Group bases of group rings

Héctor A. Merklen

1. Preliminaries.

The isomorphism problem, since first formulated by Thrall almost 40 years ago, has made a very slow progress, even though a great deal of work has been done considerably improving our knowledge of group rings (see [5]). The most important case, that of group rings over $\mathbb{Z}$, has been solved only when the finite group G is abelian (Higman, 1940), nilpotent of class 2 (Cohn & Livingstone, 1965, and Passman, 1965), metabelian (A. Whitcomb, 1968), and for some special classes of groups (P. Sandling, 1972)

It is well known, and has been exploited by several authors, that an exact sequence of groups, $1 \to A \to G \to G/A \to 1$, with A abelian (resp. central) gives good information about $\mathbb{Z}G$ as compared with $\mathbb{Z}(G/A)$. This naturally suggests that there would be a way, by induction, of solving the isomorphism problem for solvable (resp. nilpotent) groups.

In this paper we show that, given such an exact sequence, there is an exact sequence $1 \to A \to W \to V(\mathbb{Z}(G/A)) \to 1$, where W is the group of normalized units of $\mathbb{Z}G/\Delta A \Delta G$ (see Prop. 1). This leads to a generalization of Whitcomb result: if two group bases, G, H, of $\mathbb{Z}G$ reduce, modulo ΔA, to two bases $\bar{G}$, $\bar{H}$, of $\mathbb{Z}(G/A)$ which are conjugate by a unit of this ring, then G and H are isomorphic (see Cor. to Prop. 3).

Also we show that, if $\bar{H}$ is related to $\bar{G}$ by an automorphim of $\mathbb{Z}(G/A)$, then the group structure of H (as an extension of $\bar{H}$ by A) can be explicitely computed in terms of the structure of G (as an extension of $\bar{G}$ by A) (see Prop. 4). The explicit formulas obtained here may be used to test the possibility of solving the isomorphism problem by induction or, perhaps, to find counter-examples to the conjecture.

Finally, it is shown throughout that a good amount of our techniques apply also to the case in which the coefficients ring is the prime field of p elements, provided that the abelian group A is p-elementary.

Throughout let G be a group and R a commutative ring with 1. If B is a subgroup of G, ΔB is the left ideal of the group ring RG generated

Recebido em janeiro de 1979.

by $B\text{-}1 = \{b-1/b \in B\}$. Hence, if B is normal in G, ΔB is a two-sided ideal. In particular, ΔG is the augmentation ideal, i.e. the kernel of the augmentation map $\varepsilon: RG \to R$.

We will denote by A an abelian, normal subgroup of G, and bars will denote objects modulo A or modulo ΔA, depending on the context.

The units of RG have augmentation a unit of R. Those units with augmentation 1 are called normalized; they form the group $V(RG) = U(RG) \cap (1 + \Delta G)$, which is normal in $U(RG)$ and contains G. In the sequel, unless otherwise indicated, all units of group rings will be assumed to be normalized.

A group of units which is an R-basis for a group ring over R will be called a *group basis* for that ring.

Most of the time, one of the following hypotheses will be assumed:

$H1$. $R = \mathbb{Z}$, the ring of rational integers;
$H2$. $R = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, and A is p-elementary.

Lemma 1. *If B is a normal subgroup of G, the following sequences of RG-modules are exact.*

$$0 \to \Delta B \to RG \to R(G/B) \to 0;$$
$$0 \to \Delta B \to \Delta G \to \Delta(G/B) \to 0.$$

Proof. See [5], 1.10, and [3], Prop. (7.4).

Lemma 2. *Assume $H1$. The map $a \to a - 1$ induces an isomorphism from A onto $\Delta A/(\Delta A \Delta G)$, so that the following are exact sequences of RG-modules:*

$$1 \to A \to \frac{RG}{\Delta A \Delta G} \to R\bar{G} \to 0,$$
$$1 \to A \to \frac{\Delta G}{\Delta A \Delta G} \to \Delta \bar{G} \to 0.$$

Proof. See [4], lemma 6, and [3], lemma (12.17). Here G (or, also, $\bar{G}$) acts on A by conjugation, because given g in G and a in A:

$$g(a-1) \equiv g(a-1)g^{-1} = gag^{-1} - 1 \qquad (mod\ \Delta A \Delta G).$$

Remarks.

