Can. J. Math. Vol. **48** (5), 1996 pp. 1064–1078.

THE MODULAR GROUP ALGEBRA PROBLEM FOR SMALL p-GROUPS OF MAXIMAL CLASS

MOHAMED A. M. SALIM AND ROBERT SANDLING

ABSTRACT. We show that p-groups of maximal class and order p^5 are determined by their group algebras over the field of p elements. The most important information requisite for the proof is obtained from a detailed study of the unit group of a quotient algebra of the group algebra, larger than the small group algebra.

Introduction. Among the p-groups for which the isomorphism problem for modular group algebras has received a positive answer, groups of maximal class have often set the greatest challenge. It is a long standing result that such groups for $p = 2$ are characterised by their group algebras over any field of characteristic 2. For $p = 3$, work done principally by Coleman and Wursthorn has settled the cases of orders 3^5 and 3^6; this involved the use of computers, the software packages Cayley [4] and Sisyphos [16] and algorithms of Roggenkamp and Scott and of Wursthorn [10, 16]. For odd p, Bagiński and Caranti [1] produced a positive answer for groups of order $\leq p^{p+1}$ which have an abelian maximal subgroup. Here we remove this last restriction but only for groups of order p^5.

THEOREM. *A p-group of maximal class and of order p^5 is determined by its modular group algebra over the field of p elements.*

We note that, as reported in [13], uncirculated work of L. G. Kovacs and M. F. Newman also covers this case; their methods are different, however. In the main our approach mimics that of [1] but in a more complicated setting. 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. 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 [13] $I(G)I(G_2)+I(G_2)I(G)$ was used, and $I(G)I(G_2)$ to a lesser extent; the latter, whose quotient algebra is termed the small group algebra, is the main ideal used in [11]. In [1] it is the quotient by $FGI(G_2)^2$ which is pursued. Here we introduce and exploit $I(G)I(G_2)^2 + I(G)^{p+1}I(G_2) + I(G)^{2p+1}$.

Our paper has two sections, the latter mainly taken up with the resolution of the isomorphism problem for p-groups of maximal class, p odd, which are of order p^5 and which have no abelian maximal subgroup. The former is preparatory. It can be read as a pilot study of unit groups of quotient algebras of FG. Its main objective, however,

Received by the editors August 3, 1994.
AMS subject classification: Primary: 20C05; secondary: 16S34, 16U60, 17B50, 20D15, 20F05.
Key words and phrases: modular group algebra, p-group, isomorphism problem, maximal class.

is the determination of the nilpotency class of the unit group in the particular quotient introduced here. This is accomplished by analysing a chain of ideals of FG, analogous to the ideals J_n of [1], which gives rise to a descending central series of the unit group in question. While this is adequate for $p \geq 7$, an approximation to an ascending central series had to be invented for the case $p = 5$; even then, the deduction of the main theorem in this case presented many obstacles. The difficulty in the $p = 5$ case was foreseen by the authors of [9] who commented: "New problems appear to arise for groups of order 5^5 over $GF(5)$." The $p = 3$ case is also given here but is attacked in a completely different and *ad hoc* manner.

Throughout, p will denote a fixed prime and F the field of p elements. G will be a finite p-group with FG its modular group algebra. The augmentation ideal of FG will be denoted as $I(FG), I(G)$ or I. As $I(FG)$ is nilpotent, the subset $V = V(FG) = 1 + I(FG)$ is a group, the group of normalised units of the unit group $U(FG)$.

The terms of the lower central series of a group X will be denoted by X_n or $\gamma_n(X)$ for $n \geq 2$ although its commutator subgroup will be denoted by X' as well. Its nilpotency class will be denoted by $c\ell(X)$. The subgroups $X \cap \left(1 + I(X)^n\right)$, the dimension subgroups of X over F, will be denoted $D_n = D_n(X)$; recall that $D_n = \prod_{ip^j \geq n} X_i^{p^j}$. The abbreviation I_n for the subring $I(G_n)$, $n \geq 1$, of FG will be convenient (G_1 is defined below). Recall that $I_n \subseteq I^n$. It will also be convenient to have a convention for nonpositive powers of $I = I(X)$: $I^0 = FX$; $I^n = 0$ if $n < 0$.

1. **A quotient of the modular group algebra.** Throughout this section, p will be an odd prime and G a finite p-group of nilpotency class $c := c\ell(G)$.

The subgroup $C_G(G_2/G_4)$ plays an important role in the study of groups of maximal class. For such groups, it can also be expressed as $C_G(G_2D_4/D_4)$, a form more suitable for the slightly more general context addressed in this section; here we will denote this subgroup by G_1, an unconventional usage. Our results require certain assumptions concerning the subgroups G_n, $n \geq 1$; they are set out in Hypothesis 1.1 which will be assumed in this section. All hold in a group of maximal class of order p^5.

HYPOTHESIS 1.1. *G_2 and G/G_2 are elementary abelian;*
$3 \leq c\ell(G) \leq 2p + 1$;
$G_1 \leq C_G(G_n/G_{n+2})$ *for* $n \geq 1$.

The setting for our results is the quotient algebra of FG obtained by factoring out the ideal $\Omega := I(G)I(G_2)^2 + I(G)^{p+1}I(G_2) + I(G)^{2p+1}$. Since the ideal $FGI(G_2)$ is canonical, *i.e.*, an invariant of FG itself and so independent of normalised group basis, Ω and the quotient algebra FG/Ω are also canonical. We will use the bar convention to denote the images of subsets of FG in this quotient algebra or in its normalised unit group $\bar{V} = V(FG)/(1 + \Omega)$. As G embeds in the latter, its elements and subsets will not be subject to the convention. The embedding is justified by the following lemma because, under Hypothesis 1.1, $G_2 = \Phi(G)$ and is abelian so that each of the constituent ideals of Ω satisfies its hypothesis. We omit the proof of the lemma as being straightforward and, as with many arguments involving Jennings' basis, notationally unpleasant.

LEMMA 1.2. *Suppose that a sequence X of elements of G give rise to a Jennings' basis for FG and that J is an ideal of FG spanned by those elements of this Jennings' basis which it contains. Then $G \cap (1+J) = \langle x \in X : x - 1 \in J \rangle$. Consequently, if J_i, $1 \leq i \leq n$, are such ideals, then $G \cap (1 + \sum J_i)$ is the product of the normal subgroups $G \cap (1 + J_i)$.*

Define the subgroup T of $\bar{V}$ as $G_1\left(\overline{1 + I(G)^2}\right)$. Since $1 + I^2 \geq V'$, T is normal in $\bar{V}$. As the dimension subgroup D_2 coincides with G_2 and so is contained in G_1, $T \cap G = G_1$. Other expressions for T include $\overline{1 + I_1 + I^2}$ and $\overline{G_1 + I^2}$.

Our first objective is the calculation of a useful upper bound on the nilpotency class of the group T. For this we need to gain control over the n-th term T_n of the lower central series of T.

While the calculation of commutators in the group V is formidable, the calculation of Lie commutators of ideals of FG is manageable. In some circumstances, the latter can serve for the former. For example, if J, K and L are ideals of FG, then $[1+J, 1+K] \leq 1+L$ if and only if $(J, K) \subseteq L$.

