*J. Austral. Math. Soc.* (*Series A*) **61** (1996), 229–237

# THE MODULAR GROUP ALGEBRA PROBLEM FOR GROUPS OF ORDER $p^5$

**MOHAMED A. M. SALIM and ROBERT SANDLING**

(Received 5 August 1994; revised 23 February 1996)

Communicated by R. Howlett

**Abstract**

We show that $p$-groups of order $p^5$ are determined by their group algebras over the field of $p$ elements. Many cases have been dealt with in earlier work of ourselves and others. The only case whose details remain to be given here is that of groups of nilpotency class 3 for $p$ odd.

1991 *Mathematics subject classification* (*Amer. Math. Soc.*): primary 20C05; secondary 16S34, 20D15.
*Keywords and phrases*: modular group algebra, $p$-group, isomorphism problem.

The modular group algebra problem has come to mean the issue of whether, for a finite $p$-group $G$ and a field $F$ of characteristic $p$, the algebra structure of the group algebra $FG$ contains enough information for the isomorphism type of the group $G$ to be deduced. This paper contributes the following positive result to the efforts at the problem's resolution.

THEOREM 1. *Let $G$ be a group of order $p^5$ for some prime $p$. Let $F$ be the field of $p$ elements. Then $G$ is determined up to isomorphism by the group algebra $FG$.*

The problem is a long-standing one. Its history and progress is surveyed in [18, §6]. The present result has been anticipated by L. G. Kovacs and M. F. Newman (see [19]) who have not circulated their work. In any event the approach taken here seems to be novel. In previous efforts at characterising groups of a given order from their modular group algebras, the starting point has been a pre-existing list of the groups in question. There is a list of the groups of order $p^5$, $p$ odd [5]. While used for development and referred to as an aid to the reader, the logical necessity for James' or any other list was wholly avoided in the thesis [15] on which this paper is based (albeit at the expense of reconstructing some of the arguments involved in the preparation of such lists). Although no list is used here, to an extent we have availed ourselves of lists in the papers [20, 17] which support this one in order to keep our exposition within conventional bounds.

One treatment of the $p^5$, $p \geq 5$, case which relied on a list was that of [10] in which the dimension subgroups $D_n = D_n(FG)$ were calculated (here $D_n = G \cap (1 + I^n)$, where $I = I(FG)$ is the augmentation ideal of $FG$). This data does not go far in distinguishing these groups by means of their group algebras. The calculations do facilitate the use in this case of a stronger invariant, the graded restricted Lie algebra $\mathscr{L}(G) := \bigoplus D_n/D_{n+1}$ [18, 6.18]. For small $p$ this has the potential for differentiating some individual groups; an example for $p = 3$ is given in [15, §6.1.1]. As this Lie algebra determines the graded associative algebra $\bigoplus I^n/I^{n+1}$ (see [12, §VIII.5]), information from the latter is already available from $\mathscr{L}(G)$; the associative algebra has been used in the isomorphism problem in the past, originally in [3, p.166] and also in [13, 2, 21].

For $p = 2$, the theorem is already in the literature. The primary reference is the thesis work of Makasikis [9] (but see [18, Note on 6.33]). An alternative treatment can be found in [11] or gleaned from the work on the groups of order $2^6$ in [21]. Some of the hardest cases are metacyclic, for which there is now a simplified treatment in [20]. Even the cohomology ring goes a long way in distinguishing the groups of order 32 [14].

We will assume henceforth that $p$ is odd. Let $G$ be a group of order $p^5$. We have already shown in [17] that, if $G$ has maximal class, then $G$ is determined by $FG$. We may assume then that $G_4 = 1$. By [19] we may also assume that $G_2^p G_3 \neq 1$. We begin by establishing some properties of the remaining groups.