1. Notice that multiplication on the right by an element of augmentation 1 gives the identity operator on ΔA modulo $\Delta A \Delta G$.
2. Observe that the second sequence in *lemma* 2 is naturally an exact sequence of $R\bar{G}$-modules.

3. Let $R = \mathbb{Z}$ and A be p-elementary (that is $a^p = 1$ for each a in A), then *lemma* 2 implies that $p\Delta A \subset \Delta A \Delta G$. It follows that *lemma* 2 is also valid under $H2$.
4. Define $X = RG/\Delta A \Delta G$, $Y = \Delta G/\Delta A \Delta G$. The ring X will play a significant role in what follows.

Proposition 1. *Assume either $H1$ or $H2$. Let $\bar{\varepsilon}$ be the map $X \to R$ induced by the argmentation map ε, and let W be the group of normalized units of X (i.e., units of X with augmentation 1).*
Then

(i) *Define* $\tilde{W} = \left\{x \in X / \frac{\Delta A}{\Delta A \Delta G} + x \text{ is invertible in } \frac{X}{\Delta A/\Delta A \Delta G}\right\}$, *then* $\tilde{W} = W$.

(ii) *There is an exact sequence of groups*:

$$1 \to A \to W \to V(RG) \to 1.$$

Proof. The canonical map $RG \to R\bar{G}$ induces an epimorphism of semigroups: $1 + \Delta G \to 1 + \Delta \bar{G}$. The commutative diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \Delta A \Delta G & & \Delta A \Delta G & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \Delta A & \to & \Delta G & \to & \Delta \bar{G} & \to & 0 \\
 & & \downarrow & & \downarrow \alpha & & \downarrow \cong & & \\
0 & \to & \frac{\Delta A}{\Delta A \Delta G} & \to & \frac{\Delta G}{\Delta A \Delta G} & \to & \frac{\Delta G}{\Delta A} & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

where α is the canonical epimorphism $RG \to X$, induces then an exact, commutative diagram in the category of semigroups:

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & 1 + \Delta A \Delta G & = & 1 + \Delta A \Delta G & \to & 1 & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & 1 + \Delta A & \to & 1 + \Delta G & \to & 1 + \Delta \bar{G} & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & T & \to & S & \to & 1 + \Delta \bar{G} & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

where S, T, are, respectively, the images under α of $1 + \Delta G$, $1 + \Delta A$. As it is easily seen, T is isomorphic to A.

The pull-back construction gives the following exact, commutative diagram:

$$\begin{array}{ccccccccc} 1 \to & T & \to & W & \to & V(R\bar{G}) & \to & 1 \\ & \| & & \downarrow & & \downarrow & & \\ 1 \to & T & \to & S & \to & 1+\Delta\bar{G} & \to & 1 \end{array}$$

It is clear that the group of normalized units in X is contained in the semigroup $\tilde{W}$ but, since both A and $V(R\bar{G})$ are groups, $\tilde{W}$ itself is a group and hence equal to the group of normalized units. Since T is isomorphic to A, the proof is complete.

Q.E.D.

Remark. For the sake of clarity, the group A will be identified only to the ideal $\Delta A/(\Delta A \Delta G)$ of X. Despiste the statement of *Prop.* 1, T will not be replaced by A in what follows.

2. The classification of group bases.

Proposition 2. *Assume H1 and that G is a finite group.*

(i) *If H is a finite subgroup of $V(\mathbb{Z}G)$, H is $\mathbb{Z}$-free;*

(ii) *If H is a finite subgroup of $V(\mathbb{Z}G)$, $\mathbb{Z}H$ is purely embedded in $\mathbb{Z}G$, as $\mathbb{Z}$-modules.*

(iii) *A group of normalized units in $\mathbb{Z}G$ is a group basis if and only if its order is equal to the order of G.*

(iv) *A finite subgroup H of $V(\mathbb{Z}G)$ is $\mathbb{Z}$-free if and only if $-1 \notin H$. If -1 is in H, then $H = \{1, -1\} \times (H \cap V(\mathbb{Z}G))$.*

Proof. Almost all the above is an easy consequence of a well-known result of Berman's (see [1]) and [3], (11.2)): if $h = \sum_{g \in G} \alpha_g g$, then either $\alpha_1 = 0$ or $h = \pm 1$.

For the proof of (i) see [3], (12.3).

