Publl. Math. Debrecen
71/1-2 (2007), 83–93

A note on the modular group algebras of odd p-groups of M-length three

By MARTIN HERTWECK (Stuttgart)

Dedicated to Prof. Adalbert Bovdi on the occasion of his 70th birthday

Abstract. Let G be a finite p-group of odd order. It is shown that if the Brauer–Jennings–Zassenhaus series (also termed M-series) of G has length three, then the isomorphism type of G is determined by its modular group algebra kG, k being the field with p elements.

1. Introduction

The (still open) modular isomorphism problem is about the question whether for a finite p-group G, there are possibly other groups H, non-isomorphic to G, such that $kG \cong kH$ as algebras, where k denotes the field with p elements. If this is not the case one says that G is determined by its modular group algebra. More generally, a property of G is said to be *determined* (by its modular group algebra) if any other group basis of kG also has this property, with a *group basis* of kG being a subgroup of the group of units of kG which forms a basis of the underlying vector space. In the present context, an *invariant* of kG will simply be a property of a group basis which is determined by kG.

Many fundamental observations on various isomorphism problems for group rings were published during the 1970s (or earlier) and discussions of these problems were included in the books of Passman [11] (Chapter 14) and Sehgal [17]

Mathematics Subject Classification: Primary: 16S34, 20D15; Secondary: 16U60.
Key words and phrases: p-group, Jennings basis, modular isomorphism problem.

(Chapter III), thus giving further impetus to the whole subject. Concerning the modular isomorphism problem, Sandling's 1984 survey [15] still gives an impression of the state of the art, cf. [9]. Bovdi's more recent survey [5] on units in modular group algebras may be chosen for some complementary reading.

Throughout this paper, G will denote a finite p-group. Jennings introduced certain bases of kG (as a vector space) which can easily be derived from the group bases and which are compatible with the radical filtration of kG (for details, see Chapter 3, §3 and Chapter 11, §1 from [11]). This laid the foundation for much of the work to follow, and ours is not an exception. Such a Jennings basis, obtained from the group basis G, is defined in terms of the Brauer–Jennings–Zassenhaus series for G, called M-series by Jennings, which is defined inductively by $\mathrm{M}_1(G) = G$ and for $i \geq 2$

$$\mathrm{M}_i(G) = \langle [G, \mathrm{M}_{i-1}(G)], \mathrm{M}_{\lceil i/p \rceil}(G)^p \rangle$$

where $\lceil i/p \rceil$ is the smallest integer $\geq i/p$. This means that the M-series is the fastest descending p-restricted N-series, and Jennings has shown that this series coincides with the series of dimension subgroups, defined by

$$\mathrm{D}_i(G) = G \cap (1 + \mathrm{I}(kG)^i)$$

where $\mathrm{I}(kG)$ denotes the augmentation ideal of kG. The aim of this note is to prove the following result (or rather Theorem′ below from which it immediately follows).

Theorem. *Let p be an odd prime. Then for a finite p-group G, the quotient $G/\mathrm{M}_4(G)$ is determined by its modular group algebra kG over the field k with p elements.*

To put it in perspective: For arbitrary p, Jennings has shown that the ranks of the elementary abelian quotients $\mathrm{M}_i(G)/\mathrm{M}_{i+1}(G)$ are determined, and Passi and Sehgal [10] showed that $G/\mathrm{M}_3(G)$ is determined. An important generalization was given by Sandling [16] who showed that the largest central-elementary-by-abelian quotient of G, now called Sandling-quotient, is determined. All these quotients in particular have class 2, while $G/\mathrm{M}_4(G)$ may have class 3. More generally, Passi and Sehgal proved that all the quotients $\mathrm{M}_i(G)/\mathrm{M}_{i+2}(G)$ are determined by kG, a result which was later improved by Ritter and Sehgal [12] when showing that $\mathrm{M}_i(G)/\mathrm{M}_{2i+1}(G)$ is determined (still, all quotients are central-elementary-by-abelian). Further work may show whether our result extends in this direction.

