INTEGRAL GROUP RINGS OF FINITE GROUPS

B. Banaschewski

(received March 15, 1967)

Introduction. The main object of this paper is to show that the existence of a particular kind of isomorphism between the integral group rings of two finite groups implies that the groups themselves are isomorphic. The proof employs certain types of linear forms which are first discussed in general. These linear forms are in some way related to the bilinear forms used by Weidmann [3] in showing that groups with isomorphic character rings have the same character table, and a shorter and, in a sense, more natural proof of this result is included here as another application of these linear forms.

1. Linear forms on an algebra. Let R be a commutative ring with unit 1, A an associative algebra over R with unit e, and $A^* = \mathrm{Hom}_R(A, R)$ the R-dual of A as R-module with the usual A-module structure given by the definition $(a\varphi)(x) = \varphi(xa)$ for $a \in A$, $\varphi \in A^*$, and $x \in A$. We shall call a linear form $\lambda \in A^*$ regular if $\{\lambda\}$ is an A-basis for A^* and central if $\lambda(xy) = \lambda(yx)$ for all $x, y \in A$.

LEMMA 1. *If $\lambda, \nu \in A^*$ are regular then $\nu = a\lambda$ where $a \in A$ is invertible; moreover, if λ and ν are also central then a belongs to the centre of A.*

Proof. One has $\nu = a\lambda$ for suitable $a \in A$ since $A^* = A\lambda$; then, also, $A^* = A\nu = Aa\lambda$, and thus $\lambda = a'a\lambda$ for suitable $a' \in A$ which implies $e = a'a$, i.e. a has a left inverse. By the same reasoning for $\lambda = a'\nu$ one obtains a left inverse a'' for a', and it follows that $a'' = a$; hence a is invertible. Now assume further that λ and ν are central; for ν this means $\lambda(xya) = \lambda(yxa)$ for all $x, y \in A$, and the centrality of λ implies that $\lambda(yxa) = \lambda(xay)$; from this one obtains that $(ya - ay)\lambda = 0$ and thus $ya = ay$ for all $y \in A$.

Canad. Math. Bull. vol. 10, no. 5, 1967

LEMMA 2. If A has a finite basis $\{x_i\}$ and $\lambda \in A^*$ is such that $\det(\lambda(x_i x_k))$ is invertible in R then λ is regular.

Proof. From $a\lambda = 0$ it follows that $\Sigma c_k \lambda(x_i x_k) = 0$ where $a = \Sigma c_k x_k$, and this implies $c_k = 0$ for all k, i.e. $a = 0$. Secondly, for any $\nu \in A^*$, the equations $\nu(x_i) = \Sigma c_k \lambda(x_i x_k)$ can be solved for c_k in R, and for $a = \Sigma c_k x_k$ one then has $\nu = a\lambda$.

Let now $R = Z$, and assume for the algebra A that A is finitely generated over Z and $A_C = C \otimes_Z A$ is Artinian semi-simple. Each $\lambda \in A^*$ has a unique C-linear extension $\tilde{\lambda} : A_C \to C$, and if a relation $\nu = a\lambda$ holds for $\lambda, \nu \in A^*$ and some $a \in A$ then also $\tilde{\nu} = a\tilde{\lambda}$. A linear form $\lambda \in A^*$ will be called normal if it is regular, central and its extension $\tilde{\lambda}$ has positive rational values for the primitive central idempotents of A_C.

LEMMA 3. There exists at most one normal $\lambda \in A^*$.

Proof. Let $u_1, \ldots, u_n$ be the primitive central idempotents of A_C, and ν and λ normal linear forms on A. Then $\nu = a\lambda$ with an invertible central element $a \in A$, and $a = \Sigma c_k u_k$ with complex coefficients c_k, clearly all non-zero.

Now, for each i, the correspondence $x \rightsquigarrow xu_i$ determines a homomorphism from the centre of A into C, and since A is finitely generated as Z-module the same holds for the image of its centre under this homomorphism. Thus $x \rightsquigarrow xu_i$ maps the centre of A into the ring of algebraic integers, and therefore the coefficients c_k of a as well as their inverses are algebraic integers, the latter since $a^{-1} = \Sigma c_k^{-1} u_k$. From $\nu(u_i) = \lambda(u_i a) = \lambda(c_i u_i) = c_i \lambda(u_i)$ and the given hypothesis on λ and ν it further follows that the c_i are positive rational, hence all $c_i = 1$, $a = e$, and thus $\nu = \lambda$.

https://doi.org/10.4153/CMB-1967-061-0 Published online by Cambridge University Press

COROLLARY. If A and B are two rings as above, with normal linear forms λ and ν respectively, and $\phi: A \to B$ is an isomorhpism then $\lambda = \nu \circ \phi$.

