

ON THE GROTHENDIECK RING OF AN ABELIAN p -GOUP

TADAO OBAYASHI

Introduction

The Grothendieck ring of a finite group has been studied by Swan ([5], [6]). At the end of [6] he determined completely the structure of the Grothendieck ring $G(Z\mathfrak{G})$ of a cyclic p -group \mathfrak{G} over the ring of rational integers Z .

In this paper we investigate the structure of $G(Z\mathfrak{G})$ of an abelian p -group \mathfrak{G} .

In the first section we consider some properties of the integral group ring of \mathfrak{G} . The results of this section are applied in the second section to investigate the additive structure of $G(Z\mathfrak{G})$. Let \mathfrak{o} be a maximal order of the group ring $Q\mathfrak{G}$ over the rational number field Q and let $Co(\mathfrak{o})$ be the reduced projective class group of \mathfrak{o} (Rim [4]). We show that $G(Z\mathfrak{G})$ is isomorphic to the splitting Z -algebra extension of $Co(\mathfrak{o})$ by $G(Q\mathfrak{G})$ (§ 2, § 3). The latter half of the third section is devoted to study the action of $G(Q\mathfrak{G})$ to $Co(\mathfrak{o})$. Some examples are given in the final section.

The author wishes to express his hearty thanks to Professor A. Hattori for his many helpful suggestions during the preparation of this paper.

§ 1. The integral group ring of a finite abelian group

Let R be the ring of integers of an algebraic number field K . The group ring $K\mathfrak{G}$ of a finite abelian group \mathfrak{G} over K decomposes into a direct sum of algebraic number fields K_i over K

$$K\mathfrak{G} = K_1 \oplus \cdots \oplus K_s, \quad (1.1)$$

and K_1, \dots, K_s are a full set of non-isomorphic irreducible $K\mathfrak{G}$ -modules. This decomposition induces the decomposition of the maximal order \mathfrak{o} of $K\mathfrak{G}$ into a direct sum of maximal orders \mathfrak{o}_i of K_i , i.e. the ring of integers of K_i . Since

Received April 19, 1965.

\mathfrak{O} contains $R\mathfrak{G}$, each projection π_i of $K\mathfrak{G}$ onto K_i induces a ring homomorphism of $R\mathfrak{G}$ into \mathfrak{O}_i . We will denote by A_i the kernel of this ring homomorphism and we will set $\Gamma_i = \prod_{j \neq i} A_j$.

PROPOSITION 1.1. *Let \mathfrak{G} be a finite abelian group of order n and exponent n_0 and let $K = Q(\zeta_m)$ be a cyclotomic field, where ζ_m means a primitive m -th root of 1. Then*

- (1) *in (1.1), each K_i is also a cyclotomic field $Q(\zeta_{m_i})$ for some m_i which divides $L.C.M. (m, n_0)$,*
- (2) *each projection π_i induces a surjection of $R\mathfrak{G}$ onto \mathfrak{O}_i .*
- (3) *for each i , $A_i + \Gamma_i \supseteq n^{s-1}R\mathfrak{G}$, and*
- (4) *there exists a positive integer l such that*

$$\Gamma_1 + \dots + \Gamma_s \supseteq n^l R\mathfrak{G}.$$

Proof. Let $\mathfrak{G} = \mathfrak{G}_1 \times \dots \times \mathfrak{G}_t$ be the decomposition of \mathfrak{G} into a direct product of cyclic subgroups \mathfrak{G}_h and let g_h be the fixed generator of \mathfrak{G}_h .

Then we have $K_i = K(\pi_i(g_1), \dots, \pi_i(g_t))$. But for each h $\pi_i(g_h)^{n_0} = 1$, which implies that $K_i = Q(\zeta_{m_i})$ for some m_i which divides $L.C.M.(m, n_0)$. This shows (1). Each π_i gives rise to the surjection of $R\mathfrak{G}$ onto $R[\pi_i(g_1), \dots, \pi_i(g_t)] = Z[\zeta_{m_i}]$, which is the maximal order of $K_i = Q(\zeta_{m_i})$. This proves (2). (3) and (4) is proved by an induction on t . First, we suppose that \mathfrak{G} is a cyclic group generated by an element g . We have a ring isomorphism $K\mathfrak{G} \cong K[x]/(x^n - 1)K[x]$, where $K[x]$ is the polynomial ring over K in an indeterminate x . If

$$x^n - 1 = f_1(x) \cdot \dots \cdot f_s(x) \tag{1.2}$$

is the factorization of $x^n - 1$ into irreducible non-constant monic polynomials in $K[x]$, by the Chinese remainder theorem we have

$$K[x]/(x^n - 1)K[x] \cong K[x]/f_1(x)K[x] \oplus \dots \oplus K[x]/f_s(x)K[x]. \tag{1.3}$$

Obviously every root of $f_i(x)$ is a primitive n_i -th root of 1 for some n_i which divides n . Let ζ_{n_i} be one of these roots and let $K_i = K(\zeta_{n_i})$. Then the map $g \rightarrow \zeta_{n_i}$ gives rise to the projection π_i of $K\mathfrak{G}$ onto K_i . This shows that the kernel of π_i is $f_i(g)K\mathfrak{G}$, so that A_i is just given by $R\mathfrak{G} \cap f_i(g)K\mathfrak{G} = f_i(g)R\mathfrak{G}$. By a simple calculation, we have from (1.2)

$$f_i(x)R[x] + f_j(x)R[x] \supseteq nR[x] \quad (i \neq j). \tag{1.4}$$

Replacing x by g , we have

$$A_i + A_j \supseteq nR\mathbb{G} \quad (i \neq j). \tag{1.5}$$

This implies that $A_i + \prod_{j \neq i} A_j \supseteq n^{s-1}R\mathbb{G}$, which shows (3). (1.2) yields also that

$$\prod_{j \neq 1} f_j(x)R[x] + \cdots + \prod_{j \neq s} f_j(x)R[x] \supseteq nR[x]. \tag{1.6}$$

Since $\prod_{j \neq i} f_j(g)R\mathbb{G} = \Gamma_i$, this implies (4).

