Advanced Studies in Pure Mathematics 12, 1987
Galois Representations and Arithmetic Algebraic Geometry
pp. 287–314

Wild Ramification in the Imperfect Residue Field Case

Osamu Hyodo

Introduction

The aim of this paper is to study wild ramification of complete discrete valuation fields without the assumption that the residue field is perfect. In the case where the residue field is perfect, there is a beautiful theory of ramification groups (Serre [14] §4). The difficulty of our case is that there seems to be no such a theory in general. As applications of our study, we shall show the following three results. In the following, let K be a complete discrete valuation field of mixed characteristics $(0, p)$.
(1) Miki [9], [10] studied $\boldsymbol{Z}_p$-extensions of K. He showed that any $\boldsymbol{Z}_p$-extension of K is contained in a composite of an unramified extension of K and a $\boldsymbol{Z}_p$-extension of the "canonical subfield" k of K. Here, k is characterized by the following properties.

(0–1–1) k is complete with respect to the valuation induced from K.

(0–1–2) The residue field of k is the maximal perfect subfield of the residue field $\bar{K}$ of K.

(0–1–3) k is algebraically closed in K.

We generalize his result by using continuous cohomology (Tate [16]). Let $H^q(G, A)$ be the q-th continuous cohomology group of a topological group G with coefficients in a topological G-module A. Let $G_E = \mathrm{Gal}(E_{\mathrm{sep}}/E)$ be the absolute Galois group of a field E, and let (r) denote the r-th Tate twist for $r \in \boldsymbol{Z}$ (cf. Tate [16] p. 262).

Theorem (0–2). *Assume that the residue field $\bar{K}$ of K is separably closed. Then the inflation map induces an isomorphism*

$$H^1(G_k, \boldsymbol{Z}_p(r)) \xrightarrow{\simeq} H^1(G_K, \boldsymbol{Z}_p(r)) \quad \text{if} \quad r \neq 1.$$

As $H^1(G_E, \boldsymbol{Z}_p) \simeq \mathrm{Hom}(G_E, \boldsymbol{Z}_p)$ classifies $\boldsymbol{Z}_p$-extensions of a field E, Miki's result is the particular case $r=0$ of Theorem (0–2). (Miki's result can be reduced to the case where $\bar{K}$ is separably closed).

Received November 11, 1985.

(2) Miki also studied the inseparable degree of the residue field extension of cyclic extension of K. Let e_K be the absolute ramification index of K. He showed that for any *cyclic* extension L/K,

(0–3–1) the residue field extension $\bar{L}/\bar{K}$ is separable if $e_K<p-1$ ([10] Prop. 9),

(0–3–2) the inseparable degree $[\bar{L}:\bar{K}]_{\text{insep}}\leqq p^{e_K}$ if $[L:K]=[\bar{L}:\bar{K}]$ ([9] Prop. 6).

We give a more precise estimate depending only on e_K. Define integers $f(n)$ and $g(n)$ for $n\geqq 1$ as follows.
In the case $(p-1)|n$, we put

$$f(n)=\max\{1+a+b \mid p^a+(p^{2b}-1)(p+1)^{-1}p^{-b}\leqq n\cdot(p-1)^{-1},\ a,\ b\in \boldsymbol{Z},\ 0\leqq b\},$$

$$g(n)=\max\{1+a+b \mid p^a+p^b-1\leqq n\cdot(p-1)^{-1},\ a,\ b\in \boldsymbol{Z},\ 0\leqq b\}.$$

Otherwise, we put

$$f(n)=\max\{a+b \mid r\cdot p^{a-1}+p^{b-2}(p^2-p+1)(p-1)(p+1)^{-1}<n,\ a,\ b\in \boldsymbol{Z},\ 0\leqq b\},$$

$$g(n)=\max\{a+b \mid r\cdot p^{a-1}+p^{b-2}(p^2-p+1)(p-1)<n,\ a,\ b\in \boldsymbol{Z},\ 0\leqq b\},$$

where r is the minimal non-negative integer such that $r\equiv n \bmod (p-1)$ (In particular, $g(n)\leqq f(n)\leqq 3+2\cdot\log_p(n)$ and $g(n)=f(n)=0$ if $n<p-1$). The following result includes (0–3–1) and (0–3–2).

Proposition (0–4). *For any cyclic extension* L/K,

(0–4–1) *we have* $[\bar{L}:\bar{K}]_{\text{insep}}\leqq p^{f(e_K)}$.

If we assume moreover $[L:K]=[\bar{L}:\bar{K}]$,

(0–4–2) *we have* $[\bar{L}:\bar{K}]_{\text{insep}}\leqq p^{g(e_K)}$.

(3) The following result is interesting even if $\bar{K}$ is perfect. Let A be an abelian variety defined over K which has good reduction. We define the "connected part" $\pi_1{}^{\text{con}}(A)$ of the geometric fundamental group $\pi_1{}^{\text{geo}}(A)$ (by definition $\pi_1{}^{\text{geo}}(A)$ is the G_K-co-invariant of the Tate module $T(A)$ of A) as the kernel of the specialization

$$\pi_1{}^{\text{geo}}(A)\twoheadrightarrow \pi_1{}^{\text{geo}}(A_s),$$

where A_s is the reduction of A. It is well-known that $\pi_1{}^{\text{con}}(A)$ is a finite

p-group (Bloch [1] Prop. 2.4). We can deduce the finiteness *effectively* from (0–4–2) by considering the p-adic completion of the function field of A.

Proposition (0–5). *$\pi_1^{\mathrm{con}}(A)$ is killed by $p^{g(e_K)}$.*

As $g(n)=0$ if $n<p-1$, we have;

Corollary (0–6) (Kato-Saito [7] Prop. 7). *If $e_K<p-1$, we have $\pi_1^{\mathrm{geo}}(A)\simeq\pi_1^{\mathrm{geo}}(A_s)$.*

To show the above results (1), (2) and (3), we define the depth of ramification as a measure of wild ramification and study its behaviour in cyclic extensions. Our key tools are inequalities concerning the depth of ramification (§4). In the classical case (i.e. the residue field is finite), they can be obtained by using the local class field theory (Serre [14] §15). In our general case, we make use of higher local class field theory (Kato [5] and Paršin [12]). We study the information about wild ramification which is contained in higher local class field theory (Kato [5] and Paršin [16]), and deduce some of the inequalities.

The plan of this paper is as follows. In Section 1, we give the result (Theorem (1–5)) concerning wild ramification and higher local class field theory. Section 2 is devoted to show some general properties of the depth of ramification, and Section 3 to the proof of Theorem (1–5). Our key inequalities are treated in Section 4. In Section 5, (resp. Section 7) we prove Proposition (0–4) (resp. Theorem (0–2)). We give a proof of Proposition (0–5) in a little more general situation in Section 6.

I am grateful to Professor Hiroo Miki. He kindly pointed out his results to me. I am also grateful to Professor Kazuya Kato for his valuable advices and encouragements.

Contents

§1. Ramification and local class field theory

Let K be a complete discrete valuation field with finite residue field and with the normalized valuation v_K. It is well-known that the homomorphism of the local class field theory

$$\Psi_1 : K^\times \longrightarrow \mathrm{Gal}(K_{ab}/K)$$

contains information about ramification. Namely,

(1–1–1) $\Psi_1(O_K^\times)$ corresponds to the maximal unramified abelian extension of K (here, $O_K^\times$ is the unit group of K).

(1–1–2) $\Psi_1(U_K^i)$ coincides with the i-th upper ramification group of $\mathrm{Gal}(K_{ab}/K)$ for $i \geqq 1$, (here $U_K^i = \{1+y \mid v_K(y) \geqq i\}$ is the i-th principal unit group).

Kato [5] and Paršin [12] generalized the local class field theory for an "n-dimensional local field" K by using Milnor's K-group $K_n^M(K)$. They constructed a homomorphism generalizing Ψ_1,

$$\Psi_n : K_n^M(K) \longrightarrow \mathrm{Gal}(K_{ab}/K).$$

We naturally hope that the above homomorphism contains information about ramification. The result corresponding to (1–1–1) was shown in [5], and Kato [6] and Lomadze [8] generalized (1–1–2) under some (restrictive) condition. The trouble in generalizing (1–1–2) without any restriction is that there seems to be no nice theory of ramification groups (Kato [6] Rem. (3.7) and Lomadze [8] p. 364). (Principal unit group as U_K^i can be defined for Milnor's K-groups $K_n^M(K)$.)

What we shall do is to define the depth of ramification which works well in general, and to give our result (Theorem (1–5)) which may be interpreted as a generalization of (1–1–2).

Definition (1–2). An n-dimensional complete discrete valuation field K (we abbreviate it as "n-DVF" in what follows) is a field endowed with a sequence of fields $\{k_i\}_{0 \leqq i \leqq n}$ such that

(1–2–1) k_i is a complete discrete valuation field with residue field k_{i-1} for $1 \leqq i \leqq n$.

(1–2–2) $K = k_n$.

An n-DVF K has a (not necessarily unique) n-dimensional valuation (we abbreviate it as "n-DV" in what follows)

$$v_K : K^\times \twoheadrightarrow \boldsymbol{Z}^n \subset \boldsymbol{Q}^n,$$

where $\boldsymbol{Q}^n$ has the lexicographic order, such that

$$v_K(\pi_{n+1-i})=(0,\dots,0,\underset{i}{1},0,\dots,0),$$

where π_i denotes a lifting of some prime element of k_i. For any finite extension L/K, L is an n-DVF and v_K extends uniquely to L. Thus v_K extends to the valuation of an algebraic closure K_{alg}

$$v_K\colon (K_{\mathrm{alg}})^\times \longrightarrow \mathbf{Q}^n.$$

Definition (1–3). Let M/L be a finite separable extension of algebraic (finite if $n\geqq 2$) extensions of K. We define the depth of ramification of M/L by

$$d_K(M/L)=\inf\{v_K(\mathrm{Tr}_{M/L}(y)/y)\mid y\in M^\times\}.$$

We shall show (Proposition (2–2)) that the right-hand-side of (1–3) exists. In the case where $n=1$ and L/K is finite, the depth of ramification is closely related to the different (note that the definition of the different is possible only in this case). To be precise, we have the formula

(1–4) $$d_K(M/L)=v_K(\mathscr{D}_{M/L})-(v_K(\pi_L)-v_K(\pi_M)),$$

where $\mathscr{D}_{M/L}$ denotes the relative different of M/L and π_L (resp. π_M) denotes a prime element of L (resp. M). In particular $d_K(M/L)=0$ if and only if M/L is tamely ramified.

