Y. Miyata
Nagoya Math. J.
Vol. 107 (1987), 49-62

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

YOSHIMASA MIYATA

Let k be a $\mathfrak{p}$-adic number field with the ring $\mathfrak{o}$ of all integers in k, and K be a finite normal extension with Galois group G. Π denotes a prime element of the ring $\mathfrak{O}$ of all integers in K. Then, an ideal (Π^a) of $\mathfrak{O}$ is an $\mathfrak{o}G$-module. E. Noether [5] showed that if K/k is tamely ramified, $\mathfrak{O}$ is a free $\mathfrak{o}G$-module. A. Fröhlich [2] 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 is the first ramification group of K/k. Now we define the vertex $V(\Pi^a)$ of (Π^a) as the minimal normal subgroup S of G such that (Π^a) is relatively projective with respect to a subgroup S of G (cf. [7] § 1). Then, the above generalization by A. Fröhlich implies $V(\mathfrak{O}) = G_1$. In the previous paper [7], we proved $G_1 \supseteq V(\Pi^a) \supseteq G_2$, where G_2 is the second ramification group of K/k (cf. [7] Theorem 5). Further, we dealt with the case where $G = G_1$ is of order p^2, and proved that if $V(\Pi^a) \neq G_1$, then $a \equiv 1(p^2)$ and $t_2 \equiv 1(p^2)$ for the second ramification number t_2 of K/k (cf. [7] Theorems 15 and 21). The purpose of this paper is to prove the similar theorem for the wildly ramified p-extension of degree p^n (Theorem 7).

Throughout this paper, we assume that p is an odd prime and the p-extension K/k is wildly ramified. In the first section § 1, we shall prove that (Π^a) is an indecomposable $\mathfrak{o}G$-module under the assumption relating to the ramification numbers of subextension of K/k (Theorem 2), which is a generalization of S.V. Vostokov's theorem concerning to the indecomposablity of ideals (Π^a) of abelian p-extensions ([10] Theorem 5). In the second section § 2, we shall deal with the case where G_2 is of order p, and we shall prove that if $a \not\equiv 1$ $(|G_1|)$, then $V(\Pi^a) = G_1$, where $|G_1|$ denotes the order of G_1 (Theorem 6). In the last section § 3, we shall prove that if $V(\Pi^a) \neq G_1$ and $t_1 = 1$, then $a \equiv 1$ $(|G_1|)$ and $t_i \equiv 1$ $(|G_1/G_{i+1}|)$ for $1 \leqq i \leqq r$, where $t_1, t_2, \cdots, t_r$ are ramification numbers of K/k and G_i is

Received January 30, 1986.

the t_i-th ramification group of K/k (Theorem 7).

§ 1.

Let K/k be a wildly ramified p-extension of degree p^n, and $t_1, t_2, \cdots, t_r$ be ramification numbers of K/k with $t_1 < t_2 < \cdots < t_r$. In this section, we shall prove that (Π^a) is $\mathfrak{o}G$-indecomposable. First we observe that if $a \equiv a' \ (p^n)$, then $(\Pi^{a'})$ is $\mathfrak{o}G$-isomorphic to (Π^a). Therefore, without loss of generality, we assume

$$0 \leqq a < p^n .$$

We define a function $m(t)$ by

$$m(t) = t - [t/p] ,$$

where $[x]$ denotes an integer such that $[x] \leqq x < [x] + 1$. Denote by e_K the absolute ramification index of K. For $1 \leqq i \leqq r$, let G_i be the t_i-th ramification group of K/k and K_i be the subfield corresponding to G_i. Clearly,

$$k = K_1 \subset K_2 \subset \cdots \subset K_r \subset K .$$

We state now S. V. Vostokov's results which are used in the following. First, from [9] Proposition 1, we have

Proposition 1. *Let K/k and t_i be as in the above. Let e_i be the absolute ramification index of K_i. Then, $m(t_r) = e_K/p$ if and only if K/k is cyclic and $m(t_i) = e_i$ for $1 \leqq i \leqq r$.*

From [10] Theorem 5, we have

Theorem 1. *Let K/k be an abelian p-extension. Then, if $m(t_r) < e_K/p$, (Π^a) is $\mathfrak{o}G$-indecomposable.*

Then, from Proposition 1 and Theorem 1, we can prove

Corollary 1. *If K/k is a non-cyclic abelian p-extension, then (Π^a) is $\mathfrak{o}G$-indecomposable.*

In this section, we assume

$$(1) \qquad m(t_r) < e_K/p .$$

Further, we need some lemmas. Let σ be an element of G_r with $\sigma \neq 1$. Then, it is well known that $\sigma^p = 1$ and σ belongs to the center of G (for example, see [8] p. 77). Denote by Z and K_Z the subgroup generated by

σ and the subfield corresponding to Z, respectively. Clearly, the ramification number t of K/K_Z is t_r. Let $\bar{t} = t - p[t/p]$ and so $\bar{t} \neq 0$ since $(t, p) = 1$ by (1). For $0 \leqq i < p^{n-1}$ and $0 \leqq j < p$, we define integers $a(i, j)$ and $b(i, j)$ as follows:

$$a(i, j) = [(pi + jt + \bar{t} - a)/p^n] \quad \text{and} \quad b(i, j) = pi + jt + \bar{t} - a(i, j)p^n .$$