PROPOSITION 2. *Let $G$ be a $p$-group of order $p^5$, $p$ odd. Suppose that $G_4 = 1$. Then the Frattini subgroup of $G$ is abelian.*

PROOF. We may assume that $|\Phi(G)| = p^3$. Let $N$ be a normal subgroup of order $p^2$ contained in $\Phi(G)$. Since $G/C_G(N)$ is isomorphic to a subgroup of the automorphism group of $N$, $|G : C_G(N)| \leq p$ and hence $G^p \leq C_G(N)$. Thus $\Phi(G) \leq C_G(N)$ and $N \leq \zeta(\Phi(G))$. As $|\Phi(G) : \zeta(\Phi(G))| \leq p$, $\Phi(G)$ is abelian.

The fact that $G_2$ is abelian, has the useful consequence that $[x, y^n] = [x, y]^n [x, y, y]^{\binom{n}{2}}$ for any $x, y \in G$, $n \geq 1$ (multiple commutators are left normed). From this we may derive the following corollary.

COROLLARY 3. *Let $G$ be a $p$-group of order $p^5$, $p$ odd. Suppose that $G_4 = 1$. Then $G_2^p$ is central and $G_3^p = 1$. Consequently, for all $x, y \in G$, $[x, y]^p = [x, y^p]$.*

PROOF. Let $c \in G_2$ and $y \in G$. Then, as $G_4 = 1$, $[c^p, y] = [c, y]^p = [c, y^p]$. But $[G_2, G^p] = 1$ by the proposition so that the first points follow. The last point now follows from the second.

Our next reduction is to the class of groups for which the commutator subgroup is elementary abelian. Suppose that $G_2^p \neq 1$. Then there are elements $x, y$ in $G$ such that $[x, y]^p \neq 1$. Since $[x, y]^p = [x^p, y]$, $x^p \notin \langle y^p, [x, y]^p \rangle$, a subgroup of $C_G(y)$ of order at least $p^2$. It follows that $|G : G^p| \leq p^2$, a fact which implies that $G$ is metacyclic [4, III.11.4]. But metacyclic $p$-groups are known to be determined by their modular group algebras (see [20], or [1] whose proof applies in the $p = 3$ case as well).

All that remains is the case of $p$-groups of order $p^5$, $p$ odd, which are of class 3 and have elementary abelian commutator subgroups. Such groups have a restricted subgroup lattice and many other properties, collected together in our next result, which make it possible to identify them from their modular group algebras.

PROPOSITION 4. *Let $G$ be a $p$-group of order $p^5$, $p$ odd. Suppose that $G_3 > 1$, $G_4 = 1$ and $G_2^p = 1$. Then*

(i) $1 < G_3 G^p \leq \zeta(G)$;
(ii) $C_G(G_2)' \leq G_2 \cap \zeta(G) = G_3$;
(iii) $\Phi(G) \leq \zeta_2(G) = C_G(G/G_3) \leq C_G(G_2)$;
(iv) $\zeta_2(G)$ *is abelian;*
(v) $\Phi(G) \leq \Omega(G \bmod G_2) := \langle x \in G : x^p \in G_2 \rangle$;
(vi) *for* $x, y \in G$, $(xy)^p = x^p y^p$ *for* $p \geq 5$ *while, for* $p = 3$, $(xy)^3 = x^3 y^3 [y, x, x][y, x, y]^{-1}$;
(vii) *for each* $g \in G$ *the mapping* $x \to [x, g]$ *defines a homomorphism* $C_G(G_2) \to G_2$ *whose kernel is* $C_G(G_2) \cap C_G(g)$; *if* $|G_2| = p^2$ *and* $C_G(G_2)$ *is abelian and* $g \notin C_G(G_2)$, *then the kernel is* $\zeta(G)$.