In the general case, let $\mathbb{G}' = \mathbb{G}_1 \times \cdots \times \mathbb{G}_{t-1}$ and let n' and n'' be the order of \mathbb{G}' and \mathbb{G}_t , respectively. If $x^{n''} - 1 = f_1(x) \cdots f_s(x)$ is the factorization of $x^{n''} - 1$ into irreducible monic polynomials in $K[x]$ and ζ_{n_i} is a root of $f_i(x)$, the map $g_t \rightarrow \zeta_{n_i}$ gives an isomorphism $K\mathbb{G}/f_i(g_t)K\mathbb{G} \cong K(\zeta_{n_i})\mathbb{G}'$. Denoting $K(\zeta_{n_i})$ by K_i , we have $K\mathbb{G} \cong K_1\mathbb{G}' \oplus \cdots \oplus K_s\mathbb{G}'$. On the other hand, (1) implies that each $K_i\mathbb{G}'$ is a direct sum of cyclotomic fields $K_{i,j}$:

$$K_i\mathbb{G}' = K_{i,1} + \cdots + K_{i,s_i}.$$

Let R_i and $\mathfrak{o}_{i,j}$ be the rings of integers of K_i and $K_{i,j}$, respectively, and let $A_{i,j}$ be the kernel of the surjection of $R\mathbb{G}$ onto $\mathfrak{o}_{i,j}$. This surjection is given by the combined map $R\mathbb{G} \rightarrow R_i\mathbb{G}' \rightarrow \mathfrak{o}_{i,j}$. Since $f_i(g_t)R\mathbb{G}$ is the kernel of the surjection $R\mathbb{G} \rightarrow R_i\mathbb{G}'$, we see that

$$A_{i,j} \supseteq f_i(g_t)R\mathbb{G} \quad (j = 1, \dots, s_i), \tag{1.7}$$

and that the image $\bar{A}_{i,j}$ in $R_i\mathbb{G}'$ of $A_{i,j}$ is the kernel of $R_i\mathbb{G}' \rightarrow \mathfrak{o}_{i,j}$. Now for any distinct $A_{i,j}$ and $A_{h,k}$, we will show that $A_{i,j} + A_{h,k} \supseteq nR\mathbb{G}$. When \mathbb{G} is a cyclic group, this is given in (1.5). Then for any distinct k and k' , the induction hypothesis shows that $\bar{A}_{i,k} + \bar{A}_{i,k'} \supseteq n'R_i\mathbb{G}'$. Since n' divides n , this implies that $A_{i,k} + A_{i,k'} \supseteq nR\mathbb{G}$. On the other hand, for any distinct i and i' , we see easily that $f_i(g_t)R\mathbb{G} + f_{i'}(g_t)R\mathbb{G} \supseteq n''R$ similarly as in (1.4). Since n'' divides n , (1.7) shows that $A_{i,j} + A_{i',j'} \supseteq nR\mathbb{G}$. Let $\Gamma_{i,j}$ be the product of all $A_{h,k}$ but $A_{i,j}$. Then a simple calculation shows that $A_{i,j} + \Gamma_{i,j} \supseteq n^{2s_k-1}R\mathbb{G}$ from the above result, which proves (3). Let $A_{i,j} = \prod_{k \neq j} A_{i,k}$. Then by the induction hypothesis, there exists a positive integer l_i such that $\bar{A}_{i,1} + \cdots + \bar{A}_{i,s_i} \supseteq n^{l_i}R_i\mathbb{G}'$, which shows that

$$A_{i,1} + \cdots + A_{i,s_i} \supseteq n^{l_i}R\mathbb{G}, \tag{1.8}$$

Since $A_{h,k} + A_{h,k} \supseteq nR\mathfrak{G}$ for any distinct k and k' , it follows that $A_{h,1} \cdots A_{h,s_h} \supseteq n^{s_h(s_h-1)/2} (A_{h,1} \cap \cdots \cap A_{h,s_h})$. But each $A_{h,k}$ contains $f_h(g_t)R\mathfrak{G}$ from (1.6), so that $A_{h,1} \cdots A_{h,s_h} \supseteq n^{s_h(s_h-1)/2} f_h(g_t)R\mathfrak{G}$. Let $l' = \text{Max. } \{l_1, \dots, l_s\}$ and $l'' = \text{Max. } \left\{ \frac{1}{2} \sum_{h \neq 1} s_h(s_h - 1), \dots, \frac{1}{2} \sum_{h \neq s} s_h(s_h - 1) \right\}$. Then we have from (1.8)

$$\sum_{i,j} \Gamma_{i,j} = \sum_{i,j} \Delta_{i,j} \prod_{h \neq i} (A_{h,1} \cdots A_{h,s_h}) \supseteq n^{l''} n^{l'} \sum_i \prod_{h \neq i} f_h(g_t)R\mathfrak{G}.$$

As in (1.5) we have $\sum_i \prod_{h \neq i} f_h(g_t)R\mathfrak{G} \supseteq n^l R\mathfrak{G}$. Hence $l = l' + l''$ satisfies (4). This completes the proof of the proposition.

§ 2. The additive structure of $G(Z\mathfrak{G})$

We are now ready to investigate the additive structure of $G(Z\mathfrak{G})$ of an abelian p -group \mathfrak{G} . Let \mathfrak{G} be of order p^e and exponent p^{e_0} . We denote by ζ_d a primitive p^d -th root of 1.

From Proposition 1.1, $Q\mathfrak{G}$ is a direct sum of cyclotomic fields $K_i = Q(\zeta_{d_i})$ for some d_i such that $0 \leq d_i \leq e_0$ and the maximal order \mathfrak{o} of $Q\mathfrak{G}$ is also a direct sum of the maximal orders $\mathfrak{o}_i = Z[\zeta_{d_i}]$ of K_i . Furthermore, the surjection of $Z\mathfrak{G}$ onto \mathfrak{o}_i induced by π_i gives a ring isomorphism

$$Z\mathfrak{G}/A_i \cong \mathfrak{o}_i. \tag{2.1}$$

Let M be any regular (i.e. finitely generated and Z -torsion free) $Z\mathfrak{G}$ -module and let

$$M_i = \{m \in M : \lambda_i m = 0 \text{ for any } \lambda_i \in A_i\}.$$

Then M_i is a Z -pure submodule of M . Since A_i annihilates M_i , we may turn M_i into an \mathfrak{o}_i -module from (2.1). Clearly M_i is finitely generated and torsion free as an \mathfrak{o}_i -module, so that M_i is projective since \mathfrak{o}_i is a Dedekind ring. Thus M_i is isomorphic to the direct sum of $l_i - 1$ copies of \mathfrak{o}_i and an ideal \mathfrak{a} of \mathfrak{o}_i

