

ON THE EQUIVALENCE OF REPRESENTATIONS OF FINITE GROUPS BY GROUPS OF AUTOMORPHISMS OF MODULES OVER DEDEKIND RINGS

J.-M. MARANDA

1. Introduction. Let i be a Dedekind ring whose quotient field we denote by K . If \mathfrak{p} is a prime ideal of i , let \mathfrak{o} denote the ring of all \mathfrak{p} -regular elements of K . If \mathfrak{M} is a torsion free i -module, let $K\mathfrak{M}$ denote the smallest K -module into which \mathfrak{M} can be embedded and let $\mathfrak{o}\mathfrak{M}$ denote the \mathfrak{o} -submodule of $K\mathfrak{M}$ generated by \mathfrak{M} .

Let \mathfrak{G} be a group of finite order N and let A , \mathfrak{D} and \mathfrak{F} denote the group rings of \mathfrak{G} over K , \mathfrak{o} and i respectively.

If \mathfrak{M} is an \mathfrak{F} -module which is torsion free over i , then there is a unique way of defining $K\mathfrak{M}$ ($\mathfrak{o}\mathfrak{M}$) as an A -module (\mathfrak{D} -module) so that it is an extension of the \mathfrak{F} -module \mathfrak{M} . If \mathfrak{M} and \mathfrak{N} are two \mathfrak{F} -modules that are torsion free over i , we will say that \mathfrak{M} and \mathfrak{N} are

- (1) i -equivalent if they are \mathfrak{F} -isomorphic;
- (2) K -equivalent if $K\mathfrak{M}$ and $K\mathfrak{N}$ are A -isomorphic;
- (3) \mathfrak{o} -equivalent if $\mathfrak{o}\mathfrak{M}$ and $\mathfrak{o}\mathfrak{N}$ are \mathfrak{D} -isomorphic;
- (4) of the same genus if they are \mathfrak{o} -equivalent for every prime ideal \mathfrak{p} of i .

Let \mathfrak{S} be a class of K -equivalent \mathfrak{F} -modules that are torsion free and finitely generated over i . We will assume that \mathfrak{S} is complete in the sense that if an \mathfrak{F} -module \mathfrak{M} is K -equivalent to an \mathfrak{F} -module in \mathfrak{S} , then \mathfrak{M} is i -equivalent to an \mathfrak{F} -module in \mathfrak{S} . Let \mathfrak{R} , $\mathfrak{R}(\mathfrak{p})$ and $\mathfrak{R}_\mathfrak{o}$ denote the partitions of \mathfrak{S} into complete subclasses of i -equivalent \mathfrak{F} -modules, \mathfrak{o} -equivalent \mathfrak{F} -modules and \mathfrak{F} -modules of the same genus respectively, and let \mathbf{r} , $\mathbf{r}(\mathfrak{p})$ and $\mathbf{r}_\mathfrak{o}$ denote the number of subclasses of \mathfrak{S} determined by \mathfrak{R} , $\mathfrak{R}(\mathfrak{p})$ and $\mathfrak{R}_\mathfrak{o}$ respectively.

We will show first of all that if $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ are the prime ideal divisors of N , then

$$\mathfrak{R}_\mathfrak{o} = \prod_{i=1}^r \mathfrak{R}(\mathfrak{p}_i)$$

and that

$$\mathbf{r}_\mathfrak{o} = \prod_{i=1}^r \mathbf{r}(\mathfrak{p}_i).$$

Secondly, we will show that if for every \mathfrak{F} -module $\mathfrak{M} \in \mathfrak{S}$, the representation of A belonging to $K\mathfrak{M}$ is absolutely irreducible, then $\mathbf{r} = h\mathbf{r}_\mathfrak{o}$, where h is the ideal class number of i . In the case where i is the ring of algebraic integers of

Received August 24, 1954; in revised form March 30, 1955. This paper is based on work done at the Summer Research Institute of the Canadian Mathematical Congress. The author is indebted to Prof. H. Zassenhaus for proposing this problem and to both Prof. Zassenhaus and Prof. R. Brauer for their advice and valuable suggestions.

an algebraic number field K , then h is finite, and we will show that each $\mathfrak{r}(\mathfrak{p}_i)$ is finite, so that \mathfrak{r} is also finite.

In §2, we will speak in terms of matrix representations of \mathfrak{G} . This will not constitute a restriction, since in this section we will speak of representations of \mathfrak{G} over principal ideal rings.

2. Integral representations of finite groups over fields with \mathfrak{P} -adic valuations.

Let \mathfrak{G} be a group of finite order N and let \mathfrak{o} be a commutative ring with unity element. By an \mathfrak{o} -representation of \mathfrak{G} of degree n , we mean a homomorphism of Γ of \mathfrak{G} into the multiplicative semi-group of all $n \times n$ \mathfrak{o} -matrices which maps the identity element of \mathfrak{G} onto the identity matrix. We will denote the image by Γ of any $x \in \mathfrak{G}$ by Γ_x .

If R is a commutative extension ring of \mathfrak{o} , then two \mathfrak{o} -representations Γ and Δ of \mathfrak{G} will be said to be R -equivalent if they are of the same degree n and if there is an invertible $n \times n$ R -matrix T such that $\Gamma_x T - T \Delta_x = 0$ for all $x \in \mathfrak{G}$. If the \mathfrak{o} -representation Γ of \mathfrak{G} is \mathfrak{o} -equivalent to a representation of the type

$$x \rightarrow \begin{pmatrix} \Gamma'_x & \Lambda_x \\ 0 & \Gamma''_x \end{pmatrix}$$

where Γ' and Γ'' are \mathfrak{o} -representations of \mathfrak{G} , then we say that Γ is reducible; otherwise, we say that Γ is irreducible.

Let K be a field of characteristic zero with a \mathfrak{P} -adic valuation ϕ , that is, ϕ is non-archimedean and discrete of rank 1, and the residue class field determined by ϕ is of finite characteristic. If K is complete with respect to ϕ , then K is said to be a \mathfrak{P} -adic field. Let \mathfrak{o} denote the ring of integers of K , i.e., the set of all elements with values ≤ 1 , let \mathfrak{P} denote the prime ideal of \mathfrak{o} , i.e., the set of all elements with values < 1 , and let \mathfrak{p} be a generator of \mathfrak{P} . In general, we will denote the complete extension of K with respect to ϕ by K^* . The ring of integers of K^* will be denoted by \mathfrak{o}^* and its prime ideal by \mathfrak{P}^* . Let \mathfrak{P}^{k_0} be the highest power of \mathfrak{P} dividing N .