Obviously, $a \leqq b(i, j) < a + p^n$ and

$$a(i, 0) \leqq a(i, 1) \leqq \cdots \leqq a(i, p-1) . \tag{2}$$

LEMMA 1. *Suppose $m(t) < e_K/p$. Then, $b(i', j') \equiv b(i, j)(p^n)$ if and only if $i' = i$ and $j' = j$.*

Proof. Suppose $b(i', j') \equiv b(i, j)(p^n)$. Then, $b(i', j') \equiv b(i, j)(p)$ and so $j' = j$ because $(t, p) = 1$ as remarked above. Thus $i' = i$. The proof of the converse is obvious.

Next, we define submodules L_i of (Π^a) for $0 \leqq i < p^{n-1}$. For $0 \leqq i < p^{n-1}$ and $0 \leqq j < p$, elements $A_{i,j}$ of K are defined by

$$A_{i,j} = \Pi_1^i x^j(\Pi^{\bar{t}})\pi^{-a(i,j)} ,$$

where $x = \sigma - 1$, and Π_1 and π are prime elements of K_Z and k, respectively. Let L_i be

$$L_i = \mathfrak{o}A_{i,0} + \mathfrak{o}A_{i,1} + \cdots + \mathfrak{o}A_{i,p-1} .$$

We shall prove that L_i is an $\mathfrak{o}G$-module.

LEMMA 2. *Let val_K denote the valuation of K. Then,*

$$\mathrm{val}_K (A_{i,j}) = b(i, j) .$$

Proof. From $(j, p) = 1$ for $1 \leqq j < p$, it follows

$$\mathrm{val}_K (x^j(\Pi^{\bar{t}})) = jt + \bar{t} .$$

Thus, $\mathrm{val}_K (A_{i,j}) = pi + jt + \bar{t} - p^n a(i, j)$ and hence $\mathrm{val}_K (A_{i,j}) = b(i, j)$.

By Lemma 1 and Lemma 2, we have

$$(\Pi^a) = L_0 \oplus L_1 \oplus \cdots \oplus L_{p^{n-1}-1} .$$

Clearly, for $0 \leqq j < p - 1$,

$$x(A_{i,j}) = \pi^{a(i,j+1)-a(i,j)} A_{i,j+1} . \tag{3}$$

Since $(x+1)^p = \sigma^p = 1$, $x^p = -\sum_{j=1}^{p-1}\binom{p}{j}x^j$. Then, we have

$$x(A_{i,p-1}) = -\sum_{j=1}^{p-1}\binom{p}{j}\pi^{a(i,j)-a(i,p-1)}A_{i,j}\,. \tag{4}$$

LEMMA 3. *For $0 \leqq i < p^{n-1}$, L_i is an $\mathfrak{o}Z$-module.*

Proof. By (2), $\pi^{a(i,j+1)-a(i,j)} \in \mathfrak{o}$. Then, by (3), $x(A_{i,j}) \in L_i$ for $0 \leqq j < p-1$. Define integers b_i by

$$b_i = pi + (p-1)t + \bar{t} - a - p^n a(i, p-1)\,.$$

By the definition of $a(i, p-1)$, we have $0 \leqq b_i < p^n$. Since $pm(t) = (p-1)t + \bar{t} < e_K$ by (1),

$$pi + e_K - a \geqq p^n a(i, p-1) + b_i\,.$$

Then,

$$e_K - p^n a(i, p-1) \geqq b_i + a - pi > -p^n\,.$$

Therefore, we obtain $e_K - p^n a(i, p-1) \geqq 0$. By (4), $x(A_{i,p-1}) \in L_i$, which completes the proof of Lemma 3.

Now, let θ be a primitive p-th root of 1 and $k_0 = k(\theta)$. For $0 \leqq j < p$, E denotes a central idempotent $(\sum_{u=0}^{p-1}\theta^{ju}\sigma^u)/p$ of k_0Z. According to the arguments used in [6], we can prove

LEMMA 4. *Let E be a central idempotent of kZ and α be an element of $\mathfrak{O}$ such that* $\mathrm{val}_K(\alpha) \equiv \bar{t}(p)$. *Then,*

$$\mathrm{val}_K(pE\alpha) \leqq \mathrm{val}_K((\textstyle\sum \sigma^u)\alpha)\,.$$

LEMMA 5. *Let e be the absolute ramification index of k and suppose that $m(t) < p^{n-1}e - p^{n-1} + 1$. Then, for $0 \leqq i < p^{n-1}$, L_i is $\mathfrak{o}Z$-indecomposable.*

Proof. By the definition of $A_{i,0}$, we have

$$\mathrm{val}_K(A_{i,0}) \equiv \bar{t}(p)\,.$$

Let E be an idempotent of kZ. Then, from Lemma 4, it follows

$$\mathrm{val}_K(pEA_{i,0}) \leqq \mathrm{val}_K((\textstyle\sum \sigma^u)A_{i,0}) = pi + (p-1)t + \bar{t} - p^n a(i, 0)\,.$$