Nowadays there are powerful computer algebra systems available – in the present context, we mention GAP [7] – which provide a convenient programming environment as well as databases of groups of "small" order. We also mention the GAP package LAGUNA [6] which provides functionality for calculation of the group of units of the modular group algebra of a finite p-group and which soon will provide tools related to the modular isomorphism problem.

One line of reasoning about the modular isomorphism problem suggests to work through these databases to find either a counterexample or to settle the problem for a specific group order. Then the first step consists in splitting the cluster of all (isomorphism classes of) groups of some fixed order p^n into sets of smaller clusters by successively considering different group-theoretical invariants of kG. At the end of this process (i.e., when "running out" of invariants), one is left, at best, with only a few clusters containing only a few groups each. Even only rudimentary programming skills allow everyone to reproduce such cluster splittings on the own PC. To deal with the remaining clusters it seems inevitable to do a large number of calculations inside the group algebras themselves. The stand-alone program `SISYPHOS`[1] written by Wursthorn served this purpose and enabled its author to demonstrate that the groups of order 2^6 and 2^7 are determined by their modular group algebras (see [18], [3], and [9]).

In [3, Theorem 7], the most common and powerful group-theoretical invariants so far known are listed (cf. also [15] and [9]). Among them (item 3) are the above-mentioned sections along the M-series, but Wursthorn pointed out that "It should be noted that invariant 3. usually does not distinguish any more groups that share all of the other invariants." Not surprisingly, our new invariant has more potential. The groups of order 3^6 provide a good example: Splitting the 504 groups of order 3^6 using the common group-theoretical invariants leaves 174 groups (all of them metabelian) distributed among 76 clusters: $[[2,62],[3,8],[4,4],[5,2]]$, meaning that 62 clusters consist of pairs, and so on.[2] Use of the new invariant eliminates further 110 groups: 64 groups in 29 clusters will be left, with distribution $[[2,24],[3,4],[4,1]]$.

One may call "small group algebra" any quotient algebra of kG into which each group basis of kG embeds. Though it is well-known that in general G is not determined by a small group algebra, not even in "classical cases" (see [1, Section 4], [8]), many authors examined the embedding of group bases into such

[1] In the future, GAP and LAGUNA should provide the full functionality of `SISYPHOS`.

[2] The referee pointed out that the nilpotency class of G is determined if G has cyclic derived subgroup [2]. Use of this invariant would eliminate a pair and one group from a triple from our list.

quotients. To quote Salim and Sandling from one of their 1996 papers [14]: “One can chart a progression in recent papers on the modular isomorphism problem. Each sets out to deduce as much as possible from a quotient algebra of FG.[3] The ideals which are divided out have become smaller and smaller, resulting in larger and larger sections of FG susceptible to purposeful analysis. At each stage a more complicated group basis becomes embeddable in the quotient algebra and thence its structure made accessible.” In retrospect this sounds quite optimistic. To the best of our knowledge, the last paper where this strategy was successfully applied dates back to 1999 when Bagiński [1], only using information provided by the quotient algebra $kG/\mathrm{I}(kG')^2kG$, showed that an elementary abelian-by-cyclic p-group G is determined.

The ideas addressed above revolve around the problem of the existence of a normal complement for G in the group $\mathrm{V}(kG)$ of augmentation one units in kG, a problem for which only a few results are known (see Section 3 in [9] for some references). We remark that it is still an open problem whether a finite p-group G admitting a normal complement in $\mathrm{V}(kG)$ is determined by kG.[4]

Our theorem resulted from the attempt to find *directly* large normal subgroups in $\mathrm{V}(kG)$ such that each group basis embeds into the quotient. In fact, the theorem follows immediately from:

Theorem′. *Let p be an odd prime, let G be a finite p-group, and set $\mathcal{V} = \mathrm{V}(kG)$. Then $\mathcal{V}$ has a normal subgroup $\mathcal{N}$ such that $\mathcal{V}/\mathcal{N}$ is naturally isomorphic to $H/\mathrm{M}_4(H)$ for each group basis H of kG.*