For completeness, we will state some theorems obtained previously by the author, and refer the reader to (2) for the proofs.

THEOREM 1. *If Γ and Δ are two \mathfrak{o} -representations of \mathfrak{G} , then Γ and Δ are \mathfrak{o} -equivalent if and only if the \mathfrak{P}^k -modular representations $\bar{\Gamma}$ and $\bar{\Delta}$, induced by Γ and Δ respectively, are $(\mathfrak{o}/\mathfrak{P}^k)$ -equivalent, for any $k > k_0$.*

For the proof, we refer the reader to (2, p. 347). Although in the paper referred to one is only concerned with the case where K is complete, it is obvious that this condition is not essential for this theorem. The argument applied is due to Schur (3).

COROLLARY 1. *Γ and Δ are \mathfrak{o}^* -equivalent if and only if they are \mathfrak{o} -equivalent.*

Proof. Assume that Γ and Δ are \mathfrak{o}^* -equivalent, i.e., that Γ and Δ are of the same degree n and that there is an $n \times n$ \mathfrak{o}^* -matrix T such that $\Gamma_x T - T \Delta_x = 0$

for all $x \in \mathfrak{G}$, and that $|T| \notin \mathfrak{P}^*$. Let T' be an \mathfrak{o} -matrix congruent to T , modulo \mathfrak{P}^{*k} . Such a matrix always exists since $(\mathfrak{o}/\mathfrak{P}^k) \cong (\mathfrak{o}^*/\mathfrak{P}^{*k})$. Then

$$\Gamma_x T' - T' \Delta_x \equiv 0 \pmod{\mathfrak{P}^k}$$

for all $x \in \mathfrak{G}$ and $|T'| \notin \mathfrak{P}$. Taking $k > k_0$, by Theorem 1 Γ and Δ are \mathfrak{o} -equivalent.

COROLLARY 2. *If $(\mathfrak{o}/\mathfrak{P})$ is a finite ring, then any class of K -equivalent \mathfrak{o} -representations of \mathfrak{G} contains only a finite number of complete subclasses of \mathfrak{o} -equivalent representations.*

Proof. From Theorem 1, the number of classes of \mathfrak{o} -equivalent \mathfrak{o} -representations of \mathfrak{G} of a given degree is less than or equal to the number of classes of $(\mathfrak{o}/\mathfrak{P}^k)$ -equivalent $(\mathfrak{o}/\mathfrak{P}^k)$ -representations of \mathfrak{G} of the same degree, for any $k > k_0$, and if $(\mathfrak{o}/\mathfrak{P}^k)$ is a finite ring, this number is evidently finite.

THEOREM 2. *If $N \notin \mathfrak{P}$, and if the \mathfrak{o} -representation Γ of G is \mathfrak{o} -equivalent to a representation of the type*

$$x \rightarrow \begin{pmatrix} \Gamma'_x & \Lambda_x \\ 0 & \Gamma''_x \end{pmatrix},$$

where Γ' and Γ'' are \mathfrak{o} -representations of \mathfrak{G} , then Γ is \mathfrak{o} -equivalent to the representation

$$x \rightarrow \begin{pmatrix} \Gamma'_x & 0 \\ 0 & \Gamma''_x \end{pmatrix}.$$

For the proof, see (2, p. 353). The remarks made after Theorem 1 also apply to this theorem.

THEOREM 3. *If K is complete, if \mathfrak{D} is an \mathfrak{o} -representation of \mathfrak{G} and if \mathfrak{D} is \mathfrak{o} -equivalent to a representation of the type*

$$x \rightarrow \begin{pmatrix} \Gamma_x & \Lambda_x \\ p^k \theta_x & \Delta_x \end{pmatrix}$$

where Γ and Δ induce \mathfrak{P}^k -modular representations of \mathfrak{G} and where $k > 2k_0$, then \mathfrak{D} is \mathfrak{o} -equivalent to a representation of the type

$$x \rightarrow \begin{pmatrix} \Gamma_x^* & \Lambda_x \\ 0 & \Delta_x^* \end{pmatrix}$$

where Γ^* and Δ^* are \mathfrak{o} -representations of \mathfrak{G} that coincide with Γ and Δ respectively, modulo \mathfrak{P}^{k-k_0} .

For the proof, see (2, p. 348).

COROLLARY. *If K is complete, if $N \notin \mathfrak{P}$, if Γ and Δ are irreducible \mathfrak{o} -representations of \mathfrak{G} of degree n and if T is a non-zero $n \times n$ \mathfrak{o} -matrix such that $\Gamma_x T - T \Delta_x = 0$ for all $x \in \mathfrak{G}$, then $T = p^m T'$, where T' is an \mathfrak{o} -matrix and $|T'| \notin \mathfrak{P}$.*

Proof. Since $N \notin \mathfrak{P}$, by Theorem 3, the \mathfrak{P} -modular representations $\bar{\Gamma}$ and $\bar{\Delta}$ induced by Γ and Δ respectively are irreducible. Let p^m be the highest power of p dividing all the entries of T and let $T = p^m T'$. Surely,

$$\Gamma_x T' - T' \Delta_x \equiv 0 \pmod{\mathfrak{P}}$$

so that by Schur's lemma, T' is non-singular, modulo \mathfrak{P} , since p does not divide all the entries of T' , i.e., $|T'| \notin \mathfrak{P}$.

