BULL. AUSTRAL. MATH. SOC. 16A26, 20C05
VOL. 21 (1980), 329-350.

ON CERTAIN GROUP RING PROBLEMS

G. KARPILOVSKY

Recent developments on the isomorphism and other group ring problems are amply reviewed in Sehgal's book, *Topics in group rings*. The aim of this expository paper is to complement the content of Sehgal's book. Our main emphasis is the presentation of some results due to Saksonov which are published in Russian and do not seem well-known to the English reader. We also draw the reader's attention to some unpublished results of Higman.

Introduction

Let KG be a group ring of a finite group G over a commutative ring K with unit. There has been a considerable amount of work over the years dedicated to the following problem: To what extent does KG determine the group G ? A favourite gambit of group ring theorists has been to impose some conditions on the ring K in the expectation that KG determines G up to isomorphism. There is a striking example of Dade [19] of two nonisomorphic metabelian groups G and H such that for all choices of the field K , KG and KH are isomorphic.

Therefore, generally speaking, a field is not a suitable candidate for K . The rings K for which the group ring KG yields the most information on the structure of G are integral domains of characteristic 0 in which no rational prime divisor of the order of G is invertible.

Typical examples of such rings are as follows:

The ring R of algebraic integers in some finite extension of the

Received 30 October 1979.

rationals (in particular, the ring Z of rational integers), the ring $Z_{(G)} = \{a/b \mid a, b \in Z, (b, |G|) = 1\}$ and, in the case when G is a p-group, the ring O_p of p-adic integers.

Before we embark on our exposition proper, a historical note is worth inserting.

The study of the isomorphism problem was pioneered by Higman in 1940. Some of his significant results, regrettably never published (except in an Oxford D.Phil. Thesis, "Units in group rings") were virtually unknown. One of these results states that if G is metabelian and hilpotent then any group of normalised units of finite order in RG is isomorphic to a subgroup of G. It took 25 years to re-discover a special case of this result. Namely, in 1965 Passman [33] proved that a nilpotent group G of class 2 is determined by RG.

One of the most important results so far achieved is due to Whitcomb [35]. In 1968 Whitcomb proved that a metabelian group is determined by its integral group ring. It is interesting to note that Whitcomb's result can be easily deduced from the proof of Theorem 14 of Higman's unpublished thesis.

We also remark that Conjecture II.1.5 of [52] for the case when G is a finite group was first established by Saksonov [44] and that Sehgal was probably unfamiliar with it. We present this result of Saksonov in the first part of the article (§2). In the second part (§3) we show how Whitcomb's result can be easily deduced from Theorem 14 of Higman's unpublished thesis. In the third part (§§4, 5), we discuss conjugacy of group bases and normal subgroup correspondence of groups having isomorphic group rings.

1. The setting

In this section we shall describe the notation, recall the definitions and record some elementary properties of group rings. Throughout we shall use the following notation:

RG the group ring of a finite group G over R where R is an integral domain of characteristic 0 in which no rational prime divisor of the order of G

https://doi.org/10.1017/S0004972700006195 Published online by Cambridge University Press

is invertible.

C the complex numbers.

Q the rational numbers

$Z_{(G)} = \{a/b \mid a, b \in Z, (b, |G|) = 1\}$.

$Z(G)$ the centre of G .

$T_p(G \bmod G')$ the subgroup of G generated by all elements of G some pth power of which is in G' .

Let G be a group and let K be an associative ring with unit. We denote by KG the group ring of G over K ; this ring is a free K-module with basis indexed by the elements of G , and most of the time we identify this basis with G . Each element x of KG can then be uniquely written in the form

$$x = \sum_{g \in G} x_g g \ , \quad x_g \in K \ ,$$

where only finitely many x_g are distinct from 0 and multiplication in KG extends that in G .

A homomorphism from the group ring KG_1 to the group ring KG_2 is a ring homomorphism which is also a K-module homomorphism. The augmentation ideal $I(K, G)$ is the kernel of the homomorphism from the group ring KG to K induced by collapsing G to the unit group. Explicitly, $I(K, G)$ consists of all

$$x = \sum_{g \in G} x_g g \ , \quad x_g \in K \ , \text{ for which } \varepsilon(x) = \sum_{g \in G} x_g = 0 \ .$$

We shall write $I(G)$ instead of $I(K, G)$ when there is no danger of confusion. A unit u in KG is called trivial (respectively normalised) if $u = u_g g$ for some unit $u_g \in K$ and some $g \in G$ (respectively if $\varepsilon(u) = 1$).

A normalised group basis of KG is a group basis consisting of normalised units. We shall write $KG = KH$ for H being a normalised group basis of KG . Note that if H_1 is another group basis of KG then

https://doi.org/10.1017/S0004972700006195 Published online by Cambridge University Press

$$KG = KH \quad \text{where} \quad H = \left\{\varepsilon(t^{-1})t \mid t \in H_1\right\}$$

and $H \cong H_1$.

Therefore the isomorphism problem may be stated as follows:

Does $KG = KH$ imply $G \cong H$?

Suppose that H is a normalised group basis of KG and let ε' be a homomorphism from KG to K induced by collapsing H to the unit group. Then for any

$$x = \sum_{h \in H} x_h h \ , \quad x_h \in K \ ,$$

$$\varepsilon(x) = \sum_{h \in H} x_h = \varepsilon'(x) \ ; \quad \text{that is} \quad \varepsilon = \varepsilon' \ .$$

Consequently $I(G) = I(H)$ and every unit normalised with respect to G is also normalised with respect to H . For J an ideal of KG the multiplicative kernel of the map $G \to KG/J$ is $G \cap (1+J)$ and $G + J$ will stand for the image of G under this map. In other words,

$$G + J = \{g+J \mid g \in G\}$$

and $G \cap (1+J)$ consists of all g in G for which $g - 1$ is in J . Note that

(1.1) for $N = G \cap (1+J)$, $G/N \cong G + J$.