Direct calculation of the lower central series of V or T in terms of ideals, particularly those related to subgroups of G, seems impossible ($V' - 1$, for example, seems to have no interpretation in ideals; conversely, a subgroup like $1 + FGI(G_3)$ coming from an important ideal seems to have no special role in V in general). We seek to approximate the lower central series of T by a descending central series of subgroups which do come from ideals and so are relatively easy to manipulate. These will be the images of subgroups $1 + \Lambda_n$ of V, where Λ_n is an ideal of FG and $T_n \leq \overline{1 + \Lambda_n}$, $n \geq 2$. This will allow us to substitute Lie commutator calculations for the more intractable group commutator ones. From the expression of T as $\overline{1 + I_1 + I^2}$, we take the first of our ideals: $\Lambda_1 = I_1 + I^2 = FGI_1 + I^2$. The remaining ideals are defined by setting, for $n \geq 2$,

$$\Lambda_n = \sum I^i I_j + \sum I_\ell I_m + \Omega,$$

where the first sum is over all i, j satisfying $i \geq 0, j \geq 2$, $i + j = 2n - 1$, and the second is over all ℓ, m with $\ell, m \geq 2$, $\ell + m = 2n - 2$ (note that, as G_2 is abelian, $I_\ell I_m = I_m I_\ell$). It is straightforward to show that $I_2^2 + \Omega$ is an ideal; the same considerations prove that the Λ_n are ideals. We wish to show that $[1 + \Lambda_n, 1 + \Lambda_1] \leq 1 + \Lambda_{n+1}$. For this, it suffices to show that (Λ_n, I_1) and (Λ_n, I^2) are contained in Λ_{n+1}.

Our proof that the series of subgroups $\{1 + \Lambda_n\}$ is a central series, requires a good deal of routine manipulation with ideals, most of it suppressed here in the interests of brevity. It is helpful to have to hand a number of general formulae. They may be proved by the use of standard identities and by induction. The main principle applied in taking Lie brackets of ideals or subspaces of FG is the following.

LEMMA 1.3. *For any subspaces A, B and C of FG, $(AB, C) \subseteq A(B, C) + (A, C)B$.*

The other formulae show how products and Lie products of powers of $I(G)$ and the augmentation ideals of normal subgroups of G are interrelated.

https://doi.org/10.4153/CJM-1996-055-x Published online by Cambridge University Press

LEMMA 1.4. *For normal subgroups M and N of G, $\big(I(M), I(N)\big) \subseteq F(MN)I([M,N])$.*

The next item transfers a result from [11] to this setting.

LEMMA 1.5. *For $i,j \geq 1$, $[1+I^i, 1+I^j] \leq G_{i+j}(1+II_2)$ and so $(I^i, I^j) \subseteq II_2 + I_{i+j}$.*

LEMMA 1.6. *For $k \geq 1$, $I_k I \subseteq II_k + I_{k+1}$. For $\ell \geq 1$ and $j \geq 0$, $I_\ell I^j \subseteq \sum_{k\geq \ell} I^{\ell+j-k} I_k$.*

COROLLARY 1.7. *For $\ell \geq 1$ and $r \geq 0$, $\sum_{i+j=r} I^i I_\ell I^j \subseteq \sum_{k\geq \ell} I^{\ell+r-k} I_k$.*

The last of our preparatory lemmas is that in which the assumptions concerning G_1 in Hypothesis 1.1 are used.

LEMMA 1.8. *For $i,j \geq 1$,*
(i) $(I_j, I_1) \subseteq FGI_{j+2}$;
(ii) $(I^i, I_1) \subseteq \sum_{k\geq 2} I^{i+1-k} I_k$;
(iii) $(I_j, I^2) \subseteq II_{j+1} + I_{j+2}$;
(iv) $(I^i, I^2) \subseteq II_2 + I_{i+2}$.

We may now state the main result and give a sketch of its proof.

PROPOSITION 1.9. *For $n \geq 1$, $(\Lambda_n, \Lambda_1) \subseteq \Lambda_{n+1}$. Consequently, $T_n \leq \overline{1+\Lambda_n}$.*

PROOF. It suffices to show that (Λ_n, I_1) and (Λ_n, I^2) are contained in Λ_{n+1}. For $n = 1$, $\Lambda_1 = I_1 + I^2$ and $\Lambda_2 = II_2 + I_3 + \Omega$. By Lemma 1.8(i), $(I_1, I_1) \subseteq FGI_3$ while $(I_1, I^2) \subseteq II_2 + I_3$ by Lemma 1.8(ii); lastly, $(I^2, I^2) \subseteq II_2 + I_4$ by Lemma 1.5.

The general case is similar. Its proof may be effected by application of the following more specialised formulae which are deduced from the earlier ones:

$$(I^i I_j, I_1) \subseteq I^i I_{j+2} + I_{i+1} I_j + \Omega \quad i \geq 0, j \geq 2$$
$$(I_\ell I_m, I_1) \subseteq I_\ell I_{m+2} + I_{\ell+2} I_m + \Omega \quad \ell, m \geq 2$$
$$(I^i I_j, I^2) \subseteq I^{i+1} I_{j+1} + I^i I_{j+2} + I_{i+2} I_j + \Omega \quad i \geq 0, j \geq 2$$
$$(I_\ell I_m, I^2) \subseteq I_\ell I_{m+2} + I_{\ell+1} I_{m+1} + I_{\ell+2} I_m + \Omega \quad \ell, m \geq 2.$$

If n is an integer for which $\Lambda_n \subseteq \Omega$, then the class of T is bounded by $n-1$; this is the way in which the following theorem is approached.

THEOREM 1.10. *Let G be a finite p-group with $c = c\ell(G)$. Then $c\ell(T) \leq p+1$ if $c \geq p$, and $c\ell(T) \leq \frac{1}{2}(p+c+1)$ if $c < p$.*

PROOF. We seek a lower bound on n such that $\Lambda_n \subseteq \Omega$. The ideals Λ_n are combinations of ideals of the forms $I^i I_j$ and $I_\ell I_m$. We examine conditions on n which will ensure that $I^i I_j$ and $I_\ell I_m$ are contained in $\Omega = II_2^2 + I^{p+1} I_2 + I^{2p+1}$.

As $I^i I_j \subseteq I^{i+j}$, $I^i I_j \subseteq \Omega$ if $2n - 1 = i + j \geq 2p + 1$. But the ideals $I^{2n-3} I_2$, $I^{2n-4} I_3, \ldots, I^{2n-c-1} I_c$ are in Ω if $2n - c - 1 \geq p + 1$. Here then we want $n \geq n_1 = 1 + \min\{p, (p+c)/2\}$.

As $I_\ell I_m \subseteq I^{\ell+m}$, $I_\ell I_m \subseteq \Omega$ if $2n - 2 = \ell + m \geq 2p + 1$. Again the ideals $I_{2n-4} I_2$, $I_{2n-5} I_3, \ldots, I_{2n-c-2} I_c$ are in Ω if $2n - c - 2 \geq p + 1$. This time we want $n \geq n_2 = \frac{1}{2} \min\{2p+3, p+c+3\}$.

