ILLINOIS JOURNAL OF MATHEMATICS
Volume 31, Number 2, Summer 1987

VERTICES OF IDEALS OF A $\mathfrak{p}$-ADIC NUMBER FIELD

BY

YOSHIMASA MIYATA

Let k be a $\mathfrak{p}$-adic number field with the ring $\mathfrak{o}$ of all integers, and K be a finite normal extension with Galois group G. Let Π denote a prime element of the ring $\mathfrak{O}$ of integers in K. Then, an ideal (Π^i) of $\mathfrak{O}$ is an $\mathfrak{o}G$-module. E. Noether [5] showed that if K/k is tamely ramified, $\mathfrak{O}$ is isomorphic to $\mathfrak{o}G$. S. Ullom [10] proved that (Π^i) has a normal basis if and only if $\mathrm{tr}_{K/K_1}(\Pi^i) = (\Pi^i) \cap K_1$, where K_1 is the ramification subfield of K/k. A. Fröhlich [3] generalized E. Noether's theorem as follows: $\mathfrak{O}$ is relatively projective with respect to a subgroup S of G if and only if $S \supseteq G_1$, where G_1 denotes the first ramification group of K/k. Now we define the vertex $V(\Pi^i)$ of (Π^i) as the minimal normal subgroup S of G such that (Π^i) is (G, S)-projective. Then, the above generalization by A. Fröhlich implies that $V(\mathfrak{O}) = G_1$ (cf. [6], Theorem 3). The purpose of this paper is to study the vertex $V(\Pi^i)$ of (Π^i). In the first section, we shall show that $G_1 \supseteq V(\Pi^i) \supseteq G_2$ for any i (Theorem 5) and that if the second ramification group G_2 is trivial, then $V(\Pi^i)$ is either G_1 or $\{1\}$ (Theorem 6). The next two sections deal with the restricted case where K/k is a wildly ramified extension of degree p^2. We shall show that if $i \not\equiv 1$ (p^2), then $V(\Pi^i) = G_1$ (Theorem 15) and we shall obtain the necessary and sufficient conditions for $V(\Pi^i)$ to be equal to G_2 for the case where $i \equiv 1$ (p^2) (Theorem 21).

Section 1

Let $\mathfrak{o}$ be the ring of all integers of a $\mathfrak{p}$-adic number field k. Let S be a subgroup of a finite group G. We begin this section with recalling the definition of (G, S)-projectivity. An $\mathfrak{o}G$-module M is (G, S)-projective if there exists an $\mathfrak{o}S$-endomorphism γ such that

$$(1) \qquad \sum_{i=1}^{n} g_i \gamma g_i^{-1} = 1_M,$$

where $G = \cup g_i S$ (for example, see [2], p. 449, (19.1) Definitions and (19.2)

Received February 28, 1985.

Theorem). Moreover, from [2], p. 452 (19.5) Proposition, there exists a unique minimal normal subgroup S such that M is (G, S)-projective. Now let K/k be a finite Galois extension with Galois group G, and denote by π a prime element of K. Then, applying the above results to an $\mathfrak{o}G$-module (Π^i), we can define the vertex $V(\Pi^i)$ of (Π^i) stated in the introduction, i.e., $V(\Pi^i)$ is a unique minimal normal subgroup V of G such that (Π^i) is (G, V)-projective.

Remark. For an indecomposable $\mathfrak{o}G$-module M, the vertex of M stated in the above is the minimal normal subgroup containing an ordinary vertex of M defined in the module representation theory of groups.

PROPOSITION 1. *Let K/k and Π be as in the above, and denote by G_1 the first ramification group of K/k. Then, $V(\Pi^i) \subseteq G_1$.*

Proof. Let $\mathfrak{O}_1$ be the ring of all integers in K_1. An element α of $\mathfrak{O}_1$ defines an $\mathfrak{o}G_1$-endomorphism of (Π^i) given by multiplication by α. Let $G = \cup g_i G_1$. Then, for $\beta \in (\Pi^i)$,

$$\sum g_i \alpha g_i^{-1}(\beta) = \left(\sum g_i(\alpha)\right)\beta. \tag{2}$$

As K_1/k is tamely ramified, there exists α such that $\Sigma g_i(\alpha) = 1$. Thus, by (1) and (2), (Π^i) is (G, G_1)-projective, which means $V(\Pi^i) \subseteq G_1$.

We denote by G_i the i-th ramification group. From [10] Theorem 3 and its corollary, we immediately have the following lemma.

LEMMA 2. *Let K/k be as above and denote by $|G_1|$ the order of G_1. Then, if (Π^i) is $\mathfrak{o}G$-projective, $i \equiv 1$ $(|G_1|)$ and $G_2 = \{1\}$.*

Next, let $\varphi(t)$ be the Herbrand function for the extension K/k, and $\psi(t)$ be the inverse function of $\varphi(t)$. Then, the upper numbering of the ramification groups is given by

$$G^t = G_{\psi(t)}.$$

Let V be $V = V(\Pi^i)$ and $\varphi_2(t)$ be the Herbrand function for K/K_V, where K_V is the subfield of K corresponding to V. Then, we have

$$(G/V)^t = G^t V/V \tag{3}$$

(for example, see [1], p. 38).

