \\ &\equiv [\alpha_1, \dots, \alpha_n] \bmod J_{n+1},\end{aligned}$$

because $[\beta, \alpha_n] \in J_{n+1}$ and $[\alpha_1, \dots, \alpha_n] \in J_n$.

PROPOSITION 1.2. *For every finite p-group G, the two groups*

$$\frac{G}{\Phi(G_2)}, \qquad \frac{U(G)}{1 + I(G)I(G_2)}$$

have the same nilpotency class. Therefore, the nilpotency class of the first group is determined by the group algebra $\mathbf{F}G$.

Proof. Let n be the class of $G/\Phi(G_2)$, i.e., n is the smallest natural number such that $G_{n+1} \leqq \Phi(G_2)$. By the lemma, we have, for all $\alpha_1, \dots \alpha_n \in U(G)$,

$$(\alpha_1, \dots, \alpha_{n+1}) \in 1 + J_{n+1}.$$

But

$$\begin{aligned}J_{n+1} &= I(G)^{n-1}I(G_2) + \cdots + I(G)^{n-i+1}I(G_i) + \cdots + \mathbf{F}G\, I(G_{n+1}) \\ &\subseteq I(G)I(G_2) + \mathbf{F}G\, I(G_{n+1}),\end{aligned}$$

and

$$\mathbf{F}G\, I(G_{n+1}) \subseteq \mathbf{F}G\, I(\Phi(G_2)) \subseteq \mathbf{F}G\, I(G_2)^2 \subseteq I(G)I(G_2),$$

so that

$$(\alpha_1, \dots, \alpha_{n+1}) \in 1 + I(G)I(G_2),$$

and thus the class of

$$\frac{U(G)}{1 + I(G)I(G_2)}$$

is at most n.

On the other hand, we will prove that the image of G in this latter group is isomorphic to $G/\Phi(G_2)$. This will show that the class of this group is at least n, and thus exactly n, as required.

In fact, we need only to prove that

$$G \cap 1 + I(G)I(G_2) = \Phi(G_2), \tag{4}$$

and this follows from 3.1.19 of [**9**].

COROLLARY 1.3. *Let G be a p-group with the property that $G/\Phi(G_2)$ has maximal class. Let H be another p-group, with*

$$\frac{\mathbf{F}G}{\mathbf{F}G\, I(G_2)^2} \cong \frac{\mathbf{F}H}{\mathbf{F}H\, I(H_2)^2}.$$

Then $H/\Phi(H_2)$ is also a p-group of maximal class.

In particular, if G is a p-group of maximal class with G_2 elementary abelian, so is H.

This follows immediately from Proposition 1.2, since $I(G)I(G_2) \supseteq I(G_2)^2$. Note that by III.14.14 and III.14.16 of [**3**], the condition G_2 elementary abelian is equivalent to G_2 abelian, and $|G| \leqq p^{p+1}$.

The method of proof of the next proposition is related to Lemma 10 of [**5**]. See also Proposition 2.1 below.

PROPOSITION 1.4. *Let G be a finite p-group, and assume that the subgroup*

$$N = C_G\left(\frac{G_2}{\Phi(G_2)}\right)$$

is maximal in G. Then

$$I(N) + \mathbf{F}G\, I(G_2) = C_{I(G)}\left(\frac{\mathbf{F}G\, I(G_2)}{\mathbf{F}G\, I(G_2)^2}\right).$$

In particular

(i) *the subring $I(N) + \mathbf{F}G\, I(G_2)$ is determined by $\mathbf{F}G$, i.e., is canonical in the sense of Passman* ([**5**]), *and*

(ii) *the algebra*

$$\frac{I(N) + \mathbf{F}G\, I(G_2)}{\mathbf{F}G\, I(G_2)^2}$$

is commutative if and only if the section

$$\frac{N}{\Phi(G_2)}$$

of G is commutative.

