Arch. Math., Vol. 52, 22–27 (1989)

0003-889X/89/5201-0022 $ 2.70/0

The modular group algebra of a central-elementary-by-abelian p-group

By

ROBERT SANDLING

In this paper two issues in the study of group rings are addressed for the modular group algebras of certain finite p-groups: the isomorphism problem, the extent to which a group is determined by its group ring; the problem of the existence of a normal complement for a group in the unit group. In the case of an integral group ring $\mathbb{Z}G$, there are satisfactory results when G is metabelian. It is a theorem of Jackson and of Whitcomb [cf. 22] that the isomorphism type of a finite metabelian group G is determined by $\mathbb{Z}G$. Metabelian groups figure prominently among the groups for which it has been established that G has a normal complement in $U(\mathbb{Z}G)$ [14; 3; 17, Prop. 1] but there are metabelian groups known for which G is not so complemented [17]. For the modular group algebra, the appropriate analogue to the class of metabelian finite groups may be that of elementary-abelian-by-abelian p-groups. Here we obtain the following two positive results for the subclass of *central-elementary-by-abelian p-groups*, p-groups G which have an elementary abelian central subgroup Z whose quotient G/Z is abelian.

1.1 Theorem. *Let G be a finite p-group. Suppose that $\gamma_2(G)^p\gamma_3(G) = 1$. Then there is a normal complement to G in $V(FG)$.*

1.2 Theorem. *Let G be a finite p-group. Then the section $G/\gamma_2(G)^p\gamma_3(G)$ is determined by FG.*

In these statements and in the paper, the notation is as follows: G will generally denote a finite p-group, F is the field of p elements, FG the modular group algebra, $I = I(FG)$ its augmentation ideal, $U = U(FG)$ its group of units, $V = V(G) = V(FG) = 1 + I$ its group of normalised units. The commutator subgroup $[G, G]$ is denoted variously as G' and $\gamma_2(G)$ while $\gamma_{n+1}(G) := [\gamma_n(G), G]$. The subgroup generated by the p-th powers of elements of a group G is denoted G^p. The Frattini subgroup $\Phi(G)$ is $G^p\gamma_2(G)$. A feature of G is said to be *determined by FG* if a group G^* also has this feature whenever FG is isomorphic to FG^* as algebra. A subset $S(G)$ of FG is said to be *canonical* if, under an augmented isomorphism φ from FG to FG^*, $\varphi(S(G)) = S(G^*)$.

Results on the modular isomorphism problem are surveyed in [22, §6]. Theorem 1.2 is reported there. It is a generalisation of two important cases for which positive results had been obtained: $G/\gamma_2(G)$ done by S. Takahashi and by Ward [24]; $G/M_3(G)$ done by Passi

and Sehgal [13; new generalisation in 19] (here $M_3(G)$ denotes the third dimension subgroup modulo p and is $G^p\gamma_3(G)$ for p odd and $G^4\gamma_3(G)$ for $p = 2$). A variety of methods have shown that many individual groups G, which happen to satisfy $\gamma_2(G)^p\gamma_3(G) = 1$, are determined by FG as can be seen in [22]. Certain classes of such groups have also yielded positive results: p-groups G for which $p = 2$, $|G:\zeta(G)| = 4$ and $\zeta(G)/\Omega(\zeta(G))$ is cyclic or elementary [11; 12] over any field of characteristic 2 (V. Drensky informs me that he has generalised this to $|G:\zeta(G)| = p^2$, any p, with the final condition removed); metacyclic p-groups with $|\gamma_2(G)| = p$, p odd [1].

Concerning normal complements fewer results are known. The question of whether G has a normal complement in $U(RG)$ seems to have originated in [24] and, in fact, in the setting of $R = F$ and G a finite p-group. It reappeared in [4], [8] and, to an extent, [20]. Ward showed that a finite abelian p-group G has a normal complement in $U(FG)$, a result in [8; 10] as well. For various other G, many of them central-elementary-by-abelian, normal complements to G in $V(FG)$ were exhibited in [8; 10; 6; 7; 18]. In [10; 6], examples of p-groups G were given for which there is no normal complement to G in $V(FG)$; none are elementary-abelian-by-abelian.

