PACIFIC JOURNAL OF MATHEMATICS
Vol. 78, No. 2, 1978

INVARIANTS OF INTEGRAL REPRESENTATIONS

IRVING REINER

Let ZG be the integral group ring of a finite group G. A ZG-lattice is a left G-module with a finite free Z-basis. In order to classify ZG-lattices, one seeks a full set of isomorphism invariants of a ZG-lattice M. Such invariants are obtained here for the special case where G is cyclic of order p^2, where p is prime. This yields a complete classification of the integral representations of G. There are also several results on extensions of lattices, which are of independent interest and apply to more general situations.

Two ZG-lattices M and N are placed in the same genus if their p-adic completions M_p and N_p are Z_pG-isomorphic. One first gives a full set of genus invariants of a ZG-lattice. There is then the remaining problem, considerably more difficult in this case, of finding additional invariants which distinguish the isomorphism classes within a genus. Generally speaking, such additional invariants are some sort of ideal classes. In the present case, these invariants will be a pair of ideal classes in rings of cyclotomic integers, together with two new types of invariants: an element in some factor group of the group of units of some finite ring, and a quadratic residue character (mod p).

For arbitrary finite groups G, the classification of ZG-lattices has been carried out in relatively few cases. The problem has been solved for G of prime order p or dihedral of order $2p$. It was also solved for the case of an elementary abelian (2, 2)-group, and for the alternating group A_4 (see [10a] for references).

The main results of the present article deal with the case where G is cyclic of order p^2, where p is prime. In Theorem 7.3 below, there is a full list of all indecomposable ZG-lattices, up to isomorphism. Theorem 7.8 then gives a full set of invariants for the isomorphism class of a finite direct sum of indecomposable lattices.

Sections 1 and 2 contain preliminary remarks about extensions of lattices over orders. Sections 3 and 5 consider the following problem: given two lattices M and N over some order, find a full set of isomorphism invariants for a direct sum of extensions of lattices in the genus of N by lattices in the genus of M. The results of these sections are applied in §§ 4 and 6 to the special case of ZG-lattices, where G is any cyclic p-group, p prime. Finally, § 7 is devoted to detailed calculations for the case where G is cyclic of order p^2.

Throughout the article, R will denote a Dedekind ring whose

quotient field K is an algebraic number field, and Λ will be an R-order in a finite dimensional semisimple K-algebra A. For P a maximal ideal of R, the subscript P in R_P, K_P, Λ_P, etc., denotes P-adic completion. Let $S(\Lambda)$ be a finite nonempty set of P's, such that Λ_P is a maximal R_P-order in A_P for each $P \notin S(\Lambda)$; such a set can always be chosen. (In the special case where $\Lambda = RG$, $S(\Lambda)$ need only be picked so as to include all prime ideal divisors of the order of G.) A *Λ-lattice* is a left Λ-module, finitely generated and torsionfree (hence projective) over R. Two Λ-lattices M, N are in the same *genus* if $M_P \cong N_P$ as Λ_P-modules for all P (or equivalently, for all $P \in S(\Lambda)$). For M a Λ-lattice, $\mathrm{End}_\Lambda(M)$ denotes its endomorphism ring, and $M^{(n)}$ the external direct sum of n copies of M. Let $\coprod M_i$ denote the external direct sum of a collection of modules $\{M_i\}$.

1. **Generalities about extensions of modules.** We briefly review some known facts about extensions (see, for example, [3] and [16]). Let Λ be an arbitrary ring, and let M, N be left Λ-modules. We shall write $\mathrm{Ext}(N, M)$ instead of $\mathrm{Ext}^1_\Lambda(N, M)$ for brevity, when there is no danger of confusion. Let

$$\Gamma = \mathrm{End}_\Lambda(M), \ \Delta = \mathrm{End}_\Lambda(N) ,$$

and view $\mathrm{Ext}(N, M)$ as a (Γ, Δ)-bimodule. For later use, we need to know explicitly how Γ and Δ act on $\mathrm{Ext}(N, M)$.

Consider a Λ-exact sequence

$$\xi\colon 0 \longrightarrow M \xrightarrow{\mu} X \xrightarrow{\nu} N \longrightarrow 0 , \qquad \xi \in \mathrm{Ext}(N, M) .$$

For each $\gamma \in \Gamma$, we may form the pushout ${}_\gamma X$ of the pair of maps $\gamma\colon M \to M$, $\mu\colon M \to X$, so

$${}_\gamma X = (X \oplus M)/\{(\mu m, -\gamma m)\colon m \in M\} .$$

Then we obtain a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} \xi\colon & 0 & \longrightarrow & M & \xrightarrow{\mu} & X & \xrightarrow{\nu} & N & \longrightarrow 0 \\ & & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 1} & \\ \gamma\xi\colon & 0 & \longrightarrow & M & \longrightarrow & {}_\gamma X & \longrightarrow & N & \longrightarrow 0 , \end{array} \tag{1.1}$$

and the bottom row corresponds to the extension class $\gamma\xi \in \mathrm{Ext}(N, M)$. Applying the Snake Lemma to the above (see [11, Exercise 2.8]), we obtain

$$\ker \gamma \cong \ker \varphi , \quad \mathrm{cok}\, \gamma \cong \mathrm{cok}\, \varphi . \tag{1.2}$$

Analogously, given any $\delta \in \Delta$, let

$$X_\delta = \{(x, n) \in X \oplus N : \nu x = \delta n\},$$

the pullback of the pair of maps $\nu: X \to N$, $\delta: N \to N$. Then we obtain a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} \xi: & 0 & \longrightarrow & M & \xrightarrow{\mu} & X & \xrightarrow{\nu} & N & \longrightarrow 0 \\ & & & \uparrow 1 & & \uparrow \psi & & \uparrow \delta & \\ \xi\delta: & 0 & \longrightarrow & M & \longrightarrow & X_\delta & \longrightarrow & N & \longrightarrow 0, \end{array}$$

and the bottom now gives the extension class $\xi\delta$. By the Snake Lemma,

$$\ker \psi \cong \ker \delta, \quad \operatorname{cok} \psi \cong \operatorname{cok} \delta.$$

Formules such as $(\gamma\gamma')\xi = \gamma(\gamma'\xi)$ are easily verified, and yield Λ-isomorphisms

$${}_\gamma X \cong X \text{ if } \gamma \in \operatorname{Aut}(M), \quad X_\delta \cong X \text{ if } \delta \in \operatorname{Aut}(N),$$

where Aut means $\operatorname{Aut}_\Lambda$.

For later use, an alternative description of the action Δ on $\operatorname{Ext}(N, M)$ is important. Consider a Λ-exact sequence

$$0 \longrightarrow L \xrightarrow{i} P \longrightarrow N \longrightarrow 0$$

in which P is Λ-projective. Applying $\operatorname{Hom}_\Lambda(\cdot, M)$, we obtain an exact sequence of additive groups

$$0 \longrightarrow \operatorname{Hom}(N, M) \longrightarrow \operatorname{Hom}(P, M) \xrightarrow{i^*} \operatorname{Hom}(L, M) \longrightarrow \operatorname{Ext}^1_\Lambda(N, M) \longrightarrow 0,$$

and thus

$$\operatorname{Ext}(N, M) \cong \operatorname{Hom}(L, M)/\operatorname{im} i^*.$$

Each $\xi \in \operatorname{Ext}(N, M)$ is thus of the form $\bar{f}$, where $f \in \operatorname{Hom}(L, M)$ and where $\bar{f}$ denotes its image in $\operatorname{cok} i^*$. Now let $\delta \in \Delta$; we can lift δ to a map $\delta_1 \in \operatorname{End}(P)$, and δ_1 then induces a map $\delta_2 \in \operatorname{End}(L)$ for which the following diagram commutes:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \longrightarrow & P & \longrightarrow & N & \longrightarrow 0 \\ & & \downarrow \delta_2 & & \downarrow \delta_1 & & \downarrow \delta & \\ 0 & \longrightarrow & L & \longrightarrow & P & \longrightarrow & N & \longrightarrow 0. \end{array}$$

Of course End L acts from the right on Hom (L, M), and for $\xi = \bar{f}$ as above, we have $\xi\delta = \overline{f\delta_2}$ in Ext (N, M).

PROPOSITION 1.3. *For $i = 1, 2$, let M_i and N_i be Λ-modules,*

and let $\xi_i \in \mathrm{Ext}^1_\Lambda(N_i, M_i)$ *determine a* Λ*-module* X_i. *Assume that* $\mathrm{Hom}_\Lambda(M_1, N_2) = 0$. *Then* $X_1 \cong X_2$ *if and only if*

(1.4) $\gamma\xi_1 = \xi_2\delta$ *for some* Λ*-isomorphisms* $\gamma: M_1 \cong M_2$, $\delta: N_1 \cong N_2$.

Proof. Let $\varphi \in \mathrm{Hom}\,(X_1, X_2)$, and consider the diagram

$$\begin{array}{ccccccccc} \xi_1\colon 0 & \longrightarrow & M_1 & \xrightarrow{\mu_1} & X_1 & \xrightarrow{\nu_1} & N_1 & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle\varphi} & & & & \\ \xi_2\colon 0 & \longrightarrow & M_2 & \xrightarrow{\mu_2} & X_2 & \xrightarrow{\nu_2} & N_2 & \longrightarrow & 0\,. \end{array}$$

Since $\mathrm{Hom}\,(M_1, N_2) = 0$ by hypothesis, we have $\nu_2\varphi\mu_1 = 0$. Therefore $\varphi\mu_1(M_1) \subset \mathrm{im}\ \mu_2$, so φ induces maps γ, δ making the following diagram commute:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \longrightarrow & X_1 & \longrightarrow & N_1 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\gamma} & & \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle\delta} & & \\ 0 & \longrightarrow & M_2 & \longrightarrow & X_2 & \longrightarrow & N_2 & \longrightarrow & 0\,. \end{array}$$

But this means that $\gamma\xi_1 = \xi_2\delta$ in $\mathrm{Ext}\,(N_1, M_2)$. Furthermore, by the Snake Lemma, φ is an isomorphism if and only if both γ and δ are isomorphisms. Hence (1.4) holds if $X_1 \cong X_2$.

Conversely, assume that (1.4) is true; since $\gamma\xi_1 = \xi_2\delta$, there exists a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \longrightarrow & X_1 & \longrightarrow & N_1 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\gamma} & & \downarrow{\scriptstyle\psi_1} & & \downarrow{\scriptstyle 1} & & \\ 0 & \longrightarrow & M_2 & \longrightarrow & Y_1 & \longrightarrow & N_1 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle 1} & & \downarrow{\scriptstyle\psi_2} & & \downarrow{\scriptstyle 1} & & \\ 0 & \longrightarrow & M_2 & \longrightarrow & Y_2 & \longrightarrow & N_1 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle 1} & & \downarrow{\scriptstyle\psi_3} & & \downarrow{\scriptstyle\delta} & & \\ 0 & \longrightarrow & M_2 & \longrightarrow & X_2 & \longrightarrow & N_2 & \longrightarrow & 0\,. \end{array}$$

But γ and δ are isomorphisms, whence so is each ψ_i. Thus $X_1 \cong X_2$, as desired. (This part of the argument does not require the hypothesis that $\mathrm{Hom}\,(M_1, N_2) = 0$.)

COROLLARY 1.5. *Let* M, N *be* Λ*-modules such that* $\mathrm{Hom}\,(M, N) = 0$. *Let* $\xi_i \in \mathrm{Ext}\,(N, M)$ *determine a* Λ*-module* X_i, $i = 1, 2$. *Then* $X_1 \cong X_2$ *if and only if*

(1.6) $\gamma\xi_1 = \xi_2\delta$ *for some* $\gamma \in \mathrm{Aut}\,(M)$, $\delta \in \mathrm{Aut}\,(N)$.

We shall call ξ_1 and ξ_2 *strongly equivalent* (notation: $\xi_1 \approx \xi_2$) whenever condition (1.6) is satisfied.

2. **Extensions of lattices.** Keeping the notation used in the introduction, let Λ be an R-order in the semisimple K-algebra A. Choose a nonempty set $S(\Lambda)$ of maximal ideals P of R, such that for each $P \notin S(\Lambda)$, the P-adic completion Λ_P is a maximal R_P-order in A_P. Now let M and N be Λ-lattices, so M_P and N_P are Λ_P-lattices. For $P \notin S(\Lambda)$, the maximal order Λ_P is hereditary, and so the Λ_P-lattice N_P is Λ_P-projective (see [11, (21.5)]); thus $\mathrm{Ext}_{\Lambda_P}(N_P, M_P) = 0$ for each $P \notin S(\Lambda)$.

Now consider $\mathrm{Ext}^1_\Lambda(N, M)$, which we will denote for brevity by $\mathrm{Ext}(N, M)$ when there is no danger of confusion. Then $\mathrm{Ext}(N, M)$ is a finitely generated torsion R-module, with no torsion at the maximal ideals $P \notin S(\Lambda)$. As in [4, (75.22)], we have

$$\mathrm{Ext}^1_\Lambda(N, M) \cong \prod_{P \in S(\Lambda)} \mathrm{Ext}^1_{\Lambda_P}(N_P, M_P)\ . \tag{2.1}$$

The following analogue of Schanuel's Lemma will be useful:

LEMMA 2.2. *Let X, X', Y, Y' be Λ-lattices, and let T be an R-torsion Λ-module such that $T_P = 0$ for each $P \in S(\Lambda)$. Suppose that there exist a pair of Λ-exact sequences*

$$0 \longrightarrow X' \longrightarrow X \xrightarrow{f} T \longrightarrow 0\ , \quad 0 \longrightarrow Y' \longrightarrow Y \xrightarrow{g} T \longrightarrow 0\ .$$

Then there is a Λ-isomorphism

$$X \oplus Y' \cong X' \oplus Y\ .$$

Proof. Let W be the pullback of the pair of maps f, g. Then we obtain a commutative diagram of Λ-modules, with exact rows and columns:

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & X' & \xrightarrow{1} & X' & & \\
 & & & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & Y' & \longrightarrow & W & \longrightarrow & X & \longrightarrow & 0 \\
 & & 1\downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & Y' & \longrightarrow & Y & \longrightarrow & T & \longrightarrow & 0\ . \\
 & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0 & & & &
\end{array}$$

At each $P \in S(\Lambda)$, we have $T_P = 0$ by hypothesis. However, the process of forming P-adic completions preserves commutativity and

exactness, since R_P is R-flat. Hence both of the Λ-exact sequences

$$(2.3)\quad 0 \longrightarrow X' \longrightarrow W \longrightarrow Y \longrightarrow 0,\ 0 \longrightarrow Y' \longrightarrow W \longrightarrow X \longrightarrow 0\ ,$$

are split at each $P \in S(\Lambda)$. On the other hand, for $P \notin S(\Lambda)$ we know that Λ_P is a maximal order, so the Λ_P-lattices X_P, Y_P are Λ_P-projective. Hence the sequences (2.3) are also split at each $P \notin S(\Lambda)$. Therefore they split at every P, and hence split globally (see [11, (3.20)]). This gives

$$W \cong X' \oplus Y\ ,\quad W \cong X \oplus Y'\ ,$$

and proves the result. This result is due to Roiter [15].

