Tôhoku Math. Journ.
32 (1980), 49-62.

A NORMAL INTEGRAL BASIS THEOREM FOR DIHEDRAL GROUPS

Dedicated to Professor Yoshikazu Nakai on his sixtieth birthday

TAKEHIKO MIYATA

(Received February 19, 1979, revised May 28, 1979)

1. Statement of the main theorem and its consequences. Let D_n be a dihedral group of order $2n$ generated by σ and τ with relations $\sigma^n = \tau^2 = 1$ and $\tau^{-1}\sigma\tau = \sigma^{-1}$. Set $C_n = \langle\sigma\rangle$. Then C_n is a normal subgroup of D_n. Throughout this paper all modules will be finitely generated left modules. The main result of this paper is

MAIN THEOREM 1.1. *Let P be a projective $\boldsymbol{Z}D_n$-module. Then P is free if and only if P is free as a $\boldsymbol{Z}C_n$-module.*

Let A be an order in a finite dimensional semi-simple $\boldsymbol{Q}$-algebra $\boldsymbol{Q}A$. $C(A)$ denotes the locally free class group of A. Let $B \subseteq \boldsymbol{Q}A$ be a maximal order containing A. Then the kernel $D(A)$ of the natural homomorphism of $C(A)$ onto $C(B)$ does not depend on the choice of B. Viewing projective $\boldsymbol{Z}D_n$-modules as $\boldsymbol{Z}C_n$-modules we obtain the restriction map

$$\mathbf{res}\colon C(\boldsymbol{Z}D_n) \to C(\boldsymbol{Z}C_n) .$$

It is well known that $\mathbf{res}(D(\boldsymbol{Z}D_n)) \subseteq D(\boldsymbol{Z}C_n)$. For an arbitrary finite group G, every projective $\boldsymbol{Z}G$-module is locally free and *vice versa* ([17]). Hence Main Theorem can be reformulated as

THEOREM 1.2. $\mathbf{res}\colon C(\boldsymbol{Z}D_n) \to C(\boldsymbol{Z}C_n)$ *is injective.*

If $n = 2^e$, then (1.2) is an easy consequence of $D(\boldsymbol{Z}D_{2^e}) = 0$ ([14]). Namely,

PROPOSITION 1.3. $\mathbf{res}\colon C(\boldsymbol{Z}D_{2^e}) \to C(\boldsymbol{Z}C_{2^e})$ *is injective.*

PROOF. Let B be a maximal order of $\boldsymbol{Q}D_{2^e}$ containing $\boldsymbol{Z}D_{2^e}$. Since $D(\boldsymbol{Z}D_{2^e}) = 0$, we have $C(\boldsymbol{Z}D_{2^e}) \cong C(B) \cong \prod_{1\leq j\leq e} C(\boldsymbol{Z}[\zeta_{2^j} + \zeta_{2^j}^{-1}])$, where $\zeta_m = \exp(2\pi i/m)$. By Weber's theorem ([7]) the order of $C(\boldsymbol{Z}D_{2^e})$ is odd. On the other hand, Ker (**res**) is an elementary 2-group by Artin's induction theorem (note that the Artin exponent of D_{2^e} is 2). This shows that **res** is injective.

In this section we will discuss consequences of Main theorem. Let

E/K be a finite normal extension of finite algebraic number fields with $\mathrm{Gal}(E/K) = G$. The ring of algebraic integers $\mathcal{O}_E$ of E can be viewed as a module over $\boldsymbol{Z}G$. It is a classical result that $\mathcal{O}_E$ is a locally free $\boldsymbol{Z}G$-module if and only if E/K is tame, i.e., tamely ramified. It is known that if E/K is tame, then the class of $\mathcal{O}_E$ in $C(\boldsymbol{Z}G)$ is in $D(\boldsymbol{Z}G)$ (so-called Martinet's conjecture solved by Fröhlich ([5])). Recently Taylor proved a remarkable extension of the classical Hilbert-Speiser theorem in [18]:

THEOREM 1.4 (Taylor). *If E/K is a tame abelian extension of algebraic number fields with* $\mathrm{Gal}(E/K) = G$, *then $\mathcal{O}_E$ is a free $\boldsymbol{Z}G$-module.*

If E/K is a tame extension of algebraic number fields with $\mathrm{Gal}(E/K) = D_n$, then E/E^{C_n} is a tame extension with $\mathrm{Gal}(E/E^{C_n}) = C_n$. Taylor's theorem implies that $\mathcal{O}_E$ is a free $\boldsymbol{Z}C_n$-module. Hence by Main theorem we have the following theorem which establishes a conjecture for dihedral groups made in [5, p. 420]:

THEOREM 1.5. *If E/K is a tame extension of algebraic number fields with* $\mathrm{Gal}(E/K) = D_n$, *then $\mathcal{O}_E$ is a free $\boldsymbol{Z}D_n$-module.*

If $K = \boldsymbol{Q}$ and n is an odd prime, this result was proved by Martinet ([13]) before the appearance of Fröhlich's theory ([5]). If n is odd, this follows from Taylor's theorem and the results of Cassou-Noguès in [2]. If n is a power of 2, (1.5) was proved by showing that $D(\boldsymbol{Z}D_{2^e}) = 0$ ([4], [5]). If n is a power of an odd prime p, (1.5) follows from Corollary 2 in [19] and the fact that the order of $D(\boldsymbol{Z}D_n)$ is also a power of p. If $n < 60$, (1.5) was proved in [3] by directly computing $D(\boldsymbol{Z}D_n)$.