Proof. Let

$$S = I(N) + \mathbf{F}G\, I(G_2), \qquad U = C_{I(G)}\left(\frac{\mathbf{F}G\, I(G_2)}{\mathbf{F}G\, I(G_2)^2}\right).$$

To show that $S \subseteq U$, we expand

$$[I(N), \mathbf{F}G\,I(G_2)] \subseteq [I(N), \mathbf{F}G]I(G_2) + \mathbf{F}G[I(N), I(G_2)].$$

Now the first term is clearly contained in $\mathbf{F}G\,I(G_2)^2$, and for the second we have, using (2) and the definition of N

$$[I(N), I(G_2)] \subseteq \mathbf{F}G\,I((N, G_2)) \subseteq \mathbf{F}G\,I(\Phi(G_2)) \subseteq \mathbf{F}G\,I(G_2)^2.$$

We now prove the opposite inclusion, $S \supseteq U$.

Let $g \in G - N$, and take $h_1, \dots, h_k \in N$ such that the elements

$$(g-1)^i(h_1-1)^{i_1}\dots(h_k-1)^{i_k},$$

$0 \leqq i, i_1, \dots, i_k < p$, form a Jennings' basis of $I(G)$ modulo $\mathbf{F}G\,I(G_2)$.

Let n be the smallest natural number such that

$$I(G)^n \subseteq \mathbf{F}G\,I(G_2)$$

and let u be an element of U. Write u with respect to a Jennings' basis of $I(G)$ assuming that no terms from S occur in the representation of u. By induction on t, we show that if $u \in I(G)^t$, then $u \in I(G)^{t+1}$, for all $t < n$.

Now let

$$(5)\qquad \begin{aligned} u \equiv \sum a_{i_1,\dots,i_k}&(g-1)^{t-w(h_1)i_1-\dots-w(h_k)i_k} \\ &\times (h_1-1)^{i_1}\dots(h_k-1)^{i_k} \bmod I(G)^{t+1}, \end{aligned}$$

where no exponent is greater than $p-1$, and the exponent of $g-1$ is at least 1. Here $w(h_j)$ is the weight of h_j.

Take any element $z \in G_2$ such that $(z, g) = z_1 \notin \Phi(G_2)$, and let $w(z_1) = s$. We have, by assumption, $[z-1, u] \in \mathbf{F}G\,I(G_2)^2$. Moreover,

$$\begin{aligned} [z-1, u] \equiv \sum a_{i_1,\dots,i_k}&[z-1, (g-1)^{t-w(h_1)i_1-\dots-w(h_k)i_k}] \\ &\times (h_1-1)^{i_1}\dots(h_k-1)^{i_k} \equiv 0 \bmod I(G)^{t+s} + FG\,I(G_2)^2 \end{aligned}$$

since

$$[z-1, I(G)^{t+1}] \subseteq I(G)^{t+s} + \mathbf{F}G\,I(G_2)^2.$$

In fact, since z is in G_2 and the h_i's are in N, we have

$$[z-1, \mathbf{F}G\,I(G_2)] \subseteq \mathbf{F}G\,I(G_2)^2, \text{ and}$$

$$[z-1, h_i-1] \subseteq \mathbf{F}G\,I(\Phi(G_2)) \subseteq \mathbf{F}G\,I(G_2)^2,$$

https://doi.org/10.4153/CJM-1988-065-2 Published online by Cambridge University Press

and moreover, by (*) the commutator $[z - 1, (g - 1)^k]$ lies in $I(G)^{k+s-1}$.

Take, by way of contradiction, t_0 to be the largest integer smaller than p such that there exist $i_1, \cdots, i_k < p$ with

$$t_0 = t - w(h_1)i_1 - \ldots - w(h_k)i_k$$

and $a_{i_1,\ldots,i_k} \neq 0$. Using (*), we obtain

$$\begin{aligned}[z - 1, u] \equiv \sum a_{i_1,\ldots,i_k} t_0 (g - 1)^{t_0 - 1}(h_1 - 1)^{i_1} \ldots (h_k - 1)^{i_k}(z_1 - 1) \\ + u_1 \bmod I(G)^{t+s} + \mathbf{F}G\, I(G_2)^2,\end{aligned}$$

where u_1 is a sum of terms in which $g - 1$ occurs with exponent smaller than $t_0 - 1$. This forces all $a_{i_1,\ldots,i_k}$'s to be zero, and this contradiction shows that $u \in I(G)^{t+1}$.

Now (i) is clear, and (ii) follows from the formula

$$[I(N), I(N)] \subseteq \mathbf{F}G\, I((N, N))$$

and the argument we used at the end of the proof of Proposition 1.2.