The examples in [18] are of p-groups, $p = 3$, which are elementary-abelian-by-C_3 and so of nilpotency class $\leqq 3$ (here C_3 denotes the cyclic group of order 3). They are only instances of a broader theory for elementary-abelian-by-abelian p-groups, p odd, in which Roggenkamp and Scott describe a large subgroup of $V(FG)$ which contains G and in which G has a normal complement. A more detailed exposition is given in [16]. It is possible to simplify their proof and some of the techniques developed here arose in doing so.

Further motivation for the results here came from computer-aided empirical work (computers played a role in [10; 6] as well). Using Fortran programs for group ring calculations and the packages Sogos [9] and Cayley [2] I obtained presentations for $V(G)$ for small G [23]. This facilitated the determination of such structural features as normal complements. In specific cases such as those done by Ivory and by Roggenkamp and Scott, I was able to produce a normal complement in a systematic manner. It sometimes differed from the known complement. For example, for the non-abelian group G of order 27 and exponent 9, the normal complement here and that from [16] are different but isomorphic.

L. G. Kovacs has proven theorems like those here for the subgroup $\Phi(G)^p[\Phi(G), G]$ instead of $\gamma_2(G)^p\gamma_3(G)$. Using them, he and M. F. Newman have shown that any group of order p^5 is determined by its modular group algebra.

Acknowledgements. I wish to thank the originators of Sogos and Cayley for making their packages available. I also wish to thank for its hospitality the Mathematische Forschungsinstitut Oberwolfach where these results were first presented.

Section 2: Proofs of Theorems 1.1 and 1.2. We begin the proofs with some general points about modular group algebras and with a review of the main technique of [21].

2.1 Lemma. *Let α and β be elements of I and L a left ideal of I. Then α and β are in the same coset of L if and only if $1 + \alpha$ and $1 + \beta$ are in the same left coset of the subgroup $1 + L$ of V.*

Proof. If $\alpha = \beta + \lambda$ for some λ in L, then

$$1 + \alpha = 1 + \beta + \lambda = (1 + \beta)(1 + (1 + \beta)^{-1}\lambda)$$

as required. Conversely, if $1 + \alpha = (1 + \beta)(1 + \lambda)$, $\alpha = \beta + (1 + \beta)\lambda$.

The next lemma has a long history (see the references for 3.13 and 6.13 of [22]). The first part is true for the arbitrary group G.

2.2 Lemma. *Let N be a normal subgroup of G. Then $I(N)FG/I(G)I(N)$ and $N/N'N^p$ are isomorphic as right FG-modules. Consequently, $I(N)FG/I(G)I(N) + I(N)I(G)$ is isomorphic to $N/[N, G]N^p$ and $G \cap 1 + I(G)I(N) + I(N)I(G) = [N, G]N^p$.*

In addition, $N/N'N^p$ is isomorphic to the multiplicative group

$$1 + I(N)FG/1 + I(G)I(N),\ 1 + I(N)FG = N(1 + I(G)I(N)) \text{ and}$$

$$\begin{aligned} 1 + I(G)I(N) + I(N)I(G) &= (1 + I(G)I(N))(1 + I(N)I(G)) \\ &= [N, G]N^p(1 + I(G)I(N)). \end{aligned}$$

2.3 Notation. Let $J = J(G)$ denote the ideal $I(G)I(G') + I(G')I(G)$ of FG. It follows from the previous lemma that $J = I(G_3)FG + I(G')I(G)$, that $G \cap 1 + J = \gamma_2(G)^p\gamma_3(G)$ and that $1 + I(G')FG = G'(1 + J)$. As the ideal $I(G')FG$ is canonical, it is clear that $J(G)$ is also canonical.

2.4 Lemma. *The ideal I^2/J is central in FG/J and the group $1 + I^2/1 + J$ is central in $V/1 + J$. Consequently, if α and β are in I and n is a positive integer, $(\alpha\beta)^n \equiv \alpha^n\beta^n$ modulo J.*

Proof. For the first point, it suffices to show that I^2 is centralised by G modulo J. This follows from the fact that, for all x, y, g in G, $((x-1)(y-1))^g = (x[x, g] - 1)(y[y, g] - 1)$ which is equivalent to $(x-1)(y-1)$ modulo J by standard identities. The second point is implied by Lemma 2.1. The final point is proved by induction.