LEMMA 3. *Let K/k and ψ_2 be as above. Then, $V(\Pi^i) \supseteq G_{\psi_2(2)}$.*

Proof. Let $(\Pi^i)_V = K_V \cap (\Pi^i)$. We can easily show that $(\Pi^i)_V$ is $\mathfrak{o}[G/V]$-projective. Then, it follows from Lemma 2 that $(G/V)_2 = \{1\}$. Let

φ_1 be the Herbrand function for K_V/k, so by (3),

$$G^{\varphi_1(2)}V/V = (G/V)_2 = \{1\},$$

and hence $V \supseteq G^{\varphi_1(2)}$. From $\psi = \psi_2\psi_1$, it follows that

$$G^{\varphi_1(2)} = G_{\psi(\varphi_1(2))} = G_{\psi_2(2)},$$

which establishes $V \supseteq G_{\psi_2(2)}$.

COROLLARY 4. *Let K/k be as above. If $G_1 = G_2$, then $V(\Pi^i) = G_1$.*

Proof. From $G_1 = G_2$, we have $V_2 = V_1$ $(= V)$, so $\psi_2(2) = 2$. Therefore,

$$G_{\psi_2(2)} = G_2 = G_1,$$

and hence $V(\Pi^i) = G_1$ by Lemma 3.

We can now prove one of the main results.

THEOREM 5. *Let K/k and Π be as above. Then, $G_1 \supseteq V(\Pi^i) \supseteq G_2$.*

Proof. At first we treat the case where $G_1 = G_2$. For this case, the result follows at once from Corollary 4. Next, we treat the case $G_1 \neq G_2$. Suppose $G_2 \not\subseteq V$. Then, $G_2 \cap V \neq G_2$ and there exists a maximal normal subgroup H of G_2 such that $H \supseteq G_2 \cap V$. Therefore,

$$HV \cap G_2 = H. \tag{4}$$

Let $\overline{G} = G/H$ and F be the subfield of K corresponding to H. t_i denotes the i-th ramification number of K/k. From $G_1 \neq G_2$, it follows that $t_1 = 1$. Let $t = t_2$ for brevity. Since H is the maximal subgroup of G_2, we have $H = H_1 = \cdots = H_t \supset H_{t+1} = G_{t_3}$. By (3),

$$(\overline{G})_i = G^{\varphi_{F/k}(i)}H/H.$$

Since $G^{\varphi_{F/k}(i)} = G_{\psi_{K/k}(\varphi_{F/k}(i))}$, $(\overline{G})_i = G_{\psi_{K/F}(i)}H/H$. For $i \leq t$, $\psi_{K/F}(i) = i$ and for $i > t$, $\psi_{K/F}(i) > t$. Therefore, $G_{\psi(i)} = G_2$ for $2 \leq i \leq t$ and $G_{\psi(i)} \subseteq G_{t+1}$ for $i > t$. Then, we have

$$\overline{G}_1 = (\overline{G})_1 \supset \overline{G}_2 = (\overline{G})_2 = \cdots = (\overline{G})_t \supset (\overline{G})_{t+1} = \{1\} \tag{5}$$

and

$$\overline{HV} = (\overline{HV})_1 \supset (\overline{HV})_2 = \{1\}, \tag{6}$$

since $V \subseteq G_1$. Let $\bar{\psi}$ denote the Herbrand function for $K_{HV/F}$ and $|\overline{HV}|$ the order of $\overline{HV}$. Then, by (6),

$$\bar{\psi}(2) = 1 + |\overline{HV}|. \tag{7}$$

By (4), $\overline{HV}$ is isomorphic to a subgroup of G_1/G_2, so $\overline{HV}$ is abelian. Since $H \supseteq [G_2, G_2]$ by the definition of H, $\overline{G}_2$ is also abelian, and hence by (4), $\overline{G}_2 \cdot \overline{HV}$ is abelian. Let k' be a subfield of F corresponding to $\overline{G}_2 \cdot \overline{HV}$ and denote by r_i the ramification number of F/k'. Then, $r_1 = 1$ and $r_2 = t$ again. Since F/k' is an abelian extension, from [4], p. 171, (V), and by (6), it follows that

$$t \equiv 1 \quad (|\overline{HV}|).$$

Therefore, by (7), $\bar{\psi}(2) \leqq t$, and by (5),

$$(\overline{G})_{\bar{\psi}(2)} = \overline{G}_2. \tag{8}$$

Since (Π^i) is (G, V)-projective, $(\Pi^i)_H$ is $(\overline{G}, \overline{HV})$-projective and hence $\overline{HV} \supseteq (\overline{G})_{\bar{\psi}(2)}$ by Lemma 3. From (8), $\overline{HV} \supseteq \overline{G}_2$. Since $HV \supseteq H$ and $G_2 \supset H$, $HV \supseteq G_2$, which is contrary to (4). This completes the proof of Theorem 5.

We shall conclude this section with the proof of the next theorem.

