BULL. AUSTRAL. MATH. SOC. MOS 2080

VOL. 1 (1969), 245-261.

On the group ring of a finite abelian group

Raymond G. Ayoub and Christine Ayoub

The group ring of a finite abelian group G over the field of rational numbers Q and over the rational integers Z is studied. A new proof of the fact that the group ring QG is a direct sum of cyclotomic fields is given - without use of the Maschke and Wedderburn theorems; it is shown that the projections of QG onto these fields are determined by the inequivalent characters of G. It is proved that the group of units of ZG is a direct product of a finite group and a free abelian group F and the rank of F is determined. A formula for the orthogonal idempotents of QG is found.

Introduction

In this paper we study the group ring of a finite abelian group G over the field Q of rational numbers and over the (rational) integers Z. We give a new proof of the well-known fact that the group ring QG is a direct sum of cyclotomic fields [G. Higman] which enables us to say which fields arise and with what multiplicity (see also [5]). We show that the projections of QG onto these fields are determined by the inequivalent characters of G. This proof is to our mind conceptually much simpler than the one using representation theory. Granted an acquaintance with the elementary properties of tensor products (of commutative algebras) all that is needed is developed in the paper itself.

In §3 we consider the group U of units of ZG; we find that U is the direct product of a finite group and a free abelian group F of finite rank - a fact already established by Higman (cf. [4]) - but our results

Received 21 March 1969. Received by J. Austral. Math. Soc. 17 September 1968. Revised 17 December 1968. Communicated by G.B. Preston. This research was done under NSF Contract GP-5593.

enable us to calculate the rank of the group F (Theorem 4). Theorem 5 gives a formula for the orthogonal idempotents of QG. Finally in the last paragraph we study the embedding of ZG in the direct sum of cyclotomic fields, in the case when G is cyclic of prime power order.

Definitions and notations

We list the notations which will be used throughout the paper. Some of these are standard, while others are our own invention - most of the latter will be explained in the body of the paper but are listed here for the convenience of the reader.

$\oplus$ is used for the direct sum of rings.

If X_i are rings and if $x_i \in X_i$ (for $i \in I$), we write $\bigoplus_{i\in I} x_i$ for the element of $\bigoplus_{i\in I} X_i$ whose i-th component is x_i.

$\otimes$ denotes the tensor product over the rational field.

If R is a ring, we write mR for $R \oplus \ldots \oplus R$ (m terms) and R^m for $R \otimes \ldots \otimes R$ (m terms).

Q is the field of rational numbers.

ζ_d denotes a primitive (complex) d-th root of unity. $\Phi_d(x)$ denotes the cyclotomic polynomial satisfied by the primitive d-th roots of unity over the rationals.

Q_d is the splitting field of $\Phi_d(x)$, so that Q_d is obtained from Q by adjunction of ζ_d.

$F[x]$ denotes the ring of the polynomials in x over the field F and $F(\alpha)$ the field obtained by adjunction of α to F.

If $f(x) \in F[x]$, deg $(f(x))$ = degree of $f(x)$, $(f(x))$ = ideal generated by $f(x)$.

The exponent of a finite group G is the least positive integer m such that $g^m = 1$ for all $g \in G$. (a) is the cyclic group generated by a, and $o(a)$ = order of a.

$\times$ denotes the direct product of multiplicative groups.

https://doi.org/10.1017/S0004972700041496 Published online by Cambridge University Press

We write our mappings on the left so that $\alpha \circ \beta$ denotes the mapping β followed by the mapping α.

For the homomorphism η, $\mathrm{Ker}(\eta)$ = kernel of η and $(\eta|G)$ = restriction of η to G (G a group).

N and Z denote the natural numbers and integers, respectively.

Z_d denotes the polynomials in ζ_d over Z.

$\mathrm{Mod}_Z\{S\}$ = module generated by S over Z.

QG and ZG are the group rings of G over Q and Z, respectively.

Actually only finite abelian groups are considered - but this is explicitly stated in the theorems.

1. The structure of QG

DEFINITION 1. If ζ_d is a (complex) primitive d-th root of unity, $Q_d = Q(\zeta_d)$. We note that Q_d does not depend on the particular d-th root of unity chosen.

PROPOSITION 1. *Let G be a cyclic group of order n, and Q the field of rational numbers. Then*

$$QG \simeq \bigoplus_{d|n} Q_d . \tag{1}$$

Proof. Let $\Phi_d(x)$ be the cyclotomic polynomial satisfied by the primitive d-th roots of unity over Q. Then

$$QG \simeq Q[x] \Big/ (x^n - 1) \simeq \bigoplus_{d|n} Q[x] \Big/ (\Phi_d(x)) .$$

But $Q[x] \Big/ (\Phi_d(x)) \simeq Q(\zeta_d) = Q_d$. Hence (1) $QG \simeq \bigoplus_{d|n} Q_d$.

