J. Math. Soc. Japan
Vol. 29, No. 2, 1977

On unramified abelian extensions of a complete field under a discrete valuation with arbitrary residue field of characteristic $p \neq 0$ and its application to wildly ramified $\boldsymbol{Z}_p$-extensions

By Hiroo MIKI*)

(Received Dec. 5, 1974)
(Revised Sept. 30, 1975)

Introduction.

Let k be a complete field under a discrete valuation with residue field $\bar{k}$ of characteristic $p \neq 0$. In this paper we shall state a theory of unramified abelian extensions of k (see the main theorem below) and apply this result to fully ramified $\boldsymbol{Z}_p$-extensions of k (see §4, Theorem 4, Remarks 1 and 2).

The main result of this paper is as follows.

Fix a fully ramified cyclic extension k' of k of degree m, and for a finite unramified extension K of k, put

$$G^*(K) = N_{K'/K}(U_{K'}) \cap k / N_{k'/k}(U_{k'}),$$

where $K' = Kk'$ and U_k is the group of units of k. Put $W(k'/k) = \bigcup G^*(K)$, where the union is taken in $U_k / N_{k'/k}(U_{k'})$ over all finite unramified extensions K of k. Let $\mathcal{F}_m$ be the set of all finite abelian unramified extensions K of k such that $\sigma^m = 1$ for all $\sigma \in G(K/k)$, where $G(K/k)$ is the Galois group of K/k, and let $\widetilde{W}(k'/k)$ be the set of all finite subgroups of $W(k'/k)$. Then we have the following

MAIN THEOREM.(1) *Under the above assumptions, the following statements* (1) *and* (2) *are valid:*

(1) *If* $K \in \mathcal{F}_m$, *then* $G^*(K)$ *is canonically isomorphic to the character group of* $G(K/k)$.

(2) $\mathcal{F}_m$ *corresponds bijectively to* $\widetilde{W}(k'/k)$ *by* $K \mapsto G^*(K)$. *Moreover, we have* $G^*(K_1) \subset G^*(K_2)$ *if and only if* $K_1 \subset K_2$ *for* $K_1, K_2 \in \mathcal{F}_m$.

---

*) Partly supported by Fūjukai Foundation.

(1) We found this theorem to simplify the proof of [5], §6, Theorem and its Corollary 2, which is the original form of Theorem 4 in this paper. Our first motivation of [5] was to consider the problem of finding the class field theory of $\boldsymbol{Q}(t)_p$ (see Ihara [2]).

This theorem can be regarded as an analogue of the theory of Kummer extensions and Witt theory [10] and it contains both of them essentially. When $m\not\equiv 0 \pmod p$, this is equivalent to Kummer theory; when m is a power of p, it is equivalent to Witt theory [10] essentially. However, our formulation is more useful for our application. For $W(k'/k)$, see the Remarks at the end of § 3.

Table of Contents

Notations.

(1) (For a complete field k under a discrete valuation) ord_k: the normalized additive valuation of k. $\mathcal{O}_k$: the ring of integers of k. U_k: the group of units of k. $U_k^{(i)}=\{u\in U_k \mid \mathrm{ord}_k(u-1)\geqq i\}$ for $i\geqq 1$. $\bar{k}$: the residue field of k. $\bar{a}$ (for $a\in\mathcal{O}_k$): the image of a by the canonical homomorphism of $\mathcal{O}_k$ to $\bar{k}$.

(2) $\boldsymbol{Z}$: the ring of rational integers. $\boldsymbol{Z}_p$: the ring of p-adic integers. $\boldsymbol{Q}_p$: the field of p-adic numbers. $\boldsymbol{N}=\{z\in\boldsymbol{Z} \mid z\geqq 1\}$. $m|n$: m divides n for $m, n\in\boldsymbol{N}$.

(3) $K^\times$: the multiplicative group of a field K. $G(K/k)$: the Galois group of a Galois extension K/k. $\mathrm{Hom}(G_1, G_2)$: the group of homomorphisms of a group G_1 to an abelian group G_2. $N_{K/k}$: the norm map of K to k for a finite Galois extension K of k. $[G, G]$: the commutator group of a group G. $\langle u\rangle$ or $\langle u|u\in S\rangle$: the subgroup of a group G, generated by $u\in G$ or by a subset S of G respectively. $\sharp(S)$: the number of elements of a finite set S. $\mathrm{Ker}\,F$ (for a homomorphism F of a group G to a group G'): the kernel of F. $\mathrm{Im}\,F$: the image of F.

