J. Austral. Math. Soc. (Series A) 29 (1980), 385–392

ON SOME PROPERTIES OF GROUP RINGS

G. KARPILOVSKY

(Received 7 August; revised 11 December 1979)

Communicated by H. Lausch

Abstract

Let Out(RG) be the set of all outer R-automorphisms of a group ring RG of arbitrary group G over a commutative ring R with 1. It is proved that there is a bijective correspondence between the set Out(RG) and a set consisting of $R(G \times G)$-isomorphism classes of R-free $R(G \times G)$-modules of a certain type. For the case when G is finite and R is the ring of algebraic integers of an algebraic number field the above result implies that there are only finitely many conjugacy classes of group bases in RG. A generalization of a result due to R. Sandling is also provided.

1980 Mathematics subject classification (Amer. Math. Soc.): primary 20 C 07; secondary 20 C 05.

For R a commutative ring and A an R-algebra, let $\mathrm{Pic}_R(A)$ be the group of isomorphism classes of invertable (A, A)-bimodules for which the left and the right R-module structure coincide. The significance of $\mathrm{Pic}_R(A)$ in its relation to the automorphism group $\mathrm{Aut}_R(A)$ of the algebra A was vividly demonstrated in Fröhlich (1973) which contained among other results the existence of a homomorphism Ω of $\mathrm{Aut}_R(A)$ into $\mathrm{Pic}_R(A)$ whose kernel is the group of all inner automorphisms of A.

In the first part of the paper we give an explicit description of Ω for the case when A is a group algebra RG of an arbitrary group G over a commutative ring R with 1.

We shall say that two group bases G_1 and G_2 of RG are conjugate in RG if $u^{-1}G_1u = G_2$ for some invertible element u in RG. It is a consequence of the above description that if G is finite and if R is the ring of algebraic integers of an algebraic number field then there are only finitely many conjugacy classes of group bases in RG. As another application of the above description we shall establish a criterion for when two isomorphic group bases in the integral group ring ZG of a finite group G are conjugate in QG. In the second part of the paper we prove that if G is an arbitrary group, K is an arbitrary associative ring with 1, $I(G)$ is the augmentation ideal of KG and N/M is an abelian section of G then there is a K-module isomorphism

$$\frac{I(N)\,KG}{I(N)\,I(G)+I(M)\,KG} \simeq K \otimes_Z N/M.$$

Moreover, if M/N is a normal abelian section then the above isomorphism is a KG-isomorphism where the KG-module structure on $K \otimes_Z N/M$ is defined by

$$g(k \otimes_Z nM) = k \otimes_Z gng^{-1}\mathrm{M}\ (k \in K, n \in N, g \in G).$$

This result was established by R. Sandling in Sandling (1972) for the case $K = Z$.

1. Automorphisms of RG and $R(G \times G)$-modules

Let RG be a group algebra of an arbitrary group G over a commutative ring R with 1. Denote by $U(RG)$ the group of units of RG and by $\mathrm{Aut}(RG)$ the group of all R-automorphisms of RG. For each $u \in U(RG)$ let i_u be the inner automorphism of RG defined by $i_u(x) = u^{-1}xu$, $x \in RG$. The group of inner automorphisms of RG is defined as $\mathrm{In}(RG) = \{i_u \mid u \in U(RG)\}$. It is clear that $\mathrm{In}(RG)$ is a normal subgroup of $\mathrm{Aut}(RG)$. We set $\mathrm{Out}(RG) = \mathrm{Aut}(RG)/\mathrm{In}(RG)$, the outer automorphism group of RG. We shall also write $RG = RH$ when H is a group basis of RG.

We first need the following.