Note. If G is generated by a, then under the isomorphism (1),

$$a^i \leftrightarrow \bigoplus_{d|n} \zeta_d^i \in \bigoplus_{d|n} Q_d . \tag{2}$$

https://doi.org/10.1017/S0004972700041496 Published online by Cambridge University Press

PROPOSITION 2. *If the groups* A_i $(1 \leq i \leq k)$ *are subgroups of the group* G *such that* $G = A_1 \times \ldots \times A_k$ *(direct product) then*

$$QG \simeq QA_1 \otimes \ldots \otimes QA_k \quad \text{(tensor product over } Q\text{)} . \tag{3}$$

Note. If Z denotes the integers then we also have $ZG \simeq ZA_1 \otimes \ldots \otimes ZA_k$. The proof follows in the same way.

Proof. If $g = a_1 \ldots a_k$, where $a_i \in A_i$ $(1 \leq i \leq k)$, map g onto $a_1 \otimes \ldots \otimes a_k \in QA_1 \otimes \ldots \otimes QA_k$. This mapping sends a basis for QG onto a basis for $QA_1 \otimes \ldots \otimes QA_k$ and hence we can extend it to an isomorphism.

PROPOSITION 3. $Q_k \otimes Q_l \simeq$ *direct sum of* $\phi(d)$ *copies of* $Q_m = \phi(d)\, Q_m$, *where* $d = \text{g.c.d.}(k,l)$, $m = \text{l.c.m.}(k,l)$ *and* ϕ *denotes the Euler* ϕ*-function.*

Proof. Let $m = ks = lt$, where $(s,t) = 1$. Then ζ_m^s and ζ_m^t are clearly primitive k-th and l-th roots of unity respectively. Thus the field $Q(\zeta_k, \zeta_l)$, obtained by adjoining to Q primitive k-th and l-th roots of unity, is contained in Q_m ; on the other hand, if we choose u and v such that $us + vt = 1$, then $\zeta_m = (\zeta_m^s)^u (\zeta_m^t)^v$ and hence ζ_m is in the field $Q(\zeta_k, \zeta_l) = Q_k(\zeta_l)$. Therefore, we have shown that

$$Q_m = Q_k(\zeta_l) . \tag{4}$$

Now let

$$\Phi_l(x) = f_1(x) \ldots f_s(x) \tag{5}$$

be the decomposition of the cyclotomic polynomial into irreducible factors in $Q_k[x]$. Since by (4) Q_m is obtained from Q_k by adjoining any root of $\Phi_l(x)$ (and therefore, any root of any $f_i(x)$) $Q_m \simeq Q_k[x] \Big/ (f_i(x))$ $(1 \leq i \leq s)$. Thus each $f_i(x)$ has degree

https://doi.org/10.1017/S0004972700041496 Published online by Cambridge University Press

$$[Q_m:Q_k] = \frac{[Q_m:Q]}{[Q_k:Q]} = \frac{\phi(m)}{\phi(k)} = \frac{\phi(l)}{\phi(d)} ,$$

since $\phi(k)\ \phi(l) = \phi(m)\ \phi(d)$. Also

$$\phi(l) = \deg\ (\Phi_l(x)) = s[\deg\ (f_i(x))] = s\frac{\phi(l)}{\phi(d)}$$

so that

$$s = \phi(d) . \tag{6}$$

From a known theorem we have that $Q_k \otimes Q_l \simeq Q_k[x] \Big/ (\Phi_l(x))$, and from the decomposition (5) and (6) this is isomorphic to $\overset{\phi(d)}{\underset{i=1}{\oplus}} Q_k[x] \Big/ (f_k(x)) \simeq \phi(d)\ Q_m$, since $Q_k[x] \Big/ (f_i(x)) \simeq Q_m$ for $1 \leq i \leq \phi(d)$.

Note. Applying Proposition 3 several times we could establish that for positive integers $k_1,\ldots,k_r$

$$Q_{k_1} \otimes \ldots \otimes Q_{k_r} \simeq s\ Q_m ,$$

where $m = \text{l.c.m.}(k_1,\ldots,k_r)$ and s is a positive integer (which we could calculate). In particular, if $\text{g.c.d.}(k_i,k_j) = 1$ for $i \neq j$,

$$Q_{k_1} \otimes \ldots \otimes Q_{k_r} = Q_m \quad (\text{i.e. } s = 1) . \tag{7}$$

THEOREM 1. *If G is a finite abelian group of exponent m , there exist integers $u_d \geq 0$ such that*

$$QG \simeq \underset{d|m}{\oplus} u_d\ Q_d . \tag{8}$$

Proof. Let $G = A_1 \times \ldots \times A_k$, where A_i is cyclic of order d_i for $1 \leq i \leq k$ and $d_1 \mid d_2 \mid \ldots \mid d_k = m$. Then by Proposition 2, $QG \simeq QA_1 \otimes \ldots \otimes QA_k$ and hence by Proposition 1, $QG \simeq \underset{d|d_1}{\oplus} Q_d \otimes \ldots \otimes \underset{d|d_k}{\oplus} Q_d$. Now if we expand using the distributive law and the note after Proposition 3, we see that QG is the direct sum of

https://doi.org/10.1017/S0004972700041496 Published online by Cambridge University Press

cyclotomic fields Q_d, where each d divides m.