Let $G = PSL(2, p^f)$ be a projective special linear group over the finite field with p^f elements, where p is an odd prime. By Dickson's classification of all subgroups of G ([9]) and the hyperelementary induction theorem, we obtain

$$(1.6)\qquad C(\boldsymbol{Z}G) \subseteqq C(\boldsymbol{Z}D_{(p^f-1)/2}) \oplus C(\boldsymbol{Z}D_{(p^f+1)/2}) \oplus C(\boldsymbol{Z}(\overbrace{C_p \times C_p \times \cdots \times C_p}^{f\ \text{times}})) \oplus C(\boldsymbol{Z}C_p * C_{(p-1)/2}),$$

where $C_p * C_{(p-1)/2}$ is a semi-direct product of C_p and $C_{(p-1)/2}$, with $C_{(p-1)/2}$ acting faithfully on C_p. Fröhlich showed in [6] that if $E/\boldsymbol{Q}$ is a tame extension of algebraic number fields with $\mathrm{Gal}(E/\boldsymbol{Q}) = C_p * C_q$, where $q \mid (p-1)$ and C_q acts on C_p faithfully, then $E/\boldsymbol{Q}$ has a normal integral basis, i.e., $\mathcal{O}_E$ is a free $\boldsymbol{Z}C_p * C_q$-module. Thanks to Taylor's theorem his arguments in [6] work for a relative extension case. From (1.5) and (1.6) we obtain a normal integral basis theorem for G. For $p = 2$, a similar argument works. Therefore

PROPOSITION 1.7. *If E/K is a tame extension of algebraic number fields with* $\mathrm{Gal}(E/K) = PSL(2, p^f)$ *for a prime p, then $\mathcal{O}_E$ is a free $ZPSL(2, p^f)$-module.*

Let G be a finite group of order m. Following Swan [16] we define $T(ZG)$ to be the subgroup of $C(ZG)$ generated by the locally free ideals $rZG + Z\Sigma$ of ZG, where $r \in Z$, $(r, m) = 1$ and $\Sigma = \sum_{g \in G} g$. Fundamental properties of $T(ZG)$ are found in [20]. Since $T(ZC_n) = 0$ (see [16], for example), by Main Theorem we obtain

THEOREM 1.8. $T(ZD_n) = 0$.

This fact can also be shown by directly finding a generator of an ideal $rZD_n + Z\Sigma$ of ZD_n. This proof will be presented in a forthcoming paper with S. Endo.

Let $(ZC_n)^{\langle\tau\rangle} = \{a \in ZC_n \mid a = \tau^{-1}a\tau\}$. By Main theorem and Jacobinski-Roiter's theory on genera of modules ([10], [15] or [17]), we have

PROPOSITION 1.9. $C(ZD_n) \cong C((ZC_n)^{\langle\tau\rangle})$.

If n is an odd integer, this easily follows from Section 3 of [1]. For an arbitrary n, this will be proved in Section 2.

2. **Twisted group rings.** Let R be an order in a finite dimensional commutative semi-simple Q-algebra QR. Let τ be a non-trivial automorphism of R such that $\tau^2 = 1$, i.e., an involution. We denote by $S = R\langle\tau\rangle$ the twisted group ring of $\langle\tau\rangle$ over R with a trivial cocycle. Using this notation we can write $ZD_n = ZC_n\langle\tau\rangle$, since τ acts on ZC_n by inner conjugation. R has the obvious S-module structure ($\cong S(1 + \tau)$). We assume that R is a faithful S-module. If P is a locally free left ideal of S, then by Roiter's theorem ([15]) there is an S-module M locally isomorphic to R such that as S-modules we have

$$M \oplus S \cong R \oplus P . \tag{2.1}$$

Conversely if M is given we can find P satisfying the formula (2.1). Viewing S-modules as R-modules we have the restriction map

$$\mathbf{res}^S_R \colon C(S) \to C(R) .$$

By (2.1) it is clear that $\mathbf{res}^S_R$ sends the class of P to the class of M considered as R-modules.

LEMMA 2.2. *Let M be an S-module locally isomorphic to R. Then there exists a locally free ideal X of the invariant subring $R^{\langle\tau\rangle}$ of R such that*

$$M \cong XR(\cong X \otimes_{R^{\langle\tau\rangle}} R) .$$

PROOF. Since $R^{\langle\tau\rangle} \cong \mathrm{Hom}_S(M, M) \cong \mathrm{Hom}_S(R, R)$ and M is locally isomorphic to R, $X = \mathrm{Hom}_S(R, M)$ is a locally free ideal of $R^{\langle\tau\rangle}$. Let us consider the natural pairing

$$\Phi: \mathrm{Hom}_S(R, M) \otimes_{R^{\langle\tau\rangle}} R \to M .$$

Obviously Φ is an S-module homomorphism. By localization it is easy to see that Φ is bijective. Hence $X \otimes_{R^{\langle\tau\rangle}} R \cong M$.

Combining (2.2) with the formula (2.1) we have

LEMMA 2.3. *If P is a locally free left ideal of S, then there exists a locally free ideal X of $R^{\langle\tau\rangle}$ such that*

$$XR \oplus S \cong R \oplus P .$$

Conversely if X is given we can find P satisfying the above formula.

If the natural homomorphism $i: C(R^{\langle\tau\rangle}) \to C(R)$ defined by tensoring is injective, then (2.3) shows that sending the class of P to the class of X defines a surjection ϕ from $C(S)$ to $C(R^{\langle\tau\rangle})$. Now we have the commutative diagram:

(2.4)
$$\begin{array}{ccc} C(S) & \xrightarrow{\mathbf{res}_R^S} & C(R) \\ & \nwarrow_{\phi} \quad \swarrow_{i} & \\ & C(R^{\langle\tau\rangle}) . & \end{array}$$

LEMMA 2.5. *We assume that i is injective. Then ϕ is an isomorphism if* (i) $\mathbf{res}_R^S$ *is injective or* (ii) *R is a projective S-module. If* (ii) *holds, then* $\mathbf{res}_R^S$ *is injective.*

PROOF. The first case follows from the commutative diagram (2.4) directly. The second case follows from Jacobinski's cancellation theorem ([10] or [17]). More precisely if we have $R \oplus S \cong R \oplus P$, then the projectivity of R implies that $S \oplus S \cong S \oplus P$. Hence we have $S \cong P$. The last assertion is straightforward.

