Math. J. Okayama Univ. **37**(1995), 15–25

THE UNIT GROUP OF THE MODULAR SMALL GROUP ALGEBRA

MOHAMED A. M. SALIM and ROBERT SANDLING

The unit group of the small group algebra of a finite p-group in characteristic p has a structure which mimics that of the original group. The normalised unit group is also a p-group. As such its structure is dependent on the behaviour of commutators and p-th powers. In the case studied here this behaviour is particularly favourable. Its upper and lower central series are described. Attractive commutator formulae, both for elements and for certain subgroups, are presented. Facts concerning p-th power structure are given. These results are of value in the study of the isomorphism problem. New invariants of a group determined by its modular group algebra are derived, some involving centralisers of sections of the group, others amplifying those stated in [7].

Let p be a fixed prime and let G be a finite p-group. FG will denote its modular group algebra over the field F of p elements. The augmentation ideal of FG will be denoted as $I = I(G) = I(FG)$. 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 quotient $FG/I(G)I(G_2)$, where G_2 denotes the commutator subgroup of G, is called the small group algebra of G over F. Often we will abbreviate $I(G_2)$ to I_2. The quotient $V/(1+II_2)$ may be identified with the group of normalised units of the unit group of the small group algebra. This is the group which is the object of study here; it will be denoted by $S = S(FG)$. Note that S is the Sylow p-subgroup of $U(FG/II_2)$.

As $G \cap 1 + II_2 = \Phi(G_2) = G_2'G_2^p$, studies of the small group algebra give information only about the group $G/G_2'G_2^p$. Unless stated otherwise we will assume throughout that the subgroup $G_2'G_2^p = 1$, that is, that the commutator subgroup of G is elementary abelian. As justified by this assumption we will view G as embedded in the small group algebra and in S.

Recall from [6] that the group algebra FG determines $|G_2|$ and $|G_2 : \Phi(G_2)|$. It follows that any group basis of FG has an elementary abelian commutator subgroup and also embeds in the unit group of the small group algebra. There it supplements the image of the canonical subgroup $1 + I^2$. Our second section studies subgroups with this latter property, showing them to share many features with G and with S. The results here establish various aspects of G as group algebra invariants. Our third section adds to this list of invariants, focussing on centralisers in G of certain canonical sections. Some of the results are valid for the general p-group.

The n-th term of the lower central series of a group X will be denoted either by X_n or by $\gamma_n(X)$, of the lower central series of a Lie algebra L by $\gamma_n(L)$, of the upper central series of X by $\zeta_n(X)$ and of the upper central series of L by $\zeta_n(L)$. The convention followed here has $X_1 = X$. The n-th modular dimension subgroup will be denoted by $D_n = D_n(X)$. For $Y, Z \subseteq X$, the subgroup generated by all commutators $[y, z]$, $y \in Y, z \in Z$, will be denoted $[Y, Z]$.

The following observations are used repeatedly in the paper without comment. Recall that, if N is a normal subgroup of a p-group X, then $X \cap 1 + I(X)I(N) = \Phi(N)$. If N is elementary abelian so that N may be interpreted as a right FX-module, then its submodule $NI(X)$ is the subgroup $[N, X]$. Thus, for $m \geq 1$, $N{\cdot}I(X)^m = [N, \overbrace{X, \ldots, X}^{m}]$. In particular, if X_k is elementary abelian, then $X_n I(X)^m = X_{n+m}$, for all $m \geq 1$, $n \geq k$.

Group ring elements will be denoted by Greek letters, e.g., α, β, … ; units will be denoted by Roman letters, e.g., u, v, … . Group commutators will be denoted by square brackets and Lie commutators by round ones, viz., for $\alpha, \beta \in I$, $(\alpha, \beta) = \alpha\beta - \beta\alpha$ while $[1 + \alpha, 1 + \beta] = (1 + \alpha)^{-1}(1 + \beta)^{-1}(1 + \alpha)(1 + \beta)$. Longer commutator expressions are left-normed. Note that $(FG, FG) = FGI_2$ so that $V' \leq 1 + FGI_2$.

The symbol $\equiv$ will denote congruence of elements of FG modulo II_2 or of units in V modulo $1 + II_2$. Note that, for $u, v \in V$, $u \equiv v$ in FG is the same as $u \equiv v$ in V. Also the bar notation will be used to denote equivalence classes modulo II_2 or $1 + II_2$ as appropriate to the context (e.g., $\overline{1 + I^n}$).