We define "principal unit groups" for the Milnor's K-group of an n-DVF K with an n-DV v_K. Recall that the Milnor's K-group $K_n^M(E)$ for a field E is by definition the quotient of $E^\times\otimes_{\mathbf{Z}}\cdots\otimes_{\mathbf{Z}}E^\times$ (n times) by the subgroup generated by the elements of the form $a_1\otimes\cdots\otimes a_n$ such that $a_s+a_t=1$ for some $s\neq t$. We denote the image of $a_1\otimes\cdots\otimes a_n$ by the symbol $\{a_1,\dots,a_n\}$. For $\mathbf{Z}^n\ni i>0=(0,\dots,0)$, let $U^iK_n^M(K)$ be the subgroup generated by the symbols of the form $\{1+x, y_1,\dots,y_{n-1}\}$ where $v_K(x)\geqq i$ and $y_j\in K^\times$ for $1\leqq j\leqq n-1$. (If $n=1$, $U^iK_1^M(K)=U_K^i$.)

To the end of this section, let K be an n-dimensional local field. By definition, K is an n-DVF and k_0 is a finite field (cf. (1–2–1)). Fix an n-DV v_K and let $\mathrm{ch}(k_0)=p$. Let L/K be a finite abelian extension. Then Ψ_n induces an isomorphism (Kato [5] II §3.1 Theorem 1 (1))

$$K_n^M(K)/N_{L/K}(K_n^M(L))\simeq \mathrm{Gal}(L/K),$$

where N denotes a norm homomorphism. We define the subgroup $G^i(L/K)$ for $i>0$ by the image of $U^iK_n^M(K)$, i.e.

$$G^i(L/K)=U^iK_n^M(K)/(N_{L/K}(K_n^M(L))\cap U^iK_n^M(K)).$$

Then we can show that $G^i(L/K)=0$ for sufficiently large i and that $G^1(L/K)$

is a p-group, where $1=(0,\ldots,0,1)$. By (1–1–2), $G^i(L/K)$ coincides with the i-th upper ramification group when $n=1$.

We define the jumping numbers $j(l)$ for $l \geqq 1$ by

$$j(l)=\max\{1 \leqq i \in \boldsymbol{Z}^n \mid \# G^i(L/K) \geqq p^l\} \cup \{0\}.$$

For the later use, we note (i) $j(l)=0$ if $\# G^1(L/K)<p^l$, and (ii) both $\# G^{j(l)}(L/K) \geqq p^l$ and $\# G^{j(l)+1}(L/K) \leqq p^{l-1}$ if $\# G^1(L/K) \geqq p^l$.

In case $n=1$, we can show by using (1–1–2) and (1–4)

$$d_K(L/K)=(p-1)\sum_{l=1}^{\infty} j(l)\cdot p^{-l}.$$

Conversely we can deduce (1–1–2) from the above formula in this case.

In the general case, we have;

Theorem (1–5). *There are inequalities*

$$(p-1)\sum_{l=1}^{\infty} j(l)\cdot p^{-l} \leqq d_K(L/K) \leqq p^{-1}(p-1)\sum_{l=1}^{\infty} j(l).$$

We shall give examples ((3–4) and (3–5)) which show (1–5) is best possible. It seems that we can define nice ramification groups only when the first equality of (1–5) holds.

§2. The properties of the depth of ramification

In this section, we show some general properties of the depth of ramification. Throughout this section, let K be an n-DVF and fix an n-DV v_K of K. As is explained in Section 1, v_K extends uniquely to K_{sep}.

We give some notations. Let $\{k_i\}_{0 \leqq i \leqq n}$ be as in (1–2–1). We call k_0 the residue field of K. Let $O_K=\{x \in K \mid v_K(x) \geqq 0\}$ be the valuation ring. Note that O_K does not depend on the choice of v_K. Let L be a finite extension of K and fix another n-DV

$$v_L \colon L^\times \longrightarrow \boldsymbol{Z}^n.$$

Then there exists an upper triangle matrix $T(L/K) \in M_n(\boldsymbol{Z})$ such that

$$v_K(x)\cdot T(L/K)=v_L(x)$$

for any $x \in (K_{\text{alg}})^\times$. So we have by definition

(2–1) $$d_K(M/L)\cdot T(L/K)=d_L(M/L)$$

for any finite separable extension M/L. Here we consider an element of $\boldsymbol{Q}^n$ as a row vector. It is easily seen that the diagonal components of

$T(L/K)$ do not depend on the choice of v_K and v_L, and that $[l_0: k_0]\cdot \det(T(L/K))=[L: K]$.

We call L/K unramified if all diagonal components of $T(L/K)$ equal one and the residue field extension is separable. A tamely ramified extension is defined to be a composition of an unramified extension and an extension whose degree is prime to the characteristic of the residue field. We can see $G_K=\mathrm{Gal}(K_{\mathrm{sep}}/K)$ has a normal subgroup I (resp. P) which corresponds to the maximal unramified (resp. tamely ramified) extension of K. It is well-known $G_K/I\simeq G_{k_0}$, $I/P\simeq \prod_{l\neq \mathrm{ch}(k_0)} Z_l^n$ and P is a pro-ch (k_0)-group. In particular, I is a pro-solvable group.

We first show that the right-hand-side of (1–3) exists. (If $n=1$, this is trivial.)

Proposition (2–2). *Let M/L be a finite separable extension of finite extensions of K. Then there exists a minimal element in*

$$\{v_K(\mathrm{Tr}_{M/L}(y)/y)\mid y\in M^\times\}.$$

By the structure of G_L, we see that there are subextensions $M=L_m\supset\cdots\supset L_1\supset L$ such that

(2–3–1) $[L_{i+1}: L_i]$ is a prime for $1\leqq i\leqq m-1$,

(2–3–2) L_1/L is unramified.

So, to prove (2–2) it suffices to show the following Lemmas (2–4) ~ (2–6).

Lemma (2–4). *Let N be a subextension of M/L. Assume* (2–2) *holds for both M/N and N/L. Then* (2–2) *holds for M/L. Moreover we have*

$$d_K(M/L)=d_K(M/N)+d_K(N/L).$$

Lemma (2–5). *If M/L is unramified, then* (2–2) *holds for M/L. Moreover we have $d_K(M/L)=0$.*

Lemma (2–6). *Let p be a prime and assume $[M: L]=p$. Then* (2–2) *holds for M/L.*

We prove (2–4). By the assumption, we can choose $a\in M^\times$ (resp. $b\in N^\times$) such that

$$d_K(M/N)=v_K(\mathrm{Tr}_{M/N}(a)/a)\quad (\text{resp. } d_K(N/L)=v_K(\mathrm{Tr}_{N/L}(b)/b)).$$

Let $c=b\cdot(\mathrm{Tr}_{M/N}(a))^{-1}$, then we have

$$v_K(\mathrm{Tr}_{M/L}(c\cdot a)/c\cdot a)=v_K((\mathrm{Tr}_{M/N}(a)/a)\cdot(\mathrm{Tr}_{N/L}(b)/b)).$$

So we obtain $\qquad d_K(M/N)+d_K(N/L)=v_K(\mathrm{Tr}_{M/L}(c\cdot a)/c\cdot a)$.

On the other hand, it can be easily seen

$$d_K(M/N)+d_K(N/L)\leqq v_K(\mathrm{Tr}_{M/L}(y)/y) \qquad \text{for any} \quad y\in M^\times.$$

This proves (2–4). To prove (2–5), it suffices to show

$$v_K(\mathrm{Tr}_{M/L}(y)/y)=0 \qquad \text{for some} \quad y\in M^\times,$$

since $\qquad v_K(\mathrm{Tr}_{M/L}(y)/y)\geqq 0 \qquad$ for any $y\in M^\times$.

Let m_0 (resp. l_0) be the residue field of M (resp. L). If M/L is unramified, we have

$$\overline{\mathrm{Tr}_{M/L}(y)}=\mathrm{Tr}_{m_0/l_0}(\bar{y}) \qquad \text{for any} \quad y\in O_M,$$

where $^-$ denotes the reduction to the residue field. So for any $y\in O_M$ such that $\mathrm{Tr}_{m_0/l_0}(\bar{y})\neq 0$, we have

$$v_K(\mathrm{Tr}_{M/L}(y)/y)=v_K(\mathrm{Tr}_{M/L}(y))-v_K(y)=0-0=0.$$

We proceed to prove (2–6). Choose an element $y\in M^\times$ such that

(2–7–1) $\qquad v_K(y)\notin v_K(L^\times) \quad$ if $\quad v_K(L^\times)\subsetneqq v_K(M^\times)$,

(2–7–2) $\qquad y\in O_M$ and $\bar{y}\notin l_0 \quad$ if $\quad v_K(L^\times)=v_K(M^\times)$.

In both cases consider the minimal polynomial $f(X)$ of y over L. Then $f(X)$ is a monic polynomial of degree p. By Euler's lemma (Serre [14] p. 65) we have

$$\text{(2–8)} \qquad \mathrm{Tr}_{M/L}(y^j(f'(y))^{-1})=\begin{cases} 0 & \text{if} \quad 0\leqq j\leqq p-2,\\ 1 & \text{if} \quad j=p-1.\end{cases}$$

Any element z of M is a summation

$$z=\sum_{j=0}^{p-1} a_j\cdot y^j(f'(y)^{-1}) \quad \text{where} \quad a_j\in L \qquad \text{for} \quad 0\leqq j\leqq p-1,$$

and by (2–7–1) and (2–7–2) we have

$$v_K(z)=\min\{v_K(a_j\cdot y^j(f'(y)^{-1}))\,|\,0\leqq j\leqq p-1\}.$$

Hence we obtain by (2–8)

$$\text{(2–9)} \qquad v_K(\mathrm{Tr}_{M/L}(z)/z)=v_K(a_{p-1})-v_K(z)\geqq v_K(y^{1-p}f'(y)).$$

The equality of (2–9) holds if $v_K(z)=v_K(a_{p-1}\cdot y^{p-1}f'(y)^{-1}))$. In particular it is the case if $a_j=0$ for $0 \leqq j \leqq p-2$. Thus (2–6) is proved.

The above proof of (2–6) shows:

Lemma (2–10). *Assume M/L is a cyclic extension of a prime degree p. Then for any generator σ of* Gal(M/L) *and for any $y \in M^\times$ satisfying the condition* (2–7–1) *or* (2–7–2), *we have*

$$d_K(M/L)=(p-1)\cdot v_K(1-(\sigma\cdot y)/y).$$

In fact, as $f(X)=\prod_{\sigma\in \mathrm{Gal}(M/L)}(X-\sigma\cdot y)$, we have

$$y^{1-p}f'(y)=\prod_{1\neq\sigma\in \mathrm{Gal}(M/L)}(1-(\sigma\cdot y)/y). \tag{2–11}$$

And it is easily checked that $v_K(1-(\sigma\cdot y)/y)$ coincide for all $1\neq\sigma\in$ Gal (M/L).

