ON THE RING OF INTEGERS IN AN ALGEBRAIC NUMBER FIELD AS A REPRESENTATION MODULE OF GALOIS GROUP

HIDEO YOKOI

1. Introduction. It is known that there are only three rationally inequivalent classes of indecomposable integral representations of a cyclic group of prime order l. The representations of these classes are:

(I) identical representation,

(II) rationally irreducible representation of degree $l-1$,

(III) indecomposable representation consisting of one identical representation and one rationally irreducible representation of degree $l-1$ (F. E. Diederichsen [1], I. Reiner [2]).

We now consider the special case where the representation module is the ring of algebraic integers of a number field and the operator group is a cyclic group of Galois automorphisms of prime order, and show that the multiplicity in this representation of indecomposable components belonging to each one of the above standing rationally inequivalent classes is determined by ramification numbers.[0)]

2. Theorem on the different. In this note, we denote by $\mathfrak{o}_\Omega$ for an algebraic number field Ω the ring of integers of Ω and by $D_{\Omega/L}$ for an extension Ω of an algebraic number field L the relative different of Ω/L.

The main aim of this article is to prove the following

THEOREM 1. *Let k be an algebraic number field of finite degree and K be a normal extension of k. Then the relative traces of all integers of K to k constitute an integral ideal of k and the ideal is characterized as the maximal divisor of k dividing the relative different $D_{K/k}$.*

We must first establish two lemmas.

Received August 5, 1959.

0) In the case of absolutely abelian number fields, some results in this note have recently been proved by H. W. Leopoldt [2a]. (This foot-not and [2a] are added September 15, 1959.)

LEMMA 1. *Let $\mathfrak{P}$ be any prime ideal of K and $\mathfrak{p}$ be the prime ideal of k contained in $\mathfrak{P}$. Denote by $K_{\mathfrak{P}}$ resp. $k_{\mathfrak{p}}$ the $\mathfrak{P}$-adic completion of K resp. the $\mathfrak{p}$-adic completion of k. Then the relative different $D_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}$ is characterized as the highest power of $\mathfrak{P}$ such that for any fixed natural number n we have $S_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}A \equiv 0$ mod. $\mathfrak{p}^n$ for every number A in $K_{\mathfrak{P}}$ with the congruence $A \equiv 0$ mod. $\mathfrak{p}^n \cdot (D_{K_{\mathfrak{P}}/k_{\mathfrak{p}}})^{-1}$.*

Proof. Since the set of traces $S_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}A$ of all elements in an ideal $\mathfrak{A}$ of the ring $\mathfrak{o}_{K_{\mathfrak{P}}}$ forms clearly an ideal of the ring $\mathfrak{o}_{k_{\mathfrak{p}}}$, we denote the ideal by $S_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}\mathfrak{A}$. Then we can prove that the ideal $S_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(\mathfrak{a} \cdot \mathfrak{A})$ coincides with the ideal $\mathfrak{a} \cdot S_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}\mathfrak{A}$ for any ideal $\mathfrak{a}$ resp. $\mathfrak{A}$ of $k_{\mathfrak{p}}$ resp. $K_{\mathfrak{P}}$. Namely, since all the ideals of $k_{\mathfrak{p}}$ are principal, the ideal $\mathfrak{a}$ of $k_{\mathfrak{p}}$ is generated by an element a of $k_{\mathfrak{p}}$, hence if A runs over all the elements of $\mathfrak{A}$, then $a \cdot A$ also runs over all the elements of the ideal $\mathfrak{a} \cdot \mathfrak{A}$. Therefore, our assertion follows at once from $S_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(a \cdot A) = a \cdot S_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}A$.

We next prove that we have $S_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(D_{K_{\mathfrak{P}}/k_{\mathfrak{p}}})^{-1} = \mathfrak{o}_{k_{\mathfrak{p}}}$. If we assume that $S_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(D_{K_{\mathfrak{P}}/k_{\mathfrak{p}}})^{-1}$ is not equal to $\mathfrak{o}_{k_{\mathfrak{p}}}$, but is equal to a proper subideal $\mathfrak{b}$ of $\mathfrak{o}_{k_{\mathfrak{p}}}$, then it follows from the above result that $S_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(D_{K_{\mathfrak{P}}/k_{\mathfrak{p}}} \cdot \mathfrak{b})^{-1}$ is equal to $\mathfrak{o}_{k_{\mathfrak{p}}}$, which is contrary to the fact that the different $D_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}$ is the highest power of $\mathfrak{P}$ such that the inverse of every element in it has an integral trace with respect to $K_{\mathfrak{P}}/k_{\mathfrak{p}}$.