Proof. Consider the linear form $\mu = \nu \circ \phi$ on A. It is clearly central, and from $a\mu = (\phi(a)\nu) \circ \phi$ one readily obtains that it is regular. Now, if $u_1, \ldots, u_n$ are the primitive central idempotents of A_C and $\tilde{\phi}: A_C \to B_C$ is the C-linear extension of ϕ then $\tilde{\phi}(u_1), \ldots, \tilde{\phi}(u_n)$ are the primitive central idempotents of B_C, and hence $\tilde{\mu}(u_i) = \tilde{\nu}(\tilde{\phi}(u_i))$ is positive rational. This shows μ is normal, and thus $\lambda = \mu = \nu \circ \phi$.

It might be added that the above considerations still hold if Z is replaced by an arbitrary subring of C which is finitely generated as Z-module.

2. Integral group rings. On the integral group ring Z[G] of a finite group G one has the linear form λ defined by $\lambda(\Sigma h_s s) = h_e$ where e is now the unit of G. Since G is a basis of Z[G] and

$$\lambda(st) = \begin{cases} 1 & \text{if } s = t^{-1} \\ 0 & \text{if } s \neq t^{-1} \end{cases}$$

λ is regular. Also, for $x = \Sigma g_s s$ and $y = \Sigma h_s s$ one has $\lambda(xy) = \Sigma_s g_s h_{s^{-1}} = \Sigma_s h_s g_{s^{-1}} = \lambda(yx)$, i.e. λ is central. Finally, the primitive central idempotents of $C \otimes_Z [G] = C[G]$ are of the form [1]

$$u = \frac{d}{g} \sum_{s \in G} \chi(s^{-1}) s$$

where χ is an irreducible C-character of G and d the C-dimension of the representation module associated with χ. Therefore, $\lambda(u) = (d/g)\chi(e) = d^2/g$ which is positive rational. Thus λ is normal.

https://doi.org/10.4153/CMB-1967-061-0 Published online by Cambridge University Press

On $Z[G]$ one has a particular involution J determined by $J(s) = s^{-1}$ for $s \in G$, and G is a basis of $Z[G]$ which is orthonormal in the sense that

$$\lambda(sJ(t)) = \begin{cases} 1 & \text{if } s = t \\ 0 & \text{if } s \neq t \end{cases}$$

This condition plays the following interesting role:

LEMMA 4. *For any orthonormal basis B of $Z[G]$ which is closed with respect to multiplication there exists a homomorphism $\eta : G \to \{1, -1\}$ such that $B = \{\eta(s)s \mid s \in G\}$.*

Proof. It is immediate that any orthonormal basis of $Z[G]$ is of the type $\{\eta(s)s \mid s \in G\}$ where $\eta(s) = \pm 1$. Closure with respect to multiplication then means that for any $s, t \in G$ there exists an $x \in G$ for which $\eta(s)s\eta(t)t = \eta(x)x$, but this implies that $x = st$ and hence $\eta(s)\eta(t) = \eta(x) = \eta(st)$, which shows that $\eta : G \to Z$ is a homomorphism.

We are now ready to obtain our main result.

PROPOSITION 1. *Let G and H be two finite groups and $\phi : Z[G] \to Z[H]$ an involution preserving isomorphism, i.e. $\phi \circ J = I \circ \phi$ for the involutions J and I of $Z[G]$ and $Z[H]$ respectively. Then, there exists an isomorphism $\varphi : G \to H$ and a homomorphism $\eta : G \to \{1, -1\}$ such that $\phi(s) = \eta(s)\varphi(s)$ for all $s \in G$.*

