J. Math. Soc. Japan
Vol. 28, No. 1, 1976

On some Galois cohomology groups of a local field and its application to the maximal p-extension

By Hiroo MIKI*)

(Received Feb. 27, 1975)

Introduction.

In this paper we shall prove that some Galois modules of a local field are cohomologically trivial, and as an application of this result we shall give another proof of Šafarevič-Marshall's theorem(1) (see below). This is a generalization of [7], § 8.

Now we formulate our result as follows.

Let k be a complete field of characteristic 0 under a discrete valuation with perfect residue field $\bar{k}$ of characteristic $p\neq 0$ and with absolute ramification order e_k, i.e., $e_k=\mathrm{ord}_k(p)$, where ord_k is the normalized additive valuation of k. Let $\mathfrak{F}_k(p)$ be the set of all finite Galois extensions of k of p-power degree contained in the fixed algebraic closure of k and let k_p be the maximal p-extension of k, i.e., the composite field of all fields belonging to $\mathfrak{F}_k(p)$. *Fix* a generator σ of the Galois group $G(k_p(\zeta)/k_p)$, where ζ is a primitive p-th root of unity, and let η be the unique element of $\boldsymbol{Z}_p^{\times}$ such that $\zeta^{\sigma}=\zeta^{\eta}$ and $\eta^N=1$, where $N=[k(\zeta):k]$. The group ring $\boldsymbol{Z}_p[G(k_p(\zeta)/k_p)]$ operates on $U^{(1)}_{K(\zeta)}$ for any $K\in\mathfrak{F}_k(p)$, hence on $U^{(1)}_{k_p(\zeta)}=\varinjlim U^{(1)}_{K(\zeta)}$ (the inductive limit is taken over all $K\in\mathfrak{F}_k(p)$) in the natural way (for the definition of $U^{(1)}_{k(\zeta)}$, see Notations).

DEFINITION. For each $K\in\mathfrak{F}_k(p)$, put

$$A(K)=\{x\in U^{(1)}_{K(\zeta)} \mid x^{\sigma-\eta}=1\}$$

and

$$A(k_p)=\{x\in U^{(1)}_{k_p(\zeta)} \mid x^{\sigma-\eta}=1\}\ .$$

Identifying $G(K/k)$ and $G(K(\zeta)/k(\zeta))$, $A(K)$ becomes $G(K/k)$-module and $A(k_p)$ becomes $G(k_p/k)$-module.

Under the above notations and assumptions we have the following:

---

*) Partly supported by Fūjukai Foundation.

(1) We obtained this independently of Marshall [5]. When I finished to write the manuscript, I knew in Reviews in Number theory Vol. 5 (edited by W. J. Leveque, A. M. S., 1974) that Marshall [5] had already obtained this result, and I rewrited this paper in this form.

MAIN THEOREM. *Let notations and assumptions be as above. Then the following two statements* (I), (II) *are valid:*

(I) *If* $\zeta \notin k$, *then* $H^1(G(K/k), A(K))=0$ *for any* $K \in \mathfrak{F}_k(p)$.

(II) *Moreover suppose that one of the following conditions* (i), (ii) *and* (iii) *is satisfied:*

(i) $e_k \not\equiv 0 \pmod{p-1}$.

(ii) k_1/k *is unramified of degree* >1 *and* $\{x \in \bar{k}_1 \mid x^q = \eta x\} \subset \mathfrak{p}\bar{k}_1$, *where* $k_1 = k(\zeta)$ *and* $\mathfrak{p}(x) = x^p - x$.

(iii) $k \ni \zeta$ *and any algebraic extension of* $\bar{k}$ *of degree* p *is cyclic. Then* $H^2(G(K/k), A(K))=0$ *for any* $K \in \mathfrak{F}_k(p)$.

COROLLARY. *Under the condition* (i), (ii) *or* (iii), $G(K/k)$*-module* $A(K)$ *is cohomologically trivial for any* $K \in \mathfrak{F}_k(p)$, *i.e.,* $H^i(H, A(K))=0$ *for all* $i \in \boldsymbol{Z}$ *and all subgroups* H *of* $G(K/k)$.