PROOF. (i). That $G^p$ is central follows from Corollary 3 and the fact that $G_2^p = 1$. (ii). The first part follows from the Three Subgroups Lemma. The second part is easy, as is (iii). (iv). $G_2\zeta(G)$ is central in $\zeta_2(G)$ and of index at most $p$. That $\exp G/G_2$ divides $p^2$ proves (v) while (vi) follows from the Hall-Petrescu formula [4, III.9.4] for $p \geq 5$ and by direct calculation for $p = 3$. The last part of (vii) follows from the fact that $|G_2| = p^2$ implies that $|G : C_G(G_2)| \leq p$ whence any element commuting with $g$ and $C_G(G_2)$ is central.

It follows that $p^2 \leq |G_2| \leq p^3$ while $p \leq |\zeta(G)| \leq p^2$. Of the four possible pairs of values for these parameters, one cannot occur: that in which $|G_2| = p^3$ and $|\zeta(G)| = p$; in such a group, $G_2/G_3$ would be cyclic and so of order $p^2$, contradicting

https://doi.org/10.1017/S1446788700000215 Published online by Cambridge University Press

the fact that $G_2$ is elementary. For convenience of notation, often in what follows we will denote $C_G(G_2)$ by $C_G$, and similarly $\Omega(G \bmod G_2)$ by $L_G$.

We treat the groups remaining by dividing them into families according to the sizes of the centre and of the commutator subgroup. These are invariants recognised by the modular group algebra [18]. Groups in different subdivisions cannot have isomorphic group algebras. Our task is then to show that different groups in the same family have non-isomorphic group algebras. Any group $G$ in one of our subdivisions admits a power-commutator presentation [6] which is tightly specified. In each case we take a group basis $H$ for $FG$ and a power-commutator presentation for it; we then use properties of the small group algebra from [16] to obtain generators of $G$ which satisfy relations sufficiently close to those posited for $H$ that it is not difficult to conclude that $G$ and $H$ are isomorphic.

Relationships between the subgroups of $G$ and $H$ are obtained from [16]. The normalised unit group of the small group algebra, denoted by $S = S(FG)$, is defined as $V(FG)/(1 + I(G)I(G_2))$, where $V(FG)$ is the normalised unit group of $FG$. Recall that $S$ is determined by $FG$ and that $G$ embeds in $S$. The bar notation will be used to denote equivalence classes modulo $1 + I(G)I(G_2)$.

PROPOSITION 5. *Let $G$ be a $p$-group of order $p^5$, $p$ odd. Suppose that $G_3 > 1$, $G_4 = 1$ and $G_2^p = 1$. Let $H$ be a normalised group basis of $FG$. Then, in the group $S$,*

(i) $H_n = G_n$ *for* $n \geq 2$;
(ii) $\zeta_2(H)(\overline{1 + I^2}) = \zeta_2(G)(\overline{1 + I^2})$;
(iii) $C_H(H_2)(\overline{1 + I^2}) = C_G(G_2)(\overline{1 + I^2})$;
(iv) $(\overline{1 + I(G)^2})^p = \overline{1 + I(G^p)^2}$;
(v) $(\overline{1 + I^2})^p = 1$ *if* $G^p \leq G_2$;
(vi) $G \cap (\overline{1 + I^2})^p = G^{p^2}$.

*Moreover, the orders of $\Phi(G)$, $\zeta_2(G)$ and $C_G(G_2)$ are determined by $FG$ so that whether or not any of these subgroups coincide is also determined by $FG$. Whether or not $C_G(G_2) = \Omega(G \bmod G_2)$ is determined by $FG$.*

PROOF. The numbered items are specialisations of results in [16] to the situation here. That $FG$ determines $|\Phi(G)|$ was one of the first facts discovered [18]. That $FG$ determines $|\zeta_2(G)|$ and $|C_G(G_2)|$ under the present hypotheses on $G$ follows from (ii), (iii) and Proposition 4(iii) as $\Phi(G) = G \cap \overline{1 + I^2}$. The final point derives from Proposition 4(v) and was discussed in [16, 2.7].