THEOREM 6. *Let K/k be as above, and suppose $G_2 = \{1\}$.*
(a) *If $i \not\equiv 1(|G_1|)$, then $V(\Pi^i) = G_1$.*
(b) *If $i \equiv 1(|G_1|)$, then $V(\Pi^i) = \{1\}$.*

Now, to prove Theorem 6, we need the following lemma.

LEMMA 7. *Let V be a normal subgroup of G and $\mathrm{tr}_V = \sum_{v \in V} v$. Let M be an $\mathfrak{o}G$-module and suppose M is (G, V)-projective. Then, $\mathrm{tr}_V M$ is (G/V)-projective.*

Proof. Since M is (G, V)-projective, there exists an $\mathfrak{o}G$-module N and an $\mathfrak{o}V$-module L such that

$$M \oplus N = \mathfrak{o}G \otimes_V L.$$

Let $G = \cup g_i V$. As is a normal subgroup of G, $g_i V = V g_i$ and $\mathrm{tr}_V g_i = g_i \mathrm{tr}_V$. Therefore,

$$\mathrm{tr}_V M \oplus \mathrm{tr}_V N = \sum g_i \otimes \mathrm{tr}_V L.$$

Let $\{x_1, \ldots, x_n\}$ be a basis of $\mathrm{tr}_V L$ over $\mathfrak{o}$, and so

$$\sum g_i \oplus \mathrm{tr}_V L = \sum_j \Big(\sum_i \mathfrak{o} g_i\Big) \otimes x_j.$$

This implies that $\mathrm{tr}_V M \oplus \mathrm{tr}_V N$ is an $\mathfrak{o}[G/V]$-free module. Hence $\mathrm{tr}_V M$ is (G/V)-projective.

Proof of Theorem 6. (a) Let Π_V be a prime element of K_V and (Π^m) be the different of K/K_V. Then, since $G_2 = \{1\}$ and $V \subseteq G_1$, it follows that

$$m = 2(|V| - 1). \tag{9}$$

Let $(\Pi_V^n) = \mathrm{tr}_V(\Pi^i)$. Then, from [9] Proposition 1.1 and by (9),

$$n = 2 + [(i-2)/|V|]. \tag{10}$$

Write $i = i_1|V| + i_0$ with $0 \leqq i_0 < |V|$. We distinguish two cases: (i) $1 < i_0 < |V|$ and (ii) $i_0 = 0$. We first treat case (i). By (10), $n = 2 + i_1$. Since (Π^i) is (G, V)-projective, it follows from Lemma 7 and Lemma 2 that $2 + i_1 \equiv 1$ $(|G_1/V|)$, so

$$i_1 \equiv |G_1/V| - 1 \quad (|G_1/V|)$$

and i_1 can be written in the form

$$i_1 = i_2|G_1/V| + |G_1/V| - 1. \tag{11}$$

Let $(\Pi^i)_V = K_V \cap (\Pi^i)$ and Π_1 be a prime element of K_1. Then, $(\Pi^i)_V$ is (G,V)-projective, i.e., $\mathfrak{o}[G/V]$-projective. Since $G_1/V \subseteq G/V, (\Pi^i)_V$ is $\mathfrak{o}[G_1/V]$-projective. From (11), it follows that

$$(\Pi^i)_V = \left(\Pi_V^{i_1+1}\right) = \Pi_1^{i_2+1}\mathfrak{O}_V,$$

where Π_1 denotes a prime element of K_1. Hence $\mathfrak{O}_V$ is $\mathfrak{o}[G_1/V]$-projective and $\mathrm{tr}_{G_1/V}\mathfrak{O}_V = \mathfrak{O}_1$. Then, from H. Yokoi [12], Theorem 1, K_V/K_1 is tamely ramified. Thus $K_V = K_1$ and $V = G_1$, which is the desired result.

In case (ii), where $i_0 = 0$, we obtain $V = G_1$ in a manner similar to case (i).

(b) Applying arguments similar to the above, for $i = i_1|V| + 1$, we have

$$\mathrm{tr}_V(\Pi^i) = \left(\Pi_V^{i_1+1}\right) \quad \text{and} \quad i_1 \equiv 0\,(|G_1/V|).$$

Therefore, $i \equiv 1\,(|G_1|)$; let $i = i_2|G_1| + 1$. Then, $(\Pi^i) = \Pi_1^{i_2}(\Pi)$ and so (Π^i) is $\mathfrak{O}_1G_1$-isomorphic to (Π). From [10], Theorem 2 and Proposition 5, (Π^i) is $\mathfrak{O}_1G_1$-projective and $\mathfrak{o}G$-projective. Hence $V(\Pi^i) = \{1\}$, and Theorem 6 is proved.

Section 2

Throughout the rest of this paper, we assume that K/k is a wildly ramified extension of degree p^2, and we shall calculate the vertex $V(\Pi^i)$. Then, if

$G_1 = G_2$ or $G_2 = \{1\}$, $V(\Pi^i)$ is determined by Theorems 5 and 6 in §1. Thus, we treat the case where $G_1 \neq G_2$ and $G_2 \neq \{1\}$ in the following. Since the order $|G|$ of G is p^2, $G = G_1$ and $|G_2| = p$. Let $i = i_1p^2 + i_0$ for $0 \leqq i_0 < p^2$. Then, (Π^i) is $\mathfrak{o}G$-isomorphic to (Π^{i_0}), and there is no loss of generality in assuming $0 \leqq i < p^2$. We distinguish four cases: (i) $i = 0$,, (ii) $i = 1$, (iii) $1 < i \leqq p$ and (iv) $p < i < p^2$. In case (i), it follows from [6], Theorem 3, that $V(\mathfrak{O}) = G_1$. In the rest of this section, we treat the cases (iii) and (iv). First we consider the case (iv).