Note that the above condition (i) is equivalent to $e(k(\zeta)/k) > 1$, where $e(k(\zeta)/k)$ is the ramification index of $k(\zeta)/k$ (apply Serre [**13**], Corollary 2 to Proposition 6 to the completion of the maximal unramified extension of k; see also Lemma 4) and that the condition (iii) implies the condition (ii) if $e_k \equiv 0 \pmod{p-1}$ (it is easily verified by Lemma 2).

By using the above main theorem, we shall obtain another proof of the following:

Šafarevič-Marshall's theorem ([**10**], [**5**]). *Under the condition* (i), (ii) *or* (iii) *in the main theorem, the Galois group* $G_k(p)$ *of* k_p/k *is a free pro-p-group of rank* $[k : \boldsymbol{Q}_p] + \dim_{\boldsymbol{F}_p} \bar{k}/\mathfrak{p}\bar{k}$.

Conversely the statement (II) of the main theorem follows from the statement (I) of the main theorem and Šafarevič-Marshall's theorem (see Remark in § 4).

Table of Contents

Notations

(1) (For a complete field k of characteristic 0 under a discrete valuation) ord_k: the normalized additive valuation of k. $\mathcal{O}_k$: the ring of all integers of k. U_k: the group of all units of $\mathcal{O}_k$. $U_k^{(i)} = \{u \in U_k \mid \mathrm{ord}_k(u-1) \geqq i\}$ for $i \geqq 1$. $\bar{k}$: the residue field of k. e_k: the absolute ramification order of k, i.e., $e_k =$

$\mathrm{ord}_k(p)$, where $p\neq 0$ is the characteristic of $\bar{k}$. $\bar{a}$ (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 all rational integers. $\boldsymbol{Z}_p$: the ring of all p-adic integers. $\boldsymbol{Q}_p$: the field of p-adic numbers. $\boldsymbol{F}_p$: the finite field of p elements. (For a commutative ring R) $R^\times$: the multiplicative group of all units of R. $G(K/k)$: the Galois group of a Galois extension K of k. (For two fields k and K such that $k\subset K$) $[K:k]$: the dimension of K over k, regarding K as a vector space over k. (For a subset S of a group G) $\langle S\rangle$: the subgroup of G generated by S. (For a finite set S) $\sharp(S)$: the number of elements of S.

§ 1. Kummer and Artin-Schreier extensions.

In this section we shall state two lemmas verified easily by the theory of Kummer and Artin-Schreier extensions.

LEMMA 1. *Let p be a prime number and let k be a field of characteristic different from p. Let ζ be a primitive p-th root of unity and put $k'=k(\zeta)$. Let σ be a generator of $G(k'/k)$. Put $K'=k'(\sqrt[p]{x})$ with an $x\in k'$, $\notin (k')^p$. Then the following statements* (1) *and* (2) *are valid:*

(1) *K'/k is a Galois extension if and only if $x^{\sigma-m}\in(k')^p$ with some $m\in\boldsymbol{Z}$ such that $m\not\equiv 0 \pmod p$.*

(2) *K'/k is abelian if and only if $x^{\sigma-l}\in(k')^p$, where $l\in\boldsymbol{Z}$ is such that $\zeta^\sigma=\zeta^l$.*

LEMMA 2. *Let k be a field of characteristic $p\neq 0$ and let k' be a cyclic extension of k. Let σ be a generator of $G(k'/k)$. Put $\mathfrak{p}(x)=x^p-x$. For $x\in k'$ such that $x\notin\mathfrak{p}(k')$, put $K'=k'(y)$ where $y^p-y=x$. Then the following statements* (1) *and* (2) *are valid:*

(1) *K'/k is a Galois extension if and only if $(\sigma-m)x\in\mathfrak{p}(k')$ with some $m\in\boldsymbol{F}_p^\times$.*

(2) *K'/k is abelian if and only if $(\sigma-1)x\in\mathfrak{p}(k')$.*

§ 2. Proof of the main theorem.

In this section we shall give an elementary proof of the main theorem stated in the introduction.

For the proof of the main theorem we need some lemmas, and for the proof of these lemmas we use Serre [11], Chap. V, § 3.

LEMMA 3. *Notations and assumptions being as in the introduction, there exists $\Omega\in\boldsymbol{Z}_p[G(k_p(\zeta)/k_p)]$ satisfying the following properties:*

(1) $(U^{(1)}_{K(\zeta)})^\Omega=A(K)$ *for any* $K\in\mathfrak{T}_k(p)$.