Proof. $\phi(G)$ is clearly a multiplicatively closed Z-basis of $Z[H]$. Now, if λ and μ are the normal linear forms on $Z[G]$ and $Z[H]$ respectively then

$$\mu(\phi(s)\, I(\phi(t))) = \mu(\phi(s)\phi(J(t))) =$$

$$(\mu \circ \phi)\ (sJ(t)) = \lambda(sJ(t)),$$

and hence $\phi(G)$ is an orthonormal basis of $Z[H]$. It follows from Lemma 4 that there exists a homomorphism $\varepsilon : H \to \{1, -1\}$ such that $\phi(G) = \{\varepsilon(s)s \mid s \in H\}$. Now, the desired isomorphism φ is the inverse of the isomorphism $H \to G$ given by $s \to \phi^{-1}(\varepsilon(s)s)$, and η is given by $\eta(s) = \varepsilon(\varphi(s))$, $s \in G$.

https://doi.org/10.4153/CMB-1967-061-0 Published online by Cambridge University Press

We do not know whether all isomorphisms between integral group rings are involution preserving, or whether the existence of an isomorphism $\phi: Z[G] \to Z[H]$ at least implies the existence of an involution preserving isomorphism $\psi: Z[G] \to Z[H]$ - questions obviously related, in the light of the above proposition, to the unsolved problem whether groups with isomorphic integral group rings must be isomorphic.

The case in which this is known to be so, i.e. for abelian groups, is a simple consequence of Proposition 1; in fact, one has the following, more detailed version of the original result of Higman's [2]:

COROLLARY: Let $\phi: Z[G] \to Z[H]$ be an isomorphism where G and H are finite abelian groups. Then there exists an isomorphism $\varphi: G \to H$ and a homomorphism $\eta: G \to \{1, -1\}$ such that $\phi(s) = \eta(s)\varphi(s)$ for all $s \in G$.

Proof. It clearly suffices to show that ϕ is involution preserving. For this one observes first that the extension $\tilde{J}: C[G] \to C[G]$ of J given by $\tilde{J}(cx) = \bar{c}\, J(x)$ for $c \in C$, $x \in Z[G]$, leaves the primitive central idempotents

$$u = \frac{d}{g} \sum_s \chi(s^{-1})s$$

of $C[G]$ fixed, and that for abelian G this property completely characterizes J. It follows from this that the involution $\phi^{-1} \circ I \circ \phi$ of $Z[G]$, I the "natural" involution of $Z[H]$, is equal to J since it clearly has the same property. This, then, proves that $\phi \circ J = I \circ \phi$.

3. Character rings and character tables. In this section we present an alternative, more algebraic approach to the result of Weidman [3] which is closely parallel to the above discussion of group rings.

The character ring $\mathcal{C}(G)$ of a finite group G, i.e. the ring of complex-valued functions on G generated by the C-characters of G, has the irreducible C-characters $\chi_1, \ldots, \chi_n$ as a basis, and has the further property that $C \otimes_Z \mathcal{C}(G)$ is isomorphic to the ring of all complex-valued functions on G which are constant on the conjugacy classes and hence is

https://doi.org/10.4153/CMB-1967-061-0 Published online by Cambridge University Press

semi-simple. Identifying $C \otimes_Z \mathcal{C}(G)$ with the latter, the functions of the type

$$\eta = \frac{k}{g} \sum_i \overline{\chi_i(s)}\, \chi_i ,$$

k the number of elements in the conjugacy class of s and g the order of G, are the primitive (central) idempotents.

Now, on $\mathcal{C}(G)$ one has the linear form $\lambda : \mathcal{C}(G) \to Z$ defined by

$$\lambda(\varphi) = \frac{1}{g} \sum_{s \in G} \varphi(s).$$

λ is, of course, central, and the orthogonality relations for the characters χ_i show that λ is regular. Finally, for an idempotent η as given above one has $\tilde{\lambda}(\eta) = k/g$, and thus λ is normal.

In addition, one also has an involution J on $\mathcal{C}(G)$, given by taking the usual complex conjugate $\bar{\varphi}$ for $\varphi \in \mathcal{C}(G)$. The extension $\tilde{J}$ of J to $C \otimes_Z \mathcal{C}(G)$ defined by $\tilde{J}(c\varphi) = \bar{c}\, J(\varphi)$, $c \in C$ and $\varphi \in \mathcal{C}(G)$, clearly leaves the primitive idempotents of $C \otimes_Z \mathcal{C}(G)$ fixed, and the χ_i are orthonormal in the sense that $\lambda(\chi_i J(\chi_k)) = \delta_{ik}$. Moreover, the set $\{\chi_i\}$ has the property that its additive closure is multiplicatively closed since $\chi_i \chi_k = \sum m_{ikl} \chi_l$ with natural numbers m_{ikl}. This is almost a characterizing property for $\{\chi_i\}$.