Since $(p-1)t + \bar{t} = pm(t) < p^n e - p^n + p$ by the assumption, we have

$$pi + (p-1)t + \bar{t} - p^n a(i, 0) < p^n e - p^n + p + pi - p^n a(i, 0)\,. \tag{5}$$

We distinguish two cases: (i) $pi + \bar{t} \geqq a$, (ii) $pi + \bar{t} < a$. In case (i), $pi + \bar{t} \geqq a$, we have $a(i, 0) = 0$ because $0 \leqq a < p^n$. Therefore, by (5),

$\mathrm{val}_K(EA_{i,0}) < 0$ and so

$$\mathrm{val}_K(EA_{i,0}) < a\,,$$

which implies that L_i is $\mathfrak{o}Z$-indecomposable. In case (ii) $pi + \bar{t} < a$, we have $a(i, 0) = -1$ because $0 \leqq a < p^n$. From (5), it follows

$$pi + pm(t) - p^n e < pi + p\,.$$

Since p divides $(pi + pm(t) - p^n e)$,

$$pi + pm(t) - p^n e \leqq pi\,.$$

As $pi + \bar{t} < a$, we have

$$\mathrm{val}_K(EA_{i,0}) < a\,.$$

This also implies that L_i is $\mathfrak{o}Z$-indecomposable, and the proof is completed.

We finally request the next proposition.

PROPOSITION 2. *Let K/k be a wildly ramified p-extension of degree p^n, and let Z, L_i $(0 \leqq i < p^{n-1})$ be as above. Suppose that $(\Pi^a) \cap K_Z$ is an indecomposable $\mathfrak{o}[G/Z]$-module and $\mathfrak{o}Z$-modules L_i are indecomposable. Then, (Π^a) is an indecomposable $\mathfrak{o}G$-module.*

Proof. Let f be an $\mathfrak{o}G$-endomorphism of (Π^a) such that $f^2 = f$. Then, f is a kG-endomorphism of K. Let $E_j = (\sum \theta^{ju}\sigma^u)/p$ as before. Since Z is contained in the center of G, E_0 is a kG-endomorphism of K. Let $f_0 = E_0 f$ and so f_0 is an kG-endomorphism of K. Clearly, for $\alpha \in K_Z$, $f(\alpha) = f_0(\alpha)$ and $f(\alpha) \in K_Z$. Therefore, by the assumption that $(\Pi^a) \cap K_Z$ is indecomposable, we have $f_0 = E_0$. Since $f((\Pi^a))$ is an $\mathfrak{o}Z$-module, $f((\Pi^a))$ can be expressed as a direct sum of indecomposable $\mathfrak{o}Z$-modules M_u for $1 \leqq u \leqq v$:

$$f((\Pi^a)) = M_1 \oplus M_2 \oplus \cdots \oplus M_v\,.$$

Since L_i is $\mathfrak{o}Z$-indecomposable by the assumption, it follows from Krull-Schmidt Theorem that for some $i(u)$ with $0 \leqq i(u) < p^{n-1}$, M_u is isomorphic to $L_{i(u)}$. We note that $kL_i \cong kZ$ and hence $kM_u \cong kZ$. Thus

$$kf((\Pi^a)) = kZ \oplus \cdots \oplus kZ\,.$$

Since $f_0 = E_0$ as verified above, $kf((\Pi^a)) \supseteq K_Z$ and so $v = p^{n-1}$. This implies $f = 1$ and hence (Π^a) is $\mathfrak{o}G$-indecomposable.

We are ready to prove the following theorem, which is one of the main results of this paper.

THEOREM 2. *Let K/k be a wildly ramified p-extension of degree p^n. Let L/F be a subextension of degree p in the extension K/k, and t be the ramification number of L/F. Suppose $m(t) < e_F - ([F: k] - 1)$ for each extension L/F, where $[F: k]$ denotes the degree of F/k. Then, (Π^a) is $\mathfrak{o}G$-indecomposable for each $a \geqq 0$.*

Proof. We use induction on n. For $n = 1$, the result follows from Theorem 1. Let Z be as above. Then, by the induction hypothesis, we have $(\Pi^a) \cap K_Z$ is $\mathfrak{o}[G/Z]$-indecomposable. By Lemma 5, L_i is $\mathfrak{o}Z$-indecomposable for $0 \leqq i < p^{n-1}$. Hence, the result follows from Proposition 2, and the proof of Theorem 2 is completed.

§ 2.

Let K/k be a wildly ramified p-extension of degree p^n as before. In the rest of this paper, we deal with investigating the vertex $V(\Pi^a)$ of (Π^a). Let us begin with recalling the results of the previous paper [7].

THEOREM 3 ([7] Theorem 5). *Let K/k be a wildly ramified extension. Let G_1 and G_2 be the first and second ramification groups of K/k, respectively. Then, $G_1 \supseteq V(\Pi^a) \supseteq G_2$.*

THEOREM 4 ([7] Theorem 6). *Let K/k, G_1 and G_2 be as in Theorem 3. Suppose $G_2 = \{1\}$.*

(i) *If $a \not\equiv 1$ $(|G_1|)$, then $V(\Pi^a) = G_1$.*

(ii) *If $a \equiv 1$ $(|G_1|)$, then $V(\Pi^a) = \{1\}$.*

By the definition of the vertex of the ideal and [7] Lemma 7, we can prove

LEMMA 6. *Let K/k be as above and V be the vertex of (Π^a). Let L/F be a subextension of K/k such that $K_V \subseteq F \subseteq L \subseteq K$. Then,*

(i) $V((\Pi^a) \cap L) \subseteq V$.