2. The projections of QG

DEFINITION 2. Let G be a finite abelian group. The characters χ and ψ are equivalent if $\mathrm{Ker}(\chi) = \mathrm{Ker}(\psi)$.

LEMMA 1. *Let G be a finite abelian group of order n and exponent m; let d divide m and let t_d be the number of cyclic subgroups of G of order d. Then*

(1) The number of inequivalent characters χ such that $\chi(G) = (\zeta_d)$ is t_d.

(2) If $\chi(G) = (\zeta_d)$, the number of characters equivalent to χ is $\phi(d)$.

(3) $\sum_{d \mid m} t_d \, \phi(d) = n$.

Proof. *(1)* Let D be a subgroup of G such that G/D is cyclic of order d, and let ζ_d be a primitive d-th root of unity. Then there exists an epimorphism from G to (ζ_d) with kernel D - i.e. a character with kernel D. Therefore, the number of inequivalent characters χ such that $\chi(G) = (\zeta_d)$ is equal to the number of subgroups D such that G/D is cyclic of order d and this is equal to the number of cyclic subgroups of order d.

(2) Let χ be a character with $\chi(G) = (\zeta_d)$ and $D = \mathrm{Ker}(\chi)$. Then for α in the automorphism group of (ζ_d) $\psi_\alpha = \alpha \circ \chi$ is a character of G with kernel D - i.e. ψ_α is equivalent to χ - and distinct automorphisms α give rise to distinct characters ψ_α. Furthermore, any character ψ of G which is equivalent to χ is of this form, since the mapping α defined by $\alpha(\chi(g)) = \psi(g)$ for $g \in G$ is an automorphism of (ζ_d). But the automorphism group of (ζ_d) has order $\phi(d)$. Thus there are $\phi(d)$ characters equivalent to χ.

(3) From (2) and (3) the total number of characters of G is

https://doi.org/10.1017/S0004972700041496 Published online by Cambridge University Press

$\sum_{d|m} t_d \phi(d)$. Hence $n = \sum_{d|m} t_d \phi(d)$, since G has n distinct characters.

COROLLARY. *If* $\chi_1,\dots,\chi_l$ *are inequivalent characters of the finite abelian group* G *of order* n *and if* $\sum_{i=1}^{l} \phi(d_i) = n$, *where* $\chi_i(G) = (\zeta_{d_i})$ *for* $1 \leq i \leq l$, *then the characters* $\chi_i (1 \leq i \leq l)$ *form a complete set of inequivalent characters of* G .

THEOREM 2. *Let* G *be a finite abelian group of exponent* m . *Then* $QG \simeq \bigoplus_{d|m} t_d Q_d$, *where* t_d *is the number of cyclic subgroups of* G *of order* d . *The projection* π *of* QG *onto the component* Q_d *defines a character* $\chi = (\pi|G)$ *of* G *onto* (ζ_d) *and the characters so defined form a complete set of inequivalent characters of* G .

Proof. From Theorem 1, we have

$$QG \simeq \bigoplus_{d|m} u_d Q_d . \tag{8}$$

It is clear that for each projection π onto a component Q_d we get a character $\chi = (\pi|G)$ of G . We show first that if π_1 and π_2 are projections onto different components then the characters $\chi = (\pi_1|G)$ and $\psi = (\pi_2|G)$ are not equivalent. For suppose to the contrary that ψ is equivalent to χ . Then if $\chi(G) = (\zeta_d)$ there is an automorphism α of (ζ_d) such that $\psi = \alpha \circ \chi$. Let $\overline{\alpha}$ be the automorphism of Q_d which takes ζ_d into $\alpha(\zeta_d)$.

Since $QG \simeq \bigoplus_{d|m} t_d Q_d$, there is an element $r \in QG$ with $\pi_1(r) = 0$ and $\pi_2(r) \neq 0$. Now $r = \sum_{g \in G} r(g)g$ with $r(g) \in Q$ and we have:

$0 = \pi_1(r) = \sum_{g \in G} r(G)\, \pi_1(g) = \sum_{g \in G} r(g)\, \chi(g)$. On the other hand,

https://doi.org/10.1017/S0004972700041496 Published online by Cambridge University Press

$$0 \neq \pi_2(r) = \sum_{g\in G} r(g) \quad \pi_2(g) = \sum_{g\in G} r(g)\,\psi(g) = \sum_{g\in G} r(g)(\alpha \circ \chi)(g)$$
$$= \overline{\alpha}\left(\sum_{g\in G} r(g)\,\chi(g) \right) = 0 .$$

This is clearly impossible so that χ and ψ cannot be equivalent.

