S. HAMADA
KODAI MATH. J.
3 (1980), 415—428

ON THE CONDUCTORS OF p-CYCLIC KUMMER EXTENSIONS OF LOCAL NUMBER FIELDS

BY SUGURU HAMADA

Introduction. Let p be a prime number, $\mathbf{Q}_p$ be the rational p-adic number field, and K be a finite extension over $\mathbf{Q}_p$ containing a primitive p^n-th root of unity.

An explicit formula of the norm residue symbol for the elements of K is known (H. Hasse [3], M. Kneser [4], and I. R. Šafarevič [5]).

In this paper, using the explicit formula we describe the conductor of Kummer extension $K(\sqrt[p^n]{A})/K$ in some cases by means of the "exponents" of A in its Šafarevič's representation (Theorem 1 and 2).

When $n=1$ the result is found in H. Hasse [1] (Remark 2). In §1, for convenience, we write down the outline of the Šafarevič's representation of the elements of K and the explicit formula, following H. Hasse [3] and M. Kneser [4]. In §2, we give our theorems, in §3 we prove our theorems, and in §4 we give some remarks and examples.

§1. Notations.

$\mathbf{Z}$: the ring of rational integers. p: a prime number. $\mathbf{Q}_p$: the rational p-adic number field. $\mathbf{Z}_p$: the ring of integral elements of $\boldsymbol{Q}_p$. ζ_n: a primitive p^n-th root of unity. K: a finite extension of $\mathbf{Q}_p$, containing ζ_n. $K^\times$: the multiplicative group of non-zero elements of K. $\mathfrak{p}$: the maximal ideal of K. π: a prime element of K. H_m: the multiplicative group $1+\mathfrak{p}^m$ ($m=1, 2, \cdots$). $\mathrm{ord}^\times$: for a principal unit η of K we write $\mathrm{ord}^\times(\eta)=m$ if and only if $\eta\in H_m$ and $\eta\notin H_{m+1}$.

$\underset{p^m}{\sim}$: for elements A, B of $K^\times$ we write $A\underset{p^m}{\sim}B$ if and only if $A\in BK^{\times p^m}$.
Ω: the group of p^n-primary numbers of K. T: the inertia field of $K/\mathbf{Q}_p$. I: the ring of integral elements of T. R: the multiplicative representatives of the residue class field of K, $R\subset I$. $R^\times$: $R^\times=R-\{0\}$. ord: the p-adic order function on T. S_p: the trace mapping from T to $\mathbf{Q}_p$.

$\bar{T}$: the completion of the maximal unramified extension of $\boldsymbol{Q}_p$. $\bar{I}$: the ring of integral elements of $\bar{T}$. $\bar{R}$: the multiplicative representatives of the residue class field of $\bar{T}$, $\bar{R}\subset\bar{I}$. P: the Frobenius automorphism of the extension $T/\boldsymbol{Q}_p$. $\mathfrak{P}$: the additive endomorphism of $\bar{I}$ defined by $\mathfrak{P}(\bar{\alpha})=\bar{\alpha}^P-\bar{\alpha}$ ($\bar{\alpha}\in\bar{I}$). e: the

Received September 18, 1979

ramification index of the extension $K/\mathbf{Q}_p$. e_m: the ramification index of the extension $K/T(\zeta_m)$, where $\zeta_m=\zeta_n^{p^{n-m}}$ $(1\leqq m\leqq n)$. We have $e_1+e=e_1p$, $e_1=e_mp^{m-1}$.

$$F: F=\{i\,|\,1\leqq i<e_1p,\ (i,\ p)=1\}\ .$$

π_n, π_1: $\pi_n=1-\zeta_n$, $\pi_1=1-\zeta_1$. We have

$$\pi_n^{p^n}\equiv-\pi_n^{p^{n-1}}p\equiv\pi_1^p=-\pi_1p \qquad \mathrm{mod}\ \mathfrak{p}^{e_1p+1}\ .$$

e_0, κ, ε_0, ε: $e_1=e_0p^{\kappa-1}$ where $(e_0,\ p)=1$ $(\kappa\geqq n)$,

$$\pi^{e_1p}\equiv\varepsilon_0^{p^\kappa}\pi_1^p \qquad \mathrm{mod}\ \mathfrak{p}^{e_1p+1}\ (\varepsilon_0\in R^\times)$$

and

$$-p\equiv\varepsilon\pi^e \qquad \mathrm{mod}\ \mathfrak{p}^{e+1}\ (\varepsilon\in R^\times)\ .$$

Now, for convenience, we write down the outline of Šafarevič's representation of elements of K following H. Hasse [3]. Generally, if a system $S=\{\eta_k(\gamma)\,|\,\gamma\in R,\ k=1,\ 2,\ \cdots\}$ is given so that $\eta_k(\gamma)\equiv1-\gamma\pi^k$ mod $\mathfrak{p}^{k+1}$, then every element $\eta\in H_1$ is written uniquely as follows:

(1) $$\eta=\prod_{k=1}^{\infty}\eta_k(\gamma)\ , \qquad \eta_k(\gamma)\in S\ .$$

Such a system S is given by Šafarevič's E-function and E^*-function. The definitions and some properties of these functions are as follows. We define:

$$E(\alpha,\ x)=\prod_{\substack{m=1\\(m,\,p)=1}}^{\infty}(1-\alpha^mx^m)^{\mu(m)/m}\ , \qquad \text{where}\quad \alpha\in R,\ x\in\mathfrak{p}$$

and μ is the Möbius function.

$$E(\alpha,\ x)=\sum_{\nu=0}^{\infty}E(\alpha_\nu,\ x)^p\ , \qquad \text{where}\ \alpha=\sum\alpha_\nu p^\nu\in I\ (\alpha_\nu\in R)\ .$$

Then

(2) $$E(\alpha,\ x)\equiv1-\alpha x \bmod x^2$$

and $$E(\alpha+\beta,\ x)=E(\alpha,\ x)\cdot E(\beta,\ x)$$

$$E(a\alpha,\ x)=E(\alpha,\ x)^a \qquad \text{where}\quad \alpha,\ \beta\in I\quad \text{and}\quad a\in\mathbf{Z}_p$$

Next, for $\alpha\in I$ we define

$$E^*(\alpha)=E(p^n\bar{\alpha},\ \tilde{\pi}_n)=E(\bar{\alpha},\ \tilde{\pi}_n)^{p^n}$$

where $\mathfrak{P}(\bar{\alpha})=\alpha$ $(\bar{\alpha}\in I)$, $\zeta_n=E(1,\ \tilde{\pi}_n)$ and $E(\bar{\alpha},\ \tilde{\pi}_n)$ is defined by the same formula as before. Then

(3) $$E^*(\alpha)\equiv1-\alpha^{p^{n-1}}\pi_1^p \qquad \mathrm{mod}\ \mathfrak{p}^{e_1p+1}\ (\alpha\in R)\quad \text{and}$$

$$E^*(\alpha+\beta)=E^*(\alpha)E^*(\beta)$$

$$E^*(a\alpha)=E^*(\alpha)^a \quad \text{where} \quad \alpha, \beta\in I \quad \text{and} \quad a\in \mathbf{Z}_p .$$

Moreover, $\{E^*(\alpha)\,|\,\alpha\in I\}\cdot K^{\times p^n}=\Omega$.

