SUT Journal of Mathematics
Vol. 31, No. 1 (1995), 33–37

INTEGRAL REPRESENTATIONS OF CYCLIC GROUPS

Kenshi KIDA

(Received November 4, 1994)

Abstract. The purpose of this paper is to determine the set of non- isomorphic indecomposable RG-lattices, where R is a certain ring of algebraic integers, and G is a cyclic group of prime order.

AMS 1991 *Mathematics Subject Classification.* Primary 16S34; Secondary 16U60.

Key words and phrases. Cyclic group, extension, indecomposable module, integral representations.

§1. Introduction.

Let G be a finite group, and let R be a ring of integers. By RG, we denote the group ring consisting of all formal combinations of the elements of G with coefficients in R. We shall here be concerned with representations of G by matrices with entries in R, or equivalently, with left RG-modules having a free finite R-basis.

The first systematic study of this problem occurred in a paper by Diederichsen [1]. Let G denote a cyclic group generated by an element g of prime order p. Also we set

$$K = \mathbb{Q}(\zeta_p), \qquad S = \text{alg. int.}\{K\} = \mathbb{Z}[\zeta_p],$$

where for a positive integer s, ζ_s is a primitive s-th root of 1 over $\mathbb{Q}$. The following result was shown:

Theorem. (*Diederichsen* [1], *Reiner* [3]). *Every $\mathbb{Z}G$-module M is isomorphic to a direct sum*

$$(A_1, a_1) \oplus \cdots \oplus (A_r, a_r) \oplus A_{r+1} \oplus \cdots \oplus A_n \oplus Y$$

where the $\{A_\nu\}$ are S-ideals in K, the $\{a_\nu\}$ are chosen so that $a_i \in A_i, a_i \notin (\zeta_p - 1)A_i$, and Y is a $\mathbb{Z}$-module having a finite $\mathbb{Z}$-basis such that $gy = y$ for all $y \in Y$. The isomorphism class of M is determined by the integers r, n, the $\mathbb{Z}$-rank of Y, and the ideal class of $A_1 \cdots A_n$ in K.

In this paper, we shall classify all left RG-modules, where G is a cyclic group of order p, and

$$R = \text{alg. int.}\{\mathbb{Q}(\zeta_q)\} = \mathbb{Z}[\zeta_q].$$

Our proof will be based on the treatment given by Heller-Reiner [2].

§2. Representations of a cyclic group of order p

Throughout this section, let G be a cyclic group generated by an element σ of prime order p.

For convenience, we set

$$R = \mathbb{Z}[\zeta_q], \qquad B = R[\zeta_p] = \mathbb{Z}[\zeta_{pq}],$$

where p and q are distinct odd primes. We have ring isomorphisms

$$\frac{RG}{(\sigma - 1)RG} \simeq R, \tag{2.1}$$

$$\frac{RG}{(\Phi_p(\sigma))RG} \simeq B, \tag{2.2}$$

given by $\sigma \longmapsto 1$, and $\sigma \longmapsto \zeta_p$, respectively, where $\Phi_p(x)$ is the cyclotomic polynomial of order p (and degree $p-1$). By (2.1) and (2.2), both R and B are left RG-modules.

Let M be any RG-module, and set

$$N = \{m \in M \ ; \ (\sigma - 1)m = 0\}.$$

Then N is an RG-submodule of M annihilated by $(\sigma - 1)$. Therefore we may consider that N is R-torsion-free.

Hence there exist ideals $I_1, I_2, \cdots, I_t$ of R such that

$$N \simeq I_1 \oplus I_2 \oplus \cdots \oplus I_t.$$

This gives the structure of N both as R-module and as RG-module.

On the other hand M/N is annihilated by $\Phi_p(\sigma)$, so that it may be viewed as B-module. Also M/N is B-torsion-free. Therefore there exist ideals $J_1, J_2, \cdots, J_u$ of B such that

$$M/N \simeq J_1 \oplus J_2 \oplus \cdots \oplus J_u.$$

This shows that M/N is considered both as B-module and as RG-module. The problem of classifying all RG-modules is reduced to that of determining extensions of $J_1 \oplus J_2 \oplus \cdots \oplus J_u$ by $I_1 \oplus I_2 \oplus \cdots \oplus I_t$.