Let $\pi_1,\ldots,\pi_l$ be the projections of QG defined by (8), and let $\chi_i = (\pi_i|G)$ for $1 \leq i \leq l$. We establish the fact that the χ_i form a complete set of inequivalent characters of G. Clearly if $\chi_i(G) = (\zeta_{d_i})$, $\pi_i(QG) = Q_{d_i}$ since G generates QG over Q. Hence $QG \simeq \bigoplus_{i=1}^{l} Q_{d_i}$ so that comparing dimensions we have: $n = \sum_{i=1}^{l} \phi(d_i)$. Hence by the Corollary to Lemma 1, the χ_i are a complete set of inequivalent characters of G. Thus also

$$QG \simeq \bigoplus_{d|m} t_d\, Q_d . \tag{9}$$

REMARK. It may happen that $Q_d = Q_{d'}$ with $d < d'$ - in fact, this is the case if, and only if, d is odd and $d' = 2d$. It can be shown that the expression (8) (obtained by use of Propositions 1-3) is the same as (9) - i.e. $u_d = t_d$. However, the proof is a little tedious and so we thought it not of sufficient interest to include.

3. The units of ZG

THEOREM 3. (G. Higman) *The only units of finite order in ZG are of the form $\pm g$ $(g \in G)$.*

Proof. Let $u \in ZG$ be a unit of finite order. Then if π is the projection of QG in the isomorphism $QG \simeq \bigoplus_{d|m} t_d\, Q_d$, $\pi(u)$ is a unit of finite order in Q_d - i.e. $\pi(u)$ is a root of unity. Thus if

$$u = \sum_{g\in G} u(g)g \quad \text{with } u(g) \in Z , \quad \pi(u) = \sum_{g\in G} u(g)\,\pi(g) = \sum_{g\in G} u(g)\,\chi(g) = \rho_\chi ,$$

where $\chi = (\pi|G)$ and ρ_χ is a root of unity. Since these characters χ form a complete set of inequivalent characters we have:

https://doi.org/10.1017/S0004972700041496 Published online by Cambridge University Press

(10) $$\sum u(g)\,\chi(g) = \rho_\chi \quad \text{for every} \quad \chi \in \hat{G}\,,$$

the character group G and where each ρ_χ is a root of unity. Using the orthogonality relations of the characters, we obtain $nu(g) = \sum_{x\in\hat{G}} \rho_\chi\,\overline{\chi(g)}$ for $g \in G$ and from this it is easy to deduce that there exists a $g_0 \in G$ such that $u(g_0) = \pm 1$ and $u(g) = 0$ for $g \neq g_0$ (cf. e.g. [1]). Thus $u = \pm g$.

THEOREM 4. *Let G be a finite abelian group of order n and let U denote the group of units of ZG . Then $U = T \times F$ with $T = \{\pm g \mid g \in G\}$ and F free abelian of rank $\frac{1}{2}(n + 1 + t_2 - 2l)$, where t_2 = number of elements of G of order 2 and l = number of cyclic subgroups of G .*

Proof. ZG is isomorphically embedded in $\oplus_{d|m} t_d Z_d$ under the isomorphism (9) (here $Z_d = Z(\zeta_d)$). Since both ZG and $\oplus_{d|m} t_d Z_d$ are free abelian of rank n , ZG is of finite index k in $\oplus_{d|m} t_d Z_d$ (identifying ZG with its image under the isomorphism). Let U denote the group of units of ZG and U_1 the group of units of $\oplus t_d Z_d$. Then U_1 is generated by the units of the components Z_d - and the unit group of each Z_d is finitely generated by Dirichlet's Unit Theorem (cf. [3] p. 124 Satz 100; we note that Z_d is the ring of integers of Q_d - cf. [6], p. 264, 7-5-4 Theorem). Now we show that U_1/U is finite. It is sufficient to show that every unit u of Z_d has finite order, mod $Z(G)$. Letting $\underline{\underline{A}}$ = principal ideal generated by k in Z_d , we have $u^{\phi(\underline{\underline{A}})} \equiv 1 \pmod{\underline{\underline{A}}}$ where $\phi(\underline{\underline{A}})$ denotes the number of reduced residue classes, mod $\underline{\underline{A}}$. Hence $u^{\phi(\underline{\underline{A}})} = 1 + \lambda k$ (cf. [3], Satz 84), where $\lambda \in Z_d$ and so $u^{\phi(\underline{\underline{A}})} \in ZG$ since $[\oplus t_d Z_d : ZG] = k$. Hence $U = T \times F$, where T is finite and F is free abelian of rank = the torsion-free rank of U_1 . In Theorem 2, we have determined T so it remains to calculate the torsion-free rank of U_1 .