The following congruences are well known (H. Hasse [2]). For an integral element α of K, let $\eta\equiv 1-\alpha\pi^i \bmod \mathfrak{p}^{i+1}$ then

(4) $$\eta^p\equiv\begin{cases} 1-\alpha^p\pi^{ip} & \bmod \mathfrak{p}^{ip+1} \quad \text{if} \quad i<e_1 \\ 1-(\alpha^p-\varepsilon\alpha)\pi^{e_1p} & \bmod \mathfrak{p}^{e_1p+1} \quad \text{if} \quad i=e_1 \\ 1-\alpha p\pi^i & \bmod \mathfrak{p}^{i+e+1} \quad \text{if} \quad i>e_1 . \end{cases}$$

Now, as in Notations, let $F=\{i\,|\,1\leqq i<e_1p,\ (i,\ p)=1\}$ then the e integers k $(e_1<k\leqq e_1p)$ are written uniquely

$$k=ip^{\kappa_i} \ (i\in F,\ \kappa_i\geqq 0,\ \kappa_{e_0}=\kappa)$$

and every positive integer k is written uniquely as follows:

$$\text{if} \quad k\leqq e_1 \quad \text{then} \quad k=ip^{\nu_i} \ (i\in F,\ 0\leqq\nu_i<\kappa_i)$$

$$\text{if} \quad k>e_1 \quad \text{then} \quad k=ip^{\kappa_i}+\nu_i'e \ (i\in F,\ \nu_i'\geqq 0) .$$

From (2) and (4) we have

(5) $$E(\alpha p^{\nu_i},\ \pi^i)=E(\alpha,\ \pi^i)^{p^{\nu_i}}\equiv(1-\alpha\pi^i)^{p^{\nu_i}}$$

$$\equiv 1-\alpha^{p^{\nu_i}}\pi^k \qquad \bmod \mathfrak{p}^{k+1}$$

$(\alpha\in R,\ 1\leqq k\leqq e_1,\ k=ip^{\nu_i})$.

The above congruences hold also for $\nu_i=\kappa_i$ if $i\neq e_0$ (i. e. $e_1<k<e_1p$, $k=ip^{\kappa_i}$). And

(6) $$E(\alpha p^{\kappa_i+\nu_i'},\ \pi^i)\equiv 1-\alpha^{p^{\kappa_i}}p^{\nu_i'}\pi^{ip^{\kappa_i}} \qquad \bmod \mathfrak{p}^{k+1} .$$

$(\alpha\in R,\ e_1p<k,\ k=ip^{\kappa_i}+\nu_i'e\ (i\neq e_0),\ \nu_i'>0)$. For the exceptional $k=e_1p+\nu'e$ $(\nu'\geqq 0)$ corresponding to $i=e_0$, we have from (3) and (4)

(7) $$E^*(\alpha p^{\nu'})=E^*(\alpha)^{p^{\nu'}}\equiv(1-\alpha^{p^{n-1}}\pi_1^p)^{p^{\nu'}}\equiv 1-\alpha^{p^{n-1}}p^{\nu'}\pi_1^p$$

$\bmod \mathfrak{p}^{k+1}$ $(\alpha\in R)$.

Since $R^{p^m}=R$ $(m\geqq 1)$, a desired system S has been given and from (1) every $\eta\in H_1$ is represented by E-function and E^*-function. Consequently every element $A\in K^\times$ is represented uniquely as follows:

(Š) $$A=\pi^a\rho\prod_{i\in F}E(\alpha_i,\ \pi^i)E^*(\alpha) \ (a\in\mathbf{Z},\ \rho\in R^\times,\ \alpha_i,\ \alpha\in I\ \ \alpha_{e_0}:\ \text{mod}\ p^\kappa \text{ reduced.})$$

Now, for every m $(1\leqq m\leqq n)$, we have

(8) $$\pi^a\rho\prod_{i\in F}E(\alpha_i,\ \pi^i)E^*(\alpha)\underset{p^m}{\sim}\pi^{a'}\rho'\prod_{i\in F}E(\alpha'_i,\ \pi^i)E(\alpha')$$

if and only if $a\equiv a'$ mod p^m, $\alpha_i\equiv\alpha'_i$ mod p^m $(i\in F)$, and $\alpha\equiv\alpha'$ mod p^m, $\mathfrak{P}$ where the last congruence means that there exist δ, $\theta\in I$ such that $\alpha-\alpha'=p^m\delta+\mathfrak{P}(\theta)$.

In the following we write $\prod_i$ instead of $\prod_{i\in F}$ and $\sim$ instead of $\underset{p^n}{\sim}$.

[EXPLICIT FORMULA] (H. Hasse [3], M. Kneser [4] and I. R. Šafarevič [5]) *Let* A, B *be two elements of* $K^\times$ *such that*

$$A\sim\pi^a\prod_i\mathrm{E}(\alpha_i,\ \pi^i)\mathrm{E}^*(\alpha),\qquad B\sim\pi^b\prod_j\mathrm{E}(\beta_j,\ \pi^j)\mathrm{E}^*(\beta)$$

then the norm residue symbol $(A,\ B)$ *is given by*

(9) *If* $p\neq2$ $(A,\ B)=\zeta_n^{\mathrm{Sp}(a\beta-b\alpha+\gamma)}$

where $\prod_{i,j\in F}\mathrm{E}(j\alpha_i\beta_j,\ \pi^{i+j})\sim\prod_k\mathrm{E}(\gamma_k,\ \pi^k)\mathrm{E}^*(\gamma)$.

(10) *If* $p=2$ $(A,\ B)=\zeta_n^{\mathrm{Sp}(a\beta-b\alpha+\gamma)}$

where

$$(-1)^{ab}\prod_{i,j\in F}^{\infty}\Big[\mathrm{E}(j\alpha_i\beta_j,\ \pi^{i+j})\prod_{\mu,\nu\geqq1}^{\infty}\mathrm{E}((i2^{\mu-1}+j2^{\nu-1})\alpha_i^{P^\mu}\beta_j^{P^\nu},\ \pi^{2^\mu i+2^\nu j})\Big]$$
$$\sim\prod_k\mathrm{E}\gamma_k,\ \pi^k)\mathrm{E}^*(\gamma).$$

§2. Theorems.

We write also $\pi^a\prod_iE(\alpha_i,\ \pi^i)E^*(\alpha)=\langle\alpha_0,\ \alpha_1,\ \cdots,\ \alpha\rangle$ where $\alpha_0=a$.

The aim of this paper is to describe, in some cases, the conductor $\mathfrak{p}^f$ of the extension $K(\sqrt[p^n]{A})/K$ by means of conditions on α_0, α_i $(i\in F)$.

From the facts in §1, the extension $K(\sqrt[p^n]{A})/K$ is unramified if and only if $\alpha_i\equiv0$ mod p^n for all $i\in F$ and $i=0$.

Thus we consider only the case when for some r $(1\leqq r\leqq n)$ there exists i $(i=0$ or $i\in F)$ such that $\alpha_i\not\equiv0$ mod p^r. And we denote i_r the least suffix i for which $\alpha_i\not\equiv0$ mod p^r. If i_r exists then $i_{r+1},\ \cdots,\ i_n$ exist and

$$e_1p-1\geqq i_r\geqq\cdots\geqq i_{n-1}\geqq i_n\geqq0.$$

When i_r exists we set $f_r=e_1p+(n-r)e-i_r+1$.

Moreover, for convenience, we set $i_{n+1}=i_n$ and $f_{n+1}=e_1p-e-i_{n+1}+1$. Then $f_n>f_{n+1}$ holds. This definition is natural in the following sense; if i_{n+1} is the least suffix i for which $\alpha_i\not\equiv0$ mod p^{n+1}, we have $i_{n+1}\leqq i_n$; here if $i_{n+1}<i_n$ we can take $B=\langle0,\ \cdots,\ \overset{i_{n+1}}{\check{0}},\ \cdots,\ \alpha_{i_n},\ \cdots\rangle$ instead of A; for this B we have $i_{n+1}=i_n$.

Now, it follows from §1 that the extension $K(\sqrt[p^n]{A})/K$ is a totally ramified extension of degree p^n if and only if i_1 exists.

THEOREM 1. *The extension* $K(\sqrt[p^n]{A})/K$ *is a totally ramified extension of degree* p^n *if and only if there exists* i ($i=0$ *or* $i\in F$) *such that* $\alpha_i\not\equiv 0 \bmod p$. *And, then*

$$f\leqq \text{Max}\{f_1, f_2\}$$

where $\mathfrak{p}^f$ *is the conductor of the extension* $K(\sqrt[p^n]{A})/K$.