In each case we will adapt the following notation. Let $H = \langle h_1, h_2, h_3, h_4, h_5 \rangle$, where the first 2 or 3 generators form a minimal generating set for $H$ and the remainder are defined in terms of them as commutators or $p$th powers. For each of the 'minimal generators' $h_i$, an element $g_i \in G$ is obtained by writing $h_i = g_i(1+\alpha_i)$ where $\alpha_i \in I^2$ (recall that $V(FG) = G(1+I^2)$). The remainder of the $g_i$ are defined as commutators or $p$th powers by the formulae analogous to those used in the definition of the corresponding $h_i$. Information about the relations between these elements may be derived from the small group algebra according to the results established in [16]. For example, as $G_4 = 1$, $\overline{(1+I^2)}$ is abelian and centralises $G_2$ [16, 1.7]; it follows that, if $h = g(1+\alpha)$ and $h' = g'(1+\alpha')$ where $\alpha, \alpha' \in I^2$, then $[h, h'] = [g, g'][g', \overline{(1+\alpha)}][\overline{(1+\alpha')}, g]$ in the unit group of the small group algebra of $G$ over $F$; thus $[h, h'] \equiv [g, g']$ modulo $G_3$. There is also a relationship in the case of $p$th powers. Again take $h = g(1+\alpha)$, $\alpha \in I^2$. By the Hall-Petrescu formula, $h^p = g^p\overline{(1+\alpha)}^p u_2^{\binom{p}{2}} u_3^{\binom{p}{3}} \cdots u_p$, for some $u_j \in \gamma_j(\langle g, \overline{1+\alpha}\rangle)$ for $2 \le j \le p$. By [16, 1.8], $\gamma_j(\langle g, \overline{1+\alpha}\rangle) \le G_{j+1}$; as $G_2^p = 1$ and $G_4 = 1$, $u_j^{\binom{p}{j}} = 1$ for $2 \le j \le p$. Thus $h^p = g^p\overline{(1+\beta)}$, where $\beta \in I(G^p)^2$ by Proposition 5(iv); further, if $\exp(G/G_2) = p$, then, by Proposition 5(v), $h^p = g^p$ in $S$.

FAMILY 1. $|G_2| = p^2$ and $|\zeta(G)| = p$.

This is the isoclinism family $\Phi_7$ of [5]. Let $H$ be a group basis of $FG$. As noted, $H$ is a group in this same family. As such it has some further properties of use:

$$H_2 = \Phi(H);\ H_3 = \zeta(H);\ H > C_H(H_2) > \zeta_2(H) > \Phi(H);\ C_H(H_2) \textit{ is non-abelian.}$$

The first two of these are immediate. That $|H : C_H(H_2)| = p$ follows from the fact that $|H_2| = p^2$. The last then follows from Proposition 4(vii) since, if $C_G(G_2)$ is abelian, then $|\zeta(G)| = p^2$. Now $C_H(H_2) > \zeta_2(H)$ is clear from Proposition 4(iv). That $\zeta_2(H) > \Phi(H)$ can be seen from an argument in the next paragraph.