(2) $x^\Omega=x$ *for any* $x\in A(k_p)$.

(3) $x^\Omega=1$ *for any* $x\in U^{(1)}_K$ *if* $\zeta\notin k$.

PROOF. Put $\Omega=N^{-1}\eta(\sigma^{N-1}+\sigma^{N-2}\eta+\cdots+\sigma\eta^{N-2}+\eta^{N-1})$. Since $N\in\boldsymbol{Z}_p^\times$, we have $\Omega\in\boldsymbol{Z}_p$ $[G(k_p(\zeta)/k_p)]$. Since $\Omega(\sigma-\eta)=0$, we have $(U^{(1)}_{K(\zeta)})^\Omega\subset A(K)$. Since $x^\sigma=x^\eta$ if $x\in A(K)$, we have $x^\Omega=x^{N^{-1}\eta\cdot\eta^{N-1}N}=x$. If $x\in U^{(1)}_K$ and $N\neq1$, then $x^\Omega=x^{N^{-1}\eta(1+\eta+\cdots+\eta^{N-1})}=1$, since $1+\eta+\cdots+\eta^{N-1}=0$. (q. e. d.)

LEMMA 4 ([7], Lemma 8). *Notations and assumptions being as in the beginning of the introduction, the ramification index of $k(\zeta)/k$ is $(p-1)/(e_k, p-1)$.*

LEMMA 5. *Let k be as in Lemma 4 and assume $\zeta\notin k$. Let Ω be as in Lemma 3. Let K/k be a fully ramified cyclic extension of p-power degree. Put*

$$T_K=\{x^{\tau-1}\mid x\in K(\zeta)^\times\}\quad\text{and}\quad V_K=\{x^{\tau-1}\mid x\in U^{(1)}_{K(\zeta)}\},$$

where τ is a generator of $G(K(\zeta)/k(\zeta))$. Then $T_K^\Omega\subset V_K^\Omega$.

PROOF. By Serre [11], Chap. V, § 7, Lemma 8, T_K/V_K is a cyclic group of order $[K:k]$ generated by $(\Pi^{\tau-1} \bmod V_K)$, where Π is a prime element of $K(\zeta)$. Since $[K(\zeta):K]\not\equiv0 \pmod p$, T_K/V_K is also generated by $(\pi_K^{\tau-1} \bmod V_K)$, where π_K is a prime element of K. This implies $T_K=\langle\pi_K^{\tau-1}\rangle V_K$. Since $\zeta\notin k$, by (3) of Lemma 3 $\langle\pi_K^{\tau-1}\rangle^\Omega=1$. Hence $T_K^\Omega\subset V_K^\Omega$. (q. e. d.)

LEMMA 6. *Let k be as in Lemma 4 and assume $\zeta\notin k$. Let K/k be a cyclic extension of degree p. Then $H^1(G(K/k), A(K))=0$.*

PROOF. By Serre [11], Chap. VIII, § 4, it is sufficient to prove that if $z\in A(K)$ satisfies $N_{K(\zeta)/k(\zeta)}(z)=1$, then $z\in A(K)^{\tau-1}$, where τ is a generator of $G(K/k)$. It suffices to prove it in the next two cases (1) and (2):

(1) The case where K/k is unramified. By Hilbert's theorem 90, there exists $y\in K(\zeta)^\times$ such that $y^{\tau-1}=z$. Since K/k is unramified, we can write $y=y_0y_1$ with a $y_0\in k(\zeta)^\times$ and a $y_1\in U_{K(\zeta)}$. Then $z=y_1^{\tau-1}$. Hence $1=(\bar{y}_1)^{\tau-1}$. This implies that $y_1=y_2y_3$ with a $y_2\in U_{k(\zeta)}$ and a $y_3\in U^{(1)}_{K(\zeta)}$. Then $z=y_3^{\tau-1}$. By making Ω operate on $z=y_3^{\tau-1}$ and using Lemma 3, $z\in A(K)^{\tau-1}$.

(2) The case where K/k is fully ramified. By Hilbert's theorem 90, $z\in T_K$, where T_K is as in Lemma 5. By making Ω operate on $z\in T_K$ and by using Lemmas 3 and 5, we have $z\in V_K^\Omega$. By Lemma 3, $V_K^\Omega=A(K)^{\tau-1}$, hence $z\in A(K)^{\tau-1}$. (q. e. d.)