For the proof, we may assume that $\mathrm{M}_4(G) = 1$. The normal subgroup $\mathcal{N}$ will emerge from the following procedure. We take a Jennings basis of kG specified by generators $g_1, \dots, g_n$ of G and let S be the span of all basis elements which do not lie in $G - 1$. Then S is multiplicatively closed since $\mathrm{I}(kG)^4 \subseteq S$. Thus if S would be invariant under conjugation with the g_i, then $1 + S$ would be the desired normal subgroup since S is “complementary” to the Zassenhaus ideals, but this is rarely the case. So we have a close look at the conjugates of the basis elements spanning S which, interestingly enough, reveals an almost canonical way of how to modify the basis elements so to get a modified, G-invariant subspace S' and one can set $\mathcal{N} = 1 + S'$. The modified basis elements reflect the relations between the pc-generators $g_1, \dots, g_n$.

A striking feature is that the terms which have to be added to the basis

[3] F stands for the field with p elements.

[4] In [13], it is claimed that the answer is in the affirmative, but the proof of Theorem 3.2 contains an obvious mistake (on page 617).

elements have a factor of 1/2. This reminds us that there is no perfect correspondence between (discrete) p-groups and Lie algebras of characteristic p, due to the non-existence of mutually-inverse functions exp and log; in general, the best one can consider are the truncations

$$\exp(x) = 1 + x + \mathscr{O}(x^2), \qquad \log(1+x) = x + \mathscr{O}(x^2).$$

Nevertheless, the hope may be entertained that further investigations along the line presented here will actually lead to connections between group and Lie-algebra objects!

In the next section, we present some well-known facts as well as a small example which hopefully eases the access to the main idea of the proof. The necessary calculations are given in the final section.

2. Preliminaries and an illustrating example

We briefly introduce the notions of Jennings basis and Zassenhaus ideal. Suppose that G has order p^n. A set of pc-generators of G is a sequence $g_1, \dots, g_n$ of generators of G that have the property that for each i between 1 and n the elements $g_{i+1}, \dots, g_n$ generate a subgroup of order p^{n-i} that is normal in G. Notice that $g_i^p \in \langle g_{i+1}, \dots, g_n \rangle$. (The prefix "pc" stands for "power-commutator.") It is possible to choose pc-generators $g_1, \dots, g_n$ such that the first r generators lie in $G \setminus \mathrm{M}_2(G)$, the next s generators lie in $\mathrm{M}_2(G) \setminus \mathrm{M}_3(G)$, and so on. If a generator g_i lies in $\mathrm{M}_j(G) \setminus \mathrm{M}_{j+1}(G)$, then $j = w(g_i)$ is called its *weight.* There are p^n products of the form $(g_1 - 1)^{\nu_1} \cdots (g_n - 1)^{\nu_n}$ with $0 \leq \nu_i < p$. The *weight* of such a product is $\sum w(g_i)\nu_i$. Jennings' theorem states that the set of products of weight j lie in $\mathrm{I}(kG)^j$, and forms a basis of $\mathrm{I}(kG)^j$ modulo $\mathrm{I}(kG)^{j+1}$. Thus the set $\mathscr{B}$ of all these products is a basis of kG, called a Jennings basis, which is compatible with the radical filtration. The set $1 + \mathscr{B} \setminus \{1\}$ consists of pc-generators for $\mathrm{V}(kG)$, the group of augmentation one units of kG. We remark that Bovdi noted that a smaller generating set of $\mathrm{V}(kG)$ possibly may be obtained from this set by leaving out certain elements (see [4] or [5, Section 10]).

The Zassenhaus ideals $\mathrm{H}_i(kG)$ of kG are defined in terms of kG alone, but for us the essential point will be that these ideals also have the alternative description $\mathrm{H}_i(kG) = \mathrm{M}_i(G) - 1 + \mathrm{I}(kG)^{i+1}$ which – on first sight – seems to depend on the chosen group basis G of kG (see [10]). Here is a consequence of that result. Suppose that we are given a subspace S' of $\mathrm{I}(kG)$ which is multiplicatively closed, so that $\mathcal{S} = 1 + S'$ is a subgroup of $\mathrm{V}(kG)$. Suppose further that $S' \cap \mathrm{H}_i(kG) \subseteq$