Assuming Main theorem, we show that there is a similar commutative diagram for $S = ZD_n$ similar to (2.4). Put

$$\Sigma_0 = \begin{cases} 1 + \sigma^2 + \sigma^4 + \cdots + \sigma^{2(n/2-1)} & \text{if } n \text{ is even} \\ 1 + \sigma + \sigma^2 + \cdots + \sigma^{n-1} & \text{if } n \text{ is odd} . \end{cases}$$

Since we are assuming Main theorem, we have $T(ZD_n) = 0$, so that argument in Section 3 of [3] shows that the natural maps

$$C(\boldsymbol{Z}D_n) \to C(\boldsymbol{Z}D_n/\Sigma_0 \cdot \boldsymbol{Z}D_n)\ , \qquad C(\boldsymbol{Z}C_n) \to C(\boldsymbol{Z}C_n/\Sigma_0 \cdot \boldsymbol{Z}C_n)$$

and

$$C((\boldsymbol{Z}C_n)^{\langle\tau\rangle}) \xrightarrow{\pi} C((\boldsymbol{Z}C_n/\Sigma_0 \cdot \boldsymbol{Z}C_n)^{\langle\tau\rangle})$$

are all isomorphisms. If we assume that $C((\boldsymbol{Z}C_n)^{\langle\tau\rangle}) \to C(\boldsymbol{Z}C_n)$ is injective, then these isomorphisms imply that

$$C((\boldsymbol{Z}C_n/\Sigma_0 \cdot \boldsymbol{Z}C_n)^{\langle\tau\rangle}) \to C(\boldsymbol{Z}C_n/\Sigma_0 \cdot \boldsymbol{Z}C_n)$$

is injective too. Since $\boldsymbol{Z}C_n/\Sigma_0 \cdot \boldsymbol{Z}C_n$ is a faithful $\boldsymbol{Z}D_n/\Sigma_0 \cdot \boldsymbol{Z}D_n$-module, there is a surjective homomorphism

$$\phi_0\colon C(\boldsymbol{Z}D_n/\Sigma_0 \cdot \boldsymbol{Z}D_n) \to C((\boldsymbol{Z}C_n/\Sigma_0 \cdot \boldsymbol{Z}C_n)^{\langle\tau\rangle})$$

which makes the diagram (2.4) commutative for $S = \boldsymbol{Z}D_n/\Sigma_0 \cdot \boldsymbol{Z}D_n$. Let ϕ be the composition of maps

$$C(\boldsymbol{Z}D_n) \longrightarrow C(\boldsymbol{Z}D_n/\Sigma_0 \cdot \boldsymbol{Z}D_n) \xrightarrow{\phi_0} C((\boldsymbol{Z}C_n/\Sigma_0 \cdot \boldsymbol{Z}C_n)^{\langle\tau\rangle}) \xrightarrow{\pi^{-1}} C((\boldsymbol{Z}C_n)^{\langle\tau\rangle})\ .$$

Then ϕ is surjective and the diagram

$$\begin{array}{ccc} C(\boldsymbol{Z}D_n) & \xrightarrow{\text{res}} & C(\boldsymbol{Z}C_n) \\ & {\scriptstyle\phi}\nwarrow \quad \swarrow{\scriptstyle i} & \\ & C((\boldsymbol{Z}C_n)^{\langle\tau\rangle}) & \end{array}$$

is commutative.

Now if we assume Main theorem, then in order to prove (1.9), i.e., that ϕ is an isomorphism it is sufficient to show by the above commutative diagram that the natural map $i\colon C((\boldsymbol{Z}C_n)^{\langle\tau\rangle}) \to C(\boldsymbol{Z}C_n)$ is injective. We will prove a general version of the injectivity of the map i. Let G be a finite abelian group and g the standard involution of $\boldsymbol{Z}G$, i.e., the automorphism of $\boldsymbol{Z}G$ induced by $g(h) = h^{-1}$ $(h \in G)$. A character $\chi\colon G \to \boldsymbol{C}^*$ can be extended to the algebra homomorphism of $\boldsymbol{Z}G$ into $\boldsymbol{C}$ by linearity, which we denote by the same symbol χ.

LEMMA 2.6. *If G is a finite abelian group, then we have the following.*

(i) *If u is a unit of $\boldsymbol{Z}G$ satisfying $u \cdot u^g = 1$, then u is a trivial unit of $\boldsymbol{Z}G$, i.e., $u \in \pm G$.*

(ii) *Let u be a trivial unit of $\boldsymbol{Z}G$. If $\chi(u) = 1$ for every real character $\chi\colon G \to \boldsymbol{R}^*$, then there is a $v \in G$ such that $u = v^2$.*

PROOF. Projecting u to a simple component of $\boldsymbol{Q}G$ on which g acts as the complex conjugation, we easily see that u is a unit of finite order in every simple component of QG. Hence u is of finite order in ZG, so that u is a trivial unit by Higman's theorem ([8]). The proof of (ii) is clear.

REMARK 2.7. We denote by $U(A)$ the unit group of a ring A. By (2.6) and an argument similar to that in the proof of Lemma 3.1 in [11], we have $U(ZG) = G \cdot U((ZG)^{\langle g \rangle})$. Indeed, let u be a unit of ZG. Then $v = u^g/u$ is a unit of finite order, say $v = \pm h$ for $h \in G$. Since $\chi(v) = \chi(u^g/u) = 1$ for every real character $\chi: ZG \to R^*$, $v = h$ and $h = w^2$ for a suitable $w \in G$ by (2.6). Noting that $(wu)^g = w^{-1}u^g = wh^{-1}u^g = wu$, we see that $u = w^{-1}(wu) \in G \cdot U((ZG)^{\langle g \rangle})$.

THEOREM 2.8. *For a finite abelian group G, the natural homomorphism of $C((ZG)^{\langle g \rangle})$ into $C(ZG)$ is injective.*

PROOF. Let M be a locally free ideal of $(ZG)^{\langle g \rangle}$. By [15] there exists an ideal N of $(ZG)^{\langle g \rangle}$ such that $N \cong M$ and $(ZG)^{\langle g \rangle}/N$ is annihilated by an odd integer, say d. We assume that $N \cdot ZG$ is a principal ideal $a \cdot ZG$. Since $a \cdot ZG$ is g-stable, there is a unit u in ZG such that $a^g = u \cdot a$. a being a regular element, we have $u \cdot u^g = 1$. Hence u is a trivial unit by (2.6). Let $\chi: G \to R^*$ be a real character. Then $\chi(a^g) = \chi(a) \neq 0$, hence $\chi(u) = \chi(a^g)\chi(a)^{-1} = 1$. By (2.6) we have $u = v^2$ for some $v \in G$ and therefore, $(v^{-1}a)^g = v^{-1}a$. Set $b = v^{-1}a$. Since $b \in N \cdot ZG$, we can write $b = n_1a_1 + n_2a_2 + \cdots + n_ra_r$ with $n_i \in N$ and $a_i \in ZG$ for $1 \leqq i \leqq r$. From this we have $2b = b + b^g = \sum_{1 \leqq i \leqq r} n_i(a_i + a_i^g) \in N$. On the other hand, $db \in N$, hence $b \in N$. This shows that N is a principal ideal.