§ 1. Norm groups.

In this section we shall prove the following Theorem 1, which will be used for the proof of Theorem 2. When $\bar{k}$ is finite, Theorem 1 is well known (e. g. Artin-Tate [1], Chap. XI, § 4 and Iyanaga [3], Chap. V, § 2). However, its proof is not valid for arbitrary residue field $\bar{k}$. We use Sen [7], Lemma 1 and Serre [8], Chap. V.

THEOREM 1. *Let k be a complete field under a discrete valuation with residue field of characteristic $p\neq 0$ and let k' be a finite fully ramified cyclic extension of k. Then we have $N_{k'/k}(U_{k'}^{(j)})=N_{k'/k}(U_{k'}^{(1)})\cap U_k^{(i)}$ for each $i, j\in N$ such that $\psi(i-1)<j\leqq\psi(i)$, where ψ is the Hasse function of k'/k.*

We need also the following

LEMMA 1. *Let p and k be as in Theorem 1 and let k_n be a fully ramified cyclic extension of k of degree p^n. Let $t_1<t_2<\cdots<t_n$ be the sequence of all the ramification numbers of k_n/k and let ψ be the Hasse function of k_n/k. Put $S_1=\{N\in \boldsymbol{N} \mid N\neq\psi(m)$ for all $m\in\boldsymbol{N}$ and $N<t_n\}$ and $S_2=\{N\in\boldsymbol{N} \mid N=t_j+mp^{j-1}$ with $1\leqq j<n$, $m\not\equiv 0 \pmod p$, $m\in\boldsymbol{N}$ and $N<t_n\}$. Then $S_1=S_2$.*

PROOF. Let s_i be such that $\psi(s_i)=t_i$ for $i=1, 2, \cdots, n$ and let $t_0=s_0=0$. By Hasse-Arf's theorem, $s_i\in\boldsymbol{Z}$. Then we have easily $S_1=\{N\in\boldsymbol{N} \mid N\neq t_i+(m_i-s_i)p^i$ for $s_i\leqq m_i\ (\in\boldsymbol{Z})<s_{i+1}$ and $i=0, 1, \cdots, n-1\}$. Now let $N\in S_2$. Then $N=t_j+mp^{j-1}$ with $1\leqq j<n$, $m\not\equiv 0 \pmod p$ and $m\in\boldsymbol{N}$. Let $i\in\boldsymbol{N}$ be such that $t_i\leqq N<t_{i+1}$. Since $N>t_j$, we have $j\leqq i\leqq n-1$. If $N\notin S_1$, then $N=t_i+sp^i$ with $0\leqq s<s_{i+1}-s_i$ and $s\in\boldsymbol{Z}$. Since $t_i-t_j\equiv 0 \pmod{p^j}$ and $i\geqq j$, this implies that $mp^{j-1}\equiv 0 \pmod{p^j}$ hence $m\equiv 0 \pmod p$, which is a contradiction, hence $N\in S_1$. Hence $S_2\subset S_1$. Conversely let $N\in S_1$. If $N\notin S_2$, then $N=t_j+m_jp^j$ with $1\leqq j\leqq n-1$, $m_j\in\boldsymbol{Z}$ and $m_j\geqq 0$. Let j_0 be the maximum of such j, then we have easily $t_{j_0}\leqq N<t_{j_0+1}$. This implies that $N\notin S_1$, which is a contradiction, hence $N\in S_2$. Hence $S_1\subset S_2$. Therefore $S_1=S_2$.

LEMMA 2. *Let notations be as in Lemma 1 and let σ be a generator of $G(k_n/k)$. Let $N\in\boldsymbol{N}$ be such that $N\neq\psi(m)$ for all $m\in\boldsymbol{N}$ and $N<t_n$ and let $A\in k_n$ be such that $\mathrm{ord}_{k_n}(A)=N$. Then there exists $x\in U_{k_n}^{(1)}$ such that $x^{\sigma-1}\equiv 1+A \pmod{\pi_n^{N+1}}$, where π_n is a prime element of k_n.*

PROOF. By Lemma 1, $N=t_j+mp^{j-1}$ with $1\leqq$some $j<n$, some $m\not\equiv 0 \pmod p$ and $m\in N$. By Sen [7], Lemma 1, there exists $y\in k_n^{\times}$ such that $\mathrm{ord}_{k_n}(y)=mp^{j-1}$ and $\mathrm{ord}_{k_n}(y^{\sigma}-y)=N$. For $\lambda\in U_k$, put $z_\lambda=1+\lambda y$ and $B=y^{\sigma}-y$, then $z_\lambda^{\sigma}-z_\lambda=\lambda B$, hence $(z_\lambda)^{\sigma-1}\equiv 1+\lambda B \pmod{\pi_n^{N+1}}$. There exists $\lambda\in U_k$ such that $A\equiv\lambda B \pmod{\pi_n^{N+1}}$. For this $\lambda\in U_k$, put $x=z_\lambda$, then the assertion follows.