Moreover, $f=\text{Max}\{f_1, f_2\}$ *holds if and only if* $e+i_2\neq i_1$ (*i.e.* $f_2\neq f_1$) *or* $\alpha_{i_2}\varepsilon\not\equiv\alpha_{i_1}p \bmod p^2$, *where* $-p\equiv\varepsilon\pi^e \bmod \mathfrak{p}^{e+1}$ ($\varepsilon\in R^{\times}$).

Remark. By the above remark, in the case $n=1$, our Theorem asserts that $f=f_1$. Moreover, for $n\geqq 2$, $e+i_1=i_2$ and $\alpha_{i_2}\varepsilon\equiv\alpha_{i_1}p \bmod p^2$ occures in these cases when $p\neq 2$ or $p=2$ and $T\supsetneqq \boldsymbol{Q}_2$. For example, in these cases, let $1\leqq i_2<e_1$, $e+i_2=i_1$ and $A\sim E(\gamma p, \pi^{i_2})E(1, \pi^{i_1})$ where $\gamma\varepsilon=1$ ($\gamma\in R^{\times}$).

Now, THEOREM 1 can be generalized easily to the case when $K(\sqrt[p^n]{A})/K$ contains an unramified subfield:

THEOREM 2. *For integer* m ($1\leqq m\leqq n$), *if* $\alpha_i\equiv 0 \bmod p^{m-1}$ *for all* $i\in F$ *and* $i=0$ *and there exists some* i ($i\in F$ *or* $i=0$) *such that* $\alpha_i\not\equiv 0 \bmod p^m$, *then*

$$f\leqq \text{Max}\{f_m, f_{m+1}\}$$

where $\mathfrak{p}^f$ *is the conductor of the extension* $K(\sqrt[p^n]{A})/K$. *Moreover,* $f=\text{Max}\{f_m, f_{m+1}\}$ *holds if and only if* $e+i_{m+1}\neq i_m$ (*i.e.* $f_{m+1}\neq f_m$) *or* $\alpha_{i_{m+1}}\varepsilon\not\equiv\alpha_{i_m}p \bmod p^{m+1}$, *where* $-p\equiv\varepsilon\pi^e \bmod \mathfrak{p}^{e+1}$ ($\varepsilon\in R^{\times}$).

Remark. In the case $m=n$, our Theorem asserts that $f=f_n$. In fact, Theorem 2 is proved by Theorem 1 as follows: By assumption,

$$\alpha_0=\alpha_0' p^{m-1} \quad \text{and} \quad \alpha_i=\alpha_i' p^{m-1}\ (i\in F) \quad \text{for some} \quad \alpha_0'\in\boldsymbol{Z} \quad \text{and} \quad \alpha_i'\in I.$$

So we have $A\underset{p^{m-1}}{\sim}E^*(\alpha)$ and $L=K(\sqrt[p^{m-1}]{A})=K(\sqrt[p^{m-1}]{E^*(\alpha)})$ is unramified over K.

Let $B=\sqrt[p^{m-1}]{A}$ then $K(\sqrt[p^n]{A})=K(\sqrt[p^{n-m+1}]{B})$ and $B\underset{p^{n-m+1}}{\sim}\langle\alpha_0', \alpha_1', \cdots, \gamma\rangle$ in L where γ is an integral element of the inertia field of $L/\boldsymbol{Q}_p$.

Now, the least suffix such that $\alpha_i'\not\equiv 0 \bmod p$ is i_m. Applying Theorem 1 to the totally ramified extension $K(\sqrt[p^{n-m+1}]{B})/L$ we have $f\leqq\text{Max}\{f_m, f_{m+1}\}$, where $\mathfrak{p}^f$ is the conductor of $K(\sqrt[p^{n-m+1}]{B})/L$. And, remarking that $\alpha'_{i_{m+1}}\varepsilon\equiv\alpha_{i_m}p_i' \bmod p^2$ is equivalent to $\alpha_{i_{m+1}}\varepsilon\equiv\alpha_{i_m}p \bmod p^{m+1}$ we have also the necessary and sufficient conditions for $f=\text{Max}\{f_m, f_{m+1}\}$. Since L/K is unramified, as for the conductor of $K(\sqrt[p^n]{A})/K$ we have Theorem 2.

§3. Proof of Theorem 1.

Now, for the proof of Theorem 1, we prove some Lemmas. In the proofs we use following facts.

For a principal unit B in K and positive integer r,

(11) if $B\equiv 1 \bmod \mathfrak{p}^{e_1p+(r-1)e+1}$ then $B\underset{p^r}{\sim}1$.

(J.P. Serre [5], p. 219, Proposition 9).

By (5), (6), and (7)

(12) if (Š) $B=\prod_j E(\beta_j, \pi^j)\equiv 1 \bmod \mathfrak{p}^k$ $(k\geqq 1)$ then $E(\beta_j, \pi^j)\equiv 1$ mop $\mathfrak{p}^k$ for all $j\in F$ and $E^*(\beta)\equiv 1 \bmod \mathfrak{p}^k$. By (2) and (4)

(13) if $s>e_1$ then $\mathrm{ord}^{\times}E(\alpha p^m, \pi^s)=s+me$ $(\alpha\in I,\ \alpha\not\equiv 0 \bmod p,\ m\geqq 0:$ integer).

(14) if $i<j$ $(i, j\in F,\ i\neq e_0,\ j\neq e_0)$

$\mathrm{ord}^{\times}E(p^m, \pi^i)<\mathrm{ord}^{\times}E(p^m, \pi^j)$ and when $m\leqq\kappa-1$ (especially when $m\leqq n-1$) this inequality holds also for $i=e_0$ or $j=e_0$.

In fact, let $i\neq e_0$ and $j\neq e_0$, since $i<j$ we have $\kappa_i\geqq\kappa_j$, if $\kappa_i=\kappa_j$ then the result follows immediately, so let $\kappa_i>\kappa_j$. If $m\leqq\kappa_j<\kappa_i$ then $\mathrm{ord}^{\times}E(p^m, \pi^i)=ip^m<jp^m=\mathrm{ord}^{\times}E(p^m, \pi^j)$, if $\kappa_j<m\leqq\kappa_i$ then $\mathrm{ord}^{\times}E(p^m, \pi^j)-\mathrm{ord}^{\times}E(p^m, \pi^i)=jp^{\kappa_j}+(m-\kappa_j)e-ip^m>0$, because $jp^{\kappa_j}-ip^m>e_1-e_1p=-e$, $(m-\kappa_j)e\geqq e$, and if $\kappa_j<\kappa_i<m$ then $\mathrm{ord}^{\times}E(p^m, \pi^j)-\mathrm{ord}^{\times}E(p^m, \pi^i)=jp^{\kappa_j}-ip^{\kappa_i}+(\kappa_i-\kappa_j)e>0$, because $jp^{\kappa_j}-ip^{\kappa_i}>-e$ and $(\kappa_i-\kappa_j)e\geqq e$. Furthermore, if $m\leqq\kappa-1$ then, since $\mathrm{ord}^{\times}E(p^m, \pi^{e_0})=e_0p^m$, the inequality holds also for $i=e_0$ or $j=e_0$.

LEMMA 1. *Let $n\geqq 1$, for a given integer t $(t=0$ or $t\in F)$, let $k=e_1p+(n-1)e-t+1$ and*

(Š) $$B=\prod_j E(\beta_j, \pi^j)E^*(\beta)\equiv 1 \quad \bmod \mathfrak{p}^k.$$

Then, (i) *when $t=0$, $\beta_j\equiv 0 \bmod p^n$ for all $j\in F$ and $\beta\equiv 0 \bmod p^n$, $\mathfrak{P}$.*

(ii) *When $1\leqq t<e$, $\beta_j\equiv 0 \bmod p^{n-1}$ for all $j\in F$ and $\beta\equiv 0 \bmod p^{n-1}$, $\mathfrak{P}$ and moreover $\beta_j\equiv 0 \bmod p^n$ if $j\leqq e_1p-t$.*

(iii) *When $e<t<e_1p$, $\beta_j\equiv 0 \bmod p^{n-2}$ for all $j\in F$, $\beta\equiv 0 \bmod p^{n-2}$, $\mathfrak{P}$ and moreover*

$$\beta_j\equiv\begin{cases} 0 \bmod p^{n-1} & \text{if } j\leqq e_1p+e-t \\ 0 \bmod p^n & \text{if } j\leqq e_1p-t. \end{cases}$$

Remark. For $n=1$, the parts of mod p^{n-1} and p^{n-2} in the Lemma 1 and its proof may be omitted.