We will choose minimal generators $h_1, h_2, h_3$ for $H$ so as to reflect the above properties and to achieve some simplification in calculations. First take $h_1 \in H \setminus C$, where $C = C_H(H_2)$. As the homomorphism in Proposition 4(vii) defined by $h_1$ is onto, $|C_C(h_1)| = p^2$ so that this subgroup contains an element $h$ not in $H_2$. But then $[h, H] = [h, C] \le \zeta(H)$ so that $h \in \zeta_2(H)$. Choose $h_2 \in C \setminus \zeta_2(H)$ and put $h_3 = h$ so that $h_3 \in \zeta_2(H) \setminus \Phi(H)$. Define $h_4 = [h_2, h_1]$ and $h_5 = [h_4, h_1]$. By the hypotheses, $[h_3, h_1]$ and all commutators $[h_j, h_i]$, for $j = 5$ or for $j = 4, i \ne 1$, vanish, while, by Proposition 4(ii), $[h_3, h_2] = h_5^a$ for some $a$, $0 < a \le p-1$. As $H_2$ is elementary, the only $p$th power relations remaining to be specified are those for the minimal generating set; by Proposition 4(i), there are integers $\ell, m, n$, $0 \le \ell, m, n \le p-1$, such that $h_1^p = h_5^\ell$, $h_2^p = h_5^m$ and $h_3^p = h_5^n$. Note that, if $n \ne 0$, we may replace $h_1$ by $h_1 h_3^{-\ell n'}$, where $nn' \equiv 1$ modulo $p$, with consequent alterations to $h_4$ and $h_5$; using Proposition 4(vi), we obtain a set of relations identical to the original set but in which $\ell = 0$; that is, we may assume that $\ell = 0$ or $n = 0$.

We now turn to the original group basis $G$. By Proposition 5(ii, iii), the minimal generators $g_1, g_2, g_3$ for $G$ satisfy: $g_1 \in G \setminus C_G(G_2)$, $g_2 \in C_G(G_2) \setminus \zeta_2(G)$, $g_3 \in \zeta_2(G) \setminus \Phi(G)$. Note that the $g_i$ were defined only modulo $\Phi(G)$; if necessary, we can redefine $g_3$ so as to achieve the relation $[g_3, g_1] = 1$. Define $g_4 = [g_2, g_1]$ and $g_5 = [g_4, g_1]$ so that $G_2 = \Phi(G) = \langle g_4, g_5 \rangle$ and $G_3 = \zeta(G) = \langle g_5 \rangle$. As seen earlier, $g_4 \equiv h_4$ modulo $G_3$ while $g_5 = h_5$ by a similar argument. This last point and the fact that $\exp(G/G_2) = p$ show that the $p$th power relations among the $g_i$ are the same as those among the $h_i$. All the commutator relations match those in $H$ save possibly that for $[g_3, g_2]$. As seen from the general setting, this lies in $G_3$ and is not 1. Let $[g_3, g_2] = g_5^b$, $0 < b \leq p - 1$, and let $b'$ be such that $bb' \equiv a$ modulo $p$. If $n = 0$, replacing $g_3$ by $g_3^{b'}$ will result in relations identical with those in $H$. If $\ell = 0$, replacing $g_2$ by $g_2^{b'}$ and $g_3$ by $g_3^{b'}$ will have the same effect. We conclude that $H \approx G$.

FAMILY 2. $|G_2| = p^3$ and $|\zeta(G)| = p^2$.

This is the isoclinism family $\Phi_6$ of [5]. Let $H$ be a group basis of $FG$, whence $H$ is a group in this same family. To deal with this case it suffices to observe that $H_2 = \Phi(H)$ and $H_3 = \zeta(H)$. Choose minimal generators $h_1, h_2$ for $H$ and define $h_3 = [h_2, h_1]$, $h_4 = [h_3, h_1]$ and $h_5 = [h_3, h_2]$. As $H_3$ is central, all commutators $[h_j, h_i]$ for $j = 4$ or 5 vanish. As $H_2$ is elementary, the only $p$th power relations to be specified are those for the minimal generating set; there are integers $k, \ell, m, n$, $0 \leq k, \ell, m, n \leq p - 1$, such that $h_1^p = h_4^k h_5^\ell$ and $h_2^p = h_4^m h_5^n$.

We now turn to $G$. This time the minimal generators for $G$ are $g_1$ and $g_2$. Define $g_3 = [g_2, g_1]$, $g_4 = [g_3, g_1]$ and $g_5 = [g_3, g_2]$ so that $G_2 = \Phi(G) = \langle g_3, g_4, g_5 \rangle$ and $G_3 = \zeta(G) = \langle g_4, g_5 \rangle$. As before, $g_3 \equiv h_3$ modulo $G_3$ while $g_4 = h_4$ and $g_5 = h_5$. Again, as $\exp(G/G_2) = p$, the $p$th power relations among the $g_i$ are the same as those among the $h_i$ while, in this case, the commutator relations are as well. We conclude that $H \approx G$.