Now we can prove Theorem 1.

PROOF OF THEOREM 1. It is easily verified that it is enough to prove the theorem when $k'=k_n$, where k_n is as in Lemma 1. By Serre [8], Chap. V, § 6, Proposition 8, $N_{k_n/k}(U_{k_n}^{(j)})\subset N_{k_n/k}(U_{k_n}^{(1)})\cap U_k^{(i)}$. By Serre [8], Chap. V, § 6, Corollary 3, we may suppose $\psi(i)\leqq t_n$. Now conversely let $N_{k_n/k}(z)\in N_{k_n/k}(U_{k_n}^{(1)})\cap U_k^{(i)}$ with $z\in U_{k_n}^{(1)}$. Then by Lemma 2 and Serre [8], Chap. V, § 6, Proposition 9, there exists $z_1\in k_n^{\times}$ such that $z\cdot z_1^{\sigma-1}\in U_{k_n}^{(\psi(i))}$, hence $N_{k_n/k}(z)=N_{k_n/k}(z\cdot z_1^{\sigma-1})\in N_{k_n/k}(U_{k_n}^{(j)})$.

§ 2. Canonical isomorphism.

In this section we shall prove the following Theorem 2 and Corollaries to Theorem 2, which will be used for the proof of the main theorem. The statement (1) of the main theorem is an immediate consequence of Theorem 2 (see

Corollary 1 to Theorem 2).

THEOREM 2. *Let k be a complete field under a discrete valuation with residue field of characteristic $p\neq 0$ and let k'/k be a finite fully ramified cyclic extension. Let K/k be a finite unramified Galois extension and put $K'=Kk'$, $T_{K'}=\{y^{s-1}|y\in K'^{\times}\}$, $V_{K'}=\{y^{s-1}|y\in U_{K'}\}$, $G^*(K)=N_{K'/K}(U_{K'})\cap k/N_{k'/k}(U_{k'})$ and $G=G(K/k)$, where s is a generator of $G(K'/K)$. Then there exists a canonical isomorphism $F_K: G^*(K)\to\mathrm{Hom}(G, T_{K'}/V_{K'})$.*

2.1. Proof of Theorem 2.

For the proof of Theorem 2 we need Theorem 1 and the following two lemmas.

LEMMA 3. *Let k and K be two complete fields under a discrete valuation and let k'/k be a finite fully ramified cyclic extension. Suppose that K is an extension of k with ramification index 1. Put $K'=Kk'$. Let $T_{k'}$, $V_{k'}$, $T_{K'}$ and $V_{K'}$ be as in Theorem 2. Then the following* (1), (2), (3) *are valid:*

(1) (Serre [8], p. 104, Exercise.) *$G(k'/k)\simeq T_{k'}/V_{k'}$ by $\sigma\mapsto(\pi'^{(\sigma-1)} \bmod V_{k'})$, where π' is a prime element of k'.*

(2) *$T_{k'}/V_{k'}\simeq T_{K'}/V_{K'}$ by $(x \bmod V_{k'})\mapsto(x \bmod V_{K'})$, where $x\in T_{k'}$.*

(3) *$V_{K'}\cap T_{k'}=V_{k'}$.*

PROOF. Since π' is also a prime element of K', it follows from the statement (1) that $(\pi'^{(s-1)} \bmod V_{K'})$ generates $T_{K'}/V_{K'}$, where s is a generator of $G(K'/K)$. Therefore the given homomorphism in the statement (2) is surjective, hence bijective by (1). The statement (2) implies the statement (3).