Proof. (i) follows immediately from (11) and (8).

(ii) Since $t<e$ we have $k>e_1p+(n-2)e+1$ and $B\underset{p^{n-1}}{\sim}1$ by (11) and so by (8), $\beta_j\equiv 0 \bmod p^{n-1}$ for all $j\in F$ and $\beta\equiv 0 \bmod p^{n-1}$, $\mathfrak{P}$.

Next we show that $\beta_j\equiv 0 \bmod p^n$ if $j\leqq e_1p-t$. For, let $\beta_j\not\equiv 0 \bmod p^n$ for some j, $j\leqq e_1p-t$ then since $e_1p-t>e_1$ we have $\mathrm{ord}^{\times}E(\beta_j, \pi^j)\leqq\mathrm{ord}^{\times}E(p^{n-1}, \pi^{e_1p-t})=e_1p-t+(n-1)e<k$ by (13) and (14), this contradicts to the assumption $E(\beta_j, \pi^j)\equiv 1 \mod \mathfrak{p}^k$.

(iii) Since $t<e_1p\leqq 2e$ we have $k>e_1p+(n-3)e+1$. It follows that $B\underset{p^{n-2}}{\frown}1$ and $\beta_j\equiv 0 \mod p^{n-2}$ for all $j\in F$, $\beta\equiv 0 \mod p^{n-2}$, $\mathfrak{P}$. Next we show that $\beta_j\equiv 0 \mod p^{n-1}$ if $j\leqq e_1p+e-t$. Let $\beta_j\not\equiv 0 \mod p^{n-1}$ for some j, $j\leqq e_1p+e-t$, then

$$\mathrm{ord}^{\times}E(\beta_j, \pi^j)\leqq\mathrm{ord}^{\times}E(p^{n-2}, \pi^{e_1p+e-t})=e_1p+e-t+(n-2)e<k\,,$$

by (13) and (14) but this contradicts to our assumption.

Finally we show that $\beta_j\equiv 0 \mod p^n$ if $j\leqq e_1p-t$. Let $\beta_j\not\equiv 0 \mod p^n$ for some j, $j\leqq e_1p-t$, then $\mathrm{ord}^{\times}E(\beta_j, \pi^j)\leqq\mathrm{ord}^{\times}E(p^{n-1}, \pi^i)$ where $i=e_1p-t$. We show that $\mathrm{ord}^{\times}E(p^{n-1}, \pi^i)=m<k$ then the proof is completed.

Since $i<e_1$ it follows that $\kappa_i\geqq 1$. Now, in the case $\kappa_i\leqq n-1$, we have

$$k-m=i+(n-1)e+1-(ip^{\kappa_i}+(n-1-\kappa_i)e)=i-ip^{\kappa_i}+\kappa_ie+1$$

by (6). If $\kappa_i=1$ then

$$k-m=-i(p-1)+e+1>-e_1(p-1)+e+1>0\,,$$

if $\kappa_i\geqq 2$ then $k-m>0$ because $ip^{\kappa_i}\leqq e_1p\leqq 2e$.

And in the case $\kappa_i>n-1$, we have $m=ip^{n-1}\leqq e_1$ by (5), and $k-m=i+(n-1)e+1-ip^{n-1}$. If $n=1$ then clearly $k-m>0$ and if $n\geqq 2$ we have $k-m>0$ since $ip^{n-1}\leqq ip^{\kappa_i-1}\leqq e_1\leqq e$. Q. E. D.

Proof of Theorem 1 *in the case* $p\neq 2$.

In the following, when the conductor of $K(\sqrt[p^n]{A})/K$ is $\mathfrak{p}^f$ we write $f=f(A)$.

LEMMA 2. *Let* $n\geqq 1$ *and* $p\neq 2$ *then*

(i) *if* $A\sim\pi^a$ ($a\in\boldsymbol{Z}$, $a\not\equiv 0 \mod p$),

$$f(A)=e_1p+(n-1)e+1\,,$$

(ii) *if* $A\sim E(\alpha_i, \pi^i)$ ($i\in F$, $\alpha_i\in I$, $\alpha_i\not\equiv 0 \mod p$),

$$f(A)=e_1p+(n-1)e-i+1\,.$$

Proof. (i) Let $B\equiv 1 \mod \mathfrak{p}^{e_1p+(n-1)e+1}$ then $B\sim 1$ by (11) so we have $(A, B)=1$ and $f(A)\leqq e_1p+(n-1)e+1$. Next, let $B=E^*(\delta p^{n-1})$ where $\delta\in R^{\times}$ and $\mathrm{Sp}(\delta)\equiv 1 \mod p$. Then $B\equiv 1 \mod \mathfrak{p}^{e_1p+(n-1)e}$ by (7) and $(A, B)=\zeta_n^{\mathrm{Sp}(a\delta p^{n-1})}\neq 1$. So we have

$$f(A)\leqq e_1p+(n-1)e+1\,.$$

(ii) Proof of $f(A)\leqq e_1p+(n-1)e-i+1$. Let

$$(\check{\mathrm{S}})\quad B=\prod_j E(\beta_j, \pi^j)E^*(\beta)\equiv 1 \qquad \mod \mathfrak{p}^{e_1p+(n-1)e-i+1}$$

We show that $E(j\alpha_i\beta_j, \pi^{i+j})\sim 1$ for all $j\in F$ by showing that $\alpha_i\beta_j\equiv 0 \bmod p^n$ or $\mathrm{ord}^\times E(j\alpha_i\beta_j, \pi^{i+j})>e_1p+(n-1)e$. Then we have the result by the explicit formula (9).

Case 1; $1\leqq i<e$. By Lemma 1, if $j\leqq e_1p-i$ then $\beta_j\equiv 0 \bmod p^n$ so we have $\alpha_i\beta_j\equiv 0 \bmod p^n$. If $j>e_1p-i$ then $j>e_1$ and $\beta_j\equiv 0 \bmod p^{n-1}$ by Lemma 1 so we have $\mathrm{ord}^\times E(j\alpha_i\beta_j, \pi^{i+j})\geqq i+j+(n-1)e>e_1p+(n-1)e$ by (13).

Case 2; $e<i<e_1p$. By Lemma 1, if $j\leqq e_1p-i$ then $\alpha_i\beta_j\equiv 0 \bmod p^n$, if $e_1p-i<j\leqq e_1p+e-i$ then $\alpha_i\beta_j\equiv 0 \bmod p^{n-1}$ and so $\mathrm{ord}^\times E(j\alpha_i\beta_j, \pi^{i+j})>e_1p+(n-1)e$ by (13), and if $e_1p+e-i<j$ then $\alpha_i\beta_j\equiv 0 \bmod p^{n-2}$ and $\mathrm{ord}^\times E(j\alpha_i\beta_j, \pi^{i+j})>e_1p+e+(n-2)e=e_1p+(n-1)e$ by (13).