LEMMA. *Let $\bar{G} = G \times G$ and let for any $f \in \mathrm{Aut}(RG)$, M_f be the additive group of RG. Then M_f is a (left) R-free $R\bar{G}$-module under the following action of $R\bar{G}$:*

$$\text{for each } t = \sum_{i=1}^{n} \alpha_i(a_i, b_i) \in R\bar{G} \text{ and for each } x \in M_f,$$

$$t \circ x = \sum_{i=1}^{n} \alpha_i\, a_i\, x f(b_i^{-1}).$$

PROOF. To prove that M_f is an $R\bar{G}$-module it is enough to check that M_f is a $\bar{G}$-module under the composition $(a,b) \circ x = axf(b^{-1})$, $(a,b) \in \bar{G}$, $x \in M_f$. It is clear that for any $x_1, x_2 \in M_f$, $(a,b) \circ (x_1 + x_2) = (a,b) \circ x_1 + (a,b) \circ x_2$ *and that* $(1,1) \circ x = x$ *for any* $x \in M_f$. Let $(c,d) \in G$. Then for any $x \in M_f$,

$$[(a,b)(c,d)] \circ x = acxf(d^{-1})f(b^{-1}) = (a,b) \circ [cxf(d^{-1})] = (a,b) \circ [(c,d) \circ x].$$

Hence M_f is an $R\bar{G}$-module. Since the group algebra RG is an R-free module and since $r(1,1) \circ x = rx$ for any $r \in R$, $x \in RG$ it follows that M_f is also R-free, regarded as $R\bar{G}$-module, proving the lemma.

Denote by $P(RG)$ the set, consisting of all $R\bar{G}$-isomorphism classes (M_f) of $R\bar{G}$-modules M_f, where f ranges all elements of $\mathrm{Aut}(RG)$. Let also $M_f = M$ for $f =$ identity automorphism. We are now ready to prove the following.

THEOREM 1. *The mapping* $\Omega\colon \mathrm{Out}(RG) \to P(RG)$ *defined by* $\Omega[f\,\mathrm{In}(RG)] = (M_f)$ *is a bijection. In particular,* $f \in \mathrm{In}\,(RG)$ *if and only if the* $R\bar{G}$*-modules* M *and* M_f *are isomorphic.*

PROOF. Let $\varphi \in \mathrm{Aut}(RG)$, $u \in U(RG)$ and let $\psi = \varphi . i_u$. Consider the mapping:

$$\mu : M_\varphi \to M_\psi \text{ defined by } \mu(x) = x\varphi(u)$$

for any $x \in M_\varphi$. It is clear that μ is an R-isomorphism of $R\bar{G}$-modules M_φ and M_ψ. On the other hand, for any $(a,b) \in \bar{G}$ and for any $x \in M_\varphi$ we have

$$\mu((a,b)\circ x) = \mu(ax\varphi(b^{-1})) = ax\varphi(b^{-1})\,\varphi(u) = ax\varphi(u)\,\varphi(u^{-1}b^{-1}u) = a\mu(x)\,\psi(b^{-1})$$
$$= (a,b)\circ\mu(x).$$

Hence μ is an $R\bar{G}$-isomorphism and therefore the map Ω is well defined. Now let

$$\theta : M_\varphi \to M_f \text{ be an } R\bar{G}\text{-isomorphism and let } u = \theta(1).$$

Then for any $(a,b) \in \bar{G}$ and for any $x \in M_\varphi$, the equality $\theta[(a,b)\circ x] = (a,b)\circ\theta(x)$ implies

(1) $$\theta(ax\varphi(b^{-1})) = a\theta(x)\,f(b^{-1}).$$

Taking $x = b = 1$ in (1) we obtain $\theta(a) = au$ for any $a \in G$ and since θ is necessarily an R-isomorphism of $R\bar{G}$-modules M_φ and M_f it follows that

(2) $$\theta(x) = xu \quad \text{for any } x \in M_\varphi.$$

Next choose $a = x = 1$ in (1), whence

$$\theta[\varphi(b^{-1})] = uf(b^{-1})$$

for any $b \in G$ and it follows from (2) that $\varphi(g)u = uf(g)$ for any $g \in G$. Hence

(3) $$\varphi(x)\,u = uf(x) \quad \text{for any } x \in M_\varphi$$

Therefore $RGu = uRG$ and it follows from (2) that $RG = RGu$ and $RG = uRG$ whence $u \in U(RG)$. It follows from (3) that for any $x \in M_\varphi$,

$$f(x) = u^{-1}\,\varphi(x)\,u, \quad \text{that is, } f = i_u\,\varphi.$$

This shows that the map Ω is one-to-one and since Ω is obviously surjective, the proof is complete.