$\mathrm{I}(kG)^{i+1}$ for all i less than a given natural number l. Then $H \cap \mathcal{S} \leq \mathrm{M}_l(H)$ for each group basis H of kG. Indeed, it suffices to show this only for the group basis G. Let $g \in G \cap \mathcal{S}$. Then $g \in \mathrm{M}_1(G)$ and as long as $i < l$ and $g \in \mathrm{M}_i(G)$ we have $g - 1 \in S' \cap \mathrm{H}_i(kG) \subseteq \mathrm{I}(kG)^{i+1}$, that is, $g \in \mathrm{M}_{i+1}(G)$. Thus $g \in \mathrm{M}_l(G)$. We may use a Jennings basis of kG to obtain such subspaces. More precisely, we can proceed as follows. Fix some natural number l. Let $\mathscr{B}$ be a Jennings basis of kG consisting, as described above, of products $(g_1 - 1)^{\nu_1} \cdots (g_n - 1)^{\nu_n}$. Let $\mathscr{C}$ be the set of all basis elements in $\mathscr{B}$ for which $\sum_i \nu_i \geq 2$, and let C be the subspace of kG spanned by $\mathscr{C}$. Let D be the subspace spanned by the $g_i - 1$, so that $\mathrm{I}(kG) = C \oplus D$. Notice that $\mathrm{H}_i(kG) \subseteq D + \mathrm{I}(kG)^{i+1}$, so $(C + \mathrm{I}(kG)^l) \cap \mathrm{H}_i(kG) \subseteq \mathrm{I}(kG)^{i+1}$ for $i < l$ since the Jennings basis is adapted to the radical filtration. Thus the subspace $S = C + \mathrm{I}(kG)^l$ satisfies the above condition of being "complementary" to the Zassenhaus ideals, but in general this subspace will not be multiplicatively closed. Notice that if S happens to be multiplicatively closed, then $\mathcal{S} = 1 + S$ is a subgroup of $\mathrm{V}(kG)$ satisfying $\mathrm{V}(kG) = H\mathcal{S}$ and $H \cap \mathcal{S} = \mathrm{M}_l(H)$ for each group basis H of kG. Then the question arises as to whether $\mathcal{S}$ is a normal subgroup of $\mathrm{V}(kG)$, i.e., whether S is invariant under conjugation with the g_i. In principal, there are two possibilities to find a remedy. First, one could try to remove "interfering" elements from $\mathscr{C}$, starting with elements of weight $l-1$, so to obtain a smaller set $\mathscr{C}'$ spanning a subspace C' with $\mathcal{S} = 1 + C' + \mathrm{I}(kG)^l$ having all the desired properties (cf. [9, Section 3]). While this will always work, it has the disadvantage of producing (normal) subgroups $\mathcal{S}$ which are possibly smaller than one would like to expect. Nevertheless, this kind of reasoning led to a practicable approach for the groups of order 2^6, see [9]. Second, one could try to "modify" the elements from $\mathscr{C}$ to obtain a modified set $\mathscr{C}'$ spanning a subspace C' (still complementing D in $\mathrm{I}(kG)$) with $\mathcal{S} = 1 + C' + \mathrm{I}(kG)^l$ again having all the desired properties. Thereby, one might be guided by the shape of the G-conjugates of the elements of $\mathscr{C}$, starting with conjugates of elements of weight 2. This is the approach taken in this note.

An example. We found our theorem while considering the group G of order 729 which has pc-generators a_1, a_2, b_1, c_1, c_2, c_3 and relations

$$a_1^3 = c_1, \quad a_2^3 = c_2, \quad a_2^{a_1} = a_2 b_1, \quad b_1^{a_1} = b_1 c_2, \quad b_1^{a_2} = b_1 c_3.$$

Note that only nontrivial relations are listed. For example, there is no relation involving b_1^3, so it is understood that $b_1^3 = 1$. Likewise we have that the c_i are in the center of G since there is no relation listed that has the form $g^{-1} c_i g$ with a pc-generator g listed before c_i.

