ON THE CLASS NUMBER OF REPRESENTATIONS OF AN ORDER

IRVING REINER

1. Introduction. We shall use the following notation throughout:

R = Dedekind ring **(5)**.
$\mathfrak{u}$ = multiplicative group of units in R.
h = class number of R.
K = quotient field of R.
p = prime ideal in R.
R_p = ring of p-adic integers in K.

We assume that h is finite, and that for each prime ideal p, the index $(R:p)$ is finite.

Let A be a finite-dimensional separable algebra over K, with an identity element e **(4**, p. 115**)**. Let G be an R-order in A, that is, G is a subring of A satisfying

(i) $e \in G$,
(ii) G contains a K-basis of A,
(iii) G is a finitely-generated R-module.

By a G-module we shall mean a left G-module which is a finitely-generated torsion-free R-module, on which e acts as identity operator. An A-module is defined analogously, replacing R by K. We shall assume, unless otherwise stated, that K is a splitting field for A; thus, the only possible A-endomorphisms of an irreducible A-module X are the scalar multiplications $x \to \alpha x$, $x \in X$, where $\alpha \in K$.

As in **(3)**, we may form the non-zero ideal $\mathfrak{g} \subset R$, defined as the intersection of the ideals which annihilate the one-dimensional cohomology groups $H(G, T)$, where T ranges over the set of two-sided G-modules. (In the special case where $G = R(\Pi)$ is the group ring of a finite group Π, the ideal $\mathfrak{g}$ is the principal ideal generated by the group order $(\Pi : 1)$.) Let $P = \{p_1, \ldots, p_l\}$ be the set of distinct prime divisors of $\mathfrak{g}$, and set

$$\mathfrak{g} = \prod_{p \in P} p^{\gamma(p)}. \tag{1}$$

For any G-module M, let KM be the A-module which consists of the K-linear combinations of the elements of M. If we set $A_p = R_pG$, we may likewise define the A_p-module $M_p = R_pM$. Two G-modules M and N are said to be in the same *genus* (notation: $M \vee N$) if and only if for each p, the modules

Received June 12, 1958. This research was supported in part by the Office of Naval Research.

https://doi.org/10.4153/CJM-1959-061-5 Published online by Cambridge University Press

M_p and N_p are A_p-isomorphic. As is shown in **(7)**, $M \vee N$ if and only if $KM \cong KN$ and $M_p \cong N_p$ for each $p \in P$.

For any A-module L', let $S(L')$ be the collection of G-modules L for which $KL \cong L'$. Suppose that $S(L')$ splits into r_g genera, and into r_G classes under G-isomorphism. As is shown in **(6**; **7**; and **9)**, both r_g and r_G are finite. The purpose of this paper is to consider the relation between r_g and r_G. For the special case where L' is irreducible, Maranda **(7)** has shown that $r_G = hr_g$. We shall restrict ourselves to the case where the irreducible constituents of L' are distinct from one another. If L' has k distinct irreducible constituents, we shall prove

$$r_G \geqslant h^k r_g. \tag{2}$$

Further, we shall show that equality holds provided that

(3) For each $\alpha \in R$ such that $(\alpha) + \mathfrak{g} = R$, there exists $\beta \in \mathfrak{u}$ for which $\beta \equiv \alpha \pmod{\mathfrak{g}^{k-1}}$.

Finally, we shall obtain formulas for r_g and r_G in the special case where $k = 2$. These formulas will show that if condition (3) fails, then r_G may exceed $h^2 r_g$ for this case.

2. Binding homomorphisms. In this section, we shall drop the hypothesis that K is a splitting field for the algebra A. Let L be a G-module which contains a submodule M, and assume that M is an R-direct summand of L. Define $N = L/M$ to be the factor G-module. Every element of L is then uniquely representable as an ordered pair (n, m), $n \in N$, $m \in M$, where the structure of L as R-module is given by

$$(n, m) + (n', m') = (n + n', m + m'), \qquad \alpha(n, m) = (\alpha n, \alpha m), \tag{4}$$

for $n, n' \in N$, $m, m' \in M, \alpha \in R$. Further, the action of G on L is given by

$$g(n, m) = (gn, \Lambda_g(n) + gm), \qquad g \in G, \text{ where } \Lambda_g \in \operatorname{Hom}_R(N, M). \tag{5}$$

Let $\Lambda : G \to \operatorname{Hom}_R(N, M)$ be the R-homomorphism defined by $g \to \Lambda_g$. The condition $(gh)(n, m) = g(h(n, m))$ is equivalent to

$$\Lambda_{gh}(n) = g\Lambda_h(n) + \Lambda_g(hn), \qquad g, h \in G, n \in N. \tag{6}$$

Call $\Lambda \in \operatorname{Hom}_R(G, \operatorname{Hom}_R(N, M))$ a *binding homomorphism* if (**6**) holds, and let $B(N, M)$ be the R-module consisting of all binding homomorphisms relative to N, M. The R-G-module L is then completely determined by equations (4) and (5), once an element $\Lambda \in B(N, M)$ is fixed. Let us denote this module L by $(N, M; \Lambda)$.