COROLLARY 2.9. $D(ZD_n) \cong D((ZC_n)^{\langle \tau \rangle})$.

PROOF. We have an injection $f: ZC_n \to T = \prod_{r|n} Z[\zeta_r]$. Since $ZD_n = ZC_n\langle \tau \rangle$, we have the injection f' induced by f.

$$f': ZD_n \to T\langle \tau \rangle = \prod_{r|n} Z[\zeta_r]\langle \tau \rangle .$$

If r is not a power of 2, $Z[\zeta_r]\langle \tau \rangle$ is a hereditary order in $Q(\zeta_r)\langle \tau \rangle$, therefore, $C(Z[\zeta_r]\langle \tau \rangle) \cong C(Z[\zeta_r + \zeta_r^{-1}])$. If r is a power of 2, (1.3) implies that $C(Z[\zeta_r])\langle \tau \rangle \cong C(Z[\zeta_r + \zeta_r^{-1}])$. Hence $C(T\langle \tau \rangle) \cong \prod_{r|n} C(Z[\zeta_r + \zeta_r^{-1}]) \cong C(B)$, where B is a maximal order of QD_n containing ZD_n. Now we have a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & D(ZD_n) & \longrightarrow & C(ZD_n) & \longrightarrow & C(T\langle \tau \rangle) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi'} & & \\ 0 & \longrightarrow & D((ZC_n)^{\langle \tau \rangle}) & \longrightarrow & C((ZC_n)^{\langle \tau \rangle}) & \longrightarrow & C(T^{\langle \tau \rangle}) & \longrightarrow & 0 \end{array}$$

where ϕ' is the map constructed in (2.3). Note that $C(T^{\langle\tau\rangle}) \to C(T)$ is injective by the classical Kummer theorem. Since ϕ and ϕ' are isomorphisms, we have $D(ZD_n) \cong D((ZC_n)^{\langle\tau\rangle})$.

3. A certain factor ring of ZD_n. Let $D_n = \langle\sigma, \tau \mid \sigma^n = \tau^2 = 1, \tau^{-1}\sigma\tau = \sigma^{-1}\rangle$ be a dihedral group of order $2n$. We write $n = 2^e m$, where m is an odd integer, and $\sigma = \rho\cdot\mu$, where ρ is of order m and μ is of order 2^e. Let us set $\Sigma = 1+\rho+\rho^2+\cdots+\rho^{m-1}$, $S = ZD_n/\Sigma\cdot ZD_n$ and $R = ZC_n/\Sigma\cdot ZC_n$, where C_n is the subgroup of D_n generated by σ. $\bar\sigma$, $\bar\rho$, $\bar\mu$ and $\bar\tau$ denote the images of σ, ρ, μ and τ in S, respectively. S is the twisted group ring of $\langle\bar\tau\rangle$ over R, where $\bar\tau$ acts on R by inner conjugation. Let R_0 be $\{r \in R \mid \bar\tau^{-1} r \bar\tau = r\}$, the invariant subring of R under $\langle\bar\tau\rangle$. Then R is a free R_0-module with basis $(1, \bar\sigma)$. For the remainder of this paper we will use these notations and will assume $m > 1$.

As R-modules $R \cong S(1+\bar\tau)$ and $R \cong S(1-\bar\tau)$. These isomorphisms impose on R two S-module structures. As S-modules we set

$$R_+ \cong S(1+\bar\tau) \quad \text{and} \quad R_- \cong S(1-\bar\tau)\ .$$

Since the left multiplications by elements of S on R_+ are R_0-endomorphisms, we have an imbedding $S \to \mathrm{End}_{R_0}(R_+)$. By this imbedding we view S as a subring of $\mathrm{End}_{R_0}(R_+)$. Using the free R_0-basis $(1, \bar\sigma)$ we identify $\mathrm{End}_{R_0}(R_+)$ with $M_2(R_0)$, the ring of 2×2-matrices with entries in R_0. By this identification an arbitrary element $a + b\bar\tau + c\bar\sigma + d\bar\sigma\bar\tau \in S$ $(a, b, c, d \in R_0)$ is represented by the matrix

$$\begin{pmatrix} a+b & b\omega - c + d \\ c+d & a - b + c\omega \end{pmatrix}, \tag{3.1}$$

where $\omega = \bar\sigma + \bar\sigma^{-1}$. We set this matrix equal to $\begin{pmatrix} x & y \\ z & u \end{pmatrix} \in M_2(R_0)$. Then we obtain the following relations:

$$\begin{aligned} a(\omega^2-4) &= x\omega^2 - (y-z)\omega - 2(x+u) \\ c(\omega^2-4) &= 2(y-z) - (x-u)\omega\ . \end{aligned} \tag{3.2}$$

Since $\omega = \bar\rho\bar\mu + \bar\rho^{-1}\bar\mu^{-1}$, we have $\omega^2 - 4 = \bar\rho^2\bar\mu^2 + \bar\rho^{-2}\bar\mu^{-2} - 2$. This shows that $(\bar\rho^2\bar\mu^2 + \bar\rho^{-2}\bar\mu^{-2})^2 - 4 = \bar\rho^4\bar\mu^4 + \bar\rho^{-4}\bar\mu^{-4} - 2 \in (\omega^2-4)R_0$. Repeating this procedure we have $\bar\rho^{2^e} + \bar\rho^{-2^e} - 2 \in (\omega^2-4)R_0$. Since $\bar\rho$ is of odd order m, we have that $\bar\rho + \bar\rho^{-1} - 2 \in (\omega^2-4)R_0$. From this we obtain

LEMMA 3.3. *$R_0/(\omega^2-4)R_0$ is annihilated by m.*

Since m is an odd integer,

LEMMA 3.4. *$(\omega-2)R_0$ and $(\omega+2)R_0$ are coprime ideals, namely,*

$$(\omega - 2)R_0 + (\omega + 2)R_0 = R_0 \quad and \quad (\omega - 2)R_0 \cap (\omega + 2)R_0 = (\omega^2 - 4)R_0 .$$

LEMMA 3.5. $\begin{pmatrix} x & y \\ z & u \end{pmatrix}$ *belongs to* S *if and only if*

(i) $2(x - u) \equiv (y - z)\omega \bmod (\omega^2 - 4)R_0$ *if* $e \geqq 0$

or

(ii) $x - u \equiv y - z \bmod (\omega - 2)R_0$ *if* $e = 0$.

