JOURNAL OF ALGEBRA 7, 77-90 (1967)

Multiplication in Grothendieck Rings of Integral Group Rings

D. L. STANCL

Mathematics Institute, University of Warwick, Coventry, England

Communicated by J. A. Green

Received September 6, 1966

1. INTRODUCTION

Let A be a ring, and consider the category of all finitely generated left A-modules. Recall that the Grothendieck group $K^0(A)$ of this category is the abelian additive group generated by all symbols $[M]$, where M ranges over all finitely generated left A-modules, with relations

$$[M] = [M'] + [M'']$$

whenever there exists a short exact sequence of A-modules

$$0 \to M' \to M \to M'' \to 0.$$

In particular, let G be a finite group, and let $R =$ alg. int. $\{F\}$, the ring of all algebraic integers of the algebraic number field F. Denote by FG the group algebra of G over F, and by RG the integral group ring of G over R. The Grothendieck group $K^0(RG)$ may be given a ring structure as follows: for all $[M]$, $[N] \in K^0(RG)$, set $[M][N] = [M \otimes_R N]$, where $M \otimes_R N$ is an RG-module with action of G given by $g(m \otimes n) = gm \otimes gn$, for all $g \in G$. Similarly define multiplication in $K^0(FG)$ by $[M^*][N^*] = [M^* \otimes_F N^*]$. Swan [5] has shown that this makes $K^0(RG)$ and $K^0(FG)$ into commutative rings with identities $[R]$ and $[F]$, respectively.

The Grothendieck ring $K^0(RG)$ has been studied by Heller and Reiner [2, 3] and Swan [5, 6]. In [3], Heller and Reiner have given an explicit formula for the additive structure of $K^0(RG)$, and in [6], Swan has given a formula for multiplication in $K^0(ZG)$ when G is cyclic of prime power order. In this paper we shall generalize Swan's results to the case where G is an arbitrary cyclic group, and in addition shall show how multiplication in $K^0(ZG)$ may be determined when G is an elementary abelian group.

2. Statement of the Problem

Keeping the notation of Section 1, we define a mapping

$$\theta : K^0(RG) \to K^0(FG)$$

by $\theta[M] = [F \otimes_R M]$. Here $F \otimes_R M$ is an FG-module with action of F given by $\beta(\alpha \otimes m) = \beta\alpha \otimes m$, for all $\beta \in F$, and action of G given by $g(\alpha \otimes m) = \alpha \otimes gm$, for all $g \in G$. It is easily verified that θ is a ring epimorphism, and we thus obtain an exact sequence

$$0 \to \ker \theta \to K^0(RG) \xrightarrow{\theta} K^0(FG) \to 0.$$

Definition 2.1. A linear mapping $f: K^0(FG) \to K^0(RG)$ such that $\theta f = 1$ is called a *lifting map for* $K^0(RG)$.

We summarize some results of Swan as

Proposition 2.2. (Swan [6]) *Let f be a lifting map for $K^0(RG)$. Then, as Abelian groups, $K^0(FG) + \ker\theta \cong K^0(RG)$, the isomorphism being given by $(x, y) \to f(x) + y$. Furthermore,* $\ker \theta$ *is a square-nilpotent ideal in* $K^0(RG)$.

Proposition 2.2 shows that in order to determine multiplication in $K^0(RG)$ we must calculate all products of the form

$$(f(x_1) + y_1)(f(x_2) + y_2) = f(x_1) f(x_2) + f(x_1) y_2 + f(x_2) y_1 .$$

For each FG-module M^*, denote by $\chi(M^*)$ the F-character of M^*. One verifies without difficulty that the mapping $[M^*] \to \chi(M^*)$ is a ring isomorphism between $K^0(FG)$ and the character ring of G, and thus $K^0(FG)$ may be regarded as a known ring. Also, if $\{M_i^* : 1 \leqslant i \leqslant m\}$ is a full set of non-isomorphic irreducible FG-modules, then the Jordan–Hölder theorem for FG-modules implies that $K^0(FG)$ is the free abelian group with basis $\{[M_i^*] : 1 \leqslant i \leqslant m\}$. Thus, in order to determine multiplication in $K^0(RG)$ it will suffice to find the following products:

$$f[M_i^*] \cdot f[M_j^*], \quad \text{for} \quad 1 \leqslant i, j \leqslant m \tag{1}$$

and

$$f[M_i^*] \cdot y, \quad \text{for} \quad 1 \leqslant i \leqslant m, y \in \ker\theta. \tag{2}$$

The remainder of this paper will be devoted to determining the products (1) and (2) for various choices of G and R.

3. The Cyclic Case

Throughout this section, G will denote a cyclic group of order n with generator g. Let Q be the rational field and Z the ring of rational integers. We shall determine multiplication in $K^0(ZG)$.

Let ρ_n be a fixed primitive nth root of unity, and for each s dividing n, set $\rho_s = \rho_n^{n/s}$. Then ρ_s is a primitive sth root of unity. Denote by Q_s the QG-module $Q(\rho_s)$ on which g acts as ρ_s. If g' is a generator of G such that $g' \neq g$, let Q'_s denote the QG-module $Q(\rho_s)$ on which g' acts as ρ_s.

Lemma 3.1. *$Q'_s \cong Q_s$ as QG-modules.*

Proof. Since g' and g both generate G, $g' = g^k$, for some k, $(k, n) = 1$. Let σ denote the Q-automorphism of $Q(\rho_s)$ induced by the mapping $\rho_s \to \rho_s{}^k$. The mapping of Q'_s onto Q_s defined by $\alpha \to \alpha^\sigma$, for all $\alpha \in Q'_s$, is the desired QG-isomorphism.

The above Lemma shows that we may refer unambiguously to the QG-module Q_s. Similarly, we may refer to the ZG-module Z_s, where Z_s denotes the ZG-module $Z[\rho_s]$ on which g acts as ρ_s.