(ii) $V(\mathrm{tr}_{K/F}((\Pi^a) \cap L)) \subseteq V$, *where $\mathrm{tr}_{L/F}$ is the trace map from L to F.*

Proof. (i) By the definition of the vertex of (Π^a), there exists an $\mathfrak{o}V$-endomorphism f of (Π^a) such that $1 = \sum_g gfg^{-1}$, where the sum is taken over a set of coset representatives of left cosets of V in G. Since the Galois group S of K/L is contained in V, we have $f((\Pi^a) \cap L) \subseteq (\Pi^a) \cap L$, which implies that $(\Pi^a) \cap L$ is relatively projective with respect to

V/S of G/S. Thus $V((\Pi^a)\cap L)\subseteq V$ and the proof of (i) is completed.

(ii) It is sufficient to prove that $V(\mathrm{tr}_{L/F}((\Pi^a)\cap L))\subseteq V((\Pi^a)\cap L)$. Therefore, we may assume $L=K$. Let T be a subgroup of G corresponding to F and $\mathrm{tr}_T=\sum_{g\in T} g$. By the definition of the vertex of (Π^a), there exist an $\mathfrak{o}G$-module M and an $\mathfrak{o}V$-module N such that

$$(\Pi^a)\oplus M=\mathfrak{o}G\otimes_V N\,.$$

Thus,

$$\mathrm{tr}_{K/F}((\Pi^a))\oplus \mathrm{tr}_T M=\mathfrak{o}G\otimes_V \mathrm{tr}_T N\,.$$

Since $\mathrm{tr}_T N$ is an $\mathfrak{o}[V/T]$-module, $\mathrm{tr}_{K/F}((\Pi^a))$ is relatively projective with respect to V/T. The proof is completed.

Now, from Theorem 3, we can conclude that if $G_1=G_2$, then $V(\Pi^a)=G_1$. Therefore, throughout the rest of this paper, we may assume $G_1\neq G_2$. In this section, we treat the case where G_2 is of order p. Denote by p^m the order of the factor group G_1/G_2. In [7], we treated the case where $m=1$ and proved the following theorem.

THEOREM 5 ([7] Theorems 15 and 21). *Let K/k be a wildly ramified p-extension of degree p^2. Assume $G_1\neq G_2$. Then, $V(\Pi^a)\neq G_1$ if and only if $a\equiv 1\ (p^2)$ and $t_2\equiv 1\ (p^2)$.*

In this section, we treat the case where $m\geqq 2$ and prove the next theorem.

THEOREM 6. *Let K/k be a wildly ramified p-extension of degree p^n. Suppose that $G_1\neq G_2$ and G_2 is of order p. Then, if $a\not\equiv 1\ (p^n)$, $V(\Pi^a)=G_1$.*

At first, we remark that $t_2\equiv 1\ (p)$ because $t_1=1$ by the assumption $G_1\neq G_2$. Then, from [8] p. 91 Lemma 4, we have

LEMMA 7. *Let K/L be a wildly ramified extension of degree p with the remification number t. Suppose $t\equiv 1\ (p)$. Then, (i) and* (ii) *hold.*

(i) *For $p\geqq a\geqq 2$, $\mathrm{tr}_{K/L}((\Pi^a))=(\pi^b)$, where $b=(p-1)[t/p]+2$.*

(ii) *For $a=1$, $\mathrm{tr}_{K/L}((\Pi))=(\pi^b)$, where $b=(p-1)[t/p]+1$.*

As in Section 1, we note that if $a\equiv a'\ (p^n)$, then $(\Pi^{a'})$ is $\mathfrak{o}G$-isomorphic to (Π^a) and $V(\Pi^{a'})=V(\Pi^a)$. Therefore, there is no loss of generality in assuming $2\leqq a<p^n$. Let K_2 be a subfield corresponding to G_2 and denote by Π_1 the prime element of K_2. Let $(\Pi_1^{a_1})=(\Pi^a)\cap K_2$, and so $p^m>a_1\geqq 1$ by $p^n>a\geqq 2$.

PROPOSITION 3. *Let K/k be a wildly ramified extension of degree p^{m+1} and suppose that $G_1 \neq G_2$ and G_2 is of order p. Let a_1 be as in the above. Then, if $p^m > a_1 > 1$, $V(\Pi^a) = G_1$.*

Proof. By Theorem 4 and the assumption $p^m > a_1 > 1$, we have $V(\Pi_1^{a_1}) = G_1$. From Lemma 6, it follows that $V(\Pi_1^{a_1}) \subseteq V(\Pi^a)$, which implies $V(\Pi^a) = G_1$.