If $e = 0$, i.e., n is odd, ω and $\omega + 2$ are units. Hence (i) implies (ii). (i) follows easily from the formula (3.2).

The reduced norm map Nrd: $S \to R_0$ is the composition of maps

$$S \longrightarrow M_2(R_0) \xrightarrow{\det} R_0 .$$

Hence it is easy to check that $\mathrm{Nrd}(a + b\bar{\tau}) = a \cdot a^{\tau} - b \cdot b^{\tau}$ $(a, b \in R)$, where $a^{\tau} = \bar{\tau}^{-1} a \bar{\tau}$ and $b^{\tau} = \bar{\tau}^{-1} b \bar{\tau}$. (3.5) shows that

LEMMA 3.6. Nrd: $U(S) \to U(R_0)$ *is surjective.*

LEMMA 3.7. R_+ *and* R_- *are projective* S*-modules and* $S \cong R_+ \oplus R_-$.

PROOF. Let p be a prime. If $p \nmid m$, $\boldsymbol{Z}_p \otimes_Z S \cong \boldsymbol{Z}_p \otimes_Z \mathrm{End}_{R_0}(R_+)$ by (3.3), which implies that $\boldsymbol{Z}_p \otimes_Z R_+$ is a projective $\boldsymbol{Z}_p \otimes_Z S$-module. If $p \mid m$, 2 is invertible in $\boldsymbol{Z}_p$, hence we get $\boldsymbol{Z}_p \otimes_Z R_+ \cong (\boldsymbol{Z}_p \otimes_Z S \cdot (1 - \bar{\tau})/2) \oplus (\boldsymbol{Z}_p \otimes_Z S \cdot (1 + \bar{\tau})/2)$. Therefore $\boldsymbol{Z}_p \otimes_Z R_+ \cong \boldsymbol{Z}_p \otimes_Z S \cdot (1 + \bar{\tau})/2$ is a projective $\boldsymbol{Z}_p \otimes_Z S$-module. From the exact sequence $0 \to R_- \to S \to R_+ \to 0$, we obtain $S \cong R_+ \oplus R_-$.

We prove an analogue of Main theorem for S and R, namely,

THEOREM 3.8. $\mathbf{res}^S_R$: $C(S) \to C(R)$ *is an injection.*

Thanks to (2.5), in order to prove (3.8) it is sufficient to prove the following.

PROPOSITION 3.9. *The natural homomorphism* $C(R_0) \to C(R)$ *is an injection.*

To prove this we need one more lemma.

LEMMA 3.10. *If* $u \in R$ *is a unit of finite order, then* $u^m = \pm \bar{\mu}^i$ *for some* i.

PROOF. We have an injection $f: R \to \prod_{r \mid m, r > 1} \boldsymbol{Z}[\zeta_r, \bar{\mu}]$, where the projection $f_r: R \to \boldsymbol{Z}[\zeta_r, \bar{\mu}]$ is given by sending $\bar{\rho}$ to ζ_r. Since $f_r(u)$ is a unit of finite order in $U(\boldsymbol{Z}[\zeta_r, \bar{\mu}])$, we have $f_r(u) = \pm \zeta_r^j \bar{\mu}^k$ by Higman's theorem ([8]). Put $f_r(u^m) = h(r)\bar{\mu}^{a(r)}$, where $h(r) = \pm 1$. We show that $h(r)$ and $a(r) \bmod 2^e$ do not depend on r. Let $p^s m_0$ and $p^t m_0$ be divisors of m, where p is an odd prime. Then we have

$$f_{p^s m_0}(u^m) \equiv f_{p^t m_0}(u^m) \qquad \mathrm{mod}\,(\zeta_{p^s} - \zeta_{p^t}) \ .$$

This shows that $h(p^s m_0) = h(p^t m_0)$ and $a(p^s m_0) \equiv a(p^t m_0) \bmod 2^e$. By induction on the number of primes dividing m we see that $h(r)$ and $a(r) \bmod 2^e$ do not depend on $r \mid m$. Hence $u^m = \pm \bar{\mu}^i$ for some i.

REMARK 3.11. If $u \in U(R)$, then $u^m \in \langle \bar{\mu} \rangle U(R_0)$ (cf. (2.7)).

Now we prove (3.9). Let M be a locally free ideal of R_0. We can choose an ideal N of R_0 such that $N \cong M$ and R_0/N is annihilated by an integer d coprime to $2m$. We assume that $N \cdot R$ is a principal ideal $c \cdot R$. There is a unit u in R such that $c^\tau = u \cdot c$. We have $u \cdot u^\tau = 1$ and hence, u is a unit of finite order. By (3.10) $u^m = \pm \bar{\mu}^i$ for some i. If $e \geqq 1$, let us look at algebra homomorphisms

$$\kappa: R \xrightarrow{f_p} \boldsymbol{Z}[\zeta_p, \bar{\mu}] \longrightarrow \boldsymbol{F}_p[\bar{\mu}]/(\bar{\mu} - 1) \cong \boldsymbol{F}_p$$

and

$$\kappa': R \xrightarrow{f_p} \boldsymbol{Z}[\zeta_p, \bar{\mu}] \longrightarrow \boldsymbol{F}_p[\bar{\mu}]/(\bar{\mu} + 1) \cong \boldsymbol{F}_p \ ,$$

where p is an odd prime dividing m. Since $c \cdot R$ is coprime to $2mR$, $\kappa(c)$ and $\kappa'(c)$ are non-zero. This shows that $u^m = \bar{\mu}^i$ and i is even, say $i = 2j$. If $e = 0$, i.e., $n = m$ is odd, it is easy to see that $u^m = 1$. In both cases $(\bar{\mu}^j c^m)^\tau = \bar{\mu}^j c^m$. By the same argument as in (2.8) we see that N^m is principal. On the other hand, $N \cdot R \cong N \oplus N$ as R_0-modules. Note that R is a free R_0-module of rank 2. This shows that $\mathrm{Ker}\,(C(R_0) \to C(R))$ is an elementary 2-group. Hence the class of N in $C(R_0)$ is trivial. This completes the proof.

