TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 170, August 1972

CLASS GROUPS OF INTEGRAL GROUP RINGS([1])

BY

I. REINER AND S. ULLOM

ABSTRACT. Let Λ be an R-order in a semisimple finite dimensional K-algebra, where K is an algebraic number field, and R is the ring of algebraic integers of K. Denote by $C(\Lambda)$ the reduced class group of the category of locally free left Λ-lattices. Choose $\Lambda = ZG$, the integral group ring of a finite group G, and let Λ' be a maximal Z-order in QG containing Λ. There is an epimorphism $C(\Lambda) \to C(\Lambda')$, given by $M \to \Lambda' \otimes_\Lambda M$, for M a locally free Λ-lattice. Let $D(\Lambda)$ be the kernel of this epimorphism; the groups $D(\Lambda)$, $C(\Lambda)$ and $C(\Lambda')$ are all finite. Our main theorem is that $D(ZG)$ is a p-group whenever G is a p-group. This generalizes Fröhlich's result for the case where G is an abelian p-group. Our proof uses some facts about the center F of QG, as well as information about reduced norms. We also calculate $D(ZG)$ explicitly for G cyclic of order $2p$, dihedral of order $2p$, or the quaternion group. In these cases, the ring ZG can be conveniently described by a pullback diagram.

1. Introduction. Let $R = \text{alg int}\{K\}$ be the ring of all algebraic integers in an algebraic number field K, and let Λ be an R-order in a semisimple finite dimensional K-algebra A. By a Λ-*lattice* we mean always a left Λ-module which is finitely generated and torsionfree as R-module. For each maximal ideal P of R, let R_P denote the localization of R at P, that is,

$$R_P = \{\alpha/\beta\colon \alpha, \beta \in R,\ \beta \notin P\}.$$

Set $\Delta_P = R_P \otimes_R \Lambda$, an R_P-order in A.

Two Λ-lattices M, N are in the same *genus* if $M_P \cong N_P$ for each maximal ideal P of R. We shall call M *locally free* if M is in the same genus as some free Λ-lattice $\Lambda^{(r)}$; here, $\Lambda^{(r)}$ denotes the direct sum of r copies of Λ. In this case, we call r the Λ-rank of M, and write $r = \text{rank}_\Lambda M$. Of course, every locally free Λ-lattice is projective as left Λ-module.

We next define the (locally free) projective class group $P(\Lambda)$ as follows: let $\mathfrak{B}$ denote the free abelian group generated by symbols $[M]$, one for each isomorphism class of locally free Λ-lattices. Let $\mathfrak{B}_0$ be the subgroup of $\mathfrak{B}$ generated by all expressions $[L \oplus M] - [L] - [M]$ where L, M are locally free Λ-lattices. Then set $P(\Lambda) = \mathfrak{B}/\mathfrak{B}_0$, an abelian additive group. There is an additive epimorphism $P(\Lambda) \to Z$, induced by the mapping $[M] \to \text{rank}_\Lambda M$; this epimorphism is split by the mapping $n \to \Lambda^{(n)}$, $n \in Z$, $n > 0$. Let $C(\Lambda)$ be the kernel of this

Received by the editors July 1, 1971.
AMS 1970 *subject classifications.* Primary 16A54; Secondary 20C05, 20C10.
([1]) This research was partially supported by a grant from the National Science Foundation.

epimorphism, so $C(\Lambda)$ is the subgroup of $P(\Lambda)$ consisting of all expressions $[M] - [N]$, with M, N locally free of the same Λ-rank. Clearly,

$$P(\Lambda) \cong Z \dotplus C(\Lambda)$$

as additive groups. For brevity, we refer to $C(\Lambda)$ as the *class group* of Λ. It is easily seen that $[M] - [N] = 0$ in $C(\Lambda)$ if and only if M and N are stably isomorphic, that is, $M \dotplus \Lambda^{(s)} \cong N \dotplus \Lambda^{(s)}$ for some nonnegative integer s.

The methods of proof in Swan [13] show at once that every element of the class group $C(\Lambda)$ is expressible in the form $[J] - [\Lambda]$, where J is a locally free left Λ-lattice in A. Since there are only a finite number of isomorphism classes of such J's (by the Jordan-Zassenhaus theorem), it follows that $C(\Lambda)$ is necessarily a finite group. Note further that $[J_1] - [\Lambda] = [J_2] - [\Lambda]$ in $C(\Lambda)$ if and only if J_1 and J_2 are stably isomorphic; that is, $J_1 \dotplus \Lambda^{(s)} \cong J_2 \dotplus \Lambda^{(s)}$ for some nonnegative integer s.

For the case where $\Lambda = RG$, the integral group ring of a finite group G, Swan [13] proved that *every* projective Λ-lattice is locally free. Thus our $C(\Lambda)$ is the usual "reduced projective class group."

On the other hand, let Λ' be a maximal R-order in a semisimple K-algebra A. A projective Λ'-lattice M' is called *special* if $K \otimes_R M'$ is A-free. From the theory of maximal orders (see [4], [12] or [15]), we know that *every* Λ'-lattice M' is projective, and that M' is locally free if and only if M' is special. Thus our $C(\Lambda')$ is the usual "reduced special projective class group." Since most of our calculations below depend on working with locally free lattices, it seems desirable to single out this class of projective lattices rather than the class of special projectives.

Suppose now that Λ' is a maximal R-order in A containing Λ. There is then an additive homomorphism $P(\Lambda) \longrightarrow P(\Lambda')$, induced by letting

$$[M] \longrightarrow [\Lambda' \otimes_\Lambda M], \quad M = \text{locally free } \Lambda\text{-lattice}.$$

This homomorphism induces a homomorphism $\eta\colon C(\Lambda) \longrightarrow C(\Lambda')$, and Swan [14] showed that η is in fact an epimorphism. Let $D(\Lambda)$ be the kernel of η, so there is an exact sequence of additive groups

$$0 \longrightarrow D(\Lambda) \longrightarrow C(\Lambda) \longrightarrow C(\Lambda') \longrightarrow 0,$$

and obviously

$$|C(\Lambda)| = |D(\Lambda)| \cdot |C(\Lambda')|.$$

The class group $C(\Lambda')$ of the maximal order Λ' is easily determined, and hence we can find the order of $C(\Lambda)$ by calculating that of $D(\Lambda)$. In this direction, Fröhlich [8] has shown that $|D(ZG)|$ is a power of p whenever G is an abelian p-group. One of the main results of the present article is the fact that $|D(ZG)|$ is a power of p, for an arbitrary finite p-group G, not necessarily abelian. We may remark that this conclusion need not hold, even for abelian p-groups, when Z is replaced by some larger ring of algebraic integers. This

already follows from the work of Ullom [16].

We have also included explicit calculations of $C(ZG)$ and $D(ZG)$ for the following groups G: cyclic group of order $2p$, dihedral group of order $2p$, quaternion group of order 8. Here, p is any odd prime. Some of these calculations could be simplified slightly by using Milnor's Mayer-Vietoris sequence in K-theory (see Bass [1]). We have avoided using this sequence, however, in order to illustrate the computational aspects of our present approach. A later work [18] will be devoted to K-theory calculations.

The following notation will be used throughout:

rad = Jacobson radical.

$(R)^{n\times n}$ = ring of all $n \times n$ matrices over a ring R.

$M^{(k)}$ = direct sum of k copies of M.

$R_{\hat{P}}$ = P-adic completion of the integral domain R at a prime P of the quotient field of R.

$\Sigma^{\cdot}$, $\dot{+}$: direct sum.

$\operatorname{ann}_R X = \{\alpha \in R: \alpha X = 0\}$ = R-annihilator of the R-module X.

$u(\Lambda)$ = group of units(2) of the ring Λ.

General references for this paper are [11], [12] and [15]. The authors wish to thank Professor A. Fröhlich for some helpful conversations, and for pointing out Lemma 3.4 below.

2. **Addition in the class group.** The purpose of this section is to review some well-known results for the convenience of the reader; proofs may be found in the general references cited at the end of §1. As before, we let Λ be any R-order in the semisimple K-algebra A.

Suppose that M is a locally free Λ-lattice of Λ-rank r. It follows readily from the approximation theorem for algebraic numbers that, given any nonzero ideal $\mathfrak{q}$ of R, there exists a Λ-embedding $M \to \Lambda^{(r)}$ such that

$$\operatorname{ann}_R(\Lambda^{(r)}/M) + \mathfrak{q} = R.$$

The methods of proof in Swan [13] then show that there exists a locally free left Λ-lattice J in A such that $M \cong \Lambda^{(r-1)} \dot{+} J$. Hence every element of the (locally free) class group $C(\Lambda)$ is expressible in the form

$$x_j = [J] - [\Lambda], \qquad J = \text{locally free } \Lambda\text{-free lattice in } A.$$

As pointed out in §1, we have $x_{J_1} = x_{J_2}$ if and only if J_1 and J_2 are stably isomorphic.

How can we calculate $x_{J_1} + x_{J_2}$ in $C(\Lambda)$? First of all, embed J_1 in Λ so as to get a Λ-exact sequence

(2) A *unit* of Λ is an element of Λ which has a two-sided inverse in Λ.

$$0 \to J_1 \xrightarrow{i_1} \Lambda \to T_1 \to 0, \tag{2.1}$$

with T_1 an R-torsion Λ-module. Then choose a Λ-exact sequence

$$0 \to J_2 \xrightarrow{i_2} \Lambda \to T_2 \to 0, \tag{2.2}$$

with T_2 an R-torsion Λ-module such that

$$\operatorname{ann}_R T_1 + \operatorname{ann}_R T_2 = R. \tag{2.3}$$

It follows easily that the map (i_1, i_2): $J_1 \dotplus J_2 \to \Lambda$ is a Λ-epimorphism, and hence that

$$J_1 \dotplus J_2 \cong \Lambda \dotplus J_3 \tag{2.4}$$

for some Λ-lattice J_3 in A. We may conclude from this that for each maximal ideal P of R,

$$\Lambda_{\hat{P}} \dotplus \Lambda_{\hat{P}} \cong \Lambda_{\hat{P}} \dotplus (J_3)_{\hat{P}},$$

where the subscript $\hat{P}$ indicates passage to P-adic completions. Since the Krull-Schmidt theorem is valid for $\Lambda_{\hat{P}}$-modules, the above isomorphism implies that $\Lambda_{\hat{P}} \cong (J_3)_{\hat{P}}$. This in turn implies that $\Lambda_P \cong (J_3)_P$, so we have verified that J_3 is also locally free. The operation of addition in $C(\Lambda)$ is then given by the formula: $x_{J_1} + x_{J_2} = x_{J_3}$.

For the remainder of this section, suppose that A is commutative. Let us show that the Λ-lattice J_3 occurring in (2.4) is such that

$$J_3 \cong J_1 \cdot J_2 \quad (= \text{product of } \Lambda\text{-ideals in } A).$$

Indeed, from (2.1) we obtain an exact sequence of Λ-modules

$$0 \to J_1 \otimes J_2 \to J_2 \to T_1 \otimes J_2 \to 0,$$

where $\otimes$ means $\otimes_\Lambda$. On the other hand, from (2.2) we get an exact sequence

$$\operatorname{Tor}_1^\Lambda(T_1, T_2) \to T_1 \otimes J_2 \to T_1 \to T_1 \otimes T_2 \quad (\to 0).$$

By virtue of (2.3), the first and last terms of the above sequence vanish, and thus $T_1 \otimes J_2 \cong T_1$. Consequently there is an exact sequence

$$0 \to J_1 \otimes J_2 \to J_2 \to T_1 \to 0. \tag{2.5}$$

Applying Schanuel's lemma to the pair of sequences (2.1) and (2.5), we obtain

$$J_1 \dotplus J_2 \cong \Lambda \dotplus (J_1 \otimes J_2).$$

Since the map $\xi \otimes \eta \to \xi\eta$ gives an isomorphism $J_1 \otimes J_2 \cong J_1 \cdot J_2$, we may conclude that

$$J_1 \dotplus J_2 \cong \Lambda \dotplus J_1 J_2 \quad \text{and} \quad x_{J_1} + x_{J_2} = x_{J_1 J_2} \quad \text{in } C(\Lambda). \tag{2.6}$$

On the other hand, since A is commutative, we may define an ideal class group $\overline{C}(\Lambda)$ in a more natural manner, as follows: Relative to the usual multiplication of Λ-ideals in A, the locally free Λ-lattices[3] in A form a multiplicative group $\overline{I}(\Lambda)$. The set of all principal ideals

[3] Note that every locally free Λ-lattice in A is invertible.

$$\{\Lambda x\colon x \in A,\ x \text{ invertible in } A\}$$

forms a subgroup $\overline{I}_0(\Lambda)$ of $\overline{I}(\Lambda)$. We now set

$$\overline{C}(\Lambda) = \overline{I}(\Lambda)/\overline{I}_0(\Lambda),$$

the multiplicative group of classes of locally free Λ-ideals in A. (This group $\overline{C}(\Lambda)$ is the same as $\mathrm{Pic}(\Lambda)$; see Bass [1].)