Lemma 1 follows immediately from these two assertions.

LEMMA 2.[1] *Let e be the ramification order of $\mathfrak{P}$ with respect to $K_{\mathfrak{P}}/k_{\mathfrak{p}}$, and put $D_{K_{\mathfrak{P}}/k_{\mathfrak{p}}} = \mathfrak{p}^r \cdot \mathfrak{P}^s$ $(e > s \geqq 0,\ r \geqq 0)$. Then we have $S_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}\mathfrak{o}_{K_{\mathfrak{P}}} = \mathfrak{p}^r$.*

Proof. By Lemma 1 we have $S_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}A \equiv 0$ mod. $\mathfrak{p}^r$ for every number A in $K_{\mathfrak{P}}$ such that

$$A \equiv 0 \text{ mod. } \mathfrak{p}^r \cdot (D_{K_{\mathfrak{P}}/k_{\mathfrak{p}}})^{-1} \text{ i.e. mod. } \mathfrak{P}^{-s}.$$

In particular, we have $S_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}A_0 \equiv 0$ mod. $\mathfrak{p}^r$ for every integer A_0 of $\mathfrak{o}_{K_{\mathfrak{P}}}$.

---

[1] A. Speiser and E. Noether have proved the following theorem on *integral normal basis:* When $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ is normal, there exists an integral normal basis of $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ if and only if the ramification group is trivial, i.e. $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ is tamely ramified (A. Speiser [3], E. Noether [4]).

Lemma 2 together with this theorem implies that there exists an integral normal basis of $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ if and only if the 0-dimensional Galois cohomology group of $\mathfrak{o}_{K_{\mathfrak{P}}}$ with respect to $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ is trivial (cf. Corollary 1).

On the other hand, by Lemma 1, there is an integer B of $\mathfrak{o}_{K_\mathfrak{P}}$ such that $B \equiv 0 \bmod. \mathfrak{p}^{r+1} \cdot \mathfrak{P}^{-(er+e)}$ i.e. mod. $\mathfrak{P}^0$, but $S_{K_\mathfrak{P}/k_\mathfrak{p}} B \not\equiv 0 \bmod. \mathfrak{p}^{r+1}$.

Since the set of traces $S_{K_\mathfrak{P}/k_\mathfrak{p}} A$ of all integers A in $K_\mathfrak{P}$ forms an ideal of $\mathfrak{o}_{k_\mathfrak{p}}$, our lemma is proved.

Proof of Theorem 1. Let $\mathfrak{p} = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$ be the decomposition of a prime $\mathfrak{p}$ of k into powers of distinct prime divisors in K, and $\mathfrak{a}$ be the ideal $S_{K/k}\mathfrak{o}_K$. Denote by r the exponent of $\mathfrak{p}$ in $D_{K/k}$ ($\mathfrak{p}^r \| D_{K/k}$ in notation). Then from Lemma 2 and the product theorem of different,[2] it follows that $S_{K_{\mathfrak{P}_i}/k_\mathfrak{p}} A \equiv 0 \bmod. \mathfrak{p}^r$ for every $i = 1, 2, \ldots, g$ and for any integer A of $\mathfrak{o}_K$, and hence we obtain the following congruence:

$$S_{K/k} A = \sum_{i=1}^{g} S_{K_{\mathfrak{P}_i}/k_\mathfrak{p}} A \equiv 0 \qquad \bmod. \mathfrak{p}^r$$

