東海大学紀要情報通信学部
vol.4,No.2,2011,pp.28-31

Technical Survey

On Representations of Cyclic Groups over the Ring of Gaussian Integers

by

Kenshi KIDA*[1]

(received on November 21, 2011 & accepted on December 12, 2011)

Abstract

The purpose of this paper to determine and classify the indecomposable RG-lattices, where R is the ring of Gaussian integers, and G is a cyclic group of prime order.

Keywords : Representation, Cyclic Group, Gaussian Integer, Lattice, Ext

1. Introduction

Let G be a finite group, and R 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 be concerned here with representations of G by matrices with entries in R, or equivalently, with left $RG-$modules having a free finite $R-$basis. However, it is useful to work with a slightly larger class of modules, namely $RG-$lattices (that is left $RG-$modules which are finitely generated and projective as $R-$modules).

The fundamental problem in integral representation theory is to determine and classify the $RG-$lattices. Every $RG-$lattice is expressible as a direct sum of indecomposable lattices, though not a unique manner. If there are only finitely many isomorphism classes of indecomposable $RG-$lattices, we say that RG has finite representation type.

In particular, in the case where G is a cyclic group of prime order p, the following results are known:Diederichsen [1], Heller-Reiner [2], Kida [3],[4], and Reiner [5].

In this paper, in the case where R is the ring of Gaussian integers, we shall determine all $RG-$indecomposable lattices up to isomorphism. The method of the proof is based on the treatment given by Heller-Reiner [2]. Besides we shall show that calculations of Ext modules play an important role in this discussion.

2. Representation of cyclic group of order p

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

We set

$$R = A = \mathbf{Z}[i], \qquad B = R[\zeta_p] = \mathbf{Z}[\zeta_{4p}],$$

where ζ_s is a primitive s-th root of 1 over $\mathbf{Q}$, and p is odd prime. We have ring isomorphisms

$$\frac{RG}{(\sigma-1)RG} \cong R = A, \tag{2.1}$$

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

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), we may view both A and B as left RG-modules.

Let M be arbitrary RG-lattice, and put

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

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

*[1] Junior Associate Professor, School of Science, Tokai University

Because R is a principal ideal domain, we obtain

$$N \cong \overbrace{R \oplus R \oplus \cdots \oplus R}^{t}.$$

We may view N both as R-module and RG-module.

Furthermore M/N is annihilated by $\Phi_p(\sigma)$, so that it may be viewed as B-module. Also M/N is B-torsion-free. Consequently there exist ideals $I_1, I_2, \cdots, I_u$ of B such that

$$M/N \cong I_1 \oplus I_2 \oplus \cdots \oplus I_u.$$

From the preceding discussion, we obtain that M/N is considered both as B-module and RG-module. By the following exact sequence

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0,$$

the problem of classifying the RG-lattices is reduced to that of determining extensions of $I_1 \oplus I_2 \oplus \cdots \oplus I_u$ by $\overbrace{R \oplus R \oplus \cdots \oplus R}^{t}$.

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

Suppose that integral ideals $B_1, \cdots, B_h$ are representatives of the h distinct ideal classes of $\mathbf{Q}(\zeta_{4p})$.

The following discussion is similar to that of [3]. By (2.2), the following sequence

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

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

$$0 \longrightarrow \Phi_p(\sigma) \cdot RG \xrightarrow{\iota} S_j \longrightarrow B_j \longrightarrow 0 \tag{2.3}$$

is exact. From (2.3), we get the following long exact sequence

$$0 \longrightarrow \mathrm{Hom}_{RG}(B_j, A) \longrightarrow \mathrm{Hom}_{RG}(S_j, A) \xrightarrow{\iota^*}$$
$$\mathrm{Hom}_{RG}(\Phi_p(\sigma) \cdot RG, A) \longrightarrow \mathrm{Ext}(B_j, A) \longrightarrow \mathrm{Ext}(S_j, A) \longrightarrow \cdots.$$

The mapping ι^* is induced from ι as follows: for any $f \in \mathrm{Hom}_{RG}(S_j, A)$, we have

$$(\iota^* f)x = f(\iota x), \qquad x \in \Phi_p(\sigma) \cdot RG.$$

Since S_j is $RG-$projective, we obtain $\mathrm{Ext}(S_j, A) = 0$.

For this reason, we get

$$\mathrm{Ext}(B_j, A) \cong \mathrm{Hom}_{RG}(Y, A)/\iota^* \mathrm{Hom}_{RG}(S_j, A), \tag{2.4}$$

where $Y = \Phi_p(\sigma) \cdot RG$.