Remark (2–12). In fact $d_K(M/L)=0$ if M/L is tamely ramified. This can be seen easily from (2–4), (2–5) and the fact $v_K(m)=0$ for any integer m prime to ch(k_0).

Secondly we calculate the norm groups. The proof of the following Proposition (2–13) is the same as Serre [14] §5 Proposition 4.

Proposition (2–13). *Let L/K be a cyclic extension of degree a prime p and let $\varphi(s)=(s-d_K(L/K))\cdot T(L/K)$ for $s\in \boldsymbol{Z}^n$. Then we have*

$$N_{L/K}(U_L^{\varphi(s)})=U_K^s \quad \text{if } (p-1)^{-1}p\cdot d_K(L/K)<s\in \boldsymbol{Z}^n.$$

Proposition (2–14). *Let the notations be as above. We have*

(2–14–1) $N_{L/K}(U^{\varphi(s)}K_n^M(L))\supset U^sK_n^M(K)$ *if* $(p-1)^{-1}p\cdot d_K(L/K)<s\in \boldsymbol{Z}^n$.

(2–14–2) $N_{L/K}(U^{s\cdot T(L/K)+1}K_n^M(L))\subset U^{s+1}K_n^M(K)$ *if* $0\leqq s\in \boldsymbol{Z}^n$.

The assertion (2–14–1) can be seen from (2–13) and the formula $N_{L/K}\{x, y\}=\{N_{L/K}(x), y\}$ for $x\in L^\times$ and $y\in K_{n-1}^M(K)$. The assertion (2–14–2) can be seen by using Kato [5] I p. 322 Lemma 2.

Thirdly we study the depth of ramification in the case where $n=1$, i.e. K is a complete discrete valuation field. Recall that in this case $d_K(M/L)$ is defined even if L/K is infinite algebraic. (But in this case $d_K(M/L)$ may not be a rational number.)

Lemma (2–15). *Let $L=\varinjlim_{j\in J} L_j$ be an algebraic extension of a com-*

plete discrete valuation field K (each L_j is finite over K) and let M_0 be a finite separable extension of L_{j_0} linearly disjoint from L over L_{j_0} for some $j_0 \in J$. Let $M_j = L_j M_0$ for $j \geqq j_0$ and $M = \varinjlim_J M_j = M_0 L$. Then we have

$$d_K(M_j/L_j) \leqq d_K(M_{j'}/L_{j'}) \quad \text{if} \quad j_0 \leqq j' \leqq j,$$
$$d_K(M/L) = \inf\{d_K(M_j/L_j) \mid j_0 \leqq j \in J\}.$$

Lemma (2–15) can be seen easily. The following Lemma (2–16) can be seen by a straightforward calculation using (2–10) and shall be used in the proof of (4–2) and (7–5).

Lemma (2–16). *Let K be a complete discrete valuation field of mixed characteristics* (0, *p*), *and assume K contains a primitive p-th root ζ of unity. Then we can classify all cyclic extensions L/K of degree p as in the following table.*

	$L=K(y)$ with the equation	; ramification	; $d_K(L/K)$
a)	$y^p = w \cdot \pi$	; $\bar{L} = \bar{K}$	; e_K
b)	$y^p = u$	; $[\bar{L}: \bar{K}]_{\text{insep}} = p$	; e_K
c)	$y^p = 1 + w \cdot \pi^s$, $0 < s < e'p$, $(s, p) = 1$	; $\bar{L} = \bar{K}$	; $e_K - p^{-1}(p-1) \cdot s$
d)	$y^p = 1 + u \cdot \pi^{p \cdot t}$, $0 < t < e'$	; $[\bar{L}: \bar{K}]_{\text{insep}} = p$	; $e_K - (p-1) \cdot t$
e)	$y^p = 1 + w \cdot (1-\zeta)^p$, $\bar{w} \notin Q$	; $[\bar{L}: \bar{K}]_{\text{sep}} = p$	; 0

where $u, w \in O_K^\times$, $\bar{u} \notin \bar{K}^p$, $e' = (p-1)^{-1} e_K$ $(e_K = v_K(p))$, $Q = \{x^p - x \mid x \in \bar{K}\}$ and π is a prime element of K.

§ 3. The proof of Theorem (1–5)

In this section we prove Theorem (1–5) and give some examples.

We first prove (1–5) in the case where L/K is cyclic of a prime degree. Note that the left-hand-side and the right-hand-side of (1–5) coincide in this case. So it suffices to show $p^{-1}(p-1) \cdot j(1) = d_K(L/K)$ since $j(l) = 0$ for $l \geqq 2$. If $d_K(L/K) = 0$, then we can see easily $j(1) = 0$ by (2–14–1). If $d_K(L/K) > 0$, we may assume without loss of generality that the first component of $d_K(L/K)$ is greater than zero by Lemma 6 (2) of Kato [5] II p. 664. We may assume moreover that K is a complete discrete valuation field with residue field $F = \boldsymbol{F}_{p^h}((X_1))\cdots((X_{n-1}))$. Then the assersion $p^{-1}(p-1) \cdot j(1) = d_K(L/K)$ follows from (2–10), Kato [5] II p. 668 ~ 670 (C) and (D) and an isomorphism

$$\begin{array}{ccc} \boldsymbol{Z}/p\boldsymbol{Z} & \xrightarrow{\simeq} & \Omega_F^{n-1}/(1-\gamma)\Omega_F^{n-1} \\ \cup\!\!\!\shortmid & & \cup\!\!\!\shortmid \\ 1 & \longmapsto & \dfrac{dX_1}{X_1} \wedge \cdots \wedge \dfrac{dX_{n-1}}{X_{n-1}} \end{array} \qquad (\gamma \text{ is a Cartier operator})$$

which can be seen easily from Lemma 3 of Kato [5] II p. 624.

Next we prove (1–5) in general. Let L_0 be a subextension of L/K of a prime degree, such that

$$\begin{cases} (p-1)^{-1}p\cdot d_K(L_0/K)=\min\{j(l)\,|\,j(l)\neq 0\} & \text{if} \quad \mathrm{Gal}(L/K)=G^1(L/K), \\ d_K(L_0/K)=0 & \text{otherwise.} \end{cases}$$

Let $\{j'(l)\}$ be the jumping numbers of L/L_0. (We fix an n-DV v_{L_0} of L_0 and $T(L_0/K)\in M_n(\boldsymbol{Z})$ as in (2–1), and write T instead of $T(L_0/K)$ for simplicity).

We claim

(3–1–1) $j'(l)=0$ if $j(l)=0$ or both $j(l+1)=0$ and

$d_K(L_0/K)=p^{-1}(p-1)\cdot j(l)$,

(3–1–2) $\varphi(j(l))\leqq j'(l)\leqq j(l)\cdot T$ otherwise,

where $\varphi(s)=(s-d_K(L_0/K))\cdot T$.

The assertion (3–1–1) is trivial. To show (3–2–2), we consider a commutative diagram (Kato [5] II p. 661 Corollary 1)

$$\text{(3–2)} \qquad \begin{array}{ccc} K_n^M(L_0)/N_{L/L_0}(K_n^M(L)) & \xrightarrow{N_{L_0/K}} & K_n^M(K)/N_{L/K}(K_n^M(L)) \\ \wr\| & & \wr\| \\ \mathrm{Gal}(L/L_0) & \hookrightarrow & \mathrm{Gal}(L/K)\,. \end{array}$$

First we prove the first inequality of (3–1–2). On the contrary, assume $\varphi(j(l))>j'(l)$. Then by the definition of jumping numbers we have

$$\sharp G^{\varphi(j(l))}(L/L_0)\leqq \sharp G^{j'(l)+1}(L/L_0)\leqq p^{l-1}.$$

On the other hand, if $j(l)>(p-1)^{-1}p\cdot d_K(L_0/K)$, we have by (2–14–1) and (3–2)

$$G^{\varphi(j(l))}(L/L_0)\supset G^{j(l)}(L/K).$$

Thus we obtain

$$p^l\leqq \sharp G^{j(l)}(L/K)\leqq \sharp G^{\varphi(j(l))}(L/L_0)\leqq p^{l-1}.$$

This is a contradiction. If $j(l)=(p-1)^{-1}p\cdot d_K(L_0/K)$, we have by (2–14–1), (3–2) and Kato [5] II p. 668 ∼ 670 (C) and (D)

$$G^{\varphi(j(l))}(L/L_0)\supset G^{j(l)}(L/K)\cap \mathrm{Gal}(L/L_0)\,.$$

By the fact $\mathrm{Gal}(L/K)=G^{j(l)}(L/K)$ (recall the choice of L_0), we have

$$[L: L_0]=\#(G^{j(l)}(L/K)\cap \mathrm{Gal}(L/L_0))\leqq \#G^{\varphi(j(l))}(L/L_0)\leqq p^{-1}[L: L_0].$$

This is a contradiction. We next prove the second inequality of (3–2–2). On the contrary, assume $j'(l)>j(l)\cdot T$. Then we have

$$p^l\leqq \#G^{j(l)\cdot T+1}(L/L_0).$$

On the other hand, we have

$$G^{j(l)\cdot T+1}(L/L_0)\subset G^{j(l)+1}(L/K)$$

by (2–13–2) and (3–2). Thus we obtain

$$p^l\leqq \#G^{j(l)\cdot T+1}(L/L_0)\leqq \#G^{j(l)+1}(L/K)\leqq p^{l-1}.$$

This is a contradiction.

Now we can prove (1–5) by induction on $[L: K]$. If $d_K(L_0/K)=0$, we have by (3–2–1) and (3–2–2)

$$j'(l)=j(l)\cdot T.$$

As $d_K(L/K)\cdot T=d_{L_0}(L/L_0)$ in this case, the assertion (1–5) for L/K follows from that for L/L_0. If $d_K(L_0/K)>0$, let $[L: K]=p^m$ (note in this case $\mathrm{Gal}(L/K)=G^1(L/K)$ is a p-group). The inequalities (1–5) for L/L_0 are

$$(p-1)\sum_{l=1}^{m-1} j'(l)\cdot p^{-l}\leqq d_{L_0}(L/L_0)\leqq p^{-1}(p-1)\sum_{l=1}^{m-1} j'(l)\cdot p^{-l}.$$

As

$$d_{L_0}(L/L_0)\cdot T^{-1}=d_K(L/K)-d_K(L_0/K)=d_K(L/K)-(p-1)^{-1}p\cdot j(m),$$

we have

$$j(m)+\Big(\sum_{l=1}^{m-1} j'(l)\cdot p^{1-l}\Big)\cdot T^{-1}\leqq (p-1)^{-1}p\cdot d_K(L/K)\leqq j(m)+\Big(\sum_{l=1}^{m-1} j'(l)\Big)T^{-1}.$$

On the other hand we have the following inequalities by (3–1–2).