Let $\lambda : G \to H$ be a group epimorphism and let $\overline{\lambda} : KG \to KH$ be the group ring epimorphism which is the extension of λ by K-linearity. Then $\operatorname{Ker} \overline{\lambda} = KG \cdot I(N)$ where $N = \operatorname{Ker} \lambda$ and therefore

(1.2) $$G \cap \left(1+KG \cdot I(N)\right) = N \ .$$

If $x \in KG$ then the equality $x = \varepsilon(x) + \left(x-\varepsilon(x)\right)$ implies

$$KG = K \oplus I(G) \quad \text{(direct sum of } K\text{-modules)}.$$

Hence

(1.3) $$KG \cdot I(N) = I(N) + I(G) \cdot I(N) \ .$$

We now record the following identities:

https://doi.org/10.1017/S0004972700006195 Published online by Cambridge University Press

(1.4) $ab - 1 = (a-1)(b-1) + (a-1) + (b-1)$, a, b in KG ,

(1.5) $[a, b] - 1 = a^{-1}b^{-1}[(a-1)(b-1)-(b-1)(a-1)]$, a, b in $U(KG)$.

Note also that for any natural number m dividing the order of G the mapping

$$\begin{cases} Z_{(G)} \to Z/mZ , \\ a/b \to \bar{a}(\bar{b})^{-1} , \quad \bar{a} = a + mZ , \quad \bar{b} = b + mZ , \end{cases}$$

is a ring epimorphism with kernel $mZ_{(G)}$ and therefore

(1.6) $$Z_{(G)}/mZ_{(G)} \cong Z/mZ .$$

We conclude this section by recording the following standard number theoretic properties:

(i) Let $\varepsilon_1, \ldots, \varepsilon_n$ be mth roots of unity over Q and let $\alpha = \frac{\varepsilon_1+\ldots+\varepsilon_n}{n}$. If α is an algebraic integer then either $\alpha = 0$ or

(1.7) $$\varepsilon_1 = \varepsilon_2 = \ldots = \varepsilon_n .$$

(ii)

(1.8) $$O_p/p^nO_p \cong Z/p^nZ .$$

2. Saksonov's result

The main purpose of this section is to prove Theorem 2.1 due to Saksonov and to make some observations which will be used in §3.

The reader should note that Theorems 2.1, 2.2 and 2.3 of this section for the case when R is the ring of algebraic integers were first established by Higman [21].

We start by recording the following simple observation, which is valid for $K = Z_{(G)}$ and, in the case when G is a p-group also, for $K = O_p$ (see (1.6) and (1.8)).

LEMMA 2.1. *Let m be the exponent of G/G' and let K be a ring with 1 such that $K/mK \cong Z/mZ$. Then for any $t \in I(K, G)$ there exists*

https://doi.org/10.1017/S0004972700006195 Published online by Cambridge University Press

$g \in G$ *such that* $t \equiv g - 1 \pmod{I(K, G)^2}$.

Proof. It follows from (1.4) and (1.5) that $\phi : G \to I(K, G)/I(K, G)^2$ where $\phi(g) = (g-1) + I(K, G)^2$ is a homomorphism with $G' \subseteq \operatorname{Ker} \phi$. Since $g^m \in G'$ for any $g \in G$, $I(K, G)^2 = \phi(g^m) = m\phi(g) = m(g-1) + I(K, G)^2$ and therefore $mk(g-1) \in I(K, G)^2$ for any $k \in K$. Since a typical element of K is $k = t \cdot 1 + mk_1$ where $k_1 \in K$ and $t \in \{0, 1, \ldots, m-1\}$, then $\phi(g^t) = k(g-1) + I(K, G)^2$. This shows that ϕ is an epimorphism, and completes the proof. □

The following lemma is due to Saksonov [44, p. 190].

LEMMA 2.2. *Let* α *be an algebraic number and let* n *be a natural number such that* $n\alpha$ *is an algebraic integer. If* $\{\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_t\}$ *is the set of all* Q*-conjugates of* α *then either* α *is an algebraic integer or in the ring* $Z[\alpha_1, \alpha_2, \ldots, \alpha_t]$ *at least one rational prime divisor of* n *is invertible.*

Proof. Suppose that α is not an algebraic integer. Then there exists an elementary symmetric function f of t variables such that $f(\alpha_1, \alpha_2, \ldots, \alpha_t) \notin Z$. Since $n\alpha$ is an algebraic integer

$$f(\alpha_1, \alpha_2, \ldots, \alpha_t) = a/b \quad \text{for some } a, b \in Z ,$$

such that $(a, b) = 1$, $b > 1$ and all the prime divisors of b are divisors of n . If p is one of these divisors then because of $(a, p) = 1$ there exist $c, d \in Z$ such that $ac + dp = 1$. It is clear that

$$f(\alpha_1, \alpha_2, \ldots, \alpha_t) \in Z[\alpha_1, \alpha_2, \ldots, \alpha_t]$$

and hence

$$a/p \in Z[\alpha_1, \alpha_2, \ldots, \alpha_t] .$$

But then

$$1/p = (ac+dp)/p = (a/p)\cdot c + d \in Z[\alpha_1, \alpha_2, \ldots, \alpha_t]$$

as desired. □

https://doi.org/10.1017/S0004972700006195 Published online by Cambridge University Press

We are now ready to prove the following:

THEOREM 2.1 (Saksonov [44, p. 191]). *If* $u = \sum_g u_g g$ *is a unit of finite order in* RG *with* $u_1 \neq 0$ *then* $u = u_1 \cdot 1$. *In particular, all central units of finite order in* RG *are trivial.*

Proof. Let $z = \sum_{g \in G} z_g g$ be a central unit of finite order. Then $z_t \neq 0$ for some $t \in G$ and therefore $u = zt^{-1}$ is a unit of finite order with $u_1 = z_t \neq 0$. Hence it suffices to show that if $u^m = 1$ and $u_1 \neq 0$ then $u = u_1 \cdot 1$.