It is convenient to turn $\operatorname{Hom}_R(N, M)$ into a two-sided G-module T by defining

$$(gt)(n) = g(t(n)), \quad (tg)n = t(gn), \quad g \in G, n \in N, t \in \operatorname{Hom}_R(N, M).$$

We may then characterize $B(N, M)$ as the set of all $\Lambda \in \operatorname{Hom}_R(G, T)$ for which

$$\Lambda_{gh} = g\Lambda_h + \Lambda_g h, \qquad g, h \in G. \tag{7}$$

https://doi.org/10.4153/CJM-1959-061-5 Published online by Cambridge University Press

Now fix $t \in T$, and define $\Lambda \in \mathrm{Hom}_R (G, T)$ by

$$\Lambda_g = gt - tg, \qquad g \in G.$$

We find readily that $\Lambda \in B(N, M)$. Let $B' (N, M)$ be the R-module consisting of all the binding homomorphisms so obtained by letting t range over all elements of T. Define the R-module

$$C(N, M) = B(N, M)/B'(N, M).$$

From **(9)** we know that $C(N, M)$ contains only finitely many elements. Furthermore, from the definition of the ideal $\mathfrak{g}$, we have

$$\mathfrak{g}\cdot B(N, M) \subset B'(N, M)$$

for any N, M. Finally, if $[\Lambda]$ denotes the class $\Lambda + B'(N, M)$ of the element $\Lambda \in B(N, M)$, then we have:

$$[\Lambda] = [\Lambda'] \Rightarrow (N, M; \Lambda) \cong (N, M; \Lambda').$$

In fact, if $t \in T$ is such that $\Lambda_g' - \Lambda_g = gt - tg$, $g \in G$, then the map $(n, m) \to (n, m - tn)$ gives the desired isomorphism.

In the above discussion, replace R by R_p. If L^* is an A_p-module which contains a submodule M^* as R_p-direct summand, then $L^* = (N^*, M^*; \Lambda^*)$, where $N^* = L^*/M^*$, and where

$$\Lambda^* : A_p \to \mathrm{Hom}_{R_p} (N^*, M^*).$$

is an R_p-homomorphism satisfying $\Lambda^*_{xy} = x\Lambda^*_y + \Lambda^*_x y$, $x, y \in A_p$. Define $B(N^*,M^*)$, $B'(N^*, M^*)$ and $C(N^*, M^*)$ as above. For $\Lambda^* \in B(N^*, M^*)$, again let $[\Lambda^*] = \Lambda^* + B'(N^*, M^*)$. If $\gamma(p)$ is defined as in (1), we have

$$\pi^{\gamma(p)}B(N^*, M^*) \subset B'(N^*, M^*) \tag{8}$$

where π is an element of p such that $\pi \notin p^2$.

Now let N, M be G-modules, and let N_p, M_p be the corresponding A_p-modules. There is a natural isomorphism of $B(N, M)$ into $B(N_p, M_p)$ which may be described as follows: for each $\Lambda \in B(N, M)$ and each $g \in G$, the map $\Lambda_g \in \mathrm{Hom}_R(N, M)$ may be extended in a unique manner to an element of $\mathrm{Hom}_{R_p}(N_p, M_p)$; we may then define Λ_x for each $x \in A_p$ by linearity. In this way, Λ is extended in a unique manner to an element $\Lambda^p \in B(N_p, M_p)$. The map $\Lambda \to \Lambda^p$ carries $B'(N, M)$ into $B'(N_p, M_p)$, and so induces an R-homomorphism of $C(N, M)$ into $C(N_p, M_p)$.

We may now define an R-homomorphism

$$\phi : \quad C(N, M) \to \sum_{p \in P} C(N_p, M_p)$$

by means of

$$\phi[\Lambda] = ([\Lambda^{p_1}], \ldots, [\Lambda^{p_l}]).$$

https://doi.org/10.4153/CJM-1959-061-5 Published online by Cambridge University Press

From **(8)**, we know that ϕ has kernel 0. We shall in fact show that ϕ is an isomorphism "onto."

THEOREM 1.

$$C(N, M) \cong \sum_{p \in P} C(N_p, M_p).$$

Remark. A slightly different version of this was first proved by deLeeuw **(1)**. We shall not use the results of **(8)**, but instead shall give a self-contained proof of the theorem.

Proof. We show firstly that the ϕ is an "onto" mapping. For each $p \in P$ suppose an element $\Omega^p \in B(N_p, M_p)$ chosen. We must prove the existence of an element $\Lambda \in B(N, M)$ such that $[\Lambda^p] = [\Omega^p], p \in P$. Let $T = \mathrm{Hom}_R(N, M)$, and let us set

$$T_p = \mathrm{Hom}_{R_p}(N_p, M_p) = R_p \, \mathrm{Hom}_R\,(N, M) = R_p T$$

for each prime ideal p.

For each $p \in P$, we may choose an element $\pi \in p$ such that $\pi \notin p^2$, and such that π does not lie in any other prime ideal in the set P. Set

$$a = \prod_{p \in P} \pi^{\gamma(p)};$$

then $a \in R$, and for each $p \in P$ we may write

$$a = \pi^{\gamma(p)} d_p, \qquad d_p \in R, \qquad d_p = \text{unit in } R_p.$$

Define the integral ideal $\mathfrak{b}$ by

$$(a) = \mathfrak{b} \cdot \prod_{p \in P} p^{\gamma(p)}.$$

Then $\mathfrak{b}$ is not a multiple of any of the prime ideals in P.