$$M_i \cong \mathfrak{o}_i \oplus \cdots \oplus \mathfrak{o}_i \oplus \mathfrak{a}, \tag{2.2}$$

where the \mathfrak{o}_i -rank l_i of M_i and the ideal class $C_i(\mathfrak{a})$ of \mathfrak{a} are complete invariants of M_i (Curtis and Reiner [3]). By Proposition 1.1, (3), we have $M_i \cap (M_1 + \cdots + M_{i-1} + M_{i+1} + \cdots + M_s) = 0$. This shows that the sum of M_i is a direct sum. Now we denote by \overline{M} the quotient $M/\sum \oplus M_i$. Since $A_i \Gamma_i = 0$, \overline{M} is annihilated by $\Gamma_1 + \cdots + \Gamma_s$. Then Proposition 1.1, (4) implies that \overline{M} may be regarded as a module over $Z/(p^{el})\mathfrak{G}$ for some positive integer l . But the

only irreducible $Z/(p^{el})\mathfrak{G}$ -module is $Z/(p)$ on which \mathfrak{G} acts trivially. Hence \overline{M} has a composition series with factors $Z/(p)$. The sequence

$$0 \rightarrow Z \xrightarrow{p} Z \rightarrow Z/(p) \rightarrow 0$$

shows that $[Z/(p)] = 0$ in $G(Z\mathfrak{G})$, where $[Z/(p)]$ means the element of $G(Z\mathfrak{G})$ associated with $Z/(p)$, so that $[\overline{M}] = 0$ in $G(Z\mathfrak{G})$. This implies that $[M] = \sum [M_i]$. For any ideal \mathfrak{a} of \mathfrak{o}_i we denote by \mathfrak{a}_i^* the element $[\mathfrak{a}] - [\mathfrak{o}_i]$ of $G(Z\mathfrak{G})$. The map $\mathfrak{a} \rightarrow \mathfrak{a}_i^*$ defines a homomorphism of the ideal class group of \mathfrak{o}_i to $G(Z\mathfrak{G})$, and from (2.2), any element x of $G(Z\mathfrak{G})$ may be written in the form

$$x = \sum_i (l_i [\mathfrak{o}_i] + \mathfrak{a}_i^*) \quad (l_i \in Z).$$

The uniqueness of this expression follows immediately from the following proposition.

PROPOSITION 2.1. *For any exact sequence of regular $Z\mathfrak{G}$ -modules*

$$0 \rightarrow M' \rightarrow M \xrightarrow{\psi} M'' \rightarrow 0, \tag{2.3}$$

we have $C_i(\mathfrak{a}) = C_i(\mathfrak{a}') \cdot C_i(\mathfrak{a}'')$, where $C_i(\mathfrak{a})$, $C_i(\mathfrak{a}')$ and $C_i(\mathfrak{a}'')$ are ideal class invariants of M_i , M'_i and M''_i , respectively.

Proof. The sequence (2.3) induces an exact sequence

$$0 \rightarrow \text{Hom}_{Z\mathfrak{G}}(\mathfrak{o}_i, M') \rightarrow \text{Hom}_{Z\mathfrak{G}}(\mathfrak{o}_i, M) \rightarrow \text{Hom}_{Z\mathfrak{G}}(\mathfrak{o}_i, M'') \rightarrow \text{Ext}_{Z\mathfrak{G}}^1(\mathfrak{o}_i, M').$$

But $\text{Hom}_{Z\mathfrak{G}}(\mathfrak{o}_i, M)$ is isomorphic to M_i by the map $f \rightarrow f(1)$. Hence we have an exact sequence

$$0 \rightarrow M'_i \rightarrow M_i \rightarrow M''_i \rightarrow \text{Ext}_{Z\mathfrak{G}}^1(\mathfrak{o}_i, M').$$

Since the order p^e of \mathfrak{G} annihilates $\text{Ext}_{Z\mathfrak{G}}^1(\mathfrak{o}_i, M')$ (Cartan and Eilenberg [2]), we see that

$$p^e M''_i \subseteq \psi(M_i) \subseteq M''_i, \tag{2.4}$$

where $\psi(M_i)$ is also a projective \mathfrak{o}_i -module whose \mathfrak{o}_i -rank is equal to that of M''_i . Thus by Invariant factor theorem ([3]), there exist elements u_1, \dots, u_i of M''_i and ideals $\mathfrak{b}_1, \dots, \mathfrak{b}_i$ of \mathfrak{o}_i such that

$$\begin{aligned} M''_i &= \mathfrak{o}_i u_1 \oplus \dots \oplus \mathfrak{o}_i u_{i-1} \oplus \mathfrak{a}'' u_i \\ \psi(M_i) &= \mathfrak{b}_1 u_1 \oplus \dots \oplus \mathfrak{b}_{i-1} u_{i-1} \oplus \mathfrak{b}_i \mathfrak{a}'' u_i. \end{aligned}$$

Then the inclusion (2.4) shows that each b_k divides (p^e) . But p is a power of the principal prime ideal $(1 - \zeta_{d_i})$ of \mathfrak{o}_i , which implies that b_k is also a principal ideal. Then $C_i(b_1 \cdots b_t a'') = C_i(a'')$. Furthermore, M_i is isomorphic to the direct sum of M_i' and $\phi(M_i)$ since $\phi(M_i)$ is projective. Therefore $C_i(a) = C_i(a') \cdot C_i(b_1 \cdots b_t a'')$, which coincides with $C_i(a') \cdot C_i(a'')$. This completes the proof.