FAMILY 3. $|G_2| = p^2$ and $|\zeta(G)| = p^2$.

This is the isoclinism family $\Phi_3$ of [5]. We have found it necessary to separate this case into three subcases depending on the minimal number of generators of $G$ and on whether or not $C_G = C_G(G_2)$ and $L_G = \Omega(G \bmod G_2)$ coincide; both of these features are determined by $FG$, the latter because of Proposition 5. Let $H$ be a group basis of $FG$, a group in this family. As $\zeta_2(H) = H_2\zeta(H)$ and so is central in $C_H$, the subgroup $C_H$ is an abelian maximal subgroup of $H$.

CASE 1. $d(G) = 3$: Choose minimal generators $h_1, h_2, h_3$ for $H$ as follows. Take as before $h_1 \in H \setminus C_H$ and $h_2 \in C_H \setminus \zeta_2(H)$. Lastly it is possible to choose $h_3 \in \zeta(H) \setminus \Phi(H)$. Define $h_4 = [h_2, h_1]$ and $h_5 = [h_4, h_1]$. By the hypotheses

https://doi.org/10.1017/S1446788700000215 Published online by Cambridge University Press

and the properties noted, $[h_4, h_2]$, $[h_4, h_3]$ and all commutators $[h_j, h_i]$ for $j = 3$ or $5$ vanish. As $H_2$ is elementary, the only $p$th power relations remaining to be specified are those for the minimal generating set; by Proposition 4(ii), there are integers $\ell, m, n$, $0 \le \ell, m, n \le p-1$, such that $h_1^p = h_5^\ell$, $h_2^p = h_5^m$ and $h_3^p = h_5^n$.

Again we turn to $G$. By Proposition 5(ii, iii), the minimal generators $g_1, g_2, g_3$ for $G$ satisfy: $g_1 \in G \setminus C_G$, $g_2 \in C_G \setminus \zeta_2(G)$, $g_3 \in \zeta(G) \setminus \Phi(G)$ (in this case the content of Proposition 5(ii) is that $\zeta(H)\overline{(1+I^2)} = \zeta(G)\overline{(1+I^2)}$). Define $g_4 = [g_2, g_1]$ and $g_5 = [g_4, g_1]$ so that $G_2 = \Phi(G) = \langle g_4, g_5 \rangle$ and $\zeta(G) = \langle g_3, g_5 \rangle$. As usual, $g_4 \equiv h_4$ modulo $G_3$ and $g_5 = h_5$. Thus, as $G^p \le G_2$, the $p$th power relations among the $g_i$ are the same as those among the $h_i$. The commutator relations match those in $H$. We conclude that $H \approx G$.

In the final cases the minimal number of generators of a group basis is 2 so that $H_2 < \Phi(H) = \zeta(H)H_2 = \zeta_2(H)$ and, because of the structure of $H/H_2$, $L := L_H$ is a maximal subgroup. The two cases are divided on the grounds of whether or not $L$ and $C := C_H$ coincide. Since $H_2 \le L$, this is the same issue as whether or not $L$ is abelian.

CASE 2. $d(G) = 2$, $L_G$ abelian: Choose minimal generators $h_1, h_2$ for $H$ by taking $h_1 \in H \setminus C$ and $h_2 \in C \setminus \Phi(H)$. Define $h_3 = h_1^p$, $h_4 = [h_2, h_1]$ and $h_5 = [h_4, h_1]$. Note that $h_3 \in \zeta(H) \setminus H_2$. By the hypotheses, $[h_4, h_2]$, $[h_4, h_3]$ and all commutators $[h_j, h_i]$ for $j = 3$ or $5$ vanish. As $H_2$ is elementary, the only $p$th power relations remaining to be specified are those for $h_2$ and $h_3$; there are integers $m, n$, $0 \le m, n \le p-1$, such that $h_2^p = h_5^m$ and $h_3^p = h_5^n$.