LEMMA 4. *Let k, k', K, K', $V_{K'}$ and G be as in Theorem 2. Let $u\in U_k\cap N_{K'/K}(U_{K'})$ and $A\in U_{K'}$ be such that $N_{K'/K}(A)=u$. Suppose that $A^{\sigma-1}\in V_{K'}$ for all $\sigma\in G$,* identifying G and $G(K'/k')$. *Then $u\in N_{k'/k}(U_{k'})$.*

PROOF. Since $V_{K'}\subset U_{K'}^{(1)}$, we have $(\bar{A})^{\sigma}=\bar{A}$ for all $\sigma\in G$, hence $A=aA_1$ with $a\in U_{k'}$ and $A_1\in U_{K'}^{(1)}$, since K'/k' is unramified. Therefore we may suppose that $A\in U_{K'}^{(1)}$ from the beginning. Suppose that $u\in U_k^{(m)}$ with some $m\geqq 1$. By applying Theorem 1 to K'/K, we may suppose that $A\equiv 1+\lambda\pi'^{\psi(m)} \pmod{\pi'^{\psi(m)+1}}$, where π' is a prime element of k', ψ is the Hasse function of K'/K and $\lambda\in\mathcal{O}_{K'}$. Then $A^{\sigma-1}\equiv 1+(\lambda^{\sigma}-\lambda)\pi'^{\psi(m)} \pmod{\pi'^{\psi(m)+1}}$. Since $V_{K'}\cap U_{K'}^{(\psi(m))}\subset U_{K'}^{(\psi(m)+1)}$ (see Serre [7], p. 104, Ex. a)), we have $(\bar{\lambda})^{\sigma}=\bar{\lambda}$ for all $\sigma\in G$, hence we can take λ in $\mathcal{O}_k$. Put $B=(1-\lambda\pi'^{\psi(m)})A$. Then $B\in U_{K'}^{(\psi(m)+1)}$, $A^{\sigma-1}=B^{\sigma-1}\in V_{K'}$, and $N_{K'/K}(B)\in U_k^{(m+1)}$ by Serre [8], Chap. V, Proposition 8. Applying the above procedure to B, we have $u\in N_{k'/k}(U_{k'})$ by induction on m.

PROOF OF THEOREM 2. Identify G with the Galois group $G(K'/k')$. For $u\in N_{K'/K}(U_{K'})\cap k$ and $\sigma\in G$, put $f_u(\sigma)=A^{\sigma-1} \bmod V_{K'}$, where $A\in U_{K'}$ is such that $N_{K'/K}(A)=u$. It is easily verified that $f_u(\sigma)\in T_{K'}/V_{K'}$ and that $f_u(\sigma)$ is independent of the choice of A and that $f_u\in\mathrm{Hom}(G, T_{K'}/V_{K'})$. Put $F_K(u)=f_u$, then it is easily verified that F_K is a homomorphism of $N_{K'/K}(U_{K'})\cap k$ to

$\mathrm{Hom}(G, T_{K'}/V_{K'})$. By Lemma 4, $\mathrm{Ker}\, F_K = N_{k'/k}(U_{k'})$. Now we shall show that F_K is *surjective*. Let $\chi \in \mathrm{Hom}(G, T_{K'}/V_{K'})$. Let L' be the subfield of K' fixed by $\mathrm{Ker}\,\chi$ and put $L = L' \cap K$. Let $\sigma_1 \in G$ be such that $\chi(\sigma_1)$ generates $\mathrm{Im}\,\chi$. By (2) of Lemma 3, $\chi(\sigma_1) = x^{s-1} \bmod V_{K'}$ with some $x \in k'^{\times}$. If $d = [L' : k']$, then $\chi(\sigma_1)^d = 1$, hence $(x^d)^{s-1} \in V_{K'} \cap T_{k'}$, so $(x^d)^{s-1} = y^{s-1}$ with $y \in U_{k'}$, by (3) of Lemma 3. This implies that $x^d/y \in k$. Since k'/k is fully ramified, we can take y in $U_{k'}^{(1)}$. Since L'/k' is unramified, $y = N_{L'/k'}(z)$ with some $z \in U_{L'}^{(1)}$. Put $w = x/z$, then $N_{L'/k'}(w) = x^d/y \in k$ and $\chi(\sigma_1) = w^{s-1} \bmod V_{K'}$. Since $N_{L'/k'}(w^{s-1}) = (x^d/y)^{s-1} = 1$ and since L'/k' is cyclic, by Hilbert's theorem 90, $w^{s-1} = A^{(\sigma_1 - 1)}$ with $A \in L'^{\times}$. Since L'/k' is unramified, we may suppose that $A \in U_{L'}$. Since $N_{L'/L}(A)^{\sigma_1 - 1} = 1$, we have $N_{L'/L}(A) = u \in k$. Then $\chi(\sigma_1) = f_u(\sigma_1)$ and $\chi = f_u = 1$ on $\mathrm{Ker}\,\chi$. Since $\{\sigma_1, \mathrm{Ker}\,\chi\}$ generates G, we have $\chi = f_u$ on G. This completes the proof.