In order to prove (ii), let x be a torsion element of $\mathbb{Z}G$ modulo $\mathbb{Z}H$. It may be assumed that there is a prime p such that px is in $\mathbb{Z}H$. In other words, if $\mathbb{Z}H$ is not purely embedded in $\mathbb{Z}G$, there exists a relation of the form $\Sigma \alpha_h h \in p\mathbb{Z}G$, where not all the integers α_h are divisible by p. This again leads to a contradiction with Berman's Theorem.

Part (iii) is a direct consequence of (i) and (ii).

Finally, let H be any finite group of units (not necessary normalized). The mapping $x \to \varepsilon(x)x$ defines a homomorphism of H onto a group of normalized units, K, with kernel $\{1, -1\} \cap H$. When -1 lies outside

H, then H is isomorphic to the $\mathbb{Z}$-free group K and generates the same group ring. Therefore, H is $\mathbb{Z}$-free in this case. The last assertion follows from the fact that, when -1 lies in H, then K is a normal subgroup of H.

Q.E.D.

Remark. This proposition allows one to give a good description of homomorphisms of integral group rings.

Let E be a finite group and $f : \mathbb{Z}G \to \mathbb{Z}E$ a homomorphism. Let H be the image of G under f.

If H does not contain -1, f can be factored thus:

$$\begin{array}{ccc} \mathbb{Z}G & \xrightarrow{f} & \mathbb{Z}E \\ \phi \downarrow & & \uparrow \\ \mathbb{Z}\bar{G} & \xrightarrow{\cong} & \mathbb{Z}H \end{array}$$

Where the arrow upwards is the natural injection, the bottom arrow is induced by the canonical isomorphism $G/ker(f \mid G) \to f(G)$ and ϕ is induced by the natural epimorphism $G \to G/ker(f \mid G) = : \bar{G}$. Hence, this first kind of homomorphisms are essentially the epimorphisms induced on group rings by epimorphisms of the groups.

If H does contain -1, one has a little more complicated kind of homomorphism. In this case, one writes: $H = \{1, -1\} \times K$, *as in* Prop. 2, (iv), and calling ε' the augmentation map of $\mathbb{Z}E$, one obtains that $f \mid G$ is the product of $\varepsilon \circ f : G \to \{1, -1\}$ and $f_1 = (\varepsilon \circ f) f : G \to K$, which is a homomorphism of the first kind discussed above.

The following facts are well known, at least for the case of integral group rings, but the author does not know a good reference. Hence, the proof is given.

Proposition 3. *Let G be a finite group. Assume H1. The natural map $\alpha : RG \to X$ (cf. proof of Prop. 1) embeds each group basis H onto some subgroup of W. Two group bases having the same image in W are isomorphic. The same is also true under H2 if it is assumed further that $\bar{H}$ is a group basis of $R\bar{G}$.*

Proof. Given the group basis H, $H \cap (1 + \Delta A)$ is an abelian, normal subgroup A', of H such that $\Delta A' = \Delta A$. This shows that there is no loss of generality in assuming that the group basis is G (for the first assertion) and that one of the group bases is G (for the second assertion). Since the kernel of $\alpha : U(RG) \to W$ is contained in $1 + \Delta A \Delta G$ and since, by *Lemma* 2, $G \cap (1 + \Delta A \Delta G) = \{1\}$, the first assertion follows.

Assume now that $G \equiv H (\mathrm{mod}\ 1 + \Delta A \Delta G)$ (multiplicative congruence). Then, for each g in G there is exactly one h in H which is additively con-

gruent to g modulo $\Delta A \Delta G$. This defines a bijection $g \to h$ which is an isomorphism.

Q.E.D.

Remark. By one of the basic isomorphism theorems, each subgroup of W containing T is determined by its image in $R\bar{G}$, and this is a one-to-one correspondence.

Hence, by *Prop.* 3, each group basis of $\mathbb{Z}G$ is determined, up to isomorphism, by its image in $\mathbb{Z}\bar{G}$ (which, of course, is again a group basis of this group ring). These facts suggest the following questions:

Q1. To determine all groups H in W which contain T and map onto group bases of $R\bar{G}$.
Q2. To classify those groups H of Q1 into isomorphism classes.
Q3. To determine the groups H of Q1 which correspond to group bases of RG.

Prop. 4 below gives a fairly satisfactory answer to Q1, while Prop. 5 is a partial answer to Q2.

