222. Remark on Yokoi's Theorem Concerning the Basis of Algebraic Integers and Tame Ramification

By Yoshimasa MIYATA

(Comm. by Kenjiro SHODA, M. J. A., Dec. 12, 1968)

In this paper we shall prove a theorem (Theorem 1 in the following) which, the author thinks, is essentially a refinement of Yokoi's theorem (Theorem 2 of [2]). From it follows a characterization of tame ramification, which we shall state as Theorem 2.

Theorem 1. *Let k be a finite algebraic number field and K/k be a cyclic extension of prime degree l. Let $\mathfrak{o}$ and $\mathfrak{O}$ be the rings of algebraic integers of k and K. Then we have the following basis x_i, y_i, z_m ($i=1, \cdots, t$, $j=t+1, \cdots, n$, $m=1, \cdots, n(l-1)$) of $\mathfrak{O}$ over the rational integer ring $\boldsymbol{Z}$, i.e.:*

$$\mathfrak{O}=\boldsymbol{Z}[x_1, \cdots, x_t, y_{t+1}, y_n, z_1, \cdots, z_{n(l-1)}]$$

*such that $x_1, \cdots, x_t, S_{K/k}y_{t+1},\ldots, S_{K/k}y_n$ consist a basis of $\mathfrak{o}$ over $\boldsymbol{Z}$ and $S_{K/k}z_m=0$ for $1\leqq m\leqq n(l-1)$, where $S_{K/k}$ denotes the relative trace of K to k.**)

Let H be the Galois group of K/k. We denote the group ring $\boldsymbol{Z}[H]$ of H over $\boldsymbol{Z}$ by Λ. Obiously $\mathfrak{O}$ is a Λ-module. We consider it as a representation module of H (accordingly of Λ).

Theorem 2. *Let K/k and $\mathfrak{O}$ be as in Theorem 1. Then K/k is tamely ramified at every prime ideal of k if and only if no Λ-module on which H acts trivially appears as a direct summand of $\mathfrak{O}$ (considered as Λ-module).*

At first we state the following well known facts which are useful in the proof of the theorems; let H be a cyclic group of prime order l (for example, the Galois group of K/k stated in the above) and $\Lambda=\boldsymbol{Z}[H]$ be its group ring over $\boldsymbol{Z}$ (as before). Let h be a fixed generator of H and let $\theta=\cos 2\pi/l+i\sin 2\pi/l$, so that θ is a primitive lth root of 1. Let $R=\boldsymbol{Z}[\theta]$. As is shown in [1], there are three and only three classes of indecomposable Λ-modules, i.e.:

i) H-trivial modules, i.e., modules on which H acts trivially.

ii) Taking A to be *a* R-fractional ideal, we may turn A into *a* Λ-module by defining

$$ha=\theta a \text{ for } a\in A.$$

iii) Let y be an indeterminate and A be *a* R-fractional ideal. We

---

*) We need not suppose that k and K are absolute Galois number fields, which is different from [2].

can turn a direct sum $Zy \oplus A$ of the Z-module A and the free Z-module Zy into a Λ-module by defining

$$hy = y + a_0 \quad ha = \theta a \quad \text{for} \quad a \in A$$

where a_0 is a fixed element of A such that $a_0 \notin (\theta - 1)A$.

We call Λ-module M A-type if and only if M is isomorphic to A defined in ii), and we call M (A, a_0)-type if and only if M is isomorphic to (A, a_0) defined in iii). Then it holds the following fundamental theorem.

Theorem 3 ([1] (74.3)). *Every Λ-module is isomorphic to a direct sum*

$$X \oplus A_1 \oplus \cdots \oplus A_r \oplus (A_{r+1}, a_{r+1}) \oplus \cdots \oplus (A_n, a_n)$$

where A_i defined in ii) and (A_j, a_j) defined in iii), and where X is a H-trivial module having a finite basis over Z. Moreover let M and N be Λ-modules. M and N are isomorphic if and only if they satisfy the following four conditions such that

i) The numbers r of A-type components of M and N are same.

ii) The numbers n of H-non-trivial components of M and N are same.

iii) Two Z-ranks of X are same.

iv) Two ideal classes of $A = A_1 \cdots A_n$ are same, where $A_1 \cdots A_n$ denotes the product of ideals A_i.

n is R-rank of M_S, where $M_S = \{m \in M \mid (1 + h + \cdots + h^{l-1})m = 0\}$, and $M_S \cong R_1 \oplus \cdots \oplus R_{n-1} \oplus A_1 \cdots A_n$.

Now we shall begin the proof of Theorem 1. At first we state

Lemma 1. *Let M and I_M be a projective Λ-module and its Λ-submodule consisting of all elements m in M satisfying $hm = m$. Let $S = 1 + h + \cdots + h^{l-1}$. Then*

$$I_M = SM.$$

Proof. Let M and N be Λ-modules. Then $I_{M \oplus N} = I_M \oplus I_N$. Therefore we can restrict our proof only to the case that M is Λ, without any loss of generality. In this case every element m in I_Λ is written in the form aS with $a \in Z$. Clearly $I_\Lambda = S\Lambda$.

Let H be again the Galois group of K/k and $\mathfrak{O}$ be the ring of algebraic integers of K as before. $\mathfrak{O}$ is a Λ-module. Since H is a cyclic group of order l, we can apply Theorem 3 and obtain

$$\mathfrak{O} \cong X \oplus A_1 \oplus \cdots \oplus A_r \oplus (A_{r+1}, a_{r+1}) \oplus \cdots \oplus (A_n, a_n).$$

Clearly $I_x = X$ and $I_{A1 \oplus \cdots \oplus Ar} = 0$. As (A_j, a_j) is projective, from Lemma 1 follows that $I_{(A_r+1, a_r+1) \oplus \cdots \oplus (A_n, a_n)} = ZS_{K/k} y_{r+1} \oplus \cdots \oplus ZS_{K/k} y_n$. Thus the proof is completed.

Lemma 2. *Let $\mathfrak{O}$ be as in Theorem 1, and we consider its decomposition into a direct sum of indecomposable Λ-submodules. Then the number of A-type modules appearing in its decomposition coincides with the Z-rank of the H-trivial component.*

Proof. Since $K=\boldsymbol{Q}\otimes_{\boldsymbol{Z}}\mathfrak{O}$ has a normal basis, where $\boldsymbol{Q}$ is the rational number field, K is isomorphic to a direct sum of $\boldsymbol{Q}[H]$. For (A, a_0)-type module M, it holds $\boldsymbol{Q}\otimes_{\boldsymbol{Z}}M=\boldsymbol{Q}[H]$. For A-type module M, $\boldsymbol{Q}\otimes_{\boldsymbol{Z}}M$ is a non-trivial rational irreducible $\boldsymbol{Q}[H]$-module. Then the number of A-type modules in the direct decomposition of $\mathfrak{O}$ is equal to the $\boldsymbol{Z}$-rank of H-trivial component.

Now we can easily obtain Theorem 2 as follows: As is known, K/k is tamely ramified if and only $\mathfrak{o}=S_{K/k}\mathfrak{O}$([2]). Then Theorem 2 is clear from Theorem 1 and Lemma 2.

References

[1] C. W. Curtis and I. Reiner: Representation Theory of Finite Groups and Associative Algebras. Interscience, New York (1962).

[2] H. Yokoi: On the ring of integers in an algebraic number field as a representation of Galois group. Nagoya Math. J., **16**, 83–90 (1960).