We shall apply this lemma to the following situation. Each $\xi \in \mathrm{Ext}\,(N, M)$ determines a Λ-exact sequence

$$\xi\colon\quad 0 \longrightarrow M \longrightarrow X \longrightarrow N \longrightarrow 0\ ,$$

with X unique up to isomorphism. The sequence is R-split since N is R-projective, and so $X \cong M \oplus N$ as R-modules. Thus X is itself a Λ-lattice, called an *extension* of N by M. There is an embedding $M \to K \otimes_R M$, given by $m \to 1 \otimes m$ for $m \in M$; we shall always identify M with its image $1 \otimes M$, so that $K \otimes_R M$ may be written as KM. We shall set

$$\Gamma = \mathrm{End}_\Lambda(M)\ ,\quad \Delta = \mathrm{End}_\Lambda(N)\ .$$

Then $K\Gamma = \mathrm{End}_A(KM)$, and Γ is an R-order in the semisimple K-algebra $K\Gamma$. Likewise $K\Delta = \mathrm{End}_A(KN)$, and Δ is an R-order in the semisimple K-algebra $K\Delta$. For each $\gamma \in \Gamma$, $\delta \in \Delta$, we may form the Λ-lattices ${}_\gamma X$ and X_δ as in § 1. We now prove

(2.4) Exchange Formula. *Let X and Y be a pair of extensions of N by M, and let $\gamma \in \mathrm{End}\,(M)$ satisfy the condition*

$$(2.5)\qquad \gamma_P \in \mathrm{Aut}\,(M_P)\ \textit{for each}\ P \in S(\Lambda)\ .$$

Then there is a Λ-isomorphism

$$(2.6)\qquad X \oplus {}_\gamma Y \cong {}_\gamma X \oplus Y\ .$$

Proof. For each $P \in S(\Lambda)$, we have

$$(\ker \gamma)_P \cong \ker(\gamma_P) = 0\ ,\quad (\mathrm{cok}\,\gamma)_P \cong \mathrm{cok}\,(\gamma_P) = 0\ .$$

Now $\ker \gamma$ is an R-submodule of the Λ-lattice M, and thus $\ker \gamma$ is itself an R-lattice. Since $(\ker \gamma)_P = 0$ for at least one P (namely, for any $P \in S(\Lambda)$), it follows that $\ker \gamma = 0$.

From (1.1) and (1.2) we obtain Λ-exact sequences

$$0 \longrightarrow X \longrightarrow {}_\gamma X \longrightarrow \operatorname{cok}\gamma \longrightarrow 0\ ,\quad 0 \longrightarrow Y \longrightarrow {}_\gamma Y \longrightarrow \operatorname{cok}\gamma \longrightarrow 0\ ,$$

where $\operatorname{cok}\gamma = M/\gamma(M)$. But $(\operatorname{cok}\gamma)_P = 0$ for each $P \in S(\Lambda)$, so we may apply Lemma 2.2 to the above sequences. This gives the isomorphism in (2.6), and completes the proof.

In the same manner, we obtain

(2.7) ABSORPTION FORMULA. *Let X be an extension of N by M, and let $\gamma \in \operatorname{End}(M)$ satisfy condition* (2.5). *Then*

$$X \oplus M \cong {}_\gamma X \oplus M\ .$$

Proof. Apply Lemma 2.2 to the pair of exact sequences

$$0 \longrightarrow X \longrightarrow {}_\gamma X \longrightarrow \operatorname{cok}\gamma \longrightarrow 0\ ,\quad 0 \longrightarrow M \xrightarrow{\gamma} M \longrightarrow \operatorname{cok}\gamma \longrightarrow 0\ .$$

REMARK 2.8. There are obvious analogues of (2.6) and (2.7), in which we start with an element $\delta \in \operatorname{End}(N)$ such that $\delta_P \in \operatorname{Aut}(N_P)$ for each $P \in S(\Lambda)$.

Now let M, N be Λ-lattices, and let $M' \vee M$, $N' \vee N$. It is clear from (2.1) that $\operatorname{Ext}(N', M') \cong \operatorname{Ext}(N, M)$. In fact, by Roiter's Lemma (see [11, (27.1)]), we can find Λ-exact sequences

$$(2.9)\quad 0 \longrightarrow M \xrightarrow{\varphi} M' \longrightarrow T \longrightarrow 0\ ,\quad 0 \longrightarrow N' \xrightarrow{\psi'} N \longrightarrow U \longrightarrow 0\ ,$$

in which $T_P = 0$ and $U_P = 0$ for all $P \in S(\Lambda)$. The pair (ϕ, ψ') induces an isomorphism

$$(2.10)\qquad t\colon \operatorname{Ext}(N, M) \cong \operatorname{Ext}(N', M')\ ,$$

(hereafter called a *standard* isomorphism), which may be described explicitly as follows: if $\xi \in \operatorname{Ext}(N, M)$, then $t(\xi) = \phi\xi\psi'$ (in the notation of § 1). Thus, if ξ determines the Λ-lattice X (up to isomorphism), then $t(\xi)$ determines the Λ-lattice ${}_\phi(X)_{\psi'}$, which lies in the same genus as X.

LEMMA 2.11. *The inverse of a standard isomorphism is also a standard isomorphism.*

Proof. We may choose a nonzero proper ideal $\mathfrak{a}$ of R, all of whose prime ideal factors lie in $S(\Lambda)$, such that $\mathfrak{a} \cdot \operatorname{Ext}(N, M) = 0$. If $\mu \in \operatorname{End}(M)$ is such that $\mu - 1 \in \mathfrak{a} \cdot \operatorname{End}(M)$, it then follows that μ acts as the identity map on $\operatorname{Ext}(N, M)$.

Let t be a standard isomorphism as in (2.10), induced from the pair of maps (ϕ, ψ') as in (2.9). Since ϕ_P is an isomorphism for each $P \in S(\Lambda)$, we can find a map $\phi' \in \operatorname{Hom}(M', M)$ such that ϕ'_P approxi-

mates ϕ_P^{-1} at each $P \in S(\Lambda)$; indeed, we can choose ϕ' so that

$$\phi' \cdot \phi \equiv 1 \bmod \mathfrak{a} \cdot \mathrm{End}(M) .$$

Then ϕ' is an inclusion, and $\phi'\phi$ acts as 1 on $\mathrm{Ext}(N, M)$. Likewise, we may choose an inclusion $\psi: N \to N'$ such that $\psi'\psi$ acts as 1 on $\mathrm{Ext}(N, M)$. The pair (ϕ', ψ) then induces a standard isomorphism $t': \mathrm{Ext}(N', M') \cong \mathrm{Ext}(N, M)$ such that $t't = 1$. This completes the proof.

We wish to determine all isomorphism classes of Λ-lattices X which are extensions of a given lattice N by another given lattice M. Let us show that under suitable hypotheses on M and N, this determination depends only upon the genera of M and N. A Λ-lattice M is called an *Eichler lattice* if $\mathrm{End}_A(KM)$ satisfies the Eichler condition over R (see [11, (38.1)]). This condition depends only on the A-module KM and on the underlying ring of integers R. (In the special case where $R =$ alg. int. $\{K\}$, M is an Eichler lattice if and only if no simple component of $\mathrm{End}_A(KM)$ is a totally definite quaternion algebra.) Of course, M is an Eichler lattice wherever $\mathrm{End}_A(KM)$ is a direct sum of matrix algebras over fields.

We now establish

THEOREM 2.12. *Let M and N be Λ-lattices such that $M \oplus N$ is an Eichler lattice, and let $M' \vee M$, $N' \vee N$. Let*

$$t: \mathrm{Ext}(N, M) \cong \mathrm{Ext}(N', M')$$

be a standard isomorphism as in (2.10). *Then t induces a one-to-one correspondence between the set of isomorphism classes of extensions of N by M, and that of extensions of N' by M'.*

Proof. Each Λ-lattice X, which is an extension of N by M, determines an extension class $\xi \in \mathrm{Ext}(N, M)$. Two X's which yield the same ξ must be isomorphic to one another, but the converse of this statement need not be true. (Herein lies the difficulty in the proof.) In any case, given the extension X, let ξ be its extension class; set $\xi' = t(\xi) \in \mathrm{Ext}(N', M')$, and let ξ' determine the Λ-lattice X' (up to isomorphism). Then X' is an extension of N' by M', and $X' \vee X$. Now let Y be another extension of N by M, and let Y' be the corresponding extension of N' by M'. We must prove that $X \cong Y$ if and only if $X' \cong Y'$. (Note that every extension of N' by M' comes from some X, by virtue of Lemma 2.11.)

It suffices to prove the implication in one direction, since by (2.11) the inverse of a standard isomorphism is again standard. Furthermore, every standard isomorphism can be expressed as a

product of two standard isomorphisms, each of which involves a change of only one of the "variables" M and N. It therefore suffices to prove the desired result for the case in which there is a change in only one variable, say M. Thus, let us start with an inclusion $\phi: M \longrightarrow M'$ as in (2.9), such that $(\operatorname{cok}\phi)_P = 0$ for all $P \in S(\Lambda)$. Given an exact sequence

$$0 \longrightarrow M \xrightarrow{\mu} X \longrightarrow N \longrightarrow 0\,,$$

define a Λ-module X' as the pushout of the pair of maps (μ, ϕ). We then obtain a commutative diagram of Λ-modules, with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{\mu} & X & \longrightarrow & N & \longrightarrow & 0 \\ & & \phi\downarrow & & \downarrow & & 1\downarrow & & \\ 0 & \longrightarrow & M' & \longrightarrow & X' & \longrightarrow & N & \longrightarrow & 0\,. \end{array} \tag{2.13}$$

Then X' is precisely the Λ-lattice determined by X as above, by means of the standard isomorphism $t: \operatorname{Ext}(N, M) \cong \operatorname{Ext}(N, M')$ induced by ϕ. Let Y be another extension of N by M, and let Y' denote the extension of N by M' corresponding to Y. It then suffices for us to prove that $X' \cong Y'$ whenever $X \cong Y$.

Applying the Snake Lemma to (2.13), we obtain an exact sequence of Λ-modules

$$0 \longrightarrow X \longrightarrow X' \longrightarrow \operatorname{cok}\phi \longrightarrow 0\,,$$

with $(\operatorname{cok}\phi)_P = 0$ for all $P \in S(\Lambda)$. Likewise, there is an exact sequence

$$0 \longrightarrow Y \longrightarrow Y' \longrightarrow \operatorname{cok}\phi \longrightarrow 0\,.$$

Therefore we obtain

$$X \oplus Y' \cong X' \oplus Y \tag{2.14}$$

by Lemma 2.2.

Suppose now that $X \cong Y$; since $X' \vee X$ and $Y' \vee Y$, the lattices X, X', Y, Y' are in the same genus, and we may rewrite (2.14) as

$$X \oplus Y' \cong X \oplus X'\,. \tag{2.15}$$

Clearly $KX \cong K(M \oplus N)$, and thus X is an Eichler lattice (since $M \oplus N$ is an Eichler lattice by hypothesis). By Jacobinski's Cancellation Theorem [8], we may then conclude from (2.15) that $X' \cong Y'$. This completes the proof of the theorem.

REMARKS. (i) It seems likely that the conclusion of the theorem

holds true whether or not $M \oplus N$ is an Eichler lattice.

(ii) Suppose that $\mathrm{Hom}(M, N) = 0$. By (1.5), there is a one-to-one correspondence between the set of all isomorphism classes of Λ-lattices X which are extensions of N by M, and the set of orbits of the bimodule $\mathrm{Ext}(N, M)$ under the left action of $\mathrm{Aut}(N)$ and the right action of $\mathrm{Aut}(M)$. By definition, two elements of $\mathrm{Ext}(N, M)$ are *strongly equivalent* if they lie in the same orbit. The preceding theorem then shows, in this case where $\mathrm{Hom}(M, N) = 0$ and where $M \oplus N$ is an Eichler lattice, that the orbits depend only upon the genera of M and N. Indeed, we have shown above that under these hypotheses, standard isomorphisms preserve strong equivalence.

(iii) In the special cases of interest in §§ 4-7, one can prove (2.12) directly without using Jacobinski's Cancellation Theorem (see [13], for example).

The author wishes to thank Professor Jacobinski for some helpful conversations, which led to a considerable simplification of the original proof of Theorem 2.12.