(3–3–1) $$\sum_{l=1}^{m} j(l)\cdot p^{1-l}\leqq j(m)+\Big(\sum_{l=1}^{m-1} j'(l)\cdot p^{1-l}\Big)\cdot T^{-1}$$

(3–3–2) $$j(m)+\Big(\sum_{l=1}^{m-1} j'(l)\Big)\cdot T^{-1}\leqq \sum_{l=1}^{m} j(l)$$

Thus (1–5) follows.

We give some examples concerning Theorem (1–5). The following Proposition (3–4) and Example (3–5) show that the inequalities of (1–5) are best possible in general.

Proposition (3–4). *The first equality of* (1–5) *holds if at most one diagonal component of* $T(L/K)$ *is divisible by* p.

Example (3–5). Let $q=p^h$ and K be a complete discrete valuation field with residue field $F_q((X_1))\cdots((X_{n-1}))$. Then K is an n-dimensional local field. Let L_i $(1\leqq i\leqq n)$ be a cyclic extension of K of degree p, such that the i-th diagonal component of $T(L_i/K)$ equals p (then the other diagonal components are necessarily one). This assumption does not depend on a choice of n-DV's v_K and v_{L_i}. Let L be the composition of all L_i. Then the set of jumping numbers $\{j(l)\mid 1\leqq l\leqq n\}$ of L/K coincides with $\{(p-1)^{-1}p\cdot d_K(L_i/K)\mid 1\leqq i\leqq n\}$ and we have

$$d_K(L/K)=\sum_{i=1}^{n} d_K(L_i/K)=p^{-1}(p-1)\sum_{l=1}^{n} j(l).$$

We first show (3–5). The assertion

$$\{j(l)\mid 1\leqq l\leqq n\}=\{(p-1)^{-1}p\cdot d_K(L_i/K)\mid 1\leqq i\leqq n\}$$

can be seen easily by the definition of jumping numbers. Let M_i be the composition of all L_j except L_i. By the assumption we have $v_{M_i}(x)\notin \boldsymbol{Z}^n$ for any element $x\in L_i^\times$ such that $v_K(x)\notin \boldsymbol{Z}^n$. So we can show

$$d_K(L/K)=\sum_{i=1}^{n} d_K(L_i/K)$$

by using (2–10) and (2–4).

To prove (3–4), we may assume $\mathrm{Gal}(L/K)=G^1(L/K)$ replacing K by the maximal tamely ramified subextension (cf. Remark (2–12)). Then only one diagonal component of $T(L/K)$ is greater than one. Let s be the integer such that the $(n-s)$-th diagonal component of $T(L/K)$ is greater than one. We may also assume K is as in (3–5).

Lemma (3–6). *Let the assumption be as above. If* $G^t(L/K)/G^{t+1}(L/K)$ *is not trivial for* $0<t\in \boldsymbol{Z}^n$, *then the elements of* $K_n^M(K)$ *of the following form generate the group* $G^t(L/K)/G^{t+1}(L/K)$ *via the homomorphism* Ψ_n *of local class field theory.*

(3–6–1) $\{1+u, X_1,\dots, X_s, X_{s+2},\dots, X_{n-1}, \pi_K\}$ *if* $s\neq n-1$,

(3–6–2) $\{1+u, X_1,\dots, X_{n-1}\}$ *if* $s=n-1$,

where $v_K(u)=t$.

We prove (3–4) and (3–6) simultaneously by induction on $[L\colon K]$. If $[L\colon K]=p$, (3–4) is trivial and (3–6) can be seen from Kato [5] II p. 668∼670 (C) and (D). If $[L\colon K]>p$, we fix a subextension L_0 of degree p as in the proof of (1–5). Assume (3–4) and (3–6) are valid for L/L_0. By Kato [5] I p. 322 Lemma 2, we may suppose the elements of $K_n^M(L_0)$ satisfying the condition of (3–6) are the symbols such that all except the first component are contained in $K^\times$. By the proof of (1–5) and the formula $N_{L_0/K}\{x, y\}=\{N_{L_0/K}(x), y\}$ where $x\in L_0^\times$ and $y\in K_{n-1}^M(K)$, we see that it suffices to show

$$\text{(3–7)} \qquad \varphi(j(l))=j'(l) \qquad \text{for} \quad 1\leqq l\leqq(\log_p[L:K])-1.$$

Here the notations are as in (3–1–2). We have shown $j'(l)\geqq\varphi(j(l))$ in the proof of (1–5). Assume $j'(l)>\varphi(j(l))$. Then we can deduce

$$G^{j'(l)}(L/L_0)\subset G^{j(l)+1}(L/K)$$

by (2–13) and (3–6). This is impossible, because

$$\sharp G^{j'(l)}(L/L_0)\geqq p^l \quad \text{and} \quad \sharp G^{j(l)+1}(L/K)\leqq p^{l-1}.$$

§ 4. Inequalities

In this section we shall prove the following inequalities, which are key to the proof of (0–2) and (0–4).

Lemma (4–1). *Let K be a complete discrete valuation field with residue field $\bar{K}$ of characteristic $p>0$, K_2 be a cyclic extension of K of degree p^2 and K_1 be the subextension of degree p. Let $e_K=v_K(p)$ (if* ch $(\bar{K})=p$, we put $e_K=\infty$).

(4–1–1) *Assume $d_K(K_1/K)\geqq p^{-1}e_K$. Then we have*

$$0\leqq e_K-d_K(K_2/K_1)\leqq p^{-1}(e_K-d_K(K_1/K)).$$

(4–1–2) *Assume $d_K(K_1/K)\leqq p^{-1}e_K$. Then we have*

$$p^{-1}(p^2-p+1)\cdot d_K(K_1/K)\leqq d_K(K_2/K_1).$$

Lemma (4–2). *Let K be as in* (4–1), *K_{n+1} be a cyclic extension of K of degree p^{n+1}, and K_n be the subextension of degree p^n. Assume $0<d_K(K_{n+1}/K_n)\leqq 2^{-1}e_K$. Then we have*

$$(p-1)\cdot d_K(K_n/K)<d_K(K_{n+1}/K_n).$$

Remark (4–3). It seems that Lemma (4–2) in the case ch$(K)=0$ is valid under the weaker assumption $e_K-d_K(K_{n+1}/K_n)>p^{-1}(e_K-d_K(K_n/K_{n-1}))$, where K_{n-1} is the subextension of degree p^{n-1}. This can be checked when $\bar{K}$ is finite, by using the formula above Theorem (1–5) and (4–7) below.

Corollary (4–4). *Let K be an algebraic extension of a complete discrete valuation field of mixed characteristics* $(0, p)$, *K_∞ be a $\boldsymbol{Z}_p$-extension of K, K_n be the subextension of degree p^n and $b_n = p^n(e_K - d_K(K_{n+1}/K_n))$. Then only the following two cases can occur.*

(4–4–1) $$d_K(K_{n+1}/K_n) = 0 \quad \text{for all} \quad n.$$

(4–4–2) $$\{b_n \mid n \geqq 0\} \text{ is bounded.}$$

Corollary (4–5). *Let K be as in* (4–1), *K_n be a cyclic extension of K of degree p^n and K_m be the subextension of degree p^m for $0 \leqq m \leqq n$. Assume K_1/K is wildly ramified.*

(4–5–1) *If $d_K(K_m/K_{m-1}) \leqq 2^{-1}e_K$, we have*
$$d_K(K_m/K_{m-1}) \geqq (p^{2m-1}+1)(p-1)(p+1)^{-1}p^{-m} \quad \text{and}$$
$$d_K(K_m/K) \geqq (p^{2m}-1)(p+1)p^{-m}.$$

(4–5–2) *Assume moreover $[K_n : K] = [\overline{K_n} : \overline{K}]$. Then if $d_K(K_m/K_{m-1}) \leqq 2^{-1}e_K$, we have*

$$d_K(K_m/K_{m-1}) \geqq p^m - p^{m-1} \quad \text{and} \quad d_K(K_m/K) \geqq p^m - 1.$$

First we deduce Corollaries (4–4) and (4–5) from (4–1) and (4–2). By (2–15) we see that (4–1) is still valid if we take K as in (4–4). So (4–4) can be seen from (4–1). In fact if $d_K(K_{m+1}/K_m) > 0$ for some m, (4–1–2) assures us that $d_K(K_{n+1}/K_n) \geqq p^{-1}e_K$ for sufficiently large n and then we can apply (4–1–1). In the case $n=1$, (4–5–1) (resp. (4–5–2)) follows from the fact $(p-1)^{-1}p \cdot d_K(K_1/K) \in \boldsymbol{Z}$ (resp. $(p-1)^{-1}d_K(K_1/K) \in \boldsymbol{Z}$) (cf. (2–10)). The general case can be shown by induction by using the following (4–6).

Sublemma (4–6) *Assume $d_K(K_m/K_{m-1}) \leqq 2^{-1}e_K$. Then we have*

(4–6–1) $$d_K(K_m/K_{m-1}) \geqq (p-1) \cdot d_K(K_{m-1}/K) + (p-1) \cdot p^{-m}$$

(*Note $e_{K_m} \leqq p^m \cdot e_K$*). *If we assume moreover $[K_m : K] = [\overline{K_m} : \overline{K}]$,*

(4–6–2) $$d_K(K_m/K_{m-1}) \geqq (p-1) \cdot d_K(K_{m-1}/K) + (p-1).$$

Sublemma (4–6) is a consequence of (4–2) and the fact $(p-1) \mid e_{K_m} \cdot e_K^{-1} d_K(K_m/K_{m-1})$ (cf. (2–10)).

Secondly we prove (4–1). The first inequality of (4–1–1) can be seen from (2–16) (or from the fact $v_K(p) = e_K$). We shall show the other inequalities. We can reduce (4–1) to the case where $\overline{K}$ is finitely generated over $\boldsymbol{F}_p$, as any complete discrete valuation field is the completion of an inductive limit of a directed system of complete discrete valuation fields whose residue fields are finitely generated over $\boldsymbol{F}_p$ (Kato [5] II §1.5 Cor. 2 to Lemma 10). Let $(n-1)=\text{trans. degree}_{\boldsymbol{F}_p}\ \bar{K}$. Then $\bar{K}$ is a finite extension of $\boldsymbol{F}_p(X_1,\dots,X_{n-1})$. Let $E=\bar{K}\cdot\boldsymbol{F}_p((X_1))\cdots((X_{n-1}))$, then $E/\bar{K}$ is a separable extension of $\bar{K}$. So we can reduce (4–1) moreover to the case where K is an n-dimensional local field.