THEOREM 4. *If $N \notin \mathfrak{P}$, then two \mathfrak{o} -representations Γ and Δ of \mathfrak{G} are K -equivalent if and only if they are \mathfrak{o} -equivalent.*

Proof. Let us assume that Γ and Δ are K -equivalent and let us first suppose that K is complete. If Δ is irreducible, by (5, p. 283) Γ is also irreducible, so that the statement follows from the Corollary to Theorem 3. If Δ is reducible, by Theorem 2 we may assume that

$$\Delta = \begin{pmatrix} \Delta_1 & 0 \\ 0 & \Delta_2 \end{pmatrix}$$

where Δ_1 and Δ_2 are \mathfrak{o} -representations of \mathfrak{G} . Since Γ is K -equivalent to Δ , by (5, p. 283) and by Theorem 2, Γ is \mathfrak{o} -equivalent to a representation of the type

$$\begin{pmatrix} \Gamma_1 & 0 \\ 0 & \Gamma_2 \end{pmatrix}$$

where Γ_1 and Γ_2 are \mathfrak{o} -representations of \mathfrak{G} that are K -equivalent to Δ_1 and Δ_2 respectively. If we use induction with respect to the number of irreducible constituents of Δ , the K -equivalence implies the \mathfrak{o} -equivalence of Γ_1 and Γ_2 with Δ_1 and Δ_2 respectively, so that Γ and Δ are \mathfrak{o} -equivalent.

Now, if we consider the general case, where K is not necessarily complete if Γ and Δ are K -equivalent, then we have just seen that they are \mathfrak{o}^* -equivalent, so that by Corollary 1 to Theorem 1 they are \mathfrak{o} -equivalent.

COROLLARY. *If $N \notin \mathfrak{P}$ and if \mathfrak{D} is any \mathfrak{o} -representation of \mathfrak{G} , then in any reduction of \mathfrak{D} into irreducible constituents, these constituents are unique up to order and \mathfrak{o} -equivalence.*

Proof. Let

$$\begin{pmatrix} \Gamma_1 & * \\ & \Gamma_2 \dots \\ 0 & \Gamma_r \end{pmatrix} \text{ and } \begin{pmatrix} \Delta_1 & * \\ & \Delta_2 \dots \\ 0 & \Delta_s \end{pmatrix}$$

be two reductions of \mathfrak{D} into irreducible constituents. Then, by (5, p. 283), the Γ_i and Δ_i are also irreducible when considered as K -representations of \mathfrak{G} . Therefore $r = s$ and there is a permutation i_1, i_2, \dots, i_r of the indices $1, 2, \dots, r$ such that, for $j = 1, 2, \dots, r$, Γ_j is K -equivalent to Δ_{i_j} . Then by Theorem 4, Γ_j is \mathfrak{o} -equivalent to Δ_{i_j} .

3. On modules over Dedekind rings. Let i be a Dedekind ring, so that i is an integral domain and every non-null fractional ideal of i is invertible, and let K denote the quotient field of i .

Whenever we consider an i -module \mathfrak{M} , we will always assume that $1.u = u$, for all $u \in \mathfrak{M}$. If \mathfrak{M} is an i -module, the set of all $\alpha \in i$ for which $\alpha u = 0$ for all $u \in \mathfrak{M}$ is an ideal of i which we will call the annihilator of \mathfrak{M} .

We define the order ideal¹ of a finitely generated i -module \mathfrak{M} as follows: If \mathfrak{M} contains an element without torsion, then its order ideal is null, while if \mathfrak{M} is a torsion module, its annihilator \mathfrak{a} is non-null, and since both chain conditions hold for the integral ideals of i that contain \mathfrak{a} , \mathfrak{M} has a composition series and its order ideal is the product of the annihilators of its composition factors.

If \mathfrak{N} is an i -submodule of \mathfrak{M} , since the ascending chain condition holds for the integral ideals of i , \mathfrak{N} is also finitely generated. We denote the order ideal of $\mathfrak{M}/\mathfrak{N}$ by $(\mathfrak{M}:\mathfrak{N})$. From the definition, it follows immediately that $(\mathfrak{M}:O) = (\mathfrak{M}:\mathfrak{N}) \cdot (\mathfrak{N}:O)$ and that $(\mathfrak{M}:O)$ is contained in the annihilator of \mathfrak{M} .

Let \mathfrak{o} denote the ring of all elements of K that are regular with respect to each element of a finite set of prime ideals of i . The ring \mathfrak{o} is a Dedekind ring, indeed a principal ideal domain, and its ideals are just those that are generated over \mathfrak{o} by ideals of i .

If \mathfrak{M} is a torsion free i -module, let $K\mathfrak{M}$ denote the smallest K -module into which \mathfrak{M} can be embedded and let $\mathfrak{o}\mathfrak{M}$ denote the \mathfrak{o} -submodule of $K\mathfrak{M}$ generated by \mathfrak{M} . From the definition of the order ideal, one can verify that if \mathfrak{N} is an i -submodule of \mathfrak{M} , then $(\mathfrak{o}\mathfrak{M}:\mathfrak{o}\mathfrak{N}) = \mathfrak{o}(\mathfrak{M}:\mathfrak{N})$ and $(K\mathfrak{M}:K\mathfrak{N}) = K(\mathfrak{M}:\mathfrak{N})$.

LEMMA 1. *If \mathfrak{M} is a finitely generated torsion free i -module and if \mathfrak{a} is an integral ideal of i , then $(\mathfrak{M}:\mathfrak{a}\mathfrak{M}) = \mathfrak{a}^m$, where m is the rank of \mathfrak{M} (dimension of $K\mathfrak{M}$).*

Proof. If $\mathfrak{a} = 0$, then the statement is trivially true so that we may suppose that $\mathfrak{a} \neq 0$. Let us assume that \mathfrak{o} is the ring of all elements of K that are regular with respect to each of the prime ideal divisors of $(\mathfrak{M}:\mathfrak{a}\mathfrak{M})$ and \mathfrak{a} .