THEOREM 2.1. *If \mathfrak{G} is an abelian p -group, $G(Z\mathfrak{G})$ is isomorphic to the direct sum of $C_0(\mathfrak{o})$ and $G(Q\mathfrak{G})$ as an additive group*

$$G(Z\mathfrak{G}) \cong C_0(\mathfrak{o}) \oplus G(Q\mathfrak{G}). \tag{2.5}$$

Proof. Since \mathfrak{o} is the direct sum of the \mathfrak{o}_i , $C_0(\mathfrak{o}) = \sum \oplus C_0(\mathfrak{o}_i)$ and each $C_0(\mathfrak{o}_i)$ is isomorphic to the ideal class group of \mathfrak{o}_i (Rim [4]). Then the map $C_i(a) \rightarrow a_i^*$ defines a homomorphism $\phi : C_0(\mathfrak{o}) \rightarrow G(Z\mathfrak{G})$, where the action of \mathfrak{G} on a is given by setting $g \cdot a = \pi_i(g)\alpha$, $g \in \mathfrak{G}$, $\alpha \in a$. On the other hand, $[K_1], \dots, [K_s]$ make a base for $G(Q\mathfrak{G})$. We define a linear map $\varphi : G(Q\mathfrak{G}) \rightarrow G(Z\mathfrak{G})$ by $\varphi([K_i]) = [o_i]$. Then we have an additive isomorphism $C_0(\mathfrak{o}) \oplus G(Q\mathfrak{G}) \rightarrow G(Z\mathfrak{G})$ by $(x, y) \rightarrow \phi(x) + \varphi(y)$ because the image $\phi(x) + \varphi(y)$ in $G(Z\mathfrak{G})$ is uniquely determined by Proposition 2.1. This proves Theorem 2.1.

§ 3. Ring structure

We will now study the multiplicative structure of $G(Z\mathfrak{G})$. In (2.5), Swan [6] showed that $\phi(C_0(\mathfrak{o}))^2 = 0$. Hence $G(Z\mathfrak{G})$ is a Z -algebra extension over an abelian kernel, and is determined by the action of $G(Q\mathfrak{G})$ to $C_0(\mathfrak{o})$ and the associated 2-cohomology class of $H^2(G(Q\mathfrak{G}), C_0(\mathfrak{o}))$.

In this section we denote by p^{e_h} the order of a cyclic factor \mathfrak{G}_h of \mathfrak{G} . As in § 2, each $\pi_i(g_h)$ is of the form $\zeta_{d_i}^{i_h}$ for some integer i_h such that $0 \leq i_h \leq e_0$, which satisfies $i_h p^{e_h} \equiv 0 \pmod{p^{d_i}}$. In general, given a t -tuple (ξ_1, \dots, ξ_t) of integers which satisfy that $\xi_h p^{e_h} \equiv 0 \pmod{p^{d_i}}$ for each h , we may construct a regular $Z\mathfrak{G}$ -module as follows. Let a be an ideal of $Z[\zeta_{d_i}]$. We turn a into a regular $Z\mathfrak{G}$ -module by defining

$$g_h \cdot \alpha = \zeta_{d_i}^{i_h} \alpha, \quad \alpha \in a.$$

We denote this module by $(a; \xi_1, \dots, \xi_t)$. In particular, for the t -tuple (i_1, \dots, i_t) , i_h being as above, we denote $(a; i_1, \dots, i_t)$ by a_i . Then the element a_i^* of $G(Z\mathfrak{G})$ can be written in the form $[a_i] - [o_i]$.

PROPOSITION 3.1. *For any ideal \mathfrak{a} of $Z[\zeta_{d_i}]$, $(\mathfrak{a}; \xi_1, \dots, \xi_t)$ is reducible if and only if every ξ_h is divisible by p .*

Proof. $(\mathfrak{a}; \xi_1, \dots, \xi_t)$ is reducible if and only if $Q \otimes_Z (\mathfrak{a}; \xi_1, \dots, \xi_t)$ is reducible. Let $Q \otimes_Z (\mathfrak{a}; \xi_1, \dots, \xi_t)$ be reducible. Then this contains, as a direct summand, K_j for some j such that $d_j < d_i$ and each g_h acts on K_j as the multiplication of $\zeta_{d_j}^{\xi_h}$. This shows that every ξ_h is divisible by p . Conversely let every ξ_h be divisible by p and let $p^{d_i-d_j}$ be the highest power of p which divides every ξ_h . Set $\xi_h = \xi'_h \cdot p^{d_i-d_j}$. Then $Q \otimes_Z (Z[\zeta_{d_j}]; \xi'_1, \dots, \xi'_t)$ is obviously a direct summand of $Q \otimes_Z (\mathfrak{a}; \xi_1, \dots, \xi_t)$. This proves the proposition.

PROPOSITION 3.2. *Let \mathfrak{a} be any ideal of $Z[\zeta_{d_i}]$. If $(\mathfrak{a}; \xi_1, \dots, \xi_t)$ is irreducible, there exist some j and an ideal \mathfrak{b} of $Z[\zeta_{d_j}]$ such that $d_j = d_i$ and $(\mathfrak{a}; \xi_1, \dots, \xi_t) \cong \mathfrak{b}_j$ as $Z\mathfrak{G}$ -modules. Otherwise, there exist some j and an ideal \mathfrak{b} of $Z[\zeta_{d_j}]$ such that $d_j < d_i$ and $(\mathfrak{a}; \xi_1, \dots, \xi_t) \cong \mathfrak{o}_j \oplus \dots \oplus \mathfrak{o}_j \oplus \mathfrak{b}_j$ ($p^{d_i-d_j}$ summands) as $Z\mathfrak{G}$ -modules.*

Proof. Let $(\mathfrak{a}; \xi_1, \dots, \xi_t)$ be irreducible. Then this is annihilated by only one A_j , so that this can be regarded as an \mathfrak{o}_j -module as in §2. By the irreducibility, $(\mathfrak{a}; \xi_1, \dots, \xi_t)$ is, then, isomorphic to some \mathfrak{b}_j . Hence the Z -rank of \mathfrak{o}_j is equal to that of \mathfrak{o}_i , and we have $d_j = d_i$. This proves the first assertion.

Let $(\mathfrak{a}; \xi_1, \dots, \xi_t)$ be reducible. Then each ξ_h is divisible by p (Proposition 3.1). Let $p^{d_i-d_{j'}}$ be the highest power of p which divides every ξ_h and let $\xi_h = \xi'_h \cdot p^{d_i-d_{j'}}$. Then each g_h acts on $(\mathfrak{a}; \xi_1, \dots, \xi_t)$ as the multiplication of $\zeta_{d_i}^{\xi_h} = \zeta_{d_{j'}}^{\xi'_h}$. Since \mathfrak{a} is, as a $Z[\zeta_{d_{j'}}]$ -module, finitely generated and projective, \mathfrak{a} is isomorphic to the direct sum of $p^{d_i-d_{j'}} - 1$ copies of $Z[\zeta_{d_{j'}}]$ and an ideal \mathfrak{b}' of $Z[\zeta_{d_{j'}}]$. Then we have a $Z\mathfrak{G}$ -isomorphism