Let us show that the multiplicative group $\overline{C}(\Lambda)$ is isomorphic to the additive group $C(\Lambda)$. Define a map $\mu\colon \overline{C}(\Lambda) \longrightarrow C(\Lambda)$ by

$$\mu(\text{ideal class of } J) = [J] - [\Lambda],$$

where J is any locally free left Λ-lattice in A. The definition is meaningful, since if J_1 is in the same ideal class as J_2, then $J_1 \cong J_2$ as left Λ-modules, and thus

$$[J_1] - [\Lambda] = [J_2] - [\Lambda] \quad \text{in } C(\Lambda).$$

We have already remarked at the beginning of this section that μ is epic. We claim that μ is one-to-one. For if $[J] - [\Lambda] = 0$ in $C(\Lambda)$, then

$$J \dotplus \Lambda^{(r)} \cong \Lambda \dotplus \Lambda^{(r)} \tag{2.7}$$

for some nonnegative integer r. But the $(r+1)$st exterior power (over Λ) of $J \dotplus \Lambda^{(r)}$ is J itself. Hence (2.7) implies that $J \cong \Lambda$, that is, $J \in \overline{I}_0(\Lambda)$. This completes the proof that μ gives a one-to-one mapping of $\overline{C}(\Lambda)$ onto $C(\Lambda)$. Equations (2.6) show that μ is a group homomorphism, so we have established the isomorphism $C(\Lambda) \cong \overline{C}(\Lambda)$.

In a forthcoming article [17], Fröhlich has considered the group $\mathrm{Pic}(ZG)$ for non-abelian G. The authors wish to thank Professor Fröhlich for the opportunity of reading a preliminary version of this article. The relationship between $\mathrm{Pic}(ZG)$ and our $C(ZG)$ will be investigated in a future work [19].

3. **Explicit formulas for the class group.** Returning to the general case, we fix the following notation for the remainder of this article. Let Λ be any R-order in the semisimple K-algebra A, and let Λ' be some maximal R-order in A containing Λ. We may write

$$A = \sum_{i=1}^{m}{}^{\cdot} A_i \qquad \text{(simple components)},$$

$$\Lambda' = \sum_{i=1}^{m}{}^{\cdot} \Lambda_i, \qquad \Lambda_i = \text{maximal } R\text{-order in } A_i, \tag{3.1}$$

$$F = \sum_{i=1}^{m}{}^{\cdot} K_i, \qquad K_i = \text{center of } A_i, \qquad C = \sum_{i=1}^{m}{}^{\cdot} R_i, \qquad R_i = \text{alg int}\{K_i\} \subset \Lambda_i.$$

Each Λ_i is then a maximal R_i-order in the ith simple component A_i of A. Further, F is the center of A, and C is the unique maximal R-order in F.

(i) *Reduced norms.* Let $N_i: A_i \longrightarrow K_i$ be the reduced norm map. If A_i happens to be a full matrix algebra $(K_i)^{m_i \times m_i}$ over the field K_i, and if we let the element $x \in A_i$ map onto the $m_i \times m_i$ matrix x over K_i, then $N_i(x) = \det x$. In the general case (see [2]), the reduced norm N_i is obtained by first passing to a splitting field for A_i, and then using the preceding comment.

Now define the reduced norm map N: $A \longrightarrow F$ by working in each simple component separately, that is, $N = \Sigma \cdot N_i$.

In order to describe the image $N_i(A_i)$ in K_i, we proceed as follows. For P any prime of K_i (finite or infinite), let $(K_i)_{\hat{P}}$ denote the P-adic completion of K_i. Set

$$(A_i)_{\hat{P}} = (K_i)_{\hat{P}} \otimes_{K_i} A_i,$$

a simple algebra with center $(K_i)_{\hat{P}}$. We shall say that P *ramifies* in A_i if $(A_i)_{\hat{P}}$ is *not* a full matrix algebra over the field $(K_i)_{\hat{P}}$. A proof of the following result of Hasse may be found in Swan-Evans [15, Theorem 7.6]:

(3.2) **Theorem.** *A nonzero element $\alpha \in K_i$ lies in $N_i(A_i)$ if and only if $\alpha_{\hat{P}} > 0$ for every real infinite prime P of K_i which ramifies in A_i. Here, $\alpha_{\hat{P}}$ denotes the image of α in $(K_i)_{\hat{P}}$.*

(ii) *The Eichler condition.* Call A_i a *totally definite quaternion algebra* (over its center K_i) if every infinite prime P of K_i is real, and for every such P the algebra $(A_i)_{\hat{P}}$ is a quaternion skewfield over its center $(K_i)_{\hat{P}}$.

We shall say that the algebra A *satisfies the Eichler condition* if no simple component A_i of A is a totally definite quaternion algebra. Commutative algebras automatically satisfy the Eichler condition.

(iii) *Localization.* Let $\mathfrak{f}$ be a nonzero ideal of R (eventually to be chosen so that $\mathfrak{f} \cdot \Lambda' \subset \Lambda$). Call an element $\alpha \in F$ *prime* to $\mathfrak{f}$ if, for each prime ideal P of R dividing $\mathfrak{f}$, α is a unit in the localization C_P. Rather than use idèles, we introduce the semilocal ring

$$R_{\mathfrak{f}} = \bigcap_{P \text{ divides } \mathfrak{f}} R_P = \{\alpha/\beta: \alpha, \beta \in R, \ \beta \text{ prime to } \mathfrak{f}\}.$$

This ring is a principal ideal domain, with maximal ideals $\{P \cdot R_{\mathfrak{f}}: P \text{ divides } \mathfrak{f}\}$. Now set

$$\Lambda_{\mathfrak{f}} = R_{\mathfrak{f}} \otimes_R \Lambda, \qquad C_{\mathfrak{f}} = R_{\mathfrak{f}} \otimes_R C,$$

and so on. It is then clear that an element $\alpha \in F$ is prime to $\mathfrak{f}$ if and only if $\alpha \in u(C_{\mathfrak{f}})$, the group of units of $C_{\mathfrak{f}}$.

Likewise, an element $x \in \Lambda$ is said to be *prime* to $\mathfrak{f}$ if $x \in u(\Lambda_{\mathfrak{f}})$, that is, if $\Lambda_{\mathfrak{f}} = \Lambda_{\mathfrak{f}} \cdot x$. In this case, it follows that $\Lambda'_{\mathfrak{f}} = \Lambda'_{\mathfrak{f}} \cdot x$, so that x is prime to $\mathfrak{f}$ when we view x as an element of the larger order Λ'. The converse is also true, however:

(3.3) **Lemma.** *Let $x \in \Lambda \subset \Lambda'$, and suppose that x is a unit in $\Lambda'_{\mathfrak{f}}$. Then x is also a unit in $\Lambda_{\mathfrak{f}}$. Hence the property of being "prime to $\mathfrak{f}$" is independent of the choice of R-order.*

This lemma is an immediate consequence of the following more general fact:

(3.4) **Lemma.** *Let $\Lambda \subset \Lambda'$ be R-orders in A. Then $\Lambda \cap u(\Lambda') = u(\Lambda)$.*

Proof. Let $x \in \Lambda$; we must show that $x \in u(\Lambda)$ if and only if $x \in u(\Lambda')$. Now $x \in u(\Lambda)$ if and only if $\Lambda = \Lambda x$, so we need to prove that $\Lambda = \Lambda x$ if and only if $\Lambda' = \Lambda' x$. Let $[\Lambda : \Lambda x]$ denote the order ideal of the R-torsion Λ-module $\Lambda/\Lambda x$, that is, $[\Lambda : \Lambda x]$ is the product of the R-annihilators of the R-composition factors of $\Lambda/\Lambda x$ (see [3] or [7]). Relative to a K-basis of A, right multiplication by x acting on A gives rise to a matrix $\mathbf{M}(x)$, and we have

$$[\Lambda : \Lambda x] = R \cdot \det \mathbf{M}(x).$$

Since the same equation holds with Λ replaced by Λ', we obtain $[\Lambda : \Lambda x] = [\Lambda' : \Lambda' x]$. This implies the desired result.

Remark. Using the notation of the preceding proof, we may observe that every prime ideal of R which divides $C \cdot N(x)$ also divides $R \cdot \det \mathbf{M}(x)$, and conversely: Hence an element $x \in \Lambda$ is a unit in Λ if and only if $N(x)$ is a unit in R.

Now let $u(\Lambda_{\mathfrak{f}})$ be the group of units of the ring $\Lambda_{\mathfrak{f}}$. Obviously

$$\{x \in \Lambda: x \text{ prime to } \mathfrak{f}\} \subset u(\Lambda_{\mathfrak{f}}),$$

by definition of "prime to $\mathfrak{f}$". On the other hand, any element $y \in u(\Lambda_{\mathfrak{f}})$ is expressible as $y = x/r$, with $x \in \Lambda$, $r \in R$, where r is prime to $\mathfrak{f}$. Then both x and r are elements of Λ prime to $\mathfrak{f}$. This shows that $u(\Lambda_{\mathfrak{f}})$ is the multiplicative group generated by the set

$$\{x \in \Lambda: x \text{ prime to } \mathfrak{f}\}.$$

Furthermore, the preceding remark shows that an element $x \in \Lambda$ is prime to $\mathfrak{f}$ if and only if its reduced norm $N(x)$ is prime to $\mathfrak{f}$.

(iv) *Explicit formulas when Eichler condition holds.* Hereafter, let $\mathfrak{f}$ be a nonzero ideal of R such that $\mathfrak{f} \cdot \Lambda' \subset \Lambda$, where Λ' is a maximal R-order in A containing Λ. Such an ideal $\mathfrak{f}$ always exists. (For example, when Λ is the integral group ring RG of a finite group G, we may choose $\mathfrak{f} = |G| \cdot R$.) Denote by $I(C, \mathfrak{f})$ the multiplicative group of all C-ideals in F, nonzero at each component, which are prime to $\mathfrak{f}$.

Let $I(\Lambda)$ be the subgroup of $I(C, \mathfrak{f})$ generated by all ideals

$$\{C \cdot N(x): x \in \Lambda, x \text{ prime to } \mathfrak{f}\}.$$

Since $(C \cdot N(x)) \cdot (C \cdot N(y)) = C \cdot N(xy)$ for $x, y \in \Lambda$ prime to $\mathfrak{f}$, and since the set of elements $\{x \in \Lambda: x \text{ prime to } \mathfrak{f}\}$ generates the group $u(\Lambda_{\mathfrak{f}})$, we conclude at once that

$$I(\Lambda) = \{C \cdot N(x): x \in u(\Lambda_{\mathfrak{f}})\}. \tag{3.5}$$

Likewise, we set

$$I(\Lambda') = \{C \cdot N(y): y \in u(\Lambda'_{\mathfrak{f}})\}. \tag{3.6}$$

We now quote the following basic result due to Jacobinski [9]:

(3.7) **Theorem.** *If the algebra A satisfies the Eichler condition, then there is a commutative diagram*

$$\begin{array}{ccc} C(\Lambda) & \cong & I(C, \mathfrak{f})/I(\Lambda) \\ \eta\downarrow & & \eta'\downarrow \\ C(\Lambda') & \cong & I(C, \mathfrak{f})/I(\Lambda') \end{array}$$

where η is defined by applying $\Lambda' \otimes_{\Lambda} \cdot$ to Λ-lattices, and η' is the natural epimorphism. Consequently,

$$D(\Lambda) = \ker \eta \cong I(\Lambda')/I(\Lambda).$$

Remark. The groups $I(\Lambda')$ and $I(\Lambda)$ depend on $\mathfrak{f}$. However, Jacobinski showed that (up to isomorphism) the groups $C(\Lambda)$, $C(\Lambda')$ and $D(\Lambda)$ are independent of the choice of the maximal order Λ' containing Λ, and are also independent of the choice of the nonzero ideal $\mathfrak{f}$ of R such that $\mathfrak{f} \cdot \Lambda' \subset \Lambda$.

Let us now define a homomorphism

$$\theta: u(\Lambda'_{\mathfrak{f}}) \longrightarrow I(\Lambda')$$

by setting $\theta(x) = C \cdot N(x)$, $x \in u(\Lambda'_{\mathfrak{f}})$. Then θ is an epimorphism with kernel

$$\{x \in u(\Lambda'_{\mathfrak{f}}): N(x) = \text{unit in } C\}.$$

Denote by C^* the group of units of C, and set

$$N^{-1}(C^*) = \{x \in A: N(x) \in C^*\}.$$

Then

$$\ker \theta = u(\Lambda'_{\mathfrak{f}}) \cap N^{-1}(C^*),$$

and therefore

$$u(\Lambda'_{\mathfrak{f}})/\{u(\Lambda'_{\mathfrak{f}}) \cap N^{-1}(C^*)\} \cong I(\Lambda').$$

However, $N^{-1}(C^*) \lhd u(\Lambda'_{\mathfrak{f}}) \cdot N^{-1}(C^*)$, since $N^{-1}(C^*)$ contains the commutator subgroup of $u(\Lambda'_{\mathfrak{f}})$. We thus may deduce from the above isomorphism the fact that

$$(u(\Lambda'_{\mathfrak{f}}) \cdot N^{-1}(C^*))/N^{-1}(C^*) \cong I(\Lambda'),$$

where the isomorphism is induced by letting an element x in the numerator map onto $C \cdot N(x)$.