Since $n_2 > n_1$, we see that $\Lambda_n \subseteq \Omega$ for $n \geq p+2$ if $c \geq p$ and for $n \geq (p+c+3)/2$ if $c < p$. The desired conclusion follows.

Various more specialised results will also be needed in our subsequent analysis of the group algebras of the groups of maximal class. We begin with one which shows that the commutator subgroup of T is elementary.

LEMMA 1.11. *The commutator subgroup of the group T is of exponent p. Consequently, $\gamma_2(1+I^2)^p \leq 1+\Omega$.*

PROOF. Since $(1+\Lambda_2)^p \leq 1+\Lambda_2^p$, it suffices to show that $\Lambda_2^p \subseteq \Omega$. But $\Lambda_2^p \subseteq I^{3p} \subseteq \Omega$.

LEMMA 1.12. *Let $c = c\ell(G)$ and $c' = c\ell(\overline{1+I^2})$. Then $c' \leq \frac{1}{2}(p+c-1)$ if $c \geq 5$ and $c' \leq \frac{1}{2}(p+3)$ if $c \leq 4$.*

PROOF. Write M for $1+I^2+\Omega$. The commutator subgroup M_2 is contained in the subgroup $1+FGI(G_2)\cap I^4$. As each of these subspaces has as basis the subset of Jennings' basis elements which lie in them, their intersection has as basis those Jennings' basis elements which they have in common; it follows that $M_2 \leq 1+I^2I(D_2)+II(D_3)+I(D_4)$. As $D_n \leq G_nG^p$ for all $n \geq 2$, $I(D_n) \subseteq I_n + I^p$. Hence, $M_2 \leq 1+I^2I_2+II_3+I_4+I^p+\Omega$.

We show by induction on n that, for $n \geq 2$, $M_n \leq 1+\sum_{k\geq 2} I^{2n-k}I_k + I^{p+2(n-2)} + \Omega$. This assumed for n, we see that $M_{n+1} \leq 1+\sum_{k\geq 2}(I^{2n-k}I_k, I^2)FG + (I^{p+2(n-2)}, I^2)FG + \Omega$. Using formulae given earlier and the fact that $I_j \subseteq I^j$, we obtain

$$\begin{aligned} M_{n+1} &\leq 1+\textstyle\sum_{k\geq 2}\{I^{2n-k+1}I_{k+1} + I^{2n-k}I_{k+2} + I_{2n-k+2}I_k\} + I^{p+2(n-2)+2} + \Omega \\ &\leq 1+\textstyle\sum_{k\geq 2} I^{2(n+1)-k}I_k + I^{p+2((n+1)-2)} + \Omega. \end{aligned}$$

It follows that $M_n \leq 1+\Omega$ if $2n-c \geq p+1$ and $p+2(n-2) \geq 2p+1$, *i.e.*, if $n \geq \frac{1}{2}\max\{p+c+1, p+5\}$. The lemma follows.

Next we investigate the upper central series of the group T. By Du's theorem [5], its terms can be described by the use of subgroups derived from Lie ideals; our techniques, however, call for associative ideals. Thus we seek to approximate the pre-image of each term $\zeta_n(T)$ in $G_1(1+I^2)$ by a subgroup $1+\Upsilon_n$ of V, where Υ_n is an ideal of FG satisfying $\overline{1+\Upsilon_n} \leq \zeta_n(T)$.

In general we have been successful in achieving this in a form suitable for our applications only when $3 \leq c \leq p-1$ and only for $0 \leq n \leq c-1$. Define $\Upsilon_0 = \Omega$. For $1 \leq n \leq c-1$, define

$$\Upsilon_n = \sum I^iI_j + \sum I^kI_1I_h + \sum I_\ell I_m + \Omega,$$

where i,j satisfy $0 \leq i \leq p$, $2 \leq j \leq c$ and $i+j = (p-n)+(c-n)+1$, where k,h satisfy $0 \leq k \leq p-1$, $c-n+1 \leq h \leq c$ and $k+h = 2(c-n)$, and where ℓ, m satisfy $2 \leq \ell, m \leq c$ and $\ell + m = 2(c-n)+1$. It is again straightforward to see that the Υ's are ideals and that they form an ascending sequence. The subgroups to which they give rise do have the desired property.

PROPOSITION 1.13. *Let G be a p-group of nilpotency class c where $3 \leq c \leq p-1$. Then $\overline{1+\Upsilon_n} \leq \zeta_n(T)$ for $0 \leq n \leq c-1$.*

As before the proof reduces to the display of a relationship between ideals of FG, in this case as set out in the following result.

LEMMA 1.14. *Let G be a p-group of nilpotency class c where $3 \leq c \leq p-1$. For $1 \leq n \leq c-1$, $(\Upsilon_n, \Lambda_1) \subseteq \Upsilon_{n-1}$ and, consequently, $[\overline{1+\Upsilon_n}, T] \leq \overline{1+\Upsilon_{n-1}}$.*

PROOF. It suffices to show that both (Υ_n, I_1) and (Υ_n, I^2) are contained in Υ_{n-1}. The expressions being more complicated, this is more tedious than the last such exercise but is accomplished by the same use of the general principles of manipulation of ideals as given earlier based on the same formulae as before as well as on the following easily derived formulae: for $k \geq 0$, $h \geq 2$,

$$(I^k I_1 I_h, I_1) \subseteq I^k I_1 I_{h+2} + I_{k+3} I_h + \Omega,$$
$$(I^k I_1 I_h, I^2) \subseteq I^{k+1} I_1 I_{h+1} + I^k I_1 I_{h+2} + I^k I_2 I_{h+1} + I_{k+3} I_h + \Omega.$$

We mention a result in this context which concerns p-th powers. It can be shown by using Corollary 1.7 to prove something stronger, namely, that a product of $2p$ elements of I may be reordered at will modulo Ω if G is of nilpotency class strictly less than p.

LEMMA 1.15. *Let G be a p-group with $c\ell(G) < p$. If $\alpha, \beta \in I$, $(\alpha\beta)^p \equiv \alpha^p \beta^p$ modulo Ω.*

We conclude this section by indicating some contrasts between our work and that of Bagiński and Caranti in [1]. Much of their paper is devoted to groups G of maximal class in which our G_1 is abelian and coincides with $C_G(G_2/G_4)$, the conventional notation. At one point they focus on another centraliser in the general case, the subgroup $C_G\big(G_2/\Phi(G_2)\big)$; this is contained in G_1 in a group G of maximal class of order p^n, $n \geq 5$ (recall that p is odd throughout). Their Proposition 1.4 states that, if $C_G\big(G_2/\Phi(G_2)\big)$ is maximal in G, then:

(i) the canonical subring $C_I(FGI_2/FGI_2^2) = I\Big(C_G\big(G_2/\Phi(G_2)\big)\Big) + FGI_2$;

(ii) the algebra $\Big(I\Big(C_G\big(G_2/\Phi(G_2)\big)\Big) + FGI_2\Big) \Big/ FGI_2^2$ is commutative if and only if the group $C_G\big(G_2/\Phi(G_2)\big)/\Phi(G_2)$ is abelian.