Thus it suffices to prove (4–1) for the first component of the depth of ramification of the extension of n-dimensional local fields K_2/K. Let $\{j(l)\}$ (resp. $\{j(l)_1\}$) be the jumping numbers (resp. their first components) of K_2/K. Then by Theorem (1–5), we have

$$d_K(K_1/K)=p^{-1}(p-1)\cdot j(2) \text{ and } d_K(K_2/K)\geqq p^{-2}(p-1)(p\cdot j(1)+j(2)).$$

So $$d_K(K_2/K_1)\geqq p^{-1}(p-1)\cdot j(1)-p^{-2}(p-1)^2 j(2).$$

Now (4–1) can be seen from the following;

Lemma (4–7). *Let the assumptions be as above.*

(4–7–1) *If* $j(2)_1\geqq(p-1)^{-1}e_K$, *we have* $j(1)_1\geqq j(2)_1+e_K$.

(4–7–2) *If* $j(2)_1\leqq(p-1)^{-1}e_K$, *we have* $j(1)_1\geqq p\cdot j(2)_1$.

Let $\Psi_n\colon K_n^M(K)\longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$ be the reciprocity map. Choose $x\in U^{j(2)}K_n^M(K)$ such that $\Psi_n(x)$ is not trivial in $\mathrm{Gal}(K_1/K)$. Then, as K_2/K is cyclic, $\Psi_n(x^p)$ is not trivial in $\mathrm{Gal}(K_2/K)$. Let $m=\min\{j(2)+v_K(p),\ p\cdot j(2)\}$. As $(U_K^{j(2)})^p\subset U_K^m$, we have $x^p\in U^m K_n^M(K)$. Thus we obtain $j(1)\geqq m$. Noting that e_K is nothing other than the first component of $v_K(p)$, we have (4–7).

Remark (4–8). Though (4–2) cannot be shown by using Theorem (1–5), we can prove a similar result to its corollary (4–5–1) by using (1–5). Let the notations be as in (4–5) and let r be the minimal integer such that $p^r>(p-1)^{-1}e_K$. Then we have

$$d_K(K_m/K)\geqq(p^{2m}-1)(p-1)^{-1}p^{-m} \quad \text{if} \quad m\leqq r.$$

In fact we can reduce this to the case where K is an n-dimensional local field, and in the similar way to (4–7) we can show the first components $\{j(l)_1\}$ of jumping numbers of K_m/K satisfy

$$j(m-i)_1\geqq p^i \qquad \text{for} \quad 0\leqq i\leqq m.$$

Now our assertion follows from (1–5).

Lastly we prove (4–2). We only give a proof for the case $\mathrm{ch}(K)=0$, as it suffices for the later use. The proof of the case $\mathrm{ch}(K)=p$ is similar. Let $e_n=e_{K_n}/e_K$, π_n be a prime element of K_n, $d=d_K(K_{n+1}/K_n)$, and σ be a generator of $\mathrm{Gal}(K_{n+1}/K)$. We may assume K contains a primitive p-th root ζ of unity, for we have $d_K(M(\zeta)/L(\zeta))=d_K(M/L)$ for any finite separable extension M/L (to see this, use (2–12) and the fact that $M(\zeta)/M$ and $L(\zeta)/L$ are tamely ramified). By (2–16), we can suppose $K_{n+1}=K((1+y)^{p^{-1}})$ for some $y\in K_n$ such that

(4–9–1) $$v_K(y)=(p-1)^{-1}p\cdot(e_K-d),$$

(4–9–2) $$p\nmid e_n\cdot v_K(y) \quad \text{if} \quad \overline{K_{n+1}}=\overline{K_n},$$

(4–9–3) $$\overline{y\cdot\pi_n^{-e_n v_K(y)}}\notin\overline{K_n^p} \quad \text{if} \quad [\overline{K_{n+1}}:\overline{K_n}]_{\mathrm{insep}}=p.$$

We put $(1+y)^{p^{-1}}=1+w$. Then $v_K(w)=p^{-1}v_K(y)=(p-1)^{-1}(e_K-d)$. As $\sigma^{p^n}(1+w)=\zeta\cdot(1+w)$, we have

(4–10) $$(1-\sigma^{p^n})\cdot w\overset{def}{=}w-\sigma^{p^n}w=(1-\zeta)(1+w).$$

On the other hand, we can choose $z_n\in K_n$ and $z_{n+1}\in K_{n+1}\backslash K_n$ satisfying the following conditions. (Note that $(1-\sigma)\cdot w\notin K_n$ as $(1-\sigma^{p^n})\cdot w\notin K_n$.)

(4–11–1) $$(1-\sigma)\cdot w=z_n+z_{n+1},$$

(4–11–2) $$e_n\cdot v_K(z_{n+1})\notin \boldsymbol{Z} \quad \text{if} \quad \overline{K_{n+1}}=\overline{K_n},$$

(4–11–3) $$\overline{z_{n+1}\cdot\pi_n^{-e_n\cdot v_K(z_{n+1})}}\notin\overline{K_n} \quad \text{if} \quad [\overline{K_{n+1}}:\overline{K_n}]_{\mathrm{insep}}=p.$$

(The choice of z_n and z_{n+1} is not unique, but $v_K(z_{n+1})$ is uniquely determined). Let $1+\sigma+\cdots+\sigma^{p^n-1}$ act on both sides of (4–11–1), then we have

(4–12) $$(1-\sigma^{p^n})\cdot w=\mathrm{Tr}_{K_n/K}(z_n)+(1+\sigma+\cdots+\sigma^{p^n-1})\cdot z_{n+1}.$$

Now the key point is

(4–13) $$v_K(z_{n+1})>(p-1)^{-1}e_K.$$

We give a proof of (4–2) assuming (4–13). Note $v_K(1-\zeta)=(p-1)^{-1}e_K$ (Serre [14] §4 Proposition 17). Since we have $v_K((1-\sigma^{p^n})\cdot w)=(p-1)^{-1}e_K$ by (4–10), we have by (4–12) and (4–13)

(4–14) $$v_K(\mathrm{Tr}_{K_n/K}(z_n))=(p-1)^{-1}e_K.$$

As

(4–15) $$v_K(z_n)\geqq v_K((1-\sigma)\cdot w)>(p-1)^{-1}(e_K-d),$$

we have by the definition of the depth of ramification

(4–16) $$v_K(\mathrm{Tr}_{K_n/K}(z_n))-d_K(K_n/K)\geqq v_K(z_n)>(p-1)^{-1}(e_K-d).$$

Then, Lemma (4–2) follows from (4–14) and (4–16). Now we return to the proof of (4–13). Let $(1-\sigma)$ act on both sides of (4–12), then we have

$$(1-\sigma)\cdot w\cdot(1-\zeta)=(1-\sigma^{p^n})\cdot z_{n+1}.$$

So by (4–11–1), we have

$$(4\text{–}17)\qquad (1-\zeta)\cdot z_n+(1-\zeta)\cdot z_{n+1}=(1-\sigma^{p^n})\cdot z_{n+1}.$$

By (4–11–2), (4–11–3) and (2–10), we have

$$(4\text{–}18)\quad v_K((1-\sigma^{p^n})\cdot z_{n+1})=v_K(z_{n+1})+(p-1)^{-1}d<v_K(z_{n+1})+(p-1)^{-1}e_K.$$

By (4–15), (4–17) and (4–18), we obtain

$$v_K(z_{n+1})=v_K(z_n)+(p-1)^{-1}(e_K-d)>2\cdot(p-1)^{-1}(e_K-d).$$

Now (4–13) follows from the assumption $d\leqq 2^{-1}e_K$.

§ 5. Inseparable degrees of residue field extensions

To the end of this paper, let K be a complete discrete valuation field of mixed characteristics $(0, p)$. In this section we prove Proposition (0–4).

We may assume $\bar{K}$ is separably closed and moreover $[L: K]$ is a power of p. So let $[L: K]=p^n$ and let K_m be the subextension of degree p^m for $0\leqq m\leqq n$ $(L=K_n)$. We may also assume K_1/K is wildly ramified.

First we prove (0–4) in the case $(p-1)\nmid e_K$. The key fact is;

Lemma (5–1). *Let r be the minimal non-negative integer such that $r\equiv e_K \pmod{p-1}$ and let s be an integer such that $p^s=[\overline{K_n}: \bar{K}]$. Then we have*

$$r\leqq p^{n-s}(e_K-d_K(K_n/K_{n-1})).$$

We see that $p^{n-s}(e_K-d_K(K_n/K_{n-1}))$ is a non-negative integer by (4–1–1) and the fact $e_{K_n}/e_K=p^{n-s}$. By (2–10) we know that $p^{n-s}\cdot d_K(K_n/K_{n-1})$ is divisible by $(p-1)$. So, (5–1) follows from the fact $p^{n-s}e_K\equiv r \pmod{p-1}$.

Define an integer l by

$$l=\min\{1\leqq m\leqq n \mid d_K(K_m/K_{m-1})>p^{-1}e_K\}\cup\{n+1\}.$$

By (4–1–1) and (5–1), we have for $l\leqq n$

$$p^{s-n}r\leqq e_K-d_K(K_n/K_{n-1})\leqq p^{l-n}(e_K-d_K(K_l/K_{l-1})).$$

So

(5–2) $$p^{s-l}r+d_K(K_l/K_{l-1})\leqq e_K.$$

If $l=n+1$, (5–2) holds by replacing l by $l-1$.

We want to prove the following inequalities for $m\leqq l$.

(5–3–1) $$d_K(K_m/K_{m-1})>p^{m-3}(p^2-p+1)(p-1)(p+1)^{-1}$$

(5–3–2) $$d_K(K_m/K_{m-1})>p^{m-3}(p^2-p+1)(p-1)\quad\text{if}\quad [\overline{K_m}:\overline{K}]=p^m.$$

If $m=1$, (5–3–1) (resp. 5–3–2)) follows from the fact $d_K(K_1/K)\geqq p^{-1}(p-1)$ (resp. $d_K(K_1/K)\geqq(p-1)$) (cf. (2–16)). If $m\geqq 2$, we have by (4–1–2)

$$d_K(K_m/K_{m-1})\geqq p^{-1}(p^2-p+1)\cdot d_K(K_{m-1}/K_{m-2}).$$

So, in this case (5–3–1) and (5–3–2) follows from (4–5).

Now (0–4) in the case $(p-1)\nmid e_K$ follows from (5–2), (5–3–1) and (5–3–2).