LEMMA 7. *Assume that one of the conditions* (i), (ii) *and* (iii) *in the main theorem stated in the introduction is satisfied. Let K/k be as in Lemma 6. Then $H^2(G(K/k), A(K))=0$.*

PROOF. By Serre [11], Chap. VIII, § 4, it is enough to show that $N_{K(\zeta)/k(\zeta)}(A(K))\supset A(k)$. If K/k is unramified, then $N_{K(\zeta)/k(\zeta)}(U^{(1)}_{K(\zeta)})=U^{(1)}_{k(\zeta)}$, hence by making Ω operate on both members, $N_{K(\zeta)/k(\zeta)}(A(K))=A(k)$. Now suppose that K/k is fully ramified and that $K(\zeta)/k(\zeta)$ has the unique ramification number t. By Serre [11], Chap. V, § 3, Corollary 6 to Proposition 5, $U^{(1)}_{k(\zeta)}\subset N_{K(\zeta)/k(\zeta)}(U^{(1)}_{K(\zeta)})\cdot U^{(t)}_{k(\zeta)}$. By making Ω operate on both members and by using Lemmas 3 and 8, $A(k)\subset N_{K(\zeta)/k(\zeta)}(A(K))$. (q. e. d.)

LEMMA 8. *Let notations and assumptions be as in Lemma 7. Moreover suppose that K/k is fully ramified and let t be the unique ramification number of $K(\zeta)/k(\zeta)$. Then $(U^{(t)}_{k(\zeta)})^{\Omega}\subset N_{K(\zeta)/k(\zeta)}(A(K))$, where Ω is as in Lemma 3.*

PROOF. (1) The case where the condition (i) is satisfied. Let M be the maximum unramified extension of k in $k(\zeta)$ and put $s=[k(\zeta):M]$, then by Lemma 4, $s>1$. Let t' be the unique ramification number of K/k. By the transitivity of the Hasse function, $s\psi_{K/k}(n)=\psi_{K(\zeta)/k(\zeta)}(sn)$ for $n\in\boldsymbol{N}$, where $\psi_{K/k}$ is the Hasse function of K/k. This implies $t=st'$. Take $m\in\boldsymbol{Z}$ such that σ^m generates $G(k(\zeta)/M)$. Put $\Sigma=(\eta^m-1)^{-1}(\sigma^m-1)$, then $\Sigma\in\boldsymbol{Z}_p[G(k_p(\zeta)/k_p)]$, since $s>1$. It is clear that $x^{\Sigma}=x$ for all $x\in A(K)$ and that $(U^{(1)}_M)^{\Sigma}=1$. Since $U^{(t)}_{k(\zeta)}=U^{(t')}_M U^{(t+1)}_{k(\zeta)}$, we have $(U^{(t)}_{k(\zeta)})^{\Omega}=(U^{(t')}_M U^{(t+1)}_{k(\zeta)})^{\Omega}$, hence by making Σ operate on both members, $(U^{(t)}_{k(\zeta)})^{\Omega}=(U^{(t+1)}_{k(\zeta)})^{\Omega}$. By Serre [**11**], Chap. V, § 3, Corollary 3 to Proposition 5, $U^{(t+1)}_{k(\zeta)}\subset N_{K(\zeta)/k(\zeta)}(U^{(1)}_{K(\zeta)})$, hence by Lemma 3, $(U^{(t)}_{k(\zeta)})^{\Omega}=(U^{(t+1)}_{k(\zeta)})^{\Omega}\subset N_{K(\zeta)/k(\zeta)}(A(K))$.

(2) The case where the condition (ii) is satisfied. By Serre [**11**], Chap. V, § 3, Corollary 5 to Proposition 5, there exists $x\in K^{\times}$ and $y\in k^{\times}$ such that $\mathrm{ord}_K(x)=\mathrm{ord}_k(y)=t$ and $N_{K(\zeta)/k(\zeta)}(1+\mu x)\equiv 1+(\mu^p-\mu)y \pmod{\pi_k^{t+1}}$ for any $\mu\in\mathcal{O}_{k(\zeta)}$, where π_k is a prime element of k. Let $u\in(U^{(t)}_{k(\zeta)})^{\Omega}$ and write $u\equiv 1+\lambda y \pmod{\pi_k^{t+1}}$ with a $\lambda\in\mathcal{O}_{k(\zeta)}$. Then $\bar{\lambda}^{\sigma}=\bar{\eta}\bar{\lambda}$, hence by using the condition (ii), $(U^{(t)}_{k(\zeta)})^{\Omega}\subset N_{K(\zeta)/k(\zeta)}(U^{(t)}_{K(\zeta)})$. Making Ω operate on both members, by Lemma 3 we obtain the assertion. (q. e. d.)