1. Commutators and p-th powers. We begin by stating results which describe central series in S. The first augments Proposition 1.2 of [1], which states that G and S have the same nilpotency class. The second is no more than a special case of Du's Theorem [3] but is stated and proved here independently because of the simplicity of doing so in this case.

Theorem 1.1. *For $n \geq 2$, $S_n = G_n = 1 + \gamma_n(I/II_2)$.*

As S is an invariant of the modular group algebra of G, this result shows that FG determines the terms of the lower central series of G, except for the first, up to isomorphism as FG-modules. As with each of our results this may be interpreted as a fact about the group algebra of a general p-group G but with reference to its quotient $G/\Phi(G_2)$, viz., that FG determines the dimensions of the elementary abelian factor groups $G_n\Phi(G_2)/\Phi(G_2)$ for $n \geq 2$.

Theorem 1.2. *For $m \geq 0$, $\zeta_m(S) = 1 + \zeta_m(I/II_2)$.*

While the relationship between the upper central series of S and of G is not so close as was the case with their lower central series, the relation between the terms of the two may be specified precisely.

Theorem 1.3. *For $m \geq 0$, $\zeta_m(G) = G \cap \zeta_m(S)$. Furthermore, for $n \geq 2$ and $m \geq 0$, $G_n \cap \zeta_m(G) = S_n \cap \zeta_m(S)$; consequently, the isomorphism type of $G_n \cap \zeta_m(G)$ is determined by the group algebra of G over F.*

We begin the proofs of our results by stating two lemmas which give formulae setting out the favourable behaviour of group and Lie commutators in the small group algebra. The more fundamental and simple ones are stated in the first without proof.

Lemma 1.4. *For $u, v, w \in V$ and $\alpha, \beta, \gamma \in I$, we have*
(i) $(u, v) \equiv [u, v] - 1$; *equivalently*, $[1 + \alpha, 1 + \beta] \equiv 1 + (\alpha, \beta)$;
(ii) $\alpha\beta\gamma \equiv \alpha\gamma\beta$, *or, equivalently*, $\alpha(\beta, \gamma) \equiv 0$;
(iii) $(\alpha, \beta\gamma) \equiv (\alpha, \beta)\gamma \equiv (\alpha\gamma, \beta)$;
(iv) $(\alpha\beta)^n \equiv \alpha^n\beta^n$ *for $n \geq 0$.*

Lemma 1.5. *Let $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n \in I$, $m, n \geq 2$. Then*
(1) $(\alpha_1, \alpha_2, \ldots, \alpha_m) \equiv (\alpha_1, \alpha_2 \ldots \alpha_m)$;
(2) $[1 + \alpha_1, 1 + \alpha_2, \ldots, 1 + \alpha_m] \equiv 1 + (\alpha_1, \alpha_2, \ldots, \alpha_m)$;
(3) $[1 + \prod \alpha_i, 1 + \prod \beta_j] \equiv [1 + \alpha_1, 1 + \beta_1, 1 + \alpha_2, \ldots, 1 + \alpha_m, 1 + \beta_2, \ldots, 1 + \beta_n]$;
(4) $[1 + \sum \alpha_i, 1 + \sum \beta_j] \equiv \prod[1 + \alpha_i, 1 + \beta_j]$.

Proof. (1) This is proved by induction using (iii) and the fact that $I(G)(FG, FG) = II_2$.

(2) This generalisation of (i) is also proved by induction, (i) itself supplying the induction step.

(3) Using (1) twice, we see that

$$\begin{aligned}(\textstyle\prod \alpha_i, \prod \beta_j) &\equiv (\textstyle\prod \alpha_i, \beta_1, \beta_2, \ldots, \beta_n)\\ &= -(\beta_1, \textstyle\prod \alpha_i, \beta_2, \ldots, \beta_n)\\ &\equiv -(\beta_1, \alpha_1, \alpha_2, \ldots, \alpha_m, \beta_2, \ldots, \beta_n)\\ &= (\alpha_1, \beta_1, \alpha_2, \ldots, \alpha_m, \beta_2, \ldots, \beta_n).\end{aligned}$$

Now (i) and (2) give the required equivalence.