It is well-known that $\{Q_s : s \mid n\}$ is a full set of non-isomorphic irreducible QG-modules, and hence $K^0(QG)$ is the free abelian group with basis $\{[Q_s] : s \mid n\}$. Define $f : K^0(QG) \to K^0(ZG)$ by $f[Q_s] = [Z_s]$, for all s dividing n, f extended linearly to all of $K^0(QG)$. It is clear that f is a lifting map for $K^0(ZG)$, and Swan [6] has shown that f is in fact a ring homomorphism. Since $K^0(QG)$ is a known ring, this allows us to compute all products of the form given in (1).

It remains to determine all products of the form $[Z_r]\,y$, for all r dividing n and $y \in \ker \theta$. The results of Heller and Reiner [3] show that $\ker \theta = \{\sum_{s|n} ([A_s] - [Z_s]) : A_s = Z_s\text{-ideal in } Q_s\}$. Thus it will suffice to find $[Z_r]([A_s] - [Z_s])$, for all r, s dividing n and all choices of A_s. For each r, let G_r be the quotient group of G of order r, and form the ZG-module ZG_r. The following Lemma shows that it suffices to determine all products of the form $[ZG_r]([A_s] - [Z_s])$:

Lemma 3.2. *In $K^0(ZG)$, $[Z_r] = \sum_{d|r} \mu(r/d)[ZG_d]$, where μ is the Möbius function.*

Proof. Let $\Phi_r(x)$ be the cyclotomic polynomial of order r. It is well-known that $\Phi_r(x) = \prod_{d|r} (x^d - 1)^{\mu(r/d)}$. Now, $Z_r \cong Z[x]/(\Phi_r(x))$, where g acts on the right-hand side as x, whence $Z_r \cong Z[x]/(\prod_{d|r} (x^d - 1)^{\mu(r/d)})$. It is clear that $Z[x]/(\prod_{d|r} (x^d - 1)^{\mu(r/d)}) \cong \sum_{d|r} \mu(r/d)(Z[x]/(x^d - 1))$, and since $Z[x]/(x^d - 1) \cong ZG_d$, the Lemma is proved.

Let $s \mid n$, and let A_s be any Z_s-ideal in Q_s. Then Z_s/A_s is a ZG-module on which g acts as $\bar{\rho}_s$, where $\bar{\rho}_s$ is ρ_s reduced modulo A_s. If ω is any sth root of unity, we denote by $(Z_s/A_s)\langle\bar{\omega}\rangle$ the ZG-module Z_s/A_s on which g acts as $\bar{\omega}$. We also introduce the following notation: if $s \mid n, t \mid s$, then $\mathfrak{G}(Q_s/Q_t)$ will denote the Galois group of Q_s over Q_t and $N_{s/t}$ the norm from Q_s to Q_t.

LEMMA 3.3. *Let $\sigma \in \mathfrak{G}(Q_s/Q)$. Then $(Z_s/A_s)\langle\bar{\rho}_s{}^{\sigma}\rangle \cong Z_s/A_s^{\sigma^{-1}}$ as ZG-modules.*

Proof. Map $(Z_s/A_s)\langle\bar{\rho}_s{}^{\sigma}\rangle$ onto $Z_s/A_s^{\sigma^{-1}}$ by $\bar{\alpha} \to \bar{\alpha}^{\sigma^{-1}}$. This the desired ZG-isomorphism.

We now state the main result of this section.

THEOREM 3.4. *Let G be a cyclic group of order n. Then multiplication in $K^0(ZG)$ is given by the following formula:*

$$[ZG_r]([A_s] - [Z_s]) = \sum_d ([N_{s/t}(A_s)Z_d] - [Z_d]),$$

for all r, s dividing n, where $t = s/(r, s)$ and d ranges over all divisors of $[r, s]$ such that $([r, s]/d, t) = 1$.

Proof. The proof is by induction on m, the number of distinct prime divisors of r.

Let $m = 1$. Then $r = p^a$, for some prime p, with $a \geqslant 0$. If $a = 0$, then $ZG_r = Z$ and the theorem is trivial. Hence we may suppose $a > 0$. Let $\hat{Z} = Z_s/A_s$. Since $0 \to A_s \to Z_s \to \hat{Z} \to 0$ is an exact sequence of ZG-modules, $[ZG_r]([A_s] - [Z_s]) = -[ZG_r \otimes_Z \hat{Z}]$, and it will suffice to find the ZG-module $M = ZG_r \otimes_Z \hat{Z}$. Since $r = p^a$, $ZG_r \cong Z[x]/(x^{p^a} - 1)$, and we obtain $M \cong \hat{Z}[x]/(x^{p^a} - 1)$, where g acts as $\bar{\rho}_s x$ on the right-hand side. We now write $s = p^b s'$, where $b \geqslant 0$ and $(p, s') = 1$, and proceed by cases:

Case 1. Suppose $a \leqslant b$. Then $\rho_s = \rho\omega$, where ρ is some primitive s'th root of unity and ω is some primitive p^bth root of unity. Set $\omega_1 = \omega^{p^{b-a}}$. Then ω_1 is a primitive p^ath root of unity. Since Z_s contains all p^ath roots of unity,

$$x^{p^a} - 1 = \prod_{k=1}^{p^a} (x - \bar{\omega}_1{}^k) \quad \text{in} \quad \hat{Z}[x],$$

whence

$$M \cong \sum_{k=1}^{p^a} \hat{Z}[x]/(x - \bar{\omega}_1{}^k) \cong \sum_{k=1}^{p^a} \hat{Z}\langle\overline{\rho_s\omega_1{}^k}\rangle.$$