In the same manner, we obtain

$$(u(\Lambda_{\mathfrak{f}}) \cdot N^{-1}(C^*))/N^{-1}(C^*) \cong I(\Lambda).$$

Consequently, we have

$$D(\Lambda) \cong \frac{I(\Lambda')}{I(\Lambda)} \cong \frac{u(\Lambda'_{\mathfrak{f}}) \cdot N^{-1}(C^*)}{u(\Lambda_{\mathfrak{f}}) \cdot N^{-1}(C^*)} \cong \frac{u(\Lambda'_{\mathfrak{f}})}{u(\Lambda'_{\mathfrak{f}}) \cap \{u(\Lambda_{\mathfrak{f}}) \cdot N^{-1}(C^*)\}}. \tag{3.8}$$

Note that $u(\Lambda_{\mathfrak{f}}) \cdot N^{-1}(C^*) \lhd u(\Lambda'_{\mathfrak{f}})N^{-1}(C^*)$, since $N^{-1}(C^*)$ contains all commutators. Formula (3.8) avoids the use of reduced norms, except for the calculation of $N^{-1}(C^*)$.

We conclude this subsection by giving Jacobinski's construction for the element $\delta_x \in D(\Lambda)$ which corresponds to an element $x \in u(\Lambda'_{\mathfrak{f}})$ in the isomorphism (3.8). Namely, write $x = yz^{-1}$ with both y and z in Λ' and prime to $\mathfrak{f}$. Then $\delta_x = [\Lambda \cap \Lambda' y] - [\Lambda \cap \Lambda' z]$ is the desired element of $D(\Lambda)$. (It is easily checked that both $\Lambda \cap \Lambda' y$ and $\Lambda \cap \Lambda' z$ are locally free Λ-lattices, and that δ_x lies in the kernel of the mapping $C(\Lambda) \to C(\Lambda')$.)

(v) *Explicit formulas in the general case.* We now turn to the case where A need not satisfy the Eichler condition. Let us form

$$E(A \dotplus A) = \mathrm{Hom}_A(A \dotplus A, A \dotplus A).$$

Suppose that the ith simple component A_i of A is given by $A_i \cong (D_i)^{m_i \times m_i}$, D_i = skewfield with center K_i. Then

$$E(A \dotplus A) \cong \sum_{i=1}^{m} \cdot (D_i)^{2m_i \times 2m_i}.$$

Thus $E(A \dotplus A)$ has the same center F as A, and is a semisimple K-algebra which automatically satisfies the Eichler condition. Furthermore,

$$E(\Lambda' \dotplus \Lambda') = \mathrm{Hom}_{\Lambda'}(\Lambda' \dotplus \Lambda', \Lambda' \dotplus \Lambda')$$

is a maximal R-order in $E(A \dotplus A)$.

Let $N^*: E(A \dotplus A) \to F$ be the reduced norm map. We shall say that an element $x \in E(\Lambda \dotplus \Lambda)$ is prime to $\mathfrak{f}$ if x is a unit in $\{E(\Lambda \dotplus \Lambda)\}_{\mathfrak{f}}$, or equivalently, if $N^*(x)$ is prime to $\mathfrak{f}$. There is an obvious ring isomorphism

$$\{E(\Lambda \dotplus \Lambda)\}_{\mathfrak{f}} \cong E(\Lambda_{\mathfrak{f}} \dotplus \Lambda_{\mathfrak{f}}),$$

and we shall always identify these rings with one another. As before, let $I(C, \mathfrak{f})$ be the group of all C-ideals of F prime to $\mathfrak{f}$, and let $J(\Lambda)$ be the subgroup of $I(C, \mathfrak{f})$ generated by the set of all principal ideals

$$\{C \cdot N^*(y): y \in E(\Lambda \dotplus \Lambda),\ y \text{ prime to } \mathfrak{f}\}.$$

As in the preceding section, we obtain

$$J(\Lambda) = \{C \cdot N^*(y): \ y = \text{unit in } E(\Lambda_{\mathfrak{f}} \dotplus \Lambda_{\mathfrak{f}})\}. \tag{3.9}$$

Likewise, we set

$$J(\Lambda') = \{C \cdot N^*(y): \ y = \text{unit in } E(\Lambda'_{\mathfrak{f}} \dotplus \Lambda'_{\mathfrak{f}})\}. \tag{3.10}$$

The following basic result is due to Jacobinski [9]:

(3.11) **Theorem.** *Whether or not A satisfies the Eichler condition, there is a commutative diagram*

$$\begin{array}{ccc} C(\Lambda) \cong I(C, \mathfrak{f})/J(\Lambda) \\ \eta\downarrow \qquad\qquad \eta''\downarrow \\ C(\Lambda') \cong I(C, \mathfrak{f})/J(\Lambda') \end{array}$$

where η is defined by applying $\Lambda' \otimes_{\Lambda}$ to Λ-lattices, and η'' is the natural epimorphism. Consequently,

$$D(\Lambda) = \ker \eta \cong J(\Lambda')/J(\Lambda).$$

Up to isomorphism, these formulas are independent of the choice of maximal order Λ' containing Λ, and of the ideal $\mathfrak{f}$ of R such that $\mathfrak{f} \cdot \Lambda' \subset \Lambda$. Furthermore, when A satisfies the Eichler condition, we have

$$J(\Lambda') = I(\Lambda'), \qquad J(\Lambda) = I(\Lambda).$$

There are obvious analogues of formula (3.8), which we shall not write down explicitly.

4. **Functorial property of class groups.** We intend to show that any group epimorphism $G \twoheadrightarrow \overline{G}$ induces epimorphisms (of additive groups)

$$C(RG) \twoheadrightarrow C(R\overline{G}), \qquad D(RG) \twoheadrightarrow D(R\overline{G}). \tag{4.1}$$

This will be a consequence of some fairly general considerations, together with the formulas given in §3. Let Λ be any R-order in the semisimple algebra A, let Λ' be a maximal R-order in A containing Λ, and let $\mathfrak{f}$ be a nonzero ideal of R such that $\mathfrak{f} \cdot \Lambda' \subset \Lambda$. Let $A \to \overline{A}$ be an epimorphism of K-algebras, and let Λ map onto the R-order $\overline{\Lambda}$. We shall show that there are epimorphisms

$$C(\Lambda) \twoheadrightarrow C(\overline{\Lambda}), \qquad D(\Lambda) \twoheadrightarrow D(\overline{\Lambda}) \tag{4.2}$$

which of course imply the analogous results for the special case in (4.1). For convenience, we treat only the case where A satisfies the Eichler condition, since the proof in the general case proceeds in an entirely similar manner.

The kernel of the map $A \to \overline{A}$ is a two-sided ideal in A, hence is a direct sum of some of the simple components of A. This kernel is therefore expressible in the form $A(1 - e)$, where e is some central idempotent in A. Then e maps onto $\overline{e} \in \overline{A}$, where $\overline{e}$ is the identity element of $\overline{A}$, and we have $A = Ae \oplus A(1 - e)$,

$Ae \cong \overline{A}$, $\Lambda e \cong \overline{\Lambda}$. Letting C again denote the maximal R-order in the center F of A, it is clear that $e \in C$, and thus $C = Ce \oplus C(1 - e)$.

Let N', N'' be reduced norm maps, where

$$N'\colon Ae \longrightarrow Fe, \qquad N''\colon A(1 - e) \longrightarrow F(1 - e).$$

Then $N = N' + N''$; that is,

$$N(x) = N'(xe) + N''(x(1 - e)), \qquad x \in A.$$

There is an obvious map from the group of C-ideals in F onto the group of Ce-ideals in Fe, given by $\mathfrak{a} \longrightarrow \mathfrak{a}e$. This map induces an epimorphism

$$\tau\colon I(C, \mathfrak{f}) \longrightarrow I(Ce, \mathfrak{f}).$$

If $x \in u(\Lambda_{\mathfrak{f}})$, then $xy = 1$ for some $y \in u(\Lambda_{\mathfrak{f}})$. Therefore, $xe \cdot ye = e$, so $xe \in u(\Lambda_{\mathfrak{f}} \cdot e)$. Furthermore, for $x \in u(\Lambda_{\mathfrak{f}})$, we obtain

$$\tau\{C \cdot N(x)\} = Ce \cdot N(x) = Ce \cdot N'(xe). \tag{4.3}$$

This implies at once that τ maps $I(\Lambda)$ into $I(\Lambda e)$, where

$$I(\Lambda) = \{C \cdot N(x)\colon x \in u(\Lambda_{\mathfrak{f}})\}, \qquad I(\Lambda e) = \{Ce \cdot N'(z)\colon z \in u(\Lambda_{\mathfrak{f}} \cdot e)\}.$$

Hence τ induces an epimorphism

$$I(C, \mathfrak{f})/I(\Lambda) \twoheadrightarrow I(Ce, \mathfrak{f})/I(\Lambda e).$$

Since $\Lambda e \cong \overline{\Lambda}$, we deduce from Theorem 3.7 that there is an epimorphism $C(\Lambda) \twoheadrightarrow C(\overline{\Lambda})$, as claimed.

Next we note that $e \in \Lambda'$, and therefore $\Lambda' = \Lambda' e \oplus \Lambda'(1 - e)$. This shows that $C(\Lambda') = C(\Lambda' e) \oplus C(\Lambda'(1 - e))$, so there is also an epimorphism $C(\Lambda') \twoheadrightarrow C(\Lambda' e)$.

It remains for us to prove the existence of an epimorphism $D(\Lambda) \twoheadrightarrow D(\overline{\Lambda})$. Now $\Lambda' e$ is a maximal order in Ae containing Λe, and

$$I(\Lambda' e) = \{Ce \cdot N'(z)\colon z = \text{unit in } \Lambda'_{\mathfrak{f}} \cdot e\}.$$

Given any unit $z \in \Lambda'_{\mathfrak{f}} \cdot e$, we may find an element $x \in u(\Lambda'_{\mathfrak{f}})$ such that $z = xe$. But then formula (4.3) shows that $Ce \cdot N'(z)$ lies in the image of τ. This proves that τ maps $I(\Lambda')$ *onto* $I(\Lambda' e)$. Therefore τ induces an epimorphism

$$I(\Lambda')/I(\Lambda) \twoheadrightarrow I(\Lambda' e)/I(\Lambda e),$$

so we have shown the existence of an epimorphism $D(\Lambda) \twoheadrightarrow D(\overline{\Lambda})$, as desired.

5. **Odd p-groups.** Let G be a finite p-group, where p is any prime, and set $A = QG$, $\Lambda = ZG$. Keep the notation of §3, especially that listed in (3.1). We may choose the ideal $\mathfrak{f} = |G| \cdot Z$, and hence we may write "prime to p" in place of

"prime to $\mathfrak{f}$" throughout. The discussion splits into two cases, depending on whether or not p is odd. We shall consider first the easier case where p is odd.

We begin by recalling some preliminary results from representation theory and algebraic number theory.

(5.1) **Theorem.** *Let G be an odd p-group, and let K_i denote the center of the ith simple component of QG. Then for each i, the field K_i is a cyclotomic field $Q(\omega)$ for some p^nth root of unity ω. There is exactly one simple component, say A_1, for which $K_1 = Q$; in fact, $A_1 = K_1 = Q$. Furthermore, each A_i is a full matrix algebra over K_i.*

Reference. Feit [6, (14.5)]; the result is due to Witt and Roquette.

(5.2) **Theorem.** *Let $K_i = Q(\omega)$, where ω is a primitive p^nth root of unity, with $n \geq 1$. Let $R_i = \text{alg int}\{K_i\}$. Then there is a unique prime ideal P_i of R_i containing p, and $R_i/P_i \cong Z/pZ$. Given any element $\alpha \in R_i$ prime to P_i, there exists an element $\beta \in R_i$ such that $\beta \equiv 1 \pmod{P_i}$, and $R_i \cdot \alpha = R_i \cdot \beta$.*

Proof. The uniqueness of P_i, and the fact that $R_i/P_i \cong Z/pZ$, both follow from the well-known result that p is completely ramified in K_i. Now let $\alpha \in R_i$ be prime to P_i; then we can choose $m \in Z$ such that $\alpha \equiv m \pmod{P_i}$, and clearly $p \nmid m$. Set $u = (\omega^m - 1)/(\omega - 1)$. Then u is a unit in R_i, and $u \equiv m \pmod{P_i}$ since $P_i = (1 - \omega)R_i$. The element $\beta = u^{-1}\alpha$ satisfies the desired conditions.