(4) By (i), $[1+\sum \alpha_i, 1+\sum \beta_j] \equiv 1+\sum(\alpha_i, \beta_j)$. Since $I_2^2 \equiv 0$, this is equivalent to $\prod(1+(\alpha_i, \beta_j))$. Now (i) shows this to be the required product.

These lemmas dealt with elements. Our next applies them to give a result which describes commutators of subsets and subgroups, the first of several.

Lemma 1.6. *Let $X \subseteq S$. Then $[X, S] = [X, G]$.*

Proof. Let $x \in X$ and $s \in S$. If $s = \overline{1+\sum a_i(g_i - 1)}$ for some $g_i \in G$ and $a_i \in F$, then, by (4), $[x, s]$ is equal to $\prod [x, g_i]^{a_i}$ (here the elements of F as exponents are interpreted as the corresponding integers from the set $\{0, 1, \ldots, p-1\}$).

The proofs of our results about central series in S require little of these preliminaries.

Proof of Theorem 1.1. In the identification of G as a subgroup of S, $G_2 = G_2(\overline{1+II_2}) = \overline{1+FGI_2}$. As $FG/FGI_2 = FG/FG(FG, FG)$ is commutative, $S_2 \leq G_2$ and so $S_2 = G_2$. The proof proceeds by induction: for $n \geq 2$, $G_{n+1} = [G_n, G] = G_n I(G)$. Note that $G_2 II_2 = 1$. Any FG-module M for which $MII_2 = 0$ may be interpreted as an FS-module; moreover, in this case, $MI(G) = MI(S)$. Thus $G_n I(G) = G_n I(S)$. Lastly $G_n I(S) = S_n I(S) = S_{n+1}$.

The identification of the terms of the lower central series of I/II_2 is obtained from (2).

Proof of Theorem 1.2. Let L denote I/II_2; we want to show that, for $\alpha \in I$, $\overline{1+\alpha} \in \zeta_m(S)$ if and only if $\bar{\alpha} \in \zeta_m(L)$. Take $m > 0$. We must show that $\overline{1+\alpha} \in \zeta_m(S)$ if and only if $[\overline{1+\alpha}, \overline{1+\beta}] \equiv 1 \bmod \zeta_{m-1}(S)$ for all $\beta \in I$. But since $[\overline{1+\alpha}, \overline{1+\beta}] = \overline{1+(\alpha,\beta)}$ by (i), the above condition is equivalent to $(\bar{\alpha}, \bar{\beta}) \in \zeta_{m-1}(L)$ so that the proof follows by induction.

Proof of Theorem 1.3. As the elements of V are linear combinations of the elements of G, it is immediate that $G \cap \zeta(V) = \zeta(G)$. The same is true for S. The proof proceeds by induction. Take $m \geq 2$. It is clear that $G \cap \zeta_m(S) \leq \zeta_m(G)$. For the converse, let $g \in \zeta_m(G)$. From Lemma 1.6, $[g, S] = [g, G]$ which is in $\zeta_{m-1}(G)$; by induction, this is $G \cap \zeta_{m-1}(S)$ so that $g \in \zeta_m(S)$ as required.

The last points follow from the first because of Theorem 1.1.

We continue with further propositions advancing our intention of displaying the attractive behaviour of the powers of the augmentation ideal in commutator formulae in this context.

Proposition 1.7. *For $X \subseteq S$ and $n \geq 1$, the subgroup* $[X, \overline{1+I^n}] = [X, \overbrace{S, \ldots, S}^{n}] = [X, \overbrace{G, \ldots, G}^{n}]$. *In particular,* $[G, \overline{1+I^n}] = G_{n+1}$ *and* $[S, \overline{1+I^n}] = G_{n+1}$.

Proof. By definition $[X, \overline{1+I^n}] = \langle [x, \overline{1+\beta}] \colon x \in X, \beta \in I^n \rangle$. An element β in I^n can be written as a linear combination: $\beta = \sum a_i \beta_{i1} \beta_{i2} \cdots \beta_{in_i}$, $n_i \geq n$, $a_i \in F$, $\beta_{ij} \in I$. It follows from formula (4) that, for $\alpha \in I$, $[1+\alpha, 1+\beta] \equiv \prod [1+\alpha, 1+\beta_{i1} \cdots \beta_{in_i}]^{a_i}$. Now (3) applies to show that

$$[X, \overline{1+I^n}] = \langle [x, \overline{1+\beta_1}, \ldots, \overline{1+\beta_m}] \colon x \in X, \beta_i \in I, m \geq n \rangle,$$

that is, $[X, \overline{1+I^n}]$ is generated by all $[x, s_1, \ldots, s_m]$, $x \in X$, $s_j \in S$, $m \geq n$. But the subgroup $[X, S, \ldots, S]$ is also generated by these commutators. Equality with the other expression follows from Lemma 1.6.