Now if $a < b$, $\rho_s \omega_1{}^k$ is a primitive sth root of unity for each k, $1 \leqslant k \leqslant p^a$, and we denote by σ_k the Q-automorphism of Q_s induced by the mapping $\rho_s \to \rho_s \omega_1{}^k$. Then

$$M \cong \sum_{k=1}^{p^a} \hat{Z}\langle \bar{\rho}_s^{\sigma_k} \rangle,$$

and thus, by Lemma 3.3,

$$M \cong \sum_{k=1}^{p^a} Z_s / A_s^{\sigma_k^{-1}}.$$

But it is clear that as k ranges from 1 to p^a, σ_k ranges over all elements of $\mathfrak{G}(Q_s/Q_{p^{b-a}s'})$, and hence $M \cong \sum_\sigma Z_s/A_s^\sigma$, $\sigma \in \mathfrak{G}(Q_s/Q_{p^{b-a}s'})$. Therefore $M \cong Z_s/N_{s/p^{b-a}s'}(A_s)Z_s$. This yields the desired result when $a < b$.

If $a = b$, then $\omega_1 = \omega$, and

$$M \cong \sum_{k=1}^{p^a} \hat{Z}\langle \overline{\rho_s \omega^k} \rangle = \sum_{k=1}^{p^a} \hat{Z}\langle \overline{\rho \omega^{1+k}} \rangle = \sum_{k=1}^{p^a} \hat{Z}\langle \overline{\rho \omega^k} \rangle.$$

Thus $M \cong \sum_j \hat{Z}\langle \overline{\rho\omega^j} \rangle + \sum_i \hat{Z}\langle \overline{\rho\omega^i} \rangle$, where $1 \leqslant j \leqslant p^a$, $(j, p) = 1$, and $1 \leqslant i \leqslant p^a$, $(i, p) \neq 1$. Since $(j, p) = 1$, each $\rho\omega^j$ is a primitive sth root of unity, and an analysis similar to that carried out for the case $a < b$ shows that $\sum_j \hat{Z}\langle \overline{\rho\omega^j} \rangle \cong Z_s/N_{s/s'}(A_s)Z_s$.

Now consider

$$\sum_i \hat{Z}\langle \overline{\rho\omega^i} \rangle = \sum_{e=1}^{a} \sum_h \hat{Z}\langle \overline{\rho\omega^{hp^e}} \rangle,$$

where $1 \leqslant h \leqslant p^{a-e}$, $(h, p) = 1$. Set $Y = \hat{Z}\langle \overline{\rho\omega^{hp^e}} \rangle$. It is clear that Y is a $Z[\rho\omega^{p^e}]$-module, and as such, $Y \cong Z[\rho\omega^{p^e}]/N_{s/p^{a-e}s'}(A_s)$ (see [4], pp. 27–28). Consequently, as a ZG-module,

$$Y \cong (Z_{p^{a-e}s'}/N_{s/p^{a-e}s'}(A_s))\langle \overline{\rho\omega^{hp^e}} \rangle.$$

For each h, $1 \leqslant h \leqslant p^{a-e}$, $(h, p) = 1$, let σ_h be the element of $\mathfrak{G}(Q_{p^{a-e}s'}/Q_{s'})$ induced by the mapping $\rho_{p^{a-e}s'} \to \rho\omega^{hp^e}$. By Lemma 3.3,

$$Y \cong Z_{p^{a-e}s'}/(N_{s/p^{a-e}s'}(A_s))^{\sigma_h^{-1}},$$

and hence we find that

$$\sum_h \hat{Z}\langle \overline{\rho\omega^{hp^e}} \rangle \cong Z_{p^{a-e}s'}/N_{s/s'}(A_s)Z_{p^{a-e}s'}, \quad \text{for each } e, \text{ eq } 1 \leqslant e \leqslant a.$$

Therefore

$$M \cong Z_s/N_{s/s'}(A_s)Z_s + \sum_{e=1}^{a} Z_{p^{a-e}s'}\Big/N_{s/s'}(A_s)Z_{p^{a-e}s'} .$$

This gives the desired result when $a = b$.

Case 2. Suppose $a > b$. Then

$$x^{p^a} - 1 = (x^{p^b} - 1) \prod_{k=b+1}^{a} \Phi_{p^k}(x);$$

whence $M \cong \hat{Z}[x]/(x^{p^b} - 1) + \sum_k \hat{Z}[x]/(\Phi_{p^k}(x))$. By Case 1,

$$\hat{Z}[x]/(x^{p^b-1}) \cong \sum_{e=0}^{a} Z_{p^e s'}\Big/N_{s/s'}(A_s)Z_{p^e s'} .$$

Therefore it will suffice to find $\hat{Z}[x]/(\Phi_{p^k}(x))$ for $b + 1 \leqslant k \leqslant a$.

Fix k, and set $\omega = (\rho_{p^k})^{p^{k-b}}$. Then ω is a primitive p^bth root of unity, and in $\hat{Z}[x]$, $\Phi_{p^k}(x) = \prod_j (x^{p^{k-b}} - \bar{\omega}^j)$, where $1 \leqslant j \leqslant p^b$, $(j, p) = 1$. Thus

$$\hat{Z}[x]/(\Phi_{p^k}(x)) \cong \sum_j \hat{Z}[x]\Big/(x^{p^{k-b}} - \bar{\omega}^j).$$

Now, for each j, $\hat{Z}[x]/(x^{p^{k-b}} - \bar{\omega}^j)$ is isomorphic to $(Z_{p^k s'}/A_s Z_{p^k s'})\langle\overline{\rho_s \rho_{p^k}^j}\rangle$: the isomorphism is given by mapping an element $\sum_i \bar{\alpha}_i x^i$ of $\hat{Z}[x]/(x^{p^{k-b}} - \bar{\omega}^j)$ onto the element $\sum_i \overline{\alpha_i \rho_{p^k}^{ji}}$ of $Z_{p^k s'}/A_s Z_{p^k s'}$. Therefore

$$\hat{Z}[x]/(\Phi_{p^k}(x)) \cong \sum_j (Z_{p^k s'}/A_s Z_{p^k s'})\langle\overline{\rho_s \rho_{p^k}^j}\rangle,$$

where $1 \leqslant j \leqslant p^b$, $(j, p) = 1$.