Thanks to (3.8) we can use (2.5), i.e., we have a surjection $\phi: C(S) \to C(R_0)$, which makes the following diagram commutative (cf. (2.4)):

$$\begin{array}{ccc} C(S) & \xrightarrow{\mathbf{res}_R^S} & C(R) \\ & {}_{\phi}\searrow \quad \nearrow_{i} & \\ & C(R_0) & \end{array}$$

Since R is a projective S-module by (3.7), ϕ is an isomorphism, hence $\mathbf{res}_R^S$ is injective.

COROLLARY 3.12. *$C(S) \cong C(R_0)$ and $D(S) \cong D(R_0)$.*

The first isomorphism was proved above. The second is proved by a method similar to that in (2.9).

REMARK 3.13. (2.8) and (3.9) are clearly analogues to the following classical theorem of Kummer:

KUMMER A. *The class number of* $\boldsymbol{Q}(\zeta_n + \zeta_n^{-1})$ *divides that of* $\boldsymbol{Q}(\zeta_n)$.

In our notations this can be formulated as

KUMMER B. *The natural homomorphism of* $C(\boldsymbol{Z}[\zeta_n + \zeta_n^{-1}])$ *into* $C(\boldsymbol{Z}[\zeta_n])$ *is injective.*

According to [12] there is a modern formulation of this theorem due to Iwasawa.

KUMMER-IWASAWA. *The norm map* $C(\boldsymbol{Z}[\zeta_n]) \to C(\boldsymbol{Z}[\zeta_n + \zeta_n^{-1}])$ *is surjective.*

For a cyclic group C_m of odd order m we can give an analogue of the Kummer-Iwasawa theorem. In fact we have the inflation map **inf**: $D(\boldsymbol{Z}C_m) \to D(\boldsymbol{Z}D_m)$ defined by sending the class of P to the class of $\boldsymbol{Z}D_m \otimes_{\boldsymbol{Z}C_m} P$. Cassou-Noguès proved in [1] that **inf** is a surjection. The composition of map

$$D(\boldsymbol{Z}C_m) \xrightarrow{\textbf{inf}} D(\boldsymbol{Z}D_m) \xrightarrow{\textbf{res}} D(\boldsymbol{Z}C_m)$$

is clearly an analogue of the norm map in the Kummer-Iwasawa theorem. Hence by (2.5) we have

PROPOSITION. *If* M *is a locally free ideal of* $(\boldsymbol{Z}C_m)^{\langle\tau\rangle}$ *there exists a locally free ideal* P *of* $\boldsymbol{Z}C_m$ *such that* $P \cdot P^\tau \cong M \cdot \boldsymbol{Z}C_m$, *where* $P^\tau = \{\alpha^\tau \mid \alpha \in P\}$.

4. **The proof of Main theorem.** In this section we prove Main theorem, i.e., the injectivity of **res**: $C(\boldsymbol{Z}D_n) \to C(\boldsymbol{Z}C_n)$. If n is a power of 2, i.e., if $m = 1$, this was shown in (1.3). Hence we assume that $m > 1$.

Set $D' = D_{2^e}$ and $C' = C_{2^e}$. We have two pull back diagrams:

$$\begin{array}{ccc} \boldsymbol{Z}D_n & \longrightarrow & \boldsymbol{Z}D' \\ \downarrow & & \downarrow \\ S & \longrightarrow & \boldsymbol{F}_m D' \end{array} \quad \text{and} \quad \begin{array}{ccc} \boldsymbol{Z}C_n & \longrightarrow & \boldsymbol{Z}C' \\ \downarrow & & \downarrow \\ R & \longrightarrow & \boldsymbol{F}_m C' \end{array}$$

where $\boldsymbol{F}_m$ is a finite ring $\boldsymbol{Z}/m\boldsymbol{Z}$. From [14] we have a commutative diagram

$$\begin{array}{ccccccccc} U(S) \oplus U(\boldsymbol{Z}D') & \longrightarrow & U(\boldsymbol{F}_m D') & \longrightarrow & C(\boldsymbol{Z}D_n) & \longrightarrow & C(S) \oplus C(\boldsymbol{Z}D') & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ U(R) \oplus U(\boldsymbol{Z}C') & \longrightarrow & U(\boldsymbol{F}_m C') & \longrightarrow & C(\boldsymbol{Z}C_n) & \longrightarrow & C(R) \oplus C(\boldsymbol{Z}C') & \longrightarrow & 0\,, \end{array}$$

where the rows are exact and the vertical arrows are all restriction maps. Since the image of $U(S) \oplus U(\boldsymbol{Z}D')$ (resp. $U(R) \oplus U(\boldsymbol{Z}C')$) in

$U(F_mD')$ (resp. $U(F_mC')$) coincides with the image of $U(S)$ (resp. $U(R)$), the above diagram reduces to

$$\begin{array}{ccccccccc} U(S) & \xrightarrow{f_1} & U(F_mD')^{ab} & \longrightarrow & C(ZD_n) & \longrightarrow & C(S)\oplus C(ZD') & \longrightarrow & 0 \\ \downarrow{\scriptstyle \lambda_2} & & \downarrow{\scriptstyle \lambda_1} & & \downarrow{\scriptstyle \mathbf{res}} & & \downarrow{\scriptstyle \mathbf{res}'} & & \\ U(R) & \xrightarrow{f_2} & U(F_mC') & \longrightarrow & C(ZC_n) & \longrightarrow & C(R)\oplus C(ZC') & \longrightarrow & 0\ , \end{array}$$

where $U(F_mD')^{ab}$ is the abelization of $U(F_mD')$ and λ_1 (resp. λ_2) is the restriction map. From the left square of this diagram, we have

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \operatorname{Im} f_1 & \longrightarrow & U(F_mD')^{ab} & \longrightarrow & \operatorname{Coker} f_1 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \lambda'_2} & & \downarrow{\scriptstyle \lambda_1} & & \downarrow{\scriptstyle \lambda_3} & & \\ 0 & \longrightarrow & \operatorname{Im} f_2 & \longrightarrow & U(F_mC') & \longrightarrow & \operatorname{Coker} f_2 & \longrightarrow & 0\ , \end{array}$$

where λ'_2 is induced by λ_2 and λ_3 is induced by λ_1. By (1.3) and (3.8) we have

$$\operatorname{Ker} \lambda_3 \cong \operatorname{Ker} (C(ZD_n) \xrightarrow{\mathbf{res}} C(ZC_n)) .$$