We remark that G has elementary abelian derived subgroup $G' = \langle b_1, c_2, c_3\rangle$, and $[G, G'] = \langle c_2, c_3\rangle$, so G is of class 3.

The catalogue number of G in the Small Groups Library in GAP [7] is $[729, 10]$, and G cannot be distinguished from the group H with number $[729, 12]$ by the common group-theoretical invariants of kG. (A presentation of H is obtained by replacing the second relation above by $a_2^3 = c_3$.) This is why we had a look at G.

The M-series of G is given by

$$G > \mathrm{M}_2(G) = \langle b_1, c_1, c_2, c_3\rangle > \mathrm{M}_3(G) = \langle c_1, c_2, c_3\rangle > \mathrm{M}_4(G) = 1.$$

We shall write $A_i = a_i - 1$, $B_i = b_i - 1$ and $C_i = c_i - 1$. The Jennings basis of kG specified by the given pc-generators is depicted in Figure 1.

$$\begin{array}{c}
\boldsymbol{1}\\
\boldsymbol{A_1} \quad \boldsymbol{A_2}\\
\boldsymbol{B_1} \quad A_1^2 \quad A_1A_2 \quad A_2^2\\
\boldsymbol{C_1} \quad \boldsymbol{C_2} \quad \boldsymbol{C_3} \quad A_1B_1 \quad A_1^2A_2 \quad A_1A_2^2 \quad A_2B_1\\
\vdots
\end{array}$$

Figure 1. A Jennings basis of kG, written out up to $\mathrm{I}(kG)^4$. The basis elements $\mathscr{C}$ in the highlighted region span a subspace C which is obviously multiplicatively closed, but not G-invariant.

The interested reader is encouraged to verify the following calculations immediately by hand (congruences are modulo $\mathrm{I}(kG)^4$):

$$\begin{aligned}
(A_1^2)^{a_2} &\equiv A_1^2 + (A_1B_1 - C_2), & (A_2^2)^{a_1} &\equiv A_2^2 - (A_2B_1 - C_3),\\
(A_1A_2)^{a_1} &\equiv A_1A_2 + A_1B_1, & (A_1A_2)^{a_2} &\equiv A_1A_2 - A_2B_1 - C_3,\\
(B_1)^{a_1} &\equiv B_1 + C_2, & (B_1)^{a_2} &\equiv B_1 + C_3.
\end{aligned}$$

The first line suggests that the basis elements A_1B_1 and A_2B_1 of weight 3 should be altered as shown in Figure 2 (the reason why we have written $-1 = \frac{1}{2}$ will become evident when handling the general case). One cannot help thinking that now something should be added on both sides of the equations displayed in line two, and the third line suggests precisely what is to do. This leaves us with the satisfactory picture shown in Figure 2.

$$\begin{array}{c}
\mathbf{1}\\
\boldsymbol{A_1} \quad \boldsymbol{A_2}\\
\boldsymbol{B_1} \quad A_1^2 \quad A_1A_2+\tfrac{1}{2}B_1 \quad A_2^2\\
\boldsymbol{C_1} \quad \boldsymbol{C_2} \quad \boldsymbol{C_3} \quad A_1B_1+\tfrac{1}{2}C_2 \quad A_1^2A_2 \quad A_1A_2^2 \quad A_2B_1+\tfrac{1}{2}C_3\\
\vdots
\end{array}$$

Figure 2. The modified Jennings basis of kG. The basis elements $\mathscr{C}'$ in the highlighted region span a G-invariant subspace C', so $\mathcal{N} = 1 + C'$ is a normal complement to any group basis of kG in $\mathrm{V}(kG)$.