For each j, let σ_j be the element of $\mathfrak{G}(Q_{p^k s'}/Q_{s'})$ induced by the mapping $\rho_{p^k s'} \to \rho_s \rho_{p^k}^j$, and τ_j be σ_j restricted to Q_s. Then by Lemma 3.3,

$$(Z_{p^k s'}/A_s Z_{p^k s'})\langle\overline{\rho_s \rho_{p^k}^j}\rangle \cong Z_{p^k s'}/(A_s Z_{p^k s'})^{\sigma_j^{-1}},$$

and since

$$Z_{p^k s'}/(A_s Z_{p^k s'})^{\sigma_j} \cong Z_{p^k s'}/A_s^{\tau_j} Z_{p^k s'} ,$$

it easily follows that

$$\sum_j (Z_{p^k s'}/A_s Z_{p^k s'})\langle\overline{\rho_s \rho_{p^k}^j}\rangle \cong \sum_\tau Z_{p^k s'}/A_s^{\tau} Z_{p^k s'} , \tau \in \mathfrak{G}(Q_s/Q_{s'}).$$

Thus

$$\hat{Z}[x]/(\Phi_{p^k}(x)) \cong Z_{p^k s'}/N_{s/s'}(A_s)Z_{p^k s'},$$

and this, together with the formula for $\hat{Z}[x]/(x^{p^b}-1)$, gives the desired result for M. This completes the proof of Case 2.

We have now established the theorem for the case $m = 1$. Now let m be greater than 1, and assume the theorem true for all $[ZG_{r'}]([A_s] - [Z_s])$, where r' has fewer than m distinct prime divisors. Write $r = p^a r'$, where p is a prime, $a > 0$, and $(p, r') = 1$. We have $G_r \cong G_{p^a} \times G_{r'}$, and it is well-known that this implies $ZG_r \cong ZG_{p^a} \otimes_Z ZG_{r'}$. Thus $[ZG_r] = [ZG_{p^a}][ZG_{r'}]$ in $K^0(ZG)$. Since the theorem is true for $ZG_{r'}$ and ZG_{p^a}, we obtain

$$[ZG_r]([A_s] - [Z_s]) = [ZG_{p^a}] \sum_{d'} ([N_{s/t'}(A_s)Z_{d'}] - [Z_{d'}])$$

$$= \sum_{e} \sum_{d'} ([N_{d'/d''}(N_{s/t'}(A_s)Z_{d'})Z_e] - [Z_e]),$$

where $t' = s/(r', s)$, d' ranges over all divisors of $[r', s]$ such that $([r', s]/d', t') = 1$, and for each d', $d'' = d'/(p^a, d')$ and e ranges over all divisors of $[p^a, d']$ such that $([p^a, d']/e, d'') = 1$.

Now, since $([r', s]/d', t') = 1$, $t' \mid d'$ and hence $Q_{t'}$ is contained in $Q_{d'}$. Similarly, $Q_{d''}$ is contained in Q_e. Furthermore, $d' \mid [r', s]$, $(p, r') = 1$, and $([r', s]/d', t') = 1$ together imply that $(p^a, d') = (p^a, s)$. Then $t' \mid d'$ implies that $s/(r, s) = t$ divides d''. Hence Q_t is contained in $Q_{d''}$. We now have the following inclusion diagram:

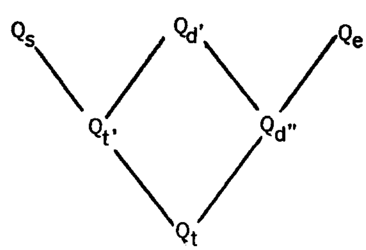

FIG. 1

It is easy to verify that $\mathfrak{G}(Q_{t'}/Q_t) = \mathfrak{G}(Q_{d'}/Q_{d''})$, and thus that

$$N_{d'/d''}(N_{s/t'}(A_s)Z_{d'})Z_e = N_{s/t}(A_s)Z_e.$$

We therefore obtain $[ZG_r]([A_s] - [Z_s]) = \sum_{d'} (\sum_e ([N_{s/t}(A_s)Z_e] - [Z_e])$, where d' ranges over all divisors of $[r', s]$ such that $([r', s]/d', t') = 1$, and for each d', e ranges over all divisors of $[p^a, d']$ such that $([p^a, d']/e, d'/(p^a, d')) = 1$.

Now write $s = p^b s'$, $(p, s') = 1$. Then $d' \mid [r', s] = p^b[r', s']$, and $(p^b[r', s']/d', p^b s'/(r', p^b s')) = 1$ implies that $d' = p^b k$, where $s'/(r', s') \mid k$, $k \mid [r', s']$, and $([r', s']/k, s'/(r', s')) = 1$. Then $e \mid [p^a, d'] = [p^a, p^b k]$, and $([p^a, p^b k]/e, p^b k/(p^a, p^b k)) = 1$. Thus, if $a < b$, then $e = d'$, while if $a \geqslant b$, we have $e = p^i k$, for $0 \leqslant i \leqslant a$. Therefore we obtain the following formulas for $[ZG_r]([A_s] - [Z_s])$:

(i) if $a < b$,

$$[ZG_r]([A_s] - [Z_s]) = \sum_{d'} ([N_{s/t}(A_s)Z_{d'}] - [Z_{d'}]),$$

where $d' \mid [r', s]$ and $([r', s]/d', t') = 1$;