2. In this section, G will be a group of maximal class of order $p^n, 4 \leqq n \leqq p + 1$, with an abelian maximal subgroup G_1. According to Section 4 of [**1**], there are elements $s \in G - G_1, s_1 \in G_1$ such that, defining recursively $s_i = (s_{i-1}, s)$, for $i > 1$,

$$\begin{aligned} G_i/G_{i+1} &= \langle s_i G_{i+1} \rangle, \\ s^p &= s_{n-1}^{\delta}, \\ s_1^p &= s_{n-1}^{\gamma} \text{ for } n < p + 1, \text{ and } s_1^p = s_p^{\gamma - 1} \text{ for } n = p + 1. \end{aligned}$$

Moreover, there are $2 + (n - 2, p - 1)$ isomorphism classes of these groups. If $\gamma = 0$, there are two classes, with $\delta = 0, 1$ respectively. If $\gamma \neq 0$, then we may take $\delta = 0$, and the isomorphism class of G is determined by the coset $\gamma(\mathbf{F}^*)^{n-2}$ of γ with respect to the subgroup of the multiplicative group $\mathbf{F}^*$ consisting of the $(n - 2)$-th powers.

Now consider, as in Lemma 9 of [**5**], the p-th power map

$$\begin{aligned} \frac{I(G)}{I(G)^2} &\longrightarrow \frac{I(G)^p}{I(G)^{p+1}}, \\ u + I(G)^2 &\longrightarrow u^p + I(G)^{p+1}. \end{aligned}$$

By just looking at it, we can distinguish the two cases: $\gamma = 0$ and $\delta = 0$; $\gamma = 0$ and $\delta = 1$. Moreover, if $\gamma \neq 0$, and thus $\delta = 0$, we can determine the subspace

$$\mathbf{F} \cdot (s - 1) + I(G)^2 \text{ of } I(G)/I(G)^2,$$

the subspace $\mathbf{F} \cdot (s_1 - 1) + I(G)^2$ being determined by Proposition 1.4.

If $n < p+1$, the p-th power map is linear, G being a regular p-group with elementary abelian derived subgroup. Therefore we just need a little linear algebra to see that $\gamma = 0$ if and only if the p-th power map vanishes on $\mathbf{F}\cdot(s_1-1)+I(G)^2$. Moreover in this case $\delta = 0$ if and only if the map is zero. If $\gamma \neq 0$, and thus we may take $\delta = 0$, then $\mathbf{F} \cdot (s - 1) + I(G)^2$ is determined as the kernel of the p-th power map.

If $n = p + 1$, using standard commutator identities one sees that the p-th power map is

$$\begin{aligned}\alpha(s-1) + \beta(s_1 - 1) + I(G)^2 &= s^{\alpha}s_1^{\beta} - 1 + I(G)^2 \\ &\longrightarrow (s^{\alpha}s_1^{\beta} - 1)^p + I(G)^2 \\ &= s^{\alpha p}s_1^{\beta p}(s_1^{\beta}, s^{\alpha}, \dots, s^{\alpha}) - 1 + I(G)^2 \\ &= (\alpha\delta + \beta(\gamma - 1) + \beta\alpha^{p-1}) \cdot (s_p - 1) + I(G)^{p+1}.\end{aligned}$$

If $\gamma = 0$ and $\delta = 0$, then $\mathbf{F}\cdot(s_1-1)+I(G)^2$ is the only 1-dimensional subspace of $I(G)/I(G)^2$ on which the p-th power map does not vanish. If $\gamma = 0$ and $\delta = 1$, the p-th power map does not vanish on any subspace. If $\gamma \neq 0$, so that we take $\delta = 0$, the p-th power map vanishes exactly on $\mathbf{F} \cdot (s - 1) + I(G)^2$ and possibly on $\mathbf{F}\cdot(s_1-1)+I(G)^2$, if $\gamma = 1$. Since this second space is determined, so is the first.

Notice that since $s_p \notin \Phi(G_2)$, formula (4) of Section 1 implies that $s_p - 1 \notin \mathbf{F}G\,I(G_2)^2$, and thus the above discussion depends only on

$$\frac{\mathbf{F}G}{\mathbf{F}G\,I(G_2)^2}.$$

The next result plays the same rôle here as does Lemma 10 in [**5**], and its proof combines the idea of the latter with the techniques already employed in Proposition 1.4 above.