To prove this assertion, let $\mathrm{tr}(x)$ be the trace of $x \in RG$ in the regular representation of RG. Then the matrix of u is conjugate to $\mathrm{diag}(\varepsilon_1, \ldots, \varepsilon_{|G|})$ and

$$\mathrm{tr}(u) = u_1 \cdot |G| = \varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_{|G|}$$

where ε_i $(i = 1, 2, \ldots, |G|)$ is an mth root of unity (belonging to a sufficiently large field containing R). By looking at the $\mathrm{tr}(u^r)$ where $(r, m) = 1$ we conclude that the set $\{\beta_1 = u_1, \beta_2, \ldots, \beta_s\}$ of all Q-conjugates to u_1 belongs to R and therefore $Z[\beta_1, \beta_2, \ldots, \beta_s] \subseteq R$. Since $|G|u_1$ is an algebraic integer, Lemma 2.2 may be employed to infer that u_1 is also an algebraic integer. The desired assertion is now a consequence of (1.7). □

Note that in Theorem 2.1 we cannot relax the conditions imposed on the integral domain R (namely,

(*) char $R = 0$ and

(**) no rational prime dividing the order of G is invertible).

This becomes clear if we look at the following two examples, the second of which is due to Saksonov [44].

EXAMPLE 1. Condition (*) is not satisfied.

https://doi.org/10.1017/S0004972700006195 Published online by Cambridge University Press

Let G be a (finite) abelian p-group and let $R = Z/pZ$. Then each element in RG which has augmentation 1 is a central unit of finite order, that is, a central unit of finite order need not be trivial.

EXAMPLE 2. Condition (**) is not satisfied.

Let $G = \{1, a, a^2, a^3\}$ and let $R = Z[\frac{1}{2}, i]$. Then $b = \left((1-i)a+(1+i)a^3\right)/2$ is a nontrivial central unit of order 2.

The next result parallels Lemma 3.1 of [17] (see also [44]).

THEOREM 2.2. *Let H be a torsion group of normalised units in RG. Then H is a linearly independent set and, in particular, H is a finite group.*

Proof. We carry out the proof by contradiction. Let $\sum_{i=1}^{n} \alpha_i h_i = 0$ where $h_i \in H$, $\alpha_i \in R$, $i \in \{1, 2, \ldots, n\}$ and let $\alpha_j \neq 0$ for some $j \in \{1, 2, \ldots, n\}$. Then

$$\alpha_j \cdot 1 = - \sum_{i \neq j} \alpha_i \left(h_i h_j^{-1}\right)$$

and if we express the elements $h_i h_j^{-1}$, $i \neq j$, in terms of the elements of G then at least one of them, say $h_k h_j^{-1}$, $k \neq j$, has a non-zero coefficient of 1. Now the argument used in the proof of Theorem 2.1 may be employed to infer that $h_k h_j^{-1} = \alpha \cdot 1$ for some $\alpha \in R$. Since $\varepsilon(h_k) = \varepsilon(h_j) = 1$ it follows that $h_k = h_j$. This gives the desired contradiction, and completes the proof of the theorem. □

We shall now make some observations which will be used in §4. Let $\pi : RG \to R\overline{G}$, $\overline{G} = G/N$ be a canonical homomorphism and let $RG = RH$. Then, by Theorem 2.2, $\overline{H}$, the image of H in $R\overline{G}$, is a linearly independent set in $R\overline{G}$ whence $R\overline{G} = R\overline{H}$. Moreover, since π can be regarded as the extension of the epimorphism $H \to \overline{H}$ (whose kernel is $N^* = H \cap \left(1+RG \cdot I(N)\right)$) by R-linearity, then $\operatorname{Ker} \pi = RG \cdot I(N) = RH \cdot I(N^*)$. Moreover because of

$$|G/N| = |\overline{G}| = |\overline{H}| = |H/N^*|$$

the groups N and N^* are of the same order. Consequently

(2.1) $RG = RH$ implies $R\overline{G} = R\overline{H}$, $RG \cdot I(N) = RG \cdot I(N^*)$ and $|N| = |N^*|$.

Let $\phi : G \to H$ be an isomorphism of G onto H and let $ZG = ZH$. Suppose that Γ is an irrediculble matrix representation of the complex group algebra CG and denote by α_1 and α_2 the irreducible matrix representations of G defined by $\alpha_1(g) = \Gamma(g)$, $\alpha_2(g) = \Gamma(\phi(g))$ for any g in G. Then

(2.2) if α_1 is a faithful representation then so is α_2.

To prove (2.2) we first observe that $CG = CH$ and that if $\operatorname{Ker} \alpha_2 \neq 1$ then $1 \neq N^* = \{h \in H \mid \Gamma(h) = 1\}$. Since $CG \cdot I(N^*) \subseteq \operatorname{Ker} \Gamma$ then, by (2.1), $CG \cdot I(N) \subseteq \operatorname{Ker} \Gamma$ for some $N \lhd G$ such that $|N| = |N^*|$. Consequently it may be inferred that $N \subseteq \operatorname{Ker} \alpha_1$, from which (2.2) follows.