The final point of the statement now follows from Theorem 1.1.

Corollary 1.8. *For $k, \ell \geq 1$,* $[\overline{1+I(G)^k}, \overline{1+I(G)^\ell}] = G_{k+\ell}$.

Proof. While a direct proof based on (3) and (4) is instructive, we deduce the statement from the Proposition: $[\overline{1+I^k}, \overline{1+I^\ell}] = [\overline{1+I^k}, G, \ldots, G] = [[G, \overline{1+I^k}], G, \ldots, G] = [G_{k+1}, G, \ldots, G] = G_{k+\ell}$.

Proposition 1.9. *Assume that $G_n = 1$. Then $\overline{1+I(G)^\ell} \leq \zeta_{n-\ell}(S)$ for ℓ in the range $1 \leq \ell \leq n-1$.*

Proof. By Proposition 1.7, $[S, \overline{1+I^{n-1}}] = G_n = 1$ so that $\overline{1+I^{n-1}} \leq \zeta(S)$. The proof proceeds by reverse induction on ℓ: for $\ell \geq 1$, $[S, \overline{1+I^{\ell}}] = G_{\ell+1} = S_{\ell+1} \leq \zeta_{(n-1)-\ell}(S)$ whence $\overline{1+I^{\ell}} \leq \zeta_{n-\ell}(S)$.

We finish this section with results on the p-th power structure of S. They have found application in the modular group algebra problem [5].

Lemma 1.10. *Let $m, n \geq 1$ and $n_i \geq n$ for $1 \leq i \leq m$. Take elements $x_{ij} \in G$ for $1 \leq i \leq m$, $1 \leq j \leq n_i$. Then, for $a \geq 0$, there is an element $g \in G_{np^a}$ such that*

$$\begin{aligned}&(\prod(1+(x_{i1}-1)(x_{i2}-1)\cdots(x_{in_i}-1)))^{p^a}\\ &\quad\equiv g\prod(1+(x_{i1}^{p^a}-1)(x_{i2}^{p^a}-1)\cdots(x_{in_i}^{p^a}-1)).\end{aligned}$$

Proof. By the Hall-Petrescu formula [4, III.9.4] and the fact that G_2 is elementary abelian, there is an element $g \in G_{np^a}$ such that

$$\begin{aligned}&(\prod(1+(x_{i1}-1)\cdots(x_{in_i}-1)))^{p^a}\\ &\quad\equiv g\prod(1+(x_{i1}-1)\cdots(x_{in_i}-1))^{p^a}.\end{aligned}$$

Using (iv) and the fact that the characteristic is p, we see that the latter is equivalent to $g\prod(1+(x_{i1}-1)^{p^a}\cdots(x_{in_i}-1)^{p^a})$ which, in turn, is equivalent to

$$g\prod(1+(x_{i1}^{p^a}-1)\cdots(x_{in_i}^{p^a}-1)).$$

Proposition 1.11. *Let K be a subgroup of G, $n \geq 1$ and $a \geq 0$. Then*

$$K_{np^a}(\overline{1+I(K)^n})^{p^a} = K_{np^a}(\overline{1+I(K^{p^a})^n}).$$

Proof. As $I(G)$ is nilpotent, each element of $1+I(K)^n$ can be expressed as a product of units $1+(x_{i1}-1)(x_{i2}-1)\cdots(x_{in_i}-1)$ as in the Lemma with $x_{ij} \in K$. The Lemma shows that the p^a-th power of the image of such a product is in $K_{np^a}(\overline{1+I(K^{p^a})^n})$. The other containment follows in the same way upon noting that the x's used above may be restricted to a generating set, i.e., each element of $1+I(K^{p^a})^n$ can be expressed as a product of factors $1+(x_{i1}^{p^a}-1)(x_{i2}^{p^a}-1)\cdots(x_{in_i}^{p^a}-1)$, $x_{ij} \in K$, $n_i \geq n$.