$$(\mathfrak{a}; \xi_1, \dots, \xi_t) \cong (Z[\zeta_{d_{j'}}]; \xi'_1, \dots, \xi'_t) \oplus \dots \oplus (Z[\zeta_{d_{j'}}]; \xi'_1, \dots, \xi'_t) \oplus (\mathfrak{b}'; \xi'_1, \dots, \xi'_t), \tag{3.1}$$

where each summand is irreducible. Hence, there exist some j and ideals \mathfrak{c} and \mathfrak{b} such that $d_j = d_{j'}$, $(Z[\zeta_{d_{j'}}]; \xi'_1, \dots, \xi'_t) \cong \mathfrak{c}_j$ and $(\mathfrak{b}'; \xi'_1, \dots, \xi'_t) \cong \mathfrak{b}_j$ (the first assertion). Setting $\mathfrak{b} = \mathfrak{c}^{p^{d_i-d_{j'}}-1} \cdot \mathfrak{b}$, we have

$$(\mathfrak{a}; \xi_1, \dots, \xi_t) \cong \mathfrak{o}_j \oplus \dots \oplus \mathfrak{o}_j \oplus \mathfrak{b}_j.$$

This proves the second assertion and completes the proof of the proposition.

COROLLARY 3.1. *If $(Z[\xi_{d_i}] ; \xi_1, \dots, \xi_t)$ is irreducible, there exists some j such that $d_j = d_i$ and $(Z[\zeta_{d_i}] ; \xi_1, \dots, \xi_t) \cong \mathfrak{o}_j$. Otherwise, there exists some j such that $d_j < d_i$ and $(Z[\zeta_{d_j}] ; \xi_1, \dots, \xi_t) \cong \mathfrak{o}_j \oplus \dots \oplus \mathfrak{o}_j$ ($p^{d_i-d_j}$ summands).*

Proof. According to Artin [1] $(D/\Delta)^{1/2}$ is the ideal class invariant of $Z[\zeta_{d_i}]$ as a $Z[\zeta_{d_j}]$ -module, where D is the discriminant of $Z[\zeta_{d_i}]$ over $Z[\zeta_{d_j}]$ and Δ is the discriminant of any equation defining the extension of $Q(\zeta_{d_i})$ over $Q(\zeta_{d_j})$. But it is easily checked that $(D/\Delta)^{1/2}$ divides some power of p . Then $(D/\Delta)^{1/2}$ is a principal ideal. Hence, by Proposition 3.2, it is sufficient to prove that \mathfrak{b} is a principal ideal. Let τ be the isomorphism $(Z[\zeta_{d_i}] ; \xi_1, \dots, \xi_t) \cong \mathfrak{b}_j$. Since $Z[\zeta_{d_i}]$ is generated by 1, \mathfrak{b} is generated by $\tau(1)$. This shows that \mathfrak{b} is a principal ideal, which completes the proof.

PROPOSITION 3.3. *Let \mathfrak{a} be any ideal of $Z[\zeta_{d_i}]$ and let σ be a Galois automorphism of $Q(\zeta_{d_i})$. If $\zeta_{d_i}^\sigma = \zeta_{d_i}^\nu$, then*

$$(\mathfrak{a} ; \xi_1, \dots, \xi_t) \cong (\mathfrak{a}^\sigma ; \xi_1^\nu, \dots, \xi_t^\nu).$$

Proof. This follows immediately from the comparison of actions of \mathfrak{G} to the both sides.

LEMMA 3.1. *If $d_i \geq d_j$, then for any ideal \mathfrak{a} of $Z[\zeta_{d_i}]$ we have*

$$[\mathfrak{o}_j][\mathfrak{a}_i] = \sum_{\sigma_\nu \in G_{d_j}} [(\mathfrak{a} : i_1 + j_1 \nu p^{d_i-d_j}, \dots, i_t + j_t \nu p^{d_i-d_j})],$$

where G_{d_j} denotes the Galois group of $Q(\zeta_{d_j})$ and σ_ν denotes an element of G_{d_j} such that $\zeta_{d_j}^{\sigma_\nu} = \zeta_{d_j}^\nu$.

Proof. Let $\Phi_{d_j}(x)$ be the cyclotomic polynomial of index p^{d_j} . Then we have $\mathfrak{o}_j \cong Z[x]/\Phi_{d_j}(x)Z[x]$. This implies the isomorphism

$$\mathfrak{o}_j \otimes_Z \mathfrak{a}_i \cong \mathfrak{a}[x]/\Phi_{d_j}(x)\mathfrak{a}[x].$$

Let $M = \mathfrak{a}_i[x]/\Phi_{d_j}(x)\mathfrak{a}_i[x]$. \mathfrak{G} operates on M by $g_h m = \zeta_{d_i}^{ih} x^{jh} \cdot m$, $m \in M$. The assumption $d_i \geq d_j$ implies that $\Phi_{d_j}(x)$ factorizes into $\prod_{\sigma_\nu \in G_{d_j}} (x - \zeta_{d_j}^\nu)$ in $\mathfrak{o}_i[x]$. Let $\sigma_{\nu_1}, \dots, \sigma_{\nu_t}$ be the elements of G_{d_j} and let $M_k = (x - \zeta_{d_j}^{\nu_1}) \cdots (x - \zeta_{d_j}^{\nu_t})M$. Then we have a series of submodules of M

$$M \supseteq M_1 \supseteq \dots \supseteq M_t = 0.$$

Each quotient M_{k-1}/M_k is $a_i[x]/(x - \zeta_{d_j}^{v_k})a_i[x]$, which is isomorphic to a by the map $x \rightarrow \zeta_{d_j}^{v_k}$. But this map carries $\zeta_{d_i}^{i_h} x^{j_h}$ into $\zeta_{d_i}^{i_h} \zeta_{d_j}^{j_h v_k} = \zeta_{d_i}^{i_h + j_h v_k p^{a_i - a_j}}$. Then each M_{k-1}/M_k is, as a $Z\mathcal{G}$ -module, isomorphic to $(a : i_1 + j_1 v_k p^{d_i - d_j}, \dots, i_t + j_t v_k p^{d_i - d_j})$. Since M is composed from these modules by forming extensions, we conclude that

$$[M] = \sum_{\sigma_v \in G_{d_j}} [(a : i_1 + j_1 v p^{d_i - d_j}, \dots, i_t + j_t v p^{d_i - d_j})].$$

This proves the lemma.