By Dirichlet's Theorem if $d > 2$, Z_d has $\frac{\phi(d)}{2} - 1$ independent units

https://doi.org/10.1017/S0004972700041496 Published online by Cambridge University Press

of infinite order. Thus the torsion-free rank of U_1 is $\sum_{\substack{d|m \\ d\neq 1,\neq 2}} t_d \left(\frac{\phi(d)}{2} - 1\right)$. But $\sum_{d|m} t_d\ (d) = n$, and $\sum t_d = l$ = number of cyclic subgroups of G and t_2 = number of elements of order 2 (by Theorem 1). An easy calculation shows that

$$\sum_{\substack{d|m \\ d\neq 1,\neq 2}} t_d \left(\frac{\phi(d)}{2} - 1\right) = \tfrac{1}{2}(n + 1 + t_2 - 2l) .$$

4. The idempotents of QG

In what follows we will identify QG with $\oplus\, t_d\, Q_d$ (using the isomorphism of Theorem 2). If D is a subgroup of G with G/D cyclic, then π_D will denote the projection of QG onto Q_d whose associated character χ_D has kernel D. By Theorem 2, there is exactly one such projection. Thus if $u = \oplus\, s_D$, then $s_D = \pi_D(u)$. It is clear that u is idempotent if, and only if, each s_D is either 0 or 1 - i.e. each idempotent is a sum of primitive idempotents u_D, where $\pi_D(u_D) = 1$ and $\pi_{D'}(u_D) = 0$ for $D' \neq D$. In Theorem 5 we obtain the representation of the idempotents u_D as elements of QG.

THEOREM 5. *For $D \leq G$ with G/D cyclic, let $u_D \in (QG)$ be the primitive idempotent which corresponds to the identity of $\pi_D(QG)$, and for $K \leq G$ let $e_K = \sum_{\substack{K\leq D \\ G/D \text{ cyclic}}} u_D$. Then*

$$e_K = \frac{1}{|K|} \sum_{k\in K} k \tag{11}$$

$$u_D = \sum_{D\leq H} \mu\,(|H/D|)\, e_H , \tag{12}$$

where μ is the Möbius μ-function.

Proof. Consider the element $r_K = \frac{1}{|K|} \sum_{k\in K} k \in QG$. For $H \leq G$ with

https://doi.org/10.1017/S0004972700041496 Published online by Cambridge University Press

G/H cyclic,

$$\pi_H(r_K) = \frac{1}{|K|} \sum_{k \in K} \pi_H(k) = \frac{1}{|K|} \sum_{k \in K} \chi_H(k) = \begin{cases} 1 & \text{if } K \leqq H, \\ 0 & \text{otherwise} \end{cases}$$

$$\pi_H(e_K) = \sum_{\substack{K \leqq D \\ G/D \text{ cyclic}}} \pi_H(u_D) = \begin{cases} 1 & \text{if } K \leqq H, \\ 0 & \text{otherwise.} \end{cases}$$

Hence $e_K = r_K = \frac{1}{|K|} \sum_{k \in K} k$, as claimed.

(12) follows from the Möbius inversion formula.[1]

COROLLARY. *Let $G = (a)$ be cyclic of order p^n (p a prime), and let*

$$e_i = \frac{1}{p^{n-i}} \sum_{k=0}^{p^{n-i}-1} \left(a^{p^i}\right)^k \in QG, \quad 0 \leqq i \leqq n, \tag{13}$$

$$u_i = e_i - e_{i-1}, \quad 1 \leqq i \leqq n. \tag{14}$$

Then

$$e_i \leftrightarrow \underbrace{1 \oplus \ldots \oplus 1}_{(i+1)} \oplus 0 \oplus \ldots \oplus 0 \in \bigoplus_{j=0}^{n} Z_{p^j},$$

$$u_i \leftrightarrow 0 \oplus \ldots \oplus 1 \oplus \ldots \oplus 0 \in \sum_{j=0}^{n} Z_{p^j}.$$

5. The index of $Z(G)$ in $\bigoplus t_d Z_d$

THEOREM 6. *Let $G = (a)$ be a cyclic of order p^n (p a prime) and let a_i be defined by* (13). *Then the set $\{e_i a^j\}$ ($0 \leqq i \leqq n$, $0 \leqq j \leqq \phi(p^i)$) is a basis for $\bigoplus_{j=0}^{n} Z_{p^j}$ over Z. (Here we*

[1] We are indebted to the referee for the use of the Möbius μ-function in the representation of u_D and for pointing out that the Möbius inversion formula holds under these circumstances.

https://doi.org/10.1017/S0004972700041496 Published online by Cambridge University Press

are identifying $e_i a^j$ *with its image in* $\bigoplus_{j=0}^{n} Z_{p^j}$) .