LEMMA 9. *Let k be a field of characteristic $p\neq 0$ and let k' be a cyclic extension of k of degree N. Suppose $N\mid(p-1)$. Let σ be a generator of $G(k'_p/k_p)$ and let $\eta\in\boldsymbol{F}_p^{\times}$ be a primitive N-th root of unity, where k_p is the maximal p-extension of k and $k'_p=k_pk'$. For any extension K of k contained in k_p, put*

$$E(K)=\{\lambda\in K' \mid (\sigma-\eta)\lambda=0\},$$

where $K'=Kk'$. Suppose $E(k)\subset\mathfrak{p}(k')$, where $\mathfrak{p}(x)=x^p-x$ with $x\in K'$. Then $E(K)\subset\mathfrak{p}(K')$.

PROOF. First we shall show $E(k)\subset\mathfrak{p}(E(k))$. Put $\bar{\Omega}=\eta\bar{N}^{-1}(\sigma^{N-1}+\sigma^{N-2}\eta+\cdots+\sigma\eta^{N-2}+\eta^{N-1})$, where $\bar{N}=N \bmod p\in\boldsymbol{F}_p$. Since $\bar{N}\in\boldsymbol{F}_p^{\times}$, we have $\bar{\Omega}\in\boldsymbol{F}_p[G(k'_p/k_p)]$. Since $\bar{\Omega}(E(k))=E(k)$ and $\bar{\Omega}(k')\subset E(k)$ and since $\mathfrak{p}$ and $\bar{\Omega}$ are commutative, by making $\bar{\Omega}$ operate on $E(k)\subset\mathfrak{p}(k')$, we have $E(k)\subset\mathfrak{p}(E(k))$. It is sufficient to prove the assertion when K is of finite degree p^n over k by induction on n. First suppose that $n=1$. Since $K\subset k_p$ and since any maximal proper subgroup of a p-group is normal, K/k is cyclic, hence $K=k(y)$ with a $y\in K$ such that $y^p-y=x\in k$. Note that $E(K)$ is a vector space of dimension 1 over K and that $(E(K))^p\subset E(K)$, since $N\mid(p-1)$. Since $E(K)=E(k)+yE(k)+\cdots+y^{p-1}E(k)$, it is enough to prove that $y^iE(k)\subset\mathfrak{p}(K')$ for $i=0, 1, \cdots, p-1$. Suppose that $y^jE(k)\subset\mathfrak{p}(K')$ for $j=0, 1, \cdots, i-1$, and we shall show that $y^iE(k)\subset\mathfrak{p}(K')$. Let

$\lambda\in E(k)$, then $\lambda=\mu^p-\mu$ with a $\mu\in E(k)$. Since $(y^i\mu)^p-(y^i\mu)=(x+y)^i\mu^p-y^i\mu=y^i(\mu^p-\mu)+\sum_{j=0}^{i-1}y^jx^{i-j}\binom{i}{j}\mu^p$ and since $\sum_{j=0}^{i-1}y^jx^{i-j}\binom{i}{j}\mu^p\in\mathfrak{p}(K')$ by assumption, we have $y^i\lambda\in\mathfrak{p}(K')$, hence $y^iE(k)\subset\mathfrak{p}(K')$. Therefore by induction on i, $y^iE(k)\subset\mathfrak{p}(K')$ for $0\leqq$ all $i\leqq p-1$, hence $E(K)\subset\mathfrak{p}(K')$. Now suppose $n\geqq 2$. By an elementary property of p-groups and Galois theory, there exists a sub-extension M/k of degree p^{n-1} such that K/M is cyclic. By the induction hypothesis on n, $E(M)\subset\mathfrak{p}(M')$, where $M'=Mk'$. Hence by the case $n=1$, $E(K)\subset\mathfrak{p}(K')$. (q. e. d.)