(ii) if $a \geqslant b$,

$$[ZG_r]([A_s] - [Z_s]) = \sum_{i=0}^{a} \sum_{k} ([N_{s/t}(A_s)Z_{p^i k}] - [Z_{p^i k}]),$$

where $s'/(r', s') \mid k \mid [r', s']$ and $([r', s']/k,\ s'/(r', s')) = 1$. Now consider

$$\sum_{d} ([N_{s/t}(A_s)Z_d] - [Z_d]),$$

where $d \mid [r, s]$ and $([r, s]/d, t) = 1$. Let $r = p^a r'$, $s = p^b s'$ as above. Then if $a < b$, $[r, s] = [r', s]$, and $([r, s]/d, t) = 1$ if and only if $([r', s]/d, t') = 1$. Thus we may take d dividing $[r', s]$ with $([r', s]/d, t') = 1$, so that if $a < b$, $\sum_d ([N_{s/t}(A_s)Z_d] - [Z_d])$ agrees with formula (i) for $[ZG_r]([A_s] - [Z_s])$. Similarly, if $a \geqslant b$, we find that $d = p^i k$, $0 \leqslant i \leqslant a$, where $s'/(r', s') \mid k \mid [r', s']$ and $([r', s']/k, s'/(r', s')) = 1$, whence $\sum_d ([N_{s/t}(A_s)Z_d] - [Z_d])$ agrees with formula (ii) for $[ZG_r]([A_s] - [Z_s])$ when $a \geqslant b$. This concludes the proof of the theorem.

4. The Elementary Abelian Case

Let G be an Abelian group, F an algebraic number field which is a splitting field for G, and $R =$ alg. int. $\{F\}$. We shall determine multiplication in $K^0(RG)$.

Write $G = G_1 \times \cdots \times G_k$, where G_i is cyclic of order n_i with generator g_i, and let ρ_i be a fixed primitive n_ith root of unity, for $1 \leqslant i \leqslant k$. Denote by $F\langle a_1, \ldots, a_k \rangle$ the FG-module F on which g_i acts as $\rho_i^{a_i}$, $1 \leqslant i \leqslant k$. Similarly, if A is an R-ideal in F, $A\langle a_1, \ldots, a_k\rangle$ will denote the RG-module A on which g_i acts as $\rho_i^{a_i}$. It is easily seen that $\{F\langle a_1, \ldots, a_k\rangle: 1 \leqslant a_i \leqslant n_i,\ 1 \leqslant i \leqslant k\}$ is a full set of non-isomorphic irreducible FG-modules, whence $\{[F\langle a_1, ..., a_k\rangle]: 1 \leqslant a_i \leqslant n_i, 1 \leqslant i \leqslant k\}$ is a basis for $K^0(FG)$.

Define $f: K^0(FG) \to K^0(RG)$ by $f[F\langle a_1, ..., a_k\rangle] = [R\langle a_1, ..., a_k\rangle]$, f extended linearly to all of $K^0(FG)$. Clearly, f is a lifting map for $K^0(RG)$.

LEMMA 4.1. *f is a ring homomorphism.*

Proof. Consider

$$[F\langle a_1, ..., a_k\rangle][F\langle b_1, ..., b_k\rangle] = [F\langle a_1, ..., a_k\rangle \bigotimes_F F\langle b_1, ..., b_k\rangle].$$

Map

$$F\langle a_1, ..., a_k\rangle \bigotimes_F F\langle b_1, ..., b_k\rangle \text{ onto } F\langle a_1 + b_1, ..., a_k + b_k\rangle \quad \text{by} \quad \alpha \otimes \beta \to \alpha\beta.$$

It is easily verified that this mapping is an FG-isomorphism, and hence

$$[F\langle a_1, ..., a_k\rangle][F\langle b_1, ..., b_k\rangle] = [F\langle a_1 + b_1, ..., a_k + b_k\rangle].$$

Similarly,

$$[R\langle a_1, ..., a_k\rangle][R\langle b_1, ..., b_k\rangle] = [R\langle a_1 + b_1, ..., a_k + b_k\rangle],$$

and therefore f is a ring homomorphism.

Heller and Reiner [2] have shown that every element of $\ker \theta$ may be written as a sum of elements of the form $[A\langle a_1, ..., a_k\rangle] - [R\langle a_1, ..., a_k\rangle]$, for various choices of the ideal A and the positive integers $a_1, ..., a_k$. The following Lemma therefore completes the description of multiplication in $K^0(RG)$.

LEMMA 4.2. *In $K^0(RG)$,*

$$[R\langle b_1, ..., b_k\rangle]([A\langle a_1, ..., a_k\rangle] - [R\langle a_1, ..., a_k\rangle])$$
$$= [A\langle a_1 + b_1, ..., a_k + b_k\rangle] - [R\langle a_1 + b_1, ..., a_k + b_k\rangle].$$

Proof. The argument of the proof of Lemma 4.1 shows that

$$[R\langle b_1, ..., b_k\rangle][A\langle a_1, ..., a_k\rangle] = [A\langle a_1 + b_1, ..., a_k + b_k\rangle],$$

and this clearly implies the Lemma.

Now let $G = G_1 \times \cdots \times G_k$ be an elementary Abelian group, with G_i cyclic of order p, $1 \leqslant i \leqslant k$. Let ρ be a fixed primitive pth root of unity, $F = Q(\rho)$, $R = Z[\rho]$. Then F is a splitting field for G, and hence multiplication in $K^0(RG)$ is known.