Proof of $f(A)\geqq e_1p+(n-1)e-i+1$. It is enough to show that there exists B such tnat

$$B\equiv 1 \mod \mathfrak{p}^{e_1p+(n-1)e-i} \quad \text{and} \quad (A, B)\neq 1\,.$$

Case 1; $1\leqq i<e$. Let $B=E(\beta_j, \pi^j)$ where $j=e_1p-i$ ($j\in F$, $j>e_1$) and $\beta_j=\delta p^{n-1}$ ($\delta\in R^\times$ will be determined below). Then $E(\beta_j, \pi^j)\equiv 1 \mod \mathfrak{p}^{e_1p-i+(n-1)e}$ by (13), and $E(j\alpha_i\beta_j, \pi^{i+j})\equiv 1-j\alpha_i\delta p^{n-1}\pi^{e_1p}\equiv 1-\delta_0\delta p^{n-1}\varepsilon_0^{p^\kappa}\pi_1^p \mod \mathfrak{p}^{e_1p+(n-1)e+1}$ where $j\alpha_i\equiv\delta_0 \bmod p$ ($\delta_0\in R^\times$) and ε_0 is that of Notations. On the other hand, by (7) $E^*((\delta_0\delta\varepsilon_0^{p^\kappa})^{p^{-(n-1)}}p^{n-1})\equiv 1-\delta_0\delta\varepsilon_0^{p^\kappa}p^{n-1}\pi_1^p \bmod \mathfrak{p}^{e_1p+(n-1)e+1}$. So, we have $E(j\alpha_i\beta_j, \pi^{i+j})\sim E^*((\delta_0\delta\varepsilon_0^{p^\kappa})^{p^{-(n-1)}}p^{n-1})$ and in explicit formula (9), we have $\gamma=(\delta_0\delta\varepsilon_0^{p^\kappa})^{p^{-(n-1)}}p^{n-1}$. Now, if we choose δ so that $\mathrm{Sp}((\delta_0\delta\varepsilon_0^{p^\kappa})^{p^{-(n-1)}})\equiv 1 \bmod p$ then $B\equiv 1 \bmod \mathfrak{p}^{e_1p+(n-1)e-i}$ and $(A, B)=\zeta_n^{\mathrm{Sp}(\gamma)}=\zeta_n^{p^{n-1}}\neq 1$.

Case 2; $i>e$. Let $B=E(\beta_j, \pi^j)$ where $j=e_1p+e-i$ ($j\in F$ and $j>e_1$) and $\beta_j=\delta p^{n-2}$ ($\delta\in R^\times$ will be determied below). Then we have $E(j\alpha_i\beta_j, \pi^{i+j})\equiv 1-j\alpha_i\delta p^{n-2}\pi^{e_1p+e}\equiv 1+j\alpha_i\delta\varepsilon^{-1}p^{n-1}\pi^{e_1p}\equiv 1-\delta_0\delta\varepsilon_0^{p^\kappa}p^{n-1}\pi_1^p \mod \mathfrak{p}^{e_1p+(n-1)e+1}$ where $-j\alpha_i\varepsilon^{-1}\equiv\delta_0 \bmod p$ ($\delta_0\in R^\times$) and ε is that of Notations. Thus, just as Case 1, we have in (9) $\gamma=(\delta_0\delta\varepsilon_0^{p^\kappa})^{p^{-(n-1)}}p^{n-1}$. Therefore, if we choose δ so that $\mathrm{Sp}(\gamma)\equiv p^{n-1} \bmod p^n$, we have $B\equiv 1 \bmod \mathfrak{p}^{e_1p+(n-1)e-i}$ and $(A, B)=\zeta_n^{\mathrm{Sp}(\gamma)}=\zeta_n^{p^{n-1}}\neq 1$.

Q. E. D.

From Lemma 2, we have following two Lemmas immediately.

LEMMA 3. *Let* $n\geqq 1$ *and* $p\neq 2$. *Then we have*
(i) *if* $A\sim\pi^a$, $a\in \boldsymbol{Z}$ *and* $\mathrm{ord}\, a=m$ $(0\leqq m\leqq n-1)$,

$$f(A)=e_1p+(n-m-1)e+1\,.$$

(ii) *if* $A=\mathrm{E}(\alpha_i, \pi^i)$, $i\in F$, $\alpha_i\in I$ *and* $\mathrm{ord}\,\alpha_i=m$ $(0\leqq m\leqq n-1)$,

$$f(A)=e_1p+(n-m-1)e-i+1\,.$$

Proof. (i) Let $a=a'p^m$ ($a'\in\boldsymbol{Z}$, $a'\not\equiv 0 \bmod p$) and $A'=\pi^{a'}$. Then $K(\sqrt[p^n]{A})=K(\sqrt[p^{n-m}]{A'})$ and the conductor of $K(\sqrt[p^{n-m}]{A'})$ is $\mathfrak{p}^{e_1p+(n-m+1)e+1}$ by Lemma 2 (i) (using $n-m$ instead of n), so we have $f(A)=e_1p+(n-m-1)e+1$. Just as (i) we have (ii) from Lemma 2 (ii). Q. E. D.

LEMMA 4. *Let* $n\geqq 1$ *and* $p\neq 2$. *Then*

(i) $f(\pi^{a})>f(E(\alpha_{i}, \pi^{i}))$ *and* $f(\pi^{a})>f(E^{*}(\alpha))$

where $a\in \boldsymbol{Z}$, $\alpha_{i}\in I$ $(i\in F)$, $0\leqq \text{ord } a\leqq n-1$, $\text{ord } a\leqq \text{ord } \alpha_{i}$ *and* $\alpha\in I$ *is arbitrary.*

(ii) $f(E(\alpha_{i}, \pi^{i}))>f(E(\alpha_{j}, \pi^{j}))$ *and* $f(E(\alpha_{i}, \pi^{i}))>f(E^{*}(\alpha))$

where $i, j\in F$ $(i<j)$, α_{i}, $\alpha\in I$ *and* $0\leqq \text{ord } \alpha_{i}\leqq n-1$, $\text{ord } \alpha_{i}\leqq \text{ord } \alpha_{j}$ *and* α *is arbitrary.*

Proof. We have the result immediately from Lemma 3 and the fact $E^{*}(\alpha)$ is p^{n}-primary.

Now, by local class field theory and by definition of conductor, we have: For elements $B_{1}, \cdots, B_{r}$ of K

$$f(B_{1}\cdots B_{r})\leqq \text{Max }\{f(B_{1}), \cdots, f(B_{r})\} \tag{15}$$

and

$$f(B_{1}\cdots B_{r})=f(B_{1}) \quad \text{if} \quad f(B_{1})>f(B_{i}) \quad (i=2, \cdots, r).$$

In fact, by local class field theory and by definition of conductor, the conductor of $L=K(\sqrt[p^n]{B_{1}}, \cdots, \sqrt[p^n]{B_{r}})$ is $\mathfrak{p}^{\text{Max}\{f^{(1)}, \cdots, f^{(r)}\}}$ where $f^{(i)}=f(B_{i})$ $(1\leqq i\leqq r)$. Since $K(\sqrt[p^n]{B_{1}\cdots B_{r}})$ is a subfield of L we have $f(B_{1}\cdots B_{r})\leqq \text{Max }\{f^{(1)}, \cdots, f^{(r)}\}$.

Next, let $f^{(1)}>f^{(i)}$ $(i=2, \cdots, r)$. Since $K(\sqrt[p^n]{B_{1}\cdots B_{r}}, \sqrt[p^n]{B_{2}}, \cdots, \sqrt[p^n]{B_{r}})=L$, we have $\text{Max }\{f(B_{1}\cdots B_{r}), f^{(2)}, \cdots, f^{(r)}\}=f^{(1)}$ and it follows that $f(B_{1}\cdots B_{r})=f^{(1)}=f(B_{1})$.

LEMMA 5. *Let* $n\geqq 2$ *and* $p\neq 2$.