The last concepts to be developed for the proofs of the theorems derive from those of [21] which we shall now recall. Assume that G is abelian with basis $\{x_1, \ldots, x_d\}$. With $\delta = (\delta_1, \ldots, \delta_d)$ a d-tuple of non-negative integers, not all zero, and with the convention that $(x-1)^0 = 1$ for $x \neq 1$, let $P(\delta) = \prod(x_j - 1)^{\delta_j}$. The main result of [21] stated that the elements $1 + P(\delta)$, $\delta \in D(G)$, form a basis of V where $D(G)$ is the set of those δ for which, for all j, $0 \leqq \delta_j < o(x_j)$, the order of x_j in G, and, for some j, p does not divide δ_j. Its proof indicates how the order of $1 + P(\delta)$ is calculated for $\delta \in D(G)$. The next lemma gives the order of any $1 + P(\delta)$.

2.5 Lemma. *Let G be abelian with basis $\{x_1, \ldots, x_d\}$. Let $\delta = (\delta_1, \ldots, \delta_d)$ be a d-tuple of non-negative integers, not all zero. Suppose that, for all j, $\delta_j \leqq o(x_j)$. If $\delta_j \neq 0$, let s_j be the*

highest power of p less than or equal to δ_j. Then the order of the element $1 + P(\delta) = 1 + \prod (x_j - 1)^{\delta_j}$ is the minimum of the numbers $o(x_j)/s_j$, taken over those j for which $\delta_j \neq 0$.

Proof. Let $q_j = o(x_j)$. We may assume that $0 < \delta_j < q_j$ for all j so that $P(\delta) \neq 0$. As the lemma is immediate if G is elementary abelian, a proof by induction is convenient. If $\delta_i \geqq q_i/p$ for some i, $(1 + P(\delta))^p = 1 + \prod (x_j^p - 1)^{\delta_j} = 1$. On the other hand, if $\delta_j \leqq q_j/p$ for all j, $(1 + P(\delta))^p = 1 + P^1(\delta)$ where $P^1(\delta) = \prod (x_j^p - 1)^{\delta_j}$ is the analogue of $P(\delta)$ for the group G^p with a subset of $x_1^p, \ldots, x_d^p$ taken as basis. By induction, $o(1 + P^1(\delta))$ $= \min \{o(x_j^p)/s_j\} = \min \{q_j/s_j\}/p$ so that $o(1 + P(\delta)) = \min \{q_j/s_j\}$ as required.

2.6 Definition. Let $\{x_1, \ldots, x_d\}$ be a minimal generating set for G. For a d-tuple δ of non-negative integers, not all zero, write $P(\delta) = (x_1 - 1)^{\delta_1}(x_2 - 1)^{\delta_2} \cdots (x_d - 1)^{\delta_d}$. Using $-$ to denote the projection from G to $\bar{G} = G/G'$ and its induced map on FG, write $\bar{P}(\delta) = \overline{P(\delta)} = \prod (\bar{x}_j - 1)^{\delta_j}$. As $\{\bar{x}_1, \ldots, \bar{x}_d\}$ forms a basis of $\bar{G}$, the subgroup of $V(\bar{G})$ generated by all $1 + \bar{P}(\delta)$, $\delta \in D(\bar{G})$ and $\sum \delta_j > 1$, is a direct complement to $\bar{G}$ in $V(\bar{G})$. Define $W = W(G)$ as the subgroup of $V(G)$ generated by $1 + J$ and by all $1 + P(\delta)$, $\delta \in D(\bar{G})$ and $\sum \delta_j > 1$. Thus $W(\bar{G}) = \overline{W(G)}$ and $V(\bar{G})$ is the direct product of $\bar{G}$ and $W(\bar{G})$. Note also that $W \leqq 1 + I^2$ so that W is a normal subgroup of V by Lemma 2.4.

2.7 Lemma. $W(G) \cap 1 + I(G')FG = 1 + J$.

Proof. It suffices to show that any product $\prod (1 + P(\delta))^{m_\delta}$ over $\delta \in D(\bar{G})$, $\sum \delta_j > 1$, which is in $1 + I(G')FG$, already is in $1 + J$. As $\prod (1 + \bar{P}(\delta))^{m_\delta} = 1$ in $V(\bar{G})$, it follows from the independence of the $1 + \bar{P}(\delta)$ that $o(1 + \bar{P}(\delta))$ divides m_δ for all δ.