As above, $F\langle a_1, ..., a_k\rangle$ will denote the FG-module F on which g_i acts as ρ^{a_i}, for $i \leqslant i \leqslant k$, and similarly for $A\langle a_1, ..., a_k\rangle$. Note that, by restriction of operators, $F\langle a_1, \ldots, a_k\rangle$ and $A\langle a_1, \ldots, a_k\rangle$ are QG- and ZG-modules, respectively. Let S be the collection of QG-modules listed below:

$$Q, F\langle p, \ldots, p, 1\rangle, F\langle p, \ldots, p, 1, a_k\rangle \quad \text{where} \quad 1 \leqslant a_k \leqslant p, \ldots,$$
$$F\langle p, 1, a_3, \ldots, a_k\rangle \quad \text{where} \quad 1 \leqslant a_i \leqslant p \quad \text{for} \quad 3 \leqslant i \leqslant k,$$
$$F\langle 1, a_2, \ldots, a_k\rangle \quad \text{where} \quad 1 \leqslant a_i \leqslant p \quad \text{for} \quad 2 \leqslant i \leqslant k.$$

For ease of notation, we shall denote an element of S of the form

$$F\langle p, \ldots, p, 1, a_{j+1}, \ldots, a_k\rangle, 1 \leqslant j \leqslant k, \quad \text{by} \quad F\langle a_{j+1}, \ldots, a_k\rangle.$$

LEMMA 4.3. *S is a full set of nonisomorphic irreducible QG-modules.*

Proof. The elements of S are clearly irreducible QG-modules, and the sum of their Q-ranks is $p^k = (G : 1)$, so there are the correct number of them. Thus it suffices to show that no two of them are isomorphic as QG-modules.

Let $1 \leqslant j \leqslant k$, and suppose that $F\langle a_{j+1}, \ldots, a_k\rangle \cong F\langle b_{j+1}, \ldots, b_k\rangle$ as QG-modules, where $a_t \neq b_t$ for some t. Then under the isomorphism, $1 \to \beta$ for some $\beta \neq 0$, whence $\rho^{a_t} = g_j^{a_t} \cdot 1 \to g_j^{a_t}\beta = \rho^{a_t}\beta$. But also, $\rho^{a_t} = g_t \cdot 1 \to g_t\beta = \rho^{b_t}\beta$, and therefore we have a contradiction. Now suppose that $F\langle a_{j+1}, \ldots, a_k\rangle \cong F\langle b_{i+1}, \ldots, b_k\rangle$, for some i, $1 \leqslant i \leqslant k$, where $i \neq j$. Without loss of generality, we may assume $j < i$. Then under the isomorphism, $1 \to \beta$, for some $\beta \neq 0$, and hence $\rho = g_j \cdot 1 \to g_j\beta = \rho^p\beta = \beta$. Therefore $1 \to \beta$ and also $\rho \to \beta$, a contradiction. Since it is clear that Q is not isomorphic to any of the other elements of S, we have thus shown that no two of the elements of S are isomorphic, and the Lemma is proved.

DEFINITION 4.4. Define $\psi : K^0(ZG) \to K^0(RG)$ by $\psi[M] = [R \otimes_Z M]$, for all $[M] \in K^0(ZG)$, where $R \otimes_Z M$ is an RG-module with action of R given by $r'(r \otimes m) = r'r \otimes m$ and action of G given by $g(r \otimes m) = r \otimes gm$, for all $r' \in R$, $g \in G$. Similarly, define

$$\eta : K^0(QG) \to K^0(FG) \quad \text{by} \quad \eta[M^*] = [F \underset{Q}{\otimes} M^*],$$

for all $[M^*] \in K^0(QG)$.

LEMMA 4.5. *ψ and η are ring homomorphisms and the following diagram commutes and is exact:*

$$\begin{array}{ccccccccc} 0 \to & \ker\theta_R & \to & K^0(RG) & \xrightarrow{\theta_R} & K^0(FG) & \to 0 \\ & \uparrow\psi & & \uparrow\psi & & \uparrow\eta & \\ 0 \to & \ker\theta_Z & \to & K^0(ZG) & \xrightarrow{\theta_Z} & K^0(QG) & \to 0 \\ & & & & & \uparrow & \\ & & & & & 0 & \end{array}$$

Proof. The proof that ψ and η are ring homomorphisms is straightforward. The rows of the diagram are exact by the remarks at the beginning of Section 2, and the Noether–Deuring Theorem ([1], p. 200]) implies that η is monic. One easily checks that ψ maps $\ker \theta_Z$ into $\ker \theta_R$ and that $\theta_R \psi = \eta \theta_Z$.

Let A be an R-ideal in F. We shall denote by $A^{(t)}$ the image of A under the Q-automorphism of F induced by the mapping $\rho \to \rho^t$, $1 \leqslant t \leqslant p-1$. Also, $A\langle a_{j+1},..., a_k\rangle$ will denote the ZG-module $A\langle p,..., p, 1, a_{j+1},..., a_k\rangle$, $1 \leqslant j \leqslant k$. By Lemma 4.3, $K^0(QG)$ is the free Abelian group with basis $\{[M^*] : M^* \in S\}$, and hence we may define a lifting map $f_Z : K^0(QG) \to K^0(ZG)$ as follows:

$$f_Z[Q] = [Z], f_Z[F\langle a_{j+1},..., a_k\rangle] = [R\langle a_{j+1},..., a_k\rangle] \quad \text{for} \quad 1 \leqslant j \leqslant k,$$

with f_Z extended linearly to all of $K^0(QG)$. The results of Heller and Reiner [3] now show that every element of $\ker \theta_Z$ is a sum of elements of the form $[A\langle a_{j+1},..., a_k\rangle] - [R\langle a_{j+1},..., a_k\rangle]$. Thus the following Lemma determines $\psi(\ker \theta_Z)$:

LEMMA 4.6.

$$\psi[A\langle a_{j+1},..., a_k\rangle] = \sum_{t=1}^{p-1} [A^{(t)}\langle p,..., p, t, ta_{j+1},..., ta_k\rangle].$$

Proof. Let $M = R \otimes_Z A\langle a_{j+1},..., a_k\rangle$, so that $\psi[A\langle a_{j+1},..., a_k\rangle] = [M]$, and let $\Phi_p(x)$ be the cyclotomic polynomial of order p. For all $r \otimes a \in M$,

$$\Phi_p(g_j)(r \otimes a) = r \otimes \Phi_p(g_j)a = r \otimes \Phi_p(\rho)a = 0;$$

so $\Phi_p(g_j)M = 0$. Let $b_0 = 1$,

$$b_t = \prod_{i=1}^{t} (g_j - \rho^i), \qquad \text{for} \quad 1 \leqslant t \leqslant p-1.$$

Then $M = b_0 M \supset b_1 M \supset \cdots \supset b_{p-1} M = 0$.