If $A_{2}\sim E(\alpha_{i_2}, \pi^{i_2})$ $(i_{2}\in F,\ \alpha_{i_2}\in I,\ \text{ord } \alpha_{i_2}=1)$ $A_{1}\sim E(\alpha_{i_1}, \pi^{i_1})$ $(i_{1}\in F,\ \alpha_{i_1}\in I,$ $\text{ord } \alpha_{i_1}=0)$ *and* $f_{2}=e_{1}p+(n-2)e-i_{2}+1$, $f_{1}=e_{1}p+(n-1)e-i_{1}+1$ *then we have* $f(A_{2}A_{1})\leqq \text{Max }\{f_{2}, f_{1}\}$. *Moreover,* $f(A_{2}A_{1})=\text{Max }\{f_{2}, f_{1}\}$ *if and only if* $e+i_{2}\neq i_{1}$ *or* $\alpha_{i_2}\varepsilon\not\equiv \alpha_{i_1}p \mod p^{2}$ *and* $e+i_{2}=i_{1}$.

Proof. By Lemma 3 (ii), $f(A_{2})=f_{2}$ and $f(A_{1})=f_{1}$. By (15) we have $f\leqq \text{Max}\{f_{2}, f_{1}\}$ where $f=f(A_{2}A_{1})$. And if $f_{2}\neq f_{1}$ (i.e. $e+i_{2}\neq i_{1}$) then $f=\text{Max}\{f_{2}, f_{1}\}$ by (15).

Next, we show that if $e+i_{2}=i_{1}$ (i.e. $f_{2}=f_{1}$) and $\alpha_{i_2}\varepsilon\not\equiv \alpha_{i_1}p \mod p^{2}$ then $f=f_{2}=f_{1}$.

Since $f\leqq f_{2}=f_{1}$ it is enough to show that there exists B such that $B\equiv 1 \mod \mathfrak{p}^{f_{2}-1}$ and $(A_{2}A_{1}, B)\neq 1$.

Since $e+i_{2}=i_{1}$ and $i_{2}, i_{1}\in F$ it follows that $e_{1}>i_{2}\geqq 1$. Let $j_{2}=e_{1}p-i_{2}$ then $j_{2}\in F$ and $j_{2}>e_{1}$.

By the assumption $\alpha_{i_2}\varepsilon\not\equiv \alpha_{i_1}p \mod p^{2}$, there exists δ_{0} $(\delta_{0}\in R^{\times})$ such that $j_{2}(\alpha_{i_2}-\alpha_{i_1}\varepsilon^{-1}p)\equiv \delta_{0}p \mod p^{2}$ and for this δ_{0} we choose δ $(\delta\in R^{\times})$ satisfying $\text{Sp}((\delta_{0}\delta\varepsilon_{0}^{p^{\kappa}})^{p^{-(n-1)}})\equiv 1 \mod p$. Now, let $B=E(\beta_{j_2}, \pi^{j_2})$ where $\beta_{j_2}=\delta p^{n-2}$ then $B\equiv 1 \mod \mathfrak{p}^{f_{2}-1}$.

And,

$$E(j_{2}\alpha_{i_2}\beta_{j_2}, \pi^{i_{1}+j_{2}})\equiv 1-j_{2}\alpha_{i_2}\delta p^{n-2}\pi^{e_{1}p} \qquad \mod \mathfrak{p}^{e_{1}p+(n-1)e+1}$$

$$E(j_2\alpha_{i_1}\beta_{j_2},\ \pi^{i_1+j_2})\equiv 1-j_2\alpha_{i_1}\delta p^{n-2}\pi^{e_1p+e} \qquad \bmod \mathfrak{p}^{e_1p+(n-1)e+1}$$

Thus,

$$E(j_2\alpha_{i_2}\beta_{j_2},\ \pi^{i_2+j_2})E(j_2\alpha_{i_1}\beta_{j_2},\ \pi^{i_1+j_2})\equiv 1-j_2(\alpha_{i_2}-\alpha_{i_1}\varepsilon^{-1}p)\delta p^{n-2}\pi^{e_1p}$$

$$\equiv 1-\delta_0\delta\varepsilon_0^{p^\kappa}p^{n-1}\pi_1^p \qquad \bmod \mathfrak{p}^{e_1p+(n-1)e+1}$$

On the other hand, by (7),

$$E^*((\delta_0\delta\varepsilon_0^{p^\kappa})^{p-(n-1)}p^{n-1})\equiv 1-\delta_0\delta\varepsilon_0^{p^\kappa}p^{n-1}\pi_1^p \qquad \bmod \mathfrak{p}^{e_1p+(n-1)e+1}.$$

So we have, in explicit formula (9), $\gamma=(\delta_0\delta\varepsilon_0^{p^\kappa})^{p-(n-1)}p^{n-1}$ where

$$E(j_2\alpha_{i_2}\beta_{j_2},\ \pi^{i_2+j_2})E(j_2\alpha_{i_1}\beta_{j_2},\ \pi^{i_1+j_2})\sim\cdots E^*(\gamma).$$

And $\mathrm{Sp}(\gamma)\equiv\mathrm{Sp}((\delta_0\delta\varepsilon_0^{p^\kappa})^{p-(n-1)}p^{n-1})\equiv p^{n-1} \bmod p^n$, so we have $(A_2A_1,\ B)=\zeta_n^{\mathrm{Sp}(\gamma)}=\zeta_n^{p^{n-1}}\neq 1$.

Finally, we show that if $e+i_2=i_1$ and $\alpha_{i_2}\varepsilon\equiv\alpha_{i_1}p \bmod p^2$ then we have $f\leqq f_2-1$.

Now, let $n\geqq 2$ and (Š) $B=\prod_j E(\beta_j,\ \pi^j)E^*(\beta)\equiv 1 \bmod \mathfrak{p}^{f_2-1}$ then we have $\beta_j\equiv 0 \bmod p^{n-2}$ for all $j\in F$ and

$$\beta_j\equiv\begin{cases} 0 \bmod p^{n-1} & \text{if} \quad j<e_1p-i_2 \\ 0 \bmod p^n & \text{if} \quad j\leqq e_1p-e-i_2\,. \end{cases}$$

The proof is quite similar to that of Lemma 1.

Therefore,

$$\prod_j E(j\alpha_{i_2}\beta_j,\ \pi^{i_2+j})E(j\alpha_{i_1}\beta_j,\ \pi^{i_1+j})\sim E(j_2\alpha_{i_2}\beta_{j_2},\ \pi^{i_2+j_2})E(j_2\alpha_{i_1}\beta_{j_2},\ \pi^{i_1+j_2}),$$

where $j_2=e_1p-i_2$, i.e. if $j\neq j_2$, $E(j\alpha_{i_2}\beta_j,\ \pi^{i_2+j})\sim 1$ and $E(j\alpha_{i_1}\beta_j,\ \pi^{i_1+j})\sim 1$. In fact, if $j<e_1p-i_2$ then $\alpha_{i_2}\beta_j\equiv 0 \bmod p^n$, if $j>e_1p-i_2$ then $\alpha_{i_2}\beta_j\equiv 0 \bmod p^{n-1}$ and $\mathrm{ord}^\times E(j\alpha_{i_2}\beta_j,\ \pi^{i_2+j})>e_1p+(n-1)e$. And if $j\leqq e_1p-e-i_2$ then $\alpha_{i_1}\beta_j\equiv 0 \bmod p^n$, if $e_1p-e-i_2<j<e_1p-i_2$ then $\alpha_{i_1}\beta_j\equiv 0 \bmod p^{n-1}$ and $\mathrm{ord}^\times E(j\alpha_{i_1}\beta_j,\ \pi^{i_1+j})>e_1p-e-i_2+i_1+(n-1)e=e_1p+(n-1)e$, because $e+i_2=i_1$. And if $e_1p-i_2<j$ then $\alpha_{i_1}\beta_j\equiv 0 \bmod p^{n-2}$ and

$$\mathrm{ord}^\times E(j\alpha_{i_1}\beta_j,\ \pi^{i_1+j})>i_1+e_1p-i_2+(n-2)e=e_1p+(n-1)e\,.$$

Now,

$$E(j_2\alpha_{i_2}\beta_{j_2},\ \pi^{i_2+j_2})E(j_2\alpha_{i_1}\beta_{j_2},\ \pi^{i_1+j_2})\equiv(1-j_2\alpha_{i_2}\beta_{j_2}\pi^{e_1p})(1-j_2\alpha_{i_1}\beta_{j_2}\pi^{e_1p+e})$$

$$=1-j_2(\alpha_{i_2}-\varepsilon^{-1}\alpha_{i_1}p)\beta_{j_2}\pi^{e_1p} \qquad \bmod \mathfrak{p}^{e_1p+(n-1)e+1}.$$

While by the assumption $\alpha_{i_2}-\varepsilon^{-1}\alpha_{i_1}p\equiv 0 \bmod p^2$ and $\beta_{j_2}\equiv 0 \bmod p^{n-2}$ so we have $E(j_2\alpha_{i_2}\beta_{j_2},\ \pi^{i_2+j_2})E(j_2\alpha_{i_1}\beta_{j_2},\ \pi^{i_1+j_2})\sim 1$ by (12). Consequently $\gamma\equiv 0 \bmod p^n$, $\mathfrak{P}$ in (9).