We conclude with two corollaries which demonstrate how this proposition may be applied.

Corollary 1.12. *Let K be a subgroup of G and $n \geq 2$. Then*

$$\log_p \exp(\overline{1+I(K)^n}) \leq \max\{\log_p \exp(KG_2/G_2), \lceil \log_p(\frac{c+1}{n})\rceil\}$$

where c denotes the nilpotency class of K.

Proof. Let a denote the expression on the right so that $(\overline{1+I(K)^n})^{p^a}$ $\leq \overline{1+I_2^2} = 1$ as $K_{np^a} = 1$.

Corollary 1.13. $G \cap (\overline{1+I^2})^p \leq G_{2p}\Phi(\Phi(G))$.

Proof. By the Proposition, $G \cap (\overline{1+I^2})^p \leq G \cap G_{2p}(\overline{1+I(G^p)^2})$ and this is contained in $G \cap G_{2p}(\overline{1+II(\Phi(G))})$. As $G_2 \leq \Phi(G)$, the latter subgroup is the same as the subgroup $G_{2p}(G \cap (1+II(\Phi(G))))$ which is $G_{2p}\Phi(\Phi(G))$.

2. Covering subgroups. In this section we examine subgroups of S which cover $S/\overline{1+I^2}$. Recall that U is such a subgroup if $S = U(\overline{1+I^2})$. Many features of S and G are shared by these subgroups. Aside from G and S itself, the most significant examples of such subgroups are group bases of FG. This follows from the fact that S and $\overline{1+I^2}$ are canonical. Our first results characterise group bases among covering subgroups.

Lemma 2.1. *Let J be a nilpotent ideal of an algebra A over a field F. Suppose that H is a subgroup of the unit group $U(A)$ which covers $(1+J)/(1+J^2)$. Then $F{\cdot}H$, the linear subspace of A spanned by H, is $F+J$.*

Proof. Let $I(H)$ denote the image of the augmentation ideal of the group ring FH under the algebra homomorphism $FH \longrightarrow A$ defined by the inclusion of H in $U(A)$. It is enough to show that $J = I(H)$. As J is nilpotent, an induction argument shows that it suffices to prove that $J^n = I(H)^n + J^{n+1}$ for all $n \geq 1$. We prove this by induction. The case $n = 1$ follows from the hypothesis as $1 + J = H(1+J^2) = 1 + I(H) + J^2$. The induction step is straightforward.

Corollary 2.2. *Let H be a subgroup of V of minimal order such that H covers $V/(1+I^2)$ or $\bar{H}$ covers $S/\overline{1+I^2}$. Then H is a group basis of FG.*

Proof. In both cases H covers $V/(1+I^2)$. The Lemma then shows that $F{\cdot}H$ is $F + I = FG$. Thus $|H| \geq |G|$. As G itself covers $V/(1+I^2)$, $|H| \leq |G|$ so that $|H| = |G|$ and the result follows.

Proposition 2.3. *Let U be a subgroup of S which covers $S/\overline{1\cdot+I^2}$. Then $U_n = S_n = G_n$ for $n \geq 2$. Consequently, $U \lhd S$, and U and G have the same nilpotency class.*

Proof. This may be proved by induction using Proposition 1.7, or by appeal to [2, 1.3] with the use of the Proposition to show that $\overline{1+I^2} \leq C_S(S/S_3)$.

Proposition 2.4. *Let G be of nilpotency class $c \geq 2$. Then $\zeta_{c-1}(S) = \zeta_{c-1}(G)(\overline{1+I^2})$. Moreover, if U covers $S/\overline{1+I^2}$, then $\zeta_{c-1}(S) = \zeta_{c-1}(U)(\overline{1+I^2})$.*

Proof. It suffices to prove the last statement. That $\zeta_{c-1}(S) = (U \cap \zeta_{c-1}(S))(\overline{1+I^2})$ follows from Proposition 1.9. We show that $U \cap \zeta_{c-1}(S) = \zeta_{c-1}(U)$, for which it need only be shown that, if $u \in \zeta_{c-1}(U)$, then $u \in \zeta_{c-1}(S)$. Let s_i, $1 \leq i \leq c-1$, be elements of S so that $s_i = u_i(\overline{1+\alpha_i})$ for elements u_i of U and α_i of I^2. Because S_c is central and so a c-fold commutator is multiplicative in each variable, $[u, s_1, \ldots, s_{c-1}] = [u, u_1, \ldots, u_{c-1}]$ by Corollary 1.8. But the latter element is the identity by hypothesis.