These have analogues in our setting. We note first a special case of Proposition 3.4 of [11].

PROPOSITION 1.16. *The centraliser in V of the quotient algebra $\big(FGI(G_2D_4)+I^4\big)/I^4$ is $C_G(G_2D_4/D_4)(1+I^2)$.*

This is now specialised further to exploit the conditions which obtain in p-groups of order p^n, $n \geq 5$, and of maximal class, and transformed to allow easier comparison with [1]. The hypothesis holds when G/G_4 is elementary.

COROLLARY 1.17. *If $D_4 = G_4$, then $C_I\big(FGI_2/(FGI_2 \cap I^4)\big) = \Lambda_1$*

https://doi.org/10.4153/CJM-1996-055-x Published online by Cambridge University Press

PROOF. $C_V\big((FGI_2+I^4)/I^4\big) = C_V\big(FGI_2/(FGI_2\cap I^4)\big)$ since the two quotient algebras are isomorphic as FV-modules (here V acts by conjugation). As in [11] we see that, for a quotient Q of ideals of FG, $C_V(Q) = 1+C_I(Q)$. As $G_2D_4 = G_2$ in this case, the proposition shows that $1 + C_I\big(FGI_2/(FGI_2^2\cap I^4)\big) = C_G(G_2/G_4)(1+I^2) = G_1(1+I^2) = 1+I_1+I^2$ as required.

For a group G of order p^n, $n \geq 5$, which is of maximal class, G_1 is maximal in G and $D_4 = G_4$. Here Λ_1 is canonical and contains $C_I(FGI_2/FGI_2^2)$. While Λ_1/I^4 is not commutative, the quotient algebra $(I_1 + FGI_2 + I^4)/I^4$ is commutative if and only if $(I_1, I_1) \subseteq I^4$, which happens if and only if the group G_1/G_4 is abelian.

2. **Groups of maximal class.** In this section we give the proof of our main theorem. First of all note that the modular group algebra distinguishes groups of maximal class of order p^5 from other groups of this order. They are precisely those groups having centres of order p and commutator factor groups of order p^2. The fact that FG determines $\zeta(G)$ and G/G' for a p-group G is among Ward's original results on the modular group algebra problem [12]. Secondly, by [1, 3.2], if G has maximal class, then FG determines whether or not G has an abelian maximal subgroup.

It is convenient to dispatch the groups for $p = 2$ and $p = 3$ separately. The groups themselves do not fit the general pattern; note in particular that, if G is of maximal class and of order 3^5, then $G' \approx C_9 \times C_3$; it is not elementary abelian as indicated in [8, Table 4.1]. There are many ways to distinguish the 2-groups of maximal class (see [6, III.11.9]) by their modular group algebras [12, 6.34]. Of those not reported there, one, initiated in [9] and used extensively in [15], is based on an invariant easy to calculate for these groups, the number of conjugacy classes of elementary abelian subgroups of rank 2 [12, 6.28]; another is direct [2].

For $p = 3$ there are only 6 groups of order 3^5 which are of maximal class, 3 have an abelian maximal subgroup [8, Family Φ_9, Table 4.5] and 3 do not [8, Family Φ_{10}, Table 4.5] (see also [3]). They are the following groups given here in power-commutator presentations; each is generated by 5 elements s, s_1, s_2, s_3, s_4 subject to the relations $s^3 = s_4^i$, $s_1^3 = s_3^{-1}s_4^j$, $s_2^3 = s_4^{-1}$ and $[s_1,s] = s_2$, $[s_2,s] = s_3$, $[s_3,s] = s_4$, $[s_2,s_1] = s_4^k$ (by convention all other p-th powers of generators are assumed to be equal to 1, as are all other commutators of generators aside from the inverses of those already specified); for the first three groups, $k = 0$ and the pair (i,j) is $(0,1), (0,-1)$ or $(1,1)$; for the second three, $j = 1$, $k = -1$ and $i = 0, 1$ or -1. It is not hard to calculate one of Scott's invariants for these groups, the number of conjugacy classes of maximal elementary abelian subgroups of rank two [12]. For the first three, they are 4, 2 and 1 respectively; for the second, 2, 1 and 3 (these values were checked by use of the software package Cayley [4]).

For the rest of this section we will assume that $p \geq 5$. The pioneering work of Bagiński and Caranti showed that, if G has maximal class, order $\leq p^{p+1}$ and an abelian maximal subgroup, then FG determines G [1, 2.2]. This allows us to focus on the groups of maximal class which do not have an abelian maximal subgroup; note that this occurs if and only if $G_1 = C_G(G_2/G_4)$ is nonabelian (our definition of G_1 and that conventional

in the study of groups of maximal class now coincide). These groups, given in [8, Family Φ_{10}, Table 4.5], admit the following power-commutator presentations given according to the convention used earlier; each such group G is generated by 5 elements s, s_1, s_2, s_3, s_4 subject to the relations $s^p = s_4^\ell$, $s_1^p = s_4^m$ and $[s_1, s] = s_2$, $[s_2, s] = s_3$, $[s_3, s] = s_4$, $[s_2, s_1] = s_4^{-1}$; here $0 \leq \ell = \ell_G$, $m = m_G \leq p - 1$. By [3, 3.2] we may assume that either ℓ or $m = 0$. Since only one of these groups is of exponent p, namely, that with $\ell = m = 0$, and since the exponent of a p-group is an invariant of its modular group algebra (see [14]), we may assume that either $\ell \neq 0$ or $m \neq 0$. It is helpful to keep in mind the relationship between the generators and the nontrivial characteristic subgroups of G:

$$G_1 = C_G(G_2/G_4) = \langle s_1, s_2, s_3, s_4 \rangle$$
$$G_2 = \Phi(G) = \langle s_2, s_3, s_4 \rangle$$
$$G_3 = \langle s_3, s_4 \rangle$$
$$G_4 = \zeta(G) = \langle s_4 \rangle.$$

Our proof will be accomplished in three propositions, each established in a similar manner. The first shows that the modular group algebra determines whether or not, for a group G at issue, the exponent of G_1 is p. The second shows that the groups for which the exponent is not p, have distinct group algebras over F while the third does the same for the remaining groups.

Much of the notation for the proofs of the three propositions can be given in common. Let G be presented as above. Suppose that H is another group basis of FG, $H \leq V$. By the earlier discussion we may assume that H is also presented as above but in generators t, t_n, $n = 1, 2, 3, 4$, and with values ℓ_H and m_H.

Each quotient $(1 + I^n)/(1 + I^{n+1})$, $n \geq 1$, is elementary abelian and admits a basis consisting of the images of units $1 + \pi$, where π is a Jennings' basis element of weight n in FG in terms of the generators given for G (which are appropriate for the purpose). We will expand the generators of H as products of these units; we need to do so only in the initial stages, that is, modulo $1 + I^2$ or $1 + I^3$. Recall that, as the embedding of $G/\Phi(G)$ in $V(FG)/\left(1 + I(G)^2\right)$ is an isomorphism, the units for the first stage are just s and s_1.