Thus, we have shown $(A_2A_1,\ B)=\zeta_n^{\mathrm{Sp}(\gamma)}=1$ for any B, such that $B\equiv 1 \bmod \mathfrak{p}^{f_2-1}$. Q. E. D.

Now, we prove Theorem 1 in the case $p\neq 2$.

Let $A\underset{p^n}{\sim}\pi^a\prod_\iota E(\alpha_\iota, \pi^i)E^*(\alpha)$ and $f=f(A)$. When $n=1$ and $i_1=0$ by Lemma 2, Lemma 4 (i) and (15), we have $f=f(\pi^a)=e_1p+1=f_1$.

If $i_1\geqq 1$, $A\underset{p}{\sim}\prod_{i\geqq \iota_1}E(\alpha_\iota, \pi^i)E^*(\alpha)$ and by Lemma 4 and (15) $f=f(E(\alpha_{\iota_1}, \pi^{\iota_1}))=e_1p-i_1+1=f_1$ and $f_1=\mathrm{Max}\{f_1, f_2\}$ because $f_2<f_1$ by the definition $i_{n+1}=i_n$. Next let $n\geqq 2$, if $0=i_2=i_1$ we have $f=e_1p+(n-1)e+1=f_1$ by Lemma 2, Lemma 4 and (15), and $f_1=\mathrm{Max}\{f_2, f_1\}$ because $i_2=\iota_1$. If $0=i_2<i_1$ then $A=A_2A_1$ where

$$A_2=\begin{cases} \pi^a: i_1=1 \quad (\mathrm{ord}\, a=1) \\ \pi^a\prod_{\iota<i_1}E(\alpha_\iota, \pi^i): i_1>1 \quad (\mathrm{ord}\, a=\mathrm{ord}\,\alpha_\iota=1)\,. \end{cases}$$

and

$$A_1=\prod_{i\geqq \iota_1}E(\alpha_\iota, \pi^i)E^*(\alpha) \quad (0=\mathrm{ord}\,\alpha_{\iota_1}\leqq \mathrm{ord}\,\alpha_\iota).$$

Thus we have $f(A_2)=e_1p+(n-2)e+1=f_2$ by Lemma 3, Lemma 4 and (15), $f(A_1)=e_1p+(n-1)e-i_1+1=f_1$ by Lemma 2, Lemma 4 and (15).

Since $e+i_2\neq i_1$, $f_1\neq f_2$ and we have $f=\mathrm{Max}\{f_2, f_1\}$ by (15).

If $1\leqq i_2<i_1$ then $A=A_3A_2A_1$ where

$$A_3=\begin{cases} \pi^a: i_2=1 \quad (\mathrm{ord}\, a\geqq 2) \\ \pi^a\prod_{\iota<i_2}E(\alpha_\iota, \pi^i): i_2>1 \quad (\mathrm{ord}\,\alpha_i\geqq 2)\,, \end{cases}$$

$$A_2=\prod_{\iota_2\leqq\iota<i_1}E(\alpha_\iota, \pi^i) \quad (\mathrm{ord}\,\alpha_i=1)$$

and

$$A_1=\prod_{i\geqq \iota_1}E(\alpha_\iota, \pi^i)E^*(\alpha) \quad (0=\mathrm{ord}\,\alpha_{\iota_1}\leqq \mathrm{ord}\,\alpha_\iota)\,.$$

Now, since $\mathrm{ord}\, a\geqq 2$ and $\mathrm{ord}\,\alpha_i\geqq 2$ $(\iota<\iota_2)$ we have $f(A_3)\leqq e_1p+(n-3)e+1$ by Lemma 3 and (15) and $e_1p+(n-3)e+1<\mathrm{Max}\{f_2, f_1\}$ because

$$f_1-(e_1p+(n-3)e+1)=2e-\iota_1\geqq 2e-(e_1p-1)>0\,.$$

And $f(A_2)=f_2$, $f(A_1)=f_1$ by Lemma 4 and (15). Therefore $f=f(A_3A_2A_1)\leqq\mathrm{Max}\{f_2, f_1\}$ by (15). Moreover if $e+i_2\neq i_1$ or if $e+i_2=i_1$ and $\alpha_{\iota_2}\varepsilon\not\equiv\alpha_{\iota_1}p \bmod p^2$, then $A_2A_1=E(\alpha_{\iota_2}, \pi^{\iota_2})E(\alpha_{\iota_1}, \pi^{\iota_1})B$ where

$$B=\prod_{\substack{i>\iota_2\\ \iota\neq i_1}}E(\alpha_\iota, \pi^i)E^*(\alpha)\,.$$

By Lemma 5 $f(E(\alpha_{\iota_2}, \pi^{\iota_2})E(\alpha_{\iota_1}, \pi^{\iota_1}))=\mathrm{Max}\{f_2, f_1\}$ and $f(B)<\mathrm{Max}\{f_2, f_1\}$ by Lemma 4 and (15), so we have $f(A_2A_1)=\mathrm{Max}\{f_2, f_1\}$ and $f=f(A_3A_2A_1)=\mathrm{Max}\{f_2, f_1\}$. If $e+i_2=i_1$ and $\alpha_{\iota_2}\varepsilon\equiv\alpha_{\iota_1}p \bmod p^2$ then $f(E(\alpha_{\iota_2}, \pi^{\iota_2})E(\alpha_{\iota_1}, \pi^{\iota_1}))<\mathrm{Max}\{f_2, f_1\}$ by Lemma 5, and $f=f(A_3A_2A_1)<\mathrm{Max}\{f_2, f_1\}$ from (15).

Finally, in the case $1\leqq i_2=\iota_1$, $A=A_3A_1$ where

$$A_3=\begin{cases} \pi^a : i_1=1 \quad (\text{ord } a\geqq 2) \\ \pi^a \prod_{i<i_1} E(\alpha_i, \pi^i) : i_1>1 \quad (\text{ord } a\geqq 2, \text{ ord } \alpha_i\geqq 2) \end{cases}$$

and

$$A_1=\prod_{i\geqq i_1} E(\alpha_i, \pi^i)E^*(\alpha) \quad (\text{ord } \alpha_i\geqq \text{ord } \alpha_{i_1}=0)\,.$$

Just as before, we have $f=f_1$ because $f(A_3)\leqq e_1 p+(n-3)e+1<f_1=f(A_1)$, and $f_1=\text{Max}\{f_2, f_1\}$ because $i_2=i_1$.

Thus the proof of Theorem 1 in the case $p\neq 2$ is completed.

PROOF OF THEOREM 1 IN THE CASE $p=2$.