It is clear from (5.1) that A satisfies the Eichler condition, and that for each i, no infinite prime of K_i ramifies in A_i. As in §3, let $I(C, p)$ be the group of all C-ideals in F which are prime to p, and set

$$I(\Lambda') = \{C \cdot N(x): x \in u(\Lambda'_p)\}, \qquad I(\Lambda) = \{C \cdot N(x): x \in u(\Lambda_p)\}.$$

We have seen that $C(\Lambda') \cong I(C, p)/I(\Lambda')$, $C(\Lambda) \cong I(C, p)/I(\Lambda)$, and that $D(\Lambda) \cong I(\Lambda')/I(\Lambda)$. Now

$$\Lambda'_p \cong \sum_{i=1}^{m} \cdot (\Lambda_i)_p, \qquad (\Lambda_i)_p \cong \text{full matrix algebra over } (R_i)_p,$$

from which it is clear that $I(\Lambda')$ consists of all principal C-ideals in F which are prime to p. Therefore,

$$C(\Lambda') \cong \prod_{i=1}^{m} C(R_i),$$

where $C(R_i)$ is the ideal class group of R_i.

One of our main results is as follows:

(5.3) **Theorem.** *Let G be an odd p-group. Then $|D(ZG)|$ is a power of p (possibly equal to 1).*

This theorem was established by Fröhlich [8] for the case where G is an abelian p-group. We devote the remainder of this section to proving the result for an arbitrary p-group, p odd. In the next section, we shall prove the corresponding result for the case where $p = 2$.

(5.4) **Lemma.** *There is an epimorphism of multiplicative groups*

$$\theta\colon 1 + \operatorname{rad}\Lambda'_p \longrightarrow I(\Lambda')/I(\Lambda),$$

given by

$$\theta(x) = C \cdot N(x) \bmod I(\Lambda), \qquad x \in 1 + \operatorname{rad}\Lambda'_p.$$

Proof. First of all, it is clear that $1 + \operatorname{rad}\Lambda'_p$ is a multiplicative group. Next, each $x \in 1 + \operatorname{rad}\Lambda'_p$ is a unit in Λ'_p, and hence $C \cdot N(x) \in I(\Lambda')$. Therefore, θ maps $1 + \operatorname{rad}\Lambda'_p$ into $I(\Lambda')/I(\Lambda)$. Since the reduced norm map N is multiplicative, θ is a homomorphism, and we need to prove that θ is an epimorphism.

Let $C\alpha \in I(\Lambda')$, where $\alpha \in F$ is prime to p. Then $\alpha = \Sigma\alpha_i$, with $\alpha_i \in K_i$ prime to P_i (using the notation of (5.2)). Fix the notation so that $A_1 = K_1 = Q$, and $K_i \neq Q$ for $i > 1$. Choose $r \in Z$ prime to p so that $r\alpha \in C$ and $r\alpha_1 \equiv 1 \pmod p$. If we replace $C\alpha$ by $C \cdot \alpha N(r)$, the coset $\bmod I(\Lambda)$ is unchanged, but now each new α_i is an element of R_i, and $\alpha_1 \equiv 1 \pmod p$.

Changing notation, consider the element $C\alpha \in I(\Lambda')$, where $\alpha = \Sigma\alpha_i$, with each $\alpha_i \in R_i$ prime to P_i, and where $\alpha_1 \equiv 1 \pmod p$. By (5.2) we can choose $\beta_i \in R_i$ with

$$\beta_i \equiv 1 \pmod{P_i}, \qquad R_i \cdot \beta_i = R_i \cdot \alpha_i \quad \text{for all } i.$$

(For $i = 1$, take $\beta_1 = \alpha_1$.) Letting $\beta = \Sigma\beta_i$, we see that $C\alpha = C\beta$, and hence it suffices to show the existence of an element $x \in 1 + \operatorname{rad}\Lambda'_p$ such that $N(x) = \beta$.

We may write

$$\Lambda' = \sum{}^{\cdot}\Lambda_i, \qquad (\Lambda')_p = \sum{}^{\cdot}(\Lambda_i)_p = \sum{}^{\cdot}(\Lambda_i)_{P_i},$$

and thus

$$\operatorname{rad}\Lambda'_p = \sum{}^{\cdot}\operatorname{rad}(\Lambda_i)_{P_i}.$$

Now each A_i is a full matrix algebra over K_i, and so the theory of maximal orders tells us that each $(\Lambda_i)_{P_i}$ is a full matrix ring over $(R_i)_{P_i}$, and furthermore $\operatorname{rad}(\Lambda_i)_{P_i} = P_i \cdot (\Lambda_i)_{P_i}$. For each i, choose $x_i \in 1 + P_i \cdot (\Lambda_i)_{P_i} \subset A_i$ such that x_i is represented by a diagonal matrix with diagonal entries $\beta_i, 1, \cdots, 1$. Then $N_i(x_i) = \beta_i$, and setting $x = \Sigma x_i$, we have found an element $x \in 1 + \operatorname{rad}\Lambda'_p$ such that $N(x) = \beta$. This completes the proof of the lemma.

(5.5) **Lemma.** *Let Γ be a ring with unity, and let L be a left ideal of Γ such that $L \subset \operatorname{rad}\Gamma$. Define $1 + L = \{1 + x : x \in L\}$. Then $1 + L$ is a multiplicative group contained in Γ.*

Proof. Clearly $1 + L$ is closed under multiplication, and we need only check the existence of inverses. Each $x \in L$ lies in rad Γ, so $1 + x$ has a two-sided inverse w in Γ. Then $w(1 + x) = 1$, so $w = 1 - wx \in 1 + L$, as desired.

(5.6) **Lemma.** *Let us set* $X' = \text{rad}\,\Lambda'_p$, $X = X' \cap \Lambda_p$. *Then* $1 + X$ *is a subgroup of the multiplicative group* $1 + X'$, *of index a finite power of* p.

Proof. We imitate Fröhlich's proof in [8]. For sufficiently large t, we have

$$(X')^t \subset p \cdot \Lambda'_p, \qquad p^t \cdot \Lambda'_p \subset \Lambda_p.$$

Thus for large r we obtain

$$(X')^r \subset p \cdot \Lambda_p, \qquad X^r \subset p \cdot \Lambda_p \subset \text{rad}\,\Lambda_p. \tag{5.7}$$

Since X is a two-sided ideal of Λ_p, and $X^r \subset \text{rad}\,\Lambda_p$, it follows that also $X \subset \text{rad}\,\Lambda_p$. Hence $1 + X$ is a multiplicative group, by (5.5).

For $i \geq 1$, we observe that $(X')^i + X$ is a two-sided ideal of the ring $(X')^i + \Lambda_p$, and

$$\{(X')^i + X\}^{r+i} \subset (X')^{r+i} + X^{r+i} \subset p\{(X')^i + \Lambda_p\} \subset \text{rad}\,\{(X')^i + \Lambda_p\}.$$

It follows from (5.5) that $1 + (X')^i + X$ is a multiplicative subgroup of $1 + X'$.

Now consider the epimorphism

$$\mu\colon 1 + (X')^i + X \longrightarrow ((X')^i + X)/((X')^{i+1} + X)$$

defined by

$$\mu(1 + x) = x + (X')^{i+1} + X, \qquad x \in (X')^i + X.$$

It is easily seen that μ is a homomorphism of a multiplicative group onto an additive group, and that

$$\text{kernel of } \mu = 1 + (X')^{i+1} + X.$$

Therefore

$$\frac{1 + (X')^i + X}{1 + (X')^{i+1} + X} \cong \frac{(X')^i + X}{(X')^{i+1} + X}. \tag{5.8}$$

Since $(X')^r \subset X$ by (5.7), we have

$$[1 + X' : 1 + X] = \prod_{i=1}^{r-1} [1 + (X')^i + X : 1 + (X')^{i+1} + X]$$

$$= \prod_{i=1}^{r-1} [(X')^i + X : (X')^{i+1} + X],$$

with the last equality a consequence of (5.8). Thus

$$[1 + X' : 1 + X] = [X' : X].$$

But $p^t X' \subset X$, and X' is finitely generated over R. Hence the index $[X' : X]$ is a finite power of p, and the lemma is established.

We are now ready to conclude the proof of our Theorem 5.3. We have just shown that $1 + X$ is a subgroup of $1 + X'$, of p-power index. Denote by $(1 + X)^*$ the normal closure of $1 + X$ in $1 + X'$. Then $(1 + X)^*$ is generated by elements of the form $y(1 + x)y^{-1}$, $y \in 1 + X'$, $x \in X$. Let $\theta: 1 + X' \to I(\Lambda')/I(\Lambda)$ be the epimorphism defined in (5.4). Then

$$\theta\{y(1 + x)y^{-1}\} = C \cdot N(1 + x) \bmod I(\Lambda),$$
$$= 1 \bmod I(\Lambda),$$

since $1 + x \in u(\Lambda_p)$. Hence θ induces an epimorphism

$$(1 + X')/(1 + X)^* \twoheadrightarrow I(\Lambda')/I(\Lambda) \cong D(\Lambda).$$

Since $[1 + X' : (1 + X)^*]$ is a divisor of $[1 + X' : 1 + X]$, it follows from (5.6) that $(1 + X')/(1 + X)^*$ is a finite p-group. Hence $D(\Lambda)$ is also a finite p-group, and the theorem is proved.

Professor L. McCulloh has suggested an alternative proof of (5.3). Denote by $I_0(C, \mathfrak{f})$ the subgroup consisting of all principal ideals of $I(C, \mathfrak{f})$, and by $S(C, \mathfrak{f})$ the subgroup of $I_0(C, \mathfrak{f})$ consisting of ideals which possess a generator α such that $\alpha \equiv 1 \pmod^* \mathfrak{f}$.(4) Those ideals $C \cdot \Sigma \alpha_i$, $\alpha_i \in K_i$, which satisfy the additional condition that $(\alpha_i)_{\hat{P}} > 0$ at those infinite primes P of K_i ramified in A_i, form a subgroup denoted by $S^+(C, \mathfrak{f})$. Of course, I_0, S, S^+ are the direct sums of the corresponding groups for each simple component.

In [9, proof of Lemma 2.6] Jacobinski proved that $I(\Lambda) \supset S^+(C, \mathfrak{f})$ if A satisfies the Eichler condition, so we have a chain of ideal groups

$$I_0(C, \mathfrak{f}) \supset I(\Lambda') \supset I(\Lambda) \supset S^+(C, \mathfrak{f}).$$

Now take $\Lambda = ZG$, G an odd p-group of order p^n. In this case $S(C, \mathfrak{f}) = S^+(C, \mathfrak{f})$. We first show that $I_0(R_i, \mathfrak{f})/S(R_i, \mathfrak{f})$ is a (finite) p-group for $i > 1$. By (7.12) we must show that $u(R_i/p^n R_i)/u'(R_i)$ is a p-group. Now the numerator has order equal to $(p - 1)$ times a p-power. Since $u'(R_i)$ contains the subgroup of order $p - 1$ generated by the cyclotomic units $(1 - \omega^r)/(1 - \omega)$, r prime to p, it follows that $u(R_i/p^n R_i)/u'(R_i)$ is a p-group. (We have used (5.1) and (5.2).)

Now $A_1 = K_1 = Q$ and

$$I_0(Z, p^n Z)/S(Z, p^n Z) \cong u(Z/p^n Z)/\{\pm 1\}.$$

(4) This notation is explained in §7 just before (7.12).

The second paragraph of the proof of (5.4) shows that the A_1-component of any element of $I(\Lambda')$ modulo $I(\Lambda)$ has a generator which is integral and $\equiv 1 \pmod{p}$. It follows that $I(\Lambda')/I(\Lambda)$ is a p-group, as claimed.

6. **The case $p = 2$.** We now turn to the more difficult case where G is a finite 2-group, again setting $A = QG$, $\Lambda = ZG$, and keeping the notation of §3. For certain choices of G, the algebra A may fail to satisfy the Eichler condition, and thus we must use Theorem 3.11 rather than (3.7) in order to calculate $D(\Lambda)$. We have $D(\Lambda) \cong J(\Lambda')/J(\Lambda)$, where

$$J(\Lambda') = \{C \cdot N^*(x): x = \text{unit in } E(\Lambda'_2 \dotplus \Lambda'_2)\},$$

$$J(\Lambda) = \{C \cdot N^*(x): x = \text{unit in } E(\Lambda_2 \dotplus \Lambda_2)\}.$$

We are going to prove the analogue of Theorem 5.3 for the present case, namely:

(6.1) **Theorem.** *For any 2-group G, the order of $D(ZG)$ is a power of 2 (possibly equal to 1).*

To start with, we need a pair of preliminary results.

(6.2) **Theorem.** *Let G be a 2-group. For each i, the center K_i of the ith simple component A_i of A is a subfield of a cyclotomic field $Q(\omega)$, where ω is some 2^nth root of unity. There is a unique prime ideal P_i of R_i containing 2, and $R_i/P_i \cong Z/2Z$. Each $\alpha \in R_i$ which is prime to P_i satisfies the congruence $\alpha \equiv 1 \pmod{P_i}$.*

Proof. The field K_i is obtained from Q by adjoining values of irreducible complex characters of G (see [3] or [6]). Therefore, $K_i \subset Q(\omega)$ for some 2^nth root of unity ω. The remaining assertions are obvious, since 2 ramifies completely in $Q(\omega)$, hence also in K_i.