2.2. Corollaries to Theorem 2.

In this section we shall state the Corollaries to Theorem 2. The Corollary 1 is the statement (1) of the main theorem in the introduction. Corollaries 2 and 3 will be used for the proof of (2) of the main theorem.

COROLLARY 1. *Let notations and assumptions be as in Theorem 2. Put* $m = [k' : k]$. *Suppose moreover that* $\sigma^m = 1$ *for all* $\sigma \in G$. *Let* $\chi(G)$ *be the character group of* G. *Then* $G^*(K)$ *is isomorphic to* $\chi(G)$.

PROOF. Since $T_{K'}/V_{K'}$ is a cyclic group of order m by (1) of Lemma 3, by assumption $\mathrm{Hom}(G, T_{K'}/V_{K'}) \cong \chi(G)$. Hence the assertion follows from Theorem 2.

COROLLARY 2. *Let notations and assumptions be as in Theorem 2. Put* $m = [k' : k]$. *Let* L *be the maximal abelian extension of* k *in* K *such that* $\sigma^m = 1$ *for all* $\sigma \in G(L/k)$. *Then* $G^*(L) = G^*(K)$.

PROOF. It is trivial that $G^*(K) \supset G^*(L)$. Put $H = [G, G]\langle g^m | g \in G \rangle$, then L is the subfield of K fixed by H. It is clear that $\mathrm{Hom}(G, T_{K'}/V_{K'}) \cong \mathrm{Hom}(G/H, T_{K'}/V_{K'})$. Hence by Theorem 2, $\sharp(G^*(K)) = \sharp(G^*(L))$, so $G^*(K) = G^*(L)$.

COROLLARY 3. *Let* K_1, K_2 *be two finite unramified Galois extensions of* k *such that* $K_1 \supset K_2$, *and put* $G_1 = G(K_1/k)$. *Let* $G^*(K_i)$, $T_{K'_i}$ *and* $V_{K'_i}$ *be as in Theorem 2, where* $K'_i = K_i k'$, *and let* $F_{K_1} : G^*(K_1) \to \mathrm{Hom}(G_1, T_{K'_1}/V_{K'_1})$ *be the canonical isomorphism defined in Theorem 2. Put* $G(K_1/K_2)^{\perp} = \{f \in \mathrm{Hom}(G_1, T_{K_1}/V_{K_1}) \mid f = 1$ *on* $G(K_1/K_2)\}$. *Then* $F_{K_1}(G^*(K_2)) = G(K_1/K_2)^{\perp}$.

PROOF. By the definition of F_{K_1}, $F_{K_1}(G^*(K_2)) \subset G(K_1/K_2)^{\perp}$. Since $T_{K'_1}/V_{K'_1} \cong T_{K'_2}/V_{K'_2}$, by Theorem 2, $\sharp(F_{K_1}(G^*(K_2))) = \sharp(G(K_1/K_2)^{\perp})$. Therefore we have the assertion.

§ 3. Proof of the main theorem.

Noting the similarity of Theorem 2 to Kummer theory, we shall prove the statement (2) of the main theorem in the introduction. For the proof we use Theorem 2, Corollaries 1, 2 and 3 to Theorem 2 and the duality of finite abelian groups.

PROOF OF THE MAIN THEOREM. The statement (1) of the main theorem is already proved in Corollary 1 to Theorem 2. By Theorem 2, if $K \in \mathcal{F}_m$, then $G^*(K) \in \widetilde{W}(k'/k)$.

Existence: Let $M \in \widetilde{W}(k'/k)$. Then by the definition of $W(k'/k)$, $G^*(K_1) \supset M$ for some finite unramified extension K_1 of k. By taking the Galois closure of K_1 over k, we may suppose that K_1/k is a Galois extension. Moreover by Corollary 2 to Theorem 2, we may suppose that $K_1 \in \mathcal{F}_m$ from the beginning. Since $K_1 \in \mathcal{F}_m$, by Corollary 1 to Theorem 2, we can regard $\mathrm{Hom}(G(K_1/k), T_{K_1'}/V_{K_1'})$ as the character group of $G(K_1/k)$. Put $H^* = F_{K_1}(M)$, where F_{K_1} is the canonical isomorphism of $G^*(K_1)$ to $\mathrm{Hom}(G(K_1/k), T_{K_1'}/V_{K_1'})$, defined in Theorem 2. Let H be the subgroup of $G(K_1/k)$ corresponding to H^* by the duality of finite abelian groups. Then $H^* = \{f \in \mathrm{Hom}(G(K_1/k), T_{K_1'}/V_{K_1'}) \mid f = 1$ on $H\}$. Let K be the subfield of K_1 fixed by H, then $K \in \mathcal{F}_m$ and $F_{K_1}(M) = F_{K_1}(G^*(K))$ by Corollary 3 to Theorem 2, hence $M = G^*(K)$ by Theorem 2.