LEMMA 5. *For any orthonormal basis $\{\varphi_i\}$ of $\mathcal{C}(G)$ whose additive closure is multiplicatively closed there exists an automorphism θ of $\mathcal{C}(G)$ such that $\{\theta(\chi_i)\} = \{\varphi_i\}$.*

Proof. Again, one has $\varphi_i = \varepsilon_i \chi_i$, with $\varepsilon_i = \pm 1$, after suitable rearrangement of the φ_i, and hence $\varphi_i \varphi_k = \varepsilon_i \varepsilon_k \chi_i \chi_k = \varepsilon_i \varepsilon_k \sum m_{ikl} \chi_l = \sum \varepsilon_i \varepsilon_k m_{ikl} \varepsilon_l \varphi_l$. On the other hand, $\varphi_i \varphi_k = \sum n_{ikl} \varphi_l$ with natural numbers n_{ikl}, and hence

https://doi.org/10.4153/CMB-1967-061-0 Published online by Cambridge University Press

$\varepsilon_i \varepsilon_k m_{ikl} \varepsilon_l = n_{ikl}$. This implies $m_{ikl} = n_{ikl}$, and therefore the multiplication tables for the χ_i and for the φ_i are the same; the mapping $\chi_i \rightsquigarrow \varphi_i$ now extends to the desired automorphism θ of $\mathfrak{C}(G)$.

The character tables of the group G are the matrices (x_{ik}) for which $x_{ik} = \chi_i(s_k)$ where the χ_i run over the different irreducible C-characters of G and the s_k over a set of representatives for the conjugacy classes of G. Any two such matrices clearly differ only by permutations of the rows and columns and are therefore elementarily equivalent.

Now we have, as in [3]:

PROPOSITION 2. Two finite groups which have isomorphic character rings have the same character tables.

Proof. Let G and H be the groups, $\phi: \mathfrak{C}(G) \to \mathfrak{C}(H)$ an isomorphism, λ and ν the normal linear forms and J and I the usual involutions on $\mathfrak{C}(G)$ and $\mathfrak{C}(H)$ respectively. Then one obtains, exactly as in the proof of Proposition 1 and its corollary that

$$\lambda(\chi_i J(\chi_k)) = \nu(\phi(\chi_i)\, I(\phi(\chi_k)))$$

for the irreducible characters χ_i of G, i.e. $\{\phi(\chi_i)\}$ is an orthonormal basis of $\mathfrak{C}(H)$. Since the additive closure of $\{\chi_i\}$ is multiplicatively closed the same holds for $\{\phi(\chi_i)\}$, and thus by Lemma 5 there exists an automorphism θ of $\mathfrak{C}(H)$ such that $\theta(\zeta_i) = \phi(\chi_i)$, $\zeta_1, \ldots, \zeta_n$ the irreducible C-characters of H in suitable arrangement. Now, let $\psi = \theta^{-1} \circ \phi$ and $\tilde{\psi}$ its C-linear extension; for the latter one has $\tilde{\psi}(\chi_i \eta_k) = \zeta_i \tilde{\psi}(\eta_k)$, η_k the primitive idempotents of $C \otimes_Z \mathfrak{C}(G)$, and putting $\chi_i \eta_k = x_{ik} \eta_k$ with $x_{ik} \in C$ one has $x_{ik} \tilde{\psi}(\eta_k) = \zeta_i \tilde{\psi}(\eta_k) = y_{ik} \tilde{\psi}(\eta_k)$. Here (y_{ik}) is a character table of H since $\{\tilde{\psi}(\eta_k)\}$ is the set of primitive idempotents of $C \otimes_Z \mathfrak{C}(H)$, and the matrix identity $(x_{ik}) = (y_{ik})$ then proves the assertion.

https://doi.org/10.4153/CMB-1967-061-0 Published online by Cambridge University Press

REFERENCES

1. C. W. Curtis and I. Reiner, Representation theory of finite groups and associative algebras. Interscience Publishers, New York, 1962.

2. G. Higman, The units of group rings. Proc. London Math. Soc. 46 (1940), 231-248.

3. D. R. Weidman, The character ring of a finite group. Ill. J. Math. 9 (1965), 462-467.

Tulane University
New Orleans and
McMaster University
Hamilton, Ontario