Proposition 2.1. *Let G be a group of maximal class of order $p^n, 4 \leqq n \leqq p+1$, with an abelian maximal subgroup, and use for G the notation described at the beginning of this section. Then*

$$\mathbf{F}G(s_{n-2} - 1) + I(G)^p + \mathbf{F}G\,I(G_2)^2 = C_{I(G)}\frac{I(G)}{(\mathbf{F}\cdot(s_{n-1} - 1) + I(G)^{p+1} + \mathbf{F}G\,I(G_2)^2)}.$$

In particular, if the subspace

$$\mathbf{F}\cdot(s_{n-1} - 1) + I(G)^{p+1} + \mathbf{F}G\,I(G_2)^2$$

is determined by $\mathbf{F}G$, *so is*

$$\mathbf{F}G(s_{n-2}-1)+I(G)^p+\mathbf{F}GI(G_2)^2.$$

Proof. Let

$$\begin{aligned} S &= \mathbf{F}G(s_{n-2}-1)+I(G)^p+\mathbf{F}G\,I(G_2)^2, \\ T &= \mathbf{F}\cdot(s_{n-1}-1)+I(G)^{p+1}, \\ U &= C_{I(G)}\left(\frac{I(G)}{T+\mathbf{F}G\,I(G_2)^2}\right). \end{aligned}$$

We show that $S = U$. As

$$\begin{aligned} &[I(G),\mathbf{F}G(s_{n-2}-1)] \\ &\qquad \subseteq \mathbf{F}G\cdot[I(G),s_{n-2}-1]+[I(G),\mathbf{F}G]\cdot(s_{n-2}-1) \\ &\qquad \subseteq \mathbf{F}\cdot(s_{n-1}-1)+I(G)^{p+1}+\mathbf{F}G\,I(G_2)^2, \end{aligned}$$

the inclusion $S \subseteq U$ is clear.

Assume, by way of contradiction, that there exists an element $u \in U - S$. Write u in terms of a Jennings' basis of $\mathbf{F}G$ modulo $I(G)^p + \mathbf{F}G\,I(G_2)^2$, assuming that no terms from S occur in the representations of u. We prove by induction on t that

$$u \in I(G)^t+\mathbf{F}G\,I(G_2)^2, \qquad \text{for } t \leqq p.$$

Therefore we will obtain $u \in I(G)^p + \mathbf{F}G\,I(G_2)^2$, as required.

Assume that $u \in I(G)^t + \mathbf{F}G\,I(G_2)^2$, with $t < p$. We show that

$$u \in I(G)^{t+1}+\mathbf{F}G\,I(G_2)^2.$$

Now

$$\begin{aligned} u \equiv\ & a_{0t}(s_1-1)^t+\sum_{i=0}^{t-1}a_{1i}(s-1)^{t-i}(s_1-1)^i \\ &+\sum_{i=0}^{t-2}a_{2i}(s-1)^{t-2-i}(s_1-1)^i(s_2-1) \\ &+\sum_{i=0}^{t-3}a_{3i}(s-1)^{t-3-i}(s_1-1)^i(s_3-1)+\cdots \\ &+\begin{cases} a_{t0}(s_t-1), & \text{if } t<n-2 \\ \displaystyle\sum_{i=0}^{t-n+3}a_{n-3,i}(s-1)^{t-n+3-i}(s_1-1)^i(s_{n-3}-1), & \text{if } t \geqq n-2 \end{cases} \\ & \bmod I(G)^{t+1}. \end{aligned}$$

Since $u \in U$, but $s_{n-2} - 1$ does not appear in u above, we have $[s_1 - 1, u]$ and $[s - 1, u]$ are in $I(G)^{t+2} + \mathbf{F}G\,I(G_2)^2$. Therefore we have, by (*),

$$\begin{aligned}
[s_1 - 1, u] &\equiv \sum_{i=0}^{t-1} a_{1i}[s_1 - 1, (s-1)^{t-i}](s_1 - 1)^i \\
&\equiv a_{10}\left(t(s-1)^{t-1}(s_2 - 1) + \binom{t}{2}(s-1)^{t-2}(s_3 - 1) + \cdots\right) \\
&\quad + a_{11}\Big((t-1)(s-1)^{t-2}(s_2 - 1) \\
&\quad + \binom{t-1}{2}(s-1)^{t-3}(s_3 - 1) + \cdots\Big)(s_1 - 1) + \cdots \\
&\quad + a_{1,t-1}(s_2 - 1)(s_1 - 1)^{t-1} \equiv 0 \bmod I(G)^{t+2} + \mathbf{F}G\,I(G_2)^2,
\end{aligned}$$

which holds exactly when all a_{1i} are zero.