Uniqueness: Let $K_1, K_2 \in \mathcal{F}_m$ be such that $G^*(K_1) \supset G^*(K_2)$. Put $K = K_1K_2$, $G = G(K/k)$ and $G_i = G(K/K_i)$ for $i = 1, 2$. Let $F_K: G^*(K) \to \mathrm{Hom}(G, T_{K'}/V_{K'})$ be the canonical isomorphism defined by Theorem 2. By Corollary 3 to Theorem 2, $F_K(G^*(K_i)) = \{f \in \mathrm{Hom}(G, T_{K'}/V_{K'}) \mid f = 1$ on $G_i\}$ for $i = 1, 2$. Since $K \in \mathcal{F}_m$, by Corollary 1 to Theorem 2 $\mathrm{Hom}(G, T_{K'}/V_{K'})$ is isomorphic to the character group of G. Then by the duality of finite abelian groups, $G^*(K_1) \supset G^*(K_2)$ implies $G_1 \subseteqq G_2$, so $K_1 \supseteqq K_2$. In particular, $G^*(K_1) = G^*(K_2)$ implies $K_1 = K_2$.

REMARK 1. Let k be a complete field under a discrete valuation ν with arbitrary residue field $\bar{k}$ of characteristic $p \neq 0$ and assume that p is a prime element of k. Let k_0 be the subfield of k satisfying the conditions: (i) k_0 is complete with respect to the restriction of ν to k; (ii) the residue field $\bar{k}_0$ is the maximum perfect subfield of $\bar{k}$, i.e., $\bar{k}_0 = \bigcap_{n=1}^{\infty} (\bar{k})^{p^n}$. By MacLane [4], such a k_0 really exists. Let $k_n^{(0)}/k_0$ be a fully ramified cyclic extension of degree p^n and put $k_n = k_n^{(0)}k$. Then *it can be proved that* $W(k_n/k) = H_n(k)/N_{k_n/k}(U_{k_n})$, *where* $H_n(k) = \{x \in U_k \mid x \equiv \sum_{i=0}^{n} \lambda_i^{p^{n-i}} p^i \pmod{p^{n+1}}$ *with* $\lambda_i \in \mathcal{O}_k\}$.

REMARK 2. If $\bar{k}$ is perfect, then $W(k'/k) = U_k/N_{k'/k}(U_{k'})$. Hence the main theorem in the introduction gives an interpretation of a quotient group $U_k/N_{k'/k}(U_{k'})$; it can be regarded as the character group of the Galois group $G(K_m/k)$, where K_m is the composite field of all fields in $\mathcal{F}_m$.

§ 4. Application.

In this section, we shall apply the main theorem to fully ramified cyclic extensions and $\boldsymbol{Z}_p$-extensions of k.

LEMMA 5. *Let k be a complete field under a discrete valuation. Let k_1, k_2 be two finite fully ramified abelian extensions of k such that $k_1L=k_2L$ with an extension L/k of ramification index* 1 *(i.e., a prime element of k is a prime element of L). Suppose that $N_{k_1/k}(k_1)\cap N_{k_2/k}(k_2)$ contains a prime element of k. Then $k_1=k_2$.*