Until now G could have been any group. The assumption that G is finite will now be brought into play. Let $ZG = ZH$ where G is a finite group, $G \cong H$ and let H be a normalized group basis of ZG, that is H is a basis consisting of units having augumentation 1. 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 S. D. Berman and A. R. Rossa (Berman and Rossa (1966)). Therefore we are led to ask whether for an arbitrary finite group G the number of conjugacy classes of group bases in ZG is finite. For the case $R = Z$ the following corollary gives a positive answer to this question.

COROLLARY 1. *There are only finitely many conjugacy classes of group bases in RG where R is the ring of algebraic integers of an algebraic number field and G is a finite group.*

PROOF. The application of Zassenhau's Theorem (Curtis and Reiner (1962)) and of the above Theorem implies that the group $\mathrm{Aut}(RG)/\mathrm{In}(RG)$ is finite. Let

$$\mathrm{Aut}(RG) = \mathrm{In}(RG) + \mathrm{In}(RG)\varphi_2 + \dots + \mathrm{In}(RG)\varphi_t$$

be the coset decomposition of $\mathrm{Aut}(RG)$ with respect to $\mathrm{In}(RG)$. Suppose that H is an arbitrary group basis of RG. Since $|H| = |G|$ there exists only a finite number of nonisomorphic group bases in RG, say, $G_1, G_2, \dots, G_n$. Hence $H \cong G_i$ for some $i \in \{1, 2, \dots, n\}$ and therefore there exists $f \in \mathrm{Aut}(RG)$ such that $f(G_i) = H$. Since $f = \theta\varphi_j$ for some $\theta \in \mathrm{In}(RG)$ and some $j \in \{1, 2, \dots, t\}$ then $f(G_i) = u^{-1}\varphi_j(G_i)u$ for some $u \in U(RG)$, that is H is conjugate to $\varphi_j(G_i)$, proving the result.

Another consequence of Theorem 1 is the following.

COROLLARY 2. *Let $ZG = ZH$ where G is finite, $H \cong G$ and let f be the automorphism of the rational group algebra QG which is the extension of the isomorphism $H \to G$ by Q-linearity. Denote by M (respectively M_f) the $Q(G \times G)$ module QG defined by $(a, b) \circ x = axb^{-1}, (a, b) \in G \times G, x \in QG$ (respectively the $Q(G \times G)$-module QG defined by $(a, b) \circ x = axf(b^{-1})$). Then H is conjugate to G in QG if and only if $\chi = \chi_f$ where χ (respectively χ_f) is the character of $G \times G$ afforded by M (respectively M_f).*

PROOF. All we have to do is to notice that $Q(G \times G)$-modules M and M_f are isomorphic if and only if $\chi = \chi_f$ and apply Theorem 1.

We now digress for a moment to make a few remarks. Note that the character table of a finite group G is determined by ZG (Saksonov (1966)). Since S_n is determined by its character table (Nagao (1957)) it follows that S_n is determined up to isomorphism by ZS_n. Hence the application of a result due to G. Peterson

(Peterson (1976)) implies that in QS_n, S_n is conjugate to any normalized group basis in ZS_n. It is not however known whether any normalized group basis in ZS_n is conjugate in ZS_n to S_n. That any normalized group basis of ZS_3 is conjugate in ZS_3 to S_3 is a result due to Hughes and Pearson (Hughes and Pearson (1972)). Finally, note that there is an intimate connection between the conjugacy of group bases and isomorphism problem. Indeed as it was pointed out in Whitcomb (1968) that if G is a p-group of class 2 and if every normalised group bases in ZG is conjugate in $O_p G$ to G where O_p the ring of p-adic integers, then any p-group of class $\leqslant 5$ is determined by its integral group ring.