PROPOSITION 8. *Let K/k be a wildly ramified extension of degree p^2, and suppose that $G_1 \neq G_2$ and $|G_2| = p$. Then, if $p < i < p^2$, $V(\Pi^i) = G_1$.*

Proof. Let $(\Pi^i)_2 = (\Pi^i) \cap K_2$ and denote by Π_2 a prime element of K_2. Then, from the assumption $p < i$, $(\Pi^i)_2 = (\Pi_2^j)$ with $j \geqq 2$. Hence, Theorem 6 yields $V((\Pi^i)_2) = G_1/G_2$. Since $(\Pi^i)_2$ is (G, V)-projective and $V \supseteq G_2$ by Theorem 5, it follows that $V((\Pi^i)_2) \subseteq V$, which implies $V(\Pi^i) = G_1$. The proof is completed.

Next we consider case (iii), $1 < i \leqq p$. Let t be the second ramification number of K/k. Then, it is easily shown that $t \equiv 1\ (p)$ (for example, see [4], p. 172); let $t = pt_1 + 1$.

PROPOSITION 9. *Let K/k be as above and suppose $1 < i \leqq p$. Then, if $t \not\equiv p + 1\ (p^2)$, $V(\Pi^i) = G_1$.*

Proof. Since $|G| = p^2$, it follows from Theorem 5 that $V = G_1$ or $V = G_2$. Assume $V = G_2$. We use the same discussion as in the proof of Theorem 6. Let $\mathrm{tr}_V(\Pi^i) = (\Pi_V^n)$, so $n = (p-1)t_1 + 2$ because the different of K/K_2 is $(\Pi^{(p-1)(t+1)})$. Then, from the (G, V)-projectivity of (Π_V^n), $(p-1)t_1 + 2 \equiv 1\ (p)$, and $t_1 \equiv 1\ (p)$. Thus we can write $t_1 = pt' + 1$, and $t \equiv p + 1\ (p^2)$. This implies the accomplishment of the proof.

For case (iii) with $t \not\equiv (p+1)\ (p^2)$ and case (iv), it follows from Propositions 8 and 9 that $V(\Pi^i) = G_1$. From now on we consider the remaining case (iii) with $t \equiv (p+1)\ (p^2)$. Now, let $t = p^2t' + p + 1$, and let τ be a generator of G_2 and $x = \tau - 1$. Denote by Π_2 and π prime elements of K_2 and k, respectively. Then, we can easily prove the following lemmas.

LEMMA 10. *Let* val $=$ val$_K$ *denote the valuation of K* (val$(\Pi) = 1$). *Then,*

$$\mathrm{val}(x^m(\Pi_2^n\Pi)) \equiv \mathrm{val}(x^r(\Pi_2^s\Pi))\ (p^2) \quad \text{for } 0 \leqq m, n, r, s < p$$

iff $m = r$ and $n = s$.

LEMMA 11. *Let (Π^i) be an ideal of K and suppose $1 < i \leqq p$. For $0 \leqq j, m < p$, define $\alpha_{j,m}$ as follows:*

(i) *If $j + m \leqq p - 1$, $\alpha_{j,m} = x^j(\Pi_2^m \Pi \pi^{-jt'})$.*

(ii) *If $j + m = p$ and $i > j + 1$, $\alpha_{j,m} = x^j(\Pi_2^m \Pi \pi^{-jt'})$.*

(iii) *If $j + m = p$ and $i \leqq j + 1$, $\alpha_{j,m} = x^j(\Pi_2^m \Pi \pi^{-jt'-1})$.*

(iv) *If $j + m > p$, $\alpha_{j,m} = x^j(\Pi_2^m \Pi \pi^{-jt'-1})$.*

Then, $\{\alpha_{j,m} | 0 \leqq j, m < p\}$ is a basis of (Π^i) over $\mathfrak{o}$.

LEMMA 12. *Let $\alpha_{j,m}$ be as in Lemma 10. Let L_{m+1} be an $\mathfrak{o}$-submodule of (Π^i) generated by $\alpha_{j,m}$ for $0 \leqq j < p$. Then, L_{m+1} is an $\mathfrak{o}G_2$-submodule of (Π^i) and*

$$(\Pi^i) = L_1 \oplus \cdots \oplus L_p.$$

Further we need two lemmas, which play the important role of the proof of the main theorem (Theorem 15).