Since \mathfrak{o} is a principal ideal domain, $\mathfrak{o}\mathfrak{M}$ has a linearly independent basis u_1, \dots, u_m over \mathfrak{o} , so that

$$\mathfrak{o}\mathfrak{M} = \sum_{i=1}^m \mathfrak{o}u_i.$$

Then

$$(\mathfrak{o}\mathfrak{a}) \cdot (\mathfrak{o}\mathfrak{M}) = \sum_{i=1}^m (\mathfrak{o}\mathfrak{a})u_i$$

¹For a general definition of the order ideal of a finitely generated module over a commutative ring with unity element, see (6, chap. III, §3 and §5). Using the fundamental theorem of Steinitz on modules over Dedekind rings (4, and also e.g. 1), one may show that this general definition is equivalent to the one given above in the case of modules over Dedekind rings.

and

$$\frac{\mathfrak{o}\mathfrak{M}}{(\mathfrak{o}\alpha) \cdot (\mathfrak{o}\mathfrak{M})} \cong \sum_{i=1}^m \frac{\mathfrak{o}u_i}{(\mathfrak{o}\alpha)u_i} \quad (\text{direct sum}).$$

Therefore, $\mathfrak{o}(\mathfrak{M}:\mathfrak{a}\mathfrak{M}) = (\mathfrak{o}\mathfrak{M}:(\mathfrak{o}\alpha) \cdot (\mathfrak{o}\mathfrak{M})) = (\mathfrak{o}\alpha)^m = \mathfrak{o}\alpha^m$, and because of the choice of \mathfrak{o} , $(\mathfrak{M}:\mathfrak{a}\mathfrak{M}) = \alpha^m$.

If \mathfrak{M} and \mathfrak{N} are torsion free i -modules, and if T is an i -homomorphism of \mathfrak{M} into \mathfrak{N} , then T may be extended to a K -homomorphism of $K\mathfrak{M}$ into $K\mathfrak{N}$ in a unique way by the following definition: $T(u/\alpha) = (T(u))/\alpha$ for all $u \in \mathfrak{M}$, and all $\alpha \in i, \alpha \neq 0$. Of course, T induces an \mathfrak{o} -homomorphism of $\mathfrak{o}\mathfrak{M}$ into $\mathfrak{o}\mathfrak{N}$ so that we may think of the i -module \mathfrak{L} of all i -homomorphisms of \mathfrak{M} into \mathfrak{N} as embedded in the \mathfrak{o} -module \mathfrak{L}_0 of all \mathfrak{o} -homomorphisms of $\mathfrak{o}\mathfrak{M}$ into $\mathfrak{o}\mathfrak{N}$, which in turn is embedded in the K -module \mathfrak{L}_K of all K -homomorphisms of $K\mathfrak{M}$ into $K\mathfrak{N}$. One can easily verify that $\mathfrak{L}_K = K\mathfrak{L}$ and that $\mathfrak{L}_0 = \mathfrak{o}\mathfrak{L}$. Now let us assume that \mathfrak{M} and \mathfrak{N} are finitely generated over i . For each $T \in \mathfrak{L}$, we define the determinant ideal $\delta(T)$ of T to be $(\mathfrak{N}:T(\mathfrak{M}))$.

If $\delta_0(T)$ and $\delta_K(T)$ denote the determinant ideals of T considered as an element of $\mathfrak{o}\mathfrak{L}$ and $K\mathfrak{L}$ respectively, then we have $\delta_0(T) = \mathfrak{o}\delta(T)$ and $\delta_K(T) = K\delta(T)$. Evidently, $T(\mathfrak{M}) = \mathfrak{N}$ if and only if $\delta(T) = i$, and if \mathfrak{M} and \mathfrak{N} have the same rank, T is biunique if and only if $\delta(T) \neq 0$, so that in this case, T is an isomorphism of \mathfrak{M} onto \mathfrak{N} if and only if $\delta(T) = i$. Furthermore, it is easily seen that in the case where \mathfrak{M} and \mathfrak{N} have the same rank, $\delta_0(T) = \mathfrak{o} \cdot |T|$ and $\delta_K(T) = K \cdot |T|$.

LEMMA 2. *If T_1 and T_2 are in \mathfrak{L} , if*

$$T_1 \equiv T_2 \pmod{\mathfrak{a}\mathfrak{L}}$$

where \mathfrak{a} is an integral ideal of i , and if $\delta(T_1) + \mathfrak{a} = i$, then $\delta(T_2) + \mathfrak{a} = i$.

Proof. We may evidently exclude the case $\mathfrak{a} = 0$ where the statement is trivially true.

Since $\delta(T_1) + \mathfrak{a} = i$, $\mathfrak{N} = i\mathfrak{N} = \delta(T_1)\mathfrak{N} + \mathfrak{a}\mathfrak{N} \subseteq T_1(\mathfrak{M}) + \mathfrak{a}\mathfrak{N}$, so that $\mathfrak{N} = T_1(\mathfrak{M}) + \mathfrak{a}\mathfrak{N}$. But

$$T_1 \equiv T_2 \pmod{\mathfrak{a}\mathfrak{L}}$$

means that $T_1(\mathfrak{M}) + \mathfrak{a}\mathfrak{N} = T_2(\mathfrak{M}) + \mathfrak{a}\mathfrak{N}$, so that $\mathfrak{N} = T_2(\mathfrak{M}) + \mathfrak{a}\mathfrak{N}$. Let us assume that \mathfrak{o} is the ring of all elements of K that are regular with respect to each of the prime ideal divisors of \mathfrak{a} . We have $\mathfrak{o}\mathfrak{N} = T_2(\mathfrak{o}\mathfrak{M}) + (\mathfrak{o}\alpha)(\mathfrak{o}\mathfrak{N})$.

Since \mathfrak{o} is a principal ideal domain, there is a basis u_1, \dots, u_n of $\mathfrak{o}\mathfrak{N}$ over \mathfrak{o} such that $\alpha_1 u_1, \dots, \alpha_n u_n$ is a basis of $T_2(\mathfrak{o}\mathfrak{M})$ over \mathfrak{o} , where the α_i are in \mathfrak{o} . Then

$$\mathfrak{o}\mathfrak{N} = \sum_{i=1}^n (\mathfrak{o}\alpha + (\alpha_i))u_i$$

so that $\mathfrak{o}\alpha + (\alpha_i) = \mathfrak{o}$ for $i = 1, 2, \dots, n$. But since

$$\frac{\mathfrak{o}\mathfrak{N}}{T_2(\mathfrak{o}\mathfrak{M})} \cong \sum_{i=1}^n \frac{\mathfrak{o}u_i}{\mathfrak{o}\alpha_i u_i} \quad (\text{direct sum}),$$

$\delta_0(T_2) = \mathfrak{o}\alpha_1\alpha_2 \dots \alpha_n$, so that $\mathfrak{o}(\delta(T_2) + \mathfrak{a}) = \delta_0(T_2) + \mathfrak{o}\mathfrak{a} = \mathfrak{o}$. Then, because of the choice of \mathfrak{o} , $\mathfrak{a} + \delta(T_2) = \mathfrak{i}$.