Now we will prove that Z -algebra extension (2.5) splits.

THEOREM 3.1. *The linear map φ defined in the proof of Theorem 2.1 is a ring homomorphism. Hence the Z -algebra extension (2.5) splits.*

Proof. Take any two generators $[K_i]$ and $[K_j]$ of $G(Q\mathcal{G})$. We may assume that $d_i \geq d_j$. From Lemma 3.1, we have

$$[0_j][0_i] = \sum_{\sigma_v \in G_{d_j}} [(Z[\zeta_{d_i}] : i_1 + j_1 v p^{d_i - d_j}, \dots, i_t + j_t v p^{d_i - d_j})].$$

But each term of the right hand is equal to either $[0_k]$ for some k such that $d_k = d_i$ or a direct sum of $p^{d_i - d_{k'}}$ copies of $[0_{k'}]$ for some k' such that $d_{k'} < d_i$ (Corollary 3.1). Then we have

$$[0_j][0_i] = \sum_{d_k = d_i} [0_k] + \sum_{d_{k'} < d_i} p^{d_i - d_{k'}} [0_{k'}].$$

This shows that φ is a ring homomorphism, and this completes the proof of Theorem 3.1.

LEMMA 3.2. *If $d_i \leq d_j$, then for any ideal a of $Z[\zeta_{d_i}]$*

$$[0_j][a_i] = \sum_{\sigma_v \in G_{d_i}} [(a : i_1 p^{d_j - d_i} + j_1 v, \dots, i_t p^{d_j - d_i} + j_t v)],$$

where \tilde{a} denotes $aZ[\zeta_{d_j}]$.

Proof. Notice that if $d_i \leq d_j$, the cyclotomic polynomial $\Phi_{d_j}(x)$ factorizes into $\prod_{\sigma_v \in G_{d_i}} (x^{p^{d_j - d_i}} - \zeta_{d_i}^v)$ in $a_i[x]$ and $\zeta_{d_j}^v$ is a root of $x^{p^{d_j - d_i}} - \zeta_{d_i}^v$. Then the lemma is proved by the same method as the proof of Lemma 3.1.

Let a be any ideal of $Z[\zeta_{d_i}]$ and (ξ_1, \dots, ξ_t) be any t -tuple of integers such that $\xi_h p^{e_h} \equiv 0 \pmod{p^{d_i}}$. We denote the element $[(a : \xi_1, \dots, \xi_t)] - [(Z[\zeta_{d_i}] : \xi_1, \dots, \xi_t)]$ by $(a : \xi_1, \dots, \xi_t)^*$. Then $(a : \xi_1, \dots, \xi_t)^*$ is obviously

contained in $\phi(C_0(\mathfrak{o}))$.

THEOREM 3.2. *For any \mathfrak{a}_i^* of $\phi(C_0(\mathfrak{o}_i))$, each generator $[K_j]$ of $G(Q\mathfrak{G})$ acts on \mathfrak{a}_i^* as follows.*

$$[K_j]\mathfrak{a}_i^* = \begin{cases} \sum_{\sigma\nu \in G_{a_j}} (\mathfrak{a} : i_1 + j_1\nu p^{d_i-d_j}, \dots, i_t + j_t\nu p^{d_i-d_j})^* & \text{if } d_i \geq d_j. \\ \sum_{\sigma\nu \in G_{\nu_i}} (\tilde{\mathfrak{a}} : i_1 p^{d_j-d_i} + j_1\nu, \dots, i_t p^{d_j-d_i} + j_t\nu)^* & \text{if } d_i \leq d_j. \end{cases}$$

Proof. The action of $[K_j]$ on $\phi(C_0(\mathfrak{o}))$ is given by the multiplication of $\varphi([K_j]) = [\mathfrak{o}_j]$. Then this theorem follows immediately from preceding two lemmas.

§ 4. Example

Let \mathfrak{G} be an abelian group of type (p, p^e) , that is, \mathfrak{G} be a direct product of cyclic groups $\mathfrak{G}_1 = (g_1)$ and $\mathfrak{G}_2 = (g_2)$ of order p and p^e , respectively. In this case we can describe more explicitly the action of $G(Q\mathfrak{G})$ to $(C_0(\mathfrak{o}))$. In this section we denote by ζ_i a primitive p^i -th root of 1 for any integer i such that $1 \leq i \leq e$.

Let \mathfrak{a} be any ideal of $Z[\zeta_i]$ and let ν be any integer such that $0 \leq \nu \leq p-1$. We denote $(\mathfrak{a} : p^{i-1}\nu, 1)$ by $\mathfrak{a}_{i,\nu}$. Put $\mathfrak{o}_{i,\nu} = (Z[\zeta_i])_{i,\nu}$ and $K_{i,\nu} = Q \otimes_{\mathbb{Z}} \mathfrak{o}_{i,\nu}$. Furthermore; for any ideal \mathfrak{a} of $Z[\zeta_i]$ we denote $(\mathfrak{a} : 1, 0)$ by \mathfrak{a}_0 . Put $\mathfrak{o}_0 = (Z[\zeta_1])_0$ and $K_0 = Q \otimes_{\mathbb{Z}} \mathfrak{o}_0$. Then we see that

$$Q\mathfrak{G} = Q \oplus K_0 \oplus \sum_{i=1}^e \sum_{\nu=0}^{p-1} K_{i,\nu}$$

and that

$$C_0(\mathfrak{o}) = C_0(\mathfrak{o}_0) \oplus \sum_{i=1}^e \sum_{\nu=0}^{p-1} C_0(\mathfrak{o}_{i,\nu}).$$

1. $[Q]$ acts on $\phi(C_0(\mathfrak{o}))$ trivially.
2. The action of $[K_0]$ on $\phi(C_0(\mathfrak{o}_0))$.