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

$$\mathrm{Hom}_{RG}(Y, A) \cong A$$

as $RG-$modules. Let us determine which elements in A correspond to elements in the image of ι^*. Since ι is the inclusion mapping, the image of ι^* in A is exactly $\Phi_p(\sigma)A$, and by using (2.4) we have

$$\mathrm{Ext}(B_j, A) \cong A/\Phi_p(\sigma)A.$$

Because

$$\Phi_p(\sigma)a = (\sigma^{p-1} + \cdots + \sigma + 1)a = pa, \qquad a \in A,$$

we get

$$\mathrm{Ext}(B_j, A) \cong A/pA. \tag{2.5}$$

Further we suppose

$$N = \overbrace{A \oplus A \oplus \cdots \oplus A}^{t}$$

and

$$M/N = B_{k_1} \oplus B_{k_2} \oplus \cdots \oplus B_{k_u},$$

where $1 \leq k_1, k_2, \cdots k_u \leq h$. Since

$$\mathrm{Ext}(B_j, R) \cong R/pR =: \overline{R}$$

by (2.5), it is easily shown that $\mathrm{Ext}(M/N, N)$ is isomorphic to the module of the $u \times t$ matrices with entries in $\overline{R}$. In order to calculate the effect of basis changes, it will be convenient to exhibit this isomorphism explicitly. Let $\sum_{i=1}^{u} S_{k_i} \cdot x_i$ be a free module with basis $x_1, x_2, \cdots, x_u$. Adding $u-$copies of the exact sequences (2.3), we obtain the exact sequence

$$0 \longrightarrow \sum \Phi_p(\sigma) \cdot RG \cdot x_i \xrightarrow{\tau} \sum S_{k_i} \cdot x_i \longrightarrow \sum B_{k_i} \cdot \overline{x_i} \longrightarrow 0$$

where $\overline{x_i}$ annihilated by $\Phi_p(\sigma)$. Set $y_i = \Phi_p(\sigma)\cdot x_i$. Then as above we obtain

$$\mathrm{Ext}(M/N, N) \cong \mathrm{Hom}_{RG}(\sum RG\cdot y_i,\ N)/\mathrm{Im}\tau^*.$$

Let $N = Aa_1 \oplus Aa_2 \oplus \cdots \oplus Aa_t$. Then each

$$F \in \mathrm{Hom}_{RG}(\sum RG\cdot y_i, N),$$

we may write

$$F(y_i) = \sum_{j=1}^{t} \alpha_{ij} a_j, \qquad \alpha_{ij}\in A_j,\ 1\le i\le u.$$

The class $[F]$ which F determines in $\mathrm{Ext}(M/N, N)$ then corresponds to the $u\times t$ matrix $\mathbf{F} = (\overline{\alpha_{ij}})$ with entries in $\overline{R}$.

Suppose that we make a basis change in M/N by leaving $\overline{x_1}, \overline{x_3}, \cdots, \overline{x_u}$ unchanged, but replacing $\overline{x_2}$ by $\overline{x_2} - \lambda\overline{x_1}$ for some λ in RG. Then $y_1, y_3, \cdots y_u$ are changed, but y_2 becomes $y_2 - \lambda y_1$, and α_{2j} is replaced by $\alpha_{2j} - \lambda\alpha_{1j},\ 1\le j\le t$.

On theother hand, if $a_1' = a_1 + \lambda a_2, a_2' = a_2, \cdots, a_t' = a_t$ is a basis change in N, then α_{i2} is replaced by $\alpha_{i2} - \lambda\alpha_{i1},\ 1\le i\le u$.

Note that p is unramified in R. Let

$$pR = P_1P_2\cdots P_g$$

be the factorization of pR into distinct prime ideals of R. So we have

$$\begin{aligned} R/pR &\cong R/P_1 \oplus R/P_2 \oplus \cdots \oplus R/P_g \\ &\cong \overbrace{F\oplus F\oplus\cdots\oplus F}^{g}, \end{aligned}$$

where F is the finite field of characteristic p. By (2.5) and (2.6), we get that $\mathrm{Ext}(B_j, A)$ is isomorphic to the direct sum of $g-$copies of the finite fields.