COROLLARY. *Let k satisfy the condition* (ii) *in the main theorem stated in the introduction. Then for any finite sub-extension K/k of k_p/k, K satisfies the condition* (ii) *for K in the main theorem.*

Now we prove the main theorem stated in the introduction. For its proof, we use Lemmas 6 and 7, Corollary to Lemma 9 and a theorem of cohomology theory (cf. Serre [11], Chap. VII, § 6, Corollary to Proposition 5).

PROOF OF THE MAIN THEOREM. Put $G=G(K/k)$ and $\sharp(G)=p^n$. We shall prove the main theorem by induction on n. As is well known, there exists a normal subgroup H of G of order p, and let M be the fixed subfield of K by H. Then by Corollary to Lemma 9, M satisfies the condition (ii) for M if k satisfies the condition (ii), and it is trivial that M satisfies the condition (i) for M if k satisfies the condition (i) for k. Hence by Lemmas 6 and 7, $H^i(H, A(K))=0$ for $i=1, 2$. Therefore by a theorem of cohomology theory (cf. Serre [11], Chap. VII, § 6, Corollary to Proposition 5), $H^i(G(M/k), A(M))\cong H^i(G(K/k), A(K))$ for $i=1, 2$, hence by using the induction hypothesis, $H^i(G(K/k), A(K))=0$ for $i=1, 2$. By induction on n, we have the assertion. (q. e. d.)

PROOF OF COROLLARY TO THE MAIN THEOREM. It follows from the main theorem and Tate-Nakayama's theorem (cf. Serre [11], Chap. IX, § 5, Theorem 8).

§ 3. Maximal elementary p-extensions.

Marshall [5] has obtained the rank of the Galois group of the maximal elementary p-extension of k, i. e., of the composite field of all cyclic extensions of k of degree p, using Serre [13].

In this section we shall give an elementary proof of this result, using Kummer theory.

THEOREM ([6], Theorem 2). *Let k, p and e_k be as in the beginning of the introduction. Assume that k does not contain a primitive p-th root ζ of unity. Put $k'=k(\zeta)$ and let N be the ramification index of k'/k. Put $e_0=\mathrm{ord}_{k'}(\zeta-1)$ and*

$$V(e_k)=\left\{t\in\boldsymbol{Z}\mid 0\leqq t<\frac{e_kp}{p-1},\ t\not\equiv 0 \pmod p \text{ if } t\neq 0\right\}.$$

For any $t\in V(e_k)$, put $A_t=(\zeta-1)^p\pi^{-t}$, where π is a prime element of k. Then the following statements (1) *and* (2) *are valid:*

(1) *Let k_1/k be a cyclic extension of degree p. Then there exist $\lambda\in U_k$ and a unique $t\in V(e_k)$ such that $k_1(\zeta)=k'(\sqrt[p]{(1+\lambda A_t)\delta})$ with some $\delta\in U_{k'}^{(e_0p-Nt+1)}$. If $t\neq 0$, then $\boldsymbol{F}_p^{\times}\bar{\lambda}$ is uniquely determined. If $t=0$ (i.e., k_1/k is unramified), then we can take $\delta=0$ and $\bar{\lambda}\boldsymbol{F}_p$ is uniquely determined modulo $\mathfrak{p}(\bar{k})$. t is the unique ramification number of k_1/k.*

(2) *Let $\lambda\in U_k$ and let $t\in V(e_k)$. Then there exists a cyclic extension k_1/k of degree p such that $k_1(\zeta)=k'(\sqrt[p]{(1+\lambda A_t)\delta})$ with some $\delta\in U_{k'}^{(e_0p-Nt+1)}$. The extension k_1/k has the unique ramification number t.*

PROOF. It is easily verified by Lemma 1, Lemmas 2 and 9 of [7].

REMARK. (1) When $e_k=1$ (i.e., p is a prime element of k), the above Theorem follows from Ihara [3], Theorems 2 and 3 (see also [7], Proposition 8).

(2) In the case where $\zeta\in k$ and $\bar{k}$ is perfect, see Hecke [2]. For the case where $\zeta\in k$ and $\bar{k}$ is imperfect, see Epp [1], Proposition (1.4) and [6], Proposition 5.