We now make use of equation (8) to deduce that for each $p \in P$, there exists an element $u^p \in T_p$ such that

$$a \cdot \Omega_g^p = g u^p - u^p g, \qquad g \in G.$$

On the other hand, T is a finitely-generated R-module, so there exist elements $t_1, \ldots, t_r \in T$ such that

$$T = Rt_1 + \ldots + Rt_r,$$

whence

$$T_p = R_p t_1 + \ldots + R_p t_r.$$

We may therefore write (for $p \in P$)

$$u^p = \sum_{i=1}^{r} \beta_i^p t_i, \qquad \beta_i^p \in R_p.$$

Let us now choose $\alpha_1, \ldots, \alpha_r \in R$ such that

$$\alpha_i \equiv \beta_i^p \pmod{\pi^{2\gamma(p)} R_p}, \qquad p \in P, \qquad \alpha_i \equiv 0 \pmod{\mathfrak{b}}.$$

Set

$$t = a^{-1} \sum_{i=1}^{r} \alpha_i t_i \in KT,$$

and define $\Lambda \in \mathrm{Hom}_R(G, KT)$ by

$$\Lambda_g = gt - tg, \qquad g \in G.$$

We shall show that this is the desired Λ, that is, $\Lambda \in B(N, M)$, and $[\Lambda^p] = [\Omega^p]$ for $p \in P$. For $p \in P$ we have

$$a(\Omega_g^p - \Lambda_g) = gv^p - v^p g, \qquad g \in G,$$

where

$$v^p = u^p - at = \sum_{i=1}^{r} (\beta_i^p - \alpha_i) t_i.$$

From the way in which the α_i were chosen, we may therefore write

$$v^p = \pi^{2\gamma(p)} d_p w^p,$$

where $w^p \in T_p$, and thus

$$\Omega_g^p - \Lambda_g = \pi^{\gamma(p)}(gw^p - w^p g), g \in G.$$

This proves that for each $p \in P$,

$$\Omega^p - \Lambda^p \in \pi^{\gamma(p)} B(N_p, M_p) \subset B'(N_p, M_p),$$

and shows incidentally that

$$\Lambda_g \in T_p, \qquad g \in G, \qquad p \in P. \tag{9}$$

On the other hand, we note that for each prime ideal $q \notin P$, the elements $a^{-1}\alpha_1, \ldots, a^{-1}\alpha_r$ all lie in R_q, and hence

$$\Lambda_g \in T_q, \qquad g \in G.$$

Coupled with (9), this implies that

$$\Lambda_g \in \bigcap_{q'} T_{q'}, \qquad g \in G,$$

where q' ranges over all prime ideals. The above intersection is precisely T, and so $\Lambda \in \mathrm{Hom}_R(G, T)$. That (7) holds follows at once from the definition of Λ; consequently, $\Lambda \in B(N, M)$. This completes the proof that ϕ is "onto."

In order to show that ϕ is an isomorphism, let $\Omega \in B(N, M)$ be such that $\Omega^p \in B'(N_p, M_p)$ for all $p \in P$; we must show that $\Omega \in B'(N, M)$. Since $\Omega^p \in B'(N_p, M_p)$, there exists for each $p \in P$ an element $u^p \in T_p$ such that

$$\Omega_g^p = gu^p - u^p g, \qquad g \in G.$$

By the preceding construction (with $a = 1$), there exists $\Lambda \in B'(N, M)$ (since now $t \in T$) such that

$$\Lambda_g^p \equiv \Omega_g^p \pmod{\pi^{\gamma(p)} T_p}, \qquad g \in G.$$

Therefore

$$\Lambda - \Omega \in \mathfrak{g}B(N, M) \subset B'(N, M),$$

which shows that $\Omega \in B'(N, M)$.

COROLLARY. *If N, N^*, M, M^* are G-modules such that $N \vee N^*$ and $M \vee M^*$, then $C(N, M) \cong C(N^*, M^*)$ as R-modules.*

More generally, let

$$L_1 \supset L_2 \supset \ldots \supset L_k \supset (0)$$

be a set of G-modules such that each is an R-direct summand of its predecessor. Define $N_i = L_i/L_{i+1}$ to be the factor G-module. Then as above, every element of L_1 is uniquely representable as an ordered k-tuple $(n_1, \ldots, n_k)$ $n_i \in N_i$, where

$$(n_1, \ldots, n_k) + (n_1', \ldots, n_k') = (n_1 + n_1', \ldots, n_k + n_k'),$$
$$\alpha(n_1, \ldots, n_k) = (\alpha n_1, \ldots, \alpha n_k)$$

for $n_i, n_i' \in N_i$, $\alpha \in R$. The action of G on L_1 is given by

$$g(n_1, \ldots, n_k) = (gn_1, gn_2 + \Lambda_g^{12} n_1, \ldots, gn_k + \Lambda_g^{1k} n_1 + \ldots + \Lambda_g^{k-1,k} n_{k-1}),$$

where each $\Lambda_g^{ij} \in \mathrm{Hom}_R(N_i, N_j)$, and where the R-homomorphisms Λ^{ij} : $g \to \Lambda_g^{ij}$ satisfy conditions analogous to (7). Let $B(N_1, \ldots, N_k)$ denote the set of systems $\{\Lambda^{ij}\}$ satisfying these conditions. We denote the module L_1 by the symbol $(N_1, \ldots, N_k; \{\Lambda^{ij}\})$.