3. Direct sums of extensions. As in § 2, let Λ be a R-order in a semisimple K-algebra A, where K is an algebraic number field. Given Λ-lattices M, N with $\mathrm{Hom}_\Lambda(M, N) = 0$, we wish to classify up to isomorphism all extensions of a direct sum of copies of N by a direct sum of copies of M. Let $\xi_1, \xi_2 \in \mathrm{Ext}^1(N^{(s)}, M^{(r)})$, and let ξ_i determine the extension Y_i of $N^{(s)}$ by $M^{(r)}$. Since $\mathrm{Hom}_\Lambda(M^{(r)}, N^{(s)}) = 0$, we may apply (1.5) to obtain

PROPOSITION 3.1. *The Λ-lattices Y_1, Y_2 are isomorphic if and only if*

$$\alpha\xi_1 = \xi_2\beta \text{ for some } \alpha \in \mathrm{Aut}\, M^{(r)},\ \beta \in \mathrm{Aut}\, N^{(s)}\ . \tag{3.2}$$

As before, call ξ_1 *strongly equivalent* to ξ_2 (notation: $\xi_1 \approx \xi_2$) whenever condition (3.2) is satisfied. We may rewrite this condition in a more convenient form, as follows: there is an isomorphism

$$\mathrm{Ext}(N^{(s)}, M^{(r)}) \cong (\mathrm{Ext}(N, M))^{r \times s}\ ,$$

where the right hand expression denotes the set of all $r \times s$ matrices with entries in $\mathrm{Ext}(N, M)$. If we put

$$\Gamma = \mathrm{End}_\Lambda(M)\ ,\quad \Delta = \mathrm{End}_\Lambda(N)\ ,$$

acting from the left on M and N, respectively, then we may identify $\mathrm{Aut}\, M^{(r)}$ with $GL(r, \Gamma)$, and $\mathrm{Aut}\, N^{(s)}$ with $GL(s, \Delta)$. Then $(\mathrm{Ext}(N, M))^{r \times s}$ is a left $GL(r, \Gamma)$-, right $GL(s, \Delta)$-bimodule, and $\xi_1 \approx \xi_2$ if and only if $\alpha\xi_1 = \xi_2\beta$ for some $\alpha \in GL(r, \Gamma)$, $\beta \in GL(s, \Delta)$.

As a matter of fact, we may choose a nonzero ideal $\mathfrak{a}$ of R, involving only prime ideals P from the set $S(\Lambda)$, such that $\mathfrak{a}\cdot\mathrm{Ext}(N, M) = 0$. Then Γ acts on $\mathrm{Ext}(N, M)$ via the map $\Gamma \to \bar{\Gamma}$, where $\bar{\Gamma} = \Gamma/\mathfrak{a}\Gamma$. Hence $GL(r, \Gamma)$ acts on $(\mathrm{Ext}(N, M))^{r\times s}$ via the map $GL(r, \Gamma) \to GL(r, \bar{\Gamma})$. A corresponding result holds for Δ.

We are thus faced with the question of determining the orbits of $(\mathrm{Ext}(N, M))^{r\times s}$ under the actions of $GL(r, \Gamma)$ and $GL(s, \Delta)$. We cannot hope to specify these orbits in general, but we shall see that they can be determined in some interesting special cases which arise in practice. Before proceeding with this determination, however, it is desirable to adopt a slightly more general point of view.

Let M and N be as above, and let $M_i \vee M$, $N_j \vee N$ for $1 \leqq i \leqq r$, $1 \leqq j \leqq s$. By hypothesis $\mathrm{Hom}(M, N) = 0$, so also $\mathrm{Hom}(M_i, N_j) = 0$ for all i, j. Now let $\xi \in \mathrm{Ext}(\coprod N_j, \coprod M_i)$ determine an extension X. It follows from §1 that a full set of isomorphism invariants of X are the isomorphism classes of $\coprod M_i$ and $\coprod N_j$, and the strong equivalence class of ξ. Further, since $\coprod M_i \vee M^{(r)}$ and $\coprod N_j \vee N^{(s)}$, there is a standard isomorphism

$$t\colon \mathrm{Ext}(\coprod N_j, \coprod M_i) \cong \mathrm{Ext}(N^{(s)}, M^{(r)})$$

as in (2.10). If we assume that both $M^{(r)}$ and $N^{(s)}$ are Eichler lattices, then by (2.11) t gives a one-to-one correspondence between strong equivalence classes in these two Ext's. We remark in passing that $M^{(r)}$ is necessarily an Eichler lattice if $r > 1$.

As a consequence, we deduce

PROPOSITION 3.3. *Let M, N be Eichler lattices such that $\mathrm{Hom}(M, N) = 0$, and let $M_i \vee M$, $N_i \vee N$, $1 \leqq i \leqq r$. For each i, let $\xi_i \in \mathrm{Ext}(N_i, M_i)$ determine an extension X_i of N_i by M_i, and let $t_i\colon \mathrm{Ext}(N_i, M_i) \cong \mathrm{Ext}(N, M)$ be a standard isomorphism. Then a full set of isomorphism invariants of $\coprod X_i$ are the isomorphism classes of $\coprod M_i$ and $\coprod N_i$, and the strong equivalence class of*

$$\mathrm{diag}(t_1(\xi_1), \cdots, t_r(\xi_r))$$

in $\mathrm{Ext}(N^{(r)}, M^{(r)})$.

Proof. The element $\mathrm{diag}(\xi_1, \cdots, \xi_r) \in \mathrm{Ext}(\coprod N_i, \coprod M_i)$ determines the extension $\coprod X_i$ of $\coprod N_i$ by $\coprod M_i$. There is a standard isomorphism

$$\mathrm{Ext}(\coprod N_i, \coprod M_i) \cong \mathrm{Ext}(N^{(r)}, M^{(r)})$$

which carries $\mathrm{diag}(\xi_1, \cdots, \xi_r)$ onto $\mathrm{diag}(t_1(\xi_1), \cdots, t_r(\xi_r))$. The proposition then follows at once from the above discussion.

4. Cyclic p-groups. We consider here the special case where G is cyclic of order p^κ, where p is prime and $\kappa \geqq 1$. We shall identify ZG with the ring $\Lambda_\kappa = Z[x]/(x^{p^\kappa} - 1)$, which we denote by Λ for brevity when there is no danger of confusion. Let $\Phi_i(x)$ be the cyclotomic polynomial of order p^i and degree $\phi(p^i)$, $0 \leqq i \leqq \kappa$. Let ω_i denote a primitive p^i-th root of 1, and set

$$K_i = Q(\omega_i),\ R_i = \text{alg. int.}\{K_i\} = Z[\omega_i],\ P_i = (1 - \omega_i)R_i\ .$$

Then $R_i \cong Z[x]/(\Phi_i(x))$, a factor ring of Λ, so every R_i-module may be viewed as Λ-module.

Given a Λ-lattice M, let

$$L = \{m \in M\colon (x^{p^{\kappa-1}} - 1)m = 0\}\ .$$

Thus L is a $\Lambda_{\kappa-1}$-lattice, and it is easily verified that M/L is an R_κ-lattice. Assuming that we can classify all L's, the problem of finding all Λ-lattices M becomes one of determining the extensions of R_κ-lattices by such L's. This procedure works well for $\kappa = 1, 2$ (see [1], [7]), but gives only partial results for $\kappa > 2$.

Let us first establish a basic result due to Diederichsen [5]:

PROPOSITION 4.1. *Let $1 \leqq j \leqq \kappa$, and let L be a Λ-lattice such that $(x^{p^{j-1}} - 1)L = 0$. Then*

$$\operatorname{Ext}^1_\Lambda(R_j, L) \cong L/pL\ .$$

Proof. From the exact sequence $0 \to \Phi_j(x)\Lambda \to \Lambda \to R_j \to 0$ we obtain

$$\operatorname{Ext}(R_j, L) \cong \operatorname{Hom}(\Phi_j(x)\Lambda, L)/\text{image of } \operatorname{Hom}(\Lambda, L)\ .$$

Each Λ-homomorphism $f\colon \Phi_j(x)\Lambda \to L$ is completely determined by the image $f(\Phi_j(x))$ in L; this image may be any element of L which is annihilated by the Λ-annihilator of the ideal $\Phi_j(x)\Lambda$. This Λ-annihilator is $\{\prod_{n=j+1}^{\kappa} \Phi_n(x)\}\cdot(x^{p^{j-1}}-1)\Lambda$, which annihilates L by hypothesis. Thus *every* element of L may serve as the image $f(\Phi_j(x))$, and so $\operatorname{Hom}(\Phi_j(x)\Lambda, L) \cong L$. In this isomorphism, the image of $\operatorname{Hom}(\Lambda, L)$ is precisely $\Phi_j(x)L$. But

$$\Phi_j(x) = \sum_{i=0}^{p-1} x^{p^{j-1}\cdot i}\ ,$$

which acts on L as multiplication by p. Therefore $\operatorname{Ext}(R_j, L) \cong L/pL$, as claimed.

We shall consider the problem of classifying extensions of R_j-lattices by R_i-lattices, where $0 \leqq i < j \leqq \kappa$. However, a slightly more general situation can be handled by the same methods, and

this extra generality will be needed later. Let E be any Z-torsionfree factor ring of Λ_{j-1}, so E is a Z-order in a Q-algebra which is a subsum of $\coprod_{i=0}^{p^{j-1}} K_i$. Let J be the kernel of the surjection $Z[x] \to E$. If $a \cdot f(x) \in J$, where $a \in Z$ is nonzero and $f(x) \in Z[x]$, then also $f(x) \in J$ since E is Z-torsionfree. This implies readily that J is a principal ideal $(h(x))$, generated by a primitive polynomial $h(x) \in J$ of least degree. Since $x^{p^{j-1}} - 1 \in J$, we find that $h(x)$ divides $x^{p^{j-1}} - 1$, so $h(x)$ is monic. This shows that E is of the form $Z[x]/(h(x))$, for some monic divisor $h(x)$ of $x^{p^{j-1}} - 1$ in $Z[x]$.

Let E be as above; an E-lattice L is called *locally free* of rank r if $L \vee E^{(r)}$. (Note that all R_j-lattices are necessarily locally free.) We intend to classify extensions of R_j-lattices by locally free E-lattices. From (4.1) we have

$$\mathrm{Ext}^1_\Lambda(R_j, E) \cong E/pE = \bar{E} \text{ (say)} .$$

Let $\bar{Z} = Z/pZ$; the surjection $\Lambda_{j-1} \to E$ induces a surjection $\bar{\Lambda}_{j-1} \to \bar{E}$. Here

$$\bar{\Lambda}_{j-1} = \bar{Z}[x]/(x^{p^{j-1}} - 1) \cong \bar{Z}[\lambda]/(\lambda^{p^{j-1}}), \text{ where } \lambda = 1 - x .$$

Thus $\bar{E}$ is a factor of a local ring $\bar{\Lambda}_{j-1}$, and hence is itself a local ring of the form

$$\bar{E} \cong \bar{Z}[\lambda]/(\lambda^e), \text{ where } e = \deg h(x) .$$

The action of E on $\mathrm{Ext}(R_j, E)$ is given via the surjection $E \to \bar{E}$. On the other hand, $\Phi_j(x) = p$ in Λ_{j-1}, hence also in E, so there is a ring surjection $R_j \to \bar{E}$. Then R_j acts on $\mathrm{Ext}(R_j, E)$ via this surjection. Now let N be any R_j-lattice. By Steinitz's Theorem, we may write $N \cong \coprod_{k=1}^{s} \mathfrak{c}_k$ where each $\mathfrak{c}_k$ is an R_j-ideal in K_j. The isomorphism class of N is determined by its rank s and its *Steinitz class* (namely, $\Pi \mathfrak{c}_k$ computed inside K_j). Analogously (see [11, Exercise 27.7]), a locally free E-lattice L may be written as $L \cong \coprod_{k=1}^{r} \mathfrak{b}_k$, where each $\mathfrak{b}_k$ is an E-lattice in $Q \otimes_Z E$ $(= QE)$ such that $\mathfrak{b}_k \vee E$. The isomorphism class of L is determined by its rank r and its Steinitz class (that is, the isomorphism class of $\Pi \mathfrak{b}_k$ computed inside QE).

Suppose that L and N are given, and let $\xi \in \mathrm{Ext}^1(N, L)$ determine a Λ-lattice X. We wish to classify all such X's up to isomorphism. We have

$$\mathrm{Ext}(N, L) \cong \mathrm{Ext}(R_j^{(s)}, E^{(r)}) \cong \{\mathrm{Ext}(R_j, E)\}^{r \times s} \cong \bar{E}^{r \times s} ,$$

where $\bar{E}^{r \times s}$ denotes the set of all $r \times s$ matrices over $\bar{E}$. Note that $\mathrm{Hom}_\Lambda(E, R_j) = 0$ since $\Phi_j(x)$ annihilates R_j, but acts as multiplication by p on the Z-torsionfree Λ-lattice E. Furthermore, both

R_j and E have commutative endomorphism rings, hence are Eichler lattices. If t: Ext $(N, L) \cong \bar{E}^{r\times s}$ is the isomorphism given above, it follows from § 3 that a full set of invariants of the isomorphism class of X are

(i) The rank s and Steinitz class of N,

(ii) The rank r and Steinitz class of L, and

(iii) The strong equivalence class of $t(\xi)$ in $\bar{E}^{r\times s}$.

We shall assume that the problem of classifying all lattices N and L can be solved somehow. To classify all R_j-lattices, we must determine all R_j-ideal classes in K_j, and we assume that this has been done by standard methods of algebraic number theory. To classify all L's, we need to determine all classes of locally free E-ideals in QE. This is a difficult problem when $j \geqq 3$, and can be handled to some extent by the recent methods due to Galovich [6], Kervaire-Murthy [9], and Ullom [18], [19].

Supposing then that N and L are known, we shall concentrate on the problem of determining all strong equivalence classes in $\bar{E}^{r\times s}$. There are homomorphisms

$$GL(r, E) \longrightarrow GL(r, \bar{E}),\ GL(s, R_j) \longrightarrow GL(s, \bar{E}) ,$$

induced by the ring surjections $E \longrightarrow \bar{E}$, $R_j \longrightarrow \bar{E}$. The strong equivalence classes in $\bar{E}^{r\times s}$ are then the orbits in $\bar{E}^{r\times s}$ under the actions of $GL(r, E)$ on the left, and $GL(s, R_j)$ on the right. In the next section, we shall treat a somewhat more general version of the question of finding all strong equivalence classes.