LEMMA 13. *Let e be the absolutely ramification index of k and $t = p^2t' + p + 1$. Then, $(p - 1)t' + 1 < e$.*

Proof. As is well known, $1 \leqq t < p^2e/(p - 1)$. Then, it follows that

$$(p - 1)t' + 1 \leqq e.$$

Suppose $(p - 1)t' + 1 = e$. Then, from [9], Proposition 1.1,

$$\mathrm{tr}_{G_2}\mathfrak{D} = \left(\Pi_2^{p(p-1)t'+p}\right),$$

and so $\mathrm{tr}_{G_2}\mathfrak{D} = (p)$. This means that $\mathfrak{D}$ is not $\mathfrak{o}G$-indecomposable. S.V. Vostokov [11] proved that if the ramification index p^m of an abelian p-extension L/k does not divide the different of L/k, then an ideal of L/k is indecomposable. By his results, we have that $\mathfrak{D}$ is indecomposable. This is a contradiction, and the proof of Lemma 13 is completed.

LEMMA 14. *Let L_1 and L_2 be as in Lemma 12. Then, L_1 is not $\mathfrak{o}G_2$-isomorphic to L_2.*

Proof. Let A_i be the matrix representation afforded by the $\mathfrak{o}G$-module L_i for $i = 1, 2$. Then,

$$A_1(x) = \begin{pmatrix} 0 & 0 & & \cdots & 0 \\ \pi^{t'+1} & & & & a_1 \\ & & & 0 & \\ & \pi^{t'} & & & \vdots \\ & 0 & \ddots & & \\ & & & \pi^{t'} & a_{p-1} \end{pmatrix}$$

and

$$A_2(x) = \begin{pmatrix} 0 & 0 & & \cdots & 0 \\ \pi^{t'} & & & & b_1 \\ & \pi^{t'} & & 0 & \vdots \\ & 0 & \ddots & & \\ & & & \pi^{t'} & b_{p-1}\pi \end{pmatrix}$$

where

$$a_j = -\binom{p}{j}\pi^{-(p-j-1)t'} \quad \text{and} \quad b_j = -\binom{p}{j}\pi^{-(p-j-1)t'-1}.$$

Suppose L_1 is isomorphic to L_2. Then, there exists an invertible matrix $A = (a_{mn})$ in $GL(p, \mathfrak{o})$ such that

$$(12) \qquad AA_1(x) = A_2(x)A.$$

Then

$$a_{12}\pi^{t'+1} = 0,\ a_{13}\pi^{t'} = 0, \dots, a_{1p-1}\pi^{t'} = 0$$

and

$$a_{12}a_1 + \cdots + a_{1p}a_{p-1} = 0.$$

Therefore, $a_{12} = \cdots = a_{1p-1} = a_{1p} = 0$. Also, from the $(2,1)$ entry of (12),

$$a_{22}\pi^{t'+1} = \pi^{t'}a_{11} + b_1 a_{p1}.$$

Lemma 13 gives $b_1 \equiv 0\ (\pi^{t'+1})$, and hence $\pi^{t'}a_{11} \equiv 0\ (\pi^{t'+1})$, so $a_{11} \equiv 0\ (\pi)$. This implies $A \notin GL(p, \mathfrak{o})$, which is a contradiction. The proof of Lemma 14 is completed.

We are ready to prove one of the main theorems.

THEOREM 15. *Let K/k be a wildly ramified extension of degree p^2, and suppose that $G_1 \neq G_2$ and $|G_2| = p$. Then, if $i \not\equiv 1\ (p^2)$, $V(\Pi^i) = G_1$.*

Proof. From Propositions 8 and 9, it is sufficient to prove Theorem 15 for case (iii) with $t \equiv p + 1\ (p^2)$, i.e., $1 < i \leq p$ and $t = p^2t' + p + 1$. By S.V.

Vostokov's results [11] together with Lemma 13, (Π^i) is an indecomposable $\mathfrak{o}G$-module. Suppose $V(\Pi^i) = G_2$. Then, from [2], p. 449, (19.2) Theorem, there is an indecomposable $\mathfrak{o}G_2$-submodule M of (Π^i) such that (Π^i) is a direct summand of $\mathfrak{o}G \otimes_{G_2} M$. Therefore, all indecomposable components of $\mathfrak{o}G_2$-module (Π^i) are isomorphic to M. Hence L_1 and L_2 are isomorphic because $\dim_{\mathfrak{o}} L_1 = \dim_{\mathfrak{o}} L_2 = p$. This is a contradiction, and Theorem 15 is proved.

Section 3

As in §2, let K/k be a wildly ramified extension of degree p^2, and assume that $G_1 \neq G_2$ and $|G_2| = p$. In this section, we consider case (ii), $i = 1$. Let t be the second ramification number of K/k. Using arguments similar to the proof of Proposition 9, we have:

PROPOSITION 16. *Let K/k and t be as above. Then, if $t \not\equiv 1\ (p^2)$, $V(\Pi) = G_1$.*

We devote the remainder of this paper to the computation of $V(\Pi)$ with $0 \leqq e_1 < p - 1$, where e denotes the absolutely ramification index of k. Since $1 \leqq t < p^2 e/(p-1)$, it is easily seen that

(13) if $e_1 \neq 0$, then $e_0 \leqq t'$ and if $e_1 = 0$, then $e_0 - 1 \leqq t'$.

Since G is of order p^2, G is either a cyclic group of order p^2 or an elementary abelian group of type (p, p). First we treat the case where G is cyclic.