The difference with the case $p\neq 2$ is that, in the explicit formula (10) another term $\prod_{\mu,\nu=1}^{\infty} E((2^{\mu-1}i+2^{\nu-1}j)\alpha_i^{P^\mu}\beta_j^{P^\nu}, \pi^{2^\mu i+2^\nu j})$ is multiplied to each $E(j\alpha_i\beta_j, \pi^{i+j})$. But for all α_i, β_j which appear in the proofs of Lemma 2 and Lemma 5 in the case $p\neq 2$, $\gamma_{ij\mu\nu}\equiv 0 \mod p^n$, $\mathfrak{P}$ for all μ, ν ($\mu\geqq 1$, $\nu\geqq 1$) where

$$E((2^{\mu-1}i+2^{\nu-1}j)\alpha_i^{P^\mu}\beta_j^{P^\nu}, \pi^{2^\mu i+2^\nu j}) \sim \cdots E^*(\gamma_{ij\mu\nu})$$

Therefore the multiplied term gives no influence to the class of $\gamma \mod p^n$, $\mathfrak{P}$. Thus, having Lemma 3, 4 which are corollaries of Lemma 2, Theorem 1 holds also for $p=2$.

§ 4. Remarks and examples.

Remark 1. By elementary but rather complicated calculations of the explicit formula we can prove Theorem 1 without (15).

Remark 2. Let $n=1$ and $A\underset{p}{\sim}\prod_i E(\alpha_i, \pi^i)E^*(\alpha)$ then Theorem 1 asserts that the conductor of $K(\sqrt[p]{A})/K$ is $\mathfrak{p}^{e_1 p-i_1+1}$. On the other hand, the number i_1 is characterized by the following congruences:

$$A\underset{p}{\equiv} 1 \mod \mathfrak{p}^{i_1} \quad \text{and} \quad A\underset{p}{\not\equiv} 1 \mod \mathfrak{p}^{i_1+1}$$

where, generally, the notation $A\underset{p^m}{\equiv} 1 \mod \mathfrak{p}^k$ ($m\geqq 1$, $k\geqq 1$) means that there exists a principal unit η of K such that $A\eta^{-p^m}\equiv 1 \mod \mathfrak{p}^k$. This result is known (H. Hasse [1], I_a, p. 90, Satz. 10). While, when $n\geqq 2$ it is impossible in general to determine the conductor of $K(\sqrt[p^n]{A})/K$ by analogous congruences.

For example, let $K=\boldsymbol{Q}_p(\zeta_2)$ ($p\neq 2$) and

$$A\underset{p^2}{\sim} E(\alpha_{i_2}, \pi^{i_2})E(\alpha_{i_1}, \pi^{i_1})$$

where

$$\text{ord } \alpha_{i_2}=1 \quad (2\leqq i_2\leqq e_1-1=p-1)$$

and

$$\operatorname{ord}\alpha_{\imath_1}=0 \quad (\imath_1=e+1=p(p-1)+1).$$

Then $A\underset{p^2}{\equiv}1 \bmod \mathfrak{p}^{\imath_2 p}$ and $A\underset{p^2}{\not\equiv}1 \bmod \mathfrak{p}^{\imath_2 p+1}$ for $i_2=2, \cdots, p-1$.

While, since $f_1=e_1p>f_2=e_1p-i_2+1$ for any $\imath_2$ $(2\leqq i_2\leqq p-1)$, the conductor of $K(\sqrt[p^2]{A})/K$ is $\mathfrak{p}^{e_1p}$ by Theorem 1.

Example 1. Let $K\ni\zeta_n$ and π be a prime of K.

(i) Let $A=\pi^a\eta$ where $a\in\boldsymbol{Z}$, $a\not\equiv 0 \bmod p$ and η is a unit of K, then the conductor of $K(\sqrt[p^n]{A})/K$ is $\mathfrak{p}^{e_1p+(n-1)e+1}$.

For, since $i_1=0$ we have $f=\operatorname{Max}\{f_1, f_2\}=f_1=e_1p+(n-1)e+1$ by Theorm 1.

(ii) Let $n\geqq 2$ and $A=\pi^p(1-\pi^j)$ $(e<j<e_1p)$, then the conductor of $K(\sqrt[p^n]{A})/K$ is $\mathfrak{p}^{e_1p+(n-2)e+1}$.

For, since $i_2=0$ and $i_1=\jmath$ we have $e+\imath_2<\imath_1$ and $f=\operatorname{Max}\{f_2, f_1\}=f_2=e_1p+(n-2)e+1$.

Example 2. Let $K=\boldsymbol{Q}_p(\zeta_n)$ then the conductor of $K(\sqrt[p^n]{\zeta_m})/K$ $(1\leqq m\leqq n)$ is $\mathfrak{p}^{e_1p+(m-1)e}$.

For, let $1-\pi=\zeta_n=\prod_{\imath} E(\alpha_\imath, \pi^i)E^*(\alpha)$ $(\alpha_1\not\equiv 0 \bmod p)$ then

$$\zeta_m=\zeta_n^{p^{n-m}}=\prod_{\imath} E(\alpha_\imath p^{n-m}, \pi^i)E(\alpha p^{n-m}).$$

Therefore, since i_{n-m} does not exist and $i_{n-m+1}=1$, we have $f=f_{n-m+1}=e_1p+(m-1)e$ by Theorem 2.

Example 3. For some Kummer extensions we can get the ramification subgroups from conductors obtained by Theorem 1. For example, let $K\ni\zeta_n$ $(n\geqq 1)$ and $L=K(\sqrt[p^n]{A_i^{\alpha_i}})$ where $i=0$ or $i\in F$ and $A_0=\pi^{\alpha_0}$ $(\alpha_0\in\boldsymbol{Z},\ \alpha_0\not\equiv 0 \bmod p)$, $A_\imath=E(\alpha_\imath, \pi^i)$ $(\imath\in F,\ \alpha_i\in I,\ \alpha_i\not\equiv 0 \bmod p)$. Now, let $G=\langle\sigma\rangle=\operatorname{Gal}(L/K)$ and $G_\jmath$ be the $\jmath$-th ramification subgroup of this extension:

$$G=G_0=\cdots=G_{m_1}=\langle\sigma\rangle\supsetneqq G_{m_1+1}=\cdots=G_{m_2}=\langle\sigma^p\rangle\supsetneqq\cdots$$
$$=G_{m_n}=\langle\sigma^{p^{n-1}}\rangle\supsetneqq G_{m_n+1}=\{1\}.$$

Then, we have $m_k=e_1p^k-\imath$ for $k=1, 2, \cdots, n$.

Proof. Since L/K is a totally ramified cyclic extension of degree p^n, we only need to calculate m_k. Now, by Theorem 1 (or by Lemma 2) we have $f^{(s)}=e_1p+(s-1)e-i+1$ $(1\leqq s\leqq n)$ where $\mathfrak{p}^{f^{(s)}}$ is the conductor of $K(\sqrt[p^s]{A_i^{\alpha_i}})$. Thus,

$$f^{(1)}=e_1p-i+1=\frac{1}{\sharp G_0}\sum_{j=0}^{m_1}\sharp G_j=m_1+1 \qquad \text{and so} \quad m_1=e_1p-i.$$

$$f^{(2)}=\frac{1}{\sharp G_0}\sum_{j=0}^{m_2}\sharp G_j=f^{(1)}+(m_2-m_1)p^{-1} \qquad \text{and so} \quad m_2=e_1p+m_1,$$

because $f^{(2)}-f^{(1)}=e$. By repeating this process, we have

$$m_k=ep^{k-1}+ep^{k-2}+\cdots+ep+m_1=e_1p^k-i,$$

because $e_1(p-1)=e$. Q. E. D.

References

[1] H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraishen Zahlenkörper, Physica-Verlag (1970).

[2] H. Hasse, Zahlentheorie, Akademie-Verlag (1969).

[3] H. Hasse, Zur Arbeit von I. R. ŠAFAREVIČ über das allgemeine Reziprozitätsgesetz, Math. Nach. **5** (1951), 301-327.

[4] M. Kneser, Zum expliziten Reziprozitätsgesetz von I. R. ŠAFAREVIČ, Math. Nach. **6** (1951), 89-96.

[5] I. R. Šafarevič, A general reciprocity law, J. Math. Sbornik **26** (1950), 113-146.

[6] J. P. Serre, Corps locaux, Hermann (1962).

Department of Mathematics,
Miyagi University of Education,
Sendai, Japan