At the first stage then, $t = s^i s_1^j(1 + \alpha)$ and $t_1 = s^h s_1^k(1 + \alpha_1)$ where $0 \leq i, j, h, k \leq p - 1$ and $\alpha, \alpha_1 \in I^2$. Since t, t_1 generate $V = V(FH)$ modulo $1 + I^2 = 1 + I(H)^2$, $s^i s_1^j, s^h s_1^k$ generate V modulo $1 + I^2$. It follows that these elements generate G and so that $d := ik - jh \not\equiv 0$ modulo p.

We next introduce an intermediary set of generators of G, both notationally convenient for the three cases and useful for contrasting the presentations of G and H. Set $x = s^i s_1^j$ and $x_1 = s^h s_1^k$, and define $x_n = [x_{n-1}, x]$, $n = 2, 3, 4$. We will examine the salient relations for the x's. Having their origin in the generators for H, they will be influenced by the relations in H. On the other hand, the x's lie in G and are constrained by its relations. If G and H are not isomorphic, this tension results in a contradiction.

Much of the examination is carried out in the context of the unit group S of the small group algebra FG/II_2. Properties established about S in [11] are crucial. Recall that, as G_2 is elementary abelian, G is embedded in S and that S shares many of the features of G; in particular, $S_n = G_n = H_n$ for $n \geq 2$. We will use the bar convention for equivalence classes modulo II_2; as G and H are embedded in the small group algebra, we do not apply this convention to their elements.

We first show that, for $n = 2, 3, 4$, $t_n \equiv x_n$ modulo G_{n+1} (note that, G being of class 4, equivalence modulo G_5 is equality in S). For $n = 2$, $t_2 = [x_1(\overline{1+\alpha_1}), x(\overline{1+\alpha})]$ which is equivalent modulo G_3 to $x_2[x_1, \overline{1+\alpha}][\overline{1+\alpha_1}, x][\overline{1+\alpha_1}, \overline{1+\alpha}]$. But, by [11, 1.7], $[S, \overline{1+I^2}] \leq G_3$ and so $t_2 \equiv x_2$ modulo G_3. The proofs of the other two cases are similar. Next we observe that $[t_2, t_1] = [x_2, x_1][x_2, \overline{1+\alpha_1}]$. The proof of this assertion is much the same but also makes use of the fact that $G_1 = C_G(G_3/G_5) = C_G(G_3)$.

Our next goal is to find expressions in the s's which are equivalent to these words in the t's. Before doing this, we pause to note that $h = 0$, that is, that $x_1 \in G_1$, a fact which simplifies calculations considerably. By [11, 3.1], $C_H(H_2/H_4)(\overline{1+I^2}) = C_S(S_2/S_4) = C_G(G_2/G_4)(\overline{1+I^2})$, from which it follows that $x_1 \in C_G(G_2/G_4)$. From this we see that $d = ik$.

We now substitute for the x's in our earlier expressions to obtain: in S, $t_2 \equiv s_2^{ik}$ modulo G_3, $t_3 \equiv s_3^{i^2k}$ modulo G_4, $t_4 = s_4^{i^3k}$ and $[t_2, t_1] = s_4^{-ik^2+a}$ where $s_4^a = [x_2, \overline{1+\alpha_1}]$ for some a, $0 \leq a \leq p-1$ [11, 1.7]. As $[t_2, t_1] = t_4^{-1}$, it follows that $a \equiv ik(k - i^2)$ modulo p.

The p-th power relations in H and G are our last object of study. As $H_2 = G_2$ is elementary abelian, this amounts to an examination of x^p and x_1^p. By the Hall-Petrescu formula [6, III.9.4], $t^p = x^p(\overline{1+\alpha})^p v_2^{\binom{p}{2}} \cdots v_p$ where, for $2 \leq n \leq p$, $v_n \in \gamma_n(\langle x, \overline{1+\alpha}\rangle)$ which is contained in G_{n+1} by [11, 1.7]. But $v_n^{\binom{p}{n}} = 1$ for $2 \leq n \leq p-1$ as G_2 is elementary abelian. Also $v_p \in G_{p+1} = 1$ as $p \geq 5$. Lastly $(\overline{1+\alpha})^p = 1$ for, by [11, 1.12], $\overline{1+I^2}$ has exponent p. Thus $t^p = x^p$. A analogous expansion of $x^p = (s^i s_1^j)^p$ by the Hall-Petrescu formula yields $x^p = s^{ip} s_1^{jp} = s_4^{i\ell+jm}$. Comparing expressions, doing similar work with t_1^p and x_1^p and appending an earlier conclusion, we are led to the following equations modulo p which interrelate our parameters:

$$i^3 k\ell_H \equiv i\ell_G + jm_G$$
$$i^3 m_H \equiv m_G$$
$$a \equiv ik(k - i^2).$$

We are now ready for the statements and proofs of the three propositions. It follows from the Hall-Petrescu identity that G_1 is of exponent p if and only if $m = 0$. Our first result shows that this is a property which FG can detect.

PROPOSITION 2.1. *Let G be a p-group of maximal class of order p^5 which has no abelian maximal subgroup. Whether or not G_1 is of exponent p is determined by FG.*

PROOF. Let H be a group basis of FG; as noted, H is also of maximal class with no abelian maximal subgroup. Suppose that $\exp(G_1) \neq p$ while $\exp(H_1) = p$. In the notation above, our assumptions are that $\ell_G = 0$ and $m_G \neq 0$ while $\ell_H \neq 0$ and $m_H = 0$. This contradicts the second equation.

We next look at groups G in which $\exp(G_1) \neq p$ [8, Family $\Phi_{10}(2111)b_r$, Table 4.5]. For such groups we may take $\ell = 0$ and m equal to one of at most three values depending on the congruence class of p modulo 3; these values can be given by representatives for the cosets of F^{*3} in F^*.

PROPOSITION 2.2. *A p-group G of maximal class which has order p^5, which has no abelian maximal subgroup and in which G_1 is not of exponent p, is determined by FG.*

PROOF. Let H be a group basis of FG and so of maximal class with no abelian maximal subgroup and with $\exp(H_1) \neq p$. Our second equation shows that $m_H \equiv m_G$ modulo F^{*3} whence $H \approx G$ by the classification of these groups.

Lastly we look at groups G in which $\exp(G_1) = p$ [8, Family $\Phi_{10}(2111)a_r$, Table 4.5]. For such groups we may take $m = 0$ and ℓ equal to one of at most four nonzero values depending on the congruence class of p modulo 4; these values can be given by representatives for the cosets of F^{*4} in F^*.

PROPOSITION 2.3. *A p-group G of maximal class which has order p^5, which has no abelian maximal subgroup and in which G_1 is of exponent p, is determined by FG.*

PROOF. Let H be a group basis of FG and so of maximal class with no abelian maximal subgroup and with $\exp(H_1) = p$. In the notation above, our assumptions are that $m_G = 0 = m_H$. Our equations tell us that $i^2 k \ell_H \equiv \ell_G$ and $a \equiv ik(k - i^2)$ modulo p. If $a = 0$, then $\ell_H \equiv \ell_G$ modulo F^{*4} so that $H \approx G$ and our proof is complete. The rest of our work is taken up with showing that $a = 0$.