(6.3) **Theorem (Eichler [5]).** *Let $S = \text{alg int}\{L\}$, and let Γ be a maximal S-order in the simple algebra B with center L. Assume that B satisfies the Eichler condition. Let $N: B \to L$ be the reduced norm map, and let $\mathfrak{a}$ be any two-sided ideal of Γ. Let $x \in \Gamma$ be such that*

$$N(x) \equiv \text{unit of } S \pmod{S \cap \mathfrak{a}}.$$

Then there exists a unit u of Γ such that $x \equiv u \pmod{\mathfrak{a}}$.

Taking this result for granted, we continue with the proof of Theorem 6.1. We have seen in §3 that $E(A \dotplus A)$ is a semisimple algebra with center F, and that A satisfies the Eichler condition. Furthermore, $E(\Lambda' \dotplus \Lambda')$ is a maximal R-order in $E(A \dotplus A)$. To simplify the notation, let us write

$$E' = E(\Lambda' \dotplus \Lambda') = \sum_{i=1}^{m}{}^{\cdot} E^i, \quad \text{where } E^i = E(\Lambda_i \dotplus \Lambda_i).$$

Let $N_i^*: E(A_i \dotplus A_i) \longrightarrow K_i$ be the reduced norm map, and define $N^*: E(A \dotplus A) \longrightarrow F$ by setting $N^* = \Sigma^{\cdot} N_i^*$.

(6.4) **Lemma.** *There is an epimorphism of multiplicative groups*

$$\varphi: 1 + \operatorname{rad} E'_2 \longrightarrow J(\Lambda'),$$

given by $\varphi(y) = C \cdot N^*(y)$, $y \in 1 + \operatorname{rad} E'_2$. *Here,* E'_2 *denotes the localization of* E' *at the rational prime* 2.

Proof. As in the proof of (5.4), it is clear that φ gives a multiplicative homomorphism of the group $1 + \operatorname{rad} E'_2$ into the group $J(\Lambda')$. This latter group is generated by the set of elements

$$\{C \cdot N^*(x): x \in E', \ x \text{ prime to } 2\}.$$

Hence, to show that φ is epic, it suffices to show that for each such x we can find an element $y \in 1 + \operatorname{rad} E'_2$ such that $C \cdot N^*(y) = C \cdot N^*(x)$.

We observe that

$$E'_2 = \sum{}^{\cdot} (E^i)_2 = \sum{}^{\cdot} (E^i)_{P_i}, \qquad \operatorname{rad} E'_2 = \sum{}^{\cdot} \operatorname{rad} (E^i)_{P_i},$$

with the $\{P_i\}$ defined as in (6.2). The entire computation can be performed componentwise, so our problem reduces to the following:

Given $x_i \in E^i$ prime to P_i, show that there exists an element $y_i \in 1 + \operatorname{rad} (E^i)_{P_i}$ such that

$$R_i \cdot N_i^*(y_i) = R_i \cdot N_i^*(x_i). \tag{6.5}$$

Now $N_i^*(x_i) \in R_i$ is prime to P_i (since x_i is prime to P_i), and therefore (by (6.2)) $N_i^*(x_i) \equiv 1 \pmod{P_i}$. We shall now use (6.3) for the case when $B = E(A_i \dotplus A_i)$, $\Gamma = E^i = E(\Lambda_i \dotplus \Lambda_i)$, $L = K_i$, $S = R_i$, $\mathfrak{a} = P_i E^i$, $\mathfrak{a} \cap S = P_i$. It follows that there exists a unit $u_i \in E^i$ such that

$$x_i \equiv u_i \pmod{P_i E^i}.$$

Hence $u_i^{-1} x_i \equiv 1 \pmod{P_i E^i}$, and thus

$$u_i^{-1} x_i - 1 \in P_i E^i \subset \operatorname{rad} (E^i)_{P_i}.$$

Let us now set $y_i = u_i^{-1} x_i$, so $y_i \in 1 + \operatorname{rad} (E^i)_{P_i}$. Since $N_i^*(u_i)$ is a unit in R_i, it is clear that (6.5) is valid. Thus y_i has the desired properties, and if we set $y = \Sigma\, y_i$, then

$$y \in 1 + \operatorname{rad} E'_2, \quad C \cdot N^*(y) = C \cdot N^*(x).$$

This completes the proof of the lemma.

Remark. If we had used Eichler's Theorem 6.3 for the case where p is odd, we would not have needed to use the result from (5.1) that A_i is a full matrix algebra over K_i.

It is now an easy matter to complete the proof that $|D(ZG)|$ is a power of 2. The argument given at the end of §5 carries over unchanged to the present case, and shows that φ induces an epimorphism

$$(1 + Y')/(1 + Y)^* \twoheadrightarrow J(\Lambda')/J(\Lambda) \cong D(\Lambda),$$

where

$$Y' = \operatorname{rad} E'_2, \qquad Y = Y' \cap \{E(\Lambda \dotplus \Lambda)\}_2,$$

and $(1 + Y)^*$ = normal closure of $1 + Y$ in $1 + Y'$. As in §5, the index $[1 + Y': 1 + Y]$ is a power of 2. Thus the order of $D(ZG)$ is also a power of 2, as claimed.

Next we shall sketch an alternate proof of (6.1), which parallels that given at the end of §5. Set $E' = E(\Lambda' \dotplus \Lambda')$ and $E = E(\Lambda \dotplus \Lambda)$. The centers of Λ' and E' are isomorphic to C, and we have $J(\Lambda') \cong I(E')$, $J(\Lambda) \cong I(E)$. Since KE' satisfies the Eichler condition, we have a chain

$$I_0(C, \mathfrak{f}) \supset J(\Lambda') \supset J(\Lambda) \supset S^+(C, \mathfrak{f}).$$

Let $|G| = 2^n$, $\mathfrak{f} = 2^n Z$. Using (7.12) and the fact that $|u(R_i/2^n R_i)|$ is a power of 2, we see that $I_0(R_i, 2^n R_i)/S(R_i, 2^n R_i)$ is a 2-group for all i. But $S(C, \mathfrak{f})/S^+(C, \mathfrak{f})$ is also a 2-group, whence so is $J(\Lambda')/J(\Lambda)$, as desired.

7. **Cyclic groups of order $2p$.** Throughout this section, let p be an odd prime, and let G be cyclic of order $2p$. We shall calculate $C(ZG)$ and $D(ZG)$ explicitly, and we begin with a few elementary results on units in cyclotomic fields. To fix the notation, let ω be a primitive pth root of unity, and set

$$\begin{aligned} &K = Q(\omega), \quad R = \text{alg int}\{K\} = Z[\omega], \quad P = (1 - \omega)R, \\ &L = Q(\omega + \omega^{-1}), \quad S = \text{alg int}\{L\} = Z[\omega + \omega^{-1}]. \end{aligned} \tag{7.1}$$

Then P is the unique prime ideal of R containing p, and we have

$$R/P \cong S/(P \cap S) \cong Z/pZ = \bar{Z} \quad \text{(say)}. \tag{7.2}$$

For each $r \in Z$, define

$$\xi_r = (\omega^r - \omega^{-r})/(\omega - \omega^{-1}) \in S. \tag{7.3}$$

If $p \nmid r$, then ω is a power of ω^r, and hence $\xi_r^{-1} \in S$. Thus ξ_r is a unit in S whenever $p \nmid r$.

Furthermore, for each $r \in Z$ we obtain

$$\xi_r \equiv r \pmod{P}. \tag{7.4}$$

This follows at once from the equations

$$\xi_r = (\omega^{-r}/\omega^{-1}) \cdot (1 - \omega^{2r})/(1 - \omega^2) = \omega^{1-r}(1 + \omega^2 + \omega^4 + \cdots + \omega^{2r-2})$$
$$\equiv r \pmod{P}, \quad \text{since } P = (1 - \omega)R.$$

Next, an elementary calculation yields

$$\xi_r^2 - \xi_s^2 = \omega^{2-2r} \cdot \frac{\omega^{2(r-s)} - 1}{\omega^2 - 1} \cdot \frac{\omega^{2(r+s)} - 1}{\omega^2 - 1}.$$

If $r \equiv \pm s \pmod{p}$, this shows that $\xi_r^2 - \xi_s^2 = 0$. If $r \not\equiv \pm s \pmod{p}$, each of the three factors on the right-hand side of the above displayed equations is a unit in R, and hence $\xi_r^2 - \xi_s^2$ is a unit in S. We have thus proved the following result, which however will not be needed until §8:

(7.5) **Lemma.** *For $r, s \in Z$, define ξ_r, ξ_s as in* (7.3). *Then*

$$\xi_r^2 - \xi_s^2 = \begin{cases} 0, & r \equiv \pm s \pmod{p}, \\ \text{unit in } S, & \text{otherwise.} \end{cases}$$

We may describe the cyclic group G of order $2p$ in terms of generators and relations; thus

$$G = \langle \sigma, \tau : \sigma^p = 1,\ \tau^2 = 1,\ \sigma\tau = \tau\sigma \rangle.$$

Let $H = \langle \tau \rangle$ be the subgroup of G of order 2. Our main result here is as follows:

(7.6) **Theorem.** *Let $u'(R)$ be the image of $u(R)$ in $u(R/2R)$. Then*

$$D(ZG) \cong u(R/2R)/u'(R),$$

and consequently

$$|C(ZG)| = |C(R)|^2[u(R/2R) : u'(R)],$$

where $C(R)$ is the ideal class group of R.

In proving Theorem 7.6, as well as in later calculations, we shall need some remarks on pullback diagrams (= fibre products). Let $\mathfrak{a}$, $\mathfrak{b}$ be two-sided ideals of an arbitrary ring Λ with 1, not necessarily commutative. Then it is easily verified that there is a pullback diagram

(7.7)
$$\begin{array}{ccc} \dfrac{\Lambda}{\mathfrak{a} \cap \mathfrak{b}} & \longrightarrow & \dfrac{\Lambda}{\mathfrak{a}} \\ \downarrow & & \downarrow \\ \dfrac{\Lambda}{\mathfrak{b}} & \longrightarrow & \dfrac{\Lambda}{\mathfrak{a} + \mathfrak{b}} \end{array}$$

that is,

$$\Lambda/(\mathfrak{a} \cap \mathfrak{b}) \cong \{(x, y) \in (\Lambda/\mathfrak{a}) \dotplus (\Lambda/\mathfrak{b}): x \equiv y \bmod (\mathfrak{a} + \mathfrak{b})\}.$$

We apply this to the case where $\Lambda = ZG$, with G cyclic of order $2p$ as above. We pick

$$\mathfrak{a} = \Phi(\sigma) \cdot \Lambda, \qquad \mathfrak{b} = (\sigma - 1) \cdot \Lambda, \tag{7.8}$$

where $\Phi(X) = 1 + X + \cdots + X^{p-1}$ is the cyclotomic polynomial of order p. Since QG is free as $Q[\sigma]$-module, it is clear that $\mathfrak{a} \cap \mathfrak{b} = 0$. Furthermore, there are ring isomorphisms

$$\Lambda/\mathfrak{a} \cong RH, \qquad \Lambda/\mathfrak{b} \cong ZH, \qquad \Lambda/(\mathfrak{a} + \mathfrak{b}) \cong \overline{Z}H,$$

with $\overline{Z} = Z/pZ \cong R/P$. The first of these isomorphisms is obtained by letting $\sigma \to \omega$, the second by $\sigma \to 1$, the third by $\sigma \to 1$, $Z \to \overline{Z}$. The pullback diagram (7.7) becomes

$$\begin{array}{ccc} \Lambda & \longrightarrow & RH \\ \downarrow & & \downarrow \\ ZH & \longrightarrow & \overline{Z}H \end{array} \tag{7.9}$$

We shall use bars to indicate images of elements of ZH or RH in $\overline{Z}H$. Tensoring with Q, we see that QG can be identified with $QH \dotplus KH$, and that the maximal order Λ' of QG may be identified with $Z^{(2)} \dotplus R^{(2)}$. Further,

$$\Lambda \cong \{(\xi, \eta) \in ZH \dotplus RH: \overline{\xi} = \overline{\eta} \text{ in } \overline{Z}H\}. \tag{7.10}$$

Once Λ' has been identified with $Z^{(2)} \dotplus R^{(2)}$, it remains for us to describe Λ as a subring of Λ'. Now $QH \cong Q^{(2)}$, $KH \cong K^{(2)}$, and

$$ZH \cong \{(a_0, a_1) \in Z^{(2)}: a_0 \equiv a_1 \pmod{2Z}\},$$

$$RH \cong \{(b_0, b_1) \in R^{(2)}: b_0 \equiv b_1 \pmod{2R}\}.$$

It follows from these isomorphisms, together with (7.10), that we may identify Λ with the subring of Λ' consisting of all 4-tuples $(a_0, a_1, b_0, b_1) \in Z^{(2)} \dotplus R^{(2)}$ which satisfy the congruence conditions

$$a_0 \equiv a_1 \pmod{2Z}, \quad b_0 \equiv b_1 \pmod{2R}, \quad a_0 \equiv b_0, \ a_1 \equiv b_1 \pmod{P}. \tag{7.11}$$