5. **Strong equivalence classes.** Throughout this section, let Γ and Δ be a pair of commutative rings, and let

$$\varphi: \Gamma \longrightarrow \bar{\Gamma},\ \psi: \Delta \longrightarrow \bar{\Gamma} ,$$

be a pair of ring surjections. We assume that $\bar{\Gamma}$ is a local principal ideal ring, whose distinct ideals are given by $\{\lambda^k\bar{\Gamma}: 0 \leqq k \leqq e\}$, with $\lambda^e\bar{\Gamma} = 0$. Here, e is assumed finite and nonzero. Let $\bar{\Gamma}^{m\times n}$ consist of all $m \times n$ matrices with entries in $\bar{\Gamma}$. The maps φ, ψ induce homomorphisms

$$\varphi_*: GL(m, \Gamma) \longrightarrow GL(m, \bar{\Gamma}),\ \psi_*: GL(n, \Delta) \longrightarrow GL(n, \bar{\Gamma}) , \tag{5.1}$$

which permit us to view $\bar{\Gamma}^{m\times n}$ as a left $GL(m, \Gamma)$-, right $GL(n, \Delta)$-bimodule. As suggested by our earlier considerations, we call two elements $\xi, \xi' \in \bar{\Gamma}^{m\times n}$ *strongly equivalent* (notation: $\xi \approx \xi'$) if $\xi' = \alpha\xi\beta$ for some $\alpha \in GL(m, \Gamma)$, $\beta \in GL(n, \Delta)$; here, α acts as $\varphi_*(\alpha)$, and β as $\psi_*(\beta)$. We wish to determine the strong equivalence classes in $\bar{\Gamma}^{m\times n}$.

(We have already encountered this problem in § 4, where we had a pair of rings R_j and E, with ring surjections $R_j \to \bar{E}$, $E \to \bar{E}$, and where $\bar{E}$ was a local principal ideal ring. In order to classify all extensions of an R_j-lattice of rank s by a locally free E-lattice of rank r, we needed to determine the strong equivalence classes of $\bar{E}^{r\times s}$ under the actions of $GL(r, E)$ and $GL(s, R_j)$.)

Returning to the more general case, we note that if $\xi \approx \xi'$ in $\bar{\Gamma}^{m\times n}$, then ξ is equivalent to ξ' in the usual (weaker) sense, that is, $\xi' = \mu\xi\nu$ for some $\mu, \nu \in GL(\bar{\Gamma})$. We can use the machinery of elementary divisors over the commutative principal ideal ring $\bar{\Gamma}$; these elementary divisors may be chosen to be powers of the prime element λ. Letting el. div. (ξ) denote the set of elementary divisors of ξ, we have at once

PROPOSITION 5.2. *If* $\xi \approx \xi'$, *then* el. div. (ξ) = el. div. (ξ').

As before, let $u(\bar{\Gamma})$ denote the group of units of $\bar{\Gamma}$. The next two lemmas are simple but basic:

LEMMA 5.3. *For* $u \in u(\bar{\Gamma})$, *let* D_u *denote a diagonal matrix in* $GL(m, \bar{\Gamma})$ *with diagonal entries* $u, u^{-1}, 1, \cdots, 1$, *arranged in any order. Let* D'_u *denote an analogous matrix in* $GL(n, \bar{\Gamma})$. *Then for any* $\xi \in \bar{\Gamma}^{m\times n}$,

$$\xi \approx D_u\xi\ , \quad \xi \approx \xi D'_u\ .$$

Proof. There is an identity

$$\begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix} = \begin{pmatrix} 1 & u^{-1} \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & u^{-1} & -1 \\ 0 & 1 & \\ & & \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -u & 1 \end{pmatrix} \tag{5.4}$$

in $GL(2, \bar{\Gamma})$. This implies that D_u is expressible as a product of elementary matrices in $GL(m, \bar{\Gamma})$. Each factor is the image of an elementary matrix in $GL(m, \Gamma)$, so $\xi \approx D_u\xi$. An analogous argument proves that $\xi \approx \xi D'_u$.

LEMMA 5.5. *If* $m \leqq n$, *then each* $\xi \in \bar{\Gamma}^{m\times n}$ *is strongly equivalent to a matrix* $[D\ 0]$, *where*

$$D = \operatorname{diag}(\lambda^{k_1}u_1, \cdots, \lambda^{k_m}u_m)\ ,\ 0 \leqq k_1 \leqq \cdots \leqq k_m \leqq e,\ u_i \in u(\bar{\Gamma})\ . \tag{5.6}$$

If $m \geqq n$, *then* $\xi \approx \begin{bmatrix} D' \\ 0 \end{bmatrix}$, *where* D' *is a diagonal* $n \times n$ *matrix of the above type.*

Proof. Let $\xi \in \bar{\Gamma}^{m\times n}$, where $m \leqq n$. Since $\bar{\Gamma}$ is a local principal

ideal ring, we can bring ξ into the form $[D\ 0]$, with D as above, by a sequence of left and right multiplications by elementary matrices in $GL(\bar{\Gamma})$. Each such elementary matrix lies in either $\mathrm{im}(\varphi_*)$ or $\mathrm{im}(\psi_*)$, and thus $\xi \approx [D\ 0]$ as claimed. An analogous proof is valid for the case where $m \geqq n$.

Suppose now that $\xi \in \bar{\Gamma}^{m\times n}$; for convenience of notation let us assume that $m \leqq n$, and let $\xi \approx [D\ 0]$ with D as in (5.6). Then obviously

$$\text{el. div.}(\xi) = \{\lambda^{k_1}, \cdots, \lambda^{k_m}\}\ .$$

It follows at once from (5.2) that the set $\{\lambda^{k_1}, \cdots, \lambda^{k_m}\}$ is an invariant of the strong equivalence class of ξ. Let us show at once that this is the *only* invariant when $m \neq n$.

PROPOSITION 5.7. *Let $\xi, \xi' \in \bar{\Gamma}^{m\times n}$, where $m \neq n$. Then $\xi \approx \xi'$ if and only if* el. div. $(\xi) =$ el. div. (ξ').

Proof. By (5.2) it suffices to show that if $m \neq n$, then ξ is determined up to strong equivalence by its set of elementary divisors. For convenience of notation, assume that $m \leqq n$, and write $\xi \approx [D\ 0]$, with D as in (5.6). By (5.3) we have

$$[D\ 0] \approx [D\ 0]\cdot \mathrm{diag}\,(u_1^{-1}, u_2^{-1}, \cdots, u_m^{-1}, \underbrace{u_1\cdots u_m, 1, \cdots, 1}_{n-m})\ .$$

This gives

$$\xi \approx [D_1\ 0] \text{ where } D_1 = \mathrm{diag}\,(\lambda^{k_1}, \cdots, \lambda^{k_m})\ ,$$

and so the strong equivalence class of ξ is determined by el. div. (ξ). This completes the proof.

We are now ready to turn to the question as to when two elements ξ and ξ' in $\bar{\Gamma}^{m\times m}$ are strongly equivalent. By (5.2), it suffices to treat the case where ξ and ξ' have the same elementary divisors. We shall see that there is exactly one additional invariant needed for this case. To begin with, we introduce the following notation: let $\xi \in \bar{\Gamma}^{m\times m}$, and suppose that $\xi \approx D$, where D is given by (5.6). We set

$$\Gamma' = \bar{\Gamma}/\lambda^{e-k_m}\bar{\Gamma},\ U = u(\Gamma')/u^*(\Gamma)u^*(\Delta)\ , \tag{5.8}$$

where $u^*(\Gamma)$ denotes the image of $u(\Gamma)$ in $u(\Gamma')$, and $u^*(\Delta)$ the image of $u(\Delta)$. Define

$$u(\xi) = \text{image of } u_1\cdots u_m \text{ in } U\ . \tag{5.9}$$

The main result of this section is as follows:

THEOREM 5.10. *Let* $\xi, \xi' \in \bar{\Gamma}^{m\times m}$. *Then* $\xi \approx \xi'$ *if and only if*
(i) el. div. (ξ) = el. div. (ξ'), *and*
(ii) $u(\xi) = u(\xi')$ *in* U.

Proof. Supposing that conditions (i) and (ii) are satisfied, let

$$\xi \approx D,\ \xi \approx \operatorname{diag}(\lambda^{k_1}u_1', \cdots, \lambda^{k_m}u_m'),\ u_i' \in u(\bar{\Gamma}) ,$$

where D is given by (5.6). Setting $u = \Pi u_i$, $u' = \Pi u_i'$, it follows from the proof of (5.7) that

$$\xi \approx \operatorname{diag}(\lambda^{k_1}, \cdots, \lambda^{k_{m-1}}, \lambda^{k_m}u),\ \xi' \approx \operatorname{diag}(\lambda^{k_1}, \cdots, \lambda^{k_{m-1}}, \lambda^{k_m}u') . \tag{5.11}$$

By virtue of (ii), there exist elements $\gamma \in u(\Gamma)$, $\delta \in u(\Delta)$, such that $u' = \gamma u \delta$ in Γ'. But then

$$\lambda^{k_m}u' = \gamma \cdot \lambda^{k_m}u \cdot \delta \quad \text{in } \bar{\Gamma} ,$$

so

$$\operatorname{diag}(1, \cdots, 1, \gamma)\cdot\operatorname{diag}(\lambda^{k_1}, \cdots, \lambda^{k_{m-1}}, \lambda^{k_m}u)\cdot\operatorname{diag}(1, \cdots, 1, \delta) = \operatorname{diag}(\lambda^{k_1}, \cdots, \lambda^{k_{m-1}}, \lambda^{k_m}u') .$$

Therefore $\xi' \approx \xi$, as desired.

Conversely, assume that $\xi \approx \xi'$, so (i) holds by (5.2). In proving (ii), we may assume without loss of generality that ξ and ξ' are equal (respectively) to the diagonal matrices listed in (5.11). Since $\xi \approx \xi'$, we have $\mu\xi' = \xi\nu$ for some $\mu \in GL(m, \Gamma)$, $\nu \in GL(m, \Delta)$. It is tempting to take determinants of both sides, but this procedure fails because $\lambda^e = 0$ in $\bar{\Gamma}$. Instead, we proceed as follows: let $D_0 = \operatorname{diag}(\lambda^{k_1}, \cdots, \lambda^{k_m})$, and put

$$\mu_1 = \varphi_*(\mu)\cdot\operatorname{diag}(1, \cdots, 1, u'),\ \nu_1 = \operatorname{diag}(1, \cdots, 1, u)\cdot\psi_*(\nu) .$$

The equation $\mu\xi' = \xi\nu$ then becomes $\mu_1 \cdot D_0 = D_0 \cdot \nu_1$. By (5.12) below, this implies that $(\det \mu_1)\lambda^{k_m} = (\det \nu_1)\lambda^{k_m}$. But $\det \mu_1 = u' \cdot \varphi(\det \mu)$, and $\det \nu_1 = u \cdot \psi(\det \nu)$. Therefore the images of u and u' in $u(\Gamma')$ differ by a factor from $u^*(\Gamma)u^*(\Delta)$, which shows that $u(\xi) = u(\xi')$ in U, and completes the proof.

It remains for us to establish the following amusing result on determinants:

PROPOSITION 5.12. *Let* R *be an arbitrary commutative ring, and let* $D = \operatorname{diag}(\xi_1, \cdots, \xi_m)$ *be a matrix over* R *such that*

$$r_1\xi_1 = \cdots = r_{m-1}\xi_{m-1} = \xi_m$$

for some elements $r_i \in R$. *Let* $X, Y \in R^{m\times m}$ *be matrices for which* $XD = DY$. *Then*

$$(\det X)\cdot\xi_m = (\det Y)\cdot\xi_m$$

in R.

Proof. Let $X = (x_{ij})$, $Y = (y_{ij})$. The equation $XD = DY$ gives

$$x_{ij}\xi_j = \xi_i y_{ij},\ 1 \leqq i,\ j \leqq m\ .$$

Let $\pi\colon 1 \to i_1, \cdots, m \to i_m$, be a permutation of the symbols $\{1, \cdots, m\}$. A typical term in the expansion of $\det X$ is of the form $\pm x_{1i_1}\cdots x_{mi_m}$, and we need only show that for each π we have

$$x_{1i_1}\cdots x_{mi_m}\xi_m = y_{1i_1}\cdots y_{mi_m}\xi_m\ . \tag{5.13}$$

Write π as a product of cycles, and suppose by way of illustration that (a, b, c) is a 3-cycle occuring as a factor of π. Then

$$\begin{aligned} x_{ab}x_{bc}x_{ca}\xi_m &= r_a\cdot x_{ab}x_{bc}x_{ca}\xi_a = r_a x_{ab}x_{bc}\xi_c y_{ca} = r_a x_{ab}\xi_b y_{bc}y_{ca} \\ &= r_a\xi_a y_{ab}y_{bc}y_{ca} = y_{ab}y_{bc}y_{ca}\xi_m\ . \end{aligned}$$

The same procedure applies to each cycle occuring in π, which establishes (5.13), and completes the proof of the proposition.

The special case where $\Gamma = \Delta = Z$, $\bar{\Gamma} = Z/(p^e)$, p prime, is of interest. For a matrix $X \in Z^{m\times n}$, let p-el. div. (X) be the powers of p occurring in the ordinary elementary divisors of X (over Z). If X is square, write $\det X = (\text{power of } p)\cdot u_X$, where $p \nmid u_X$. (Take $u_X = 1$ if $\det X = 0$.) For $X, Y, \in Z^{m\times n}$, we write $X \approx Y$ if

$$Y \equiv PXQ \pmod{p^e}$$

for some $P \in GL(m, Z)$, $Q \in GL(n, Z)$. From (5.10) we obtain

COROLLARY 5.14. *Let* $X, Y \in Z^{m\times n}$. *Then* $X \approx Y$ *if and only if*
(i) p-el. div. $(X) = p$-el. div. (Y), *and*
(ii) *when* $m = n$,

$$u_Y \equiv \pm u_X \pmod{p^{e-k}}\ ,$$

where k *is the maximum of the exponents of the* p*-elementary divisors of* X. *(If* $k \geqq e$, *condition* (ii) *is automatically satisfied.)*

For the particular cases needed in §§ 6-7, one can easily deduce (5.7) and (5.10) as special cases of the results of Jacobinski [8]. However, it seemed desirable to give here a self-contained proof of (5.7) and (5.10).