We note that $a_1 > 1$ if and only if $a > p$. Therefore, from Proposition 3, we may assume

$$p \geqq a \gneqq 2 . \tag{6}$$

Let $t = t_2$ for brevity. Define an integer a_2 by

$$(\Pi_1^{a_2}) = \mathrm{tr}_{K/K_2}((\Pi^a)) .$$

Then, by Lemma 7 and (6), we have

$$a_2 = (p-1)[t/p] + 2 . \tag{7}$$

LEMMA 8. *Let K/k be as above and assume $m \geqq 2$. Then, if $V(\Pi^a) \neq G_1$, $t \equiv p^2 + p + 1$ (p^3).*

Proof. By Lemma 6, $V(\Pi_1^{a_2}) \subseteq V(\Pi^a)$ and so $V(\Pi_1^{a_2}) \neq G_1$. Then, by Theorem 4, $a_2 \equiv 1$ (p^m) and hence by (7), $(p-1)[t/p] \equiv p^m - 1$ (p^m). Therefore, $[t/p] \equiv p^{m-1} + p^{m-2} + \cdots + 1$ (p^m). Since $t \equiv 1$ (p), $\bar{t} = 1$ and so $t \equiv p^m + p^{m-1} + \cdots + 1$ (p^{m+1}). From the assumption $m \geqq 2$, it follows $t \equiv p^2 + p + 1$ (p^3).

Let p^c be the order of the maximal abelian normal subgroup of G_1. Then, we have

PROPOSITION 4. *Let K/k be as above. Then, if either $m \geqq 3$, or G_1 is abelian, $V(\Pi^a) = G_1$ for $p \geqq a > 1$.*

Proof. By [4] p. 302 Theorem 7.3, we have

$$c(c+1) \geqq 2(m+1) .$$

In case $m \geqq 3$, we have $c \geqq 3$. Therefore, there exists an abelian normal subgroup N of G such that $N \supseteq G_2$ and $|N/G_2| \geqq p^2$. Hence, from [3] p. 171 (V), it follows $t \equiv 1$ $(|N/G_2|)$ and so $t \equiv 1\,(p^2)$. Thus, by Lemma 8, $V(\Pi^a) = G_1$ in this case. Next, we treat the remained case where $m \leqq 2$ and G_1 is abelian. In case $m = 2$, applying the same arguments as in the above, we have $V(\Pi^a) = G_1$. In case $m = 1$, Theorem 5 yields the desired result.

By Proposition 4, we may assume that G_1 is a non-abelian group of order p^3. Moreover, by Lemma 8, t can be written in the form:

$$t = p^3 t' + p^2 + p + 1 . \tag{8}$$

Now, we start to prove lemmas which are used in proving Theorem 6.

LEMMA 9. *Let K/k be as stated in the above. Then, $m(t) < p^2 e - p^2 + 1$.*

Proof. By (8), $m(t) = p^2((p-1)t' + 1)$. From Proposition 1, it follows

$$m(t) < p^2 e .$$

Then, $(p-1)t' + 1 \leqq e - 1$ and so $m(t) \leqq p^2 e - p^2 < p^2 e - p^2 + 1$.

For $0 \leqq i < p^2$, i can be written in the form:

$$i = i_1 p + i_0 ,$$

where $0 \leqq i_1, i_0 < p$.

LEMMA 10. *Let K/k be as above and $t = p^3 t' + p^2 + p + 1$.*
(i) *If $0 \leqq i < (p-2)p + p - 1$, then $a(i, 1) = t'$.*
(ii) *If $i > (p-2)p + p - 1$, then $a(i, 1) = t' + 1$.*

Proof. By the definition of $a(i, 1)$,

$$\begin{aligned} a(i, 1) &= [(p^3 t' + p^2 + p + 1 + 1 + pi - a)/p^3] \\ &= t' + [(p^2(i_1 + 1) + p(i_0 + 1) + 2 - a)/p^3] . \end{aligned}$$

Since $a \leqq p$ by (6), we have that in the case (ii),

$$a(i, 1) = t' + 1 .$$

In case (i), we have

$$p^2(i_1 + 1) + p(i_0 + 1) + 2 - a < p^2(p-1) + p(p-1) + 2 - a < p^3 ,$$

and so $a(i, 1) = t'$.

For $0 \leqq i < p^2$, let L_i be the $\mathfrak{o}Z$-module as in Section 1 and let A_i be the matrix representation afforded by the $\mathfrak{o}Z$-module L_i. Then, by (3) and (4), we have that for $x = \sigma - 1$,

$$A_i(x) = \begin{pmatrix} 0 & 0 \cdots 0 & \\ x_{i,1} & 0 \cdots 0 & y_{i,1} \\ \vdots & \ddots & \vdots \\ 0 \cdots 0 & x_{i,p-1} & y_{i,p-1} \end{pmatrix},$$

where $x_{i,j} = \pi^{a(i,j)-a(i,j-1)}$ and $y_{i,j} = -\binom{p}{j}\pi^{a(i,j)-a(i,p-1)}$ for $1 \leqq j < p$.