In addition, by the following pullback diagram,

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

we define the group homomorphism

$$\varphi_j : u(A)\times u(B_j) \longrightarrow u(R/pR).$$

Moreover, the group homomorphism $\pi^{(k)}_{s_1s_2\cdots s_k}$ from

$$\overbrace{F^*\oplus F^*\oplus\cdots\oplus F^*}^{g} \cong u(R/pR)$$

to

$$\overbrace{F^*\oplus\cdots\oplus F^*}^{k} \qquad (F^* = F - \{0\})$$

is defined by

$$\pi^{(k)}_{s_1s_2\cdots s_k}(u_1, u_2, \cdots u_g) = (u_{s_1}, \cdots, u_{s_k}) \qquad 1\le s_1 < \cdots < s_k \le g$$

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

$$l_j = \sum_{k=1}^{g}\ \sum_{1\le s_1<\cdots<s_k\le g} \left| \frac{\mathrm{Im}\pi^{(k)}_{s_1\cdots s_k}}{\mathrm{Im}\pi^{(k)}_{s_1\cdots s_k}\circ\varphi_j} \right|$$

Let C_p be a cyclic group of prime order p. Now we are ready to prove the following result.

Theorem.

$\mathbf{Z}[i]C_p$ has finite representation type.

Proof. Let M be an indecomposable $RG-$lattice. By the discussion at the beginning of this section, we know that M must be an extension of $B_{k_1}\oplus B_{k_2}\oplus\cdots\oplus B_{k_u}$ by $\overbrace{A\oplus A\oplus\cdots\oplus A}^{t}$ for some t and u. If $t = 0$, then we must have $M\cong B_j$ for some j. While if $u = 0$, then $M\cong A_i$ for some i. Therefore, for the rest of the proof, we assume that both t and u are positive. Let $\mathbf{F} = (\overline{\alpha_{ij}})$ be the $u\times t$ matrix with entries in $\overline{R}$ corresponding to the extension M of M/N by N. If every entry of $\mathbf{F}$ is zero, then the extension splits, and M is decomposable. Thus, assume that $\mathbf{F}$ has a non-zero entry, and in fact, after re-numbering basis elements, that $\overline{\alpha_{11}} \ne \overline{0}$. However, there exist elements $\lambda_2, \cdots, \lambda_u$ of RG such that $\overline{\alpha_{i1}} - \lambda_i\overline{\alpha_{11}} = \overline{0},\ 2\le i\le u$. Consequently by a basis change in M/N, we may make all of the elements in the first column of $\mathbf{F}$ bellow $\overline{\alpha_{11}}$ equal to zero. Simularly, a basis change in N permits us to the $(1,2), \cdots, (1,t)$ entries of $\mathbf{F}$ equal to zero. Hence the submodule $Aa_1\oplus_R B_{k_1}\overline{x_1}$ is a direct summand of M. Because M is indecomposable, we must obtain that $M\cong Aa_i\oplus_R B_{k_j}\overline{x_j}$, that is, M must be an extension of B_j by A.

Now we consider the extensions of B_j by A; each extension determines an extension class in $\mathrm{Ext}(B_j, A)$, which is represented by an element $\overline{\alpha}$ in $\overline{A} = A/pA$. If $\overline{\alpha} = \overline{0}$, we have a split extention, which is clearly decomposable. On the other hand, the isomorphism classes of extensions of B_j by A are in bijection with the orbits of $\mathrm{Ext}(B_j, A)$ under the action of $(\mathrm{Aut}A) \times (\mathrm{Aut}B_j)$. Because φ_j is not an epimorphism, in general, there are l_j-isomorphism classes of non-splitting extensions of B_j by A. Up to $RG-$isomorphism, there are exactly $1 + h + \sum_{1 \leq j \leq h} l_j-$indecomposable $RG-$lattices,given by

$$A, \quad B_j, \quad (B_j, A)_{n_j} \qquad (1 \leq j \leq h, \quad 1 \leq n_j \leq l_j)$$

where $(B_j, A_i)_{n_j}$ are isomorphism classes of non-splitting extensions of B_j by A. This completes the proof.

References

[1] F.E.Diederichisen. *Über die Ausreduktion ganzzahliger Gruppendarsteliungen bei arithmetischer Äquivalenz.* Hamb. Abh. **14**(1940),357-412.

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

[3] K.Kida. *Integral representations of cyclic groups.* SUT J. Math. **31**(1995), 33-37.

[4] K.Kida. *On representations of cyclic groups over a ring of integers.* to appear in Comm. Algebra.

[5] I.Reiner. *Integral representations of cyclic groups of prime order.* Proc. Am. Math. Soc. **8** (1957), 142-146.

[6] S.K.Sehgal. *Units in commutative integral group rings.* Math. J. Okayama. Univ. **14** (1970), 135-138.