2. Module Isomorphisms

In this section G always denotes an arbitrary group and K denotes an associative ring with 1. The augmentation ideal $I(G)$ of the group ring KG is the kernel of the homomorphism from the group ring KG to K induced by collapsing G to the unit group. If C and D are subsets of KG, define the Lie bracket (C, D) as the subgroup of the additive group of KG generated by all $(c, d) = cd - dc$, c in C, d in D. Let N and M be subgroups of G. Then the identity $(a-1, b-1) = ba(a^{-1}b^{-1}ab - 1)$, $a, b \in G$ implies $KG \,.\, I([N, M]) \leqslant KG(I(N), I(M))$ and in particular

$$KG \,.\, I([N, G]) \leqslant KG(I(N), I(G)). \tag{4}$$

The homomorphism $G \to K \otimes_Z G/G'$ determined by $g \to 1 \otimes gG'$ is called the universal homomorphism of G into the additive group of a K-module. We shall denote the kernel of this homomorphism by $G^{\langle K \rangle}$.

In this section we shall prove the following result.

THEOREM 2. *Let N/M be an abelian section of G. Then there is a K-module isomorphism*

$$\frac{I(N)\,KG}{I(N)\,I(G) + I(M)\,KG} \cong K \otimes_Z N/M.$$

Moreover if M/N is a normal abelian section then the above isomorphism is a KG-isomorphism, where the KG-module structure on $K \otimes_Z N/M$ is defined by $g(k \otimes nM) = k \otimes gng^{-1}M$ $(g \in G, k \in K, n \in N)$.

PROOF. Let $J = I(N)\,I(G) + I(M)\,KG$, $L = I(N)\,KG$ and let T be a right transversal of G relative to N containing 1. We first observe that L is a free K-module on the basis $\{(n-1)t \mid t \in T,\ 1 \neq n \in N\}$ *and that*

$$\Psi : L/J \to K \otimes_Z N/M$$

where $\Psi[(n-1)t + J] = 1 \otimes nM$ is a K-module epimorphism.

The mapping

$$\varphi : K \otimes_Z N/M \to L/J$$

defined by $\varphi(1 \otimes nM) = (n-1)+J$ is a K-module homomorphism. It is easy to see that φ is the inverse of ψ, proving the first part of the theorem. Suppose that N/M is a normal abelian section. Since the set $X = \{(n-1)+J \mid n \in N\}$ is a generating set of a K-module L/J the second part of the theorem will be established once we verify that for any $g \in G$ and any $n \in N$, $\Psi[g(n-1)+J] = g\Psi[(n-1)+J]$. Since the last equality is a consequence of the identity $g(n-1) = (gng^{-1}-1)g$ and the congruence $(gng^{-1}-1)\,g \equiv gng^{-1}-1 \pmod J$, the result follows.

The following corollaries are well known for the case $K = Z$ (see Sehgal (1978)).

COROLLARY 1. *Let N be a subgroup of G. Then there is a K-module isomorphism*

$$\frac{I(N)\,KG}{I(N)\,.\,I(G)} \cong K \otimes_Z N/N'.$$

Moreover, if $N \lhd G$ then the above isomorphism is a KG-isomorphism where the KG-module structure on $K \otimes_Z N/N'$ is defined by $g(k \otimes {}_nN') = k \otimes gng^{-1}N'$ $(g \in G, k \in K, n \in N)$.

PROOF. Since $I(N')\,KG \subseteq I(N)^2\,KG \subseteq I(N)\,.\,I(G)$ the application of Theorem 2 for the case $M = N'$ implies the desired isomorphism.