For the rest of this section, we write Ext in place of Ext^1_{RG}. Since RG is a commutative ring, we may view Ext itself as RG-module.

Lemma. *There are RG-isomorphisms*

$$\mathit{Ext}(B_j, A_i) \simeq A_i/pA_i,$$

where integral ideals $A_1, \cdots, A_{h_R}$ are representatives of the h_R distinct ideal classes of $\mathbb{Q}(\zeta_q)$, and integral ideals $B_1, \cdots, B_{h_B}$ are representatives of the h_B distinct ideal classes of $\mathbb{Q}(\zeta_{pq})$.

Proof. By (2.2), the following sequence

$$0 \longrightarrow \Phi_p(\sigma) \cdot RG \xrightarrow{\tau} RG \longrightarrow B \longrightarrow 0$$

is exact. Then, for every B_j, there exists an integral ideal S_j of RG such that the sequence

$$0 \longrightarrow \Phi_p(\sigma) \cdot RG \xrightarrow{\tau} S_j \longrightarrow B_j \longrightarrow 0$$

is exact. It follows that

$$\begin{aligned} 0 \longrightarrow \mathrm{Hom}_{RG}(B_j, A_i) \longrightarrow \mathrm{Hom}_{RG}(S_j, A_i) \xrightarrow{\tau^*} \\ \mathrm{Hom}_{RG}(\Phi_p(\sigma) \cdot RG, A_i) \longrightarrow \mathrm{Ext}(B_j, A_i) \longrightarrow \mathrm{Ext}(S_j, A_i) \longrightarrow \cdots . \end{aligned}$$

The mapping τ^* is induced from τ as follows:
for each $f \in \mathrm{Hom}_{RG}(S_j, A_i)$,

$$(\tau^* f)x = f(\tau x), \qquad x \in \mathrm{Hom}_{RG}(\Phi_p(\sigma) \cdot RG, A_i).$$

For convenience let $Y = \Phi_p(\sigma) \cdot RG$. Since S_j is RG-projective, we obtain $\mathrm{Ext}(S_j, A_i) = 0$. Therefore,

$$\mathrm{Ext}(B_j, A_i) \simeq \mathrm{Hom}_{RG}(Y, A_i)/\tau^*\mathrm{Hom}_{RG}(S_j, A_i). \tag{2.3}$$

Now set $y = \Phi_p(\sigma) \in Y$; then each $F \in \mathrm{Hom}_{RG}(Y, A_i)$ is completely determined by the value $F(y) \in A_i$, and each $a \in A_i$ is of the form $F(y)$ for some such F. Thus

$$\mathrm{Hom}_{RG}(Y, A_i) \simeq A_i$$

as RG-modules. Let us determine which elements in A_i correspond to elements in the image of τ^*. Because τ is the inclusion mapping, the image of τ^* in A_i is exactly $\Phi_p(\sigma)A_i$, and by (2.3) we obtain

$$\mathrm{Ext}(B_j, A_i) \simeq A_i/\Phi_p(\sigma)A_i.$$

Since

$$\Phi_p(\sigma)a = pa, \qquad a \in A_i,$$

we get

$$\mathrm{Ext}(B_j, A_i) \simeq A_i/pA_i.$$

This completes the proof. □

Note that p is unramified in R. If

$$pR = P_1 P_2 \cdots P_m$$

is the factorization of pR into distinct prime ideals of R, then

$$R/pR \simeq R/P_1 \oplus R/P_2 \oplus \cdots \oplus R/P_m \simeq \underbrace{F \oplus F \oplus \cdots \oplus F}_{m},$$

where F is a finite field of characteristic p. Since

$$A_i/pA_i \simeq R/pR, \qquad 1 \leq i \leq h_R,$$

we obtain that $\mathrm{Ext}(B_j, A_i)$ is isomorphic to the direct sum of m copies of F.

