Yoshimasa Miyata
Nagoya Math. J.
Vol. 43 (1971), 151–156

ON A CHARACTERIZATION OF THE FIRST RAMIFICATION GROUP AS THE VERTEX OF THE RING OF INTEGERS

YOSHIMASA MIYATA

1. Introduction.

Let k be a $\mathfrak{p}$-adic number field and $\mathfrak{o}$ be the ring of all integers in k. Moreover, let K/k be a finite Galois extension with the Galois group $G = G(K/k)$. Then the ring $\mathfrak{O}$ of all integers in K is an $\mathfrak{o}[G]$-module. In this paper we shall give a characterization of the first ramification group G_1 of the extension K/k as the vertex of $\mathfrak{O}$ which is defined below.

To define the vertex of $\mathfrak{O}$, we remember the vertex theory ([1], [2]). Let G be an arbitrary finite group and M be an $\mathfrak{o}[G]$-module, where $\mathfrak{o}[G]$ is the group algebra of G over $\mathfrak{o}$. Let U be a subgroup of G. Then M is said to be U-projective if there is an $\mathfrak{o}[U]$-module N such that M is isomorphic to a component of the induced $\mathfrak{o}[G]$-module $\mathfrak{o}[\mathfrak{O}]\otimes_{\mathfrak{o}[U]}N$. If M is an indecomposable $\mathfrak{o}[G]$-module, then there exists a subgroup V of G, such that

(i) M is V-projective

and

(ii) if W is any subgroup of G, such that M is W-projective, then for some element g of G

$$gVg^{-1}\subset W.$$

We call such V, that is uniquely determined up to conjugate subgroups in G, a vertex of M.

Now let K/k be the finite Galois extension with the Galois group G, and $\mathfrak{O}$ the ring of all integers in K. Then, since $\mathfrak{O}$ is not always indecomposable as an $\mathfrak{o}[G]$-module, we consider the decomposition of $\mathfrak{O}$ into indecomposable $\mathfrak{o}[G]$-modules M_i

$$\mathfrak{O} = M_1 \oplus \cdots \oplus M_l. \tag{1}$$

Received September 17, 1970.
Revised October 28, 1970.

As the Krull-Schmidt theorem holds for $\mathfrak{o}[G]$-modules, the set $\{M_1, \cdots, M_l\}$ of indecomposable $\mathfrak{o}[G]$-submodules is determined uniquely, up to isomorphisms, only by $\mathfrak{O}$. For each $i(1 \leq i \leq l)$ there exists a vertex V_i of M_i. By the above remark, the set $\{V_1, \cdots, V_l\}$ of vertices is also determined uniquely, up to conjugate subgroups in G, only by $\mathfrak{O}$. We define the vertex of $\mathfrak{O}$ as the minimal normal subgroup V of G containing V_i for all i. Thus the vertex V of $\mathfrak{O}$ is defined uniquely. Our aim of this paper is to prove that the vertex V of $\mathfrak{O}$ coincides with the first ramification group G_1 of the Galois extension K/k.

To achieve our aim, we use the cohomological characterization of the tamely ramified extension which H. Yokoi gave in [6]. We state this characterization as Theorem 2 in this paper.

2. G-algebra.

In this section we summarize definitions and propositions of the representation theory from Green's paper [2] which we use in this paper. An algebra A with identity element is said to be a G-algebra if A is a left $\mathfrak{o}[G]$-module and moreover the condition

$$g(ab) = g(a)g(b)$$

is satisfied for all $g \in G$ and all $a, b \in A$. For each subgroup U of G we define A_U by

$$A_U = \{a \in A \mid g(a) = a, \text{ all } g \in U\}.$$

If U and W are subgroups of G such that $U \subset W$, then it follows clearly that

$$A_U \supset A_W.$$

Then we define the map $T_{U,W}$: $A_U \to A_W$, by

$$T_{U,W}(a) = \sum_g g(a)$$

for all $a \in A_U$, where g runs over a set of representatives of distinct left cosets of U in W. As $a \in A_U$, $T_{U,W}(a)$ does not depend on the choice of representatives. $T_{U,W}(a)$ is a element of A_W. Let $A_{U,W}$ be the image of $T_{U,W}$. From [2] 4h Lemma, we have the following lemma:

LEMMA 1. *Let U and W be subgroups of G, then*

$$A_{U,G}A_{W,G} \subset \sum_{g \in G} A_{U^g \cap W, G}$$

where U^g is a conjugate subgroup gUg^{-1} of U.

Let e be a primitive idempotent of algebra A_G, then there exists a subgroup V of G, such that

(i) $e \in A_{V,G}$

and

(ii) if U is any subgroup of G, such that $e \in A_{U,G}$, then for some element g of G

$$gVg^{-1} \subset U.$$

We call such V, that is uniquely determined up to conjugate subgroups in G, a defect group of e.