for every integer A of $\mathfrak{o}_K$. On the other hand, by Lemma 2, there are g integers A_i of $K_{\mathfrak{P}_i}$ such that $S_{K_{\mathfrak{P}_1}/k_\mathfrak{p}} A_1 \not\equiv 0 \bmod. \mathfrak{p}^{r+1}$, and $S_{K_{\mathfrak{P}_i}/k_\mathfrak{p}} A_i \equiv 0 \bmod. \mathfrak{p}^{r+1}$ for $i = 2, 3, \ldots, g$. For these numbers A_i, there is an integer B of K such that we have $B \equiv A_i \bmod. \mathfrak{P}_i^{(r+1)e_i}$ for every $i = 1, 2, \ldots, g$, hence we have

$$S_{K_{\mathfrak{P}_1}/k_\mathfrak{p}} B \equiv S_{K_{\mathfrak{P}_1}/k_\mathfrak{p}} A_1 \not\equiv 0 \qquad \bmod. \mathfrak{p}^{r+1}$$
$$S_{K_{\mathfrak{P}_i}/k_\mathfrak{p}} B \equiv S_{K_{\mathfrak{P}_i}/k_\mathfrak{p}} A_i \equiv 0 \qquad \bmod. \mathfrak{p}^{r+1}$$

for $i = 2, 3, \ldots, g$.

Consequently, we have $S_{K/k} B = \sum_{i=1}^{g} S_{K_{\mathfrak{P}_i}/k_\mathfrak{p}} B \not\equiv 0 \bmod. \mathfrak{p}^{r+1}$. Since this is true for any prime ideal $\mathfrak{p}$ of k, our theorem is proved.[3] [4]

---

[2] The product of the differents of local fields coincides with the different of the grobal field.

[3] The theorem on integral normal basis corresponding to footnote 1 is not always true in grobal fields, but it is true in absolutely abelian number fields (cf. H. W. Leopoldt [2 a]).

[4] We can also give a well-known bound of ramification number from Theorem 1 in the following way.

Let K/k be a cyclic extension of prime degree p over an algebraic number field k, $\mathfrak{p}$ be a prime divisor of p in k and let $\mathfrak{p} = \mathfrak{P}^v$ be the prime decomposition of $\mathfrak{p}$ in K. Then the relative different $D_{K/k}$ has $\mathfrak{P}^{v(p-1)}$ as its $\mathfrak{P}$-component, where v is the ramification number of $\mathfrak{P}$ in K/k, namely, the maximal exponent of $\mathfrak{P}$ such that we have $A \equiv A^\sigma \bmod. \mathfrak{P}^v$ for every integer A of $\mathfrak{o}_K$ and for any Galois automorphism σ of K/k. Furthermore, let e be the ramification order of $\mathfrak{p}$ in k/P, where P is the rational number field and $\mathfrak{p}^r$ be the $\mathfrak{p}$-component of $S_{K/k}\mathfrak{o}_K (\mathfrak{p}^r \| S_{K/k}\mathfrak{o}_K)$, then $p \in S_{K/k}\mathfrak{o}_K \subseteq \mathfrak{p}^r$ implies $r \leqq e$. From Theorem 1, we see that $v(p-1) < p(r+1)$, namely $v < 1 + pr/(p-1) + 1/(p-1)$, and since v is a natural number, we have $v \leqq 1 + pr/(p-1) \leqq 1 + pe/(p-1)$ (cf. T. Takagi [5], H. Hasse [6]).

We can deduce from Theorem 1 the following two corollaries, but we do not use them in this paper.

COROLLARY 1. *Under the same conditions in Theorem* 1, *the* 0*-dimensional Galois cohomology group of* $\mathfrak{o}_K$ *with respect to* K/k *is trivial if and only if* K/k *is tamely ramified at every prime ideal of* k.[5]

Proof. By the well-known theorem of different,[6] a prime ideal $\mathfrak{p}$ of k divides $D_{K/k}$ if and only if K/k is not tamely ramified at $\mathfrak{p}$. Hence our lemma is clear from Theorem 1.

COROLLARY 2. *Under the same conditions in Theorem* 1, *if we assume moreover that the* 0*-dimensional Galois cohomology group of* $\mathfrak{o}_K$ *with respect to* K/k *is trivial, then the Galois cohomology group of* $\mathfrak{o}_K$ *with respect to* K/Ω *is trivial for every dimension and for any intermediate field* Ω *of* K/k.[7]

Proof. If K/k is tamely ramified at $\mathfrak{p}$, then K/Ω is also tamely ramified at $\mathfrak{p}$ for any intermediate field Ω of K/k. Hence, by Corollary 1, the assertion of our lemma implies that the 0-dimensional Galois cohomology group of $\mathfrak{o}_K$ with respect to K/Ω is also trivial.