Now $D(\Lambda) \cong I(\Lambda')/I(\Lambda)$ by Theorem 3.7. In our particular case, $C = \Lambda'$ and the reduced norm map N is the identity map. Thus

$$I(\Lambda') = \{\Lambda' \cdot x: x \in u(\Lambda'_{2p})\}, \qquad I(\Lambda) = \{\Lambda' \cdot y: y \in u(\Lambda_{2p})\}.$$

Denote by $I_0(R, \mathfrak{c})$ the group of all principal R-ideals in K prime to the ideal $\mathfrak{c}$ of R, and define $I_0(Z, m)$ analogously as the group of Z-ideals in Q prime to the integer m. Since $\Lambda' = Z^{(2)} \dotplus R^{(2)}$, we have

$$I(\Lambda') = \{I_0(Z, 2p)\}^{(2)} \dotplus \{I_0(R, 2P)\}^{(2)}.$$

Before proceeding further, we require two lemmas, the first of which is a general result true for any algebraic number field Ω. Let $\mathfrak{O} = \text{alg int}\{\Omega\}$, let $\mathfrak{q}$ be a nonzero ideal of $\mathfrak{O}$, and write $\mathfrak{q} = \prod \mathfrak{p}_i^{e_i}$, $e_i > 0$, with the $\{\mathfrak{p}_i\}$ distinct prime ideals of $\mathfrak{O}$. Let v_i be the normalized $\mathfrak{p}_i$-adic valuation on Ω. For $x \in \Omega$, we shall write $x \equiv 1 \pmod^* \mathfrak{q}$, if and only if $v_i(x-1) \geq e_i$ for each $\mathfrak{p}_i$ dividing $\mathfrak{q}$. Let $I_0(\mathfrak{O}, \mathfrak{q})$ be the group of principal $\mathfrak{O}$-ideals in Ω prime to $\mathfrak{q}$, and let $S(\mathfrak{O}, \mathfrak{q})$ be the subgroup of $I_0(\mathfrak{O}, \mathfrak{q})$ defined by

$$S(\mathfrak{O}, \mathfrak{q}) = \{x\mathfrak{O}: x \in \Omega,\ x \neq 0,\ x \equiv 1 \bmod^* \mathfrak{q}\}.$$

(7.12) **Lemma.** *Let $\mathfrak{q}$ and $\mathfrak{r}$ be relatively prime ideals of $\mathfrak{O}$, and let $u'(\mathfrak{O})$ be the image of $u(\mathfrak{O})$ in $u(\mathfrak{O}/\mathfrak{q})$. Then*

$$\frac{I_0(\mathfrak{O},\ \mathfrak{q}\mathfrak{r})}{I_0(\mathfrak{O},\ \mathfrak{q}\mathfrak{r}) \cap S(\mathfrak{O},\ \mathfrak{q})} \cong \frac{u(\mathfrak{O}/\mathfrak{q})}{u'(\mathfrak{O})}.$$

Hence $I_0(\mathfrak{O}, \mathfrak{q}\mathfrak{r}) \subset S(\mathfrak{O}, \mathfrak{q})$ whenever $u'(\mathfrak{O}) = u(\mathfrak{O}/\mathfrak{q})$.

Proof. Define a mapping $\kappa: I_0(\mathfrak{O}, \mathfrak{q}\mathfrak{r}) \to u(\mathfrak{O}/\mathfrak{q})/u'(\mathfrak{O})$ by setting $\kappa(x\mathfrak{O}) =$ coset containing $\overline{x}$, where the element $x \in \Omega$ prime to $\mathfrak{q}\mathfrak{r}$ maps onto $\overline{x} \in u(\mathfrak{O}/\mathfrak{q})$. Clearly κ is a well-defined homomorphism. Further, κ is epic, since given any $\alpha \in u(\mathfrak{O}/\mathfrak{q})$, we can find an element $x \in \Omega$ such that $\overline{x} = \alpha$, $x \equiv 1 \pmod^* \mathfrak{r}$, and then $\kappa(x\mathfrak{O})$ equals the coset containing α.

It remains to determine $\ker \kappa$. Let $\kappa(x\mathfrak{O}) = 1$, where $x \in \Omega$ is prime to $\mathfrak{q}\mathfrak{r}$. Then $\overline{x} \in u'(\mathfrak{O})$; that is, $x \equiv u \pmod^* \mathfrak{q}$ for some $u \in u(\mathfrak{O})$. But then $x\mathfrak{O} = xu^{-1} \cdot \mathfrak{O} \in S(\mathfrak{O}, \mathfrak{q})$, which proves that

$$\ker \kappa \subset I_0(\mathfrak{O},\ \mathfrak{q}\mathfrak{r}) \cap S(\mathfrak{O},\ \mathfrak{q}).$$

The reverse inclusion is obvious, so the lemma is established.

Now observe that $u'(R) = u(R/P)$ by (7.4), so by the second statement in the lemma we obtain

$$I_0(R, 2P) \subset S(R, P). \tag{7.13}$$

We shall use this in a moment.

(7.14) **Lemma.** *Let $u''(R)$ be the image in $u(R/2R)$ of the group $\{u \in u(R): u \equiv 1 \pmod P\}$. Then $u''(R) = u'(R)$.*

Proof.(5) Obviously $u''(R) \subset u'(R)$, and we must prove the reverse inclusion. Let $u \in u(R)$ be given; we need to find a unit v in R such that $v \equiv u \pmod{2R}$, $v \equiv 1 \pmod P$. Let θ be the automorphism of K defined by letting $\omega \to \omega^2$. Then

$$u^\theta \equiv u^2 \pmod{2R}, \qquad u^\theta \equiv u \pmod P,$$

(5) The authors wish to thank Professor L. McCulloh for providing this simple proof.

and we need only choose $v = u^{\theta}/u$.

We shall now complete the proof of Theorem 7.6 by constructing an epimorphism

$$\psi: I(\Lambda') \longrightarrow u(R/2R)/u'(R)$$

with kernel $I(\Lambda)$. Let bars denote images in $u(R/2R)$, and define

$$\psi(Za_0, Za_1, Rb_0, Rb_1) = \text{coset containing } \overline{b}_0/\overline{b}_1,$$

where $a_i \in u(Z_{2p})$, $b_i \in u(R_{2P})$. Clearly, ψ is a homomorphism. It is epic because the map $I_0(R, 2P) \longrightarrow u(R/2R)/u'(R)$ is already epic, as follows from the proof of (7.12).

We see from (7.11) that $u(\Lambda_{2p})$ consists of all 4-tuples

$$(a_0, a_1, b_0, b_1), \qquad a_i \in u(Z_{2p}),\ b_i \in u(R_{2P}),$$

which satisfy the conditions

(7.15) $a_0 \equiv a_1 \pmod{{}^*2Z}$, $b_0 \equiv b_1 \pmod{{}^*2R}$, $a_0 \equiv b_0$, $a_1 \equiv b_1 \pmod{{}^*P}$.

For each such 4-tuple we have $\overline{b}_0 = \overline{b}_1$, whence $I(\Lambda) \subset \ker \psi$. To prove the reverse inclusion, let $(Za_0, Za_1, Rb_0, Rb_1) \in I(\Lambda')$ lie in the kernel of ψ. By (7.13), there exist elements $c_0, c_1 \in K$ such that

$$Rb_i a_i^{-1} = Rc_i, \quad c_i \equiv 1 \pmod{{}^*P}, \qquad i = 1, 2.$$

Hence $Rb_i = Ra_i c_i$, so replacing b_i by $a_i c_i$, we may henceforth assume that $a_0 \equiv b_0$, $a_1 \equiv b_1 \pmod{{}^*P}$. But $\psi(Za_0, Za_1, Rb_0, Rb_1) = 1$ implies that $\overline{b}_0/\overline{b}_1 \in u'(R)$, so by (7.14) there exists a unit $u \in R$ such that $b_0 \equiv b_1 u \pmod{{}^*2R}$, $u \equiv 1 \pmod{P}$. Replacing b_1 by $b_1 u$ does not affect the congruence $a_1 \equiv b_1 \pmod{{}^*P}$, and permits us to assume that $b_0 \equiv b_1 \pmod{{}^*2R}$. Since trivially $a_0 \equiv a_1 \pmod{{}^*2Z}$, we may conclude that the 4-tuple (a_0, a_1, b_0, b_1) satisfies all of the conditions in (7.15), and hence that $(Za_0, Za_1, Rb_0, Rb_1) \in I(\Lambda)$. This completes the proof of the assertion about $D(\Lambda)$. The second assertion in (7.6) is then obvious, since $C(\Lambda') \cong C(R) \times C(R)$.

As a matter of fact, the epimorphism $\Lambda \longrightarrow RH$ induces epimorphisms $D(ZG) \longrightarrow D(RH)$, $C(ZG) \longrightarrow C(RH)$. Ullom [16] has previously shown that

$$|D(RH)| = [u(R/2R) : u'(R)],$$

from which we may conclude that $D(ZG) \cong D(RH)$ and $C(ZG) \cong C(RH)$. These latter conclusions can also be obtained directly from (7.9) by use of Milnor's Mayer-Vietoris sequence (see [18]), but one is then left with the problem of calculating $D(RH)$.

8. **Dihedral groups of order $2p$.** Let G be the dihedral group of order $2p$, where p is an odd prime. We shall again use the notation introduced in (7.1), so

that S is the ring of algebraic integers in the subfield L of the cyclotomic field K. The class group $C(S)$ is then the ideal class group of S. We shall prove

$$C(ZG) \cong C(S), \qquad D(ZG) = 1. \tag{8.1}$$

These results are immediate consequences of Lee's classification [10] of ZG-lattices. Our proof is more direct, but of course provides no information about the nonprojective ZG-lattices.

Throughout this section, we put

$$G = \langle \sigma, \tau: \sigma^p = 1, \tau^2 = 1, \tau\sigma\tau^{-1} = \sigma^{-1} \rangle, \qquad H = \langle \tau: \tau^2 = 1 \rangle,$$

and set $A = QG$, $\Lambda = ZG$. Let $x \to x'$ be the L-automorphism of K induced by the map $\omega \to \omega^{-1}$ (see (7.1)). We introduce the twisted group algebra

$$K\langle \tau \rangle = K \oplus K\tau, \qquad \tau x = x' \cdot \tau, \qquad x \in K.$$

Then $K\langle \tau \rangle$ is a simple algebra with center L, and is split by K:

$$K\langle \tau \rangle \cong \mathrm{Hom}_L(K, K).$$

The isomorphism is obtained by mapping $x + y\tau \in K\langle \tau \rangle$ onto $\phi_{x+y\tau}$, where $\phi_{x+y\tau}(u) = xu + yu'$, $u \in K$. On the other hand, $K\langle \tau \rangle$ is a cyclic algebra, and as such has a matrix representation over K given by

$$x + y\tau \to \begin{pmatrix} x & y \\ y' & x' \end{pmatrix}, \qquad x, y \in K.$$

If $N: K\langle \tau \rangle \to L$ is the reduced norm map, the above implies that

$$N(x + y\tau) = \begin{vmatrix} x & y \\ y' & x' \end{vmatrix} = xx' - yy'. \tag{8.2}$$

We may make $K\langle \tau \rangle$ into a QG-module by letting σ act as multiplication by ω on the coefficients from K. The decomposition of A into simple components is then given by $A = Q \dotplus Q \dotplus K\langle \tau \rangle$. The first summand affords the trivial representation $\sigma \to 1, \tau \to 1$, while the second gives $\sigma \to 1, \tau \to -1$.

Let us use a pullback diagram to describe the elements of Λ in terms of their projections into the simple components of A. Since the cyclic subgroup $[\sigma]$ generated by σ is normal in G, the ideals $\mathfrak{a}$, $\mathfrak{b}$ of Λ defined by (7.8) are two-sided ideals of Λ. Furthermore, $\mathfrak{a} \cdot \mathfrak{b} = 0$ since QG is $Q[\sigma]$-free. Let

$$R\langle \tau \rangle = R \oplus R\tau \subset K\langle \tau \rangle.$$

Then there are ring isomorphisms

$$\Lambda/\mathfrak{b} \cong ZH, \qquad \Lambda/\mathfrak{a} \cong R\langle \tau \rangle, \qquad \Lambda/(\mathfrak{a} + \mathfrak{b}) \cong \overline{Z}H,$$

with $\overline{Z}$ as in (7.2). The pullback diagram (7.7) then becomes

(8.3)
$$\begin{array}{ccc} \Lambda & \xrightarrow{\alpha} & R\langle\tau\rangle \\ \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\mu} \\ ZH & \longrightarrow & \overline{Z}H \end{array}$$

The map μ is given by $\mu(x + y\tau) = \overline{x} + \overline{y}\tau$, where $x \in R$ maps onto $\overline{x} \in R/P \cong \overline{Z}$. Since $x \equiv x' \pmod{P}$ for $x \in R$, we see that $(\mathrm{mod}\ P)\ \tau$ commutes with the elements of R, and hence $\overline{Z}H$ is an ordinary untwisted group algebra. Further, α is just the projection of Λ into the simple component $K\langle\tau\rangle$, while β is the projection into $Q \dotplus Q$, once we identify QH with $Q \dotplus Q$.