Let M be a left $\mathfrak{o}[G]$-module, and let $E(M)$ denote the $\mathfrak{o}$-algebra of all $\mathfrak{o}$-endomorphisms of M. Then we obtain the following facts from [2] 5. Examples of G-algebras Example 3). We make $E(M)$ into a G-algebra as follows: if $\theta \in E(M)$ and $g \in G$, we define $g(\theta)$ by

$$(g(\theta))(m) = g(\theta(g^{-1}(m))) \tag{3}$$

for all $m \in M$. Then for any subgroup U of G, $E(M)_U$ is the algebra of all $\mathfrak{o}[U]$-endomorphisms of M. Suppose that M is an indecomposable $\mathfrak{o}[G]$-module. Then the identity endomorphism $1 \in E(M)$ is a primitive idempotent of $E(M)_G$. The defect group of 1 in the G-algebra $E(M)$ is the vertex of the indecomposable $\mathfrak{o}[G]$-module M. If M is not indecomposable, each primitive idempotent $e \in E(M)_G$ determines an indecomposable component eM of $M = eM \oplus (1-e)M$. The defect group of e in $E(M)$ is the same as the vertex of eM.

We apply the above results concerning M to $\mathfrak{o}[G]$-module $\mathfrak{O}$. We obtain the decomposition of the identity endomorphism $1 \in E(\mathfrak{O})$ into primitive idempotents e_i of $E(\mathfrak{O})_G$

$$1 = e_1 + \cdots + e_l \tag{3}$$

corresponding to the decomposition (1) of $\mathfrak{O}$. For each $i (1 \leq i \leq l)$ let V_i be the defect group of e_i. Then V_i is the vertex of $M_i = e_i M$. Hence the set $\{V_1, \cdots, V_l\}$ is determined only by $\mathfrak{O}$ up to conjugate subgroups in G. Then the vertex V of $\mathfrak{O}$ defined in the introduction is also the minimal normal subgroup of G containing all defect groups V_i.

Now we prove the lemma which we shall use later.

LEMMA 2. *Let A be a G-algebra, and f, f_1, f_2 idempotents of A_G such that*

$f = f_1 + f_2$, $f_1 f_2 = f_2 f_1 = 0$. *If U is any subgroup such that $f \in A_{U,G}$, then f_1 and f_2 belong to $A_{U,G}$.*

Proof. f_i belongs to $A_{G,G} = A_G$ from the assumption. Since $f_i = f_i f$, f_i belongs to $A_{G,G} A_{U,G}$. By Lemma 1, we obtain

$$f_i \in A_{G,G} A_{U,G} \subset \sum_{g \in G} A_{G^g \cap U, G} = A_{U,G}.$$

3. Vertex of $\mathfrak{O}$.

We use the same notation as in the last section. For any element α of $\mathfrak{O}$ we define an element $\bar{\alpha}$ of $E(\mathfrak{O})$ by

$$\bar{\alpha}(\beta) = \alpha\beta$$

for all $\beta \in \mathfrak{O}$. This map from $\mathfrak{O}$ into $E(\mathfrak{O})$ is injective. We denote $\bar{\alpha}$ simply by α. Thus in the following $\mathfrak{O} \subset E(\mathfrak{O})$. We may think two kinds of operation of G on $\mathfrak{O}$. One of them is induced by considering G as the Galois group of the extension K/k and the other is defined by (2). These two kinds of operation of G on $\mathfrak{O}$ are the same. In fact

$$\overline{g(\alpha)}(\beta) = g(\alpha)\beta = g(\alpha(g^{-1}(\beta))) = (g(\bar{\alpha}))(\beta)$$

for all $\alpha, \beta \in \mathfrak{O}$.

Let U be any subgroup of G, then $\theta \in E(\mathfrak{O})_U$ induces an $\mathfrak{o}$-endomorphism $\bar{\theta}$ of $\mathfrak{O}_U$. In fact for any $\beta \in \mathfrak{O}_U$ and any $g \in U$, we have

$$(g(\theta))(\beta) = g(\theta(g^{-1}(\beta))) = \theta(\beta).$$

Therefore

$$g(\theta(\beta)) = \theta(\beta).$$

As $\theta(\beta)$ is kept elementwise by the operation of U, $\theta(\beta)$ belongs to $\mathfrak{O}_U$.

We can consider the identity of $\mathfrak{O}$ as the identity endomorphism of $\mathfrak{O}$. In the following we denote the identity of $\mathfrak{O}$ and the identity endomorphism by the same notation 1. When G acts on $\mathfrak{O}$ as the Galois group of the extension K/k, $\mathfrak{O}$ is a G-algebra. The map $T_{U,G}$ defined in the introduction is the usual trace map from L to k, where L is a subfield of K corresponding to U, i.e. K_U. We denote $tr_{U,G}$ instead of $T_{U,G}$ in the case that A is $\mathfrak{O}$.