3. Proof of the theorem

We start right off doing the necessary calculations. Let G be a finite p-group. Throughout, "$\equiv$" shall mean "congruence modulo $\mathrm{I}(kG)^4$." Recall that for all $g \in G$ and $l \in \mathbb{N}$, we have $g-1 \in \mathrm{I}(kG)^l$ if and only if $g \in \mathrm{M}_l(G)$. First, we record a few well-known calculation rules. Let $g, h \in G$ and $x, y, x_1, \ldots, x_m \in \mathrm{M}_2(G)$. From the identities

$$gh - 1 = (g-1) + (h-1) + (g-1)(h-1) \tag{1}$$

$$hg([g,h]-1) = (g-1)(h-1) - (h-1)(g-1) \tag{2}$$

it follows that

$$(x_1 \cdots x_m) - 1 \equiv (x_1 - 1) + \ldots + (x_m - 1) \tag{3}$$

$$[g,h] - 1 \equiv -([h,g]-1) \tag{4}$$

$$[x,h] - 1 \equiv (x-1)(h-1) - (h-1)(x-1) \tag{5}$$

$$[xy,h] - 1 \equiv ([x,h]-1) + ([y,h]-1) \tag{6}$$

Indeed, (3) is immediate from (1), and (4) also follows from (1) since $[g,h] \in \mathrm{M}_2(G)$ and $([g,h]-1) + ([h,g]-1) = ([g,h]-1) + ([g,h]^{-1}-1)$. Last, (5) is immediate from (2) since $[x,h] \in \mathrm{M}_3(G)$, and (6) follows from (5) and (3).

Now let $a_1, a_2, \ldots$ be elements of G. We set $x_{ij} = [a_j, a_i]$, that is, $a_j^{a_i} = a_j x_{ij}$. We shall write $A_i = a_i - 1$ and $X_{ij} = x_{ij} - 1$.

The crucial calculation—use (3) twice for the last step:

$$\begin{aligned}
(x_{ij}-1)^{a_l} &= (a_j^{-1}a_i^{-1}a_ja_i - 1)^{a_l} = x_{lj}^{-1}a_j^{-1}x_{li}^{-1}a_i^{-1}a_jx_{lj}a_ix_{li} - 1\\
&= x_{lj}^{-1}[a_j, x_{li}]x_{li}^{-1}[a_j, a_i]x_{lj}[x_{lj}, a_i]x_{li} - 1
\end{aligned}$$

$$\equiv ([a_j, x_{li}] - 1) + (x_{ij} - 1) + ([x_{lj}, a_i] - 1) + \underbrace{([x_{lj}, x_{li}] - 1)}_{\equiv 0 \text{ by } (5)}$$

together with a little cosmetic (4) shows that for all i, j, l:

$$(X_{ij})^{a_l} = X_{ij} + ([x_{lj}, a_i] - 1) - ([x_{li}, a_j] - 1). \tag{7}$$

Furthermore,

$$(A_i A_j)^{a_l} = (a_i x_{li} - 1)(a_j x_{lj} - 1) \equiv (A_i + X_{li})(A_j + X_{lj})$$

by (1), and

$$X_{li} A_j \equiv A_j X_{li} + ([x_{li}, a_j] - 1)$$

by (5), so

$$(A_i A_j)^{a_l} \equiv A_i A_j + A_i X_{lj} + A_j X_{li} + ([x_{li}, a_j] - 1). \tag{8}$$

Setting $i = j$, we obtain in particular

$$(A_i^2)^{a_l} \equiv A_i^2 + 2 A_i X_{li} + ([x_{li}, a_i] - 1). \tag{9}$$

Now suppose that p is odd. Then it follows from (7) and (8) that for all i, j, l:

$$\begin{aligned}\left(A_i A_j + \frac{1}{2} X_{ij}\right)^{a_l} \equiv &\left(A_i A_j + \frac{1}{2} X_{ij}\right) \\ &+ A_i X_{lj} + \frac{1}{2}([x_{lj}, a_i] - 1) + A_j X_{li} + \frac{1}{2}([x_{li}, a_j] - 1).\end{aligned} \tag{10}$$

Finally, fix some indices i, j, l and suppose that $x_{lj} = x_1^{\nu_1} \cdots x_m^{\nu_m}$, all x_s in $\mathrm{M}_2(G)$ and $0 \leq \nu_s < p$. Then by (3) and (6),

$$A_i X_{lj} \equiv \nu_1 A_i X_1 + \ldots + \nu_s A_i X_s, \tag{11}$$

$$\frac{1}{2}([x_{lj}, a_i] - 1) \equiv \sum_{s=1}^{m} \nu_s \frac{1}{2}([x_s, a_i] - 1). \tag{12}$$