The theorem which follows, is very useful in its application to the isomorphism problem.

THEOREM 2.3. *Let S be a subgroup of G. Then, for $I(G) = I(R, G)$ and $I(S) = I(R, S)$,*

$$G \cap \left(1 + I(G) \cdot I(S)\right) = S'.$$

Proof. We first consider the special case when $S = G$. By taking the case $n = 2$ in Theorem 2.1 of [4&] we see that $S \cap \left(1 + I(S)^2\right) = S'$ whenever $T_p(S \bmod S') = S$ for all primes p for which $p^e R = p^{e+1} R$ for some non-negative integer e. It is clear that

$$T_p(S \bmod S') = S' \quad \text{whenever} \quad p \nmid |S|.$$

If p is a prime such that $p^e R = p^{e+1} R$ for some e then $p^e(1 - px) = 0$ for some $x \in R$ and since R has no zero divisors, p is a unit in R. This shows that $p \nmid |S|$ and completes the proof of the special case. To prove the general case, let T be a transversal of S in G containing 1 and let $g = ts$ be a typical element of G $(t \in T, s \in S)$.

Consider the R-linear map

https://doi.org/10.1017/S0004972700006195 Published online by Cambridge University Press

$$\phi : RG \to RS$$

which is the R-linear extension of $g \to s$. Then $\phi(x) = x$ for any $x \in I(S)$ and the equality

$$\phi|(g-1)(s_1-1)| = (s-1)(s_1-1) , \quad s_1 \in S ,$$

shows that $\phi\big(I(G)\cdot I(S)\big) = I(S)^2$. Consequently

$$I(G)\cdot I(S) \cap I(S) = I(S)^2 .$$

Now (1.2) may be employed to infer that

$$G \cap \big(1+I(G)\cdot I(S)\big) = S \cap \big(1+I(S)^2\big) ,$$

thus completing the proof by applying the special case proved above. □

3. The isomorphism problem and Higman's thesis

Whether the integral group ring ZG of a finite group G determines G up to isomorphism is a question which has been open for nearly 40 years. Since the problem seems so intractible one needs to impose more hypotheses to make any progress. The list of groups which are determined by their integral group rings includes S_n, A_n (both are determined by their character table), groups of order 2^n, $n \leq 7$ (see [26]) and finite circle groups (see [44]). The best result, due to Whitcomb [55], is the following.

THEOREM 3.1 (Whitcomb [55]). *If G is metabelian and $ZG = ZH$ then G is isomorphic to H.*

In this section we shall show how Whitcomb's result can be easily deduced from the proof of Theorem 14 of Higman's unpublished thesis. We first note that perusal of the proof of the mentioned theorem easily shows that the following assertion is valid.

Let $ZG = ZH$ and let u be a normalised unit of finite order in ZG. Then there exists $g \in G$ such that

$$u \equiv g \big(\mathrm{mod}\ I(G)\cdot I(G')\big) . \tag{3.1}$$

Proof of Theorem 3.1. We first note that $ZG\cdot I(G')$ is the smallest ideal L such that ZG/L is commutative whence $ZG = ZH$ implies

https://doi.org/10.1017/S0004972700006195 Published online by Cambridge University Press

$ZG \cdot I(G') = ZH \cdot I(H')$. Multiplying both sides of this equality by $I(G) = I(H)$ we get $I(G) \cdot I(G') = I(H) \cdot I(H') = J$. It follows from (3.1) that $H + J \subseteq G + J$ and since the elements of G are normalised units with respect to H , the same argument shows that $G + J \subseteq H + J$, that is, $G + J = H + J$. Now (1.1) and Theorem 2.3 may be employed to infer that $G/G'' \cong H/H''$. Hence if $G'' = 1$ then $G \cong H/H''$ and since $|G| = |H|$, $G \cong H$ as desired. □

Note that if (3.1) holds with R instead of Z then replacing Z by R in the above argument we get $G/G'' \cong H/H''$ and, in particular, if $G'' = 1$ then $G \cong H$.

We shall now show that (3.1) holds in a more general context, namely if we replace Z by a ring R such that $R/mR \cong Z/mZ$ for m equal to the exponent of G'/G'' . The rings R which satisfy this condition include $Z_{(G)}$ and, when G is a p-group, the ring of O_p of p-adic integers. From what we have said above it follows that G/G'' is determined by the group ring $Z_{(G)}G$ [49] and that, if G is a p-group, then G/G'' is determined by O_pG [51].

REMARK. Recently Roggenkamp [40] proved that if $G'' = 1$ then $RG = RH$ implies $G \cong H$.

To prove (3.1) *in a more general context*, let $\overline{G} = G/G'$ and let $\overline{x}$ be the image of $x \in RG$ under the canonical homomorphism $RG \to R\overline{G}$. Then $\overline{u}$ is a normalised central unit of finite order in $R\overline{G}$ and therefore thanks to Theorem 2.1, $\overline{u} = \overline{g}$ for some $g \in G$. Hence $u \equiv g \pmod{RG \cdot I(G')}$ and by (1.3), $u \equiv g + t \pmod{I(G) \cdot I(G')}$ for some $t \in I(G')$. By Lemma 2.1 there exists $a \in G'$ such that $t \equiv a - 1 \pmod{I(G')^2}$. Hence

$$u \equiv g + (a-1) = (1-g)(a-1) + ga \equiv ga \bmod\big(I(G) \cdot I(G')\big) ,$$

as desired. □

It would be interesting to know whether Whitcomb's result is valid for nilpotent groups. In [24] Jackson states that this is the case. However his proof is incomplete since it is based on the following false argument. Let G be a nilpotent group and let u be a normalised unit of finite order in ZG . Then he claims that

https://doi.org/10.1017/S0004972700006195 Published online by Cambridge University Press

$$u \equiv 1 \pmod{I(G)\cdot I(G')} \quad \text{implies} \quad u = 1 \ .$$

The following provides a counterexample to this claim. Let G be a nilpotent group which is not metabelian and let $1 \neq g \in G''$. Then $g - 1 \in I(G')^2 \subseteq I(G)\cdot I(G')$.