LEMMA 17. *Let G be a cyclic group of order p^2 with a generator σ, and let θ be a p^2-th root of 1. $\mathfrak{o}'$ denotes the ring of all integers of $k(\theta)$. Then, in $\mathfrak{o}'G$,*

$$\sum_{i=1}^{p^2-1} \theta^{p^2-1-i}\sigma^i \equiv \mathrm{tr} + \sum_{i=1}^{p^2-2} (\theta-1)^{p^2-1-i}(\sigma-1)^i (p(\theta-1)),$$

where $\mathrm{tr} = \sum_{i=0}^{p^2-1}\sigma^i$.

Proof. We have

$$\sum \theta^{p^2-1-i}\sigma^i = \mathrm{tr} + \sum_{i=1}^{p^2-1} (\theta^i - 1) + \sum_{i=1}^{p^2-2} \left(\theta^{p^2-1-i} - 1\right)(\sigma^i - 1).$$

Let $y = \theta - 1$ and $x = \sigma - 1$. Then,

$$\sum_{i=1}^{p^2-2} (\theta^{p^2-1-i} - 1)(\sigma^i - 1)$$
$$= \sum_{i=1}^{p^2-2} \left(\sum_{j=1}^{p^2-1-i} \binom{p^2-1-i}{j} y^j \right) \left(\sum_{m=1}^{i} \binom{i}{m} x^m \right)$$
$$= \sum_{j=1}^{p^2-2} \left\{ \sum_{m=1}^{p^2-1-j} \left\{ \sum_{m \leqq i \leqq p^2-1-j} \binom{p^2-1-i}{j} \binom{i}{m} \right\} x^m \right\} y^j.$$

From the formula

$$\sum_{i=m}^{n} \binom{i}{m} \binom{n+s-i-1}{n-i} = \binom{n+s}{m+s}$$

(for example, see [8]), this becomes

$$\sum_{j=1}^{p^2-2} \left\{ \sum_{m=1}^{p^2-1-j} \binom{p^2}{m+j+1} x^m \right\} y^j.$$

Therefore,

$$\sum \theta^{p^2-1-i} \sigma^i \equiv \sum_{m=1}^{p^2-2} y^{p^2-1-m} x^m (p(\theta - 1)),$$

which completes the proof of Lemma 17.

LEMMA 18. *Let K/k be as above, and let M be an $\mathfrak{o}$-submodule of* (Π) *generated by $\sigma^i(\Pi)$ for $0 \leqq i < p^2$. Denote by $\mathfrak{d}(M)$ the discriminant of M. Then,*

$$\mathrm{val}_k(\mathfrak{d}(M)) = 2p^2((p-1)t' + 1).$$

Proof. From [1], p. 12, Proposition 4, we have

$$\mathfrak{d}(M) = \det\left(\mathrm{tr}\, \sigma^i(\Pi) \sigma^j(\Pi)\right).$$

Since $\det(\mathrm{tr}\, \sigma^i(\Pi)\sigma^j(\Pi))$ is a cyclic determinant,

$$\det\left(\mathrm{tr}\, \sigma^i(\Pi)\sigma^j(\Pi)\right) = \Pi_\theta \left(\sum_{i=0}^{p^2-1} \theta^{-i} \mathrm{tr}\left(\Pi \sigma^i(\Pi)\right) \right), \tag{14}$$

where the product is taken over all p^2-th roots θ of 1. Then, from Lemma 17, it follows that for some integer α of $\mathfrak{O}$,

$$\sum_{i=0}^{p^2-1} \theta^{-i}\operatorname{tr}(\Pi\sigma^i(\Pi))$$
$$= \theta((\operatorname{tr}\Pi)^2 + \sum_{i=1}^{p^2-2} (\theta-1)^{p^2-1-i}\operatorname{tr}\big(\Pi(\sigma-1)^i(\Pi) + \operatorname{tr}(p\alpha)\big).$$

Let $i = i_1 p + i_0$ with $0 \leqq i_1, i_0 < p$, and so

$$\operatorname{val}_K(\sigma-1)^i(\Pi) = 1 + i_0 + i_1(p^2t' + 1)$$

since $\sigma \in G_1$ and $\sigma^p \in G_t(= G_2)$. Then, from [9], Proposition 1.1, it follows

$$\operatorname{val}_k(\operatorname{tr}\big(\Pi(\sigma-1)^i(\Pi)\big) \geqq (p-1)t' + i_1t' + 2$$

and

$$\operatorname{val}_k\big((\operatorname{tr}\Pi)^2\big) = 2((p-1)t' + 1).$$

By (13), we have

$$\begin{aligned}
&\operatorname{val}\big((\theta-1)^{p^2-1-i}\operatorname{tr}\big(\Pi(\sigma-1)^i(\Pi)\big) - \operatorname{val}\big((\operatorname{tr}\Pi)^2\big)\\
&\quad = (p^2-1-i)e/p(p-1) + i_1t' - (p-1)t'\\
&\quad = e_0 + e_1(p-i_1)/(p-1) - ((1+i_1)/p)(e/(p-1))\\
&\qquad + (p-i_1-1)(e_0-t').
\end{aligned}$$