Proof. Let $M = \mathrm{mod}_Z \{e_i\, a^j\}_{\substack{0\le i\le n \\ 0\le j\le \phi(p^i)}}$. By the Corollary to Theorem 5, $M \le \bigoplus_{j=0}^{n} Z_{p^j}$ since e_i and $a^j \in \bigoplus_{j=0}^{n} Z_{p^j}$. The number of generators $e_i\, a^j$ is $\sum_{j=0}^{n} \phi(p^j) = p^n$. Thus if we establish that $M = \bigoplus_{j=0}^{n} Z_{p^j}$, the theorem will be proved.

We prove by induction on i , that $e_i\, a^j$ and $u_i\, a^j$ (where $u_i = e_i - e_{i-1}$) are in M , $\forall\, j \in N$. Note that

$$a^j = 1 \oplus \rho_1^j \oplus \ldots \oplus \rho_i^j \oplus \ldots \oplus \rho_n^j \,, \tag{15}$$

where $\rho_i \in Z_{p^i}$ is a primitive p^i-th root of unity (strictly speaking the "=" should be "$\leftrightarrow$" but we are identifying ZG with its image). If $i = 0$, $e_0\, a^j = u_0\, a^j = e_0 \in M$, $\forall\, j \in N$. So we assume that $e_{i-1}\, a^j$ and $u_{i-1}\, a^j \in M$, $\forall\, j \in N$. $u_i\, a^j = 0 \oplus \ldots \oplus \rho_i^j \oplus \ldots \oplus 0$ and $Z(\rho_i)$ is generated over Z by 1, ρ_i, ρ_i^2, ..., $\rho_i^{\phi(p^i)-1}$; hence $u_i\, a^j \in M$, $\forall\, j \in N$ if $u_i\, a^j \in M$ for $0 \le j \le \phi(p^i)$. So consider $u_i\, a^j$ with $0 \le j \le \phi(p^i)$. We have

$$u_i\, a^j = e_i\, a^j - e_{i-1}\, a^j \tag{16}$$

and $e_i\, a^j \in M$ since it is one of the generators of M , $e_{i-1}\, a^j \in M$ by the induction assumption. Hence $u_i\, a^j \in M$. Also $e_i = u_i + e_{i-1}$ and hence

$$e_i\, a^j = u_i\, a^j + e_{i-1}\, a^j \in M, \ \forall\, j \in N \,. \tag{17}$$

https://doi.org/10.1017/S0004972700041496 Published online by Cambridge University Press

Clearly $\bigoplus_{j=0}^{n} Z_{p^j}$ is generated by $u_i a^j$; hence $\bigoplus Z_{p^j} \leq M \leq \bigoplus Z_{p^j}$ so $M = \bigoplus_{j=0}^{n} Z_{p^j}$.

THEOREM 7. *Let $G = (a)$ be cyclic of order p^n (p a prime) and let e_i ($0 \leq i \leq n$) be defined by* (13). *Then*

(A) $e_i a^j$ has order p^{n-i} , mod ZG ($\forall\, j \in N$) .

(B) The elements $e_i a^j$ ($0 \leq i \leq n-1$, $0 \leq j < \phi(p^i)$) form a basis for $\bigoplus_{j=0}^{n} Z_{p^j}$, mod ZG .

(C) $\left| \bigoplus_{j=0}^{n} Z_{p^j} : ZG \right| = p^{1+p+\ldots+p^{n-1}} = p^{\left(p^n-1/p-1\right)}$.

Proof. By the previous theorem, the $e_i a^j$ ($0 \leq i \leq n$, $0 \leq j < \phi(p^i)$) form a basis for $\bigoplus_{j=0}^{n} Z_{p^j} = M$. Since $e_n a^j = a^j \in ZG$, the elements $e_i a^j$ ($0 \leq i \leq n-1$, $0 \leq j < \phi(p^i)$) generate M , mod ZG . It is clear from the definition of e_i , that $e_i a^j$ has order p^{n-i} ($\forall j \in N$) . Hence (A) holds. To prove (B), we need only show that the $e_i a^j$ ($0 \leq i \leq n-1$, $0 \leq j < \phi(p^i)$) are linearly independent, mod ZG . We prove this by induction on n . If $n = 1$, there is just one generator e_0 and so there is nothing to prove.

Now assume the result true in case of a cyclic group of order p^{n-1} . Let $B = (b)$, where $b = a^p$; $B \leq G$ has order p^{n-1} and so if we let

$$w_i = \frac{1}{p^{(n-1)-i}} \sum_{k=0}^{p^{(n-i)-1}-1} \left(b^{p^i}\right)^k ,$$

the induction hypothesis implies that $w_i b^j$ ($0 \leq i \leq n-2$, $0 \leq j < \phi(p^i)$) are linearly independent, mod ZB . But

https://doi.org/10.1017/S0004972700041496 Published online by Cambridge University Press

$$w_i = \frac{1}{p^{n-(i+1)}} \sum_{k=0}^{p^{n-(i+1)}-1} \left(a^{p^{i+1}}\right)^k = e_{i+1}$$

and $w_i\, b^j = e_{i+1}\, a^{pj}$. Hence the elements $e_{i+1}\, a^{pj}$ $(0 \leq i \leq n-1$, $0 \leq j < \phi(p^i))$ are linearly independent, mod ZB .