3. Isomorphisms of modules. Throughout this section, we fix an A-module L' with a composition series.

$$L = L_1' \supset L_2' \supset \ldots \supset L_k' \supset (0),$$

and let $N_i' = L_i'/L_{i+1}'$. We assume here that N_i' and N_j' are not isomorphic for $i \neq j$, and further that K is a splitting field for A. For any $L \in S(L')$, the A-module KL will have a composition series

$$KL = L_1'' \supset L_2'' \supset \ldots \supset L_k'' \supset (0)$$

in which $L_i''/L_{i+1}'' \cong N_i'$. Setting $L_i = L_i'' \cap L$, we see that L_i is a G-submodule of L for which $KL_i = L_i''$. Furthermore, L_{i+1} is a pure R-submodule of L_i, and therefore (by **5**) is an R-direct summand of L_i. Put $N_i = L_i/L_{i+1}$; then $KN_i \cong N_i'$, and

$$L = (N_1, \ldots, N_k; \{\Lambda^{ij}\})$$

for some $\{\Lambda^{ij}\} \in B(N_1, \ldots, N_k)$.

LEMMA 1. *Let M_i, N_i, $\in S(N_i')$, $1 \leqslant i \leqslant k$, and suppose that*

$$(M_1, \ldots, M_k; \{\Lambda^{ij}\}) \cong (N_1, \ldots, N_k; \{\Omega^{ij}\}).$$

Then $M_i \cong N_i$, $1 \leqslant i \leqslant k$.

Proof. (A modified version of this is given in **(2)**.) It suffices to prove that if $(N, M; \Lambda) \cong (\bar{N}, \bar{M}; \bar{\Lambda})$, where $KN \cong K\bar{N}$ and $KM \cong K\bar{M}$, and where KN and KM have no common irreducible constituent, then $M \cong \bar{M}$ and $N \cong \bar{N}$. Once this is established, a simple induction argument completes the proof.

Suppose that θ: $(N, M; \Lambda) \cong (\bar{N}, \bar{M}; \bar{\Lambda})$ is given by

$$\theta(n, m) = \theta(n, 0) + \theta(0, m) = (\theta_1(n), \nu(n)) + (\mu(m), \theta_2(m)),$$

where

$$\theta_1 \in \mathrm{Hom}_R(N, \bar{N}),\ \nu \in \mathrm{Hom}_R(N, \bar{M}),\ \mu \in \mathrm{Hom}_R(\mathrm{M}, \bar{N}),\ \theta_2 \in \mathrm{Hom}_R(M, \bar{M}).$$

From $\theta g(n, m) = g\theta(n, m)$ we obtain at once

$$(10.1,10.2) \qquad \theta_1 g + \mu\Lambda_g = g\theta_1, \qquad \mu g = g\mu,$$

$$(10.3,10.4) \qquad \bar{\Lambda}_g\theta_1 + g\nu = \nu g + \theta_2\Lambda_g, \qquad \theta_2 g = \bar{\Lambda}_g\mu + g\theta_2.$$

From (10.2) we have $\mu \in \mathrm{Hom}_G(M, \bar{N})$, and hence $\mu = 0$, since by hypothesis KM and $K\bar{N}$ have no common irreducible constituents. Equations (10.1) and (10.4) then imply that $\theta_1 \in \mathrm{Hom}_G(N, \bar{N})$ and $\theta_2 \in \mathrm{Hom}_G(M, \bar{M})$. Since θ is an isomorphism of $(N, M; \Lambda)$ onto $(\bar{N}, \bar{M}; \bar{\Lambda})$, we find readily that $\theta_1 : N \cong \bar{N}$ and $\theta_2 : M \cong \bar{M}$.

LEMMA 2. *Let* $(N_1, \ldots, N_k; \{\Lambda^{ij}\})$ *and* $(N_1, \ldots, N_k; \{\Omega^{ij}\})$ *be G-isomorphic modules in* $S(L')$, *where* $N_i \in S(N_i')$. *Then there exist units* $\beta_1, \ldots, \beta_k \in \mathfrak{u}$, *and homomorphisms* $t_{ij} \in \mathrm{Hom}_R(N_i, N_j)$, *such that the isomorphism between these G-modules is given by*

$$(n_1, \ldots, n_k) \rightarrow (\beta_1 n_1, \beta_2 n_2 + t_{12}n_1, \ldots, \beta_k n_k + t_{1k}n_1 + \ldots + t_{k-1,\,k}n_{k-1}).$$

Proof. From the proof of the preceding lemma, we find that the isomorphism must be given by

$$(n_1, \ldots, n_k) \rightarrow (\theta_1 n_1, \theta_2 n_2 + t_{12}n_1, \ldots, \theta_k n_k + t_{1k}n_1 + \ldots + t_{k-1,k}n_{k-1}),$$

with each θ_i: $N_i \cong N_i$ and each $t_{ij} \in \mathrm{Hom}_R(N_i, N_j)$. Since KN_i is an absolutely irreducible A-module, θ_i must be given by scalar multiplication by a unit of R. This completes the proof.

If U, V are R-modules, and $f_1, f_2 \in \mathrm{Hom}_R(U, V)$, we shall often abbreviate the congruence $f_1 \equiv f_2 \pmod{\mathfrak{g}^a \mathrm{Hom}_R(U, V)}$ as $f_1 \equiv f_2 \pmod{\mathfrak{g}^a}$. A similar notation will be used for R_p-modules.

