On some properties of group rings

By G. KARPILOVSKY (Bundoora, Australia)

1. Introduction

The purpose of this paper is twofold. Firstly we show that there are only finitely many conjugacy classes of group bases in the integral group ring ZG of a finite group G. Secondly, as a generalization of the WHITCOMB's result [9] we prove that a finite metabelian group G is determined by the group ring RG where $R=\left\{\frac{a}{b}\,\middle|\, a, b\in Z,\ (b, |G|)=1\right\}$. We also apply the proof of this result to show that a group G of order 2^n, $n\leqq 7$, is determined by its integral group ring. For certain integral domains K we prove that any finite group which is the group of all units of some K-algebra is determined by the group ring KG.

In what follows KG denotes a group ring of a group G over an associative ring K with 1, $I(K, G)$ stands for the augmentation ideal of KG. The equality $KG=KH$ means that H is a normalised group bases of KG. We shall often write $I(G)$ instead of $I(K, G)$ when a precise situation will be clear from the context. If Λ is an ideal of KG and S is a subset of KG then put $G\cap 1+\Lambda=\{g\in G|g-1\in\Lambda\}$, $S+\Lambda=\{s+\Lambda|s\in S\}$. The group of all automorphisms of ZG and the group of inner automorphisms of ZG will be denoted by $\mathrm{Aut}\,(ZG)$ and $\mathrm{In}\,(ZG)$ respectively. Finally, O_p (respectively $Z_{(p)}$) stands for the ring of p-adic integers (respectively p-integral rationals) and $U(K)$ for the group of units in K.

2. Conjugacy classes of group bases in ZG

Let $ZG=ZH$ 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 S. D. BERMAN and A. R. ROSSA ([2] Theorem 4). 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 or infinite. The following theorem gives a positive answer to this question.

Theorem 1. *There are only finitely many conjugacy classes of group bases in ZG.*

PROOF. It follows from Theorems I and II of [4] that the group $\mathrm{Aut}\,(ZG)/\mathrm{In}\,(ZG)$ is finite. Let $\mathrm{Aut}\,(ZG)=\mathrm{In}\,(ZG)+\mathrm{In}(ZG)\varphi_2+\ldots+\mathrm{In}\,(ZG)\varphi_t$ be the coset decomposition of $\mathrm{Aut}\,(ZG)$ with respect to $\mathrm{In}\,(ZG)$. Suppose that H is an arbitrary group basis of ZG. Since $|H|=|G|$ there exists only a finite number of nonisomorphic group bases in ZG, say, $G_1, G_2, \ldots, G_n$. Hence $H \cong G_i$ for some $i \in \{1, 2, \ldots, n\}$ and therefore there exists $f \in \mathrm{Aut}(ZG)$ such that $f(G_i) = H$. Since $f = \Theta\varphi_j$ for some $\Theta \in \mathrm{In}(ZG)$ and some $j \in \{1, 2, \ldots, t\}$ then $f(G_i) = u^{-1}\varphi_j(G_i)u$ for some $u \in U(ZG)$, i.e. H is conjugate to $\varphi_j(G_i)$, proving the theorem.

3. The isomorphism problem for the group rings over some integral domains

The isomorphism problem for the group rings asks whether $KG = KH$ implies $G \cong H$. When this is so for a group G, G is said to be determined by the group ring KG. Call the ring K a $(*)$-ring if for every finite group G the coefficient of 1 in any periodic element x of $U(KG)$ is equal to 0 unless x is of the form $\alpha \cdot 1$ for some $\alpha \in K$.

Lemma 1. *Let N be a normal subgroup of a finite group G and let $\pi\colon KG \to K(G/N)$ be a canonical homomorphism where K is a $(*)$-ring. If $KG = KH$ then the following properties hold:*

(1) $K(G/N) = K\pi(H)$, $KG \cdot I(N) = KH \cdot I(N^*)$ *and* $|N| = |N^*|$ *where* $N^* = H \cap 1 + KG \cdot I(N)$. *Moreover, every normal subgroup of H is of the form N^* for some $N \lhd G$.*
(2) *Periodic elements of the centre of $U(KG)$ are trivial.*

By applying the same arguments as in the proof of Lemma 3.1 of [3] we see that $\pi(H)$ is a linearly independent set of the group ring $K(G/N)$. Hence $K(G/N) = K\pi(H)$ and therefore π can be regarded as the extension of the epimorphism $H \to \pi(H)$ by K-linearity. This shows that $\mathrm{Ker}\,\pi = KH \cdot I(N^*) = KG \cdot I(N)$. The equality $|N| = |N^*|$ is a consequence of the isomorphism $\pi(H) \cong H/N^*$.