6. Invariants of direct sums of extensions. We now return to the study of integral representations of a cyclic group G of

order p^e, keeping the notation of § 4. Let N be an R_j-lattice of rank s, and L a locally free E-lattice of rank r. We have seen that

$$\mathrm{Ext}^1_{ZG}(N, L) \cong \mathrm{Ext}^1_{ZG}(R_j^{(s)}, E^{(r)}) \cong \bar{E}^{r\times s} ,$$

where $\bar{E} \cong \bar{Z}[\lambda]/(\lambda^e)$ is a local principal ideal ring. Each extension X of N by L determines a class $\xi_X \in \bar{E}^{r\times s}$, and an element $u(\xi_X)$ in a factor group of the group of units of some quotient ring of $\bar{E}$ (see (5.9)). It follows from the results of §§ 4, 5 that a full set of isomorphism invariants of X are as follows:

(i) The rank s of N, and its Steinitz class,
(ii) The rank r of L, and its Steinitz class,
(iii) The elementary divisors of the matrix ξ_X,
(iv) For the case $r = s$ only, the element $u(\xi_X)$.

Since G is a p-group, the genus of X is completely determined by the p-adic completion X_p. In the local case, however, the ideal classes occurring above are trivial, as is the group in which $u(\xi_X)$ lies. Therefore the genus invariants of X are just r, s, and el. div. (ξ_X). Furthermore, by (5.5) the extension X must decompose into a direct sum of ideals $\mathfrak{b}$ of R_j, locally free ideals $\mathfrak{c}$ of E, and nonsplit extensions of $\mathfrak{c}$ by $\mathfrak{b}$. Let us denote by $(\mathfrak{b}, \mathfrak{c}; \lambda^k u)$ an extension of $\mathfrak{c}$ by $\mathfrak{b}$ corresponding to the extension class $\lambda^k u \in \bar{E}$, where $0 \leqq k < e$, $u \in u(\bar{E})$, and we have chosen some standard isomorphism $\mathrm{Ext}(\mathfrak{c}, \mathfrak{b}) \cong \bar{E}$. By (1.5), the lattice $(\mathfrak{b}, \mathfrak{c}; \lambda^k u)$ is indecomposable since $\lambda^k u \neq 0$ in $\bar{E}$.

Some further notation will be useful below. Let us set $E' = \bar{E}/\lambda^m\bar{E} \cong \bar{Z}[\lambda]/(\lambda^m)$, where $1 \leqq m \leqq e$. There are ring surjections $E \to E'$, $R_j \to E'$; let $u^*(E)$ denote the image of $u(E)$ in $u(E')$, and define $u^*(R_j)$ analogously. We now set

$$U_m = u(E')/u^*(E)u^*(R_j) . \tag{6.1}$$

It follows from the above discussion that a full set of isomorphism invariants of $(\mathfrak{b}, \mathfrak{c}; \lambda^k u)$ are the isomorphism classes of $\mathfrak{b}$ and $\mathfrak{c}$, the integer k, and the image of u in U_{e-k}. The genus of X depends only on k.

We may remark that the group $u(E')$ is easily described, namely,

$$u(E') \cong u(\bar{Z}) \times \prod_{i=1}^{m-1}{}' \langle 1 + \lambda^i \rangle ,$$

where in the product i ranges over the integers between 1 and $m - 1$ which are prime to p. On the other hand, the calculation of $u^*(E)$ and $u^*(R_j)$ is considerably more difficult, and the results so far known are given in [6], [9], [18], and [19]. It is easily veri-

fied that $u^*(R_j)$ contains the factor $u(\bar{Z})$, and further that $1+\lambda \in u^*(R_j)$ since $1+\lambda = x$. It follows at once that U_1 and U_2 are trivial for all p.

In the special case where $E = R_i$ with $i < j$, we claim that $u^*(R_j) \subset u^*(R_i)$, and hence that

$$U_m = u(E')/u^*(R_i) .$$

Indeed, as pointed out in [6], there is a commutative diagram

$$\begin{array}{ccc} u(R_j) & \xrightarrow{N} & u(R_i) \\ & \searrow^{\theta_j} & \downarrow{\scriptstyle \theta_i} \\ & & u(\bar{R}_i) , \end{array}$$

where $\bar{R}_i = R_i/pR_i$ and N is the relative norm map. Hence $\operatorname{im}\theta_j \subset \operatorname{im}\theta_i$, which implies that $u^*(R_j) \subset u^*(R_i)$ in $u(E')$.

The structure of U_m has been studied in detail by Galovich [6] and Kervaire-Murthy [9], especially for the case of regular primes. An odd prime p is *regular* if the ideal class number of R_1 is relatively prime to p (see [2]). For regular p, we have

$$u^*(R_j) \cong u(\bar{Z}) \times \langle 1+\lambda \rangle \times \prod \langle 1 + \lambda^{2i} + \alpha_i \lambda^{2i+1} \rangle , \tag{6.2}$$

where each $\alpha_i \in E'$, and where i ranges over all integers from 1 to $[(m-1)/2]$ which are prime to p. Furthermore, $u^*(E) \subset u^*(R_j)$ in this case, so U_m is of order $p^{f(m)}$, where $f(m)$ is the number of odd integers among $3, 5, \cdots, m-1$ which are prime to p.

Some additional information is available for the special case where $j = 2$; here, $e \leqq p$ and U_m is an elementary abelian p-group. Let $\delta(k)$ be the number of Bernoulli numbers among $B_1, B_2, \cdots, B_k$ whose numerators are divisible by p. Then (see [2]) the prime p is regular if and only if $\delta((p-3)/2) = 0$. Call p *properly irregular* if p divides the class number of R_1 but not that of $Z[\omega_1 + \omega_1^{-1}]$. For such p, one must omit from the formula (6.2) all those factors $1 + \lambda^{2i} + \alpha_i\lambda^{2i+1}$ for which $2i \leqq p-3$ and the numerator of B_i is a multiple of p. Thus for properly irregular primes p, U_m is elementary abelian of order $p^{g(m)}$, where

$$g(m) = \begin{cases} [(m-2)/2] + \delta[(m-1)/2] , & 0 \leqq m \leqq p-2 , \\ (p-3)/2 + \delta((p-3)/2) , & m = p-1 , \quad p . \end{cases} \tag{6.3}$$

Here, we must interpret the greatest integer function $[(m-2)/2]$ as 0 when $m < 2$. Further, for $j = 2$, U_m is trivial when $p = 2$.

For the case where $E = Z[x]/(x^p - 1)$ and $j = 2$, it is known (see [6], [9], [19]) that $u^*(E) = u^*(R_2)$ for all m and all regular or

properly irregular primes p. It seems likely that a corresponding result holds for $j > 2$ for arbitrary E, for all primes p (in this connection, see [19]).

From the results stated earlier in this section, we obtain

THEOREM 6.3a. *Consider the direct sum*

$$Y = \coprod_{k=1}^{b} \mathfrak{b}'_k \oplus \coprod_{n=1}^{c} \mathfrak{c}'_n \oplus \coprod_{i=1}^{d} (\mathfrak{b}_i, \mathfrak{c}_i; \lambda^{k_i} u_i) , \tag{6.4}$$

where each $\mathfrak{b}$ *is a locally free* E*-ideal, each* $\mathfrak{c}$ *an* R_j*-ideal, and* $0 \leqq k_i < e$, $u_i \in u(\bar{E})$ *for each* i. *We may view* Y *as an extension* $0 \to Y_0 \to Y \to Y_1 \to 0$, *where*

$$Y_0 = \coprod \mathfrak{b}'_k \oplus \coprod \mathfrak{b}_i , \quad Y_1 = \coprod \mathfrak{c}'_n \oplus \coprod \mathfrak{c}_i ,$$

corresponding to the $(b + d) \times (c + d)$ *matrix* $\begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$ *over* $\bar{E}$, *with* $D = \operatorname{diag}(\lambda^{k_1} u_1, \cdots, \lambda^{k_d} u_d)$. *Define* U_m *as in* (6.1), *with*

$$m = \operatorname{Min}\{e - k_i : 1 \leqq i \leqq d\} .$$

Then we have

(i) *The genus of* Y *is determined by the integer* $b + d$ (=E*-rank of* Y_0), *the integer* $c + d$ (=R_j*-rank of* Y_1), *and the set of exponents* $\{k_i\}$.

(ii) *The additional invariants of the isomorphism class of* Y, *needed to determine this class, are the isomorphism classes of*

$$\Pi\mathfrak{b}'_k \cdot \Pi\mathfrak{b}_i \quad \text{and} \quad \Pi\mathfrak{c}'_n \cdot \Pi\mathfrak{c}_i ,$$

and one further invariant which occurs only when $b = c = 0$, *namely the image of* $u_1 \cdots u_d$ *in* U_m.

Several remarks are in order concerning the above result. First of all, we note that

$$\mathfrak{b}' \oplus (\mathfrak{b}, \mathfrak{c}; \lambda^k u) \cong \mathfrak{b}' \oplus (\mathfrak{b}, \mathfrak{c}; \lambda^k) \tag{6.5}$$

as a consequence of the Absorption Formula (2.7). Namely, choose $w \in E$ with image $u \in \bar{E}$, so then

$$(\mathfrak{b}, \mathfrak{c}; \lambda^k u) = {}_w(\mathfrak{b}, \mathfrak{c}; \lambda^k)$$

in the notation of § 2. Since $\mathfrak{b}'/w\mathfrak{b}' \cong b/w\mathfrak{b}$ because $\mathfrak{b} \vee \mathfrak{b}'$, formula (6.5) follows from the proof of (2.7). Likewise, we have

$$\mathfrak{c}' \oplus (\mathfrak{b}, \mathfrak{c}; \lambda^k u) \cong \mathfrak{c}' \oplus (\mathfrak{b}, \mathfrak{c}; \lambda^k)$$

always, by using the fact that R_j maps onto E. Thus, if either b

or c is nonzero, we may replace each u_i in (6.4) by 1 without affecting the isomorphism class of Y. This agrees with our previous result.

Next, suppose that $b = c = 0$, and suppose the summands of Y numbered so that $k_d = \text{Max}\{k_i\}$. The Exchange Formula (2.4) gives $Y \cong W \oplus X$, where

$$W = \coprod_1^{d-1} (\mathfrak{b}_i, \mathfrak{c}_i; \lambda^{k_i}) , \quad X = (\mathfrak{b}_d, \mathfrak{c}_d; \lambda^{k_d} u) ,$$

and $u = u_1 \cdots u_d$. Let $X' = (\mathfrak{b}_d, \mathfrak{c}_d; \lambda^{k_d} u')$. Our previous result then takes the form of a Cancellation Theorem, namely,

$$W \oplus X \cong W \oplus X' \text{ if and only if } X \cong X' . \tag{6.6}$$

This is of special interest in that it applies to a situation in which the summands lie in different genera. We may also deduce (6.6) from Jacobinski's Cancellation Theorem [8, § 4] if desired.

To conclude these remarks, we may point out that the results of § 5 yield a slightly more general cancellation theorem, as follows: let Λ be any R-lattice in a semisimple K-algebra A, and let M, N be Λ-lattices with commutative Λ-endomorphism rings Γ, Δ, respectively. For $i = 1, \cdots, d$, let X_i be an extension of N by M corresponding to the class $\xi_i \in \text{Ext}(N, M)$. Suppose that for each i, we may write $\xi_d = \gamma_i \xi_i \delta_i$ for some $\gamma_i \in \Gamma$, $\delta_i \in \Delta$, and let X' be any Λ-lattice. Then

$$\coprod_1^{d-1} X_i \oplus X_d \cong \coprod_1^{d-1} X_i \oplus X' \text{ if and only if } X_d \cong X' .$$

Further, the same result holds if each X_i is replaced by a lattice in its genus.

7. **Cyclic groups of order p^2.** We shall now determine a full set of isomorphism invariants of ZG-lattices, where G is cyclic of order p^2. To simplify the notation, we set

$$R = Z[\omega_1], S = Z[\omega_2], E = Z[x]/(x^p - 1), \bar{E} = E/pE \cong \bar{Z}[\lambda]/(\lambda^p) ,$$

where $\bar{Z} = Z/pZ$ and $\lambda = 1 - x$. By § 4, every E-lattice is an extension of an R-lattice by a Z-lattice. In this case, we have $\text{Ext}(R, Z) \cong \bar{Z}$, and $u(R)$ maps onto $u(\bar{Z})$. Thus by § 6, the only indecomposable E-lattices are Z, $\mathfrak{b}$, and $E(\mathfrak{b}) = (Z, \mathfrak{b}; 1)$, where $\mathfrak{b}$ ranges over a full set of representatives of the h_R ideal classes of R. Here, $(Z, \mathfrak{b}; 1)$ denotes an extension of $\mathfrak{b}$ by Z corresponding to the extension class $\bar{1} \in \bar{Z}$, using a standard isomorphism $\text{Ext}(\mathfrak{b}, Z) \cong \bar{Z}$. We note that $E(\mathfrak{b}) \vee E$, so $E(\mathfrak{b})$ is a locally free E-lattice of rank 1; conversely, every such lattice is isomorphic to some $E(\mathfrak{b})$.

By § 6, every E-lattice L is of the form

$$L \cong Z^{(a)} \oplus \coprod_{i=1}^{b} \mathfrak{b}_i' \oplus \coprod_{j=1}^{c} E(\mathfrak{b}_j) , \tag{7.1}$$

and a full set of isomorphism invariants of L are the integers a, b, c (the genus invariants), and the ideal class of $\Pi\mathfrak{b}_i' \cdot \Pi\mathfrak{b}_j$.