For a fixed δ, the previous lemma shows that there is an index i and a power q of p such that $q = o(\bar{x}_i)/s_i$ divides m_δ, $0 < s_i \leqq \delta_i$. By Lemma 2.4 $P(\delta)^q \equiv P(q\delta)$ modulo J, where $(q\delta)_j = q\delta_j$, and so $(1 + P(\delta))^q \equiv 1 + P(q\delta)$ modulo $1 + J$. As $(\bar{x}_i - 1)^{q\delta_i} = 0$ in $F\bar{G}$, $(x_i - 1)^{q\delta_i}$ is in $I(G')FG$. If there is $j \neq i$ with $\delta_j \neq 0$, $P(q\delta)$ is in $I(G)I(G')$ or $I(G')I(G)$ so that $(1 + P(\delta))^q$ is in $1 + J$. If $\delta_j = 0$ for all $j \neq i$, then δ_i is not a power of p by the definition of $D(\bar{G})$ so that $(x_i - 1)^{q\delta_i}$ is in $I(G')^2 FG$ and again $(1 + P(\delta))^q$ is in $1 + J$. It is now clear that the product $\prod (1 + P(\delta))^{m_\delta}$ is in $1 + J$.

Only a little more remains for the proof of the main theorem of this section of which Theorems 1.1 and 1.2 are corollaries. For a central-elementary-by-abelian p-group it states that $W(G)$ is a normal complement to G in $V(FG)$.

2.8 Theorem. *Let G be a finite p-group. Then $V = G \cdot W(G)$ and $G \cap W(G)$ $= \gamma_2(G)^p \gamma_3(G)$. The quotient group $V/1 + J$ is isomorphic to the direct product $G/\gamma_2(G)^p \gamma_3(G) \times W(G/\gamma_2(G))$.*

Proof. As before, we use $-$ to denote projection onto $\bar{G} = G/G'$. As noted, $V(\bar{G}) = \bar{G} \cdot W(\bar{G})$ so that $V(G) = G \cdot W(G) \cdot (1 + I(G')FG) = G \cdot W(G) \cdot G'(1 + J)$ $= G \cdot W(G)$.

Since $\bar{G} \cap \bar{W} = 1$, $G \cap W \leqq G'$ and so $G \cap W = G' \cap W$ which is a subgroup of $1 + J$ by Lemma 2.7. Thus $G \cap W = G \cap 1 + J = \gamma_2(G)^p \gamma_3(G)$ by Lemma 2.2.

Lastly, W is central in V modulo $1 + J$ and $V = GW$ so that $G(1 + J)$ is normal in V. Also $G(1 + J) \cap W = (G \cap W)(1 + J) = 1 + J$. It follows that $V/1 + J$ is the direct prod-

uct of its subgroups $G(1+J)/1+J$ and $W/1+J$. But $G(1+J)/1+J$ is isomorphic to $G/G\cap 1+J = G/\gamma_2(G)^p\gamma_3(G)$ while

$$W/1+J = W/W\cap 1+I(G')FG$$
$$\approx W\cdot(1+I(G')FG)/1+I(G')FG = W(\bar{G}).$$

Our main results, Theorems 1.1 and 1.2, are readily deduced. The first is immediate. For the second recall that G/G' is determined by FG and so $W(G/G')$ is determined by the fundamental theorem of finite abelian groups. As $J(G)$ is canonical, $V(G)/1+J(G)$ is determined and Theorem 1.2 follows by the Krull-Schmidt theorem.

In conclusion we note some favourable behaviour for the broader class of elementary-abelian-by-abelian p-groups. The above results have been obtained in what Roggenkamp and Scott call a small group ring $FG/I(G)I(G')$. Let G be elementary-abelian-by-abelian so that $\gamma_2(G)^p\gamma_2(G)' = 1$ and G is embedded in this ring. The projection $V(G)\to V(\bar{G})$ gives an exact sequence

$$1\to G\to V(G)/1+I(G)I(G')\to W(\bar{G})\to 1$$

in which the last two terms are determined by FG. If $\gamma_3(G)=1$, the extension is a direct product by Theorem 2.8. If $\gamma_4(G)=1$, the sequence splits. Other considerations lead to a number of conclusions concerning the isomorphism problem. By Lemma 2.2 G' is determined as an FG-module and so as an $F\bar{G}$ module; any group basis for FG is then an extension of this module by the group $\bar{G}$ whose isomorphism type is also determined. Ward [24] showed that the centre $\zeta(X)$ of a p-group X is determined by FX; it follows from [22, 6.11] that, in this case, $G'\zeta(G)$ is determined along with its quotients by G' and by $\zeta(G)$. If $p\geqq 3$ and $\gamma_4(G)=1$, $\Phi(G)$ is in $G'\zeta(G)$ and can also be shown to be determined by FG, a slight improvement upon [5; 15].