Now if $S \lhd H$ then there exists $N \triangle G$ such that $KG \cdot I(N) = KH \cdot I(S)$. Hence $KH \cdot I(S) = KH \cdot I(N^*)$ and therefore $S = H \cap 1 + KH \cdot I(S) = H \cap 1 + KH \cdot I(N^*) = N^*$, proving (1). The proof of (2) is evident.

Let K be a commutative ring. We call a group G a unit group over K if G is isomorphic to the group of all units of some K-algebra. By taking the case $K = Z$ in the following theorem we obtain another proof of the characterization theorem for the unit groups due to R. Sandling [7].

Theorem 2. *Let G be a finite group and let A be a K-algebra, where K is an integral domain of characteristic 0 in which no prime dividing the order of G is invertible. If $KG = KH$ and if $\mu\colon G \to U(A)$ is a monomorphism then the mapping $\mu'\colon H \to U(A)$, given by $\mu\left(\sum_g \alpha_g g\right) = \sum_g \alpha_g \mu(g)$ for any $h = \sum_g \alpha_g g \in H$ is also a monomorphism. In particular, a finite group G which is a unit group over K is determined by the group ring KG.*

Proof. Let $\mu^*\colon KG \to A$ be the homomorphism of K-algebras obtained from μ by extension by K-linearity. Then μ' is the restriction of μ^* to H and therefore μ' is a homomorphism. It follows from [6] that K is a $(*)$-ring. Therefore by Lemma 1 we have $\mathrm{Ker}\,\mu' = N_1^*$ and $KG \cdot I(N_1) = KH \cdot I(N_1^*)$ for some $N_1 \lhd G$. Since $I(N_1^*) \subseteq \mathrm{Ker}\,\mu^*$ then $I(N_1) \subseteq \mathrm{Ker}\,\mu^*$ and therefore $N_1 \subseteq \mathrm{Ker}\,\mu = 1$. Thus $N_1^* = 1$, proving the theorem.

Corollary. *Let $\bar{B}$ be a subgroup of a finite abelian group B and let G be isomorphic to the group L of all automorphisms of B which leave $\bar{B}$ invariant (as a set). Then G is determined by its integral group ring.*

PROOF. Let $A=\mathrm{Hom}\,(B, B)$. Then the isomorphism $G\cong L$ induces monomorphism $G\to U(A)$. By Theorem 2 (with $K=Z$), the equality $ZG=ZH$ implies $\mu(G)=\mu'(H)$ and therefore $G\cong H$.

For the proof of our next theorem we need the following lemmas.

Lemma 2. *Let G be an arbitrary group, K an arbitrary ring with 1, N arbitrary subgroup of G. Then in the group ring KG the following equalities hold:*

$$I(G)\cdot I(N)\cap I(N) = I(N)^2 \tag{3}$$

$$G\cap 1+I(G)\cdot I(N) = N\cap 1+I(N)^2. \tag{4}$$

PROOF. Since $G\cap 1+KG\cdot I(N)=N$ it follows that $G\cap 1+I(G)\cdot I(N)=N\cap 1+ +I(G)\cdot I(N)=N\cap 1+\big(I(G)\cdot I(N)\cap I(N)\big)$ and therefore (3)$\Rightarrow$(4). Let T be a full set of cosets representatives of G with respect to N.

If $g=tn$ where $n\in N$, $t\in T$ then for $n'\in N$ we have $(g-1)(n'-1)= =(t-1)(n-1)(n'-1)+(t-1)(n'-1)+(n-1)(n'-1)$. Since the first and the second summands belong to $(t-1)\cdot I(N)$ and since $(n-1)(n'-1)\in I(N)^2$ then

$$(g-1)(n'-1)\in I(N)^2+(t-1)I(N)$$

from which follows that

$$I(G)\cdot I(N) = I(N)^2+\sum_{1\neq t\in T}(t-1)I(N).$$

Let

$$x = y+(t_1-1)[\alpha_{11}(n_1-1)+\ldots+\alpha_{1s}(n_s-1)]+\ldots+(t_k-1)[\alpha_{s1}(n_1-1)+\ldots+\alpha_{ss}(n_s-1)]$$