4. Representations of finite groups over Dedekind rings. Let A be an algebra with unity element, of finite dimension over K , let \mathfrak{F} be an \mathfrak{i} -order of A and let $\mathfrak{D} = \mathfrak{o}\mathfrak{F}$.

We propose to study representations of \mathfrak{F} by rings of \mathfrak{i} -endomorphisms of finitely generated torsion free \mathfrak{i} -modules, that map the unity element of \mathfrak{F} onto the identity transformation, i.e., we propose to study \mathfrak{F} -modules that are finitely generated and torsion free over \mathfrak{i} .

If \mathfrak{M} is such an \mathfrak{F} -module, then there is a unique way of defining $K\mathfrak{M}$ and $\mathfrak{o}\mathfrak{M}$ as an A -module and an \mathfrak{D} -module respectively so that they are extensions of the \mathfrak{F} -module \mathfrak{M} , explicitly, by setting $(a/\alpha)(u/\beta) = (au/\alpha\beta)$ for all $a \in \mathfrak{F}$, all $u \in \mathfrak{M}$ and all $\alpha, \beta \in \mathfrak{i}$, $\alpha \neq 0 \neq \beta$.

Two \mathfrak{F} -modules \mathfrak{M} and \mathfrak{N} will be said to be \mathfrak{i} -equivalent if they are \mathfrak{F} -isomorphic; they will be said to be K -equivalent if $K\mathfrak{M}$ and $K\mathfrak{N}$ are A -isomorphic and \mathfrak{o} -equivalent if $\mathfrak{o}\mathfrak{M}$ and $\mathfrak{o}\mathfrak{N}$ are \mathfrak{D} -isomorphic.

Let \mathfrak{S} be a class of K -equivalent \mathfrak{F} -modules, complete in the sense that if an \mathfrak{F} -module \mathfrak{M} is K -equivalent to an \mathfrak{F} -module in \mathfrak{S} , then \mathfrak{M} is \mathfrak{i} -equivalent to an \mathfrak{F} -module in \mathfrak{S} , and let m denote the common rank of the \mathfrak{i} -modules in \mathfrak{S} . Let \mathfrak{R} denote the partition of \mathfrak{S} into complete subclasses of \mathfrak{i} -equivalent \mathfrak{F} -modules, and if \mathfrak{o} is the ring of all elements of K that are regular with respect to each of the prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ of \mathfrak{i} , let $\mathfrak{R}(\mathfrak{p}_1, \dots, \mathfrak{p}_r)$ denote the partition of \mathfrak{S} into complete subclasses of \mathfrak{o} -equivalent \mathfrak{F} -modules. Finally, let \mathfrak{r} and $\mathfrak{r}(\mathfrak{p}_1, \dots, \mathfrak{p}_r)$ denote the number of subclasses of \mathfrak{S} determined by \mathfrak{R} and $\mathfrak{R}(\mathfrak{p}_1, \dots, \mathfrak{p}_r)$ respectively.

THEOREM 5. *If \mathfrak{M} and \mathfrak{N} are two \mathfrak{F} -modules in \mathfrak{S} , then*

$$\mathfrak{M} \equiv \mathfrak{N} \pmod{\mathfrak{R}(\mathfrak{p}_1, \dots, \mathfrak{p}_r)}$$

if and only if there is an \mathfrak{F} -homomorphism T of \mathfrak{M} into \mathfrak{N} for which $\delta(T) + \mathfrak{p}_i = \mathfrak{i}$ for $i = 1, 2, \dots, r$.

Proof. Since \mathfrak{M} and \mathfrak{N} have the same rank,

$$\mathfrak{M} \equiv \mathfrak{N} \pmod{\mathfrak{R}(\mathfrak{p}_1, \dots, \mathfrak{p}_r)}$$

if and only if there is an \mathfrak{D} -homomorphism T of $\mathfrak{o}\mathfrak{M}$ into $\mathfrak{o}\mathfrak{N}$ for which $(\mathfrak{o}\mathfrak{N} : T(\mathfrak{o}\mathfrak{M})) = \mathfrak{o}$, and we may evidently assume that T maps \mathfrak{M} into \mathfrak{N} . But it is also evident that T is \mathfrak{D} -admissible if and only if it is \mathfrak{F} -admissible, when considered as a mapping of \mathfrak{M} into \mathfrak{N} , and since $\delta_0(T) = (\mathfrak{o}\mathfrak{N} : T(\mathfrak{o}\mathfrak{M})) = \mathfrak{o}(\mathfrak{N} : T(\mathfrak{M})) = \mathfrak{o}\delta(T)$, $\delta_0(T) = \mathfrak{o}$ if and only if $\delta(T) + \mathfrak{p}_i = \mathfrak{i}$ for $i = 1, 2, \dots, r$.

THEOREM 6. *If each prime ideal $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ is different from each prime ideal $\mathfrak{q}_1, \dots, \mathfrak{q}_s$, then*

$$\mathfrak{R}(\mathfrak{p}_1, \dots, \mathfrak{p}_r, \mathfrak{q}_1, \dots, \mathfrak{q}_s) = \mathfrak{R}(\mathfrak{p}_1, \dots, \mathfrak{p}_r) \cap \mathfrak{R}(\mathfrak{q}_1, \dots, \mathfrak{q}_s)$$

Proof. It is clear, from the preceding theorem, that

$$\mathfrak{R}(p_1, \dots, p_r, q_1, \dots, q_s) \subseteq \mathfrak{R}(p_1, \dots, p_r) \cap \mathfrak{R}(q_1, \dots, q_s)$$

Suppose that \mathfrak{M} and \mathfrak{N} are \mathfrak{F} -modules in \mathfrak{S} and that

$$\mathfrak{M} \equiv \mathfrak{N} \pmod{\mathfrak{R}(p_1, \dots, p_r) \cap \mathfrak{R}(q_1, \dots, q_s)}$$

This means that there are \mathfrak{F} -homomorphisms T_1 and T_2 of \mathfrak{M} into \mathfrak{N} for which

$$\delta(T_1) + p_i = i \ (i = 1, 2, \dots, r), \quad \delta(T_2) + q_j = i \ (j = 1, 2, \dots, s).$$