On the other hand, by the following pullback diagram,

$$\begin{array}{ccc} RG & \longrightarrow & R \\ \downarrow & & \downarrow \\ B & \longrightarrow & R/pR \end{array}$$

we define the group homomorphism $\varphi_{ij} : u(A_i) \times u(B_j) \longrightarrow u(R/pR)$. In addition, we define the group homomorphism $\pi^{(k)}_{s_1 s_2 \cdots s_k}$ from $u(A/pA) \simeq \underbrace{F^* \oplus F^* \oplus \cdots \oplus F^*}_{m}$ to $\underbrace{F^* \oplus \cdots \oplus F^*}_{k}$ $(F^* = F - \{0\})$ by

$$\pi^{(k)}_{s_1 s_2 \cdots s_k}(a_1, a_2, \cdots, a_m) = (a_{s_1}, \cdots, a_{s_k})$$

for every $k = 1, 2, \cdots, m$, and set

$$l_{ij} = \sum_{k=1}^{m} \sum_{1 \leq s_1 < s_2 < \cdots < s_k \leq m} \left| \frac{\mathrm{Im}\ \pi^{(k)}_{s_1 s_2 \cdots s_k}}{\mathrm{Im}\ \pi^{(k)}_{s_1 s_2 \cdots s_k} \circ \varphi_{ij}} \right|.$$

Now we are ready to prove the following result:

Theorem. *Keep the above notations. Up to RG-isomorphism, there are* $h_A + h_B + \sum_{1 \leq i \leq h_A,\ 1 \leq j \leq h_B} l_{ij}$ *-indecomposable RG-lattices, given by*

$$A_i,\ B_j,\ \ (B_j, A_i)_{k_{ij}} \qquad (1 \leq i \leq h_A,\ 1 \leq j \leq h_B,\ 1 \leq k_{ij} \leq l_{ij})$$

where $(B_j, A_i)_{k_{ij}}$ *are the isomorphism classes of non-splitting extentions of* B_j *by* A_i.

Proof. Let M be an indecomposable RG-module. By the discussion at the beginning of this section, we know that M must be an extension of $J_1 \oplus J_2 \oplus$

$\cdots \oplus J_u$ by $I_1 \oplus I_2 \oplus \cdots \oplus I_t$ for some t and u. If $t = 0$, then we must have $M \simeq B_j$ for some j. While if $u = 0$, then $M \simeq A_i$ for some i.

Therefore, for the rest of the proof, we assume that both t and u are positive. Since M is indecomposable, we must have $t = u = 1$, that is, M must be an extension of B_j by A_i. It follows that $M \simeq A_i \oplus_R B_j$.

Now we consider the extensions of B_j by A_i; each extension determines an extension class in $\mathrm{Ext}(B_j, A_i)$, which is represented by an element $\overline{\alpha_i}$ in $\overline{A_i} = A_i/pA_i$. If $\overline{\alpha_i} = \overline{0}$, we get a split extension, which is clearly decomposable. On the other hand, we consider the orbits of $\mathrm{Ext}(B_j, A_i)$ under the action of $\mathrm{Aut}A_i \times \mathrm{Aut}B_j$. Because φ_{ij} is not an epimorphism in general, there are l_{ij}-isomorphism classes of non-splitting extensions of B_j by A_i. □

Acknowledgement

The author would like to express his sincere thanks to the referee for his useful advice.

References

[1] F. E. Diederichsen, *Über die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetischer Äquivalenz*, Hamb. Abh. **14** (1940), 357–412.

[2] A. Heller and I. Reiner, *Representations of cyclic groups in rings of integers, I*, Ann. of Math. **76** (1962), 73–92.

[3] I. Reiner, *Integral representations of cyclic groups of prime order*, Proc. Amer. Math. Soc. **8** (1957), 142–146.

Kenshi Kida
Department of Mathematics, Science University of Tokyo
26 Wakamiya, Shinjuku-ku, Tokyo 162, Japan