We shall close this section with the observation which will be used in §4. Let $ZG = ZH$ and let $G'' = 1$. For g in G let $\phi(g)$ be the unique element in H which is determined by $g \equiv \phi(g) \pmod{I(G)\cdot I(G')}$. It follows from what we have said above that $g \to \phi(g)$ determines an isomorphism of G onto H. On the other hand, by Theorem 2.1, $Z(G) = Z(H)$ whence $\phi(g) = g$ whenever $g \in Z(G)$. Consequently the map

(3.2) $\begin{cases} G \to H \\ g \to \phi(g) \end{cases}$ is an isomorphism of G onto H which is also an identity mapping on $Z(G) = Z(H)$.

4. Conjugacy of group bases

Let $ZG = ZH$ where G is a finite group and let $G \cong H$. It is natural to ask whether there is a unit u in ZG such that $H = u^{-1}Gu$. That this is not always the case was first proved in 1966 by Berman and Rossa ([11]). The following example can be found in [11].

Let $G = \{a, b \mid a^4 = b^2 = 1;\ b^{-1}ab = a^{-1}\}$ and let $H = \langle a', b' \rangle$ where

$$a' = -a + 2a^3 - b - ab + a^2b + a^3b \ ,$$

$$b' = -a + a^3 - ab + a^2b + a^3b \ .$$

Then $ZG = ZH$ but G and H are not conjugate in $U(ZG)$. Incidentally, G and H are conjugate in $U(Z_{(2)}G)$ where $Z_{(2)}$ is the ring of 2-integral rationals. Indeed, let $u = 1 - b + ab$. Then it is easy to check that u is a unit in $Z_{(2)}G$ and that

$$u^{-1}a'u = a \ , \quad u^{-1}b'u = b \ .$$

Note also that a result of Weiler [54] implies that any normalised group basis of ZG (G is dihedral of order 8) is conjugate in $U(Z_{(2)}G)$ to

G .

We next remark that S_n is determined up to isomorphism by ZS_n since S_n is determined by its character table. Hence the application of a result due to Peterson [38] implies that, in QS_n , S_n is conjugate to any normalised group basis of ZS_n . It is not known, however, whether any normalised group basis in ZS_n is conjugate in ZS_n to S_n . That any normalised group basis of ZS_3 is conjugate in ZS_3 to S_3 is a result due to Hughes and Pearson [23]. It is interesting to note that there is an intimate connection between the conjugacy of group bases and the isomorphism problem. Indeed as it was pointed out by Whitcomb [55] if G is a p-group of class 2 and if every normalised group basis in ZG is conjugate in O_pG to G $(O_p$ is the ring of p-adic integers$)$, then any p-group of class less than or equal to 5 is determined by its integral group ring. The following classical result is very useful in the study of Aut(RG) . This is a convenient place to record it for future reference.

THEOREM 4.2 [12]. *Let K be a field and let A be a semisimple finite dimensional K-algebra. If θ is an automorphism of A which is the identity mapping on the centre of A then θ is an inner automorphism.*

There is one piece of reasoning, relevant to the conjugacy of group bases, which is likely to be encountered in other contexts. We therefore isolate it in the following lemma, in which C stands for the field of complex numbers.

LEMMA 4.2. *Let G be a finite group, and let $ZG = ZH$. If G and H are conjugate in $U(CG)$ then they are conjugate in $U(QG)$.*

Proof. By hypothesis, there exists an element $u \in U(CG)$ such that $u^{-1}Gu = H$ and therefore the mapping $\phi : G \to H$ defined by $\phi(g) = u^{-1}gu$ is an isomorphism of G onto H . Let ψ be an automorphism of QG which is the extension of the map ϕ by Q-linearity. Since ψ is the identity mapping on the centre of QG then, by Theorem 4.2, ψ is an inner automorphism of QG . Consequently, there exists an element $v \in U(QG)$ such that $\psi(x) = v^{-1}xv$ for any $x \in QG$. Because

https://doi.org/10.1017/S0004972700006195 Published online by Cambridge University Press

$\psi(G) = H$, $v^{-1}Gv = H$, as desired. □

REMARK. A similar proof shows that Lemma 4.2 is valid if we replace Z by R and C by the algebraic closure of the quotient field of R .

We close this section with the simple proof of the following result which is essentially a restatement of Theorem 9 of [55] (see also [52]).

THEOREM 4.3. *Let G be a finite nilpotent group of class 2 . Then any normalised group basis H of ZG is conjugate to G in $U(QG)$.*

Before we embark on our proof it is convenient to recall some basic facts about group representations.