Two corollaries of this Proposition follow from the fact that $\Phi(G) = G \cap \overline{1+I^2}$. The second is immediate; note that the statement concerning G is satisfied if $d(G) = 2$.

Corollary 2.5. *Let G be of nilpotency class c. Then the index of $\zeta_{c-1}(G) \cap \Phi(G)$ in $\zeta_{c-1}(G)$ is determined by FG.*

Proof. By Theorem 1.1, c is a group algebra invariant for a group G in which $\Phi(G_2) = 1$; the result follows readily.

Corollary 2.6. *Let G be of nilpotency class $c \geq 2$. Then $\zeta_{c-1}(S) = \overline{1+I^2}$ if and only if $\zeta_{c-1}(G) \leq \Phi(G)$.*

Remark 2.7. Results such as those of the Propositions 2.3 and 2.4 and of the next section can be used to show that FG determines relationships between subgroups containing $\Phi(G)$. For example, suppose that a subgroup L is canonical in the sense that $FGI(L)$ is determined by FG (we have in mind subgroups such as $\Omega_i(G \bmod G_2) = \langle x \in G\colon x^{p^i} \in G_2 \rangle$ [6, Note on 6.20]). Then the subgroup $1 + I(L) + I^2$ is also determined. It may be expressed as $(1+I(L))(1+I^2)$ or $L(1+I^2)$ so that, in S, $L(\overline{1+I^2})$ is determined. Under the isomorphism $S/\overline{1+I^2} \approx G/\Phi(G)$, this subgroup is identified with $L\Phi(G)/\Phi(G)$. It follows that FG determines whether or not $L\Phi(G)$ is equal to $\zeta_{c-1}(G)\Phi(G)$, or to $C_G(G_n/G_{n+2})$ for some $n \geq 1$ (see below).

3. Centralisers. In this section we show that the orders of several centralisers are group algebra invariants. Some of these centralisers are used in the analysis of the modular group algebra problem for p-groups of order p^5 [5]. While we will relax at the end our assumption that G has an elementary abelian commutator subgroup, we begin with results which continue the theme of the previous section.

Proposition 3.1. *For $n \geq 1$, $C_S(S_n/S_{n+2}) = C_G(G_n/G_{n+2})(\overline{1+I^2})$. Moreover, if U covers $S/\overline{1+I^2}$, then $C_S(S_n/S_{n+2}) = C_U(U_n/U_{n+2})(\overline{1+I^2})$ for $n \geq 1$.*

Proof. It suffices to prove the last statement. By Propositions 1.7 and 2.3 the subgroup $\overline{1+I^2}$ is contained in $C_S(U_n/U_{n+2})$ since $U_{n+2} = S_{n+2}$. Thus $C_S(U_n/U_{n+2}) = C_U(U_n/U_{n+2})(\overline{1+I^2})$. For $n \geq 2$ it is also the case that $U_n = S_n$ and the result follows. For $n = 1$, $C_S(U/U_3) = C_S(S/S_3)$ because $S = U(\overline{1+I^2})$ and $[\overline{1+I^2}, S] \leq S_3 = U_3$.

Lemma 3.2. *For $n \geq 1$, $\Phi(G) \leq C_G(G_n/G_{n+2})$.*

Proof. We need only show that $[G_n, G^p] \leq G_{n+2}$. Let $x \in G_n$, $y \in G$. Then, by the Hall-Petrescu formula, $[x, y^p] = [x,y]^p u_2^{\binom{p}{2}} u_3^{\binom{p}{3}} \cdots u_p$ for some $u_j \in \gamma_j(\langle y^{-x}, y\rangle) = \gamma_j(\langle [x,y], y\rangle)$, $2 \leq j \leq p$. As G_2 is of exponent p, $[x, y^p] = u_p \in G_{n+p}$.

Corollary 3.3. *For $n \geq 1$, the order of $C_G(G_n/G_{n+2})$ is determined by FG.*

Proof. Because of the Lemma, the result follows from the Proposition since $\Phi(G) = G \cap \overline{1+I^2}$.