COROLLARY 2. *Let N be a normal subgroup of G. Then there is a KG-isomorphism*

$$\frac{I(N)\,KG}{I(N)\,.\,I(G)+I(G)\,.\,I(N)} \cong K \otimes_Z N/[N,G]$$

where the KG-module structure on $K \otimes_Z N/[N,G]$ is defined by

$$g(k \otimes n[N,G]) = k \otimes (gng^{-1})\,[N,G] \quad (k \in K, n \in N, g \in G)$$

PROOF. If $M = [N,G]$ then N/M is a normal abelian section of G and all we have to do is to prove that

$$(5) \qquad I(N)\,I(G)+I(G)\,.\,I(N) = I(N)\,.\,I(G)+I(M)\,KG.$$

It follows from (4) that

$$I(M)\,KG \subseteq KG\,(I(N), \quad I(G)) \subseteq I(N)I(G)+I(G)\,.\,I(N),$$

whence

$$I(N)\,.\,I(G)+I(M)\,KG \subseteq I(N)\,.\,I(G)+I(G)\,I(N).$$

On the other hand, the identity

$$(g-1)(n-1) = (n-1)(g-1)+(n-1)(g-1)(g^{-1}n^{-1}gn-1)$$
$$+(g-1)(g^{-1}n^{-1}gn-1)+(g^{-1}n^{-1}gn-1)$$
$$+(n-1)(g^{-1}\mathrm{n}^{-1}gn-1)$$

implies

$$I(G).I(N) \subseteq I(N).I(G)+I(M)KG.$$

Hence

$$I(N).I(G)+I(G).I(N) \subseteq I(N)I(G)+I(M)KG,$$

proving (5) and thus completing the proof.

The next corollary is known for the case when K is a commutative ring with 1 (see Bergman and Dicks (1975)).

COROLLARY 3. $$G \cap (1+I(G)^2) = G^{\langle K \rangle}.$$

PROOF. Let $\delta : G \to K \otimes G/G'$ where $\delta(g) = 1 \otimes gG'$. Then δ determines a K-module homomorphism $\mu : I(G) \to K \otimes_Z G/G'$ where $\mu(g-1) = 1 \otimes gG'$. Since $\delta(g) = \mu(g-1)$, so $g \in G^{\langle K \rangle}$ if and only if $g-1 \in \operatorname{Ker}\mu$. By taking the case $N = G$ and $M = G'$ in the proof of Theorem 2, we see that $\operatorname{Ker}\mu = I(G)^2$, as desired.

Acknowledgement

The author wishes to thank the referee for his valuable remarks.

References

G. M. Bergman and W. Dicks (1975), 'On universal derivations', *J. Algebra* **36**, 193–211.

S. D. Berman and A. R. Rossa (1966), 'Integral group rings of finite and periodic groups', *Algebra and Math. Logic*, Izdat Kiev, Univ. Kiev, pp. 44–53.

C. W. Curtis and I. Reiner (1962), *Representation theory of finite groups and associative algebras* (Interscience, New York and London).

A. Fröhlich (1973), 'The Picard group of noncommutative rings, in particular of orders', *Trans. Am. Math. Soc.* **180**, 1–46.

I. Hughes and K. R. Pearson (1972), 'The group of units of the integral group ring ZS_3' *Canad. Math. Bull.* **15**, 529–534.

H. Nagao (1957), 'On the groups with the same table of characters as symmetric groups' *J. Inst. Polytech. Osaka City Univ.* (Ser. A8), 1–8.

G. Peterson (1976), 'Automorphisms of the integral group ring of S_n', *Proc. Amer. Math. Soc.* **59**, 14–18.
A. I. Saksonov (1966), 'Certain integer valued rings associated with a finite group', *Dokl. Akad. Nauk SSSR* **171**, 529–532.
R. Sandling (1972), 'Note on the integral group ring problem', *Math. Z.* **124**, 255–258.
S. K. Sehgal (1978), *Topics in group rings* (Marcel Dekker, Inc., New York and Basel).
A. Whitcomb (1968), *The group ring problem* (PhD thesis, University of Chicago).

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

https://doi.org/10.1017/S1446788700021534 Published online by Cambridge University Press