Remark (5–4). If the assertion in (4–3) is true, we can replace (5–3–1) (resp. (5–3–2)) by

$$d_K(K_l/K_{l-1})\geqq(p^{2l-1}+1)(p-1)(p+1)^{-1}p^{-l}$$
$$(\text{resp. } d_K(K_l/K_{l-1})\geqq p^{l-1}(p-1)).$$

So we can prove (0–4) in the case $(p-1)\nmid e_K$ for $f(n)=\max\{a+b\mid r\cdot p^{a-1}+(p^{2b+1}+1)(p-1)(p+1)^{-1}p^{-b-1}\leqq n,\ a,\ b\in \boldsymbol{Z},\ b\geqq 0\}$ and $g(n)=\max\{a+b\mid r\cdot p^{a-1}+p^b(p-1)\leqq n,\ a,\ b\in\boldsymbol{Z},\ b\geqq 0\}$.

Next we prove (0–4) in the case of $(p-1)\mid e_K$. In this case K contains a primitive p-th root ζ of unity.

As in the proof of Miki [9] Proposition 6, we use the following well-known fact.

Lemma (5–5). *There is an element $y\in K_{n-1}$ such that*

$$N_{K_{n-1}/K}(y)=\zeta.$$

We fix $y\in K_{n-1}$ such that $N_{K_{n-1}/K}(y)=\zeta$. As $\zeta\in U_K^1$, we have $y\in U_{K_{n-1}}^1$. Let $y_m=N_{K_{n-1}/K_m}(y)$ and let $v_m=v_K(1-y_m)$ for $0\leqq m\leqq n-1$. Then by Serre [14] §5 Lemma 5, we have

(5–6–1) $$v_m\geqq v_{m+1}+d_K(K_{m+1}/K_m)\quad\text{if}\quad v_{m+1}\geqq(p-1)^{-1}d_K(K_{m+1}/K_m)$$

(5–6–2) $$v_m=p\cdot v_{m+1}\quad\text{if}\quad v_{m+1}<(p-1)^{-1}d_K(K_{m+1}/K_m).$$

Define an integer l by

$$l=\max\{0\leqq m\leqq n-2\mid v_{m+1}\geqq(p-1)^{-1}d_K(K_{m+1}/K_m)\}\cup\{-1\}.$$

As $v_{m+1}<v_m$ and $d_K(K_{m+1}/K_m)>d_K(K_m/K_{m-1})$, we have

$$v_{m+1}\geqq(p-1)^{-1}d_K(K_{m+1}/K_m) \quad \text{for} \quad 0\leqq m\leqq l.$$

Thus by (5–6–1), (5–6–2), (2–4–1) and the fact $v_0=v_K(1-\zeta)=(p-1)^{-1}e_K$, we have

(5–7) $$0<v_{n-1}\leqq p^{l-(n-2)}((p-1)^{-1}e_K-d_K(K_{l+1}/K)).$$

Let $[\overline{K_n}: \overline{K}]=p^s$. Then we have

$$[\overline{K_{n-1}}: \overline{K}]\geqq p^{s-1} \quad \text{and} \quad p^{s-n}\leqq v_{n-1}.$$

In the case $p\neq 2$, we have $d_K(K_{l+1}/K)<2^{-1}e_K$ by (5–7). So by (5–7) and (4–5–1) we have

$$p^{s-n}\leqq p^{l-n+2}((p-1)^{-1}e_K-(p^{2l+2}-1)(p+1)^{-1}p^{-l-1}).$$

So

(5–8–1) $$p^{s-l-2}+(p^{2l+2}-1)(p+1)^{-1}p^{-l-1}\leqq(p-1)^{-1}e_K.$$

Assume $s=n$. Then by (5–7) and (4–5–2), we have

(5–8–2) $$p^{n-l-2}+p^{l+1}\leqq(p-1)^{-1}e_K+1.$$

Now (0–4) in the case $(p-1)\mid e_K$ and $p\neq 2$ follows from (5–8–1) and (5–8–2). In the case $p=2$, if $d_K(K_{l+1}/K_l)\geqq 2^{-1}e_K$, we have by (5–7)

$$\begin{aligned}p^{n-l-2}v_{n-1}\leqq e_K-d_K(K_{l+1}/K)\leqq e_K-2^{-1}e_K-d_K(K_l/K)\\ <2^{-1}(e_K-d_K(K_l/K)).\end{aligned}$$

So (5–8–1) and (5–8–2) holds by replacing l by $l-1$. Thus we have completed the the proof of (0–4).

§ 6. An effective finiteness of the "connected part" of fundamental groups of abelian varieties

In this section we prove Proposition (0–5) in a little more general situation. Let K be a complete discrete valuation field of mixed characteristics (0, p) and A be an abelian variety defined over K which has *stable* reduction. We define the "connected part" $\pi_1^{\mathrm{con}}(A)$ of $\pi_1^{\mathrm{geo}}(A)$ as follows.

Let $\mathscr{A}$ be the Néron model of A (Raynaud [13]) i.e. $\mathscr{A}$ is a commutative group scheme defined over O_K characterized by the following properties.

(6–1–1) $$A\simeq\mathscr{A}\times_{O_K}K$$

(6–1–2) $\qquad \mathrm{Hom}_{O_K}(Y, \mathscr{A}) = \mathrm{Hom}_K(Y \times_{O_K} K, A)$

for any scheme Y smooth over O_K.

Let $\mathscr{A}^\circ$ be the connected component of $\mathscr{A}$, ${}_n\mathscr{A}^\circ$ be the kernel of multiplication by n, and define the fixed part $({}_n\mathscr{A}^\circ)^f$ by the maximal finite flat subgroup of ${}_n\mathscr{A}^\circ$ as in Grothendieck [3]. Then for any prime l, $\{({}_{l^n}\mathscr{A}^\circ)^f\}_n$ forms an l-divisible group. Recall that there is a canonical exact sequence of finite flat group schemes over O_K

$$0 \longrightarrow ({}_n\mathscr{A}^\circ)^{f,\mathrm{con}} \longrightarrow ({}_n\mathscr{A}^\circ)^f \longrightarrow ({}_n\mathscr{A}^\circ)^{f,\mathrm{et}} \longrightarrow 0,$$

where $({}_n\mathscr{A}^\circ)^{f,\mathrm{con}}$ (resp. $({}_n\mathscr{A})^{f,\mathrm{et}}$) is connected (resp. etale). Thus we can define the subquotients of the Tate module $T(A) = \varprojlim_n {}_nA(K_{\mathrm{sep}})$, $T^f(A)$, $T^{f,\mathrm{con}}(A)$ and $T^{f,\mathrm{et}}(A)$ as the Tate module of $\{({}_n\mathscr{A}^\circ)^f(K_{\mathrm{sep}})\}_n$, $\{({}_n\mathscr{A}^\circ)^{f,\mathrm{con}}(K_{\mathrm{sep}})\}_n$ and $\{({}_n\mathscr{A}^\circ)^{f,\mathrm{et}}(K_{\mathrm{sep}})\}_n$ respectively. (These groups are $\hat{\boldsymbol{Z}}$-G_K-modules. In fact $T^{f,\mathrm{con}}(A)$ is a $\boldsymbol{Z}_p$-module). We have an exact sequence

(6–2) $\qquad 0 \longrightarrow T^{f,\mathrm{con}}(A) \longrightarrow T^f(A) \longrightarrow T^{f,\mathrm{et}}(A) \longrightarrow 0.$

Definition (6–3). We define the "connected part" $\pi_1^{\mathrm{con}}(A)$ as the image of the natural homomorphism

$$T^{f,\mathrm{con}}(A) \longrightarrow T(A)_{G_K} \simeq \pi_1^{\mathrm{geo}}(A).$$

(Here, $T(A)_{G_K}$ is the G_K-co-invariant. For the isomorphism $T(A)_{G_K} \simeq \pi_1^{\mathrm{geo}}(A)$, see Bloch [1] Lemma 5.3.)

Remark (6–4). If A has good reduction, we have $T^f(A) = T(A)$ and $T^{f,\mathrm{et}}(A)_G = \pi_1^{\mathrm{geo}}(A_s)$ where $A_s = \mathscr{A} \times_{O_K} \bar{K}$ is the reduction of A. So by (6–2) we have an exact sequence

$$0 \longrightarrow \pi_1^{\mathrm{con}}(A) \longrightarrow \pi_1^{\mathrm{geo}}(A) \longrightarrow \pi_1^{\mathrm{geo}}(A_s) \longrightarrow 0.$$

Thus Definition (6–3) coincides with the definition in Introduction.

Now we prove (0–5) *assuming A has stable reduction.* Assume there is an element of order p^r in $\pi_1^{\mathrm{con}}(A)$. Then by definition, there is a subgroup H of ${}_{p^r}A(K_{\mathrm{sep}})$ satisfying the following properties.

(6–5–1) $\quad H \supset \{\sigma \cdot x - x \mid x \in {}_{p^r}A(K_{\mathrm{sep}}),\ \sigma \in G_K\}$

(6–5–2) $\quad {}_{p^r}(A)(K_{\mathrm{sep}})/H \simeq \boldsymbol{Z}/p^r\boldsymbol{Z}$

(6–5–3) $\quad ({}_p\mathscr{A}^\circ)^{f,\mathrm{con}}(K_{\mathrm{sep}}) \cdot H/H \simeq \boldsymbol{Z}/p^r\boldsymbol{Z}$

Let $\tilde{A} = A/H$, then by (6–5–1) $\tilde{A}$ is defined over K. Let

$$\psi: \tilde{A} \longrightarrow A/_{p^r}A \simeq A$$

be a natural homomorphism. Then ψ is a cyclic covering of degree p^r. Let $\tilde{\mathscr{A}}$ be the Néron model of $\tilde{A}$, then by (6–5–2) and (6–5–3) there exists an exact sequence of group schemes over O_K

$$(6\text{–}6) \qquad 0 \longrightarrow \mathscr{J} \longrightarrow \tilde{\mathscr{A}} \longrightarrow \mathscr{A} \longrightarrow 0,$$

where $\mathscr{J}$ is a connected finite flat group scheme over O_K of order p^r. (By (6–5–3), $\mathscr{J}$ is a subgroup of $({}_n\tilde{\mathscr{A}}^\circ)^{f,\mathrm{con}}$.) Since $\mathscr{J}$ is connected, we can replace $\tilde{\mathscr{A}}$ by $\tilde{\mathscr{A}}^\circ$ and $\mathscr{A}$ by $\mathscr{A}^\circ$ in (6–6). Let $\mathscr{K}$ (resp. $\tilde{\mathscr{K}}$) be the completion of the function field of $\mathscr{A}^\circ$ (resp. $\tilde{\mathscr{A}}^\circ$) by the discrete valuation correspondes to $\mathscr{A}^\circ \times_{O_K} \bar{K}$ (resp. $\tilde{\mathscr{A}}^\circ \times_{O_K} \bar{K}$). Then $\tilde{\mathscr{K}}$ and $\mathscr{K}$ are complete discrete valuation fields of mixed characteristics $(0, p)$. Moreover $\tilde{\mathscr{K}}/\mathscr{K}$ is a cyclic extension of degree p^r, and since $\mathscr{J}$ is connected, we have $[\tilde{\mathscr{K}} : \mathscr{K}] = [\bar{\tilde{\mathscr{K}}} : \bar{\mathscr{K}}]_{\mathrm{insep}} = p^r$. Thus by (0–4–2), we obtain $r \leqq g(e_K)$.