Therefore we have

$$\begin{aligned}
[s - 1, u] &\equiv a_{0t}[s - 1, (s_1 - 1)^t] + \sum_{i=0}^{t-2} a_{2i}(s-1)^{t-2-i}(s_1 - 1)^i(1 - s_3) \\
&\quad + \sum_{i=0}^{t-3} a_{3i}(s-1)^{t-3-i}(s_1 - 1)^i(1 - s_4) + \cdots \\
&\quad + \begin{cases} a_{t0}(1 - s_{t+1}) & \text{if } t < n - 2 \\ \displaystyle\sum_{i=0}^{t-n+3} a_{n-3,i}(s-1)^{t-n+3-i}(s_1 - 1)^i(1 - s_{n-2}), & \text{if } t \geqq n - 2 \end{cases} \\
&\equiv 0 \bmod I(G)^{t+2} + \mathbf{F}G\, I(G_2)^2.
\end{aligned}$$

Now expanding the first summand in the right hand side according to (*), we see that $a_{0t} = 0$. Then it is an easy matter to see that all other coefficients are zero, which proves the induction step.

The next theorem is our main result. The method of proof generalizes the last part of Section IV of [**5**].

THEOREM 2.2. *Let G be a p-group of maximal class having an abelian maximal subgroup. Assume $|G| \leqq p^{p+1}$. If H is another group, and*

$$\frac{\mathbf{F}G}{\mathbf{F}G\,I(G_2)^2} \cong \frac{\mathbf{F}H}{\mathbf{F}H\,I(H_2)^2},$$

then H is isomorphic to G.

In particular, $\mathbf{F}G \cong \mathbf{F}H$ *implies* $G \cong H$.

Proof. Set $|G| = p^n$, and use for G the notation described at the beginning of this section. By the argument using the p-th power map given at the beginning of the section, we just need to consider the case $\gamma \neq 0, \delta = 0$, and we need to show that

$$\frac{\mathbf{F}G}{\mathbf{F}G\,I(G_2)^2}$$

determines $\gamma(\mathbf{F}^*)^{n-2}$.

Moreover we know that the subspaces $\mathbf{F}\cdot(s-1)+I(G)^2$ and $\mathbf{F}\cdot(s_1-1)+I(G)^2$ of $\mathbf{F}G$ are determined. We choose arbitrarily elements in them,

$$0 \neq x \in \mathbf{F}\cdot(s-1)+I(G)^2, 0 \neq y \in \mathbf{F}\cdot(s_1-1)+I(G)^2,$$

so that

$$x \equiv \alpha(s-1) \bmod I(G)^2, \alpha \in \mathbf{F}^*$$

$$y \equiv \beta(s_1-1) \bmod I(G)^2, \beta \in \mathbf{F}^*.$$

Now by Lemma 1.1, and since $J_m \subseteq I(G)^m$, we have

$$[y, x, \ldots, x] \equiv \beta\alpha^{n-3}\cdot(s_{n-2}-1) \bmod I(G)^{n-1},$$

where there are $n-3x$'s in the commutator.

Now choose arbitrarily an element

$$z \in (\beta\alpha^{n-3}\cdot(s_{n-2}-1)+I(G)^{n-1}) \cap (\mathbf{F}G(s_{n-2}-1) \\ + I(G)^p + \mathbf{F}GI(G_2)^2),$$

where the second subspace is determined by Proposition 1.2, since

$$\frac{\mathbf{F}\cdot(s_{n-1}-1)+I(G)^{p+1}}{I(G)^{p+1}}$$

is the image of the p-th power map. Thus

$$z \equiv \beta\alpha^{n-3}\cdot(s_{n-2}-1) \bmod I(G)(s_{n-2}-1)+I(G)^p+\mathbf{F}G\,I(G_2)^2,$$

and we have

$$[z, x] \equiv \beta\alpha^{n-2}\cdot(s_{n-1}-1) \not\equiv 0 \bmod I(G)^{p+1}+\mathbf{F}G\,I(G_2)^2.$$