Let $\mathfrak{H}$ be the Galois group of K/Ω and put $A=\sum_{\tau\in\mathfrak{H}}\alpha^{\tau}f_{\tau}$ for any integer $\alpha\neq 0$ in $\mathfrak{o}_K$ and for any 1-cocycle $\{f_{\tau}\}$ $(\tau\in\mathfrak{H})$ of $\mathfrak{H}$ in $\mathfrak{o}_K$. Then we have $A-A^{\sigma}=(S_{K/\Omega}\alpha)\cdot f_{\sigma}$ for any σ in $\mathfrak{H}$. In particular, since we may take the integer α with $S_{K/\Omega}\alpha=1$ from the above assertion, we may write $f_{\sigma}=A-A^{\sigma}$ with an integer A in $\mathfrak{o}_K$ for every 1-cocycle $\{f_{\sigma}\}$ $(\sigma\in\mathfrak{H})$ of $\mathfrak{H}$ in $\mathfrak{o}_K$. This shows that the 1-dimensional Galois cohomology group of $\mathfrak{o}_K$ with respect to K/Ω is trivial for any intermediate field Ω of K/k. Therefore, from the well-known theorem of cohomology group[8] we obtain our lemma.

---

[5] Cf. E. Artin [7].

[6] Cf. H. Hasse [8].

[7] This corollary is of course true for local fields, and it yields the results described in footnotes 1 and 3 purely cohomologically in the following way. The 0-dimensional Galois cohomology group of $\mathfrak{o}_K$ (resp. $\mathfrak{o}_{K_{\mathfrak{P}}}$) with respect to K/k (resp. $K_{\mathfrak{P}}/k_{\mathfrak{p}}$) is trivial if and only if $\mathfrak{o}_K$ (resp. $\mathfrak{o}_{K_{\mathfrak{P}}}$) is $Z[\mathfrak{G}]$-projective, where $Z[\mathfrak{G}]$ is the group algebra of Galois group $\mathfrak{G}$ of K/k (resp. $K_{\mathfrak{P}}/k_{\mathfrak{p}}$) over the ring Z of rational integers. Therefore, in particular, there exists an integral normal basis of $K_{\mathfrak{P}}/k_{\mathfrak{p}}$, if the 0-dimensional Galois cohomology group of $\mathfrak{o}_{K_{\mathfrak{P}}}$ with respect to $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ (T. Nakayama [9]).

[8] Cf. T. Nakayama [10], G. Hochschild-T. Nakayama [11].

3. Principal results

THEOREM 2. *Let K be a normal extension of degree n over the rational number field P, and Ω be a subfield of K such that K/Ω is cyclic of prime degree l and that Ω/P is normal.*

Furthermore, let $v \geqq 1$ be the common ramification number with respect to K/Ω of all the prime divisors $\mathfrak{P}_i$ of l in K, and e be the common ramification order with respect to Ω/P of all the prime divisors $\mathfrak{l}_i$ of l in Ω. Let m be a non-negative rational integer such that $l(m-1) < v \leqq lm$, and put $n_0 = n/l$, $t = n_0(v-m)/e$. Then we have the following basis of the ring $\mathfrak{o}_K$:

$$\mathfrak{o}_K = [\beta_1, \ldots, \beta_{n_0(l-1)}, \omega_1, \ldots, \omega_t, \xi_1, \ldots, \xi_{n_0-t}]$$

with $\xi_i = (\omega_{t+i} + \alpha_i)/l$ $(i = 1, 2, \ldots, n_0 - t)$, where ω_j $(j = 1, 2, \ldots, n_0)$ is a suitable basis of $\mathfrak{o}_\Omega$, and α_i, β_k are integers of K such that

$$S_{K/\Omega}\alpha_i = 0,\ S_{K/\Omega}\beta_k = 0 \quad (i = 1, 2, \ldots, n_0 - t;\ k = 1, 2, \ldots, n_0(l-1)).^{9)}$$