We are well prepared to give a proof of Theorem′. As a matter of fact, what is left to do is just to set up a lot of notation and to check trivial things. The group G has a system of pc-generators

$$a_1, \ldots, a_r, b_1, \ldots, b_s, c_1, \ldots, c_t, \ldots$$

such that the a_i lie in $G \setminus \mathrm{M}_2(G)$, the b_i lie in $\mathrm{M}_2(G) \setminus \mathrm{M}_3(G)$, the c_i lie in $\mathrm{M}_3(G) \setminus \mathrm{M}_4(G)$ and the remaining generators lie in $\mathrm{M}_4(G)$. Actually, it can happen that the M-series “stutters.” If, e.g., $\mathrm{M}_3(G) = \mathrm{M}_4(G)$, then it is understood that $t = 0$ and $\{c_1, \dots, c_t\} = \emptyset$. The given generators give rise to a Jennings basis of kG. We set

$$\begin{aligned}
\mathcal{A}_* &= \{A_1, \dots, A_r\},\ \mathcal{B}_* = \{B_1, \dots, B_s\},\ \mathcal{C}_* = \{C_1, \dots, C_t\},\\
\mathcal{A}_{**} &= \{A_i A_j \mid 1 \le i < j \le r\},\ \mathcal{A}_*^2 = \{A_1^2, \dots, A_r^2\},\\
\mathcal{A}_*\mathcal{B}_* &= \{A_i B_j \mid 1 \le i \le r,\ 1 \le j \le s\},\\
\mathcal{A}_{***} &= \{A_i A_j A_l \mid 1 \le i \le j \le l \le r,\ \text{if } p = 3 \text{ not } i = j = l\}.
\end{aligned}$$

In the Jennings basis, we have the subsets of elements of

$$\begin{aligned}
&\text{weight 1:} && \mathcal{A}_*,\\
&\text{weight 2:} && \mathcal{B}_* \cup \mathcal{A}_{**} \cup \mathcal{A}_*^2,\\
&\text{weight 3:} && \mathcal{C}_* \cup \mathcal{A}_*\mathcal{B}_* \cup \mathcal{A}_{***}.
\end{aligned}$$

We set

$$\begin{aligned}
(\mathcal{A}_{**})' &= \left\{A_i A_j + \frac{1}{2}([a_j, a_i] - 1) \mid 1 \le i < j \le r\right\},\\
(\mathcal{A}_*\mathcal{B}_*)' &= \left\{A_i B_j + \frac{1}{2}\big([b_j, a_i] - 1\big) \mid 1 \le i \le r, 1 \le j \le s\right\}
\end{aligned}$$

and let C' be the k-span of $(\mathcal{A}_{**})' \cup \mathcal{A}_*^2 \cup (\mathcal{A}_*\mathcal{B}_*)' \cup \mathcal{A}_{***} \cup \mathrm{I}(kG)^4$. Further, let D be the k-span of $\mathcal{A}_* \cup \mathcal{B}_* \cup \mathcal{C}_*$. Obviously, C' is multiplicatively closed since it is contained in $\mathrm{I}(kG)^2$. Thus $\mathcal{N} = 1 + S'$ is a subgroup of $\mathrm{V}(kG)$. Since $\mathrm{I}(kG) = D \oplus C'$, it follows that $\mathrm{V}(kG) = H\mathcal{N}$ and $H \cap \mathcal{N} = \mathrm{M}_4(H)$ for any group basis H of kG, see the discussion in Section 2 concerning the Zassenhaus ideals. Moreover, C' is invariant under conjugation with elements of G. Therefore, it suffices to show that C' is invariant under conjugation with the a_l which holds since conjugation with an a_l maps $\mathcal{A}_*^2$ and $(\mathcal{A}_{**})'$ into C' by (9) respectively (10) and (11), (12). Thus $\mathcal{N}$ is a normal subgroup of $\mathrm{V}(kG)$, and the proof of the theorem is complete.