Moreover,

$$y^p \equiv \beta\gamma\cdot(s_{n-1}-1) \bmod I(G)^{p+1}+\mathbf{F}G\,I(G_2)^2$$

if $n < p + 1$, and

$$y^p \equiv \beta(\gamma - 1) \cdot (s_p - 1) \bmod I(G)^{p+1} + \mathbf{F}G\, I(G_2)^2.$$

Therefore

$$y^p \equiv \gamma\alpha^{-(n-2)}[z, x] \bmod I(G)^{p+1} + \mathbf{F}G\, I(G_2)^2,$$

if $n < p + 1$, and

$$y^p \equiv (\gamma - 1)[z, x] \bmod I(G)^{p+1} + \mathbf{F}G\, I(G_2)^2.$$

Now for $n < p + 1$, or $n = p + 1$ and $\gamma \neq 1$, we have y^p nonzero modulo $I(G)^{p+1} + \mathbf{F}G\, I(G_2)^2$, and thus $\gamma(\mathbf{F}^*)^{n-2}$ is determined, as required. The case $n = p + 1$ and $\gamma = 1$ is distinguished by the fact that

$$y^p = 0 \bmod I(G)^{p+1} + \mathbf{F}G\, I(G_2)^2,$$

that is by the p-th power map, as already seen at the beginning of the section.

COROLLARY 2.3. *Let G be a p-group of maximal class having an abelian maximal subgroup. If H is another group, and*

$$\frac{\mathbf{F}G}{\mathbf{F}G\, I(G_2)^2} \cong \frac{\mathbf{F}H}{\mathbf{F}H\, I(H_2)^2},$$

then $H/\Phi(H_2)$ is isomorphic to $G/\Phi(G_2)$.

This follows from Theorem 2.2, as $\mathbf{F}G\, I(\Phi(G_2)) \subseteq \mathbf{F}G\, I(G_2)^2$.

3. As we said in the introduction, we are not able to solve the isomorphism problem in general for the class of groups of maximal class with an abelian maximal subgroup.

However, in this section we show that any group which has a group algebra isomorphic to a group in the class, must itself belong to the class.

LEMMA 3.1. *Let G be a p-group of maximal class of order at most p^{p+1}. Let H be another group, such that $\mathbf{F}G \cong \mathbf{F}H$. Then H is a p-group of maximal class.*

Proof. For the terms $M_i(G)$ of the Brauer-Jennings-Zassenhaus series of G, we have

$$\left|\frac{M_1(G)}{M_2(G)}\right| = \left|\frac{G}{\Phi(G)}\right| = p^2,$$

$$\left|\frac{M_i(G)}{M_{i+1}(G)}\right| = \left|\frac{G^pG_i}{G^pG_{i+1}}\right| = \left|\frac{G_i}{G_{i+1}}\right| = p,$$

for $1 < i \leqq n - 2$, where $|G| = p^n$, as $G^p \leqq G_{n-1}$ by III.14.14 of [**3**].
Furthermore, either $G^p = 1$, so that $M_n(G) = G^pG_n = 1$,

$$\left|\frac{M_{n-1}(G)}{M_n(G)}\right| = p,$$

and all other terms are trivial, or $G^p = G_{n-1}$, so that

$$\left|\frac{M_i(G)}{M_{i+1}(G)}\right| = 1,$$

for all $n - 1 \leqq i < p$, and

$$\left|\frac{M_p(G)}{M_{p+1}(G)}\right| = p.$$

The order of the corresponding factors of H being the same, we see that if the first possibility holds, then $H^p = 1$, and H is immediately seen to be of maximal class. In the second case,

$$|H^p| = |M_p(G)| = p.$$

If, by way of contradiction, $H_{n-1} = 1$, we have $H_{n-2} \leqq Z(H)$, and

$$|H^pH_{n-2}| = |H^p| \cdot \left|\frac{H^pH_{n-2}}{H^p}\right| = p \cdot \left|\frac{M_{n-2}(G)}{M_{n-1}(G)}\right| = p^2,$$

so that $Z(H) \geqq H^pH_{n-2}$ has order at least p^2, against the fact that $p = |Z(G)| = |Z(H)|$ (see for instance [**9**], III.6.6).