In the isomorphism $QH \cong Q \dotplus Q$, the ring ZH is identified with

$$\{(a_0, a_1) \in Z \dotplus Z: a_0 \equiv a_1 \pmod{2}\}.$$

It then follows from (8.3) that we may identify Λ with the ring of all triples $\{(a_0, a_1, x + y\tau) \in Z \dotplus Z \dotplus R\langle\tau\rangle\}$ satisfying the congruences

(8.4) $\quad a_0 \equiv a_1 \pmod{2},\ x \equiv (a_0 + a_1)/2 \pmod{P},\quad y \equiv (a_0 - a_1)/2 \pmod{P}.$

Now let Λ' be a maximal Z-order in A containing Λ. Since each simple component of A is a full matrix algebra over its center, surely A satisfies the Eichler condition. Furthermore, the discussion in §3(i) shows that

$$I(\Lambda') = \{C \cdot \alpha: \alpha \in F,\ \alpha \text{ prime to } 2p\}$$

$$= \{(Zb_0, Zb_1, S\beta): b_0, b_1 \in Q,\ \beta \in L, \text{ with } b_0, b_1, \beta \text{ prime to } 2p\}.$$

On the other hand, $I(C, 2p)$ consists of all C-ideals in F which are prime to $2p$. Therefore (by (3.7))

$$C(\Lambda') \cong I(C, 2p)/I(\Lambda') \cong C(Z) \times C(Z) \times C(S) \cong C(S),$$

where $C(Z)$ = ideal class group of Z, and so on. By (3.7) we have $D(\Lambda) \cong I(\Lambda')/I(\Lambda)$, where

$$I(\Lambda) = \{C \cdot N(x): x \in \Lambda,\ x \text{ prime to } 2p\}.$$

We shall show below that $I(\Lambda) = I(\Lambda')$. This will imply that $D(\Lambda) = 1$ and $C(\Lambda) \cong C(\Lambda') \cong C(S)$, as claimed in (8.1).

(8.5) **Lemma.** (i) *The map* $\mu: R\langle\tau\rangle \longrightarrow \overline{Z}H$ *induces an epimorphism of unit groups:* $u(R\langle\tau\rangle) \twoheadrightarrow u(\overline{Z}H)$.

(ii) *Let* $\beta \in S$ *be prime to* p. *Then there exists an element* $x + y\tau \in R\langle\tau\rangle$ *such that* $S \cdot N(x + y\tau) = S\beta$.

Proof. (i) Each element of $\overline{Z}H$ is of the form $\overline{r} + \overline{s}\tau$, where $r, s \in Z$ have images $\overline{r}, \overline{s} \in \overline{Z}$. Since $(\overline{r} + \overline{s}\tau)(\overline{r} - \overline{s}\tau) = \overline{r}^2 - \overline{s}^2$, we see that $\overline{r} + \overline{s}\tau \in u(\overline{Z}H)$ if and only if $\overline{r}^2 \neq \overline{s}^2$. Given such a unit $\overline{r} + \overline{s}\tau$, we may form $\xi_r + \xi_s\tau \in R\langle\tau\rangle$. Now τ commutes with the ξ's, since they lie in S. It follows from (7.5) that $\xi_r + \xi_s\tau$ is

a unit in $R\langle\tau\rangle$, and clearly $\mu(\xi_r + \xi_s\tau) = \bar{r} + \bar{s}\tau$, as desired.

(ii) We have $S/(P \cap S) \cong \bar{Z}$, so $\beta \equiv r \pmod{P}$ for some $r \in Z$ with $p \nmid r$. The element ξ_r given in (7.3) is a unit in S such that $\xi_r \equiv r \pmod{P}$. Setting $\alpha = \beta \cdot \xi_r^{-1}$, we obtain

$$S \cdot \beta = S \cdot \alpha, \qquad \alpha \equiv 1 \pmod{P}.$$

It then suffices to find an element $x + y\tau \in R\langle\tau\rangle$ such that $N(x + y\tau) = \alpha$. We may set

$$\alpha = 1 - \gamma(\omega - \omega^{-1})^2/(\omega^2 + \omega^{-2})$$

for some $\gamma \in S$. Then define $x = x_0 + x_1\omega$, $y = y_0 + y_1\omega$, where $x_0 = 1 - \gamma$, $y_0 = \alpha - x_0$, $x_1 = -y_1 = (\omega + \omega^{-1})y_0/2$. It is then easily checked that $x + y\tau \in R\langle\tau\rangle$, and $N(x + y\tau) = xx' - yy' = \alpha$.

Let $\lambda \in \Lambda$ correspond to the triple $(a_0, a_1, x + y\tau)$; then

$$C \cdot N(\lambda) = Za_0 \dotplus Za_1 \dotplus S \cdot N(x + y\tau).$$

Further, λ is prime to $2p$ if and only if a_0, a_1, and $x + y\tau$ are prime to $2p$. Now $I(\Lambda')$ is generated by ideals of the form

$$Zb_0 \dotplus Zb_1 \dotplus S\beta, \qquad b_0, b_1, \beta \text{ prime to } 2p. \tag{8.6}$$

In order to show that $I(\Lambda') = I(\Lambda)$, we must show that given the ideal in (8.6), we can choose a_0, a_1, $x + y\tau$ prime to $2p$, and satisfying (8.4), such that

$$Za_0 = Zb_0, \quad Za_1 = Zb_1, \quad S \cdot N(x + y\tau) = S\beta. \tag{8.7}$$

Indeed, we pick $a_0 = b_0$, $a_1 = b_1$, and we must find $x + y\tau \in R\langle\tau\rangle$ such that

$$x \equiv (b_0 + b_1)/2, \quad y \equiv (b_0 - b_1)/2 \pmod{P}, \quad S \cdot N(x + y\tau) = S \cdot \beta.$$

Let $c_1 = (b_0 + b_1)/2$, $c_2 = (b_0 - b_1)/2$, so $c_1^2 - c_2^2 = b_0b_1$, whence in Z we have $\bar{c}_1^2 - \bar{c}_2^2 \neq 0$. Thus $\bar{c}_1 + \bar{c}_2\tau \in u(\bar{Z}H)$. By (8.5)(ii) we may choose $x_0 + y_0\tau \in R\langle\tau\rangle$ such that $S \cdot N(x_0 + y_0\tau) = S \cdot \beta$. Hence $x_0x_0' - y_0y_0'$ is prime to p, whence $\bar{x}_0 + \bar{y}_0\tau \in u(\bar{Z}H)$. By (8.5)(i), we may choose $u \in u(R\langle\tau\rangle)$ such that $(\bar{x}_0 + \bar{y}_0\tau) \cdot \mu(u) = \bar{c}_1 + \bar{c}_2\tau$. Set $x + y\tau = (x_0 + y_0\tau)u$; since $N(u) \in u(S)$, this gives $S \cdot N(x + y\tau) = S \cdot N(x_0 + y_0\tau) = S \cdot \beta$, and furthermore, $\bar{x} + \bar{y}\tau = \bar{c}_1 + \bar{c}_2\tau$, that is, $x \equiv c_1 \pmod{P}$, $y \equiv c_2 \pmod{P}$, as desired. This completes the proof of (8.1).

9. **The quaternion group of order 8.** Our main result here is as follows:

(9.1) **Theorem.** *Let G be the quaternion group of order 8. Then $C(ZG)$ has order 2, and equals $D(ZG)$.*

We may write

$$G = \langle\sigma, \tau: \sigma^4 = 1, \ \sigma^2 = \tau^2, \ \tau\sigma\tau^{-1} = \sigma^{-1}\rangle.$$

The group algebra $A = QG$ splits into a direct sum of five simple components:

$$A \cong Q^{(4)} \dotplus S, \qquad S = Q \oplus Qi \oplus Qj \oplus Qk. \tag{9.2}$$

The first four components correspond to the four distinct one-dimensional representations of G, namely $\sigma \to \pm 1$, $\tau \to \pm 1$. The fifth component S is the skew-field of rational quaternions, corresponding to the representation $\sigma \to i$, $\tau \to j$.

It is more convenient for us to use the isomorphism

$$f\colon QG \cong QV \dotplus S, \tag{9.3}$$

where $V = \langle s, t\colon s^2 = t^2 = 1,\ st = ts\rangle$ is an abelian (2, 2)-group, and where the isomorphism f is given by $\sigma \to (s, i)$, $\tau \to (t, j)$. We will henceforth identify QG with $QV \dotplus S$, and view ordered pairs $(v, \alpha) \in QV \dotplus S$ as elements of QG.

Now let e_0, e_1, e_2, e_3 be the primitive idempotents of QV, given by $e_i = (1 \pm s)(1 \pm t)/4$. There is an isomorphism $g\colon QV \cong Q^{(4)}$, which we may specify by setting

$$g^{-1}(x_0, x_1, x_2, x_3) = \sum_{i=0}^{3} x_i e_i, \qquad x_i \in Q. \tag{9.4}$$

Our original isomorphism (9.2) may be obtained thus:

$$QG \cong QV \dotplus S \cong Q^{(4)} \dotplus S.$$

In order to determine the image of Λ in $QV \dotplus S$, where $\Lambda = ZG$, we use a pullback diagram. Let $Q[\sigma^2]$ be the group algebra of the cyclic group $[\sigma^2]$ generated by the element σ^2 in the center of G. Set

$$\mathfrak{a} = \Lambda(\sigma^2 + 1), \qquad \mathfrak{b} = \Lambda(\sigma^2 - 1),$$

a pair of two-sided ideals in Λ. Since QG is $Q[\sigma^2]$-free, it follows at once that $\mathfrak{a} \cap \mathfrak{b} = 0$.

The projection $QG \to QV$ induces the mappings

$$\Lambda \to \Lambda/\mathfrak{b} \cong ZV, \quad \sigma \to s, \quad \tau \to t.$$

On the other hand, the projection $QG \to S$ gives

$$\Lambda \to \Lambda/\mathfrak{a} \cong H = Z \oplus Zi \oplus Zj \oplus Zk \subset S,$$

where $\sigma \to i$, $\tau \to j$. Then

$$\Lambda/(\mathfrak{a} + \mathfrak{b}) \cong \overline{Z}V \cong \overline{H},$$

where $\overline{Z} = Z/2Z$, $\overline{H} = H/2H$. Let $\gamma\colon \overline{Z}V \cong \overline{H}$ be the above isomorphism, chosen so that $\gamma(\overline{s}) = \overline{i}$, $\gamma(\overline{t}) = \overline{j}$, where bars denote images in $\overline{Z}V$ or $\overline{H}$, depending on the context.

The pullback diagram (7.7) now becomes

(9.5)
$$\begin{array}{ccccc} \Lambda & \longrightarrow & & & H \\ \downarrow & & & & \downarrow \\ ZV & \longrightarrow & \overline{Z}V & \xrightarrow[\gamma]{} & \overline{H} \end{array}$$

so under the isomorphism f, we may identify Λ with the ring

(9.6) $$\{(v, \alpha): v \in ZV,\ \alpha \in H,\ \gamma(\bar{v}) = \bar{\alpha} \text{ in } \overline{H}\}.$$

Furthermore, in terms of the isomorphism $g: QV \cong Q^{(4)}$, it follows from (9.4) that

(9.7) $$g(ZV) = \{(x_0, x_1, x_2, x_3) \in Z^{(4)}: x_0 \pm x_1 \pm x_2 \pm x_3 \equiv 0 \pmod 4\},$$

where the $\pm$ signs are chosen so that the number of minus signs is even.

Now let $H' = H + Z \cdot \zeta$, $\zeta = (1 + i + j + k)/2$, so H' is a maximal order in S containing H. As is well known, H' is a noncommutative PID and so its class group $C(H')$ is trivial. Set $\Lambda' = g^{-1}(Z^{(4)}) \dotplus H'$, a maximal Z-order in $QV \dotplus S$ containing Λ; we have

$$C(\Lambda') \cong C(Z)^{(4)} \dotplus C(H') = 0.$$

This shows that $D(\Lambda) = C(\Lambda)$, and it remains for us to prove that $D(\Lambda)$ is of order 2. Since S is a totally definite quaternion algebra, A does not satisfy the Eichler condition, and so we must use the formula $D(\Lambda) \cong J(\Lambda')/J(\Lambda)$ in Theorem 3.11 to calculate $D(\Lambda)$.