§7. A generalization of Miki's theorem

In this section we prove Theorem (0–2).

Let K be a complete discrete valuation field of mixed characteristics $(0, p)$ with separably closed residue field and let k be the canonical subfield of K (cf. (0–1–1)$\sim$(0–1–3)). For any integer $n \geqq 0$, let ζ_n be a primitive p^n-th root of unity, $K_n = K(\zeta_n)$, $k_n = k(\zeta_n)$, $K_\infty = \bigcup_{n=1}^{\infty} K_n$, $k_\infty = \bigcup_{n=1}^{\infty} k_n$ and $\widehat{K_\infty^\times}$ (resp. $\widehat{k_\infty^\times}$) be the p-adic completion of $K_\infty^\times$ (resp. $k_\infty^\times$). As k is algebraically closed in K, we have $\mathrm{Gal}(K_\infty/K) \simeq \mathrm{Gal}(k_\infty/k)$. By Tate [16] Prop. (2.2), we have

$$\widehat{K_\infty^\times} \simeq H^1(G_{K_\infty}, \boldsymbol{Z}_p(1)) \quad \text{and} \quad \widehat{k_\infty^\times} \simeq H^1(G_{k_\infty}, \boldsymbol{Z}_p(1)).$$

Proposition (7–1). *Let* $C = \mathrm{Gal}(K_\infty/K) = \mathrm{Gal}(k_\infty/k)$. *Then we have an isomorphism*

$$H^0(C, \widehat{k_\infty^\times}(r)) \xrightarrow{\simeq} H^0(C, \widehat{K_\infty^\times}(r)) \quad \textit{if} \quad r \neq 0.$$

We deduce Theorem (0–2) from (7–1). Consider the following commutative diagram of exact sequences where the vertical arrows are inflation maps.

(7–2)

$$\begin{array}{ccccccccc}
0 \longrightarrow & H^1(C, \boldsymbol{Z}_p(r)) & \xrightarrow{\mathrm{Inf}} & H^1(G_k, \boldsymbol{Z}_p(r)) & \xrightarrow{\mathrm{Res}} & H^0(C, \widehat{k_\infty^\times}(r-1)) & \longrightarrow & H^2(C, \boldsymbol{Z}_p(r)) \\
& \downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 \longrightarrow & H^1(C, \boldsymbol{Z}_p(r)) & \xrightarrow{\mathrm{Inf}} & H^1(G_K, \boldsymbol{Z}_p(r)) & \xrightarrow{\mathrm{Res}} & H^0(C, \widehat{K_\infty^\times}(r-1)) & \longrightarrow & H^2(C, \boldsymbol{Z}_p(r))
\end{array}$$

Now (0–2) follows from (7–1) and (7–2).

Before we prove (7–1), we give some notations. For an algebraic extension N of K, let $\hat{\Omega}(O_N)=\varprojlim_n \Omega_{\mathbf{Z}}(O_N)/p^n$ be the p-adic completion of the absolute differential group of the integer ring O_N and let $\hat{O_N}(I)=\varprojlim_n (\bigoplus_{i\in I} O_N)/p^n$ for a set I.

Proposition (7–1) can be seen from the following Lemmas (7–3) and (7–4).

Lemma (7–3). *We have an exact sequence of C-modules*

$$0 \longrightarrow \widehat{k_\infty^\times} \longrightarrow \widehat{K_\infty^\times} \xrightarrow{d\log} \hat{\Omega}(O_{K_\infty}),$$

where $d\log$ *is defined by* $d\log(y)=dy/y$ *for* $y\in O_{K_\infty}^\times$ *and* $d\log(w)=0$ *for* $w\in k_\infty^\times$.

Lemma (7–4). *We have* $H^0(C, \hat{\Omega}(O_{K_\infty})(r))=0$ *if* $r\neq 0$.

To prove (7–3) and (7–4), we need the following little stronger version of a theorem of Epp [2].

Proposition (7–5). *Let K and k be as above, l be a* $\boldsymbol{Z}_p$*-extension of k, and* $L=lK$. *Then for any finite extension* M/L *such that l is algebraically closed in M, we have*

$$[M: L]=[\bar{M}: \bar{L}]_{\text{insep}}.$$

We will give a proof of (7–5) at the end of this section.

Corollary (7–6). *Let* e_n *be the ramification index of* K_n/k_n. *Then we have* $e_n=1$ *for* $n\gg 0$. *In other words, a prime element of* k_n *is still a prime element of* K_n *for* $n\gg 0$.

We prove (7–6). By Theorem (31.1) of Nagata [11], we can choose a subfield K_0 of K such that

(7–7–1) K_0 is complete with respect to the valuation induced from K,

(7–7–2) $\overline{K_0}=\bar{K}$,

(7–7–3) p is a prime element of K_0,

Then K/K_0 is a totally ramified extension of degree e_K, and a prime element of k_n is a prime element of K_0k_n, so e_n equals the ramification index of K_n/K_0k_n. As $\bar{k}$ is algebraically closed, k_∞/k_2 is a totally ramified $\boldsymbol{Z}_p$-extension. We apply (7–5) for $L=k_\infty(K_0k_2)=K_0k_\infty$ and $M=K_\infty$, then we have $[K: K_0k]=[\overline{K_\infty}: \overline{K_0k_\infty}]=[\overline{K_\infty}: \bar{K}]$. Thus we obtain $[\overline{K_n}: \bar{K}]=[K: K_0k]$ for $n\gg 0$. Now (7–6) follows from the fact $e_n\cdot[\overline{K_n}: \bar{K}]=[K_n: K_0k_n]=[K: K_0k]$.

Lemma (7–8). *Fix an integer $n\geqq 2$ satisfying the condition of* (7–6). *Choose $\{u_i\}_{i\in I}\subset O_{K_n}$ such that $\{\bar{u}_i\}_{i\in I}$ forms a p-base of $\bar{K}_n$. Let $\{x_i\}_{i\in I}$ be the canonical base of $O_{K_\infty}\hat{}(I)$ and let $C_n=\mathrm{Gal}(K_\infty/K_n)$. Then we have an isomorphism of O_{K_∞}-C_n-modules*

$$\begin{array}{ccc} O_{K_\infty}\hat{}(I) & \xrightarrow{\simeq} & \hat{\Omega}(O_{K_\infty}) \\ \Psi & & \Psi \\ x_i & \longmapsto & du_i/u_i \end{array}$$

We prove (7–8). By the same argument as Hyodo [4] §4, we can show that there is an exact sequence of O_{K_∞}-C_n-modules

$$\begin{array}{ccccccc} 0 \longrightarrow K_\infty/\vartheta(1) & \longrightarrow & \varinjlim_{n<m} \hat{\Omega}(O_{K_m}) & \longrightarrow & O_{K_n}\hat{}(I)\otimes_{O_{K_n}}O_{K_\infty} & \longrightarrow 0, \\ \Psi & & \Psi & & \Psi & \\ a\cdot(\zeta_r)_r & \mapsto & p^r\cdot a\cdot d\zeta_r/\zeta_r & & & \\ & & b\cdot du_i/u_i & \mapsto & x_i\otimes b & \end{array}$$

where $\vartheta=\{y\in K_\infty\mid v_K(y)\geqq-(p-1)^{-1}e_K\}$. We see that $\hat{\Omega}(O_{K_\infty})=\varprojlim_r(\varinjlim_{n<m}\hat{\Omega}(O_{K_m}))/p^r$, and that K_∞/ϑ is p-divisible. Thus we have (7–8).

We prove (7–4). As K_∞/K_n is a $\boldsymbol{Z}_p$-extension of type (4–4–2) (note for $n\gg 0$, K_{n+1}/K_n is totally ramified), we can show $H^0(C_n, O_{K_\infty}\hat{}(I)(r))=0$ for $r\neq 0$ by the same argument as in Tate [15] §3.1 Proposition 8 (b). The assertion (7–4) follows from (7–8) and the well-known fact

$$H^0(C, \hat{\Omega}(O_{K_\infty})(r))=H^0(C/C_n, H^0(C_n, \hat{\Omega}(O_{K_\infty})(r))\,.$$

To show (7–3), it suffices to prove $\mathrm{Ker}(d\log)=\widehat{k_\infty^\times}$. It is trivial that $\mathrm{Ker}(d\log)\supset\widehat{k_\infty^\times}$, so we have to show $d\log(q)\neq 0$ for any $q\notin\widehat{k_\infty^\times}$. We may assume $q\notin\widehat{k_\infty^\times}\cdot(\widehat{K_\infty^\times})^p$ as $\widehat{K_\infty^\times}$ is torsion free. Let $q_r\in K_\infty^\times$ be a representative of q in $(K_\infty^\times)/(K_\infty^\times)^{p^r}$ and $L_{q,r}=K_\infty((q_r)^{p^{-r}})$. By (7–5) we have $[\overline{L_{q,r}}: \overline{K_\infty}]_{\mathrm{insep}}=p^r$. So, we obtain $d_K(L_{q,1}/K_\infty)>0$.

Sublemma (7–9). *Assume $d_K(L_{q,1}/K_\infty)>p^{-1}e_K$. Then we have*

$$d\log(q)\neq 0.$$

Fix an integer m such that $q_1\in K_m^\times$ and $[\overline{K_m(q_1^{p^{-1}})}: \overline{K_m}]_{\mathrm{insep}}=p$, and let $K_{m,1}=K_m(q_1^{p^{-1}})$. Note that $O_{K_\infty}(a)=O_{L_{q,1}}$ for any $a\in O_{K_{m,1}}$ such that $O_{K_m}(a)=O_{K_{m,1}}$. So we have by (2–10) $d_K(L_{q,1}/K_\infty)=d_K(K_{m,1}/K_m)$. By (2–16), we see that $q_1\equiv 1+u\cdot w\ (\mathrm{mod}\,(K_m^\times)^p)$ for $u\in O_{K_m}$ such that

$\bar{u} \notin \overline{K_m}^p$ and $w \in O_k$ such that $v_K(w) = (p-1)^{-1} p \cdot (e_K - d_K(L_{q,1}/K_\infty)) < e_K$ (here we use the assumption). So the image of q_1 by the homomorphism

$$d\log\colon K_\infty^\times/p \longrightarrow \hat{\Omega}(O_{K_\infty})/p$$

is non-trivial. Thus (7–9) follows.