We distinguish four cases as follows: (a) $e_1 \neq 0$ and $i_1 \leqq p-2$, (b) $e_1 \neq 0$ and $i_1 = p-1$, (c) $e_1 = 0$ and $i_1 \leqq p-2$, (d) $e_1 = 0$ and $i_1 = p-1$. In case (a),

$$\begin{aligned}
&\operatorname{val}\big((\theta-1)^{p^2-1-i}\operatorname{tr}\big(\Pi(\sigma-1)^i(\Pi)\big)\big) - \operatorname{val}\big((\operatorname{tr}\Pi)^2\big)\\
&\quad \geqq e_0 + 2e_1/(p-1) - e/(p-1)\\
&\quad > 0.
\end{aligned}$$

In case (b), $i_0 \leqq p-2$ because $i < p^2-1$. Then,

$$\begin{aligned}
&\operatorname{val}\big((\theta-1)^{p^2-1-i}\operatorname{tr}\big(\Pi(\sigma-1)^i(\Pi)\big) - \operatorname{val}\big((\operatorname{tr}\Pi)^2\big)\\
&\quad \geqq e_0 + e_1/(p-1) - ((p-1)/p)(e/(p-1))\\
&\quad > 0.
\end{aligned}$$

Similarly, for cases (c) and (d), we obtain

$$\operatorname{val}\left((\theta-1)^{p^2-1-i}\operatorname{tr}\left(\Pi(\sigma-1)^i(\Pi)\right)-\operatorname{val}\left((\operatorname{tr}\Pi)^2\right)>0.\right.$$

Therefore, from (14), we conclude

$$\operatorname{val}\left(\det\left(\operatorname{tr}\sigma^i(\Pi)\sigma^j(\Pi)\right)\right)=2p^2((p-1)t'+1),$$

which is the desired result.

Next, we consider the case where G is an elementary abelian group of p^2, and we prove again two lemmas.

LEMMA 19. *Let A_i be a matrix of type (p,p) for $1 \leqq i \leqq p$, and let a matrix B of type (p^2,p^2) be given by*

$$B=\begin{pmatrix} A_1 & A_2 & \dots & A_p \\ A_2 & A_3 & \dots & A_1 \\ & \dots & & \\ A_p & A_1 & \dots & A_{p-1} \end{pmatrix}.$$

Then

$$\det B=(-1)^{(p-1)/2}\Pi_\theta\left(\det\left(\sum_{i=0}^{p-1}\theta^i A_i\right)\right),$$

where the product is taken over all p-th roots θ of 1.

Proof. Using the same procedure as in the proof of the formula of cyclic determinants, we can prove Lemma 19.

LEMMA 20. *Let K/k be a non-cyclic extension of degree p^2, and let σ and τ be generators of Galois group G such that G_2 is generated by τ. M denotes an $\mathfrak{o}$-submodule generated by $\sigma^i\tau^j(\Pi)$ for $0 \leqq i, j < p$. Then*

$$\operatorname{val}_k \mathfrak{d}(M)=2p^2((p-1)t'+1).$$

Proof. Let a matrix A of type (p,p) be defined by

$$A=\left(\sigma^i\sigma^j(\Pi)\right)\quad \text{for } 0 \leqq i, j<p,$$

and let

$$A_m=\tau^{m-1}(A)\left(=\left(\tau^{m-1}\left(\sigma^i\sigma^j(\Pi)\right)\right)\right)\quad \text{for } 1 \leqq m \leqq p.$$

As in Lemma 19, let

$$B = \begin{pmatrix} A_1 & A_2 & \cdots & A_p \\ A_2 & A_3 & \cdots & A_1 \\ & & \cdots & \\ A_p & A_1 & \cdots & A_{p-1} \end{pmatrix}.$$

Then we have

$$\mathfrak{d}(M) = (\det{}^t B \cdot \det B).$$

From Lemma 19, it follows that

$$\det B = (-1)^{(p-1)/2} \Pi_\theta \left(\det\left(\sum \theta^i \tau^i (A) \right) \right).$$

By the formula of cyclic determinants and from [7] Lemma 5, we have

$$\begin{aligned} &\det\left(\sum \theta^i \tau^i (A) \right) \\ &\quad = \prod_{m=0}^{p-1} \left(\sum_{j=0}^{p-1} \zeta^{jm} \sigma^j \left(\sum \theta^i \tau^i (\Pi) \right) \right) \\ &\quad = \Pi_m \Bigg(\operatorname{tr} \Pi + \sum_{1 \leq i, j < p-1} (\zeta^{-m} - 1)^{p-1-j} \\ &\qquad\qquad \times (\theta^{-1} - 1)^{p-1-i} (\sigma - 1)^j (\tau - 1)^i (\Pi) \\ &\qquad + \sum_{1 \leq j < p-1} (\zeta^{-m} - 1)^{p-1-j} (\sigma - 1)^j \left(\sum_{i=0}^{p-1} \tau^i \right) (\Pi) + p(\theta^{-1} - 1)\alpha \Bigg), \end{aligned}$$

where $\alpha \in \mathfrak{O}$ and ζ denotes a primitive p-th root of 1. Similarly as in the proof of Lemma 18, we can obtain

$$\operatorname{val}_k(\det B) = p^2((p-1)t' + 1)$$

and

$$\operatorname{val}_k(\mathfrak{d}(M)) = 2p^2((p-1)t' + 1),$$

and the proof of Lemma 20 is completed.