where $y\in I(N)^2$, $t_j\in T$, $n_i\in N$, $1\leqq i\leqq s$, $1\leqq j\leqq k$. If $x\in I(N)$ then $z=\alpha_{11}t_1(n_1-1)+ +\ldots+\alpha_{1s}t_s(n_s-1)+\ldots+\alpha_{ss}t_k(n_s-1)\in I(N)$ and since all elements of N have coefficient 0 in z, then $z=0$. But $\{t_1(n_1-1), \ldots, t_s(n_s-1)\}$ is a linearly independent set and therefore $\alpha_{11}=\ldots=\alpha_{1s}=\ldots=\alpha_{ss}=0$. Hence $x=y\in I(N)^2$, proving the lemma.

Lemma 3. *Let G be a group containing an abelian subgroup A of a finite exponen: n and let $K=Z/mZ$ where $m\equiv 0 \pmod n$. Then the following properties holdt*

$$G\cap 1+I(G)\cdot I(A) = 1. \tag{5}$$

(6) If $x\in KG$ and if $x\equiv g\big(\mathrm{mod}\, KG\cdot I(A)\big)$ for some $g\in G$ then there exists an element $g_x=ga(a\in A)$ such that $x\equiv g_x\big(\mathrm{mod}\, I(G)\cdot I(A)\big)$.

PROOF. As in the case $K=Z$, the formula

$$f\Big(\sum_{\alpha\in A}(\alpha_a\cdot 1)(a-1)\Big) = \prod_{a\in A}a^{\alpha_a}(\alpha_a\in Z)\quad \text{defines a homomorphism of } I(A)$$

onto A with kernel $I(A)^2$. From this follows that $A\cap 1+I(A)^2=1$ and the application of (3) yields (5).

Since $f(\sum_{a\in A}(\alpha_a\cdot 1)(a-1))=f(\prod_{a\in A}a^{\alpha_a}-1)$ then

$$\sum_{a\in A}(\alpha_a\cdot 1)(a-1)\equiv\prod_{a\in A}a^{\alpha_a}-1 \pmod{I(A)^2}(\alpha_a\in Z). \tag{7}$$

Note also that $KG=K+I(G)$ whence $KG\cdot I(A)=I(A)+I(G)\cdot I(A)$ and $x\equiv g+ +t(\text{mod } I(G)\cdot I(A))$ for some $t=\sum_{s\in A}(\alpha_s\cdot 1)(s-1)\in I(A)$. Applying (7) we obtain

$$x\equiv g+(a-1)=(1-g)(a-1)+ga\equiv g_x \pmod{I(G)\cdot I(A)}$$

where $a=\prod_{s\in A}s^{\alpha_s}$. This completes the proof of the lemma.

Let K be a commutative ring and let $\varphi\colon K-\bar{K}$ be the ring epimorphism. If $x=\sum_g\alpha_g g\in KG$ then put $\bar{x}=\sum_g\bar{a}_g g$ where $\bar{a}_g=\varphi(\alpha_g)$.

It is clear that the mapping $\lambda\colon KG\to\bar{K}G$, defined by $\lambda(x)=\bar{x}$ for any $x\in KG$ is a ring epimorphism. We cal λ the projection of KG onto $\bar{K}G$. Suppose that Λ is an ideal of the group algebra $\bar{K}G$. Then the ring $\bar{K}G/\Lambda$ can be regarded as a K-algebra in the obvious way. Moreover, the mapping $\varphi^*\colon KG\to\bar{K}G/\Lambda$ defined by $\varphi^*(x)=\bar{x}+\Lambda$ is a K-algebra homomorphism. We are now ready to prove the following result.

Theorem 3. *A finite metabelian group G is determined by the group ring RG where* $R=\left\{\frac{a}{b}\,\middle|\,a,b\in Z,\ (b,|b|)=1\right\}$.