For any element \mathfrak{a}_0^* of $\phi(C_0(\mathfrak{o}_0))$ it follows immediately from Theorem 3.2 and Proposition 3.3 that

$$\begin{aligned} [K_0]\mathfrak{a}_0^* &= \sum_{\sigma\mu \in G_1} (\mathfrak{a} ; 1 + \mu, 0)^* \\ &= \sum_{\substack{\sigma\mu \in G_1 \\ \mu \not\equiv -1 \pmod{p}}} (\mathfrak{a}^{\sigma_{1+\mu}^{-1}} ; 1, 0)^* + (\mathfrak{a} ; 0, 0)^* = \sum_{\substack{\sigma\mu \in G_1 \\ \mu \not\equiv -1 \pmod{p}}} (\mathfrak{a}^{\sigma_{1+\mu}^{-1}})_0^* \end{aligned}$$

since $(\mathfrak{a} : 0, 0)^* = (Z : 0, 0)^* = 0$ by Proposition 3.2. On the other hand, $\sigma_{1+\mu}^{-1}$ such that $\mu \not\equiv -1 \pmod{p}$ ranges over all elements of G_1 but σ_1 . Then

$\prod_{\substack{\sigma_\mu \in G_1 \\ \mu \not\equiv -1 \pmod{p}}} \alpha^{\sigma_{1+\mu}^{-1}} = N_{1/0}(\alpha)\alpha^{-1}$, where $N_{i/0}$ means the norm of $Z[\zeta_i]$ over Z . Since $N_{i/0}(\alpha)$ is a principal ideal, $(N_{i/0}(\alpha))_0^* = 0$. Hence we conclude that

$$[K_0]a_0^* = -\alpha_0^*.$$

3. The action of $[K_0]$ on $\phi(C_0(0_i))$.

It follows immediately from Theorem 3.2 that

$$[K_0]a_{i,\nu}^* = \sum_{\sigma_\mu \in G_1} (\alpha ; p^{i-1}(\nu + \mu), 1)^*,$$

where $\nu + \mu$ ranges over $0, 1, \dots, \nu - 1, \nu + 1, \dots, p - 1 \pmod{p}$. Hence,

$$[K_0]a_{i,\nu}^* = \sum_{\mu=0, \mu \neq \nu}^{p-1} a_{i,\mu}^*.$$

4. The action of $[K_i, \nu]$ on $\phi(C_0(0_0))$.

Let x_μ be an integer such that $\mu x_\mu \equiv 1 \pmod{p^i}$. Then Theorem 3.2 and Proposition 3.3 imply that

$$[K_i, \nu]a_0^* = \sum_{\sigma_\mu \in G_1} (\tilde{\alpha} ; p^{i-1}(1 + \nu\mu), \mu)^* = \sum_{\sigma_\mu \in G_1} (\tilde{\alpha}^{\sigma_\mu^{-1}} ; p^{i-1}(x_\mu + \nu), 1)^*.$$

But we can easily check that $x_\mu + \nu$ ranges over $0, 1, \dots, p - 1 \pmod{p}$. Hence we have

$$[K_i, \nu]a_0^* = \sum_{\sigma_\mu \in G_1} (\tilde{\alpha}^{\sigma_\mu})_{i,\nu+\mu}^*.$$

5. The action of $[K_j, \nu]$ on $\phi(C_0(0_i, \nu))$.

The case $i > j$. Let y_μ be an integer such that $(1 + p^{i-j}\mu)y_\mu \equiv 1 \pmod{p^i}$. Then Theorem 3.2 and Proposition 3.3 imply that

$$\begin{aligned} [K_j, \nu]a_{i,\nu'}^* &= \sum_{\sigma_\mu \in G_j} (\alpha ; p^{i-1}(\nu' + \nu\mu), 1 + p^{i-j}\mu)^* \\ &= \sum_{\sigma_\mu \in G_j} (\alpha^{\sigma y_\mu} ; p^{i-1}(\nu' + \nu\mu), 1)^* \end{aligned}$$

because $y_\mu \equiv 1 \pmod{p}$. In general we denote by $G_{i/j}$ the Galois group of $Q(\zeta_i)$ over $Q(\zeta_j)$. Then $G_j = \bigcup_{\lambda=1}^{p-1} G_{j/1} \cdot \sigma_\lambda$ and $\nu' + \nu\mu \equiv \nu' + \nu\lambda \pmod{p}$ for any element σ_μ of $G_{j/1} \cdot \sigma_\lambda$. This shows that

$$[K_j, \nu]a_{i,\nu'}^* = \sum_{\lambda=1}^{p-1} \left(\prod_{\sigma_\mu \in G_{j/1} \cdot \sigma_\lambda} \alpha^{\sigma y_\mu} \right)_{i,\nu'+\nu\lambda}^*.$$

The case $i = j$. For each μ such that $\mu \not\equiv -1 \pmod{p}$, let x_μ be an integer such that $(1 + \mu)x_\mu \equiv 1 \pmod{p^i}$. Then Theorem 3.2 and Proposition 3.3 imply

that

$$\begin{aligned}
 [K_{i, \nu}]a_{i, \nu}^* &= \sum_{\substack{\sigma_\mu \in G_i \\ \mu \not\equiv -1 \pmod{p}}} (\alpha^{\sigma_\mu} ; p^{i-1}(\nu' + \nu\mu) x_\mu, 1)^* \\
 &+ \sum_{\substack{\sigma_\mu \in G_i \\ \mu \equiv -1 \pmod{p}}} (\alpha ; p^{i-1}(\nu' + \nu\mu), 1 + \mu)^*. \tag{4.1}
 \end{aligned}$$

In the first term of the right hand side, σ_{x_μ} ranges over $\bigcup_{\lambda=2}^{p-1} G_{i/\lambda} \cdot \sigma_\lambda$ and $(\nu' + \nu\mu)x_\mu \equiv (\nu' - \nu)\lambda + \nu \pmod{p}$ for any σ_{x_μ} of $G_{i/\lambda} \cdot \sigma_\lambda$. Then the first term of (4.1) is equal to

$$\sum_{\lambda=2}^{p-1} \left(\prod_{\sigma \in G_{i/\lambda} \cdot \sigma_\lambda} \alpha^\sigma \right)_{i, (\nu' - \nu)\lambda + \nu}^* = \sum_{\lambda=2}^{p-1} (N_{i/\lambda}(\alpha)^{\sigma_\lambda})_{i, (\nu' - \nu)\lambda + \nu}^*.$$