Recall that a was defined from the equation $[x_2, \overline{1 + \alpha_1}] = s_4^a$ and that α_1 derived from the expression $t_1 = s_1^k(1 + \alpha_1)$. As $\overline{1 + I^3}$ acts trivially on G_2, we need only be concerned with $1 + \alpha_1$ modulo $1 + I^3$ and so, in its expression as a product of units $1 + \pi$ where π is a Jennings' basis element, with those units for which π is of weight 2. These are $1 + (s - 1)^2$, $1 + (s - 1)(s_1 - 1)$, $1 + (s_1 - 1)^2$ and s_2. By the facts that G_2 is abelian and that G_1 centralises G_3 and by [11, 1.5], we see that, except for the first, all of these units commute with x_2. Thus $[x_2, \overline{1 + \alpha_1}] = \left[x_2, \overline{\left(1 + (s - 1)^2\right)^b}\right] = [x_2, s, s]^b = s_4^{db}$, where b is the exponent of $1 + (s - 1)^2$ in the expansion of $1 + \alpha_1$, $0 \leq b \leq p - 1$. It follows that $a = db$; our aim, then, is to show that $b = 0$.

At this point we suspend the proof of our proposition. It is here that we must go into the group ring deeper than II_2. Indeed, using Sisyphos [16], Wursthorn has shown that, for $p = 5$, the four groups of maximal class which are at issue have isomorphic small group algebras. We found it necessary to go down as far as our ideal $\Omega = II_2^2 + I^{p+1}I_2 + I^{2p+1}$, a canonical ideal. From here on, the bar convention is to be interpreted as indicating classes modulo Ω or $1 + \Omega$, depending on the context. Our earlier results concerning the group $T = \langle s_1, \overline{1 + I^2} \rangle$ are now brought to bear on the issue. Note that this group is also

https://doi.org/10.4153/CJM-1996-055-x Published online by Cambridge University Press

canonical (we showed that $t_1 \in T$). To fix notation, write $1+\alpha_1 = \left(1+(s-1)^2\right)^b(1+\beta)$, where β is in the ideal $F(s-1)(s_1-1)+F(s_1-1)^2+F(s_2-1)+I^3$.

LEMMA 2.4. *In the quotient group T, $\left(\overline{1+(s-1)^2}\right)^p \neq 1$ but $\left(\overline{1+(s-1)(s_1-1)}\right)^p = 1$, $\left(\overline{1+(s_1-1)^2}\right)^p = 1$ and $\left(\overline{1+I^3}\right)^p = 1$; thus, $(\overline{1+\beta})^p = 1$.*

PROOF. From the presentation of G we see that $\left(1+(s-1)^2\right)^p = 1+(s^p-1)^2 = 1+(s_4^\ell-1)^2$. Now $(s_4-1)^2$ is an element of the Jennings' basis constructed using the s's. By Lemma 1.2, Ω has a basis consisting of the union of all Jennings' basis elements in the ideals II_2^2, $I^{p+1}I_2$ and I^{2p+1}. But $(s_4-1)^2$ is not among these while $(s_4^\ell-1)^2 \equiv \ell^2(s_4-1)^2$ modulo Ω. As $\ell \neq 0$, $(s_4^\ell-1)^2 \notin \Omega$ and so $\left(1+(s-1)^2\right)^p \not\equiv 1$ modulo $1+\Omega$.

Next, for any $g \in G$, $\left(1+(g-1)(s_1-1)\right)^p = 1+\left((g-1)(s_1-1)\right)^p$, which, by Lemma 1.15, is equivalent modulo $1+\Omega$ to $1+(g-1)^p(s_1-1)^p$. But this is 1 as s_1 is of order p. Also, as $I^{3p} \subseteq \Omega$, $(\overline{1+I^3})^p = 1$.

The last point can be seen by the use of the Hall-Petrescu formula, by the previous points and by the facts that $\exp(G_2) = p$, that $\gamma_2(\overline{1+I^2})^p = 1$ by Lemma 1.11 and that $\gamma_p(\overline{1+I^2}) = 1$ by Lemma 1.12.

PROOF OF PROPOSITION 2.3 (CONTINUED). Suppose first that $p \geq 7$. The Hall-Petrescu formula, applied in T, shows that $1 = t_1^p = x_1^p(\overline{1+\alpha_1})^p v_2^{\binom{p}{2}} \cdots v_n^{\binom{p}{n}} \cdots v_p$, where, for $2 \leq n \leq p$, $v_n \in T_n$. But $v_n^{\binom{p}{n}} = 1$ for $2 \leq n \leq p-1$ as T_2 is elementary by Lemma 1.11; also $T_p = 1$ by Theorem 1.10 so that $v_p = 1$. As $\exp(G_1) = p$, $x_1^p = 1$. Using the Hall-Petrescu formula again, we find that $1 = (\overline{1+\alpha_1})^p = \left(\overline{1+(s-1)^2}\right)^{pb}(\overline{1+\beta})^p$. As the last factor vanishes and as $\left(\overline{1+(s-1)^2}\right)^p \neq 1$, we conclude that $b = 0$ as desired.

For $p = 5$ we no longer have available the conclusion that $T_p = 1$; that $c\ell(T) \leq 5$ is all that Theorem 1.10 provides. The argument which shows that $b = 0$ is much more taxing in this case. It is here that the approximation to the upper central series of T plays its role. We begin by specifying explicitly the ideals of Section 1:

$$\Lambda_1 = I_1 + I^2$$
$$\Lambda_2 = II_2 + I_3 + \Omega$$
$$\Lambda_3 = I^3I_2 + I^2I_3 + II_4 + I_2^2 + \Omega$$
$$\Lambda_4 = I^5I_2 + I^4I_3 + I^3I_4 + I_2I_4 + I_3^2 + \Omega$$
$$\Lambda_5 = I^5I_4 + I_4^2 + \Omega$$
$$\Upsilon_0 = \Omega = II_2^2 + I^6I_2 + I^{11}$$
$$\Upsilon_1 = I^5I_3 + I^4I_4 + I^2I_1I_4 + I_3I_4 + \Omega$$
$$\Upsilon_2 = I^4I_2 + I^3I_3 + I^2I_4 + II_1I_3 + I_1I_4 + I_2I_3 + \Omega$$
$$\Upsilon_3 = I^2I_2 + II_3 + I_4 + I_1I_2 + \Omega$$
$$\Upsilon_4 := II_1 + I_2 + \Omega.$$

The last ideal is introduced here for its utility in this case; such an ideal does not seem to be readily available in the more general context. That the condition $(\Upsilon_n, \Lambda_1) \subseteq \Upsilon_{n-1}$ is

https://doi.org/10.4153/CJM-1996-055-x Published online by Cambridge University Press

satisfied for $1 \leq n \leq 3$ follows from Lemma 1.14; it is not difficult to use the techniques of Section 1 to show that it is true for $n = 4$ as well. It is also simple to check that $I\Lambda_n \subseteq \Upsilon_{5-n}$ for $2 \leq n \leq 5$.