For each t, $1 \leqslant t \leqslant p-1$, define

$$\gamma_t : M \to A^{(t)}\langle p,..., p, t, ta_{j+1},..., ta_k\rangle \quad \text{by} \quad \gamma(r \otimes a) = ra^{(t)}.$$

It is easily seen that γ_t is a well-defined RG-epimorphism for each t. Consequently, $\gamma_t : b_{t-1}M \to b_{t-1}A^{(t)}\langle p,..., p, t, ta_{j+1},..., ta_k\rangle$ is an epimorphism. However, $A^{(t)}\langle p,..., p, t, ta_{j+1},..., ta_k\rangle$ is isomorphic to

$$b_{t-1}A^{(t)}\langle p,..., p, t, ta_{j+1},..., ta_k\rangle$$

by the mapping $y \to b_{t-1}y$; hence we may assume that γ_t maps $b_{t-1}M$ onto

$A^{(t)}\langle p,..., p, t, ta_{j+1} ,..., ta_k\rangle$, for $1 \leqslant t \leqslant p - 1$. Note that b_tM is contained in the kernel of this mapping, since $(g_j - \rho^t)$ annihilates

$$A^{(t)}\langle p,..., p, t, ta_{j+1} ,..., ta_k\rangle.$$

Consider γ_1 mapping $b_0M = M$ onto $A^{(1)}\langle p,..., p, 1, a_{j+1} ,..., a_k\rangle$. Let M_1 be the kernel of this mapping. Then $M/M_1 \cong A^{(1)}\langle p,..., p, 1, a_{j+1} ,..., a_k\rangle$, and M_1 contains b_1M. Since M_1 contains b_1M, γ_2 maps M_1 onto

$$A^{(2)}\langle p,..., p, 2, 2a_{j+1} ,..., 2a_k\rangle.$$

Let M_2 be the kernel of this mapping. Then

$$M_1/M_2 \cong A^{(2)}\langle p,..., p, 2, 2a_{j+1} ,..., 2a_k\rangle,$$

and M_2 contains b_2M. Continuing in this manner, we obtain

$$M = M_0 \supset M_1 \supset \cdots \supset M_{p-1} \supset 0,$$

where $M_{t-1}/M_t \cong A^{(t)}\langle p,..., p, t, ta_{j+1} ,..., ta_k\rangle$, for $1 \leqslant t \leqslant p - 1$. Hence, in $K^0(RG)$,

$$[M] = \sum_{t=1}^{p-1} [M_{t-1}/M_t] + [M_{p-1}]$$

$$= \sum_{t=1}^{p-1} [A^{(t)}\langle p,..., p, t, ta_{j+1} ,..., ta_k\rangle] + [M_{p-1}].$$

Now, $(M : R) = p - 1$ and $(A^{(t)}\langle p,..., p, t, ta_{j+1} ,..., ta_k\rangle : R) = 1$ for $1 \leqslant t \leqslant p - 1$, so a consideration of R-ranks shows that $(M_{p-1} : R) = 0$. However, M_{p-1} is a submodule of the R-torsion-free R-module M, and thus is itself R-torsion-free. Hence $(M_{p-1} : R) = 0$ implies that $[M_{p-1}] = 0$, and the Lemma is proved.

PROPOSITION 4.7. *$\psi : K^0(ZG) \to K^0(RG)$ is a monomorphism.*

Proof. Let $x \in \ker \theta_Z$. Then x is a sum of elements of $K^0(ZG)$ of the form

$$[A\langle a_{j+1} ,..., a_k\rangle] - [R\langle a_{j+1} ,..., a_k\rangle],$$

where $1 \leqslant j \leqslant k$ and $1 \leqslant a_i \leqslant p$ for $j < i \leqslant k$, for various R-ideals A. Thus, by Lemma 4.6, $\psi(x)$ is a sum of elements of $K^0(RG)$ of the form

$$\sum_{t=1}^{p-1} ([A^{(t)}\langle p,..., p, t, ta_{j+1} ,..., ta_k\rangle] - [R\langle p,..., p, t, ta_{j+1} ,..., ta_k\rangle]).$$

Heller and Reiner [2] have shown that such a sum in $K^0(RG)$ is zero only if each ideal appearing in the sum may be written as the product of a principal ideal and a power of some prime ideal P, where P divides the order of G.

It is well-known that the only prime ideal of R which divides p is the principal ideal $(1 - \rho)$; consequently, $\psi(x) = 0$ in $K^0(RG)$ only if each ideal appearing in the sum for $\psi(x)$ is principal. However, if each ideal appearing in the sum for $\psi(x)$ is principal, then surely each ideal A appearing in the sum for $x \in \ker \theta_Z$ is principal. But if A is principal, then $A\langle a_{j+1},..., a_k\rangle \cong R\langle a_{j+1},..., a_k\rangle$ as ZG-modules, whence $[A\langle a_{j+1},..., a_k\rangle] - [R\langle a_{j+1},..., a_k\rangle] = 0$, and thus $x = 0$. Therefore $\psi : \ker \theta_Z \to \ker \theta_R$ is monic. Now apply the Five-Lemma to the diagram of Lemma 4.5 to conclude that

$$\psi : K^0(ZG) \to K^0(RG)$$

is monic.