In particular, if $\nu' = \nu$, this is equal to $-(N_{i/1}(\alpha))_{i, \nu}^*$. In the second term of (4.1), let p^h be the highest power of p which divides $1 + \mu$ and set $1 + \mu = \mu_h \cdot p^h$. Then (3.1) implies that

$$(\alpha ; p^{i-1}(\nu' + \nu\mu), 1 + \mu)^* = (N_{i/i-h}(\alpha) ; p^{i-h-1}(\nu' - \nu), \mu_h)^*$$

since the ideal class of α as a $Z[\zeta_{i-h}]$ -module is the norm $N_{i/i-h}(\alpha)$ of α from $Z[\zeta_i]$ to $Z[\zeta_{i-h}]$ ([1]). When σ_μ ranges over elements of G_i such that $1 + \mu \equiv 0 \pmod{p^h}$ and $1 + \mu \not\equiv 0 \pmod{p^{h+1}}$, $\sigma_{\mu_h}^{-1}$ obviously ranges over the elements of $G_{i-h} = \bigcup_{\lambda=1}^{p-1} G_{i-h/\lambda} \cdot \sigma_\lambda$ and $(\nu' - \nu)\gamma \equiv (\nu' - \nu)\lambda \pmod{p}$ for any σ_γ of $G_{i-h/\lambda} \cdot \sigma_\lambda$. Hence the second term of (4.1) is equal to

$$\begin{aligned}
 &\sum_{h=1}^{i-1} \sum_{\lambda=1}^{p-1} \left(\prod_{\sigma \in G_{i-h/\lambda} \cdot \sigma_\lambda} N_{i/i-h}(\alpha)^\sigma \right)_{i-h, (\nu' - \nu)\lambda}^* + (N_{i/1}(\alpha) ; \nu' - \nu, 0)^* \\
 &= \sum_{h=1}^{i-1} \sum_{\lambda=1}^{p-1} (N_{i/1}(\alpha)^{\sigma_\lambda})_{i-h, (\nu' - \nu)\lambda}^* + (N_{i/1}(\alpha) ; \nu' - \nu, 0)^*,
 \end{aligned}$$

where if $\nu' \not\equiv \nu$, $(N_{i/1}(\alpha) ; \nu' - \nu, 0)^* = (N_{i/1}(\alpha)^{\sigma_{\nu' - \nu}})_0^*$ and if $\nu' = \nu$, $(N_{i/1}(\alpha) ; \nu' - \nu, 0)^* = 0$ and $\sum_{\lambda=1}^{p-1} (N_{i/1}(\alpha)^{\sigma_\lambda})_{i-h, (\nu' - \nu)\lambda}^* = (N_{i/0}(\alpha))_{i-h, 0}^* = 0$ since $N_{i/0}(\alpha)$ is a principal ideal. The case $i < j$. From Theorem 3.2 we have

$$[K_{j, \nu}]a_{i, \nu}^* = \sum_{\sigma_\mu \in G_i} (\tilde{\alpha} ; p^{j-1}(\nu' + \nu\mu), p^{j-i} + \mu)^*.$$

Let x_μ be an integer such that $(p^{j-i} + \mu)x_\mu \equiv 1 \pmod{p^j}$. Then $(\tilde{\alpha} ; p^{j-1}(\nu' + \nu\mu), p^{j-i} + \mu)^* = (\tilde{\alpha}^{\sigma_{x_\mu}})_{j, \nu'x_\mu + \nu}^*$ by Proposition 3.3, σ_{x_μ} ranges over the elements of G_i , and $\nu'x_\mu + \nu \equiv \nu'\lambda + \nu \pmod{p}$ for any σ_{x_μ} of $G_{i/\lambda} \cdot \sigma_\lambda$. This shows that

$$[K_{j, \nu}]a_{i, \nu}^* = \sum_{\lambda=1}^{p-1} \left(\prod_{\sigma \in G_{i/\lambda} \cdot \sigma_\lambda} \tilde{\alpha}^\sigma \right)_{j, \nu'\lambda + \nu}^* = \sum_{\lambda=1}^{p-1} (\widetilde{N}_{i/1}(\alpha)^{\sigma_\lambda})_{j, \nu'\lambda + \nu}^*.$$

Summalizing, we have

PROPOSITION 4.1. *Let \mathcal{G} be an abelian group of type (p, p^e) . Then $G(Q\mathcal{G})$ acts on $\phi(C_0(\mathfrak{b}))$ as follows.*

1. $[Q]$ acts trivially.
2. $[K_0]a_0^* = -a_0^*$.
3. $[K_0]a_{i,\nu}^* = \sum_{\mu=0, \neq \nu}^{p-1} a_{i,\mu}^*$.
4. $[K_{i,\nu}]a_0^* = \sum_{\lambda=1}^{p-1} (\tilde{a}^{\sigma\lambda})_{i,\nu+\lambda}^*$.
5. $[K_{j,\nu}]a_{i,\nu'}^*$

$$= \begin{cases} \sum_{\lambda=1}^{p-1} \left(\prod_{\sigma\mu \in Gi/1, \sigma\lambda} a^{\sigma y\mu} \right)_{i,\nu'+\nu\lambda}^*, & \text{where } \sigma y\mu = \sigma_{1+p^i-j\mu}^{-1} \quad (i > j). \\ \sum_{\lambda=2}^{p-1} (N_{i/1}(a)^{\sigma\lambda})_{i,(\nu'-\nu)\lambda+\nu}^* + \sum_{h=1}^{i-1} \sum_{\lambda=1}^{p-1} (N_{i/1}(a)^{\sigma\lambda})_{i-h,(\nu'-\nu)\lambda}^* + (N_{i/1}(a)^{\sigma\nu'-\nu})_0^*, & (\nu' \neq \nu) \\ - (N_{i/1}(a))_{i,\nu}^*, & (\nu' = \nu) \\ \sum_{\lambda=1}^{p-1} (\widetilde{N}_{i/1}(a)^{\sigma\lambda})_{j,\nu'+\nu}^* & (i < j). \end{cases} \quad (i = j).$$

BIBLIOGRAPHY

[1] E. Artin: Questions de base minimale dans la théorie de nombres algébriques, Colloq. Int. Cent. Nat. Rech. Sci. **24** (1950), 19-20.
 [2] H. Cartan and S. Eilenberg: Homological algebra, Princeton University Press, 1956.
 [3] C. W. Curtis and I. Reiner: Representation theory of finite groups and associative algebras, Int. Sci. Press, 1962.
 [4] D. S. Rim: On projective class groups, Trans. Amer. Math. Soc. **98** (1961), 459-467.
 [5] R. G. Swan: Induced representations and projective modules, Ann. Math. **71** (1960), 552-578.
 [6] R. G. Swan: The Grothendieck ring of a finite group, Topology, vol. **2** (1963), 85-110.

Tokyo University of Education