Proof. Let $RG=RH$. The mapping $\varphi\colon R\to\bar{R}=Z/|G|Z$ defined by $\varphi\left(\frac{a}{b}\right)= =\bar{a}(\bar{b})^{-1}$ where $\bar{a}=a+|G|Z$ is a ring epimorphism. Consider the mapping φ^* defined as above by taking $\Lambda=I(\bar{R},G)\cdot I(\bar{R},G')$. It follows from (5) and the Theorem 2 that the restrictions of φ^* to G and H induce group isomorphisms $G\to\varphi^*(G)$ and $H\to\varphi^*(H)$, where $\varphi^*(G)=G+\Lambda$, $\varphi^*(H)=\bar{H}+\Lambda$, $\bar{H}=\{\bar{h}|h\in H\}$. Since R is a $(*)$-ring [6] the application of (2) to $R(G/G')$ yields $G+RG\cdot I(R,G')=H+ +RG\cdot I(R,G')$.

Therefore projecting RG onto $\bar{R}G$ we obtain $G+\bar{R}G\cdot I(\bar{R},G')=\bar{H}+\bar{R}GI(\bar{R},G')$. It follows from (6) that in this case $\bar{H}+\Lambda\subseteqq G+\Lambda$, i.e. $\varphi^*(H)\subseteqq\varphi^*(G)$. But $|G|= =|H|$ and therefore $G\cong H$, proving the theorem.

In [8] W. R. Weller proved that there are only two nonconjugate classes of normalised group bases of ZD_4, where D_4 is a dihedral group of order 8. By combining this result with the Theorem 4 of [2] we obtain the following property:

(8) *Every two normalised group bases of ZD_4 are conjugate in $U(Z_{(2)}D_4)$.*

Theorem 4. *Let $|G|=2^n$, $n\leqq 7$. Then the group G is determined by its integral group ring.*

Proof. Every group of order 2^n, $n\leqq 6$ is metabelian and a group G of order 2^7 has a normal abelian subgroup A of index 8 ([5], p. 120). Hence we can restrict ourselves to the case when $|G|=2^7$ and the factor group G/A is nonabelian of order 8. Let $ZG=ZH$. It follows from the proof of Theorem 3 that

(9) $$G \cong H \quad \text{whenever} \quad G+RG\cdot I(R, A) = H+RG\cdot I(R, A).$$

If G/A is the quaternion group then by [1] $G+ZG\cdot I(Z, A)=H+ZG\cdot I(Z, A)$. Thus we have only to consider the case when $G/A\cong D_4$. Let $\pi\colon ZG\to Z(G/A)$ be the canonical homomorphism. It follows from (1) that $Z\pi(G)=Z\pi(H)$ and therefore $Z_{(2)}\pi(G)=Z_{(2)}\pi(H)$.

By (8) there exists a unit $u\in Z_{(2)}\pi(G)$ such that $u^{-1}\pi(H)u=\pi(G)$ and since $Z_{(2)}D_4$ is a local ring then $u=\pi(t)$ for some $t\in Z_{(2)}G$. Therefore $\pi(t^{-1}Ht)=\pi(G)$ and $t^{-1}Ht+RG\cdot I(R, A)=G+RG\cdot (IR, A)$ for $R=Z_{(2)}$. It follows from (9) that in this case $G\cong t^{-1}Ht$, proving the theorem.

References

[1] S. D. BERMAN, On the equation $x^n=1$ in an integral group ring, *Ukrain. Math. Z.* **7** (1955), 253—261.

[2] S. D. BERMAN and A. R. ROSSA, On integral group rings of finite and periodic groups, *Algebra and Logic, Izd. Kiev University* (1966), 44—53.

[3] J. A. COHN and D. LIVINGSTONE, On the structure of group algebras, I *Canad. J. Math.* **17** (1965), 583—593.

[4] A. FRÖLICH, The Picard group of noncommutative rings, in particular orders, *Trans. Am. Math. Soc.* **180** (1973), 1—46.

[5] G. A. MILLER, H. F. BLICHFELDT, L. E. DICKSON, Theory and applications of finite groups, *Dover Publications, INC.*, New York.

[6] A. I. SAKSONOV, Group rings of finite groups I, *Publ. Math. (Debrecen)*, **18** (1971), 187—209.

[7] R. SANDLING, Group rings of Circle and Unit groups, *Math. Z.* **140** (1974), 195—202.

[8] W. R. WELLER, The units of the integral group ring ZD_4, *Ph. D. Thesis, Pennsylvania State Univ.*, 1972.

[9] A. WHITCOMB, The group ring problem, *Ph. D. Thesis, Univ. of Chicago*, 1968.

MATH. DEPT. LA TROBE UNIV.
BUNDOORA, VICTORIA, AUSTRALIA 3083

(Received December 19, 1978)