We can now prove one of the main results.

THEOREM 21. *Let K/k be a wildly ramified extension of degree p^2, and suppose $G_1 \neq G_2$ and $|G_2| = p$. Let t denote the second ramification number of K/k. Then, $V(\Pi^i) = G_2$ for $i \equiv 1\ (p^2)$ if and only if $t \equiv 1\ (p^2)$.*

Proof. As pointed out in the beginning of §2, we may set $i = 1$. Proposition 16 establishes the "only if" part of Theorem 21, so let us prove the converse part. Let $x = \tau - 1$ for a generator τ of G_2 and $t = p^2t' + 1$ as before. For $0 \leqq j < p$, define an integer α_j of (Π) by

$$\alpha_j = x^j(\Pi\pi^{-jt'}),$$

and set $L_1 = \mathfrak{o}\alpha_0 + \mathfrak{o}\alpha_1 + \cdots + \mathfrak{o}\alpha_{p-1}$. Then L_1 is an $\mathfrak{o}G_2$-submodule of (Π^i). We define an $\mathfrak{o}$-submodule L of K by $L = \sum_{i=0}^{p-1}\sigma^i(L_1)$, where $G = \bigcup \sigma^i G_2$. Let $M = \sum \mathfrak{o}\sigma^i\tau^j(\Pi)$ and $M_1 = \sum \mathfrak{o}\tau^i(\Pi)$. We calculate the module index $[L : M]$ (for the definition, see [1], p. 10). Clearly,

$$[L : M] = ([L_1 : M_1])^p.$$

Since $\sum \mathfrak{o}x^j = \mathfrak{o}G_2$, it follows easily that

$$\mathrm{val}_k([L_1 : M_1]) = t' + \cdots + (p-1)t' = p(p-1)t'/2$$

and

$$\mathrm{val}_k([L : M]) = p^2(p-1)t'/2.$$

On the other hand, we have

$$[(\Pi) : M] = [\mathfrak{O} : M]/[\mathfrak{O} : (\Pi)],$$

so

$$[(\Pi) : M]^2 = \mathfrak{d}(M)\mathfrak{d}(\mathfrak{O})^{-1}(\pi^{-2}).$$

As is easily shown, $\mathrm{val}_k(\mathfrak{d}(\mathfrak{O})) = (p-1)(p^2t' + 2) + 2p(p-1)$. Then, we obtain

$$\mathrm{val}_k([(\Pi) : M]) = p^2(p-1)t'/2 = \mathrm{val}_k([L : M]),$$

and hence $(\Pi) = L$. Since L is isomorphic to $\mathfrak{o}G \otimes_{G_2} L_1$, (Π) is also isomorphic to $\mathfrak{o}G \otimes_{G_2} L_1$. Therefore, from [2], p. 449, (19.2) Theorem, it follows that $V(\Pi) = G_2$. The proof of Theorem 21 is complete.

The author wishes to thank the referee for his advice.

References

1. J. Cassels and A. Fröhlich, *Algebraic number theory*, Academic Press, New York, 1967.
2. C.W. Curtis and I. Reiner, *Methods of representation theory* vol. 1, Interscience, New York, 1981.
3. A. Fröhlich, *Some topics in the theory of module conductors*, Oberwolfach Berichte vol. 2 (1966), pp. 59–83.

4. H. HASSE, *Führer, Discriminant und Verzweigungskörper relativ-Abelscher Zahlkörper*, J. Reine Angew. Math., vol. 162 (1930), pp. 169–184.
5. E. NOETHER, *Normalbasis bei Körpern ohne höhere Verzweigung*, J. Reine Angew. Math., vol. 167 (1932), pp. 147–152.
6. Y. MIYATA, *On a characterization of the first ramification group as the vertex of the ring of integers*, Nagoya Math. J., vol. 43 (1971), pp. 151–156.
7. ———, *On the module structure of the ring of all integers of a $\mathfrak{p}$-adic number field*, Nagoya Math. J., vol. 54 (1974), pp. 53–59.
8. Sūgaku Jiten (Mathematical dictionary), Iwanami, Tokyo, 1968.
9. S. ULLOM, *Normal bases in Galois extensions of number fields*, Nagoya Math. J., vol. 34 (1969), pp. 153–167.
10. ———, *Integral normal bases in Galois extensions of local fields*, Nagoya Math. J., vol. 39 (1970), pp. 141–148.
11. S.V. VOSTOKOV, *Ideals of an abelian p-extension of a local field as Galois modules*, Zap. Naučn. Sem. Lenigrad. Otdel. Mat. Inst. Steklov. (LOMI), vol. 57 (1976), pp. 64–84 (Russian).
12. H. YOKOI, *On the ring of integers in an algebraic number field as a representation module of Galois group*, Nagoya Math. J., vol. 16 (1960), pp. 83–90.

SHIZUOKA UNIVERSITY
SHIZUOKA, JAPAN