LEMMA 11. *For $0 < i < (p-2)p + (p-1)$, L_i is not isomorphic to L_0.*

Proof. Since $A_{i,j} = \Pi_1^i x^j(\Pi^{\bar{i}})\pi^{-a(i,j)}$ and $a \leqq p$ by (6), we have that for $i > 0$, $a(i, 0) = 0$. By Lemma 10 and the definitions of $x_{i,j}$, $x_{i,1} = \pi^{t'}$. Since $a(0, 0) = -1$, $x_{0,1} = \pi^{t'+1}$. Suppose that for some i, L_i is isomorphic to L_0. Then, there exists an invertible matrix $A = (a_{uv})$ in $GL(p, \mathfrak{o})$ such that

$$AA_0(x) = A_i(x)A\,. \tag{9}$$

Then, $a_{12}x_{0,1} = 0, \cdots, a_{1p}x_{0,p-1} = 0$. Therefore, $a_{12} = \cdots = a_{1p} = 0$. Also, from the (2, 1) entry of (9),

$$a_{22}x_{0,1} = x_{i,1}a_{11} + y_{i,1}a_{p1}\,. \tag{10}$$

By the definitions of $y_{i,1}$ and $a(i, p-1)$,

$$\begin{aligned}\mathrm{val}_K(y_{i,1}) &= p^3e + p^3a(i,1) - p^3a(i,p-1) \\ &= p^3e + p^3a(i,1) - pi - (p-1)t - \bar{t} + b(i,p-1) \\ &= p^3e - pm(t) + p^3a(i,1) + b(i,p-1) - pi\,.\end{aligned}$$

By Lemma 9 and Lemma 10,

$$\mathrm{val}_K(y_{i,1}) > p^3a(i,1) + b(i,p-1) + p^3 - p - pi > p^3t'\,.$$

Therefore, by (10), $\pi^{t'}a_{11} \equiv 0\ (\pi^{t'+1})$ and so $a_{11} \in (\pi)$. This implies $A \notin GL(p, \mathfrak{o})$, which is a contradiction. The proof of Lemma 11 is completed.

LEMMA 12. *Assume $i \geqq (p-1)p$. Then $x_{i,1} = \pi^{t'+1}$, $x_{i,2} = \cdots = x_{i,p-1} = \pi^{t'}$ and $y_{i,j} = -\binom{p}{j}\pi^{(j-p+1)}$ for $1 \leqq j < p$.*

Proof. By definitions of $a(i, j)$, we have that for $i = (p-1)p + i_0$ and $p > j \geqq 1$,

$$\begin{aligned}a(i,j) &= [(j(p^3t' + p^2 + p + 1) + 1 + p^2(p-1) + pi_0 - a)/p^3] \\ &= jt' + 1 + [((j-1)p^2 + jp + pi_0 + 1 - a)/p^3] \\ &= jt' + 1\,.\end{aligned}$$

By $a \leqq p$, $a(i, 0) = 0$. By definitions of $x_{i,j}$ and $y_{i,j}$, we can conclude Lemma 12.

Similarly as in Lemma 12, we have

LEMMA 13. *$x_{0,1} = \pi^{t'+1}$, $x_{0,2} = \cdots = x_{0,p-1} = \pi^{t'}$ and $y_{0,j} = -\binom{p}{j}\pi^{(j-p+1)}$ for $1 \leqq j < p$.*

LEMMA 14. *Let s be the number of $\mathfrak{o}G_2$-modules L_i such that L_i is isomorphic to L_0 for $0 \leqq i < p^2$. Then, s is relatively prime to p.*

Proof. By Lemma 12 and Lemma 13, L_i is isomorphic to L_0 for $p(p-1) \leqq i < p^2$. By Lemma 11, L_i is not isomorphic to L_0 for $0 < i < p(p-1) - 1$. Then, $s = p + 1$ or $p + 2$ and hence $(s, p) = 1$.

We can easily prove the following lemma.

LEMMA 15. *Let k'/k be a non-ramified extension of k with the ring $\mathfrak{o}'$ of all integers in k'. Let $\mathfrak{O}'$ be the ring of all integers in the composite field $k'K$. Then, $\mathfrak{O}'\Pi^a = \mathfrak{o}' \otimes_{\mathfrak{o}} (\Pi^a)$ and $V(\mathfrak{O}'\Pi^a) = V(\Pi^a)$.*

An $\mathfrak{o}'G$-module $\mathfrak{o}' \otimes_{\mathfrak{o}} (\Pi^a)$ is expressed as a direct sum of indecomposable $\mathfrak{o}'V$-modules M_u:

$$\mathfrak{o}' \otimes_{\mathfrak{o}} (\Pi^a) = M_1 \oplus M_2 \oplus \cdots \oplus M_v ,$$

where $V = V(\Pi^a)$. Applying [1] p. 636 (30.31), we can choose $\mathfrak{o}'$ such that M_u is absolutely indecomposable for each u.