Since $p_1 p_2 \dots p_r$ is relatively prime to $q_1 q_2 \dots q_s$, we may set $1 = \alpha_1 + \alpha_2$, where $\alpha_1 \in p_1 p_2 \dots p_r$ and $\alpha_2 \in q_1 q_2 \dots q_s$. Then if we set $T = \alpha_1 T_2 + \alpha_2 T_1$, T is an \mathfrak{F} -homomorphism of \mathfrak{M} into \mathfrak{N} , and furthermore, if \mathfrak{L} denotes the i -module of all \mathfrak{F} -homomorphisms of \mathfrak{M} into \mathfrak{N} ,

$$T \equiv T_1 \pmod{p_1 p_2 \dots p_r \mathfrak{L}}, \quad T \equiv T_2 \pmod{q_1 q_2 \dots q_s \mathfrak{L}},$$

so that by Lemma 2,

$$\delta(T) + p_i = i \ (i = 1, 2, \dots, r), \quad \delta(T) + q_j = i \ (j = 1, 2, \dots, s).$$

Therefore

$$\mathfrak{M} \equiv \mathfrak{N} \pmod{\mathfrak{R}(p_1, \dots, p_r, q_1, \dots, q_s)}$$

THEOREM 7. *If \mathfrak{M} and \mathfrak{N} are \mathfrak{F} -modules in \mathfrak{S} , and if each prime ideal p_1, \dots, p_r is different from each prime ideal q_1, \dots, q_s , then there is an \mathfrak{F} -module $\mathfrak{M}' \in \mathfrak{S}$ such that*

$$\mathfrak{M} \equiv \mathfrak{M}' \pmod{\mathfrak{R}(p_1, \dots, p_r)}, \quad \mathfrak{M}' \equiv \mathfrak{N} \pmod{\mathfrak{R}(q_1, \dots, q_s)}.$$

Proof. Since \mathfrak{M} and \mathfrak{N} are K -equivalent, there is an A -isomorphism T of $K\mathfrak{M}$ onto $K\mathfrak{N}$, and we may evidently assume that T maps \mathfrak{M} into \mathfrak{N} .

Let \mathfrak{o} be the ring of all elements of K that are regular with respect to the prime ideal divisors of $\delta(T) = (\mathfrak{N}: T(\mathfrak{M}))$.

Since \mathfrak{o} is a principal ideal domain, there is a basis u_1, \dots, u_m of $\mathfrak{o}\mathfrak{N}$ such that $\alpha_1 u_1, \dots, \alpha_m u_m$ is a basis of $T(\mathfrak{o}\mathfrak{M})$, where the α_i are in \mathfrak{o} , and furthermore, since T is non-singular, $\delta_{\mathfrak{o}}(T) = \mathfrak{o}\alpha_1 \alpha_2 \dots \alpha_m \neq 0$. We may even assume that the α_i are in \mathfrak{i} .

Let $\mathfrak{o}\alpha_i = \mathfrak{B}_i \mathfrak{C}_i$, where the \mathfrak{B}_i and \mathfrak{C}_i are integral ideals of \mathfrak{o} such that $\mathfrak{B}_i + \mathfrak{C}_i = \mathfrak{o}$, $\mathfrak{B}_i + \mathfrak{o}p_j = \mathfrak{o}$ and $\mathfrak{C}_i + \mathfrak{o}q_k = \mathfrak{o}$ for $i = 1, 2, \dots, m$, $j = 1, 2, \dots, r$ and $k = 1, 2, \dots, s$. Let \mathfrak{B} denote the intersection of the \mathfrak{B}_i . Then since

$$\mathfrak{D}(\mathfrak{B}^{-1}T(\mathfrak{o}\mathfrak{M})) = \mathfrak{B}^{-1}(\mathfrak{D}T(\mathfrak{o}\mathfrak{M})) \subseteq \mathfrak{B}^{-1}T(\mathfrak{o}\mathfrak{M}),$$

$\mathfrak{B}^{-1}T(\mathfrak{o}\mathfrak{M})$ is an \mathfrak{D} -module.

Let $\mathfrak{M}' = \mathfrak{N} \cap \mathfrak{B}^{-1}T(\mathfrak{o}\mathfrak{M})$. Then \mathfrak{M}' is surely an \mathfrak{F} -module, and since

$$\mathfrak{o}\mathfrak{M}' = \mathfrak{o}\mathfrak{N} \cap \mathfrak{B}^{-1}T(\mathfrak{o}\mathfrak{M}) = \sum_{i=1}^m (\mathfrak{o} \cap \mathfrak{B}^{-1}\alpha_i)u_i$$

$\mathfrak{o}\mathcal{M}'$ has the same rank as $\mathfrak{o}\mathcal{N}$ so that \mathcal{M}' has the same rank as \mathcal{N} and therefore, \mathcal{M}' is an \mathfrak{S} -module in \mathfrak{S} . But since $\mathfrak{B}\mathfrak{B}_i^{-1} + \mathfrak{C}_i = \mathfrak{o}$, $\mathfrak{B}\alpha_i^{-1} + \mathfrak{o} = \mathfrak{C}_i^{-1}$, so that $\mathfrak{B}^{-1}\alpha_i \cap \mathfrak{o} = \mathfrak{C}_i$ and therefore

$$\mathfrak{o}\mathcal{M}' = \sum_{i=1}^m \mathfrak{C}_i u_i$$

Since $T(\mathcal{M}) \subseteq \mathcal{M}'$, T may be considered as an \mathfrak{S} -homomorphism of \mathcal{M} into \mathcal{M}' whose determinant ideal is $(\mathcal{M}' : T(\mathcal{M}))$. But $\mathfrak{o}(\mathcal{M}' : T(\mathcal{M})) = (\mathfrak{o}\mathcal{M}' : T(\mathfrak{o}\mathcal{M})) = \mathfrak{B}_1\mathfrak{B}_2 \dots \mathfrak{B}_m$ so that

$$\mathfrak{o}((\mathcal{M}' : T(\mathcal{M})) + \mathfrak{p}_j) = \mathfrak{o}(\mathcal{M}' : T(\mathcal{M})) + \mathfrak{o}\mathfrak{p}_j = \mathfrak{B}_1\mathfrak{B}_2 \dots \mathfrak{B}_m + \mathfrak{o}\mathfrak{p}_j = \mathfrak{o},$$

and therefore, because of the choice of \mathfrak{o} ,

$$(\mathcal{M}' : T(\mathcal{M})) + \mathfrak{p}_j = \mathfrak{i}$$

and this for $j = 1, 2, \dots, r$. Therefore

$$\mathcal{M} \equiv \mathcal{M}' \pmod{\mathfrak{R}(\mathfrak{p}_1, \dots, \mathfrak{p}_r)}$$