This group is an elementary 2-group by Artin's induction theorem. Applying the snake lemma to the above diagram we have an exact sequence

$$\operatorname{Ker} \lambda'_2 \longrightarrow \operatorname{Ker} \lambda_1 \longrightarrow \operatorname{Ker} \lambda_3 \longrightarrow \operatorname{Coker} \lambda'_2 \longrightarrow \operatorname{Coker} \lambda_1 .$$

To complete the proof of Main theorem we must show that

(A) $\operatorname{Coker} \lambda'_2 \to \operatorname{Coker} \lambda_1$ *is injective*

and

(B) $\operatorname{Ker} \lambda'_2 \to \operatorname{Ker} \lambda_1$ *is surjective.*

PROOF OF (A). Let us look at λ_1 and λ_2 closely. It is easy to check that λ_2 is the composition of maps

$$U(S) \longrightarrow K_1(S) \xrightarrow{\mathbf{res}^S_R} K_1(R) \xrightarrow{\det} U(R) .$$

Let $u = a + b\bar{\tau}$ $(a, b \in R)$ be a unit of S and $\kappa_u\colon S \to S$ be an S-module homomorphism defined by $\kappa_u(s) = s \cdot u$ for all $s \in S$. The image of u in $K_1(S)$ is the class of κ_u. The map $\mathbf{res}^S_R$ sends the class of κ_u to the class of κ_u considered as an R-module homomorphism. Since $S = R \oplus R\bar{\tau}$ is a free R-module with basis $(1, \bar{\sigma})$. κ_u can be represented by a 2×2-matrix $\begin{pmatrix} a & b \\ a^{\tau} & b^{\tau} \end{pmatrix}$. Therefore we see that $\lambda_2(u) = a \cdot a^{\tau} - b \cdot b^{\tau}$, i.e., λ_2 is the reduced norm map. By the same method we can show that λ_1 is the reduced norm map too.

Now let $u \in U(R)$. If $f_2(u) \in \operatorname{Im} \lambda_1$, then $f_2(u)$ is τ-invariant. Since u^τ/u is a unit of finite order, $(u^\tau/u)^m = \pm\bar{\mu}^i$ for some i by (3.10). Since $f_2(u^\tau/u) = f_2(u)^\tau \cdot f_2(u)^{-1} = 1$, we have $f_2(\pm\bar{\mu}^i) = \pm\bar{\mu}^i = 1$. This shows that $i \equiv 0 \mod 2^e$, i.e., u^m is τ-invariant. By (3.6) Nrd: $U(S) \to U(R_0)$ is surjective, hence u^m is in the image of λ_2. This implies that Ker (Coker $\lambda_2' \to$ Coker λ_1) is a group of odd order. Since Ker $(C(ZD_n) \to C(ZC_n))$ is an elementary 2-group, Coker $\lambda_2' \to$ Coker λ_1 is injective.

PROOF OF (B). We set $\Sigma_0 = 1 + \bar{\mu}^2 + \bar{\mu}^4 + \cdots + \bar{\mu}^{2\cdot(2^{e-1}-1)}$. We have the decomposition $U(\boldsymbol{F}_m D')^{ab} = U(\boldsymbol{F}_m D'/\Sigma_0 \cdot \boldsymbol{F}_m D')^{ab} \oplus U(\boldsymbol{F}_m D'/(\bar{\mu}^2 - 1))$. It is well known that $G = U(\boldsymbol{F}_m D'/\Sigma_0 \cdot \boldsymbol{F}_m D')^{ab} = K_1(\boldsymbol{F}_m D'/\Sigma_0 \cdot \boldsymbol{F}_m D') = U((\boldsymbol{F}_m C'/\Sigma_0 \cdot \boldsymbol{F}_m C')^{\langle\tau\rangle})$. This shows that λ_1 restricted to G is injective. Now we set $\bar{S} = \boldsymbol{F}_m D'/(\bar{\mu}^2 - 1)\boldsymbol{F}_m D'$. Then $U(\bar{S}) = U(\bar{S}/(\bar{\mu} - 1, \bar{\tau} - 1)) \oplus U(\bar{S}/(\bar{\mu} - 1, \bar{\tau} + 1)) \oplus U(\bar{S}/(\bar{\mu} + 1, \bar{\tau} - 1)) \oplus U(\bar{S}/(\bar{\mu} + 1, \bar{\tau} + 1))$. Hence we can write $U(\bar{S}) = \{(a_1, a_2, a_3, a_4) \mid a_i \in U(\boldsymbol{F}_m)\}$. Under this notation we have $\operatorname{Ker} \lambda_1 = \{(u, u^{-1}, v, v^{-1}) \mid u, v \in U(\boldsymbol{F}_m)\}$ and a commutative diagram

$$\begin{array}{ccccc} U(S) & \longrightarrow & U(S/(\omega^2-4)S) & \xrightarrow{\beta} & U(\bar{S}) \\ & \searrow & \downarrow & \nearrow & \\ & & U(S/(\bar{\rho}-1)S)\,. & & \end{array}$$

Let α be the natural map $U(S) \to U(\bar{S})$. Then, to prove (B) it is sufficient to show that $\alpha(\operatorname{Ker} \lambda_2) = \operatorname{Ker} \lambda_1$. By (3.4) we have $U(S/(\omega^2 - 4)S) = U(S/(\omega - 2)S) \oplus U(S/(\omega + 2)S)$. It is easy to see that $\beta(U(S/(\omega - 2)S)) = U(\bar{S}/(\bar{\mu} - 1)\bar{S})$ (resp. $\beta(U(S/(\omega + 2)S) = U(\bar{S}/(\bar{\rho} + 1)\bar{S}))$). Since S is the subring of $\operatorname{End}_{R_0}(R_+) = M_2(R_0)$, $U(S/(\omega \pm 2)S)$ is a subgroup of $GL_2(R_0/(\omega \pm 2)R_0)$. Let $v = a + b\bar{\tau} + c\bar{\sigma} + d\bar{\sigma}\bar{\tau}$ $(a, b, c, d \in R_0/(\omega^2 - 4)R_0)$ be an arbitrary element of $U(S/(\omega^2 - 4)S)$. By the formula in Section 3, v can be written as

$$\begin{pmatrix} a+b & 2b-c+d \\ c+d & a-b-2c \end{pmatrix} \oplus \begin{pmatrix} a+b & -2b-c+d \\ c+d & a-b-2c \end{pmatrix} \in U(S/(\omega-2)S) \oplus U(S/(\omega+2)S)\,,$$

where we denote a, b, c and d mod $(\omega + 2)R_0$ or a, b, c and d mod $(\omega - 2)R_0$ by the same letters. Set

$$t = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix} \oplus \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Then by (3.5) we can write

$$t^{-1}vt = \begin{pmatrix} x & y \\ 0 & u \end{pmatrix} \oplus \begin{pmatrix} x' & y' \\ 0 & u' \end{pmatrix}.$$