THEOREM 3.2. *Let G be a p-group of maximal class with an abelian maximal subgroup. Let H be another group, such that* $\mathbf{F}G \cong \mathbf{F}H$.
Then H is also a p-group of maximal class with an abelian maximal subgroup.

Proof. By the previous results, we may assume $|G| > p^{p+1}$. By Corollary 2.3, $H/\Phi(H_2)$ is a p-group of maximal class isomorphic to $G/\Phi(G_2)$, of order p^{p+1}, with an abelian maximal subgroup $H_1/\Phi(H_2)$, where

$$H_1 = C_H(H_2/\Phi(H_2)).$$

We show first that the number of G-conjugacy classes of $\Phi(G_1)$, where G_1 is the abelian maximal subgroup of G, is the same as the number of H-conjugacy classes of $\Phi(H_1)$. Now the non central G-classes of $\Phi(G_1)$ are exactly all conjugacy classes of G which are p-powers, since $G^p \leqq \Phi(G_1)$. By [**4**], the number of conjugacy classes which are p-powers is the same for G and H. Moreover $H^p \leqq \Phi(H_1)$: therefore $\Phi(H_1)$ contains at least as many H-conjugacy classes as the number of G-conjugacy classes in $\Phi(G_1)$. Since this number is already as large as possible, the claim follows. In particular, all noncentral H-conjugacy classes of $\Phi(H_1)$ have length p.

Now let $x \in H_1 - H_2$. The p-group of maximal class $H/\Phi(H_2)$ is isomorphic to $G/\Phi(G_2)$ by Corollary 2.3. Since $|G| > p^{p+1}$, III.14.16 of [**3**] yields $x^p \in \Phi(H_1) - \Phi(H_2)$. Since $Z(H)$ is order p, it is contained in $\Phi(H_2) \neq 1$, so that $x^p \notin Z(H)$. Therefore $C_H(x) = C_H(x^p)$ has index p in H (compare [**8**]), since the conjugacy class of $x^p \in \Phi(H_1)$ is a p-th power, as seen above. In fact this centralizer is H_1, the reason being that, in the p-group of maximal class $H/\Phi(H_2)$, the centralizer of $x\Phi(H_2)$ is $H_1/\Phi(H_2)$.

Thus $x \in Z(H_1)$. Now the normal closure of $\langle x \rangle$ modulo $\Phi(H_2)$ is H_1, therefore the normal closure in H of $\langle x \rangle$ is H_1. It follows that H_1 is abelian. Now G has $|G|/p^{n-2} + p^2 - 1$ conjugacy classes ([**3**], III.14.23), so this number, being the dimension of the center of the group algebra, is the same for H. But the number of conjugacy classes of H that are contained in H_1 is $|H|/p^2 + p - 1$. It follows that the $|H| - |H|/p$ elements of $H - H_1$ are distributed among $p(p-1)$ classes. It is thus easy to see that all elements of $H - H_1$ have centralizer in H of order p^2, and thus H is of maximal class, again by [**3**], III.14.23.

Acknowledgment. We are grateful to Consiglio Nazionale delle Ricerche (Italy) for supporting the first author's stay in Trento as a Visiting Professor.

References

1. N. Blackburn, *On a special class of p-groups*, Acta Math. *100* (1958), 45–92.

2. J. Carlson, *Periodic modules over modular group algebras*, J. London Math. Soc. *15* (1977), 431–436.

3. B. Huppert, *Endliche Gruppen I* (Springer, Berlin, 1967).

4. M. M. Parmenter and C. Polcino Milies, *A note on isomorphic group rings*, Bol. Soc. Bras. Mat. *12* (1981), 57–59.

5. D Passman, *The group algebras of groups of order p^4 over a modular field*, Michigan Math. J. *12* (1965), 405–415.

6. ——— *Algebraic structure of group rings* (Interscience, New York, 1977).

7. R. Sandling, *The isomorphism problem for group rings: a survey*, Lecture Notes in Mathematics *1142* (Springer, Berlin, 1985), 256–288.

8. S. K. Sehgal, *On the isomorphism of group algebras*, Math. Z. *95* (1967), 71–75.

9. ——— *Topics in group rings* (Dekker, New York, 1978).

Warsaw University,
Biaįystok, Poland;
Università degli Studi di Trento,
Povo, Italy