Proof. Denote by $[D_{K/\Omega}]_{\mathfrak{P}_i}$ the exponent of $\mathfrak{P}_i$ in $D_{K/\Omega}$. Then we have $[D_{K/\Omega}]_{\mathfrak{P}_i} = v(l-1) = l(v-m) + (lm - v)$, $0 \leqq lm - v < l$, hence Theorem 1 implies that $S_{K/\Omega}\mathfrak{o}_K = \prod_{\mathfrak{l}_i | l} \mathfrak{l}_i^{v-m}$, where the product runs over all the prime divisors of l in Ω. Since Ω/P is normal by the assumption, the index of $S_{K/\Omega}\mathfrak{o}_K$ in $\mathfrak{o}_\Omega$ is equal to l^t:

$$[\mathfrak{o}_\Omega : S_{K/\Omega}\mathfrak{o}_K] = N_{\Omega/P}\prod_i \mathfrak{l}_i^{v-m} = l^{(v-m)n_0/e} = l^t.$$

Let $\mathfrak{o}_K^*$ be a submodule of $\mathfrak{o}_K$ which consists of all elements β in $\mathfrak{o}_K$ such that $S_{K/\Omega}\beta = 0$, and let $[\beta_1, \ldots, \beta_{n_0(l-1)}]$ be any basis of $\mathfrak{o}_K^*$. If we take the basis $[\beta_1, \ldots, \beta_{n_0(l-1)}, \eta_1, \ldots, \eta_{n_0}]$ of $\mathfrak{o}_K$ which contains the basis $[\beta_1, \ldots, \beta_{n_0(l-1)}]$ of $\mathfrak{o}_K^*$ obtained above, then $[S_{K/\Omega}\eta_1, \ldots, S_{K/\Omega}\eta_{n_0}]$ forms a basis of $S_{K/\Omega}\mathfrak{o}_K$.

On the other hand, since we may choose a basis $[\omega_1, \ldots, \omega_{n_0}]$ of $\mathfrak{o}_\Omega$ in such a way that $[\omega_1' = l\omega_1, \ldots, \omega_t' = l\omega_t, \omega_{t+1}' = \omega_{t+1}, \ldots, \omega_{n_0}' = \omega_{n_0}]$ forms a basis of $S_{K/\Omega}\mathfrak{o}_K$, there is a unimodular $n_0 \times n_0$ matrix $U = (u_{ij})$ with integral coefficients such that

$$\omega_i' = \sum_{j=1}^{n_0} u_{ij} S_{K/\Omega}\eta_j = S_{K/\Omega}\sum_{j=1}^{n_0} u_{ij}\eta_j \qquad (i = 1, 2, \ldots, n_0).$$

9) In the case where l is unramified in K/Ω, we set $v = 0$ for convenience, and then we have $m = 0$ and it implies $t = 0$.

Now, if we put $\xi_i' = \sum_{j=1}^{n_0} u_{ij}\eta_j$ $(i = 1, 2, \ldots, n_0)$, then we have $S_{K/\Omega}\xi_i' = \omega_i'$ and the set $[\beta_1, \ldots, \beta_{n_0(l-1)}, \omega_1, \ldots, \omega_t, \xi_{t+1}', \ldots, \xi_{n_0}']$ is again a basis of $\mathfrak{o}_K$. Putting $\alpha_i = l\xi_i' = \omega_i'$ $(t+1 \leqq i \leqq n_0)$, we have $S_{K/\Omega}\alpha_i = 0$, which proves our theorem.

THEOREM 3. *Under the same assumptions in Theorem* 2, *the representation of the Galois group* $\mathfrak{G}$ *of* K/Ω *by the ring* $\mathfrak{o}_K$ *is integrally equivalent with the sum of* t *identical representation,* t *rationally irreducible representations of degree* $l-1$ *and* $n_0 - t$ *indecomposable representations containing one identical representation and one rationally irreducible representation of degree* $l-1$.