By (4–4–2) we have $d_K(L_{q,r+1}/L_{q,r}) > p^{-1} e_K$ for sufficiently large r. Consider a commutative diagram

$$\begin{array}{ccc} d\log\colon \widehat{K_\infty^\times} & \longrightarrow & \hat{\Omega}(O_{K_\infty}) \\ \iota \downarrow & & \downarrow \\ d\log'\colon \widehat{L_{q,r}^\times} & \longrightarrow & \hat{\Omega}(O_{L_{q,r}}), \end{array}$$

where the vertical arrows are natural homomorphism. There is an element $q' \in \widehat{L_{q,r}^\times}$ such that $\iota(q) = (q')^{p^r}$. By (7–9), we have $d\log'(q') \neq 0$. Now Lemma (7–3) follows from the fact $\hat{\Omega}(O_{L_{q,r}})$ is torsion free.

Our final task is to prove Proposition (7–5). We may assume M/L is Galois. Let l_n be the subextension of l/k of degree p^n and K_0 be the subfield of K satisfying (7–7–1)$\sim$(7–7–3). As $K(\zeta_1)/K$ is tamely ramified, we may assume $\zeta_1 \in K$. By replacing K by $K_0 l_n$ for sufficiently large n, we may assume

(7–10–1) a prime element π_k of k is still a prime element of K

(7–10–2) there is a finite Galois extension M_0/K, linearly disjoint from L, such that $M_0 L = M$.

As $\bar{K}$ is separably closed, any tamely ramified extension of K is defined over k. So, Gal(M_0/K) is a p-group, for k is algebraically closed in M_0. By using induction, we can see easily that it suffices to show (7–5) in the case where M_0/K is cyclic of degree p.

Let $M_0 = K(a^{p^{-1}})$. We assume on the contrary $\bar{M} = \bar{L}$. Then by Tate [15] Proposition 9, we have $d_K(M/L) = 0$. By replacing K by Kl_n for sufficiently large n, we may assume $e_K < v_K(a-1) < p \cdot e'$ where $e' = (p-1)^{-1} e_K$ (cf. (2–15) and (2–16)). As $(K^\times)^p \supset U_K^{p \cdot e'}$ by the assumption that $\bar{K}$ is separably closed, we can write a as follows.

$$a \equiv \prod_{e_K < i < p \cdot e'} (1 + c_i^{p^{m(i)}} \pi_k^i) \mod (K^\times)^p. \tag{7–11}$$

Here, if $p \mid i$, we can take $m(i) = 0$ and either $c_i \in O_K$ such that $\bar{c_i} \notin \bar{K}^p$ or $c_i = 0$. If $p \nmid i$, we can take $m(i) \geqq 0$ and either $c_i \in O_K$ such that $\bar{c_i} \notin \bar{K}^p$ or $c_i \in O_k$. Let

$$h(i)=\begin{cases} e_K\cdot(1+p^{-1}+\cdots+p^{1-m(i)})+i\cdot p^{-m(i)} & \text{if} \quad c_i\notin O_k, \\ +\infty & \text{otherwise,}\end{cases}$$

$$h=\min\{h(i)\mid e_K<i<p\cdot e'\}.$$

Then $h<p\cdot e'$. Moreover h *equals* $h(i)$ *for unique* i. To see this, note that the p-adic valuation of $h(i_1)$ and $h(i_2)$ are different if $m(i_1)\neq m(i_2)$. We fix the integer j such that $h=h(j)$.

What we have to show is the following (7–12).

$$\text{(7–12)} \qquad a\equiv(1+c'_j\cdot\gamma) \quad \bmod (L^\times)^p\cdot U^h,$$

for some $c'_j\in O_K$ such that $c'_j\equiv c_j$ (mod O_K^p) and $\gamma\in k$ such that $v_K(\gamma)=h$, where $U^h=\{1+x|x\in L,\ v_K(x)\gneqq h\}$.

Recall $M=L(a^{p^{-1}})$. By (7–12) we have $[\bar{M}:\bar{L}]_{\text{insep}}=p$. This contradicts our assumption $\bar{M}=\bar{L}$. Thus Proposition (7–5) follows from (7–12).

To see (7–12), it suffices to show

$$\text{(7–13)} \qquad \begin{cases} 1+c_i^{p^{m(i)}}\pi_k^i\equiv 1 & \bmod (L^\times)^pU^h \quad \text{if} \quad i\neq j, \\ 1+c_j^{p^{m(j)}}\pi_k^j\equiv 1+c'_j\cdot\gamma & \bmod (L^\times)^pU^h,\end{cases}$$

where c'_j and γ are as in (7–12). This assertion (7–13) can be obtained by applying Lemma (7–14) below in the following way: In case $c_i\notin O_k$, we put $\varepsilon=p\cdot e'-h$, $c=c_i$, $w=\pi_k^i$ and $m=m(i)$. In case $c_i\in O_k$, we put $\varepsilon=p\cdot e'-h$, $c=1$, $w=c_i\pi_k^i$ and m to be an integer satisfying $e_K\cdot(1+p^{-1}+\cdots+p^{-m+1})+i\cdot p^{-m}>h$).

Lemma (7–14). *Keep the notation as above. Let* $y=(1+c^{p^m}w)$ *for* $m\geqq 1$, *where* $c\in O_K$ *and* $w\in O_k$ *such that* $e_K<v_K(w)<p\cdot e'$. *Then for any* $\varepsilon>0$, *there exist* $c'\in O_K$, $\gamma\in l$ *and* $\gamma'\in L=Kl$ *which satisfy*

$$\text{(7–14–1)} \qquad y\equiv 1+c'\cdot\gamma+\gamma' \quad \bmod (L^\times)^p,$$

$$\text{(7–14–2)} \qquad c'\equiv c \quad \bmod (O_K^p),$$

$$\text{(7–14–3)} \qquad v_K(\gamma)=(1+p^{-1}+\cdots+p^{-m+1})\cdot e_K+p^{-m}v_K(w),$$

$$\text{(7–14–4)} \qquad p\cdot e'-\varepsilon<v_K(\gamma').$$

By induction, it suffices to show (7–14) for the case $m=1$. Let $s(n)=(p-1)^{-1}p\cdot(e_K-d_k(l_n((1+w)^{p^{-1}})/l_n))$. *As* $\bar{k}$ is perfect, by Tate [15] Prop. 9, we have for sufficiently large $n(\varepsilon)$,

$$p\cdot e'-\varepsilon<s(n(\varepsilon)) \quad \text{and} \quad p\cdot e'-v_K(w)<s(n(\varepsilon)).$$

By (2–16) there exists $w' \in l_{n(\varepsilon)}$ such that

$$v_K((1+w)\cdot(1+w')^p-1)=s(n(\varepsilon))<v_K(w) \quad \text{and} \quad v_K(w')=p^{-1}v_K(w).$$

Noting that $e_K+2\cdot p^{-1}e_K \geqq (p-1)^{-1}p\cdot e_K=p\cdot e'$, we have

$$y=(1+c\cdot w')^p(1+c^p\cdot w)\equiv 1+p\cdot(c-c^p)\cdot w'+c^p\cdot(w+w'^p+p\cdot w') \mod (K^\times)^p.$$

Now we see that (7–14–1) ~ (7–14–4) are satisfied for

$$c'=c-c^p,\ \gamma=p\cdot w' \quad \text{and} \quad \gamma'=c^p(w+w'^p+p\cdot w').$$

Thus the proof of (7–14) is completed.

Remark (7–15). By a similar argument, we can show the following equal chracteristic version of Proposition (7–5). Let K be a complete discrete valuation field of characteristic $p>0$ and assume $\bar{K}$ is *separably closed*. Let k be a subfield of K such that

(7–15–1) k is complete with respect to the valuation induced from K,

(7–15–2) $\bar{k}$ is the maximal perfect subfield of $\bar{K}$.

(7–15–3) k is algebraically closed in K.

(Such a subfield k exists, but not necessarily uniquely). Let l be a totally ramified $\boldsymbol{Z}_p$-extension of k and let $L=lK$. Then for any finite (not necessarily separable) extension M/L such that l is algebraically closed in M, we have

$$[M: L]=[\bar{M}: \bar{L}]_{\text{insep}}.$$

References

[1] S. Bloch, Algebraic K-theory and classfield theory for arithmetic surfaces, Ann. of Math., **114** (1981), 229~265.

[2] H. P. Epp, Eliminating wild ramification, Invent. Math., **19** (1973) 235~249.

[3] A. Grothendieck, Modèle de Néron et monodromie, SGA 7I exp. IX, Lecture Notes in Math., **288**, Springer-Verlag, Berlin-Heidelberg-New York (1972).

[4] O. Hyodo, On the Hodge-Tate decomposition in the imperfect residue field case, Crellel's Journal, **365** (1986), 97~113.

[5] K. Kato, A generalization of local class field theory by using K-groups I, J. Fac. Sci. Univ. Tokyo, Sect. IA, **26** (1979), 303~376, II, ibid., **27** (1980), 603~683.

[6] K. Kato, Vanishing cycles, ramification of valuation and class field theory, to appear in Duke Math. J.

[7] K. Kato and S. Saito, Unramified class field theory of arithmetical surfaces, Ann. of Math., **118** (1983), 241~275.

[8] V. G. Lomadze, On the ramification theory of two-dimensional local fields, Math. USSR Sbornik, **37** (1980), 349~365.

[9] H. Miki, On cyclic extensions of p-power degree over complete p-adic fields (in Japanese), Master's thesis, Univ. of Tokyo (1973).
[10] H. Miki, On Z_p-extensions of complete p-adic power series fields and function fields, J. Fac. Sci. Univ. Tokyo, Sect. IA, **21** (1974), 377~393.
[11] M. Nagata, Local rings, Interscience Tracts, **13**, Interscience, New York-London (1962).
[12] A. N. Paršin, Abelian coverings of arithmetic schemes, Soviet Math. Dokl., **19** (1978), 1438~1442.
[13] M. Raynaud, Modèles de Néron, C. R. Acad. Sci. Paris, **262** (1966), 345~347.
[14] J.-P. Serre, Corps locaux, Hermann, Paris (1962).
[15] J. Tate, p-divisible groups, Proc. of a conf. on local fields, Springer, Berlin-Heidelberg-New York, (1967), 158~183.
[16] J. Tate, Relations between K_2 and Galois cohomology, Invent. Math., **36** (1976), 257~274.

Department of Mathematics
Faculty of Science
University of Tokyo
113 Hongo, Tokyo, Japan

Current address:
Department of Mathematics
Nara Women's University
630 Nara, Japan