Furthermore, the determinant ideal of the identity mapping of \mathcal{M}' into \mathcal{N} is $(\mathcal{N} : \mathcal{M}')$ and since

$$\begin{aligned} \mathfrak{o}(\mathcal{N} : \mathcal{M}') &= (\mathfrak{o}\mathcal{N} : \mathfrak{o}\mathcal{M}') = \mathfrak{C}_1\mathfrak{C}_2 \dots \mathfrak{C}_m, \mathfrak{o}((\mathcal{N} : \mathcal{M}') + \mathfrak{q}_k) \\ &= \mathfrak{C}_1\mathfrak{C}_2 \dots \mathfrak{C}_m + \mathfrak{o}\mathfrak{q}_k = \mathfrak{o} \end{aligned}$$

so that by the choice of \mathfrak{o} ,

$$((\mathcal{N} : \mathcal{M}') + \mathfrak{q}_k) = \mathfrak{i}, \quad k = 1, 2, \dots, s,$$

and therefore

$$\mathcal{M}' \equiv \mathcal{N} \pmod{\mathfrak{R}(\mathfrak{q}_1, \dots, \mathfrak{q}_s)}.$$

COROLLARY.

$$\mathfrak{r}(\mathfrak{p}_1, \dots, \mathfrak{p}_r, \mathfrak{q}_1, \dots, \mathfrak{q}_s) = \mathfrak{r}(\mathfrak{p}_1, \dots, \mathfrak{p}_r) \cdot \mathfrak{r}(\mathfrak{q}_1, \dots, \mathfrak{q}_s)$$

Theorems 6 and 7 may evidently be extended by induction so that

$$\mathfrak{R}(\mathfrak{p}_1, \dots, \mathfrak{p}_r) = \prod_{i=1}^r \mathfrak{R}(\mathfrak{p}_i)$$

and

$$\mathfrak{r}(\mathfrak{p}_1, \dots, \mathfrak{p}_r) = \prod_{i=1}^r \mathfrak{r}(\mathfrak{p}_i)$$

DEFINITION. *Two \mathfrak{S} -modules \mathcal{M} and \mathcal{N} will be said to be of the same genus² if \mathcal{M} and \mathcal{N} are \mathfrak{o} -equivalent for every ring \mathfrak{o} of all elements of K that are regular with respect to a single prime ideal of \mathfrak{i} .*

²We could say that \mathcal{M} and \mathcal{N} are of the same genus if the corresponding representations are unimodularly equivalent over all \mathfrak{P} -adic extensions of K , but because of Corollary 1 of Theorem 1, this is equivalent to the above definition.

Let \mathfrak{R}_ρ denote the partition of \mathfrak{S} into complete subclasses of \mathfrak{F} -modules of the same genus. Then, by definition,

$$\mathfrak{R}_\rho = \bigcap_{\mathfrak{p}} R(\mathfrak{p})$$

where the intersection extends over all prime ideals \mathfrak{p} of \mathfrak{i} . Let \mathfrak{r}_ρ denote the number of subclasses of \mathfrak{S} determined by \mathfrak{R}_ρ .

From now on, we will assume that A, \mathfrak{D} and \mathfrak{F} are the group rings of the finite group \mathfrak{G} of order N over K, \mathfrak{o} and \mathfrak{i} respectively.

Let $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ be the prime ideal divisors of N in \mathfrak{i} . By Theorem 4, we know that if \mathfrak{p} does not divide N and if \mathfrak{o} is the ring of all \mathfrak{p} -regular elements of K , then two \mathfrak{F} -modules are \mathfrak{o} -equivalent if and only if they are K -equivalent, so that in this case, $\mathfrak{R}(\mathfrak{p})$ determines only one subclass of \mathfrak{S} , namely \mathfrak{S} itself. Therefore

$$\mathfrak{R}_\rho = \bigcap_{i=1}^r \mathfrak{R}(\mathfrak{p}_i) = \mathfrak{R}(\mathfrak{p}_1, \dots, \mathfrak{p}_r), \quad \mathfrak{r}_\rho = \prod_{i=1}^r \mathfrak{r}(\mathfrak{p}_i).$$

Now let \mathfrak{a} be a non-null integral ideal of \mathfrak{i} and let \mathfrak{M} be an \mathfrak{F} -module in \mathfrak{S} . Since $\mathfrak{F}(\mathfrak{a}\mathfrak{M}) = \mathfrak{a}(\mathfrak{F}\mathfrak{M}) \subseteq \mathfrak{a}\mathfrak{M}$, $\mathfrak{a}\mathfrak{M}$ is an \mathfrak{F} -submodule of $K\mathfrak{M}$, and since $\mathfrak{a}\mathfrak{M}$ has the same rank as \mathfrak{M} , $\mathfrak{a}\mathfrak{M} \in \mathfrak{S}$. Then there is a non-null integral ideal \mathfrak{b} of \mathfrak{i} such that $\mathfrak{a}\mathfrak{b} = (\alpha), \alpha \in \mathfrak{i}, \alpha \neq 0$ and $\mathfrak{b} + (N) = \mathfrak{i}$. The function T mapping each $u \in \mathfrak{M}$ onto αu is an \mathfrak{F} -homomorphism of \mathfrak{M} into $\mathfrak{a}\mathfrak{M}$ and since

$$(\mathfrak{M} : \alpha\mathfrak{M}) = (\mathfrak{M} : \mathfrak{a}\mathfrak{M})(\mathfrak{a}\mathfrak{M} : \alpha\mathfrak{M}), \quad \alpha^m = \mathfrak{a}^m \cdot \delta(T),$$