Proof. As a basis of $\mathfrak{o}_K$, we may take a basis having the property stated in Theorem 2. Let σ be a generator of the Galois group $\mathfrak{G}$. Then both $(\sigma-1)\mathfrak{o}_K$ and $(\sigma-1)\mathfrak{o}_K^*$ are submodules of $\mathfrak{o}_K^*$ and are generated by $(\sigma-1)\beta_1, \ldots, (\sigma-1)\beta_{n_0(l-1)}$, $(\sigma-1)\xi_1, \ldots, (\sigma-1)\xi_{n_0-t}$ and $(\sigma-1)\beta_1, \ldots, (\sigma-1)\beta_{n_0(l-1)}$ respectively.

Therefore, $(\sigma-1)\xi_i = (\sigma-1)\alpha_i/l$ $(i = 1, 2, \ldots, n_0 - t)$ generate the factor module $\mathfrak{F} = (\sigma-1)\mathfrak{o}_K/(\sigma-1)\mathfrak{o}_K^*$ and moreover form its basis. For, if we assume that $\sum_i x_i(\sigma-1)\xi_i = (\sigma-1)\beta$ for some β in $\mathfrak{o}_K^*$ and for rational integers x_i $(i = 1, 2, \ldots, n_0 - t)$, then we have $(\sigma-1)(\sum_i x_i\alpha_i/l - \beta) = 0$ and hence $l\beta = \sum_i x_i\alpha_i$. But since $\alpha_i = l\xi_i - \omega_i$, we have $\sum_i x_i\omega_i = l(\beta - \sum_i x_i\xi_i)$, which implies $x_i \equiv 0$ mod. l for every $i = 1, 2, \ldots, n_0 - t$.

On the other hand, let $Z[\mathfrak{G}]$ be a group ring of $\mathfrak{G}$ over the rational integers and define $S = 1 + \sigma + \cdots + \sigma^{l-1} \in Z[\mathfrak{G}]$. Then we may regard $\mathfrak{o}_K^*$ as a $Z[\mathfrak{G}]/(S)$-module, where (S) is the principal ideal of $Z[\mathfrak{G}]$ generated by S. Since $Z[\mathfrak{G}]/(S)$ is a Dedekindian ring, we have by Chevalley's lemma direct decompositions

$$(*) \qquad \mathfrak{o}_K^* = \mathfrak{A}_1 \oplus \mathfrak{A}_2 \oplus \cdots \oplus \mathfrak{A}_{n_0},^{10)}$$
$$(\sigma-1)\mathfrak{o}_K = \mathfrak{B}_1 \oplus \mathfrak{B}_2 \oplus \cdots \oplus \mathfrak{B}_{n_0}$$

[10] Each direct factor $\mathfrak{A}_\nu$ of $\mathfrak{o}_K^*$ in the decomposition $(*)$ is $Z[\zeta]$-isomorphic to an ideal class of the ring $Z[\zeta]$ which consists of all integers of the field $P(\zeta)$ obtained by adjunction of a primitive l-th root of 1 to the rational number field P.

In particular, if we assume $l < 23$, then the class number of the cyclotomic field $P(\zeta)$ is equal to 1 (cf. e.g. H. W. Leopoldt [9]). Therefore, every factor $\mathfrak{A}_\nu$ is $Z[\mathfrak{G}]/(S)$-isomorphic to $Z[\mathfrak{G}]/(S)$.

of $Z[\mathfrak{G}]/(S)$-module $\mathfrak{o}_K^*$, $(\sigma-1)\mathfrak{o}_K$ with $\mathfrak{A}_i \cong \mathfrak{B}_i$ $(i=1, 2, \ldots, n_0)$.[11]

Since $(\sigma-1)\mathfrak{o}_K^*$ is the $Z[\mathfrak{G}]/(S)$-submodule of $(\sigma-1)\mathfrak{o}_K$, and since the index of $(\sigma-1)\mathfrak{A}_\nu$ in $\mathfrak{A}_\nu$ is the prime number l, each factor $\mathfrak{B}_\nu$ is either $\mathfrak{A}_\nu$ or $(\sigma-1)\mathfrak{A}_\nu$ and by permuting the summands in $(*)$ we obtain the factor module