PROOF. We may suppose that k_i/k is cyclic and that L is a Galois extension of k, by taking the Galois closure of L over k. Since $k_1(k_1k_2\cap L)=k_2(k_1k_2\cap L)$, we may suppose $L\subset k_1k_2$. Put $Lk_1=Lk_2=L_1$ and let s be a generator of $G(L_1/L)$. By assumption, there exist prime elements π_i of k_i such that $N_{k_1/k}(\pi_1)=N_{k_2/k}(\pi_2)$. Put $u=\pi_2/\pi_1$, then $u\in U_{L_1}$ and $N_{L_1/L}(u)=1$. Hence $y^{s-1}=u$ with a $y\in L_1^{\times}$. Now suppose $k_1\neq k_2$. Then there exists $\sigma\in G(L_1/k_1)$ such that $\sigma|k_2\neq 1$. By the statement (1) of Lemma 3, $\pi_2^{\sigma-1}\notin V_{k_2}$, hence by the statement (3) of Lemma 3, $\pi_2^{\sigma-1}\notin V_{L_1}$. On the other hand, $\pi_2^{\sigma-1}=u^{\sigma-1}=(y^{\sigma-1})^{s-1}\in V_{L_1}$, which is a contradiction. Therefore $k_1=k_2$.

LEMMA 6. *Let k be as in Lemma* 5 *and let k_1, k_2 be two finite fully ramified Galois extensions of k such that $k_1L=k_2L$ with a finite unramified extension L/k. Then $N_{k_1/k}(U_{k_1})=N_{k_2/k}(U_{k_2})$.*

PROOF. By taking the Galois closure of L over k, we may suppose that L is a Galois extension of k. Put $L'=Lk_1=Lk_2$. Since L'/k_i is unramified, we we have $N_{L'/ki}(U_{L'}^{(1)})=U_{k_i}^{(1)}$, hence $N_{L'/k}(U_{k1}^{(1)})=N_{ki/k}(U_{k_i}^{(1)})$. Since k_i/k is fully ramified and $[k_1:k]=[k_2:k]$, we have the assertion.

THEOREM 3. *Let k, k' and $W(k'/k)$ be as in the main theorem in the introduction. Let $\mathfrak{F}=\mathfrak{F}(k')=\{k''\mid k''$ is a fully ramified cyclic extension of k such that $k'L=k''L$ with an unramified extension L of $k\}$. Let $F_{k'}:\mathfrak{F}\to W(k'/k)$ be a map defined by $k''\mapsto(N_{k'/k}(\pi')/N_{k''/k}(\pi'')$ mod $N_{k'/k}(U_{k'}))$, where π' and π'' are prime elements of k' and k'' respectively. Then $F_{k'}$ is bijective and independent of the choice of π' and π''.*

PROOF. By Lemma 6, $F_{k'}$ is independent of the choice of π' and π''.

$F_{k'}$ is injective: Let $k_i\in\mathfrak{F}$ with $i=1,2$. By assumption, $Lk_1=Lk_2=Lk'$ with an unramified extension L of k. Suppose that $F_{k'}(k_1)=F_{k'}(k_2)$. Then by the definition of $F_{k'}$ and by Lemma 6, $N_{k_1/k}(k_1)=N_{k_2/k}(k_2)$. Hence by Lemma 5, $k_1=k_2$. Hence $F_{k'}$ is injective.

$F_{k'}$ is surjective: Let $u\in W(k'/k)$ and let m' be the order of $\langle u\rangle$. Then $m'|m$. By the main theorem, there exists an unramified cyclic extension K/k of degree m' such that $G^*(K)=\langle u\rangle$. Put $K'=Kk'$. By Galois theory, there exist m' cyclic extensions $k_1,\cdots,k_{m'}$ of degree m such that $k'\neq k_i$ and $k_i\subset K'$

for $i=1, 2, \cdots, m'$. Clearly $F_{k'}(k_i)\in\langle u\rangle$. Since $F_{k'}$ is injective, $F_{k'}(k_i)=u$ with some i. Hence $F_{k'}$ is surjective. This completes the proof.

Now we apply Theorem 3 to $\boldsymbol{Z}_p$-extensions of k. Fix a fully ramified $\boldsymbol{Z}_p$-extension k_∞ of k, and let k_n/k be the sub-extension of k_∞/k of degree p^n. For $m\geqq n\geqq 1$, let $\rho_n^m: W(k_m/k)\to W(k_n/k)$ be a homomorphism defined by $x \bmod N_{k_m/k}(U_{k_m})\mapsto x \bmod N_{k_n/k}(U_{k_n})$ with $x\in N_{\hat{k}_m/\hat{k}_{ur}}(U_{\hat{k}_m})\cap k$, where $\hat{k}_{ur}$ is the completion of the maximum unramified extension of k and $\hat{k}_m=\hat{k}_{ur}k_m$. Then $\{W(k_n/k), \rho_n^m\}$ is a projective system. Let $W(k_\infty)$ be the projective limit of this system. Then we have directly the following Theorem 4 by Theorem 3.