In our last items we drop the assumption that the commutator subgroup of G is elementary abelian. We interpret V as acting on sections of FG and of V by conjugation. Centralisers in I are with respect to the adjoint action as in [1]; thus, by definition, $C_I((FGI(N)+I^4)/I^4) = \{\alpha \in I\colon (\alpha, FGI(N)) \subseteq I^4\}$.

Proposition 3.4. *Let N be a normal subgroup of G such that $D_4 \leq N \leq \Phi(G)$. Then*

$$\begin{aligned} &C_V((1+FGI(N)+I^4)/(1+I^4)) \\ &\quad = C_V((FGI(N)+I^4)/I^4) \\ &\quad = 1+C_I((FGI(N)+I^4)/I^4) \\ &\quad = C_G(N/D_4)(1+I^2). \end{aligned}$$

Here V acts on sections of FG and of V by conjugation.

Proof. Let $U = C_V((1+FGI(N)+I^4)/(1+I^4))$. That $U = C_V((FGI(N)+I^4)/I^4)$ is immediate. Let $C = C_I((FGI(N)+I^4)/I^4)$. Note that $C = \{\alpha \in I\colon (\alpha, I(N)) \subseteq I^4\}$ because $(I, II(N)) \subseteq I^4$ as $N \leq \Phi(G) = D_2$. It is routine to show that, if $J, K, L \subseteq I$ and L is an ideal of FG, then $[1+J, 1+K] \leq 1+L$ if and only if $(J,K) \subseteq L$. It follows that $U = 1+C$.

From the assumption that $N \leq \Phi(G)$ it follows that $\Phi(G) \leq C_G(N/D_4)$ and $I^2 \subseteq C$. But then $U = (U \cap G)(1+I^2)$.

Lastly we show that $U \cap G = C_G(N/D_4)$. Put $M = C_G(N/D_4)$. Since $(I(M), I(N)) \subseteq FGI([M,N])$ and $[M,N] \leq D_4$, $(I(M), I(N)) \subseteq I^4$. It follows that $I(M) \subseteq C$ and so $M \leq U$. Conversely, if $g \in U \cap G$, then $(g-1, I(N)) \subseteq I^4$ so that $(g-1, n-1) = (g,n) \in I^4$ for all $n \in N$; as $(g,n) = ng([g,n]-1)$, $[g,n]-1 \in I^4$ whence $[g,n] \in D_4$. Consequently, $g \in C_G(N/D_4)$ as required.

Corollary 3.5. *Let N be a normal subgroup of G such that $D_4 \leq N \leq \Phi(G)$. If the ideal $FGI(N)$ is canonical in FG, then $|C_G(N/D_4)|$ is determined by FG.*

Proof. The hypothesis implies that $C = C_I((FGI(N)+I^4)/I^4)$ is also canonical in FG so that $|C|$ is determined. As seen $|C| = |M(1+I^2)|$ where $M = C_G(N/D_4)$. Thus $|C| = |M||1+I^2|/|M \cap (1+I^2)|$. Since $M \cap (1+I^2) = \Phi(G)$ and $|\Phi(G)|$ is determined, so is $|M|$.

Corollary 3.6. *$|C_G(\Phi(G)/D_4)|$ and $|C_G(G_2D_4/D_4)|$ are determined by FG.*

Proof. By [6, Note to 6.20], $FGI(\Phi(G))$ is canonical in FG. For $p \geq 5$, $G_2D_4 = \Phi(G)$ but, for $p = 2, 3$, $G_2D_4 = G_2G^{p^2}$ and the same reference applies to show that $FGI(G_2D_4)$ also is canonical in FG.

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

[3] X. Du: The centers of a radical ring, Canad. Math. Bull. **35** (1992), 174–179.

[4] B. Huppert: Endliche Gruppen I, Springer, Berlin, 1967.

[5] 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.

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

[7] R. Sandling: The modular group algebra of a central-elementary-by-abelian p-group, Arch. Math. (Basel) **52** (1989), 22–27.

M. A. M. Salim
Mathematics Department
Emirates University, Al-Ain
United Arab Emirates

R. Sandling
Mathematics Department
The University, Manchester M13 9PL
England
E-mail: rsandling@manchester.ac.uk

(*Received July 18, 1994*)
(*Revised February 15, 1996*)