$$\begin{aligned}\mathfrak{F} &= (\sigma-1)\mathfrak{o}_K/(\sigma-1)\mathfrak{o}_K^* \\ &= \mathfrak{A}_1/(\sigma-1)\mathfrak{A}_1 \oplus \cdots \oplus \mathfrak{A}_{n_0-t}/(\sigma-1)\mathfrak{A}_{n_0-t},\end{aligned}$$

which is an additive abelian group of type $(l, \ldots, l)$. Therefore, we may choose a basis $[\gamma_1, \ldots, \gamma_{n_0-t}]$ of $\mathfrak{F}$ with $\gamma_i \in \mathfrak{A}_i$, namely if we take a basis $[\beta_{\nu_1}, \ldots, \beta_{\nu l-1}]$ of the ν-th factor $\mathfrak{A}_\nu$ in $(*)$, then we may write $\gamma_i = \sum_{j=1}^{l-1} x_{ij}\beta_{ij}$ with rational integers x_{ij}.

Since both $[(\sigma-1)\xi_1, \ldots, (\sigma-1)\xi_{n_0-t}]$ and $[\gamma_1, \ldots, \gamma_{n_0-t}]$ are bases of $\mathfrak{F}$, there is a unimodular $(n_0-t)\times(n_0-t)$ matrix $S=(s_{ij})$ with integral coefficients such that

$$\sum_{j=1}^{l-1} x_{ij}\beta_{ij} = \gamma_i = \sum_{j=1}^{n_0-t} s_{ij}(\sigma-1)\xi_j = (\sigma-1)\sum_{j=1}^{n_0-t} s_{ij}\xi_j \qquad (i=1, 2, \ldots, n_0-t).$$

Now, we put $\xi_i' = \sum_{j=1}^{n_0-t} s_{ij}\xi_j$ for every i, then $\{\beta_{\nu\mu}, \omega_j, \xi_i'\}$ $(\nu=1, 2, \ldots, n_0;$ $\mu=1, 2, \ldots, l-1;$ $j=1, 2, \ldots, t;$ $i=1, 2, \ldots, n_0-t)$ again form a basis of $\mathfrak{o}_K$ and $[\omega_j]$ $(j=1, 2, \ldots, t)$, $[\beta_{\nu 1}, \ldots, \beta_{\nu l-1}]$ $(\nu=1, 2, \ldots, t)$, and $[\xi_i', \beta_{i1}, \ldots, \beta_{il-1}]$ $(i=1, 2, \ldots, n_0-t)$ give respectively t, t, n_0-t indecomposable representations in Theorem 3.

References

[1] F. E. Diederichsen, Über die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetischer Äquivalenz, Abh. Math. Sem. Univ. Hamburg, **14** (1938).

[2] I. Reiner, Integral representations of cyclic groups of prime order, Proc. Amer. Math. Soc., **8** (1957).

[2a] H. W. Leopoldt, Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers, J. Reine Angew. Math., **201** (1959).

[3] A. Speiser, Gruppendeterminante und Körperdiscriminante, Math. Ann., **77** (1916).

[4] E. Noether, Normalbasis bei Körpern ohne höhere Verzweigung, J. Reine Angew. Math., **167** (1932).

[5] T. Takagi, Daisûteki Seisûron, Tokyo (1949), p. 110.

[6] H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper I a, Jahre. Deutsch. Math. Verein. § 9, s. 75.

[11] Cf. C. Chevalley [13].

[7] E. Artin, Algebraic numbers and algebraic functions **I**, Princeton (1951), p. 66.

[8] H. Hasse, Zahlentheorie, Berlin (1949), s. 322.

[9] T. Nakayama, On modules of trivial cohomology over a finite group **II**, Nagoya Math. J., **12** (1957).

[10] T. Nakayama, Cohomology of class field theory and tensor product modules **I**, Ann. of Math., **65** (1957).

[11] G. Hochschild-T. Nakayama, Cohomology in class field theory, Ann. of Math., **55** (1952).

[12] H. W. Leopoldt, Über Einheitengruppe und Klassenzahl reeller Abelscher Zahlkörper, Abh. Deutsch. Akad. d. Wiss. zu Berlin, Math.-Naturw. Kl., Jahrg. 1953, Nr. **2** (1954).

[13] C. Chevalley, L'arithmétique dans les algèbres des Matrices, Actual. Sci. Ind., **323** (1936).