Thus the image of v in $U(\bar{S})$ is (u, x, u', x'). Hence in order to prove (B) it is sufficient to show that for an arbitrary $x \in U(R_0/(\omega - 2)R_0)$ (resp. $x' \in U(R_0/(\omega+2)R_0)$) there is $y \in R_0/(\omega-2)R_0$ (resp. $y' \in U(R_0/(\omega+2)R_0)$) such that

$$t\left(\begin{pmatrix} x & y \\ 0 & x^{-1} \end{pmatrix} \oplus 1\right)t^{-1} \quad \left(\text{resp. } t\left(1 \oplus \begin{pmatrix} x' & y' \\ 0 & x'^{-1} \end{pmatrix}\right)t^{-1}\right)$$

is the image of a suitable element of $\operatorname{Ker} \lambda_2$. If n is odd, i.e., $e = 0$, we only need to show the existence of an element of $\operatorname{Ker} \lambda_2$ in the case of x.

Now there is an element $A \in R_0$ such that $1+(\omega+2)A \equiv x \bmod (\omega-2)R_0$. Clearly the image of $1 + (\omega + 2)A$ in $R_0/(\omega^2 - 4)R_0$ is a unit. Hence $(1 + (\omega + 2)A)R_0 + (\omega^2 - 4)R_0 = R_0$. Therefore

$$(1 + (\omega + 2)A)R_0 + (\omega - 2)(\omega + 2)^2R_0 = R_0 \, .$$

We can find $B', C \in R_0$ such that $(1 + (\omega + 2)A)B' + (\omega - 2)(\omega + 2)^2C = 1$. Looking at this $\bmod\, (\omega + 2)R_0$, we see that $B' = 1 + (\omega + 2)B$ for some $B \in R_0$. Set

$$Y' = \begin{pmatrix} 1+(\omega+2)A & (\omega+2)C \\ -(\omega-2)(\omega+2) & 1+(\omega+2)B \end{pmatrix} \quad \text{and} \quad Y = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix} Y' \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix} .$$

Then

$$Y \equiv \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}\begin{pmatrix} x & 4\bar{C} \\ 0 & x^{-1} \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix} \bmod (\omega - 2)R_0 \, ,$$

where $\bar{C}$ is the image of C in $R_0/(\omega - 2)R_0$ and

$$Y \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod (\omega + 2)R_0 \, .$$

Therefore $Y \in U(S)$ by (3.5). Since $\det(Y) = 1$, we obtain $Y \in \operatorname{Ker} \lambda_2$. Therefore $(x^{-1}, x, 1, 1) \in \operatorname{Ker} \lambda_1$ is the image of an element of $\operatorname{Ker} \lambda_2$. For x' a similar argument works. This completes the proof of Main theorem.

REFERENCES

[1] P. CASSOU-NOGUÈS, Groupe des classes de l'algebre d'un groupe métacyclique, J. of Algebra 41 (1976), 116–136.
[2] P. CASSOU-NOGUÈS, Quelques théorèmes de base normale d'entiers, Ann. Inst. Fourier, Grenoble, 28 (1978), 1–33.
[3] S. ENDO AND T. MIYATA, On the class groups of dihedral groups, to appear.
[4] A. FRÖHLICH, M. E. KEATING AND S. M. J. WILSON, The class groups of quaternion and dihedral 2-groups, Mathematika 21 (1974), 64–71.

[5] A. Fröhlich, Arithmetic and Galois module structure for tame extensions, J. reine und angew. Math. 286/287 (1976), 380–440.
[6] A. Fröhlich, A normal integral basis theorem, J. of Algebra 39 (1976), 131–137.
[7] H. Hasse, Über die Klassenzahl abelscher Zahlkörper, Akademie Verlag, 1952.
[8] G. Higman, The units of group rings, Proc. London Math. Soc. 46 (1940), 231–248.
[9] H. Huppert, Endliche Gruppen I, Die Grundlehren der math. Wissenshaften, Bd. 134, Springer-Verlag, Berlin, Heidelberg and New York, 1967.
[10] H. Jacobinski, Genera and decompositions of lattices over orders, Acta Math. 121 (1968), 1–29.
[11] M. A. Kervaire and M.P. Murthy, On the projective class group of cyclic groups of prime order, Comment. Math. Helv. 52 (1977), 415–452.
[12] S. Lang, Cyclotomic fields, Springer-Verlag, Berlin, Heidelberg and New York, 1978.
[13] J. Martinet, Sur l'arithmétique des extensions Galoisiennes à groupe de Galois diédral d'ordre $2p$, Ann. Inst. Fourier, Grenoble, 19 (1960), 1–80.
[14] I. Reiner and S. Ullom, A Mayer-Vietoris sequence for class groups, J. of Algebra 31 (1974), 305–342.
[15] A. V. Roiter, On integral representations belonging to a genus, Izv. Akad. Nauk SSSR 30 (1966), 1315–1324.
[16] R. G. Swan, Periodic resolutions for finite groups, Ann. of Math. 72 (1960), 267–291.
[17] R. G. Swan, K-theory of finite groups and orders, Notes by E. G. Evans, Lect. Notes in Math., 149, Springer-Verlag, Berlin, Heidelberg and New York, 1970.
[18] M. J. Taylor, Galois module structure of integers of relative abelian extensions, preprint.
[19] M. J. Taylor, On the self-duality of a ring of integers as a Galois module, Invent. math. 46 (1978), 173–177.
[20] S. Ullom, Nontrivial lower bounds for class groups of integral group rings, Illinois J. Math. 20 (1976), 361–371.

Department of Mathematics
Osaka City University
Osaka, 558 Japan