Let G be a finite group and let

$$\Gamma_i : CG \to M_{n_i}(C) , \quad 1 \le i \le r ,$$

be the distinct irreducible matrix representations of the group algebra CG . Denote by $X_i(x) = \mathrm{Tr}\ \Gamma_i(x)$, $x \in CG$. The family (Γ_i) defines an isomorphism

$$\Gamma : CG \to \prod_{i=1}^{r} M_{n_i}(C)$$

where $\Gamma(x) = (\Gamma_1(x), \Gamma_2(x), \ldots, \Gamma_r(x))$, $x \in CG$, and where $\prod_{i=1}^{r} M_{n_i}(C)$ stands for the product of matrix algebras $M_{n_i}(C)$. The set $\{\rho_1, \rho_2, \ldots, \rho_r\}$ where $\rho_i(g) = \Gamma_i(g)$ for any $g \in G$ is a full set of nonequivalent irreducible complex representations of G . Using the bar convention for the homomorphic images, consider the canonical homomorphism

$$CG \to C\overline{G}$$

where $\overline{G} = G/N$ and $N = \mathrm{Ker}\ \rho_i$. Then

$$CG \cdot I(N) \subseteq \mathrm{Ker}\ \Gamma_i$$

and therefore the mapping

$$T : C\overline{G} \to M_{n_i}(C) \tag{4.4}$$

https://doi.org/10.1017/S0004972700006195 Published online by Cambridge University Press

defined by $T(\bar{x}) = \Gamma_i(x)$, $x \in CG$, is an irreducible matrix representation of the group algebra $C\bar{G}$. Suppose that $z \in Z(G)$. Then by Schur's lemma,

$$\rho_i(z) = \begin{pmatrix} \varepsilon & & & 0 \\ & \varepsilon & & \\ & & \ddots & \\ 0 & & & \varepsilon \end{pmatrix}$$

where ε is a root of 1 in C . Therefore if $z = [a, b]$ for some a and b in G then $\varepsilon X_i(a) = X_i(a)$. This shows that if G is nilpotent of class 2 and if ρ_i is faithful then

$$X_i(g) = 0 \quad \text{for all} \quad g \notin Z(G) . \tag{4.5}$$

Finally, let $ZG = ZH$ and let $G'' = 1$. We recall that by (3.2) the map $\phi : G \to H$, where $\phi(g) = h$ if $g \equiv h \left(\text{mod } I(G)\cdot I(G')\right)$, is both an isomorphism and the identity map on $Z(G) = Z(H)$. With these preliminary remarks, we now prove Theorem 4.3.

Proof of Theorem 4.3. Preserving the above notation, we argue first that it suffices to prove that, for any $i \in \{1, 2, \ldots, r\}$,

$$X_i(g) = X_i(h) \quad \text{whenever} \quad g \equiv h \ \text{mod}\left(I(G)\cdot I(G')\right) . \tag{4.6}$$

Indeed, if this is the case, then the irreducible matrix representations α_1 and α_2 of G defined by $\alpha_1(g) = \Gamma_i(g)$ and $\alpha_2(g) = \Gamma_i\left(\phi(g)\right)$ are equivalent; that is, there exists a non-singular matrix B_i such that $B_i^{-1}\Gamma_i(g)B_i = \Gamma_i\left(\phi(g)\right)$ for all g in G . This forces G and H to be conjugate in $U(CG)$ and thanks to Lemma 4.2, G and H are conjugate in $U(QG)$, as asserted. To prove (4.6), suppose that $g \equiv h \left(\text{mod } I(G)\cdot I(G')\right)$ with h in H . By passing to the canonical homomorphism $ZG \to Z\bar{G}$ where $\bar{G} = G/N$ and $N = \text{Ker } \alpha_1$ we therefore derive $\bar{g} \equiv \bar{h}\left(\text{mod } I(\bar{G})\cdot I(\bar{G}')\right)$. Because of (2.1), $Z\bar{G} = Z\bar{H}$ and therefore (4.4) and induction on $|G|$ may be employed to conclude that $X_i(g) = X_i(h)$ whenever $\text{Ker } \alpha_1 \neq 1$. Finally, if α_1 is a faithful representation then so is α_2 (see (2.2)). Since by (3.2), $g = h$ if $g \in Z(G)$, the application of (4.5) yields the

https://doi.org/10.1017/S0004972700006195 Published online by Cambridge University Press

desired assertion, thus completing the proof. □

REMARK. A similar proof shows that Theorem 4.3 is valid, if we replace Z by R and Q by the quotient field of R where $R = Z_{(G)}$ or, in the case when G is a p-group, $R = O_p$.

5. Normal subgroup correspondence

Suppose that G and H are groups with isomorphic group algebras KG and KH over the ring K of integers in some finite algebraic extension of the rationals. In [33] Passman established a bijective correspondence between the set of normal subgroups of G and that of H which preserves many natural operations and properties defined on these sets. Some of Passman's results, however, depend on nilpotency conditions.

In this section we state generalisations of Passman's result in two directions. Namely, we remove the nilpotency condition and replace K by R. Note also that the result presented in this section is sharper than that in [52].

Elements of particular interest in RG are the class sums. These are the sum of all the group elements in any given class of G. That $RG = RH$ implies existence of a bijective correspondence between the conjugacy classes of G and those of H such that the corresponding classes have identical class sums was proved by Saksonov [44]. Note also that Berman [2] proved this result for the case $R = Z$, and for the case $R = K$ the same result was proved by Glauberman (see [33]), Poljak [39] and Saksonov [42].

Our result is as follows.

THEOREM [27]. *Let $RG \cong RH$. Then there exists an isomorphism between the lattice of normal subgroups G and that of H which preserves the following:*

(a) the commutation of any two normal subgroups;

(b) normal abelian sections and the isomorphism class of normal abelian sections;

(c) the order and period of normal sections.

In fact, the corresponding normal sections have the same number of

https://doi.org/10.1017/S0004972700006195 Published online by Cambridge University Press

elements of any given order.

COROLLARY. *The above isomorphism preserves the following:*

(I) Nilpotency, solvability, class of nilpotency and the derived length of N, N being an arbitrary normal subgroup of G; in particular the Fitting subgroup of N.

(II) A central series of N consisting of normal subgroups of G and the isomorphism class of corresponding factors; in particular, the upper central series and the lower central series of N and any central series of G.