Once again we set out to expand t_1^p but this time for $p = 5$. We factor the element differently to avail ourselves of the more precise results we have proved concerning the nilpotency class of the group $\overline{1 + I^2}$. To ease the notation, write $u := 1 + (s-1)^2$. By the Hall-Petrescu formula, $1 = t_1^5 = (x_1\bar{u}^b)^5(\overline{1+\beta})^5 v_2^5 v_3^5 v_4^5 v_5$ where, for $2 \leq n \leq 5$, $v_n \in \gamma_n(\langle x_1\bar{u}^b, \overline{1+\beta}\rangle)$. Now $(\overline{1+\beta})^5 = 1$ by Lemma 2.4. For $2 \leq n \leq 4$, $v_n^5 = 1$ since $T_2^5 = 1$ by Lemma 1.11. Lastly we show that $v_5 = 1$. Note that $\overline{1+(s-1)(s_1-1)}$, $\overline{1+(s_1-1)^2}$ and s_2 are in $1 + II_1 + I_2$, a subset of $1 + \Upsilon_4$, and that $\overline{1+\Upsilon_4} \leq \zeta_4(T)$ by the remark in the previous paragraph. Next we show that $\overline{1+I^3} \leq \zeta_4(T)$ as well. Now (I^3, I) is contained in I^4 and in FGI_2; as seen in the proof of Lemma 1.12, it follows that $(I^3, I) \subseteq I^2 I_2 + II_3 + I_4$ which is in Υ_3; hence $[\overline{1+I^3}, T] \leq \overline{1+\Upsilon_3} \leq \zeta_3(T)$ by Proposition 1.13; thus $\overline{1+I^3} \leq \zeta_4(T)$ as desired. Consequently, $\gamma_5(\langle x_1\bar{u}^b, \overline{1+\beta}\rangle) = 1$. Thus $(x_1u^b)^5 \equiv 1$ modulo $1 + \Omega$.

As we can go no further using the Hall-Petrescu identity, we will calculate $(x_1u^b)^5$ by using the techniques of restricted Lie algebras. For this we view x_1u^b as $x_1(u^b - 1) + x_1$. Working in FG/Ω as restricted Lie algebra of characteristic 5 and adapting the notation standard in this setting [7, Section V.7], we see that, modulo Ω,

$$(x_1u^b)^5 \equiv \big(x_1(u^b-1)\big)^5 + x_1^5 + \sum_{1\leq i\leq 4} S_i\big(x_1(u^b-1), x_1\big).$$

But, modulo I^3, $x_1(u^b - 1) \equiv u^b - 1 \equiv b(s-1)^2$ so that $\big(x_1(u^b-1)\big)^5 \equiv b^5(s-1)^{10} \equiv b(s_4-1)^2$ modulo Ω as $b^5 = b$ in F, $(s-1)^5 = s_4 - 1$ and $I^{11} \subseteq \Omega$. Therefore, modulo Ω,

$$(x_1u^b)^5 \equiv 1 + b(s_4-1)^2 + \sum_{1\leq i\leq 4} S_i\big(x_1(u^b-1), x_1\big).$$

For $p = 5$, Jacobson has conveniently given the values of the S_i in [7, Section V.7]. If μ, ν are elements of a restricted Lie algebra, then

$$\begin{aligned}
S_1(\mu,\nu) &= (\mu,\nu,\nu,\nu,\nu),\\
2S_2(\mu,\nu) &= (\mu,\nu,\mu,\nu,\nu) + (\mu,\nu,\nu,\mu,\nu) + (\mu,\nu,\nu,\nu,\mu),\\
3S_3(\mu,\nu) &= (\mu,\nu,\mu,\mu,\nu) + (\mu,\nu,\mu,\nu,\mu) + (\mu,\nu,\nu,\mu,\mu),\\
4S_4(\mu,\nu) &= (\mu,\nu,\mu,\mu,\mu).
\end{aligned}$$

The reliable calculation of the values of the S_i in our case is not a easy matter. As a check for the industrious reader, we give the results of our calculations, modulo Ω, for $\mu = x_1(u^b - 1)$ and $\nu = x_1$. Indication of our intermediate steps is also provided along with some general principles. We begin with these.

LEMMA 2.5. *Let $\tau_i \in \Lambda_1 \cup (1 + \Lambda_1)$, $1 \leq i \leq 5$. Suppose that, for some j, $\tau_j = \tau_j'\tau_j''$ where $\tau_j', \tau_j'' \in 1 + \Lambda_1$. Then, modulo Ω,*

$$(\tau_1, \ldots, \tau_j, \ldots, \tau_5) \equiv (\tau_1, \ldots, \tau_j', \ldots, \tau_5) + (\tau_1, \ldots, \tau_j'', \ldots, \tau_5).$$

PROOF. We may assume that, for $i \neq j$, $\tau_i \in \Lambda_1$. The following is the key observation; its proof makes use of the properties of and interrelationships between the Λ and Υ ideals. For $2 \leq m \leq 5$ and $1 \leq i \leq m$, let $\sigma_i \in \Lambda_1$. Then, modulo $1 + \Upsilon_{5-m}$,

$$[1 + \sigma_1, \ldots, 1 + \sigma_m] \equiv 1 + (\sigma_1, \ldots, \sigma_m).$$

To prove this, note first that, for $1 \leq n \leq 4$, if $\rho \in \Lambda_n$ and $\sigma \in \Lambda_1$, then $(\rho, \sigma) = (1 + \sigma)(1 + \rho)([1 + \rho, 1 + \sigma] - 1)$ whence $[1 + \rho, 1 + \sigma] \equiv 1 + (\rho, \sigma)$ modulo $1 + \Upsilon_{5-(n+1)}$. This is because $[1 + \Lambda_n, 1 + \Lambda_1] \leq 1 + \Lambda_{n+1}$ and $I\Lambda_{n+1} \subseteq \Upsilon_{5-(n+1)}$. The observation now follows by induction on m. The case $m = 2$ has just been demonstrated. If $m < 5$, the induction hypothesis shows that, for some $\gamma \in \Upsilon_{5-m}$,

$$\begin{aligned}[1 + \sigma_1, \ldots, 1 + \sigma_{m+1}] &= [1 + (\sigma_1, \ldots, \sigma_m)(1 + \gamma), 1 + \sigma_{m+1}] \\ &\equiv [1 + (\sigma_1, \ldots, \sigma_m), 1 + \sigma_{m+1}] \\ &\equiv 1 + (\sigma_1, \ldots, \sigma_{m+1}) \bmod 1 + \Upsilon_{5-(m+1)};\end{aligned}$$

the last steps follow from Lemma 1.14 and the previous remark since $(\sigma_1, \ldots, \sigma_m) \in \Lambda_m$ by Proposition 1.9.

To make use of this observation in the proof of the lemma, we rely upon the fact that, in a group of nilpotency class c, c-fold commutators are multiplicative in each variable [6, III.6.8]. Thus, modulo $1 + \Omega$,

$$[1 + \tau_1, \ldots, \tau_j, \ldots, 1 + \tau_5] \equiv [1 + \tau_1, \ldots, \tau_j', \ldots, 1 + \tau_5][1 + \tau_1, \ldots, \tau_j'', \ldots, 1 + \tau_5].$$

The observation then gives

$$1 + (\tau_1, \ldots, \tau_j, \ldots, \tau_5) \equiv \big(1 + (\tau_1, \ldots, \tau_j', \ldots, \tau_5)\big)\big(1 + (\tau_1, \ldots, \tau_j'', \ldots, \tau_5)\big)$$

as $\Omega = \Upsilon_0$. But the product of two such 5-fold Lie commutators is 0 modulo Ω because $\Lambda_5 \subseteq I^8$ and $I^{16} \subseteq \Omega$. The result follows.