References

[1] C. BAGINSKI, Groups of units of modular group algebras. Proc. Amer. Math. Soc. **101,** 619–624 (1987).

[2] J. J. CANNON, An introduction to the group theory language, Cayley. Computational group theory, 145–183, New York-London 1984.

[3] G. H. CLIFF, S. K. SEHGAL and A. R. WEISS, Units of integral group rings of metabelian groups. J. Algebra **73**, 167–185 (1981).

[4] R. K. DENNIS, The structure of the unit group of group rings. Ring theory II, 103–130, New York 1977.

[5] T. FURUKAWA, A note on isomorphism invariants of a modular group algebra. Math. J. Okayama Univ. **23**, 1–5 (1981).

[6] L. R. IVORY, A note on normal complements in mod p envelopes. Proc. Amer. Math. Soc. **79**, 9–12 (1980).

[7] L. R. IVORY, Normal complements in mod p envelopes. Ph.D. Thesis, Univ. of Alabama 1981.

[8] D. L. JOHNSON, The modular group-ring of a finite p-group. Proc. Amer. Math. Soc. **68**, 19–22 (1978).

[9] R. LAUE, J. NEUBÜSER and U. SCHOENWAELDER, Algorithms for finite soluble groups and the SOGOS system. Computational group theory, 105–135, New York-London 1984.

[10] L. E. MORAN and R. N. TENCH, Normal complements in mod p-envelopes. Israel J. Math. **27**, 331–338 (1977).

[11] N. A. NACHEV and T. ZH. MOLLOV, An isomorphism of modular group algebras of finite 2-groups for which the order of the factor group with respect to the center has order four (Russian). C.R. Acad. Bulgare Sci. **34**, 1633–1636 (1981).

[12] N. A. NACHEV and T. ZH. MOLLOV, An isomorphism of modular group algebras of finite 2-groups for which the order of the quotient-group with respect to the center is equal to four (Russian). PLISKA Stud. Math. Bulgar. **8**, 3–20 (1986).
[13] I. B. S. PASSI and S. K. SEHGAL, Isomorphism of modular group algebras. Math. Z. **129**, 65–73 (1972).
[14] D. S. PASSMAN and P. F. SMITH, Units in integral group rings. J. Algebra **69**, 213–239 (1981).
[15] J. RITTER and S. SEHGAL, Isomorphism of group rings. Arch. Math. **40**, 32–39 (1983).
[16] K. W. ROGGENKAMP, The isomorphism problem and units in group rings of finite groups. Groups – St. Andrews 1981, 313–327, Cambridge 1982.
[17] K. W. ROGGENKAMP and L. L. SCOTT, Units in metabelian group rings: non-splitting examples for normalized units. J. Pure Appl. Algebra **27**, 299–314 (1983).
[18] K. W. ROGGENKAMP and L. L. SCOTT, Units in group rings: splittings and the isomorphism problem. J. Algebra **96**, 397–417 (1985).
[19] F. RÖHL, On automorphisms of complete algebras and the isomorphism problem for modular group rings. To appear.
[20] R. SANDLING, Group rings of circle and unit groups. Math. Z. **140**, 195–202 (1974).
[21] R. SANDLING, Units in the modular group algebra of a finite abelian p-group. J. Pure Appl. Algebra **33**, 337–346 (1984).
[22] R. SANDLING, The isomorphism problem for group rings: a survey. Orders and their applications (Oberwolfach, 1984), 256–288, LNM **1142**, Berlin-Heidelberg-New York 1985.
[23] R. SANDLING, Presentations for unit groups of modular group algebras of groups of order 2^4. To appear.
[24] H. N. WARD, Some results on the group algebra of a group over a prime field. Seminar on Finite Groups and Related Topics, 13–19, Mimeographed notes, Harvard Univ. 1960–1961.

Eingegangen am 26. 8. 1987

Anschrift des Autors:

Robert Sandling
Department of Mathematics
The University of Manchester
Manchester M13 9PL
England