LEMMA 3. *Let* $M_1, \ldots, M_k$ *be G-modules, not necessarily irreducible, and let*

$$L = (M_1, \ldots, M_k; \{\Lambda^{ij}\}), \qquad \bar{L} = (M_1, \ldots, M_k; \{\Omega^{ij}\})$$

be G-modules for which

$$\Lambda^{ij} \equiv \Omega^{ij} \pmod{\mathfrak{g}^n}, \qquad 1 \leqslant i < j \leqslant k,$$

https://doi.org/10.4153/CJM-1959-061-5 Published online by Cambridge University Press

where n is a fixed integer $\geqslant k-1$. Then there exists a G-isomorphism $\theta: L \cong \bar{L}$ such that $\theta \equiv I \pmod{\mathfrak{g}^{n-k+1}}$, where $I: L \cong \bar{L}$ is the R-isomorphism given by $(m_1, \ldots, m_k) \to (m_1, \ldots, m_k)$.

Proof. The result is trivial for $k = 1$; let $k > 1$, and assume the result holds at $k - 1$. Let us set

$$\Delta = (M_2, \ldots, M_k; \Lambda^{23}, \ldots, \Lambda^{k-1,k}),$$
$$\bar{\Delta} = (M_2, \ldots, M_k; \Omega^{23}, \ldots, \Omega^{k-1,k}).$$

From the induction hypothesis we deduce the existence of a G-isomorphism $\theta_1: \Delta \cong \bar{\Delta}$ such that

$$\theta_1 \equiv I \pmod{\mathfrak{g}^{n-k+2}}.$$

The map $(m_1, \delta) \to (m_1, \theta_1\delta)$, where $m_1 \in M_1$, $\delta \in \Delta$, then gives a G-isomorphism

$$\theta_2 : (M_1, \Delta; \Lambda^{12}, \ldots, \Lambda^{1k}) \cong (M_1, \bar{\Delta}; \bar{\Lambda}^{12}, \ldots, \bar{\Lambda}^{1k})$$

for some $(\bar{\Lambda}^{12}, \ldots, \bar{\Lambda}^{1k}) \in B(M_1, \bar{\Delta})$, and we have

$$\theta_2 \equiv I \pmod{\mathfrak{g}^{n-k+2}}.$$

Now set

$$\bar{\Lambda} = (\bar{\Lambda}^{12}, \ldots, \bar{\Lambda}^{1k}), \qquad \Omega = (\Omega^{12}, \ldots, \Omega^{1k}).$$

Then we see that both $\bar{\Lambda}$ and Ω are elements of $B(M_1, \bar{\Delta})$, and that $\bar{\Lambda} \equiv \Omega \pmod{\mathfrak{g}^{n-k+2}}$. By considering this congruence for the powers of the prime ideals dividing $\mathfrak{g}$, the method of proof of Theorem 1 shows the existence of an element $W \in \text{Hom}_R(M_1, \bar{\Delta})$ such that

$$(\bar{\Lambda} - \Omega)_g = gW - Wg, \qquad g \in G,$$

and where, furthermore, $W \equiv 0 \pmod{\mathfrak{g}^{n-k+1}}$. The map $(m_1, \bar{\delta}) \to (m_1, \bar{\delta} - Wm_1)$ then yields a G-isomorphism $\theta_3 : (M_1, \bar{\Delta}; \Omega) \cong (M_1, \bar{\Delta}; \Lambda)$, where

$$\theta_3 \equiv I \pmod{\mathfrak{g}^{n-k+1}}.$$

Therefore

$$\theta_3^{-1}\theta_2 : (M_1, \Delta; \Lambda^{12}, \ldots, \Lambda^{1k}) \to (M_1, \bar{\Delta}; \Omega^{12}, \ldots, \Omega^{1k})$$

is a G-isomorphism of L onto $\bar{L}$ such that

$$\theta_3^{-1}\theta_2 \equiv I \pmod{\mathfrak{g}^{n-k+1}}.$$

4. Integral classes and genera for modules with two distinct constituents. Throughout this section, we suppose that L' is an A-module with two distinct irreducible constituents N' and M'; we assume again that K is a splitting field for A. Let $S(L')$ be partitioned into r_G classes under G-isomorphism, and into r_g genera. We shall obtain formulas for r_G and r_g.

LEMMA 4. *Let $N \in S(N')$, $M \in S(M')$. Then $(N, M; \Lambda) \cong (N, M; \bar{\Lambda})$ if and only if there exists $\beta \in \mathfrak{u}$ such that $[\bar{\Lambda}] = \beta[\Lambda]$.*

Proof. From Lemma 2 we deduce the existence of units $\beta_1, \beta_2 \in \mathfrak{u}$, and of $t \in \mathrm{Hom}_R(N, M)$, such that the isomorphism $(N, M; \Lambda) \cong (N, M; \bar{\Lambda})$ is given by $(n, m) \to (\beta_1 n, \beta_2 m + tn)$. This implies

$$\bar{\Lambda}_g = \beta_1^{-1}\beta_2\Lambda_g + g(\beta_1^{-1}t) - (\beta_1^{-1}t)g, \qquad g \in G.$$

Setting $\beta = \beta_1^{-1}\beta_2$, we have $[\bar{\Lambda}] = \beta[\Lambda]$. Conversely, starting from such a relation, we may reverse the steps to obtain an isomorphism of the modules.