so that $\delta(T) = \mathfrak{b}^m$ and therefore

$$\mathfrak{M} \equiv \mathfrak{a}\mathfrak{M} \pmod{\mathfrak{R}_\rho}.$$

Now let us assume that the \mathfrak{F} -modules $\mathfrak{M} \in \mathfrak{S}$ are such that the representations of A belonging to $K\mathfrak{M}$ are absolutely irreducible. Let \mathfrak{M} and \mathfrak{N} be two \mathfrak{F} -modules in \mathfrak{S} and suppose that

$$\mathfrak{M} \equiv \mathfrak{N} \pmod{\mathfrak{R}_\rho}.$$

This means that there is an \mathfrak{F} -homomorphism T of \mathfrak{M} into \mathfrak{N} for which $\delta(T) + (N) = \mathfrak{i}$. Let

$$\delta(T) = \mathfrak{q}_1^{f_1} \mathfrak{q}_2^{f_2} \dots \mathfrak{q}_s^{f_s}$$

be the decomposition of $\delta(T)$ into prime ideals in \mathfrak{i} . Since the representations of \mathfrak{G} belonging to $K\mathfrak{M}$ and $K\mathfrak{N}$ are absolutely irreducible, they are irreducible over the \mathfrak{P} -adic extensions of K determined by the \mathfrak{q}_j , so that by the corollary to Theorem 3, each f_j is divisible by m and

$$T \in \mathfrak{q}_j^{f_j/m} \cdot \mathfrak{F}.$$

If we set

$$\mathfrak{b} = \mathfrak{q}_1^{f_1/m} \cdot \mathfrak{q}_2^{f_2/m} \dots \mathfrak{q}_s^{f_s/m},$$

we have $T \in \mathfrak{b}\mathfrak{L}$ and $\delta(T) = \mathfrak{b}^m$. Therefore $T(\mathfrak{M}) \subseteq \mathfrak{b}\mathfrak{N}$ and since

$$\mathfrak{b}^m = \delta(T) = (\mathfrak{N}: T(\mathfrak{M})) = (\mathfrak{N}: \mathfrak{b}\mathfrak{N})(\mathfrak{b}\mathfrak{N}: T(\mathfrak{M})) = \mathfrak{b}^m(\mathfrak{b}\mathfrak{N}: T(\mathfrak{M})),$$

$$(\mathfrak{b}\mathfrak{N}: T(\mathfrak{M})) = \mathfrak{i},$$

so that $T(\mathfrak{M}) = \mathfrak{b}\mathfrak{N}$.

Let \mathfrak{S}' be a complete subclass of \mathfrak{S} determined by \mathfrak{R}_ν and let \mathfrak{M} be an \mathfrak{F} -module in \mathfrak{S}' . By the preceding argument, we may assume that \mathfrak{S}' just consists of all the \mathfrak{F} -modules $\mathfrak{b}\mathfrak{M}$ where \mathfrak{b} is a non-null integral ideal of \mathfrak{i} . If \mathfrak{b} and \mathfrak{b}' are two such ideals of \mathfrak{i} and if \mathfrak{b} and \mathfrak{b}' are in the same ideal class, then there is an $\alpha \in K, \alpha \neq 0$ such that the mapping $\beta \rightarrow \alpha\beta$, for all $\beta \in \mathfrak{b}$, is an \mathfrak{i} -isomorphism of \mathfrak{b} onto \mathfrak{b}' . Then it is easily seen that the mapping $u \rightarrow \alpha u$, for all $u \in \mathfrak{b}\mathfrak{M}$, is an \mathfrak{F} -isomorphism of $\mathfrak{b}\mathfrak{M}$ onto $\mathfrak{b}'\mathfrak{M}$.

Conversely, if T is an \mathfrak{F} -isomorphism of $\mathfrak{b}\mathfrak{M}$ onto $\mathfrak{b}'\mathfrak{M}$, since the representation of A belonging to $K\mathfrak{M} = K\mathfrak{b}\mathfrak{M} = K\mathfrak{b}'\mathfrak{M}$ is absolutely irreducible, it follows that T multiplies each element of $\mathfrak{b}\mathfrak{M}$ by some scalar $\alpha \in K, \alpha \neq 0$, so that $\mathfrak{b}'\mathfrak{M} = \alpha\mathfrak{b}\mathfrak{M}$ and therefore, $\mathfrak{b}' = \alpha\mathfrak{b}$, i.e., \mathfrak{b} and \mathfrak{b}' are in the same ideal class.

THEOREM 8. *If each \mathfrak{F} -module $\mathfrak{M} \in \mathfrak{S}$ is such that the representation of A belonging to $K\mathfrak{M}$ is absolutely irreducible, then $\mathfrak{r} = h\mathfrak{r}_\nu$, where h is the number of classes of isomorphic ideals of \mathfrak{i} .*

If \mathfrak{i} is the ring of algebraic integers of an algebraic number field K , then h is finite and also, since each integral ideal of \mathfrak{i} has a finite index in \mathfrak{i} , by Lemma 2 of Theorem 1, each $\mathfrak{r}(\mathfrak{p}_i)$ is finite, so that if \mathfrak{S} satisfies the condition of Theorem 8, the number

$$\mathfrak{r} = \mathfrak{h} \prod_{i=1}^r \mathfrak{r}(\mathfrak{p}_i)$$

is finite.

REFERENCES

1. I. Kaplansky, *Modules over Dedekind rings and valuation rings*, Trans. Amer. Math. Soc., 72 (1952), 327-340.
2. J.-M. Maranda, *On \mathfrak{P} -adic integral representations of finite groups*, Can. J. Math., 5 (1953), 344-355.
3. I. Schur, *Arithmetische Untersuchungen über endliche Gruppen linearer Substitutionen*, Berl. Ber. (1906), 164-184.
4. E. Steinitz, *Rechteckige Systeme und Moduln in algebraischen Zahlkörpern*, Math. Ann. I, 71 (1911), 328-354, II, 72 (1912), 297-345.
5. H. Zassenhaus, *Neuer Beweis der Endlichkeit der Klassenzahl bei unimodularer Äquivalenz endlicher ganzzahliger Substitutionsgruppen*, Abh. Math. Sem. Hansischen Univ. 12 (1938), 276-288.
6. ———, *The theory of groups* (New York, 1949).

Université de Montréal