(3) For the case where $\zeta\notin k$ and $\bar{k}$ is imperfect, see [6], Theorem 2.

COROLLARY (Marshall [5]). *Let notations and assumptions be as in Theorem. Let $k(p)$ be the composite field of all cyclic extensions of k of degree p. Put $G=G(k(p)/k)$ and regard G as a vector space over $\boldsymbol{F}_p$ in the natural way. Then $\dim_{\boldsymbol{F}_p}G=[k:\boldsymbol{Q}_p]+\dim_{\boldsymbol{F}_p}\bar{k}/\mathfrak{p}(\bar{k})$, where $\mathfrak{p}(x)=x^p-x$.*

PROOF. Let $S=\{\lambda_i\}_{i\in I}$ be the subset of U_k such that $\{\bar{\lambda}_i\}_{i\in I}$ is a basis of $\bar{k}$ over $\boldsymbol{F}_p$. Let $T=\{\mu_j\}_{j\in J}$ be the subset of U_k such that $\{\bar{\mu}_j \bmod \mathfrak{p}(\bar{k})\}_{j\in J}$ is a basis of $\bar{k}/\mathfrak{p}(\bar{k})$ over $\boldsymbol{F}_p$. By (2) of Theorem, there exists a fully ramified cyclic extension k_{t,λ_i} of k of degree p such that $k_{t,\lambda_i}(\zeta)=k'(\sqrt[p]{1+\lambda_iA_t+\cdots})$ for each $\lambda_i\in S$ and each $t\in V(e_k)$ such that $t\neq 0$, and there exists an unramified cyclic extension k_{μ_i} of k of degree p such that $k_{\mu_i}(\zeta)=k'(\sqrt[p]{1+\mu_iA_0})$ for each $\mu_j\in T$. Let L be the composite field of all k_{t,λ_i} and all k_{μ_i} for $t(\neq 0)\in V(e_k)$, $\lambda_i\in S$ and $\mu_j\in T$. Note that $\mathrm{ord}_{k'}(x^p-1)=mp$ or $\mathrm{ord}_{k'}(x^p-1)\geqq e_0p$ according as $1\leqq m<e_0$ or $m\geqq e_0$, where $x\in U_{k'}^{(1)}$ and $m=\mathrm{ord}_{k'}(x-1)$. Since $t\not\equiv 0 \pmod p$, from this fact and (1) of Theorem, it follows easily that any cyclic extension k_1 of k of degree p such that $k_1(\zeta)=k'(\sqrt[p]{y})$ with $y\in U_{k'}^{(1)}$ and $\mathrm{ord}_{k'}(y-1)>e_0p-Nt$ has the ramification number $t'<t$. From this, using (1) of Theorem and induction on t, we have $k(p)=L$. By Theorem and the definition of S and T, $\dim_{\boldsymbol{F}_p}G(L/k)=e_k[\bar{k}:\boldsymbol{F}_p]+\dim_{\boldsymbol{F}_p}\bar{k}/\mathfrak{p}(\bar{k})=[\bar{k}:\boldsymbol{Q}_p]+\dim_{\boldsymbol{F}_p}\bar{k}/\mathfrak{p}(\bar{k})$. (q. e. d.)

§ 4. Application of the main theorem (Another proof of Šafarevič-Marshall's theorem).

In this section we shall give another proof of Šafarevič-Marshall's theorem quoted in the introduction. We use the similar method as in the case where k is of characteristic $p\neq 0$ (cf. Serre [**12**], Chap. II, § 2, Proposition 3). For this purpose, we need the following:

LEMMA 10. *Let $A(k_p)$ be as in the introduction and let f be the endomorphism of $A(k_p)$ defined by $f(x)=x^p$. Then f is surjective.*

PROOF. Let $x\in A(k_p)$. Now suppose that $x\notin(k_p(\zeta))^p$, then by the definition of $A(k_p)$ and Lemma 1, $k_p(\zeta)(\sqrt[p]{x})$ is a cyclic extension of k_p of degree $p\cdot[k(\zeta):k]$. Hence by Galois theory, there exists a cyclic extension K of k_p of degree p such that $K(\zeta)=k_p(\zeta)(\sqrt[p]{x})$. But this contradicts the maximality of k_p, hence $x\in(k_p(\zeta))^p$. Since $x\in U^{(1)}_{k_p(\zeta)}$, we have $x\in(U^{(1)}_{k_p(\zeta)})^p$, hence by making Ω operate on both members and using Lemma 3, we have $x\in(A(k_p))^p$. (q. e. d.)