Corollary. *If, under the assumptions of Prop.* 3, *G and H are group bases of RG such that $\bar{G}, \bar{H}$, are conjugated by a unit of $R\bar{G}$, then G is isomorphic to H.*

In order to state *Prop.* 4, G is presented by a short exact sequence.

$$1 \to A \to G \to \bar{G} \to 1$$

where the action of $\bar{G}$ on A is denoted by $g : a \to a^g$ (with g in $\bar{G}$ and a in A). This action makes A into an $R\bar{G}$-module. The extension G is determined by a factor system

$$f : \bar{G} \times \bar{G} \to A$$

which is associated to a choice of representatives, $\sigma(g)$, of the g in $\bar{G}$:

$$\sigma(g)\sigma(g_1) = f(g, g_1)\sigma(gg_1).$$

For the sake of simplicity, G will be identified with its natural image in W, so that A is identified with T.

An augmented automorphism, ω, of $R\bar{G}$ is represented by its matrix with respect to the basis $\bar{G}$:

$$\omega : g \to \Sigma\, \omega_{g,t} t. \qquad (t \text{ in } \bar{G})$$

The image $\omega(\bar{G})$ will be denoted by $\bar{H}$, and its representative in W (see Remark above) by H. Then H, as well as G, is an extension:

$$1 \to T \to H \to \bar{H} \to 1.$$

This extension is determined by choosing a set of representatives, $\tau(h)$, of the elements of $\bar{H}$ and giving the action of $\tau(h)$ on T and the factor system f' defined by:

$$\tau(h)\tau(h_1) = f'(h, h_1)\tau(hh_1).$$

In what follows these representatives are fixed as follows:

$$\tau(\omega(g)) = \Sigma\, \omega_{g,t}\sigma(t). \qquad (t \text{ in } \bar{G}).$$

WARNING. The sums or products which appear below are assumed to be extended to all letters which appear twice in the formula, these letters varying over $\bar{G}$.

Proposition 4. *Let G be a finite group. Assume either H1 or H2 and use the notations explained above. To each augmented automorphism ω of $R\bar{G}$ there is a unique subgroup H of W, containing T, mapping onto $\omega(\bar{G})$. It is an extension*

$$1 \to T \to H \to \bar{H} \to 1$$

where each $\omega(g)$ in $\bar{H}$ operates on $T(\cong A)$ thus:

$$\omega(g) : a \to \Pi a^{\omega_{g,t} t}$$

and the factor system f' is given by

$$f'(\omega(g), \omega(g_1)) = \Pi f(t, t_1)^{\omega_{g,t}\, \omega_{g_1,t_1}}.$$

Proof. It is only a straight forward computation. (The letter g_2 stands here for gg_1.)

$$\begin{aligned} f'(\omega(g), \omega(g_1)) &= \tau(\omega(g))\tau(\omega(g_1))\tau(\omega(g_2))^{-1} = \\ &= \Sigma\, \omega_{g,t}\sigma(t)\omega_{g_1,t_1}\sigma(t_1)\tau(\omega(g_2))^{-1} = \\ &= \Sigma\, \omega_{g,t}\omega_{g_1,t_1} f(t, t_1)\sigma(tt_1)\tau(\omega(g_2))^{-1} = \\ &= \Sigma\, \omega_{g,t}\omega_{g_1,t_1}\sigma(tt_1)\tau(\omega(g_2))^{-1} + \\ &+ \Sigma\, \omega_{g,t}\omega_{g_1,t_1}(f(t, t_1) - 1)\sigma(tt_1)\tau(\omega(g_2))^{-1}. \end{aligned}$$

Since ω is an automorphism, the first sum is equal to 1. Since $f(t, t_1) - 1$ is in $\Delta A / \Delta A \Delta G)$, and since normalized units operate trivially on the right on this submodule (see Remark 1, after Lemma 2), the following equality is proved:

$$f'(\omega(g), \omega(g_1)) = \Sigma\, \omega_{g,t}\omega_{g_1,t_1} f(t, t_1).$$

This is an equality in X. After translation to the multiplicative notation of T(or A) it becomes the formula of the proposition.

Q.E.D.

Corollary. *If, furthermore, G is a split extension of A, then the same is true for every group basis H such that $\bar{H}$ is isomorphic to $\bar{G}$.*

Remark. In recent works of Gruenberg and Roggenkamp (see [2]), a great deal of attention has been paid to the second of the exact sequences of Lemma 2 instead of the first one. As a matter of fact, their results demonstrate very clearly the advantages of this second exact sequence.