Now let M be any ZG-lattice. By § 4, M is an extension of an S-lattice N by an E-lattice L. A full set of isomorphism invariants of M are the isomorphism class of L (just determined above), the isomorphism class of N, and the strong equivalence class in $\mathrm{Ext}(N, L)$ containing the extension class of M. Of course, N is determined up to isomorphism by its S-rank and Steinitz class. Furthermore, in calculating strong equivalence classes in $\mathrm{Ext}(N, L)$, we may replace N by any lattice in its genus, and likewise for L. Thus it suffices to treat the case where L is a sum of copies of Z, R, and E, and where N is S-free. However, our conclusions can be stated more neatly as an answer to the following equivalent question: what are the isomorphism invariants of a direct sum of indecomposable ZG-lattices?

As shown in [7], a ZG-lattice M is indecomposable if and only if M_p is indecomposable. The indecomposable Z_pG-lattices can be determined explicitly by considering strong equivalence in the local case (see [1] or [7]; the case $p = 2$ is treated in [14] and [17]). Rather than repeat the local argument here, we just state the conclusion: every indecomposable ZG-lattice is in the same genus as one (and only one) of the following $4p + 1$ indecomposable ZG-lattices:

$$\begin{cases} Z,\ R,\ E,\ S,\ (Z, S; 1)\ , \\ (E, S; \lambda^r),\ 0 \leqq r \leqq p-1\ , \\ (Z \oplus E, S; 1 \oplus \lambda^r),\ 1 \leqq r \leqq p-2\ , \\ (R, S; \lambda^r),\ 0 \leqq r \leqq p-2\ , \\ (Z \oplus R,\ S; 1 \oplus \lambda^r),\ 0 \leqq r \leqq p-2\ . \end{cases} \tag{7.2}$$

Here $(Z, S; 1)$ represents an extension of S by Z with class $\bar{1} \in \bar{Z}$, using the isomorphism $\mathrm{Ext}(S, Z) \cong \bar{Z}$. Further, $(Z \oplus E, S; 1 \oplus \lambda^r)$ denotes an extension of S by $Z \oplus E$ with class $(1, \lambda^r) \in \bar{Z} \oplus \bar{E}$, using the isomorphism $\mathrm{Ext}(S, Z \oplus E) \cong \bar{Z} \oplus \bar{E}$. Analogous definitions hold for the other cases.

A full set of nonisomorphic indecomposable ZG-lattices may now be obtained from (7.2), by finding all isomorphism classes in each of the genera occurring in (7.2). This was done in [12], but we take this opportunity to correct a misstatement in that article. Let us denote by $\tilde{U}_m$ a full set of representatives u in $u(\bar{R})$ or $u(\bar{E})$

of the elements of the factor group U_m, where the u's are chosen so that $u \equiv 1 \pmod{\lambda}$. Recall that for $1 \leqq m \leqq p-1$, U_m denotes the group of units of $\bar{Z}[\lambda]/(\lambda^m)$ modulo the image of $u(R)$, while U_p denotes $u(\bar{E})$ modulo the images of $u(S)$ and $u(E)$. The notations U_m, U_p are then consistent with those introduced in § 6. Finally, let n_0 be some fixed quadratic nonresidue (mod p).

THEOREM 7.3. *Let* $\mathfrak{b}$ *range over a full set of representatives of the* h_R *ideal classes of* R, *and* $\mathfrak{c}$ *likewise for the* h_S *ideal classes of* S. *A full list of nonisomorphic indecomposable* ZG*-lattices is as follows*:

(a) Z, $\mathfrak{b}$, $E(\mathfrak{b})$, $\mathfrak{c}$, $(Z, \mathfrak{c}; 1)$.

(b) $(E(\mathfrak{b}), \mathfrak{c}; \lambda^r u)$, $u \in \tilde{U}_{p-r}$, $0 \leqq r \leqq p-1$.

(c) $(Z \oplus E(\mathfrak{b}), \mathfrak{c}; 1 \oplus \lambda^r u)$, $u \in \tilde{U}_{p-1-r}$, $1 \leqq r \leqq p-2$.

(d) *If* $p \equiv 1 \pmod 4$, $(Z \oplus E(\mathfrak{b}), \mathfrak{c}; 1 \oplus \lambda^r u n_0)$, $u \in \tilde{U}_{p-1-r}$, $1 \leqq r \leqq p-2$.

(e) $(\mathfrak{b}, \mathfrak{c}; \lambda^r u)$, $u \in \tilde{U}_{p-1-r}$, $0 \leqq r \leqq p-2$.

(f) $(Z \oplus \mathfrak{b}, \mathfrak{c}; 1 \oplus \lambda^r u)$, $u \in \tilde{U}_{p-1-r}$, $0 \leqq r \leqq p-2$.

Proof. Observe first that $\mathfrak{b}$ gives all isomorphism classes in the genus of R, and $\mathfrak{c}$ these in the genus of S. Further $E(\mathfrak{b})$ gives all isomorphism classes in the genus of E. It remains for us to check strong equivalence classes in each of the remaining cases, and for this it suffices to treat the cases where $\mathfrak{b}=R$, $\mathfrak{c}=S$ and $E(\mathfrak{b})=E$.

Next, we have $\mathrm{Ext}(S, Z) \cong \bar{Z}$, and $u(S)$ maps onto $u(\bar{Z})$. Hence there is only one nonzero strong equivalence class in $\mathrm{Ext}(S, Z)$, so all nonsplit extensions of S by Z are mutually isomorphic. Also, $\mathrm{Ext}(S, E) \cong \bar{E} \cong \bar{Z}[\lambda]/(\lambda^p)$, and by § 6 the nonzero strong equivalence classes in $\mathrm{Ext}(S, E)$ are represented by $\{\lambda^r u: u \in \tilde{U}_{p-r},\ 0 \leqq r \leqq p-1\}$. This gives the lattices described in (b). A similar argument yields those in (e).

Consider next the classification of lattices in the genus of $(Z \oplus R, S; 1 \oplus \lambda^r)$, where $0 \leqq r \leqq p-2$. The following observation is needed both here and later: each E-lattice L is expressible as an extension $0 \to L_0 \to L \xrightarrow{\theta} L_1 \to 0$, with L_0 a Z-lattice uniquely determined inside L, and L_1 an R-lattice. The map θ induces surjections $\bar{L} \to \bar{L}_1$, $\mathrm{Ext}(S, L) \to \mathrm{Ext}(S, L_1)$, where bars denote reduction mod p, and where the surjections are consistent with the isomorphisms $\mathrm{Ext}(S, L) \cong \bar{L}$, $\mathrm{Ext}(S, L_1) \cong \bar{L}_1$. Now let M be an extension of an S-lattice N by L, so L (and hence also L_0) are uniquely determined inside M. Then there is a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \longrightarrow & M & \longrightarrow & N & \longrightarrow & 0 \\ & & \theta\downarrow & & \downarrow & & 1\downarrow & & \\ 0 & \longrightarrow & L_1 & \longrightarrow & M^* & \longrightarrow & N & \longrightarrow & 0\,, \end{array}$$

giving rise to a ZG-exact sequence

$$0 \longrightarrow L_0 \longrightarrow M \longrightarrow M^* \longrightarrow 0 .$$

The isomorphism class of M uniquely determines that of M^*, and the extension class of M^* in $\mathrm{Ext}(N, L_1)$ is the image of the class of M in $\mathrm{Ext}(N, L)$, under the map induced by θ.

Suppose in particular that $M = (Z \oplus R, S; 1 \oplus \lambda^r u)$; then $M^* \cong (R, S; \lambda^r u)$, and thus the image of u in U_{p-1-r} is an isomorphism invariant of M. Conversely, any M' in the genus of M may be written as $(Z \oplus \mathfrak{b}, \mathfrak{c}; q \oplus \lambda^r u')$, where $q \in u(\bar{Z})$. Then $M' \cong (Z \oplus \mathfrak{b}, \mathfrak{c}; q\beta \oplus \lambda^r \alpha u' \beta)$ for any $\alpha \in u(R)$, $\beta \in u(S)$. Choose β so that $q\beta = \bar{1}$ in $\bar{Z}$, and then choose α so that $\alpha u' \beta$ lies in $\tilde{U}_{p-1-r}$. This proves that M' is isomorphic to one of the lattices in (f), and therefore (f) gives a full list of nonisomorphic indecomposable ZG-lattices in the genus of $(Z \oplus R, S; 1 \oplus \lambda^r)$.

Turning to the most difficult case, we have $\mathrm{Ext}(S, Z \oplus E) \cong \bar{Z} \oplus \bar{E}$, and we must determine strong equivalence classes in $\bar{Z} \oplus \bar{E}$ under the actions of $\mathrm{Aut}(Z \oplus E)$ and $\mathrm{Aut}(S)$. We may represent the elements of $\bar{Z} \oplus \bar{E}$ as vectors $\begin{pmatrix} \bar{z} \\ \bar{e} \end{pmatrix}$ on which $\mathrm{Aut}(Z \oplus E)$ acts from the left, and $\mathrm{Aut}(S)$ from the right. Let $\Phi(x)$ denote the cyclotomic polynomial of order p. Since $\mathrm{Hom}(E, Z) \cong Z$ and $\mathrm{Hom}(Z, E) \cong \Phi(x)E$, we obtain

$$\mathrm{End}(Z \oplus E) = \left\{ f : f = \begin{pmatrix} a & b \\ \Phi(x)c & d \end{pmatrix},\ a, b \in Z,\ c, d \in E \right\} . \tag{7.4}$$

There is a fiber product diagram

$$\begin{array}{ccc} E & \xrightarrow{\varphi_1} & Z \\ {\scriptstyle \varphi_2}\downarrow & & \downarrow \\ R & \longrightarrow & \bar{Z} , \end{array} \tag{7.5}$$

and an E-exact sequence

$$0 \longrightarrow Z \oplus Z \xrightarrow{1 \oplus \Phi(x)} Z \oplus E \longrightarrow R \longrightarrow 0 .$$

Each $f \in \mathrm{End}(Z \oplus E)$, given as in (7.4), induces a map f_1 on $Z \oplus Z$ and a map f_2 on R, where

$$f_1 = \begin{pmatrix} a & b \\ p\varphi_1(c) & \varphi_1(d) \end{pmatrix}, \quad f_2 = \text{multiplication by } \varphi_2(d) .$$

Clearly, f is an automorphism if and only if $f_1 \in GL(2, Z)$ and $\varphi_2(d) \in u(R)$. Furthermore, for each $\alpha \in u(R)$ there exists an automorphism

f such that $\varphi_2(d) = \alpha$. Also, for each matrix $\mu \in GL(2, Z)$ whose (2, 1) entry is divisible by p, we can find an automorphism f such that $f_1 = \mu$.

Now let M be a lattice in the genus of $(Z \oplus E, S; 1 \oplus \lambda^r)$ with extension class $\begin{pmatrix} \bar{z} \\ \bar{e} \end{pmatrix}$. Since $\begin{pmatrix} \bar{z} \\ \bar{e} \end{pmatrix} \approx \begin{pmatrix} \bar{1} \\ \bar{e}_1 \end{pmatrix}$ for some $\bar{e}_1$, we may hereafter assume that $\bar{z} = \bar{1}$. Factoring out the submodule $Z \oplus Z$ of M as before, we obtain an extension M^* of S by R, with extension class $\bar{\varphi}_2(\bar{e})$, where $\bar{\varphi}_2 : \bar{E} \to \bar{R}$ is induced from φ_2. The isomorphism class of M^* is determined from that of M. In particular, if the extension class of M is $\begin{pmatrix} \bar{1} \\ \lambda^r u \end{pmatrix}$, where $1 \leqq r \leqq p-2$ and $u \in u(\bar{E})$, then the extension class of M^* is $\lambda^r u$, viewed as element of $\bar{R}$. Therefore the image of u in U_{p-1-r} is an isomorphism invariant of M. We shall see that when $p \equiv 3 \bmod 4$, this image of u and the integer r are a full set of isomorphism invariants of M. On the other hand, when $p \equiv 1 \bmod 4$, an additional invariant will be needed, namely the quadratic character of $u \pmod{\lambda}$ viewed as element of $u(\bar{Z})$.

Let $f \in \mathrm{Aut}\,(Z \oplus E)$, $s \in u(S)$, and let $1 \leqq r \leqq p-2$. The equation

$$\begin{pmatrix} a & b \\ \Phi(x)c & d \end{pmatrix} \begin{pmatrix} \bar{1} \\ \lambda^r u \end{pmatrix} \cdot s = \begin{pmatrix} \bar{1} \\ \lambda^r u' \end{pmatrix} \tag{7.5'}$$

becomes (since $\lambda^r b = 0$ in $\bar{Z}$)

$$as\bar{1} = \bar{1} \quad \text{in } \bar{Z}, \quad \lambda^r u' = sd\lambda^r u + \Phi(x)\bar{c}s \quad \text{in } \bar{E}\,.$$

Since $\det f_1 = \pm 1$, we have $ad \equiv \pm 1 (\bmod \lambda)$ in $\bar{E}$. Thus we obtain

$$u' \equiv sdu \equiv \pm a^{-2} u \,(\bmod \lambda)\,. \tag{7.6}$$

If $p \equiv 3 \,(\bmod 4)$, then as a ranges over all integers prime to p so does $\pm a^{-2}$, and (7.6) imposes no condition on $u \,(\bmod \lambda)$. However, if $p \equiv 1 \,(\bmod 4)$, then $\pm a^{-2}$ is always a quadratic residue $(\bmod p)$. It follows from (7.6) that the quadratic character of $u \,(\bmod \lambda)$ is an invariant of the strong equivalence class of $\begin{pmatrix} \bar{1} \\ \lambda^r u \end{pmatrix}$, and is therefore an isomorphism invariant of M. This argument, together with the discussion in the preceding paragraph, shows that no two of the lattices listed in (c) and (d) can be isomorphic.