COROLLARY 4.8. *The lifting map f_Z is a ring homomorphism.*

Proof. Let f be the lifting map for $K^0(RG)$ of Lemma 4.1. An easy calculation shows that $f_Z = \psi^{-1} f \eta$. Therefore, since η, f, and ψ^{-1} are ring homomorphisms, so is f_Z.

Let $x, y \in K^0(ZG)$. Since ψ is a ring monomorphism $xy = \psi^{-1}(\psi(x)\,\psi(y))$, and the product $\psi(x)\,\psi(y)$ may be calculated with the aid of Lemma 4.2. Thus we have shown how multiplication in $K^0(ZG)$ may be determined when G is elementaiy abelian. We proceed to give formulas which completely describe the multiplication.

THEOREM 4.9. *Let G be an elementary Abelian group. The following formulas describe multiplication in $K^0(ZG)$:*

(i) $[Z]x = x$, *for all* $x \in K^0(ZG)$

(ii) $[R\langle b_{j+1},..., b_k\rangle]([A\langle a_{i+1},..., a_k\rangle] - [R\langle a_{i+1},..., a_k\rangle])$

$$= \sum_{t=1}^{p-1} ([A^{(t)}\langle b_{j+1},..., b_{i-1}, b_i + t, b_{i+1} + ta_{i+1},..., b_k + ta_k\rangle]$$
$$- [R\langle b_{j+1},..., b_{i-1}, b_i + t, b_{i+1} + ta_{i+1},..., b_k + ta_k\rangle]), \quad \text{if } j < i,$$

$$\sum_{t=2}^{p-1} ([A^{(t)}\langle (p+1-t)b_{i+1} + ta_{i+1},..., (p+1-t)b_k + ta_k\rangle]$$
$$- [R\langle (p+1-t)b_{i+1} + ta_{i+1},..., (p+1-t)b_k + ta_k\rangle]), \quad \text{if } j = i,$$

$$\sum_{t=1}^{p-1} ([A\langle a_{i+1},..., a_{j-1}, a_j + t, a_{j+1} + tb_{j+1},..., a_k + tb_k\rangle]$$
$$- [R\langle a_{i+1},..., a_{j-1}, a_j + t, a_{j+1} + tb_{j+1},..., a_k + tb_k\rangle]), \quad \text{if } j > i.$$

Proof. Formula (i) is clearly true. In order to prove (ii), we note that, since

$$y = [R\langle b_{j+1},..., b_k\rangle]([A\langle a_{i+1},..., a_k\rangle] - [R\langle a_{i+1},..., a_k\rangle]) \in \ker \theta_Z,$$

y is a sum of elements of the form

$$[C\langle c_{r+1}, ..., c_k\rangle] - [R\langle c_{r+1}, ..., c_k\rangle],$$

and therefore $\psi(y) \in \ker \theta_R$ is a sum of elements of the form

$$\sum_{t=1}^{p-1} ([C^{(t)}\langle p, ..., p, t, tc_{r+1}, ..., tc_k\rangle] - [R\langle p, ..., p, t, tc_{r+1}, ..., tc_k\rangle]).$$

It is clear that the elements $[C\langle c_{r+1}, ..., c_k\rangle]$ appearing in the sum for y can be found by determining the elements of form $[C^{(1)}\langle p, ..., p, 1, c_{r+1}, ..., c_k\rangle]$ appearing in the sum for $\psi(y)$.

Suppose $j < i$. Applying Lemmas 4.6 and 4.2, we find that

$$\begin{aligned}\psi(y) &= \sum_{t=1}^{p-1} \sum_{s=1}^{p-1} ([A^{(t)}\langle p, ..., p, s, sb_{j+1}, ..., sb_{i-1}, sb_i + t, sb_{i+1} + ta_{i+1}, ..., sb_k + ta_k\rangle] \\ &\quad - [R\langle p, ..., p, s, sb_{j+1}, ..., sb_{i-1}, sb_i + t, sb_{i+1} + ta_{i+1}, ..., sb_k + ta_k\rangle]) \\ &= \sum_{t=1}^{p-1} ([A^{(t)}\langle p, ..., p, 1, b_{j+1}, ..., b_{i-1}, b_i + t, b_{i+1} + ta_{i+1}, ..., b_k + ta_k\rangle] \\ &\quad - [R\langle p, ..., p, 1, b_{j+1}, ..., b_{i-1}, b_i + t, b_{i+1} + ta_{i+1}, ..., b_k + ta_k\rangle]) + u,\end{aligned}$$

where $u \in \ker \theta_R$ and none of the elements appearing in u have the form $[C\langle p, ..., p, 1, c_{r+1}, ..., c_k\rangle]$. Therefore,

$$\begin{aligned}y = \sum_{t=1}^{p-1} &([A^{(t)}\langle b_{j+1}, ..., b_{i-1}, b_i + t, b_{i+1} + ta_{i+1}, ..., b_k + ta_k\rangle] \\ &- [R\langle b_{j+1}, ..., b_{i-1}, b_i + t, b_{i+1} + ta_{i+1}, ..., b_k + ta_k\rangle]),\end{aligned}$$

which agrees with the formula. The same procedure will establish the formulas for the cases $j = i, j > i$. This completes the proof of the theorem.

References

1. Curtis, C. W. and Reiner, I. "Representation Theory of Finite Groups and Associative Algebras." Interscience, New York, 1962.
2. Heller, A. and Reiner, I. Grothendieck groups of orders in semi-simple algebras. *Trans. Am. Math. Soc.* **112** (1964), 344-355.
3. Heller, A. and Reiner, I. Grothendieck groups of integral group rings. *Illinois J. Math.* **9** (1965), 349-359.
4. Serre, J.-P. "Corps Locaux." Hermann, Paris, 1962.
5. Swan, R. G. Induced representations and projective modules. *Ann. Math.* **71** (1960), 552-578.
6. Swan, R. G. The Grothendieck ring of a finite group. *Topology* **2** (1963), 85-110.