LEMMA 5. *Let $N \in S(N')$, $M \in S(M')$. Then $(N, M; \Lambda) \vee (N, M; \bar{\Lambda})$ if and only if there exists an element $\alpha \in R$ such that $(\alpha) + \mathfrak{g} = R$ and $[\bar{\Lambda}] = \alpha[\Lambda]$.*

Proof. Let $(N, M; \Lambda) \vee (N, M; \bar{\Lambda})$. As in the preceding proof, we deduce that for each $p \in P$, there exists an element α_p which is a unit in R_p such that the classes $[\Lambda^p]$ and $[\bar{\Lambda}^p]$ in $C(N_p, M_p)$ are related by

$$[\bar{\Lambda}^p] = \alpha_p[\Lambda^p].$$

Choose $\alpha \in R$ such that $\alpha \equiv \alpha_p \pmod{p^{\gamma(p)}}$ for each $p \in P$; then $(\alpha) + \mathfrak{g} = R$. Furthermore, $(\alpha - \alpha_p)B(N_p, M_p) \subset B'(N_p, M_p)$, so that

$$\alpha[\Lambda^p] = \alpha_p[\Lambda^p], \qquad p \in P.$$

Therefore $[\bar{\Lambda}^p] = [\alpha\Lambda^p]$ for all $p \in P$, and so by Theorem 1 we have $[\bar{\Lambda}] = [\alpha\Lambda] = \alpha[\Lambda]$.

Suppose now that $S(N')$ splits into ν genera; according to (7), each genus splits into h classes under G-isomorphism. Let us choose representatives of the $h\nu$ classes, say $\{N_j^i : 1 \leqslant i \leqslant \nu, 1 \leqslant j \leqslant h\}$, so that all the modules with the same subscript lie in the same genus. Likewise choose representatives $\{M_j^i : 1 \leqslant i \leqslant \mu, 1 \leqslant j \leqslant h\}$ of the $h\mu$ classes into which $S(M')$ splits. Let $(N, M; \Gamma) \in S(L')$, and suppose $N \vee N_1^i$, $M \vee M_1^j$. Then for each $p \in P$, there exists an element

$$\Omega^p \in B((N_1^i)_p, (M_1^j)_p)$$

such that

$$(N_p, M_p; \Gamma^p) \cong ((N_1^i)_p, (M_1^j)_p; \Omega^p)$$

as A_p-modules. By Theorem 1, there exists $\Lambda \in B(N_1^i, M_1^j)$ such that $[\Lambda^p] = [\Omega^p]$ for all $p \in P$. Therefore

$$(N, M; \Gamma)^p \cong (N_1^i, M_1^j; \Lambda)_p, \qquad p \in P,$$

and so

$$(N, M; \Gamma) \vee (N_1^i, M_1^j; \Lambda).$$

Hence, every module in $S(L')$ is in the same genus as $(N_1{}^i, M_1{}^j; \Lambda)$ for some choice of i and j and some $\Lambda \in B(N_1{}^i, M_1{}^j)$. Further,

$$(N_1^i, M_1^j; \Lambda) \vee (N_1^{i'}, M_1^{j'}; \Lambda')$$

implies, by the method of proof of Lemma 1, that $i = i'$ and $j = j'$. Let us set

$$H_{ij} = \{(N_1^i, M_1^j; \Lambda) : \Lambda \in B(N_1^i, M_1^j)\}, 1 \leqslant i \leqslant \nu, 1 \leqslant j \leqslant \mu, \tag{11}$$

and suppose that H_{ij} splits into r_{ij} genera. Then we have at once

$$r_g = \sum_{i,j} r_{ij}. \tag{12}$$

On the other hand, any module in $S(L')$ is G-isomorphic to $(N_\rho{}^i, M_\sigma{}^j; \Lambda)$ for some i, j, ρ, σ and Λ. Further, by Lemma 1, two such modules cannot be isomorphic unless they have the same set of indices i, j, ρ, σ. Let us set

$$S(i, \rho; j, \sigma) = \{(N_\rho^i, M_\sigma^j; \Lambda) : \Lambda \in B(N_\rho^i, M_\sigma^j)\},$$

and suppose that $S(i, \rho; j, \sigma)$ splits into $s(i, \rho; j, \sigma)$ classes. Then

$$r_G = \sum_{i,j,\rho,\sigma} s(i, \rho; j, \sigma).$$

However, Lemma 4 states that $(N_\rho{}^i, M_\sigma{}^j; \Lambda) \cong (N_\rho{}^i, M_\sigma{}^j; \bar{\Lambda})$ if and only if there exists $\beta \in \mathfrak{u}$ such that $[\bar{\Lambda}] = \beta[\Lambda]$. Furthermore, the Corollary to Theorem 1 shows that $C(N_\rho{}^i, M_\sigma{}^j)$ is (as R-module) independent of ρ and σ. Therefore $s(i, \rho; j, \sigma) = s(i, 1; j, 1)$ for all ρ and σ, and we have

$$r_G = h^2 \sum_{i,j} s_{ij}, \tag{13}$$

where $s_{ij} = s(i, 1; j, 1)$ is the number of classes into which H_{ij} splits.