ANOTHER PROOF OF ŠAFAREVIČ-MARSHALL'S THEOREM. Let W be the subgroup of $k(\zeta)^\times$ generated by ζ. By Lemma 10, the sequence

$$1\longrightarrow W\xrightarrow{\iota} A(k_p)\xrightarrow{f} A(k_p)\longrightarrow 1$$

is exact, where ι is the natural injection of W into $A(k_p)$ and f is as in Lemma 10. Then we obtain the exact sequence

$$H^1(G_k(p),\ A(k_p))\longrightarrow H^2(G_k(p),\ W)\longrightarrow H^2(G_k(p),\ A(k_p))\,.$$

By the main theorem stated in the introduction,

$$H^i(G_k(p),\ A(k_p))=0\qquad \text{for } i=1,\ 2\,.$$

Therefore $H^2(G_k(p),\ W)=0$. By Serre [**12**], Chap. I, § 4, Proposition 21 and Corollary 2 to Proposition 24, $G_k(p)$ is a free pro-p-group. By Corollary to Theorem 1, $G_k(p)$ is of rank $[k:\boldsymbol{Q}_p]+\dim_{\boldsymbol{F}_p}\bar{k}/\mathfrak{p}(\bar{k})$. (q. e. d.)

REMARK. Conversely the statement (II) of the main theorem follows from the statement (I) of the main theorem and Šafarevič-Marshall's theorem quoted in the introduction. It is shown as follows. From the exact sequence stated in the above proof, we obtain the exact sequence: $H^2(G_k(p),\ W)\to H^2(G_k(p),\ A(k_p))\to H^3(G_k(p),\ W)$. By Šafarevič-Marshall's theorem, $G_k(p)$ is a free pro-p-group, hence $H^i(G_k(p),\ W)=0$ for any $i\geqq 2$. Hence $H^2(G_k(p),\ A(k_p))=0$. Put $H=G(k_p/K)$. By the statement (I) of the main theorem, $H^1(H,\ A(k_p))=0$. Hence by the general theory of cohomology groups,

$$\mathrm{Inf}: H^2(G(K/k), A(K)) \longrightarrow H^2(G_k(\mathfrak{p}), A(k_p))$$

is injective. Therefore $H^2(G(K/k), A(K))=0$.

References

[1] H. P. Epp, Eliminating wild ramification, Invent. Math., 19 (1973), 235-246.
[2] E. Hecke, Vorlesungen über die Theorie der algebraischen Zahlen, Chelsea, New York, 1948.
[3] 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.
[4] Y. Kawada, On the structure of the Galois group of some infinite extensions, I, J. Fac. Sci. Univ. Tokyo Sec. IA, 7 (1954), 1-18.
[5] M. A. Marshall, The maximal p-extension of a local field, Canad. J. Math., 23 (1971), 398-402.
[6] H. Miki, On cyclic extensions of p-adic complete fields of p-power degree (in Japanese), Master's thesis, 1973, Univ. Tokyo.
[7] 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.
[8] H. Miki, On unramified abelian extensions of local fields with arbitrary residue field of characteristic $p\neq 0$ and its application to wildly ramified $\boldsymbol{Z}_p$-extensions.
[9] H. Miki, A note on Maus' theorem on ramification groups, to appear in Tōhoku Math. J.
[10] I. R. Šafarevič, On p-extensions, Math. Sbornik 20 (1950), 113-146, Amer. Math. Soc. Transl. Ser. 2 Vol. 4, 59-72.
[11] J. P. Serre, Corps locaux (2nd edition), Hermann, Paris, 1968.
[12] J. P. Serre, Cohomologie Galoisienne, Lecture notes in Math. 5, 3rd edition, Springer, Berlin, 1965.
[13] J. P. Serre, Sur les corps locaux à corps résiduel algébriquement clos, Bull. Soc. Math. France, 89 (1961), 105-154.

Hiroo MIKI
Department of Mathematics
Faculty of Science
University of Tokyo
Hongo, Bunkyo-ku
Tokyo, 113 Japan