It seems to be pertinent to show how one can replace the module X in the results above by the $R\bar{G}$-module $Y = \Delta G/(\Delta A \Delta G)$. This is very easily done because there is a natural way of representing any normalized unit in Y. In fact, every element of augmentation 1 is naturally represented in Y via the application $x \to x - 1$. In this way, a group basis H is represented by a set $\hat{H}$ contained in Y.

It is interesting that as H is represented in X via a pull-back construction:

$$\begin{array}{ccccccccc} 1 & \to & \mathrm{T} & \to & \mathrm{S} & \to & 1 + \Delta\bar{G} & \to & 1 \\ & & \uparrow & & \uparrow & & & & \\ & & \mathrm{H} & \to & \bar{H}, & & & & \end{array}$$

$\hat{H}$ too is obtained via a pull-back, as illustrated in the following diagram:

$$\begin{array}{ccccccccc} 1 & \to & A & \to & Y & \to & \Delta\bar{G} & \to & 0 \\ & & \uparrow & & \uparrow & & & & \\ & & \hat{H} & \to & \bar{H} & \to & 1, & & \end{array}$$

where the embedding on the right is, obviously, $h \to h - 1$, Hence, there is again a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 1 & \to & A & \to & Y & \to & \Delta\bar{G} & \to & 0 \\ & & \| & & \uparrow & & \uparrow & & \\ 1 & \to & A & \to & H & \to & \bar{H} & \to & 1. \end{array}$$

Also, the multiplication on $\hat{H}$ which corresponds to the multiplication on H may be computed directly, and it is found that it is given by the following "circle" operation:

$$x \circ y = x + \overline{x + 1}\, y. \qquad (x, y \text{ in } \hat{H})$$

In order to state Prop. 5, observe that each automorphism ω of $R\bar{G}$ defines a new $R\bar{G}$-module structure on Y. It is obtained in the usual way by saying that the new action of a g of $\bar{G}$ is given by $y \to \omega(g)y$ (for y in Y). This module structure will be denoted by Y_ω.

Proposition 5. *Let G be a finite group. Assume either $H1$ or $H2$.*

(i) *Each isomorphisms $\psi : G \to H$ between group bases of RG leaving ΔA invariant induces an isomorphism $\bar{\psi} : \bar{G} \to \bar{H}$ such that the $\bar{G}$-modules Y and $Y_{\bar{\psi}}$ are isomorphic.*

(ii) *If ω is an augmented automorphism of $R\bar{G}$ such that there is a $\bar{G}$-isomorphism $\psi : Y \to Y_\omega$ verifying $\bar{\psi} = \omega$, then the group H, which corresponds to $\omega(\bar{G})$ in W according to* Prop. 4, *is isomorphic to G.*

Proof.

(i) ψ defines an automorphism of RG which induces an additive permutation of Y which is still denoted by ψ. It verifies:

$$\psi(\bar{g}_1(g_2 - 1)) = \psi(g_1(g_2 - 1)) = \psi(g_1)\psi(g_2 - 1) = \\ = \bar{\psi}(\bar{g}_1)\psi(g_2 - 1). \qquad (g_1, g_2 \text{ in } G)$$

This means that $\psi : Y \to Y_{\bar{\psi}}$ is a $\bar{G}$-isomorphism.

(ii) Since $\overline{\psi(G - 1)} = \bar{\psi}(\bar{G}) - 1 = \omega(\bar{G}) - 1$, it is clear that $\psi(\hat{G}) = \hat{H}$. On the other hand, ψ is multiplicative because:

$$\psi(g_1 - 1 + \bar{g}_1(g_2 - 1)) = \psi(g_1 - 1) + \bar{\psi}(\bar{g}_1)\psi(g_2 - 1).$$

Q.E.D.

References

[1] Berman, S. D., *On the equation $X^m = 1$ in an integral group ring*, Ukrainsk. Matem. 2h. 7 (1955) 253-261.

[2] Gruenberg, K. W., *Relation Modules of finite groups*, C. B. M. S. N.º 25 (1976).

[3] Polcino Milies, C., *Anéis de grupos*, IV Escola de Algebra, São Paulo (1976).

[4] Sehgal, S. K., *On the isomorphism of integral group rings, II*, Canad. J. Math. XXI (1969) 1182-1188.

[5] Zaleskii, A. E. and Mikhalev, A. V., *Group rings*, J. Soviet. Math. 4 (1975) 1-78.

Instituto de Matemática e Estatística
Universidade de São Paulo
05508 São Paulo, SP, Brasil