LEMMA 16. *Let $\mathfrak{o}'$ and $\mathfrak{O}'$ be as above. Then, there exists an $\mathfrak{o}'V$-module M such that $\mathfrak{O}'\Pi^a$ is $\mathfrak{o}'G$-isomorphic to the $\mathfrak{o}'G$-module $\mathfrak{o}'G \otimes_V M$.*

Proof. By [1] p. 467 (19.24), $\mathfrak{o}'G \otimes_V M_u$ is also an absolutely indecomposable $\mathfrak{o}'G$-module. From Corollary 1 of Theorem 1, Lemma 5, Lemma 9 and Proposition 2, it follows that $\mathfrak{o}' \otimes_{\mathfrak{o}} (\Pi^a)$ is an indecomposable $\mathfrak{o}'G$-module. Therefore, by the definition of $V(\Pi^a)$, $\mathfrak{o}' \otimes_{\mathfrak{o}} (\Pi^a)$ is a direct summand of the $\mathfrak{o}'G$-module $\mathfrak{o}'G \otimes_V M_u$ for some u. Since $\mathfrak{o}'G \otimes_V M_u$ is indecomposable, $\mathfrak{o}' \otimes_{\mathfrak{o}} (\Pi^a) = \mathfrak{o}'G \otimes_V M_u$, which completes the proof of Lemma 16.

We are ready to prove Theorem 6, which is the aim of this section.

Proof of Theorem 6. By the above discussion, we may assume that $p \geqq a \geqq 2$ and G_1 is a non-abelian group of order p^3. Suppose $V(\Pi^a) \neq G_1$. Let M be the $\mathfrak{o}'V$-module as in Lemma 16. Then, M is expressed as a direct sum of indecomposable $\mathfrak{o}'G_2$-modules M_u:

$$M = a_1M_1 \oplus \cdots \oplus a_vM_v ,$$

where a_u is an integer and for $u' \neq u$, $M_{u'}$ is not $\mathfrak{o}'G_2$-isomorphic to M_u. Then, we have the decomposition of the $\mathfrak{o}'G_2$-module $\mathfrak{o}' \otimes (\Pi^a)$:

$$\mathfrak{o}' \otimes (\Pi^a) = |G_1/V|a_1M_1 \oplus \cdots \oplus |G_1/V|a_vM_v .$$

Using Krull-Schmidt Theorem, we have L_0 is isomorphic to M_u for some u. Let s be the number as in Lemma 14. Then, $s = |G_1/V|a_u$. By Lemma 14, $(p, |G_1/V|) = 1$, which implies $G_1 = V$. This is a contradiction, and the proof of Theorem 6 is completed.

§ 3.

Let K/k be a wildly ramified p-extension. In this section, we shall prove that if $a \not\equiv 1$ (p^n), then $V(\Pi^a) = G_1$. Let $t_1, t_2, \cdots, t_r$ be ramification numbers of K/k and G_i be the t_i-th ramification group of K/k for $1 \leqq i \leqq r$. As in Section 2, we may assume $t_1 = 1$. Let H be a normal subgroup of G such that $G_3 \subseteq H \subseteq G_2$ and $|G_2/H| = p$, and let Π_2 be a prime element of K_H. Then, the ramification number t of K_H/K_2 is t_2.

LEMMA 17. *Let H be as above and let $(\Pi_2^{a_3}) = (\Pi^a) \cap K_H$. Then, if $V(\Pi^a) \neq G_1$, $a_3 \equiv 1$ $(|G/H|)$ and $t_2 \equiv 1$ $(|G/H|)$.*

Proof. By Lemma 6 and the assumption $V(\Pi^a) \neq G_1$, we have $V(\Pi_2^{a_3}) \neq G_1/H$. Then, by Theorem 6, $a_3 \equiv 1$ $(|G_1/H|)$. Also, $V(\mathrm{tr}_{G_2/H}((\Pi_2^{a_3}))) \neq G_1/G_2$ by Lemma 6. Let $p^m = |G_1/G_2|$ as in Section 2. From Lemma 7, it follows that $\mathrm{tr}_{G_2/H}((\Pi_2^{a_3})) = (\Pi_1^{m(t)+a'})$, where Π_1 is a prime element of K_2 and $a' = p^m[(a_3-1)/p^{m+1}]$. By Theorem 4, $m(t) \equiv 1$ (p^m) and so $[t/p] \equiv 0$ (p^m), which completes the proof of Lemma 17.

PROPOSITION 5. *Let K/k be a wildly ramified extension of degfree p^3. Suppose that there exist three ramification numbers t_1, t_2 and t_3 with $t_1 = 1$ and G_1/G_3 is not cyclic. Then, if $a \not\equiv 1$ (p^3), $V(\Pi^a) = G_1$.*

Proof. Similarly as in Section 2, we may assume $p \geqq a \geqq 2$. By Lemma 7, we have $\mathrm{tr}_{G_3}((\Pi^a)) = (\Pi_2^{a_2})$, where $a_2 = (p-1)[t_3/p] + 2$. Suppose $V(\Pi^a) \neq G_1$. Then, by Lemma 6, $V(\Pi_2^{a_2}) \neq G_1/G_3$ and so by Theorem 5, $a_2 \equiv 1$ (p^2). Thus $t_3 \equiv p^2 + p + 1$ (p^3). Applying the similar arguments as in Section 2, we can conclude Proposition 5.

LEMMA 18. *K/k be a wildly ramified extension which is not the extension stated in Proposition* 5. *Then, if* $V(\Pi^a) \neq G_1$, $t_2 \equiv \cdots \equiv t_r \equiv 1$ (p^2).