In the original group basis $G$, by Proposition 5(iii), the minimal generators $g_1, g_2$ for $G$ satisfy: $g_1 \in G \setminus C_G$, $g_2 \in C_G \setminus \Phi(G)$. Define $g_3 = g_1^p$, $g_4 = [g_2, g_1]$ and $g_5 = [g_4, g_1]$ so that $\Phi(G) = \langle g_3, g_4, g_5 \rangle$, $G_2 = \langle g_4, g_5 \rangle$ and $\zeta(G) = \langle g_3, g_5 \rangle$. Again, $g_4 \equiv h_4$ modulo $G_3$ so that $g_5 = h_5$.

While the commutator relations in $G$ match those in $H$, the $p$th power relations among the $g_i$ need not be the same as those among the $h_i$ in this case. By Proposition 5(iv), $\overline{(1+I^2)}^{p^2} = 1$ so that $h_3^p = h_1^{p^2} = g_1^{p^2}\overline{(1+\alpha_1)}^{p^2} = g_1^{p^2} = g_3^p$. Thus only $g_2^p$ remains to be settled: $h_2^p = g_2^p\overline{(1+\alpha_2)}^p$ is in $G_3$ so that $\overline{(1+\alpha_2)}^p \in G^{p^2}$ by Proposition 5(vi). As $G^{p^2} = \langle g_5^n \rangle$, we are done if $n = 0$. If $n \ne 0$ and $g_2^p = g_5^k$, replace $g_2$ by $g_2 g_3^{mn'-k}$ where $nn' \equiv 1$ modulo $p$; now $g_2^p = g_5^m$ but none of the other generators or relations has been changed. We can once more conclude that $H \approx G$.

CASE 3. $d(G) = 2$, $L_G$ non-abelian: Choose minimal generators $h_1, h_2$ for $H$ by taking $h_1 \in C \setminus L$ and $h_2 \in L \setminus \Phi(H)$. Define $h_3 = h_1^p$, $h_4 = [h_2, h_1]$ and $h_5 = [h_4, h_2]$. Again $h_3 \in \zeta(H) \setminus H_2$. By the hypotheses, $[h_4, h_1]$, $[h_4, h_3]$ and all commutators $[h_j, h_i]$ for $j = 3$ or $5$ vanish. As $H_2$ is elementary, the only $p$th power

https://doi.org/10.1017/S1446788700000215 Published online by Cambridge University Press

relations remaining to be specified are those for $h_2$ and $h_3$; there are integers $m, n$, $0 \leq m, n \leq p-1$, such that $h_2^p = h_5^m$ and $h_3^p = h_5^n$.

Turning to $G$, we see that, by Proposition 5(iii) and by the fact that $FGI(L_H) = FGI(L_G)$ (cf. [16, 2.7]), the minimal generators $g_1, g_2$ for $G$ satisfy: $g_1 \in C_G \setminus L_G$, $g_2 \in L_G \setminus \Phi(G)$. Define $g_3 = g_1^p$, $g_4 = [g_2, g_1]$ and $g_5 = [g_4, g_2]$ so that $\Phi(G) = \langle g_3, g_4, g_5 \rangle$, $G_2 = \langle g_4, g_5 \rangle$ and $\zeta(G) = \langle g_3, g_5 \rangle$. Again, $g_4 \equiv h_4$ modulo $G_3$ and again $g_5 = h_5$. The commutator relations in $G$ match those in $H$, and the $p$th power relations among the $g_i$ can be made the same as those among the $h_i$ by altering the value of $g_2$ as in the previous case. For the last time we conclude that $H \approx G$.