THEOREM 1. *Let U be a normal subgroup of G. Then all e_i in the decomposition* (3) *lie in $E(\mathfrak{O})_{U,G}$ if and only if the identity* 1 *lies in $tr_{U,G}\mathfrak{O}_U$.*

Proof. Suppose that $e \in (\mathfrak{O})_{U,G}$ for $1 \leq i \leq l$. Then there exists $\theta_i \in E(\mathfrak{O})_U$

such that

$$e_i = \sum_{\{g\}} g(\theta_i),$$

where the $\{g\}$ are representatives of the distincet left cosets of U in G. Put $\theta = \theta_1 + \cdots + \theta_l$, then we obtain

$$1 = \sum_{\{g\}} g(\theta) \tag{4}$$

and θ induces an endomorphism $\bar{\theta}$ in $E(\mathfrak{O}_U)$ as we state above. As $\{g\}$ are all representatives, we can think that g runs over the factor group $\bar{G} = G/U$. We can consider the equation (4) as the equation in the $\bar{G}$-algebra $E(\mathfrak{O}_U)$. Thus we have

$$1 = \sum_{g \in \bar{G}} \bar{g}(\bar{\theta}).$$

$\mathfrak{O}_U$ is $\bar{G}$-weakly projective. Hence the 0-dimensional Galois cohomology group $H^0(\mathfrak{O}_U)$ is trivial (c.f. [3]). Since $H^0(\mathfrak{O}_U) = (\mathfrak{O}_U)_{\bar{G}}/tr\mathfrak{O}_U$, 1 lies in $tr_{U,G}\mathfrak{O}_U$.

Conversely, we suppose that 1 lies in $tr_{U,G}\mathfrak{O}_U$. Since $tr_{U,G}\mathfrak{O}_U \subset E(\mathfrak{O})_{U,G}$, 1 lies in $E(\mathfrak{O})_{U,G}$. Applying Lemma 2 to the case that $f = 1$, $f_1 = e_1$ and $f_2 = e_2 + \cdots + e_l$, we obtain that $e_1 \in E(\mathfrak{O})_{U,G}$. Similarly we obtain that e_i lies in $E(\mathfrak{O})_{U,G}$ for $2 \leq i \leq l$.

H. Yokoi gave the following theorem:

THEOREM 2. (*H. Yokoi* [6]). *The extension K/k is tamely ramified if and only if the 0-dimensional Galois cohomology group $H^0(\mathfrak{O})$ is trivial.*

Now we prove the main theorem of this paper.

THEOREM 3. *The vertex V of $\mathfrak{O}$ is the first ramification group G_1 of the extension K/k.*

Proof. At first we prove that G_1 contains V. By Theorem 2, $H^0(\mathfrak{O}_{G_1}) = \{0\}$. Then 1 lies in $tr_{G_1,G}\mathfrak{O}_{G_1}$. By Theorem 1, e_i lies in $E(\mathfrak{O})_{G_1,G}$ for $1 \leq i \leq l$. Hence G_1 contains the defect group V_i of e_i. As G_1 is a normal subgroup of G, G_1 contains the vertex V of $\mathfrak{O}$.

Next we prove conversely that V contains G_1. As e_i lies in $E(\mathfrak{O})_{V,G}$ for $1 \leq i \leq l$, it follows from the proof of Theorem 1 that $H^0(\mathfrak{O}_V) = \{0\}$. Let K_V be a subfield of K corresponding to V. Then, by Theorem 2 the extension K_V/k is tamely ramified. The ramification field K_{G_1} contains any tamely ramified subfield of K (c.f. [5]). Hence V contains G_1.

Finally we obtain the next corollary. It is the statement to express E. Noether's Theorem concerning the characterization of the tamely ramified extension ([4]) in other words.

COROLLARY. *The extension K/k is tamely ramified if and only if the ring $\mathfrak{O}$ of all integers in K is $\mathfrak{o}[G]$-projective.*

Proof. $\mathfrak{O}$ is $\mathfrak{o}[G]$-projective if and only if each M_i of the decomposition (1) of $\mathfrak{O}$ is $\mathfrak{o}[G]$-projective. M_i is $\mathfrak{o}[G]$-projective if and only if the vertex of M_i is trivial. Moreover, the extension K/k is tamely ramified if and only if the first ramification group G_1 is trivial (c.f. [5]). Since G_1 is the vertex of $\mathfrak{O}$, the corollary is proved.

Remark. E. Noether's Theorem is obtained by replacing *projective* by *free* in this corollary.

REFERENCES

[1] J.A. Green, Blocks of modular representation, Math. Zeit. **79** (1962), 100–115.
[2] J.A. Green, Some Remarks on Defect Groups, Math. Zeit. **107** (1968), 133–150.
[3] Y. Kawada, Daisūteki Seisūron, Kyoritsu, Tokyo (1957).
[4] E. Noether, Normalbasis bei Körpern ohne höhere Verzweigung, J. Reine Angew. Math. **167** (1932), 147–152.
[5] E. Weiss, Algebraic Number Theory, McGraw-Hill, New York (1963).
[6] H. Yokoi, On the ring of integers in an algebraic number field as a representation module of Galois group, Nagoya Math. J. **16** (1960), 83–90.

Fuculty of Education, Shizuoka University