Now assume

$$(18) \qquad c_{oo}\, e_o + \sum_{i=1}^{n} \left(\sum_{j=0}^{\phi(p^i)-1} c_{ij}\, e_i\, a^j \right) = t \in ZG \quad (\text{where } c_{ij} \in Z) .$$

Multiplying by p^n we get:

$$(19) \quad p^n\, c_{oo}\, e_o + p \left(\sum\sum c_{ij}\, p^{n-1}\, e_i \right) = p^n t \Rightarrow p^n\, c_{oo}\, e_o \in p\, ZG$$

$$\Rightarrow c_{oo} \left(\sum_{i=0}^{p^n-1} a^i \right) \in p\, ZG \text{ (using (18))}$$

$$\Rightarrow c_{oo} \equiv 0 \pmod{p} .$$

So we can set $c_{oo} = p\, c'_{oo}$ with $c'_{oo} \in Z$. Noticing that $\frac{1}{p^{n-1}} \sum_{k=0}^{p^n-1} a^k = e_1 + e_1\, a + \ldots + e_1\, a^{p-1}$, we can write (19) in the form

$$(20) \qquad c'_{oo}\, (e_1 + \ldots + e_1\, a^{p-1}) + \sum_{i=1}^{n-1} \sum_{j=0}^{\phi(p^i)-1} c_{ij}\, e^i\, a^j = t \in ZG .$$

Consider now the terms involving only the a^j with $j \equiv p - 1 \pmod{p}$. We get

$$c'_{oo}\, e_1\, a^{p-1} + \sum_{i=2}^{n-1} \sum_{\substack{\leq j < \phi(p^i) \\ j \equiv p-1 (\text{mod } p)}} c_{ij}\, e_i\, a^j$$

$$= c'_{oo}\, e_1\, a^{p-1} + \sum_{i=2}^{n-1} \sum_{l=0}^{p^{i-1}-p^{i-2}-1} c_{i,lp+(p-1)}\, e_i\, a^{lp+(p-1)}$$

$$= t'\, a^{p-1} \quad \text{with } t' \in ZB .$$

But as we saw above the $e_{i+1}\, a^{lp}$

$(0 \leq i \leq n-1\ ,\ 0 \leq l \leq \phi(p^i)-1 = p^i = p^{i-1} - 1)$ are independent, mod ZB. Therefore $c'_{oo} \equiv 0 \pmod{p^{n-1}}$ and

$$c_{i,lp+(p-1)} \equiv 0 \pmod{p^{n-i}} \quad \text{for} \quad 2 \leq i \leq n-1\ ,\ 0 \leq l < \phi(p^{i-1})\ .$$

Since $c_{oo} = p\, c'_{oo}$, $c_{oo} \equiv 0 \pmod{p^n}$ and we obtain

$$\sum_{i=1}^{n-1} \sum_{j=0}^{\phi(p^i)-1} c_{ij}\, e^i\, a^j \in ZG\ .$$

Repeating the argument (with $p - 1$ replaced by s) we obtain

$$c_{i,lp+s} \equiv 0 \pmod{p^{n-i}} \quad \text{for:} \quad 1 \leq i \leq n-1,\ 0 \leq l < \phi(p^{i-1}),\ 0 \leq s \leq p-1\ . \tag{21}$$

But if $0 \leq j < \phi(p^i)$, $j \equiv s \pmod{p}$ for some s in the range $0 \leq s \leq p-1$, and $j = lp + s$ with $0 \leq l < \phi(p^{i-1})$. Hence from (21) we deduce that

$$c_{i,j} \equiv 0 \pmod{p^{n-i}},\ 1 \leq i \leq n-1\ ,\ 0 \leq j < \phi(p^i)$$

and this is what we wanted to show. Thus (B) is established.

Finally we consider (C). Since $e_i\, a^j$ has order p^{n-i}, mod ZG, and these elements form a basis for $\bigoplus_{j=0}^{n} Z_{p^j} = M$, mod ZG, the order of the quotient group M/ZG is

$$p^n\ (p^{n-1})^{\phi(p)}\ (p^{n-2})^{\phi(p^2)}\ \ldots\ (p)^{\phi(p^{n-1})}\ .$$

But since $n + (n-1)\,\phi(p) + \ldots + \phi(p^{n-1}) = 1 + p + \ldots + p^{n-1}$ (this can easily be established by induction), we have

$$\left[\bigoplus_{j=0}^{n} Z_{p^j} : ZG\right] = p^{1+p+\ldots+p^{n-1}}\ .$$

COROLLARY. *Let $G = (a)$ be cyclic of order p^n. If we define*

https://doi.org/10.1017/S0004972700041496 Published online by Cambridge University Press

$t_i = \sum_{k=0}^{p^{n-i}-1} \left(\alpha^{p^i}\right)^k$ $0 \leq i \leq n$, *the elements* $t_i\,\alpha^j$ $(0 \leq i \leq n,\ 0 \leq j < \phi(p^i))$ *form a basis for* ZG *(over* Z*)*.