References

[1] Czesław Bagiński, On the isomorphism problem for modular group algebras of elementary abelian-by-cyclic p-groups, *Colloq. Math.* **82**, no. 1 (1999), 125–136.

[2] Czesław Bagiński and Alexander Konovalov, The modular isomorphism problem for finite p-groups with a cyclic subgroup of index p^2, Proceedings of Groups St Andrews 2005, London Mathematical Society Lecture Note Series, *Cambridge University Press.*

[3] Frauke M. Bleher, Wolfgang Kimmerle, Klaus W. Roggenkamp and Martin Wursthorn, Computational aspects of the isomorphism problem, Algorithmic algebra and number theory (Heidelberg, 1997), *Springer*, *Berlin*, 1999, 313–329.

[4] Adalbert Bovdi, Generators of the units of the modular group algebra of a finite p-group, Methods in ring theory (Levico Terme, 1997), Vol. 198, Lecture Notes in Pure and Appl. Math., *Dekker*, *New York*, 1998, 49–62.

[5] Adalbert Bovdi, The group of units of a group algebra of characteristic p, *Publ. Math. Debrecen* **52**, no. 1–2 (1998), 193–244.

[6] V. Bovdi, A. Konovalov, R. Rossmanith and C. Schneider, LAGUNA – Lie AlGebras and UNits of group Algebras, Version 3.3.1, 2005, (http://ukrgap.exponenta.ru/laguna.htm).

[7] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4, 2005, (http://www.gap-system.org).

[8] Martin Hertweck and Marcos Soriano, Parametrization of central Frattini extensions and isomorphisms of small group rings, 2005 (*to appear in* Israel Journal of Mathematics), http://www.igt.uni-stuttgart.de/LstDiffgeo/Hertweck/.

[9] Martin Hertweck and Marcos Soriano, On the modular isomorphism problem: groups of order 2^6, 2005, 1–37 (*to appear in* Groups, Rings & Algebras; Papers in Honor of Donald S. Passman's 65-th Birthday. Edited by: W. Chin, J. Osterburg, and D. Quinn, CONM book series.), http://www.igt.uni-stuttgart.de/ LstDiffgeo/Hertweck/.

[10] Inder Bir S. Passi and Sudarshan K. Sehgal, Isomorphism of modular group algebras, *Math. Z.* **129** (1972), 65–73.

[11] Donald S. Passman, The algebraic structure of group rings, Pure and Applied Mathematics, *Wiley-Interscience [John Wiley & Sons]*, *New York*, 1977, xiv+720.

[12] Jürgen Ritter and Sudarshan Sehgal, Isomorphism of group rings, *Arch. Math. (Basel)* **40**, no. 1 (1983), 32–39.

[13] Frank Röhl, Unit groups of completed modular group algebras and the isomorphism problem, *Proc. Amer. Math. Soc.* **111**, no. 3 (1991), 611–618.

[14] Mohamed A. M. Salim and Robert Sandling, The modular group algebra problem for small p-groups of maximal class, *Canad. J. Math.* **48**, no. 5 (1996), 1064–1078.

[15] Robert Sandling, The isomorphism problem for group rings: a survey, Orders and their applications (Oberwolfach, 1984), Vol. 1142, Lecture Notes in Math., *Springer*, *Berlin*, 1985, 256–288.

[16] Robert Sandling, The modular group algebra of a central-elementary-by-abelian p-group, *Arch. Math. (Basel)* **52**, no. 1 (1989), 22–27.

[17] Sudarshan K. Sehgal, Topics in Group Rings, Vol. 50, Monographs and Textbooks in Pure and Applied Math., *Marcel Dekker Inc.*, *New York*, 1978.

[18] Martin Wursthorn, Isomorphisms of modular group algebras: an algorithm and its application to groups of order 2^6, *J. Symbolic Comput.* **15**, no. 2 (1993), 211–227.

MARTIN HERTWECK
UNIVERSITÄT STUTTGART
FACHBEREICH MATHEMATIK, IGT
PFAFFENWALDRING 57
70550 STUTTGART
GERMANY

E-mail: hertweck@mathematik.uni-stuttgart.de

(Received October 27, 2005; revised August 22, 2006)