To complete the proof of the theorem, we must show that a given lattice M with extension class $\begin{pmatrix} \bar{1} \\ \lambda^r u \end{pmatrix}$, where $1 \leqq r \leqq p-2$ and $u \in u(\bar{E})$, is isomorphic to one of the lattices in (c) and (d). Choosing $a = 1$, $b = 0$, $d = 1$ in (7.5'), we see that we can change

$\lambda^r u$ modulo λ^{p-1} without affecting the strong equivalence class of $\begin{pmatrix} \bar{1} \\ \lambda^r u \end{pmatrix}$. Now suppose that $u \equiv \pm q^2 \pmod{\lambda}$, where $q \in Z$; we may choose $\rho \in u(R)$, $s \in u(S)$, such that $\rho \equiv s \equiv q^{-1} \pmod{\lambda}$. There exists an $f \in \mathrm{Aut}(Z \oplus E)$, given as in (7.4), with $\varphi_2(d) = \rho$ and $\det f_1 = \pm 1$. Therefore $ad \equiv \pm 1 \pmod{\lambda}$, and so $a \equiv \pm q \pmod{p}$. Thus (7.6) yields

$$u' \equiv (\pm a^{-2})(\pm q^2) \equiv 1 \pmod{\lambda} .$$

Now choose $\tilde{u} \in \tilde{U}_{p-1-r}$ so that $\tilde{u}$ and u' have the same image in U_{p-1-r}, so $\tilde{u} \equiv \alpha u' \pmod{\lambda^{p-1}}$ for some $\alpha \in u(R)$. Then $\alpha \equiv 1 \pmod{\lambda}$, since $u' \equiv \tilde{u} \equiv 1 \pmod{\lambda}$. It follows from (7.5) that $\alpha = \varphi_2(d)$ for some $d \in u(E)$. Then $d \cdot \lambda^r u' \equiv \lambda^r \tilde{u} \pmod{\lambda^{p-1}}$, which shows that

$$\begin{pmatrix} \bar{1} \\ \lambda^r u \end{pmatrix} \approx \begin{pmatrix} \bar{1} \\ \lambda^r u' \end{pmatrix} \approx \begin{pmatrix} \bar{1} \\ \lambda^r \tilde{u} \end{pmatrix} ,$$

as desired. On the other hand, when $p \equiv 1 \pmod{4}$ and $u \pmod{\lambda}$ is not a square in $u(\bar{Z})$, then $u \equiv n_0 q^2 \pmod{\lambda}$ for some $q \in Z$. The above reasoning shows that

$$\begin{pmatrix} \bar{1} \\ \lambda^r u \end{pmatrix} \approx \begin{pmatrix} \bar{1} \\ \lambda^r \tilde{u} n_0 \end{pmatrix} ,$$

so M is isomorphic to a lattice of type (d). This completes the proof of the theorem.

COROLLARY 7.7. *The number of isomorphism classes of indecomposable ZG-lattices equals*

$$1 + 2h_R + 2h_S + h_R h_S(3N_1 + |U_p| + \varepsilon_p(N_1 - |U_{p-1}|)) ,$$

where

$$N_1 = \sum_{r=0}^{p-2} |U_{p-1-r}| ,$$

and $\varepsilon_p = 2$ *if* $p \equiv 1 \pmod{4}$, $\varepsilon_p = 1$ *otherwise. If* p *is a regular odd prime (or if* $p = 2$*), then* $|U_m| = p^{[(m-2)/2]}$ *for* $0 \leqq m \leqq p-1$*, where the greatest integer function is interpreted as* 0 *if* $m < 2$*. Further,* $|U_p| = |U_{p-1}|$ *if* p *is regular or properly irregular; in the latter case,* $|U_m| = p^{g(m)}$ *where* g *is given by* (6.3).

Proof. In (7.3) there are $1 + 2h_R + 2h_S$ lattices of type (a), and $h_R h_S N_1$ lattices for each of types (e) and (f). Further, there are $h_R h_S(N_1 + |U_p|)$ lattices of type (b), and $\varepsilon_p h_R h_S(N_1 - |U_{p-1}|)$ of types (c) and (d). This gives the desired result.

We note that for $p = 2, 3, 5$, the number of indecomposable ZG-lattices equals 9, 13, 40, respectively.

We are now ready to give a full set of isomorphism invariants for a direct sum M of indecomposable lattices chosen from the list in (7.3). Since the Krull-Schmidt-Azumaya Theorem holds for Z_pG-lattices, it is clear that the number of summands in the genus of each of the $4p + 1$ types in (7.2) must be an invariant. This gives us a set of $4p + 1$ nonnegative integers, which are precisely the genus invariants of M. Furthermore, the ideal class of the product of all R-ideals $\mathfrak{b}$ occurring in the various summands must be an isomorphism invariant of M. Likewise, the ideal class of the product of all S-ideals $\mathfrak{c}$ which occur is another invariant.

Now let M be a direct sum of indecomposable ZG-lattices chosen from the list (a)-(f) in (7.3). For each summand of type (b)-(f), the symbol u or un_0 occurring therein may be viewed as an element of $u(\bar{E})$. We may then form the product $u_0(M)$ of all u's and un_0's which occur in the summands of M of types (b)-(f); if there are no such summands, we set $u_0(M) = 1$. Let $r_1(M)$ be the largest exponent r which occurs in any type (b) summand, and let $r_2(M)$ be the largest exponent r among all summands of types (c), (d), (e), and (f). (Choose $r_1(M) = p$ if M has no summand of type (b), and choose $r_2(M) = p - 1$ if M has no summands of types (c)-(f).) The main result of this article is as follows:

THEOREM 7.8. *Let M be a direct sum of indecomposable ZG-lattices, which we may assume are of the types listed in* (7.3). *In terms of the above notation, a full set of isomorphism invariants of M consists of*:

(i) *The $4p + 1$ genus invariants of M,*

(ii) *The R- and S-ideal classes associated with M,*

(iii) *If M has no summand of types $\mathfrak{b}$, $E(\mathfrak{b})$, $\mathfrak{c}$, $(Z, \mathfrak{c}; 1)$, and if $r_1(M) \leqq r_2(M)$, the isomorphism invariant given by the image of $u_0(M)$ in U_{p-1-r_2}, whereas if $r_1(M) > r_2(M)$, the invariant given by the image of $u_0(M)$ in U_{p-r_1}, and*

(iv) *If $p \equiv 1 \pmod 4$, and if M has no summand of types Z, $E(\mathfrak{b})$, $(Z, \mathfrak{c}; 1)$, $(E(\mathfrak{b}), \mathfrak{c}; \lambda^r u)$ or $(Z \oplus \mathfrak{b}, \mathfrak{c}; 1 \oplus \lambda^r u)$, the isomorphism invariant given by the quadratic character of the image of $u_0(M)$ in $u(\bar{Z})$.*

Proof. Step 1. We have already remarked that the isomorphism class of M determines the invariants listed in (i) and (ii), and that the only remaining invariants needed to determine M up to isomorphism are those which characterize the strong equivalence class of M. In this step (the hardest of all), we suppose that M is as in

(iii), and proceed to show that the proposed invariant is indeed an isomorphism invariant of M. Define $M^* = M/L_0$ as in the proof of (7.3); then M^* must be a direct sum of lattices in the genus of $(R, S; \lambda^r)$ for various r, because of the hypotheses on M. It follows from § 6 that the image of $u_0(M)$ in U_m is an isomorphism invariant of M^* (and hence also of M), where

$$m = p - 1 - \text{Max}\{r\} = p - 1 - \text{Max}\{r_1, r_2\}\,.$$

Thus we see that if $r_1 \leqq r_2$, then the image of $u_0(M)$ in U_{p-1-r_2} is an isomorphism invariant of M, as claimed.

Now let $r_1 > r_2$, and suppose M is as in (iii), so M is a direct sum of lattices in the genera of

$$(7.9)\quad Z,\ (Z \oplus R, S; \lambda^r),\ (R, S; \lambda^r),\ (Z \oplus E, S; 1 \oplus \lambda^r),\ (E, S; \lambda^r)$$

for various r's. Viewing M as an extension of a free S-lattice by a direct sum of copies of Z, R, and E, the extension class ξ_M of M has the form

$$\left[\begin{array}{cccc} 0 & 0 & 0 & 0 \\ I & 0 & 0 & 0 \\ 0 & 0 & I & 0 \\ \hline D_1 & 0 & 0 & 0 \\ 0 & D_2 & 0 & 0 \\ \hline 0 & 0 & D_3 & 0 \\ 0 & 0 & 0 & D_4 \end{array}\right].$$

The top row corresponds to summands of type Z; each D_i is a diagonal matrix with diagonal entries of the form $\lambda^r u$ or $\lambda^r u n_0$; the four columns correspond (respectively) to the last four types of summands listed in (7.9). Changing notation slightly, we may then write

$$\xi_M = \begin{bmatrix} H & 0 & 0 \\ 0 & I & 0 \\ D_{12} & 0 & 0 \\ 0 & D_3 & 0 \\ 0 & 0 & D_4 \end{bmatrix},\quad H = \begin{bmatrix} 0 & 0 \\ I & 0 \end{bmatrix},\quad D_{12} = \begin{bmatrix} D_1 & 0 \\ 0 & D_2 \end{bmatrix}.$$

We must show that the image of $u_0(M)$ in U_{p-r_2} is an invariant of the strong equivalence class of ξ_M.

The endomorphism ring of $Z^{(a)} \oplus R^{(b)} \oplus E^{(c)}$ consists of all matrices

$$f = \begin{bmatrix} A_{11} & 0 & A_{13} \\ 0 & A_{22} & A_{23} \\ \Phi(x)A_{31} & \lambda A_{32} & A_{33} \end{bmatrix},$$

where the rows have entries in Z, R, and E, respectively. As in the proof of (7.3), f is an automorphism if and only if

$$(7.10) \qquad \begin{bmatrix} A_{11} & A_{13} \\ p\varphi_1(A_{31}) & \varphi_1(A_{33}) \end{bmatrix} \in GL(Z), \quad \begin{bmatrix} A_{22} & A_{23} \\ \lambda\varphi_2(A_{32}) & \varphi_2(A_{33}) \end{bmatrix} \in GL(R),$$

where the φ_i are induced from those in (7.5).

Now suppose that $\xi_M \approx \xi_{M'}$, where $\xi_{M'}$ has the same form as ξ_M, but with diagonal entries $\lambda^r u'$ or $\lambda^r u' n_0$. Then we obtain

$$\begin{bmatrix} B_{11} & B_{12} & 0 & B_{14} & B_{15} \\ B_{21} & B_{22} & 0 & B_{24} & B_{25} \\ 0 & 0 & B_{33} & B_{34} & B_{35} \\ \Phi(x)B_{41} & \Phi(x)B_{42} & \lambda B_{43} & B_{44} & B_{45} \\ \Phi(x)B_{51} & \Phi(x)B_{52} & \lambda B_{53} & B_{54} & B_{55} \end{bmatrix} \begin{bmatrix} H & 0 & 0 \\ 0 & I & 0 \\ D_{12} & 0 & 0 \\ 0 & D_3 & 0 \\ 0 & 0 & D_4 \end{bmatrix}$$

$$= \begin{bmatrix} H & 0 & 0 \\ 0 & I & 0 \\ D'_{12} & 0 & 0 \\ 0 & D'_3 & 0 \\ 0 & 0 & D'_4 \end{bmatrix} \begin{bmatrix} S_{11} & S_{12} & S_{13} \\ S_{21} & S_{22} & S_{23} \\ S_{31} & S_{32} & S_{33} \end{bmatrix},$$

where $[S_{ij}]^{3\times 3} \in GL(S)$. The (4, 1) block in the left hand product equals $\Phi(x)B_{41}H + \lambda B_{43}D_{12}$. However, $\Phi(x)$ is a multiple of λ^{p-1} in $\bar{E}$, and each diagonal entry of D_{12} is of the form $\lambda^r u$ for some $r \leqq r_2$. We may therefore write this (4, 1) block as

$$(\lambda^{p-1-r_2}C_{41} + \lambda B_{43})D_{12}$$

for some C_{41}. The same procedure can be carried out for the blocks in positions (5, 1), (4, 2), and (4, 3). Setting $k = p - 1 - r_2$ for brevity, we obtain

$$(7.11) \qquad \begin{bmatrix} B_{33} & B_{34} & B_{35} \\ \lambda^k C_{41} + \lambda B_{43} & \lambda^k C_{42} + B_{44} & B_{45} \\ \lambda^k C_{51} + \lambda B_{53} & \lambda^k C_{52} + B_{54} & B_{55} \end{bmatrix} \cdot \operatorname{diag}(D_{12}, D_3, D_4)$$

$$= \operatorname{diag}(D'_{12}, D'_3, D'_4) \cdot [S_{ij}]^{3\times 3}.$$

Now $r_1 > r_2 \geqq 0$ gives $r_1 \geqq 1$; thus for each $\rho \in \bar{R}$, the product $\lambda^{r_1}\rho$ is unambiguously defined inside $\bar{E}$. The method of proof of (5.10) then shows that

$$\lambda^{r_1}\beta u_0(M) = \lambda^{r_1}\sigma u_0(M') \text{ in } \bar{E} ,$$

where β is the determinant of the first matrix appearing in (7.11), and $\sigma = \det[S_{ij}] \in u(S)$. However, $r_1 + k = r_1 + p - 1 - r_2 \geqq p$ so $\lambda^{r_1+k} = 0$ in $\bar{E}$. Therefore $\lambda^{r_1}\beta = \lambda^{r_1}\beta^*$, where

$$\beta^* = \det\begin{bmatrix} B_{33} & B_{34} & B_{35} \\ \varphi_2(\lambda B_{43}) & \varphi_2(B_{44}) & \varphi_2(B_{45}) \\ \varphi_2(\lambda B_{53}) & \varphi_2(B_{54}) & \varphi_2(B_{55}) \end{bmatrix} \in u(R) .$$

This shows that $\beta^* u_0(M) = \sigma u_0(M')$ in $\bar{Z}[\lambda]/(\lambda^{p-r_1})$, so therefore $u_0(M)$ and $u_0(M')$ have the same image in U_{p-r_1}, as desired. Thus when $r_1 > r_2$, the image of $u_0(M)$ in U_{p-r_1} is an isomorphism invariant of M.