From (9.2) or (9.3), we obtain

$$F \cong Q^{(4)} \dotplus Q, \qquad C \cong Z^{(4)} \dotplus Z,$$

where F is the center of $QV \dotplus S$, C the maximal Z-order in F. Since $C(\Lambda') = 0$, it follows from (3.11) that $J(\Lambda')$ coincides with the group $I(C, 2)$ of all C-ideals in F prime to the rational prime 2. For brevity, let I denote the group of all Z-ideals in Q prime to 2. Then $J(\Lambda') = I(C, 2) \cong I^{(5)}$.

Now let $(v, \alpha) \in QV \dotplus S$, viewed as element of QG. It is readily seen that the reduced norm $N(v, \alpha) \in F$ is given by

(9.8) $$N(v, \alpha) = (g(v), N\alpha) \in Q^{(4)} \dotplus Q, \qquad v \in QV,\ \alpha \in S,$$

where $N\alpha$ is the reduced norm of the quaternion α. (If $\alpha = x_0 + x_1 i + x_2 j + x_3 k$, then $N\alpha = \Sigma x_i^2$.)

Let $U_0 = \{1, i, j, k\}$, and let $\overline{U}_0$ be the image of U_0 in $u(\overline{H})$.

(9.9) **Lemma.** *There is an epimorphism*

$$\theta: u(Z_2V) \times u(H_2) \longrightarrow I^{(5)},$$

given by

$$\theta(v, \alpha) = Z^{(5)} \cdot N(v, \alpha) = (Z^{(4)} \cdot g(v), Z \cdot N\alpha), \qquad v \in u(Z_2V),\ \alpha \in u(H_2).$$

Furthermore, $\theta(v, \alpha) \in J(\Lambda)$ *whenever* $\gamma(\overline{v}) \in \overline{\alpha}\overline{U}_0$.

Proof. The group $I^{(5)}$ is generated by elements of the form

$$w = (Za_0, Za_1, Za_2, Za_3, Za_4), \qquad a_i \in Z, \ a_i \text{ odd}.$$

Given such an element, we may as well adjust the a's so that

$$a_i \equiv 1 \pmod 4, \qquad 0 \leq i \leq 3, \ a_4 > 0.$$

By (9.7), there exists an element $v \in ZV$ such that $g(v) = (a_0, a_1, a_2, a_3)$. On the other hand, $a_4 = N\alpha$ for some $\alpha \in H$, since every positive integer is a sum of four squares. Therefore we have $\theta(v, \alpha) = w$. Since the image of θ is a group containing the generators $\{w\}$ of $I^{(5)}$, we may conclude that θ is an epimorphism, as desired.

Next, suppose that $\gamma(\overline{v}) = \overline{\alpha}\overline{u}_0$ for some $u_0 \in U_0$. Then $(v, \alpha u_0) \in \Lambda$ by (9.6), and $\theta(v, \alpha u_0) = \theta(v, \alpha)$. Since $\theta(v, \alpha u_0) \in I(\Lambda) \subset J(\Lambda)$, the lemma is established.

Remark. Since θ is epic, and $\Lambda' \supset ZV + H$, we conclude that $I(\Lambda') = I^{(5)}$. But $I(\Lambda') \subset J(\Lambda')$ obviously holds true, and therefore $J(\Lambda') = I^{(5)} \cong I(C, 2)$, as previously stated.

We may next deduce from Lemma 9.9 the important fact that $|D(\Lambda)| \leq 2$. We shall define an epimorphism

$$\nu\colon I^{(5)} \longrightarrow u(\overline{H})/\overline{U}_0$$

by setting

$$\nu(w) = \gamma(\overline{v}) \cdot \overline{\alpha}^{-1} \cdot \overline{U}_0, \quad \text{where } w = \theta(v, \alpha), \ v \in u(Z_2V), \ \alpha \in u(H_2).$$

Let us show that $\nu(w)$ is well defined. The ideal $Z \cdot N(\alpha)$ is determined by w, so α is determined up to a factor from $u(H)$. But $u(H) = \{\pm 1, \pm i, \pm j, \pm k\}$, and $u(H)$ maps onto $\overline{U}_0 \subset u(\overline{H})$, so that $\overline{\alpha} \pmod{\overline{U}_0}$ is uniquely determined by w. Secondly, $g(v) \in Z^{(4)}$ is determined up to a factor from $u(Z^{(4)})$. The eight units $\{(\pm 1, \pm 1, \pm 1, \pm 1)\}$ in $Z^{(4)}$ are the images (under g) of the eight units $\{\pm 1, \pm s, \pm t, \pm st\}$ of ZV. Hence $\gamma(\overline{v})$ is determined up to a factor $\gamma(\overline{v}_0)$, with $v_0 \in u(ZV)$. But $\gamma(\overline{s}) = \overline{i}$, $\gamma(\overline{t}) = \overline{j}$, so $\gamma(\overline{v}_0) \in \overline{U}_0$ for each $v_0 \in u(ZV)$. Therefore $\gamma(\overline{v})$ is also uniquely determined in $u(\overline{H})/\overline{U}_0$, and so ν is well defined. Obviously, ν is an epimorphism of multiplicative groups.

The second statement in Lemma 9.9 tells us that $\ker \nu \subset J(\Lambda)$. Hence we have

$$[u(\overline{H}) : U_0] = [I^{(5)} : \ker \nu] = [J(\Lambda') : \ker \nu] \geq [J(\Lambda') : J(\Lambda)] = |D(\Lambda)|.$$

However, since $\overline{H} \cong \overline{Z}V$, we obtain $|u(\overline{H})| = |u(\overline{Z}V)| = 8$. On the other hand, $|\overline{U}_0| = 4$. Therefore, $|D(\Lambda)| \leq 2$, as claimed.

We are now ready to use the explicit definition:

$$J(\Lambda) = \{C \cdot N^*(x): x = \text{unit in } E(\Lambda_2 \dotplus \Lambda_2)\},$$

and begin by describing $E(\Lambda_2 \dotplus \Lambda_2)$ as a pullback. Indeed, from (9.5) we obtain a pullback diagram

$$\begin{array}{ccccc} E(\Lambda \dotplus \Lambda) & & \longrightarrow & & E(H \dotplus H) \\ \downarrow & & & & \downarrow \\ E(ZV \dotplus ZV) & \longrightarrow & E(\overline{Z}V \dotplus \overline{Z}V) & \longrightarrow & E(\overline{H} \dotplus \overline{H}) \end{array} \tag{9.10}$$

(It is obvious that this is a pullback, once we identify $E(\Lambda \dotplus \Lambda)$ with the matrix ring $(\Lambda)^{2\times 2}$, and so on.) Localizing (9.10) at the rational prime 2, we again obtain a pullback diagram

$$\begin{array}{ccccc} E(\Lambda_2 \dotplus \Lambda_2) & & \longrightarrow & & E(H_2 \dotplus H_2) \\ \downarrow & & & & \downarrow \\ E(Z_2V \dotplus Z_2V) & \longrightarrow & E(\overline{Z}V \dotplus \overline{Z}V) & \longrightarrow & E(\overline{H} \dotplus \overline{H}) \end{array} \tag{9.11}$$

To complete the proof of Theorem 9.1, it suffices to show that the element $w = (Z, Z, Z, Z, 3Z) \in J(\Lambda')$ does not lie in $J(\Lambda)$. Suppose to the contrary that $w \in J(\Lambda)$, so $w = Z^{(5)} \cdot N(x)$ for some unit $x \in E(\Lambda_2 \dotplus \Lambda_2)$. By (9.11), x corresponds to a pair of 2×2 matrices X, Y such that

$$\begin{cases} X = \text{unit in } (Z_2V)^{2\times 2}, \quad Y = \text{unit in } (H_2)^{2\times 2}, \\ \gamma(\overline{X}) = \overline{Y} \quad \text{as matrices over } \overline{H}, \\ Z^{(4)} \cdot N(X) = (Z, Z, Z, Z), \quad Z \cdot N(Y) = 3Z. \end{cases} \tag{9.12}$$

Since Z_2V is commutative, the reduced norm $N(X)$ is precisely $g(\det X)$. But $N(X)$ is a unit in $Z^{(4)}$, so $g(\det X) \in u(Z^{(4)})$; therefore (as shown in the proof of (9.9)), $\det X \in u(ZV)$. Hence $\gamma(\det \overline{X}) \in \gamma\{\overline{u(ZV)}\} = \overline{U}_0$. Therefore, we have

$$\det \overline{Y} \in \overline{U}_0. \tag{9.13}$$

Let us write $Y = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in (H_2)^{2\times 2}$. Since Y is invertible over H_2, it is also invertible over H'_2; but H'_2 is a local ring, so either α or γ must be a unit in H'_2. It follows from Lemma 3.3 that either α or γ is a unit in H_2. Suppose (without loss of generality) that $\alpha \in u(H_2)$. Then

$$N(Y) = N\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = N\begin{pmatrix} \alpha & \beta \\ 0 & \delta - \gamma\alpha^{-1}\beta \end{pmatrix} = N(\alpha\delta - \alpha\gamma\alpha^{-1}\beta).$$

The image of $\alpha\delta - \alpha\gamma\alpha^{-1}\beta$ in $\overline{H}$ is just $\det \overline{Y}$ (since $\overline{H}$ is commutative), and thus this image lies in $\overline{U}_0$ by (9.13). Therefore,

$$\alpha\delta - \alpha\gamma\alpha^{-1}\beta = u_0(1 + 2t) \quad \text{for some } t \in H_2.$$

But then

$$N(\alpha\delta - \alpha\gamma\alpha^{-1}\beta) = N(u_0) \cdot N(1 + 2t) = 1 + 2(t + t') + 4tt',$$

where t' is the conjugate of t in H. This shows that $N(Y)$ is a positive rational number, congruent to 1 (mod 4). The equation $Z \cdot N(Y) = 3Z$ is then impossible. This completes the proof that $J(\Lambda') \neq J(\Lambda)$, and that $D(\Lambda)$ has order 2.

REFERENCES

1. H. Bass, *Algebraic K-theory*, Math. Lecture Note Series, Benjamin, New York, 1968. MR 40 #2736.

2. N. Bourbaki, *Éléments de mathématique*. XXIII. Part I. *Les structures fondamentales de l'analyse*. Livre II: *Algèbre*. Chap. 8, Actualités Sci. Indust., no. 1261, Hermann, Paris, 1958. MR 20 #4576.

3. C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Pure and Appl. Math., vol. XI, Interscience, New York, 1962; 2nd ed., 1966. MR 26 #2519.

4. M. Deuring, *Algebren*, Springer-Verlag, Berlin, 1935; Zweite korrigierte Auflage, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 41, 1968. MR 37 #4106.

5. M. Eichler, *Allgemeine Kongruenzklasseneinteilungen der Ideale einfachen Algebren über algebraischen Zahlkörpern und ihre L-Reihen*, J. Reine Angew. Math. 179 (1938), 227–251.

6. W. Feit, *Characters of finite groups*, Math. Lecture Note Series, Benjamin, New York, 1967. MR 36 #2715.

7. A. Fröhlich, *Ideals in an extension field as modules over the algebraic integers in a finite number field*, Math. Z. 74 (1960), 29–38. MR 22 #4708.

8. ———, *On the classgroup of integral group rings of finite Abelian groups*, Mathematika 16 (1969), 143–152. MR 41 #5512.

9. H. Jacobinski, *Genera and decompositions of lattices over orders*, Acta. Math. 121 (1968), 1–29. MR 40 #4294.

10. M. P. Lee, *Integral representations of dihedral groups of order 2p*, Trans. Amer. Math. Soc. 110 (1964), 213–231. MR 28 #139.

11. I. Reiner, *A survey of integral representation theory*, Bull. Amer. Math. Soc. 76 (1970), 159–227. MR 40 #7302.

12. K. W. Roggenkamp and V. H. Dyson, *Lattices over orders*. I, II, Lecture Notes in Math., nos. 115, 142, Springer-Verlag, Berlin and New York, 1970.

13. R. G. Swan, *Induced representations and projective modules*, Ann. of Math. (2) 71 (1960), 552–578. MR 25 #2131.

14. ———, *The Grothendieck ring of a finite group*, Topology 2 (1963), 85–110. MR 27 #3683.

15. R. G. Swan and E. G. Evans, *K-theory of finite groups and orders*, Lecture Notes in Math., no. 149, Springer-Verlag, Berlin and New York, 1970.

16. S. Ullom, *A note on the classgroup of integral group rings of some cyclic groups*, Mathematika 17 (1970), 79–81. MR 42 #4650.

17. A. Fröhlich, *The Picard group* (to appear).

18. I. Reiner and S. Ullom, *A Mayer-Vietoris sequence for class groups*, J. Algebra (to appear).

19. A. Fröhlich, I. Reiner and S. Ullom, *Picard groups and class groups* (to appear).

20. J. Martinet, *Modules sur l'algèbre du groupe quaternionien*, Ann. Sci. École Norm. Sup. 4 (1971), 399–408.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN, URBANA, ILLINOIS 61801