Proof. We use induction on r. For $r = 2$, the result follows from Lemma 17 and Theorem 5. Without loss of generality, we can assume $|G_r| = p$. First, we treat the case where $|G_1/G_r| \geqq p^3$. As in Section 2, let p^c be the order of the maximal abelian normal subgroup N of G_1. Clearly, $N \supseteq G_r$. As in the proof of Proposition 4, we have

$$c(c+1) \geqq 2\cdot 4$$

and so $c \geqq 3$. Then, from the induction hypothesis $t_2 \equiv \cdots \equiv t_{r-1} \equiv 1$ (p^2), it follows that $t \equiv 1$ (p^2) for a ramification number t of K/K_N with $t \neq t_r$. By [3] p. 171 (V), we have also that $t \equiv t_r$ (p^2) and hence $t \equiv 1$ (p^2). Next, we treat the remained case where $|G_1/G_r| = p^2$. Since $r \geqq 3$ and $|G_1| = p^3$ by $|G_r| = p$, we have $r = 3$. From the assumption that K/k is not the extension stated in Proposition 5, it follows G_1/G_3 is cyclic. Hence G_1 is abelian. Applying [3] p. 171 (V) as in the above, we can conlcude the desired result.

Finally, we prove the following theorem, which is one of the main results of this paper.

THEOREM 7. *Let K/k be a wildly ramified extension of degree p^n. Let $t_1, t_2, \cdots, t_r$ be ramification numbers of K/k with $t_1 = 1$ and G_i be the t_i-th ramification group of G for $1 \leqq i \leqq r$. Then, if $V(\Pi^a) \neq G_1$,* (i) $a \equiv 1$ $(|G_1|)$ *and* (ii) $t_i \equiv 1$ $(|G_1/G_{i+1}|)$ *for* $1 \leqq i \leqq r$, *where* $G_{r+1} = \{1\}$.

Proof. Let p^l be the order of G_2. We use induction on l. For $l = 1$, the result follows from Lemma 17 and Theorem 6. Let Z be a subgroup of order p in the center of G_1, and t be the ramification number of K/K_Z. By the assumption $V(\Pi^a) \neq G_1$ and Lemma 6, we have $V((\Pi^a) \cap K_Z) \neq G_1/Z$. Therefore, we may assume $1 \leqq a \leqq p$. Also, $V(\mathrm{tr}_Z(\Pi^a)) \subseteq V(\Pi^a)$ and so $V(\mathrm{tr}_Z((\Pi^a))) \neq G_1/Z$. Suppose $2 \leqq a \leqq p$. By Proposition 5, K/k is not as stated in Proposition 5. From Lemma 7 and the induction hypothesis, it follows

$$(p-1)[t/p] + 2 \equiv 1 \ (|G_1/Z|)\,.$$

Therefore, $[t/p] \equiv 1$ $(|G_1/Z|)$ and so $t \equiv p + 1$ (p^2), which is contrary to the fact stated in Lemma 18. Thus, we have $a = 1$ and conclude (i). Next, we shall prove (ii). As in the proof of Lemma 17, we have

$$(p-1)[t/p]+1 \equiv 1 \ (|G_1/Z|)\,.$$

Therefore, $[t/p] \equiv 0 \ (|G_1/Z|)$ and so $t \equiv 1 \ (|G_1|)$. This implies (ii) and the proof is completed.

As an immediate consequence of Theorem 7, we have

COROLLARY 2. *Let K/k be as in Theorem 7. Then, if $a \not\equiv 1 \ (|G_1|)$, $V(\Pi^a) = G_1$.*

REFERENCES

[1] C. W. Curtis and I. Reiner, Methods of Representation Theory Vol. 1, Interscience, New York, 1981.
[2] A. Fröhlich, Some topics in the theory of module conductors, Oberwolfach Berichte, **2** (1966), 59–83.
[3] H. Hasse, Führer, Discriminant und Verzweigungskörper relative-Abelscher Zahlkörper, J. reine angew. Math., **162** (1930), 169–184.
[4] B. Huppert, Endliche Gruppen I, Springer-Verlag, Berlin, 1967.
[5] E. Noether, Normalbasis bei Körpern ohne höhere Verzweigung, J. reine angew. Math., **167** (1932), 147–152.
[6] Y. Miyata, On the module structure of the ring of all integers of a $\mathfrak{p}$-adic number field, Nagoya Math. J., **54** (1974), 53–59.
[7] Y. Miyata, Vertices of ideals of a $\mathfrak{p}$-adic number field, Illinois J. Math., to appear.
[8] J. P. Serre, Corps Locaux, Hermann, Paris, 1968.
[9] S. V. Vostokov, Ideals of an abelian p-extension of an irregular local field as Galois modules, Zap. Nauchn. Sem. Leningrad. Otdel. Math. Inst. Steklov. (LOMI), **46** (1974), 14–35 (Russian).
[10] S. V. Vostokov, Ideals of an abelian p-extension of a local field as Galois modules, Zap. Nauchn. Sem. Leningrad. Otdel. Math. Inst. Steklov. (LOMI), **57** (1976), 64–84 (Russian).

Faculty of Education
Shizuoka University
Shizuoka, 422
Japan