Before proceeding with the calculation of r_{ij} and s_{ij}, it will be convenient to introduce some notations. For a non-zero ideal $\mathfrak{a}$ in R, let $\phi(\mathfrak{a})$ denote the number of residue classes in $R/\mathfrak{a}$ which are relatively prime to $\mathfrak{a}$. If $\mathfrak{a} + \mathfrak{b} = R$, then $\phi(\mathfrak{a}\mathfrak{b}) = \phi(\mathfrak{a})\phi(\mathfrak{b})$. Next, let $u(\mathfrak{a})$ denote the number of distinct residue classes in $(\mathfrak{u} + \mathfrak{a})/\mathfrak{a}$; of course, $u(\mathfrak{a})$ is a divisor of $\phi(\mathfrak{a})$. However, $u(\mathfrak{a})$ is not a multiplicative function of $\mathfrak{a}$, as is seen from the example where K is the rational field.

LEMMA 6. *Let $N \in S(N')$, $M \in S(M')$, and $H = \{(N, M; \Lambda) : \Lambda \in B(N,M)\}$. Suppose H splits into r genera and s classes. Let $d(\mathfrak{a})$ be the number of elements in $C(N, M)$ with order ideal a. Then*

$$r = \sum_{\mathfrak{a}} d(\mathfrak{a})/\phi(\mathfrak{a}), \qquad s = \sum_{\mathfrak{a}} d(\mathfrak{a})/u(\mathfrak{a}),$$

both sums extending over all divisors of $\mathfrak{g}$.

(The order ideal of an element $c \in C(N, M)$ is $\{\alpha \in R : \alpha c = 0\}$.)

Proof. Let us use the symbol $(N, M; c)$ to denote the collection of mutually isomorphic modules $\{(N, M; \Lambda): \Lambda \in c\}$, where $c \in C(N, M)$. By Lemma 4, $(N, M; c)$ and $(N, M; c')$ cannot lie in the same genus unless c and c' have the same order ideal. Consider the set of $d(\mathfrak{a})$ elements of $C(N, M)$ with given order ideal $\mathfrak{a}$. For a fixed c in this set, all those c' of the form αc, where $\alpha \in R$ is such that $(\alpha) + \mathfrak{g} = R$, will yield modules in the same genus as those obtained from c. But as α ranges over all elements of R for which $(\alpha) + \mathfrak{g} = R$, αc gives exactly $\phi(\mathfrak{a})$ distinct elements of $C(N, M)$. Therefore

$$r = \sum_{\mathfrak{a}} d(\mathfrak{a})/\phi(\mathfrak{a}).$$

A similar argument gives the formula for s.

Let $d_p(p^n)$ denote the number of elements in $C(N_p, M_p)$ having order ideal p^n. Then

$$d_p(p^n) = \tau(p^n) - \tau(p^{n-1}),$$

where $\tau(p^n)$ denotes the number of elements of $C(N_p, M_p)$ which are annihilated by p^n. From Theorem 1,

$$d(\mathfrak{a}) = \prod_{p \in P} d_p(p^{a(p)}), \text{ where } \mathfrak{a} = \prod_{p \in P} p^{a(p)}.$$

We may therefore write

$$r = \prod_{p \in P} \left\{ \sum_{a=0}^{\gamma(p)} d_p(p^a)/\phi(p^a) \right\},$$

which confirms the result in (7) that the number of genera is the product over all $p \in P$ of the number of classes into which $S(L')$ splits under A_p-isomorphism. The corresponding multiplicative formula for s fails to hold, because $u(\mathfrak{a})$ is not multiplicative.

Applying Lemma 6 to our original problem, we may summarize our result as follows.

THEOREM 2. *Let $N^1, \ldots, N^\nu$ be representatives of the genera into which $S(N')$ splits, and $M^1, \ldots, M^\mu$ representatives of the genera of $S(M')$. For each divisor $\mathfrak{a}$ of $\mathfrak{g}$, let $d_{ij}(\mathfrak{a})$ denote the number of elements in $C(N^i, M^j)$ having order ideal $\mathfrak{a}$. Then $S(L')$ splits into r_g genera and r_G classes, where*

$$r_g = \sum_{\mathfrak{a}} \sum_{i,j} d_{ij}(\mathfrak{a})/\phi(\mathfrak{a}), \quad r_G = h^2 \sum_{\mathfrak{a}} \sum_{i,j} d_{ij}(\mathfrak{a})/u(\mathfrak{a}).$$

Here, $\phi(\mathfrak{a})$ is the number of residue classes in $R/\mathfrak{a}$ which are relatively prime to $\mathfrak{a}$, and $u(\mathfrak{a})$ is the number of distinct elements of $(\mathfrak{u} + \mathfrak{a})/\mathfrak{a}$.

COROLLARY. *We have $r_G \geqslant h^2 r_g$, with equality provided that $\phi(\mathfrak{g}) = u(\mathfrak{g})$. Furthermore, if any $C(N^i, M^j)$ contains an element of order ideal $\mathfrak{a}$, where $u(\mathfrak{a}) < \phi(\mathfrak{a})$, then $r_G > h^2 r_g$.*

5. Integral classes and genera in the general case. Now let L' be an A-module with k distinct irreducible constituents, and let K be a splitting field for A. We preserve the notation introduced at the beginning of § 3. In this section we shall generalize the results given in the Corollary to Theorem 2.