Proof. Let

$$M_1 = \mathrm{Mod}_Z \left\{t_i\,\alpha^j\right\}_{\substack{0 \leq i \leq n \\ 0 \leq j < \phi(p^i)}}.$$

Clearly $M_1 \leq ZG < M = \bigoplus_{\substack{0\leq i\leq n \\ 0\leq j<\phi(p^i)}} Z\,(e_i\,\alpha^j)$. Let $r \in ZG$; then $r = \sum_{\substack{0\leq i\leq n \\ 0\leq j<\phi(p^i)}} c_{ij}\,e_i\,\alpha^j$ with $c_{ij} \in Z$ so that $c_{ij} = c'_{ij}\,p^{n-i}$ with $c'_{ij} \in Z$ since the $e_i\,\alpha^j$ are linearly independent, mod ZG. Thus $r = \sum c'_{ij}\,t_i\,\alpha^j \in M_1$, since $p^{n-i}\,e_i = t_i$. Hence $M_1 = ZG$. But the $t_i\,\alpha^j$ are linearly independent since the $e_i\,\alpha^j$ are; thus

$$ZG = \bigoplus_{\substack{0\leq i\leq n \\ 0\leq j<\phi(p^i)}} Z(t_i\,\alpha^j).$$

PROPOSITION 4. *Let* $B_i \leq A_i$ *be free abelian groups of rank* n_i *and let* A_i/B_i *have elementary divisors* $d_{i1},\ldots,d_{in_i}$ $(1 \leq i \leq r)$. *Then* $A_1 \otimes \ldots \otimes A_{r/B_1 \otimes \ldots \otimes B_r}$ *has a basis of* $\prod_{i=1}^{r} n_i$ *elements whose orders are* $d_{ij_1},\ldots,d_{rj_r}$, *where* $1 \leq j_i \leq n_i$.

Proof. Let A_i have a basis $a_{i1},\ldots,a_{in_i}$ and B_i a basis $b_{i1} = d_{i1}\,a_{i1},\ldots,b_{in_i} = d_{in_i}\,a_{in_i}$ (for $1 \leq i \leq r$). Then $A_1 \otimes \ldots \otimes A_r$ has a basis $a_{1j_1} \otimes \ldots \otimes a_{rj_r}$ $(1 \leq j_i \leq n_i)$ and $B_1 \otimes \ldots \otimes B_r$ has a basis $b_{1j_1} \otimes \ldots \otimes b_{rj_r} = d_{1j_1} \ldots d_{rj_r}\left(a_{1j_1} \otimes \ldots \otimes a_{rj_r}\right)$ $(1 \leq j_i \leq n_i)$ and the Proposition follows.

COROLLARY. *Under the hypothesis of the Proposition,*

https://doi.org/10.1017/S0004972700041496 Published online by Cambridge University Press

$$[A_1 \otimes \ldots \otimes A_r : B_1 \otimes \ldots \otimes B_r] = \prod_{i=1}^{r} \left|\frac{A_i}{B_i}\right|^{\prod_{j\neq i} \operatorname{rank}(A_j)}$$

If G is a finite abelian group, and $G = C_1 \times \ldots \times C_k$, where each C_i is cyclic of prime power order, then $ZG \simeq ZC_1 \otimes \ldots \otimes ZC_k$ (note after Proposition 2) and for $1 \leq i \leq k$, ZC is isomorphically imbedded in $\bigoplus_{j=0}^{l_i} Z_{p_i^j} = M_i$, where $|C_i| = p_i^{l_i}$. Theorem 7 tells us the structure of the finite additive (abelian) group M_i / ZC_i. Hence by using Proposition 4 we could calculate $[M_1 \otimes \ldots \otimes M_k : ZG]$. However, this does not give us the index of ZG in $\bigotimes_{d|m} t_d Z_d$ since $M_1 \otimes \ldots \otimes M_k$ is only imbedded in this last group as a subgroup of finite index. The calculation of this index would seem to be rather complicated.

References

[1] S.D. Berman, "On the equation $x^m = 1$ in an integral group ring", *Ukrain. Mat. Ž.*, 7 (1955), 253-261.

[2] Charles W. Curtis and Irving Reiner, *Representation theory of finite groups and associative algebras*, (Interscience, New York, 1962).

[3] Erich Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, (Chelsea Publ., New York, 1948).

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

[5] Sam Perlis and Gordon L. Walker, "Abelian group algebras of finite order", *Trans. Amer. Math. Soc.* 68 (1950), 420-426.

[6] Edwin Weiss, *Algebraic number theory*, (McGraw-Hill, New York, 1963).

Pennsylvania State University,
University Park, Pennsylvania, USA.