(III) The derived series of N, the chief series of G and the isomorphism class of corresponding factors.

(IV) The group $C^n(N)$ generated by all nth powers of elements of N and the group $C_n(N)$ generated by all elements of N whose order divides n.

The special case of *(a)* and *(b)* when $R = Z$ was proved by Whitcomb [55] (see also [47]). When R is the ring K of algebraic integers in a finite extension of the rationals, Passman [33] proved part of *(c)* and, when G is nilpotent, he has obtained *(a)* and part of *(b)*. Obayashi [31] proved part of *(b)* for $R = K$. For other various special cases of the above theorem and corollary refer to [17], [31], [33], [42], [44] and [51].

References

[1] George M. Bergman and Warren Dicks, "On universal derivations", *J. Algebra* **36** (1975), 193-211.

[2] С.Д. Берман [S.D. Berman], "О необходимом условии изоморфизма целочисленных групповых колец" [On a necessary condition for isomorphism of integral group rings", *Dopovīdī Akad. Nauk Ukraïn. RSR* No. 5 (1953), 313-316.

[3] С.Д. Берман [S.D. Berman], "О некоторых свойствах целочисленных групповых колец" [On certain properties of integral group rings], *Dokl. Akad. Nauk SSSR (N.S.)* **91** (1953), 7-9.

[4] С.Д. Берман [S.D. Berman], "Об изоморфизме центров групповых колец p-групп" [On the isomorphism of the centers of group rings of p-groups], *Dokl. Akad. Nauk SSSR (N.S.)* 91 (1953), 185-187.

[5] С.Д. Берман [S.D. Berman], "Об уравнении $x^m = 1$ в целочисленном групповом кольце" [On the equation $x^m = 1$ in an integral group ring], *Ukrain. Mat. Ž.* 7 (1955), 253-261.

[6] С.Д. Берман [S.D. Berman], "О некоторых своиствах групповых колец над полем рациональных чисел" [On certain properties of group rings over the field of rational numbers], *Užgorod. Gos. Univ. Naučn. Zap. Him. Fiz. Mat.* 12 (1955), 88-110.

[7] С.Д. Берман [S.D. Berman], "Групповые алгебры абелевых расширений конечных групп" [Group algebras of abelian extensions of finite groups], *Dokl. Akad. Nauk SSSR (N.S.)* 102 (1955), 431-434.

[8] S.D. Berman, "Group algebras of countable abelian p-groups", *Soviet Math. Dokl.* 8 (1967), 871-873.

[9] С.Д. Берман [S.D. Berman], "Групповые алгебры счетных абелевых p-групп" [Group algebras of countable abelian p-groups], *Publ. Math. Debrecen* 14 (1967), 365-405.

[10] С.Д. Берман, Т.Ж. Моллов [S.D. Berman, T.Ž. Mollov], "О групповых кольцах абелевых p-групп любой мощности" [The group rings of abelian p-groups of arbitrary power], *Mat. Zametki* 6 (1969), 381-392.

[11] С.Д. Берман, А.Р. Росса [S.D. Berman, A.R. Rossa], "О целочисленных групповых кольцах конечных и периодических групп" [Integral group-rings of finite and periodic groups", *Алгебра и математическая логика. Алгебраические исследования* [*Algebra and mathematical logic: Studies in algebra*], 44-53 (Izdat. Kiev. University, Kiev, 1966).

[12] N. Bourbaki, *Éléments de mathématique*, Fasc. XXIII. Livre II: *Algèbre*. Chapitre 8: *Modules et anneaux semisimples* (Nouveau tirage de l'édition de 1958. Actualités Scientifiques et Industrielles, No. 1261. Hermann, Paris, 1973).

[13] А.А. Бовди [A.A. Bovdi], "Периодические нормальные делители мультипликативной группы группового кольца" [Periodic normal divisors of the multiplicative group of a group ring], *Sibirsk. Mat. Ž.* 9 (1968), 495-498.

[14] А.А. Бовди [A.A. Bovdi], "Периодические нормальные делители мультипликативной группы группового кольца. II" [Periodic normal subgroups of the multiplicative group of a group ring. II], *Sibirsk Mat. Ž.* 11 (1970), 492-511.

[15] А.А. Бовди [A.A. Bovdi], *Групповые кольца* [*Group rings*] (Užgorod. Gosudarstv. Univ., Užgorod, 1974).

[16] Richard Brauer, "Zur Darstellungstheorie der Gruppen endlicher Ordnung", *Math. Z.* 63 (1955/56), 406-444.

[17] James A. Cohn and Donald Livingstone, "On the structure of group algebras, I", *Canad. J. Math.* 17 (1965), 583-593.

[18] Charles W. Curtis, Irving Reiner, *Representation theory of finite groups* (Pure and Applied Mathematics, 11. Interscience [John Wiley & Sons], New York, London, 1962).

[19] Everett C. Dade, "Deux groupes finis distincts ayant la même algèbre de groupe sur tout corps", *Math. Z.* 119 (1971), 345-348.

[20] A. Fröhlich, "The Picard group of noncommutative rings, in particular or orders", *Trans. Amer. Math. Soc.* 180 (1973), 1-45.

[21] Graham Higman, "Units in group rings" (D. Phil. thesis, University of Oxford, Oxford, 1940).

[22] Graham Higman, "The units of group-rings", *Proc. London Math. Soc.* (2) 46 (1940), 231-248.

[23] I. Hughes and K.R. Pearson, "The group of units of the integral group ring ZS_3 ", *Canad. Math. Bull.* 15 (1972), 529-534.

[24] D.A. Jackson, "The groups of units of the integral group rings of finite metabelian and finite nilpotent groups", *Quart. J. Math. Oxford* (2) 20 (1969), 319-331.