For each κ $(1 \leqslant \kappa \leqslant k)$, let $\{N_\kappa{}^{ij}: 1 \leqslant i \leqslant \nu(\kappa), 1 \leqslant j \leqslant h\}$ be a full set of representatives of the $h\nu(\kappa)$ classes into which the set $\mathrm{S}(N_\kappa')$ splits; suppose these representative modules are so chosen that modules with the same indices i and κ lie in the same genus. Then every module in $S(L')$ is of the form

$$(N_1^{i_1 j_1}, \ldots, N_k^{i_k j_k}; \{\Lambda^{ij}\}).$$

Let $S(i_1, j_1; \ldots; i_k, j_k)$ be the set of all such modules obtained by letting $\{\Lambda^{ij}\}$ range over all systems in

$$B(N_1^{i_1 j_1}, \ldots, N_k^{i_k j_k}),$$

and let this set split into $r(i_1, j_1; \ldots; i_k, j_k)$ genera and $s(i_1, j_1; \ldots; i_k, j_k)$ classes. From the Corollary to Theorem 1, we see that $r(i_1, j_1; \ldots; i_k, j_k)$ is independent of $(j_1, \ldots, j_k)$, and therefore

$$r_g = h^{-k} \sum r(i_1, j_1, ; \ldots; i_k, j_k), \quad r_G = \sum s(i_1, j_1,; \ldots; i_k, j_k),$$

both summations extending over all possible values of the i's and j's. This implies the result that

$$r_G \geqslant h^k r_g.$$

Finally, we prove:

THEOREM 3. *If* $u(\mathfrak{g}^{k-1}) = \phi(\mathfrak{g}^{k-1})$, *then* $r_G = h^k r_g$.

Proof. We remark that the hypothesis of the Theorem is simply a restatement of condition (3) given in the introduction. To prove the theorem, we need only show that $r(i_1, j_1; \ldots; i_k, j_k) = s(i_1, j_1; \ldots; i_k, j_k)$. We simplify the notation by letting $M_\kappa \in \mathrm{S}(N_\kappa')$, $1 \leqslant \kappa \leqslant k$. We shall prove that if

$$L = (M_1, \ldots, M_k; \{\Lambda^{ij}\}), \qquad \bar{L} = (M_1, \ldots, M_k; \{\bar{\Lambda}^{ij}\})$$

are such that $L \vee \bar{L}$, then also $L \cong \bar{L}$.

Since $L_p \cong \bar{L}_p$ for each $p \in P$, Lemma 2 shows the existence of units $\beta_1{}^p, \ldots, \beta_k{}^p$ in R_p, and homomorphisms

$$t_{ij}^p \in \mathrm{Hom}_p\ ((M_i)_p, (M_j)_p)$$

such that the isomorphism $L_p \cong \bar{L}_p$ is given by

$$(m_1, \ldots, m_k) \to (\beta_1^p m_1, \beta_2^p m_2 + t_{12}^p m_1, \ldots, \beta_k^p m_k + t_{1k}^p m_1 + \ldots + t_{k-1,k}^p m_{k-1}).$$

By the hypothesis of the theorem, we may choose units $\beta_1, \ldots, \beta_k \in \mathfrak{u}$ such that

$$\beta_\kappa \equiv \beta_\kappa^p \qquad (\mathrm{mod}\ p^{(k-1)\gamma(p)}), \qquad p \in P, \qquad 1 \leqslant \kappa \leqslant k.$$

As in the proof of Theorem 1, we may choose homomorphisms $w_{ij} \in \mathrm{Hom}_R(M_i, M_j)$ such that

$$w_{ij}^p \equiv t_{ij}^p \quad \bmod p^{(k-1)\gamma(p)}, \quad 1 \leqslant i < j \leqslant k, \quad p \in P.$$

Then the map

$$(m_1, \ldots, m_k) \to (\beta_1 m_1, \beta_2 m_2 + w_{12} m_1, \ldots, \beta_k m_k + w_{1k} m_1 + \ldots + w_{k-1,k} m_{k-1})$$

gives a G-isomorphism of L onto a module L^* where $L^* = (M_1, \ldots, M_k; \{\Omega^{ij}\})$ and $\Omega^{ij} \equiv \bar{\Lambda}^{ij} \pmod{\mathfrak{g}^{k-1}}$ for $1 \leqslant i < j \leqslant k$. By Lemma 3 we then have $L^* \cong \bar{L}$, which completes the proof of the theorem.

It would be of interest to obtain formulas for r_G and r_g which generalize those given in Theorem 2.

References

1. K. deLeeuw, *Some applications of cohomology to algebraic number theory and group representations*, unpublished.
2. F. E. Diederichsen, *Ueber die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetischer Äquivalenz*, Hamb. Abh., *14* (1938), 357–412.
3. D. G. Higman, *On orders in separable algebras*, Can. J. Math., *7* (1955), 509–515.
4. N. Jacobson, *The theory of rings* (New York, 1943).
5. I. Kaplansky, *Modules over Dedekind rings and valuation rings*, Trans. Amer. Math. Soc., *7* (1952), 327–40.
6. J.-M. Maranda, *On p-adic integral representations of finite groups*, Can. J. Math., *5* (1953), 344–355.
7. ——— *On the equivalence of representations of finite groups by groups of automorphisms of modules over Dedekind rings*, Can. J. Math., *7* (1955), 516–526.
8. I. Reiner, *Maschke modules over Dedekind rings*, Can. J. Math., *8* (1956), 329–334.
9. H. Zassenhaus, *Neuer Beweis der Endlichkeit der Klassenzahl bei unimodularer Äquivalenz endlicher ganzzahliger Substitutionsgruppen*, Hamb. Abh., *12* (1938), 276–288.

University of Illinois