COROLLARY 2.6. *Let $\tau_i \in \Lambda_1 \cup (1 + \Lambda_1)$, $1 \leq i \leq 5$. Suppose that $\tau_j = x_1(u^b - 1)$ for some j. Then, modulo Ω, $(\tau_1, \ldots, \tau_j, \ldots, \tau_5) \equiv b(\tau_1, \ldots, u, \ldots, \tau_5)$. As a consequence, $S_i\big(x_1(u^b - 1), x_1\big) \equiv k^{5-i}b^i S_i(u, s_1)$ for $1 \leq i \leq 4$.*

PROOF. The fact that Lie commutators are linear in each variable gives the equation $(\tau_1, \ldots, \tau_j, \ldots, \tau_5) = (\tau_1, \ldots, x_1u^b, \ldots, \tau_5) - (\tau_1, \ldots, x_1, \ldots, \tau_5)$. But, by the lemma,

$$(\tau_1, \ldots, x_1u^b, \ldots, \tau_5) \equiv (\tau_1, \ldots, x_1, \ldots, \tau_5) + b(\tau_1, \ldots, u, \ldots, \tau_5) \bmod \Omega$$

from which the first point follows. Its repeated application, together with appeals to the lemma itself for the factors k, establishes the last.

This corollary simplifies the calculation of the required 5-fold Lie commutators. We now set about finding their values by calculating the values of the various constituent

Lie commutators in u and s_1. Because of Lemma 1.14, it is only necessary to carry out these calculations modulo the appropriate term Υ_i; this provides further simplification:

$$(u, s_1) \equiv -2(s-1)(s_2-1) - (s_3-1) \bmod \Upsilon_3$$
$$(u, s_1, s_1) \equiv 2(s-1)(s_4-1) - 2(s_2-1)^2 \bmod \Upsilon_2$$
$$(u, s_1, u) \equiv (s-1)^2(s_3-1) + (s-1)(s_4-1) \bmod \Upsilon_2$$
$$(u, s_1, s_1, s_1) \equiv -(s_2-1)(s_4-1) \bmod \Upsilon_1$$
$$(u, s_1, s_1, u) \equiv -(s_2-1)(s_4-1) - (s_3-1)^2 \bmod \Upsilon_1$$
$$(u, s_1, u, s_1) \equiv -(s_2-1)(s_4-1) - (s_3-1)^2 \bmod \Upsilon_1$$
$$(u, s_1, u, u) \equiv 2(s-1)^3(s_4-1) \bmod \Upsilon_1.$$

Thus, modulo Ω, the eight relevant 5-fold brackets are:

$$(u, s_1, s_1, s_1, s_1) \equiv (s_4-1)^2$$
$$(u, s_1, s_1, s_1, u) \equiv -(s_4-1)^2$$
$$(u, s_1, s_1, u, s_1) \equiv (s_4-1)^2$$
$$(u, s_1, s_1, u, u) \equiv 2(s_4-1)^2$$
$$(u, s_1, u, s_1, s_1) \equiv (s_4-1)^2$$
$$(u, s_1, u, s_1, u) \equiv 2(s_4-1)^2$$
$$(u, s_1, u, u, s_1) \equiv -2(s_4-1)^2$$
$$(u, s_1, u, u, u) \equiv 0.$$

We now complete the calculation of $(x_1u^b)^5$ modulo $1+\Omega$. Our work has given the values of the S_i's modulo Ω as:

$$S_1\big(x_1(u^b-1), x_1\big) \equiv b(s_4-1)^2$$
$$S_2\big(x_1(u^b-1), x_1\big) \equiv -2k^3b^2(s_4-1)^2$$
$$S_3\big(x_1(u^b-1), x_1\big) \equiv -k^2b^3(s_4-1)^2$$
$$S_4\big(x_1(u^b-1), x_1\big) \equiv 0.$$

Thus, modulo $1+\Omega$, $1 = (x_1u^b)^5 \equiv 1 - (k^2b^2 + 2k^3b + 3)b(s_4-1)^2$. Since $(s_4-1)^2 \not\equiv 0$ modulo Ω and $k^2b^2 + 2k^3b + 3 = (k^3b)^2 + 2(k^3b) + 3 \not\equiv 0$ modulo 5, it must be the case that $b = 0$, the long-sought-for conclusion. This completes the proof of Proposition 2.3 and, with it, the proof of our main theorem.

REFERENCES

1. C. Bagiński and A. Caranti, *The modular group algebras of p-groups of maximal class*, Canad. J. Math. **40**(1988), 1422–1435.
2. C. Bagiński, *Modular group algebras of 2-groups of maximal class*, Comm. Algebra **20**(1992), 1229–1241.
3. N. Blackburn, *On a special class of p-groups*, Acta Math. **100**(1958), 45–92.

https://doi.org/10.4153/CJM-1996-055-x Published online by Cambridge University Press

4. J. J. Cannon, *An introduction to the group theory language, Cayley*. In: Computational Group Theory, (ed. M. D. Atkinson), Academic Press, London, 1984, 145–183.
5. X. Du, *The centers of a radical ring*, Canad. Math. Bull. **35**(1992), 174–179.
6. B. Huppert, *Endliche Gruppen I*, Springer, Berlin, 1967.
7. N. Jacobson, *Lie Algebras*, Dover, New York, 1979.
8. R. James, *The groups of order p^6 (p an odd prime)*, Math. Comp. **34**(1980), 613–637.
9. G. O. Michler, M. F. Newman and E. A. O'Brien, *Modular group algebras*, unpublished report, Australian National Univ., Canberra, 1987.
10. K. W. Roggenkamp and L. L. Scott, *Automorphisms and nonabelian cohomology: an algorithm*, Linear Algebra Appl. **192**(1993), 355–382.
11. M. A. M. Salim and R. Sandling, *The unit group of the modular small group algebra*, Math. J. Okayama Univ., to appear.
12. R. Sandling, *The isomorphism problem for group rings: a survey*. In: Orders and Their Applications, Oberwolfach, 1984, (eds. I. Reiner and K. W. Roggenkamp), Lecture Notes in Math. **1142**, Springer, Berlin, 1985, 256–288.
13. ———, *The modular group algebra of a central-elementary-by-abelian p-group*, Arch. Math. (Basel) **52**(1989), 22–27.
14. ———, *The modular group algebra problem for metacyclic p-groups*, Proc. Amer. Math. Soc. **124**(1996), 1347–1350.
15. M. Wursthorn, *Die modularen Gruppenringe der Gruppen der Ordnung 2^6*, Diplomarbeit, Universität Stuttgart, 1990.
16. ———, *Isomorphisms of modular group algebras: An algorithm and its application to groups of order 2^6*, J. Symb. Comput. **15**(1994), 211–227.

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

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