A close look at the proofs above shows that slightly more than was claimed is true. The groups $H$ in them need not have been group bases for $FG$; it is sufficient that such an $H$ satisfy only: $H \leq S$, $|H| = p^5$ and $H$ covers $\overline{1 + I^2}$. Once it is established that $d(H) = d(G)$ and $|\zeta(H)| = |\zeta(G)|$, the arguments here remain valid; what is important for Proposition 5 is that $H$ covers $\overline{1 + I^2}$.

## Acknowledgements

We wish to thank Al Weiss and Ian Leary for bringing to our attention the two 3-groups of order $3^5$ ($\Phi_3(311)b_1$ and $\Phi_3(311)b_{-1}$ in [5]) which have the same integral cohomology [7, 8]. The effort to distinguish the modular group algebras of these groups led to the methods used in this paper.

## References

[1] C. Bagiński, 'The isomorphism question for modular group algebras of metacyclic $p$-groups', *Proc. Amer. Math. Soc.* **104** (1988), 39–42.

[2] C. Bagiński and A. Caranti, 'The modular group algebras of $p$-groups of maximal class', *Canad. J. Math.* **40** (1988), 1422–1435.

[3] R. Brauer, 'Representations of finite groups', in: *Lectures on modern mathematics, vol. I* (Wiley, New York, 1963) pp. 133–175.

[4] B. Huppert, *Endliche Gruppen I* (Springer, Berlin, 1967).

[5] R. James, 'The groups of order $p^6$ ($p$ an odd prime)', *Math. Comp.* **34** (1980), 613–637.

[6] D. L. Johnson, *Presentations of groups* (Cambridge Univ. Press, Cambridge, 1990).

[7] I. J. Leary, *The cohomology of certain finite groups* (Ph.D. Thesis, Cambridge Univ., 1990).

[8] I. Leary, '3-groups are not determined by their integral cohomology rings', *J. Pure Appl. Algebra* **103** (1995), 61–79.

[9] A. Makasikis, 'Sur l'isomorphie d'algèbres de groupes sur un champ modulaire', *Bull. Soc. Math. Belg.* **28** (1976), 91–109.

[10] A. A. Mehrvarz, *Topics in the isomorphism of group rings* (Ph.D. Thesis, Stirling Univ., 1979).

[11] G. O. Michler, M. F. Newman and E. A. O'Brien, *Modular group algebras* (Unpublished Report, Australian National Univ., Canberra, 1987).

[12] I. B. S. Passi, *Group rings and their augmentation ideals*, Lecture Notes in Math. 715 (Springer, Berlin, 1979).

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

[14] D. J. Rusin, 'The cohomology of the groups of order 32', *Math. Comp.* **53** (1989), 359–385.

[15] M. A. M. Salim, *The isomorphism problem for the modular group algebras of groups of order* $p^5$ (Ph.D. Thesis, Univ. of Manchester, 1993).

[16] M. A. M. Salim and R. Sandling, 'The unit group of the modular small group algebra', *Math. J. Okayama Univ.* , to appear.

[17] ———, 'The modular group algebra problem for small $p$-groups of maximal class', *Canad. J. Math.*, to appear.

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

[19] ———, 'The modular group algebra of a central-elementary-by-abelian $p$-group', *Arch. Math. (Basel)* **52** (1989), 22–27.

[20] ———, 'The modular group algebra problem for metacyclic $p$-groups', *Proc. Amer. Math. Soc.* **124** (1996), 1347–1350.

[21] M. Wursthorn, *Die modularen Gruppenringe der Gruppen der Ordnung* $2^6$ (Diplomarbeit, Universität Stuttgart, 1990).

Mathematics Dept.
Emirates University
P. O. Box 17551, Al-Ain
United Arab Emirates

Mathematics Dept.
The University
Manchester M13 9PL
England
e-mail: rsandling@manchester.ac.uk