THEOREM 4.(2) *Let k, p, k_∞ and $W(k_\infty)$ be as above. Let $\mathfrak{F}(k_\infty)=\{k'_\infty \mid k'_\infty$ is a fully ramified $\boldsymbol{Z}_p$-extension of k such that $k_\infty L=k'_\infty L$ with an unramified extension L of $k\}$. Let $F_\infty: \mathfrak{F}(k_\infty)\to W(k_\infty)$ be a map defined by $k'\mapsto\{N_{k'_n/k}(\pi'_n)/N_{k_n/k}(\pi_n) \bmod N_{k_n/k}(U_{k_n})\}$, where k'_n/k and k_n/k are the sub-extensions of k'_∞/k and k_∞/k of degree p^n respectively, and where π'_n and π_n are prime elements of k'_n and k_n respectively. Then F_∞ is independent of the choice of prime elements and F_∞ is bijective.*

REMARK 1. Suppose the conditions: (i) p is a prime element of k, (ii) the finite field $\boldsymbol{F}_p$ with p elements is the maximum perfect subfield of $\bar{k}$, i.e., $\boldsymbol{F}_p=\bigcap_{n=1}^{\infty}(\bar{k})^{p^n}$. As typical examples, we have k such that $\bar{k}=\boldsymbol{F}_p(t)$ (the rational function field over $\boldsymbol{F}_p$ in one variable t) or $\boldsymbol{F}_p\{t\}$ (the field of power series over $\boldsymbol{F}_p$ in one variable t). In this case, it is easily verified by [6], Theorem that *$\mathfrak{F}(k_\infty)$ is the set of all fully ramified $\boldsymbol{Z}_p$-extensions of k.*

REMARK 2. It can be proved that $W(k_\infty)=\varprojlim H_n(k)/N_{k_n/k}(U_{k_n})$ under the above conditions (i), (ii), where $H_n(k)$ is as in the Remark 1 in § 3 and the projective limit is taken with respect to a homomorphism induced by the natural injection of $H_{n'}(k)$ into $H_n(k)$ for $n'\geqq n$. Therefore under the above conditions (i), (ii), as a Corollary to Theorem 4, it can be proved that *$\bigcap_{n=1}^{\infty}N_{k'_n/k}(k'_n)$ contains a prime element of k if and only if there exists a $\boldsymbol{Z}_p$-extension k_c of $\boldsymbol{Q}_p$ such that $k'_\infty=k_ck$.*(3) Note that $W(k_\infty)=U_k^{(1)}$ if $k=\boldsymbol{Q}_p$ and that in this case Theorem 4 follows from local class field theory.

References

[1] E. Artin and J. Tate, Class field theory, Benjamin, New York, 1967.

[2] Y. Ihara, On a problem on some complete p-adic function fields (in Japanese), Kokyuroku of the Research Institute for Mathematical Sciences Kyoto Univ., **41** (1968), 7-17.

(2) This can be regarded as a generalization of [5], § 6, Corollary 2 to Theorem.

(3) This is [5], § 6, Corollary 3 to Theorem.

[3] S. Iyanaga (editors), Number theory (in Japanese), Iwanami Shoten, Tokyo, 1969=(in English), North-Holland, Amsterdam, 1975.

[4] S. MacLane, Subfields and automorphism groups of p-adic fields, Ann. of Math., **40** (1939), 424-442.

[5] H. Miki, On cyclic extensions of p-power degree over complete p-adic fields (in Japanese), Master's thesis, University of Tokyo, 1973.

[6] H. Miki, On $\boldsymbol{Z}_p$-extensions of complete p-adic power series fields and function fields, J. Fac. Sci. Univ. Tokyo Sec. IA, **21** (1974), 377-393.

[7] S. Sen, On automorphisms of local fields, Ann. of Math., **90** (1969), 33-46.

[8] J.P. Serre, Corps locaux (2nd edition), Hermann, Paris, 1968.

[9] O. Teichmüller, Diskret bewertete perfekte Körper mit unvollkommenem Restklassenkörper, J. Reine Angew. Math., **176** (1937), 141-152.

[10] E. Witt, Zyklische Körper und Algebren der Characteristik p von Grade p^n, J. Reine Angew. Math., **176** (1936), 126-140.

Hiroo MIKI
Department of Mathematics
University of Tokyo

Present address:
Department of Mathematics
Faculty of Engineering
Yokohama National University
Tokiwadai, Hodogaya-ku
Yokohama, Japan