[25] G. Karpilovsky, "On the isomorphism problem for integral group rings", *J. Algebra* 59 (1979), 1-4.

[26] G. Karpilovsky, "On group rings of finite metabelian groups", *J. Austral. Math. Soc. Ser. A* **28** (1979), 378-384.

[27] G. Karpilovsky, "Finite groups with isomorphic group algebras", *Illinois J. Math.* (to appear).

[28] G. Karpilovsky, "On some properties of group rings", *J. Austral. Math. Soc. Ser. A* (to appear).

[29] А.И. Лихтман [A.I. Lihtman], "О групповых кольцах p-групп" [On group rings of p-groups], *Izv. Akad. Nauk SSSR Ser. Mat.* **27** (1963), 795-800.

[30] G.A. Miller, H.F. Blichfeldt, L.E. Dickson, *Theory and applications of finite groups* (J. Wiley & Sons, New York; Chapman and Hall, London; 1916. Reprinted and corrected: Stechert, New York, 1938. Republished: Dover, New York, 1961).

[31] Tadao Obayashi, "Solvable groups with isomorphic group algebras", *J. Math. Soc. Japan* **18** (1966), 394-397.

[32] Tadao Obayashi, "Integral group rings of finite groups", *Osaka J. Math.* **7** (1970), 253-266.

[33] D.S. Passman, "Isomorphic groups and group rings", *Pacific J. Math.* **15** (1965), 561-583.

[34] Donald S. Passman, *The algebraic structure of group rings* (Interscience [John Wiley & Sons], New York, London, Sydney, 1977).

[35] K.R. Pearson, "On the units of a modular group ring", *Bull. Austral. Math. Soc.* **7** (1972), 169-182.

[36] K.R. Pearson, "On the units of a modular group ring II", *Bull. Austral. Math. Soc.* **8** (1973), 435-442.

[37] K.R. Pearson and D.E. Taylor, "Groups subnormal in the units of their modular group rings", *Proc. London Math. Soc.* (3) **33** (1976), 313-328.

[38] Gary L. Peterson, "Automorphisms of the integral group ring of S_n ", *Proc. Amer. Math. Soc.* **59** (1976), 14-18.

[39] С.С. Полян [S.S. Poljak], "Необходимое условие изоморфизма групполых колец над кольцом" [On a necessary condition for isomorphism of group rings over a ring], *Dokl. Užgorod Gos. Univ.* No. 3 (1960), 62.

[40] K.W. Roggenkamp, "Group rings of metabelian groups and extension categories", *Canad. J. Math.* (to appear).

[41] А.И. Саксонов [A.I. Saksonov], "О целочисленном кольце характеров конечной группы" [The integral ring of characters of a finite group", *Vesci Akad. Navuk BSSR Ser. Fiz.-Mat. Navuk* 1966,, No. 3, 69-76.

[42] А.И. Саксонов [A.I. Saksonov], "О некоторых целочислеччых кольцах, ассоциированных с конечной группой" [Certain integer-valued rings associated with a finite group", *Dokl. Akad. Nauk SSSR* 171 (1966), 529-532.

[43] А.И. Саксонов [A.I. Saksonov], "О групповых кольцах конечных p-групп над некоторыми областями целостности" [On group rings of finite p-groups over certain integral domains", *Dokl. Akad. Nauk SSSR* 11 (1967), 204-207.

[44] А.И. Саксонов [A.I. Saksonov], "О групповых кольцах конечных групп I" [Group rings of finite groups I], *Publ. Math. Debrecen* 18 (1971), 187-209 (1972).

[45] Robert Sandling, "The modular group rings of p-groups" (PhD thesis, University of Chicago, Chicago, 1969).

[46] Robert Sandling, "Subgroups dual to dimension subgroups", *Proc. Cambridge Philos. Soc.* 71 (1972), 33-38.

[47] Robert Sandling, "Note on the integral group ring problem", *Math. Z.* 124 (1972), 255-258.

[48] Robert Sandling, "Dimension subgroups over arbitrary coefficient rings", *J. Algebra* 21 (1972), 250-265.

[49] Robert Sandling, "Group rings of circle and unit groups", *Math. Z.* 140 (1974), 195-202.

[50] Sudarshan K. Sehgal, "Isomorphism of p-adic group rings", *J. Number Theory* 2 (1970), 500-508.

[51] Sudarshan K. Sehgal, "On class sums in p-adic group rings", *Canad. J. Math.* 23 (1971), 541-543.

[52] Sudarshan K. Sehgal, *Topics in group rings* (Monographs and Textbooks in Pure and Applied Mathematics, 50. Marcel Dekker, New York and Basel, 1978).

[53] D.E. Taylor, "Groups whose modular group rings have soluble unit groups", *Group theory*, 112-117 (Proc. Miniconf. Theory of Groups, Canberra, 1975. Lecture Notes in Mathematics, 573. Springer-Verlag, Berlin, Heidelberg, New York, 1977).

[54] William R. Weller, "The units of the integral group ring ZD_4 " (PhD thesis, Pennsylvania State University, Pennsylvania, 1972).

[55] Albert Whitcomb, "The group ring problem" (PhD thesis, University of Chicago, Chicago, 1968).

[56] Э.М. Жмудь, Г.Ч. Куренной [È.M. Žmud', G.Č. Kurennoĭ], "О конечных группах единиц целочисленного группового кольца" [The finite groups of units of an integral group ring], *Vestnik Har'kov. Gos. Univ.* 1967, no. 26, 20-26.

Department of Mathematics,
La Trobe University,
Bundoora,
Victoria 3083,
Australia.