Step 2. Suppose next that the hypotheses of (iv) are satisfied. Then M is a direct sum of lattices in the genera of

$$R,\ S,\ (R, S; \lambda^r),\ (Z \oplus E, S; 1 \oplus \lambda^r) , \tag{7.12}$$

and we may write the extension class ξ_M of M in the form

$$\xi_M = \begin{bmatrix} 0 & I \\ H & 0 \\ 0 & D \end{bmatrix} ,$$

with D a diagonal matrix with entries $\lambda^r u$. The first column corresponds to summands of the first three types in (7.12), and the second column to the last type. If $\xi_{M'}$ has the same form as ξ_M, then the strong equivalence $\xi_M \approx \xi_{M'}$ yields an equation

$$\begin{bmatrix} A_{11} & 0 & A_{13} \\ 0 & A_{22} & A_{23} \\ \Phi(x)A_{31} & \lambda A_{32} & A_{33} \end{bmatrix}\begin{bmatrix} 0 & I \\ H & 0 \\ 0 & D \end{bmatrix} = \begin{bmatrix} 0 & I \\ H' & 0 \\ 0 & D' \end{bmatrix}\begin{bmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{bmatrix} .$$

But $A_{13}D = 0$ over $\bar{Z}$, since every diagonal entry of D is a multiple of λ, and $\lambda\bar{Z} = 0$. Thus we obtain

$$A_{11} = S_{22} \text{ over } \bar{Z},\ \Phi(x)A_{31} + A_{33}D = D'S_{22} .$$

Consequently $|A_{11}| = |S_{22}|$ in $\bar{Z}$, and

$$\lambda^{p-2}|A_{33}|u_0(M) \equiv \lambda^{p-2}|S_{22}|u_0(M') \pmod{\lambda^{p-1}} .$$

On the other hand, $|A_{11}|\,|\varphi_1(A_{33})| \equiv \pm 1 \pmod{p}$ by (7.10), so we have

$$u_0(M) \equiv \pm\,|A_{11}|^2 u_0(M') \pmod{\lambda}\,.$$

This proves that in case (iv), the quadratic character of the image of $u_0(M)$ in $u(\bar{Z})$ is an isomorphism invariant of M. (This argument is an obvious extension of that given in the proof of (7.3).)

Step 3. To complete the proof, we must show that the set of invariants (i)-(iv) do indeed determine M up to isomorphism. We shall accomplish this by repeated use of the Absorption and Exchange Formulas of § 2, and for this purpose we need a collection of short exact sequences. For brevity of notation we omit the 0's at either end of such sequences, agreeing that the first arrow is assumed monic, the second arrow epic.

We have already pointed out that every element in a factor group U_k can be represented by an element u in E or R, such that $u \equiv 1 \pmod{\lambda}$. For such u, we have $uZ = Z$, and thus

$$R/uR \cong (E/Z)/u(E/Z) = (E/Z)/(uE/Z) \cong E/uE\,. \tag{7.13}$$

Likewise, $\mathfrak{b}/u\mathfrak{b} \cong E(\mathfrak{b}')/uE(\mathfrak{b}')$ always. Further, for $u \equiv 1 \pmod{\lambda}$ there are exact sequences

$$R \longrightarrow R \longrightarrow R/uR,\ (R, S; \lambda^r) \longrightarrow (R, S; \lambda^r u) \longrightarrow R/uR\,,$$

$$(Z \oplus E, S; 1 \oplus \lambda^r) \longrightarrow (Z \oplus E, S; 1 \oplus \lambda^r u \longrightarrow E/uE\,,$$

and so on. If M is a direct sum of indecomposable lattices of the types listed in (7.3), it thus follows from the existence of such exact sequences that we may concentrate all of the u's in any preassigned summand of M, without affecting the isomorphism class of M. This means that we can set all but one of the u's equal to 1, and replace the remaining u by the product of all of the original u's. (Caution: this does *not* enable us to move the n_0's occuring in type (d) summands!) Furthermore, if either $\mathfrak{b}$ or $E(\mathfrak{b})$ occurs as summand, then the Absorption Formula permits us to make *every* u equal to 1, without affecting the isomorphism class of M.

Next, there is a surjection $S \to \bar{E}$, so for each $u \in u(\bar{E})$ we can find an element $v \in S$ such that $\bar{v} = u^{-1}$ in $\bar{E}$; then v acts on $\bar{E}$ as multiplication by u^{-1}. From the commutative diagram

$$\begin{array}{ccccc} R & \longrightarrow & (R, S; \lambda^r u) & \longrightarrow & S \\ {\scriptstyle 1}\uparrow & & \uparrow & & \uparrow{\scriptstyle v} \\ R & \longrightarrow & (R, S; \lambda^r) & \longrightarrow & S \end{array}$$

we obtain an E-exact sequence

$$(R, S; \lambda^r) \longrightarrow (R, S; \lambda^r u) \longrightarrow S/vS .$$

Likewise, there are exact sequences

$$S \longrightarrow S \longrightarrow S/vS, \ (Z, S; 1) \longrightarrow (Z, S; 1) \longrightarrow S/vS ,$$

$$(Z \oplus E, S; 1 \oplus \lambda^r) \longrightarrow (Z \oplus E, S; u \oplus \lambda^r u) \longrightarrow S/vS ,$$

and so on. Note also that

$$(Z \oplus E, S; v \oplus \lambda^r v) \cong (Z \oplus E, S; 1 \oplus \lambda^r v)$$

whenever $v \equiv 1 \pmod{\lambda}$. It thus follows (by the Absorption Formula) that if either $\mathfrak{c}$ or $(Z, \mathfrak{c}; 1)$ is a summand of M, then we can replace u by 1 in every summand of M in which u's occur, without affecting the isomorphism class of M. This completes the proof that if M has any summand of the types in (iii), then we can eliminate all of the u's. On the other hand, if M has no such summand, then by Step 1 the image of $u_0(M)$ in either U_{p-1-r_2} or U_{p-r_1} is an isomorphism invariant of M.

Step 4. Suppose finally that $p \equiv 1 \pmod 4$. There are exact sequences

$$Z \longrightarrow Z \longrightarrow Z/n_0Z, \ (Z, S; 1) \longrightarrow (Z, S; 1) \longrightarrow Z/n_0Z ,$$

$$(7.14) \quad (Z \oplus R, S; 1 \oplus \lambda^r u) \longrightarrow (Z \oplus R, S; n_0 \oplus \lambda^r u) \longrightarrow Z/n_0Z .$$

Choose $v_0 \in u(S)$ with $v_0 = n_0$ in $u(\bar{Z})$; then u and uv_0^{-1} have the same image in U_{p-1-r} for each r, and therefore

$$\begin{aligned}(Z \oplus R, S; 1 \oplus \lambda^r u) &\cong (Z \oplus R, S; 1 \oplus \lambda^r u v_0^{-1}) \cong (Z \oplus R, S; v_0 \oplus \lambda^r u) \\ &\cong (Z \oplus R, S; n_0 \oplus \lambda^r u) .\end{aligned}$$

Thus (7.14) yields an exact sequence

$$(Z \oplus R, S; 1 \oplus \lambda^r u) \longrightarrow (Z \oplus R, S; 1 \oplus \lambda^r u) \longrightarrow Z/n_0Z .$$

Now let $u \equiv 1 \pmod{\lambda}$, and let us denote by $[un_0]$ an element $u_1 \in u(\bar{E})$ such that $u_1 \equiv 1 \pmod{\lambda}$ and $u_1 = un_0$ in U_{p-1-r} (for some given r). Then we have

$$\begin{aligned}(Z \oplus E, S; n_0^{-1} \oplus \lambda^r u_1) &\cong (Z \oplus E, S; 1 \oplus \lambda^r u_1 v_0) \\ &\cong (Z \oplus E, S; 1 \oplus \lambda^r u n_0) ;\end{aligned}$$

the second isomorphism is valid because u_1v_0 and un_0 have the same image in $u(\bar{Z})$, as well as the same image in U_{p-1-r}. Thus the exact sequence

$$(Z \oplus E, S; n_0^{-1} \oplus \lambda^r u_1) \longrightarrow (Z \oplus E, S; 1 \oplus \lambda^r u_1) \longrightarrow Z/n_0 Z$$

may be rewritten as

$$(7.15) \quad (Z \oplus E, S; 1 \oplus \lambda^r u n_0) \longrightarrow (Z \oplus E, S; 1 \oplus \lambda^r [u n_0]) \longrightarrow Z/n_0 Z .$$

Finally, there are exact sequences

$$(E, S; \lambda^r u) \longrightarrow (E, S; \lambda^r u n_0) \longrightarrow E/n_0 E ,$$
$$(Z \oplus E, S; 1 \oplus \lambda^r u) \longrightarrow (Z \oplus E, S; 1 \oplus \lambda^r u n_0) \longrightarrow E/n_0 E .$$

It now follows from (7.15), and the other sequences listed above, that if M contains any summand of the types listed in (iv), then the isomorphism class of M is unchanged if we replace un_0 by $[un_0]$ in every type (d) summand of M. In any case, if both u and u' are congruent to $1 \pmod{\lambda}$, then (7.15) gives

$$(Z \oplus E, S; 1 \oplus \lambda^r u n_0) \oplus (Z \oplus E, S; 1 \oplus \lambda^s u' n_0)$$
$$\cong (Z \oplus E, S; 1 \oplus \lambda^r [u n_0]) \oplus (Z \oplus E, S; 1 \oplus \lambda^s [u' n_0]) .$$

Hence, we can always eliminate any even number of type (d) summands of M. Further, if M contains no summands of the types listed in (iv), then we have shown in Step 2 that the quadratic character of the image of $u_0(M)$ in $u(\bar{Z})$ is an isomorphism invariant of M.

In view of the various changes which we have described in Steps 3 and 4, it is now clear that the invariants listed in (i)-(iv) completely determine the isomorphism class of M. This completes the proof of the theorem.

To conclude, we remark that many of the above results can be generalized to extensions of R_j-lattices by a direct sum of locally free lattices over several orders which are factor rings of $Z[x]/(x^{p^{j-1}}-1)$. In particular, we can classify all Λ_κ-lattices M for which QM is a direct sum of copies of Z, R_i, and R_j, where $1 \leqq i < j \leqq \kappa$. It is known (see [1]) that there are only finitely many isomorphism classes of indecomposable lattices of this type. However, this gives only a partial classification of the integral representations of a cyclic group of order p^3, since for G cyclic of order p^2, there exist ZG-lattices which are not direct sums of locally free lattices of the types just mentioned.

Even for G cyclic of order p^2, a further question remains: given a ZG-lattice M, how can one calculate the isomorphism invariants of M intrinsically, without first expressing M as a direct sum of indecomposable lattices? Such a calculation would undoubtedly help to clarify the structure of M.

REFERENCES

1. S. D. Berman and P. M. Gudivok, *Indecomposable representations of finite groups over the ring of p-adic integers*, Izv. Akad. Nauk, SSSR Ser. Mat., **28** (1964), 875-910; English transl., Amer. Math. Soc. Transl. (2) **50** (1966), 77-113.
2. Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.
3. H. Cartan and S. Eilenberg, *Homological Algebra*, Princeton University Press, Princeton, NJ, 1956.
4. 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.
5. F. E. Diederichsen, *Über die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetischer Aquivalenz*, Abh. Math. Sem. Univ. Hamburg, **13** (1940), 357-412.
6. S. Galovich, *The class group of a cyclic p-group*, J. Algebra, **30** (1974), 368-387.
7. A. Heller and I. Reiner, *Representations of cyclic groups in rings of integers. I. II*, Ann. of Math., (2) **76** (1962), 73-92; (2) **77** (1963), 318-328.
8. H. Jacobinski, *Genera and decompositions of lattices over orders*, Acta Math., **121** (1968), 1-29.
9. M. A. Kervaire and M. P. Murthy, *On the projective class group of cyclic groups of prime power order*, Comment. Math. Helvetici, **52** (1977), 415-452.
10. I. Reiner, *Integral representations of cyclic groups of prime order*, Proc. Amer. Math. Soc., **8** (1957), 142-146.
10a. ———, *A survey of integral representation theory*, Bull. Amer. Math. Soc., **76** (1970), 159-227.
11. I. Reiner, *Maximal Orders*, Academic Press, London, 1975.
12. ———, *Integral representations of cyclic groups of order p^2*, Proc. Amer. Math. Soc., **58** (1976), 8-12.
13. ———, *Indecomposable integral representations of cyclic p-groups*, Proc. Philidelphia Conference 1976, Dekker Lecture Notes **37** (1977), 425-445.
14. A. V. Roiter, *On representations of the cyclic group of fourth order by integral matrices*, Vestnik Leningrad. Univ., **15** (1960), no. 19, 65-74. (Russian)
15. ———, *On integral representations belonging to a genus*, Izv. Akad. Nauk, SSSR, Ser. Mat., **30** (1966), 1315-1324; English transl. Amer. Math. Soc. Transl. (2) **71** (1968), 49-59.
16. J. J. Rotman, *Notes on homological algebra*, van Nostrand Reinhold, New York, 1970.
17. A. Troy, *Integral representations of cyclic groups of order p^2*, Ph. D. Thesis, University of Illinois, Urbana, IL., 1961.
18. S. Ullom, *Fine structure of class groups of cyclic p-groups*, J. Algebra, **48** (1977).
19. ———, *Class groups of cyclotomic fields and group rings*, J. London Math. Soc., (to appear).

Received January 4, 1977 and in revised form November 10, 1977. This research was partially supported by the National Science Foundation.

UNIVERSITY OF ILLINOIS
URBANA, IL 61801