ON THE KUMMER-HILBERT RECIPROCITY LAW

DEDICATED TO PROFESSOR ZYOITI SUETUNA ON HIS SIXTIETH BIRTHDAY

By

Koichi YAMAMOTO

(Received July 3, 1959)

1.—Let p be an odd prime number, Q the field of rational p -adic numbers, ζ a primitive p th root of unity, and $k=Q(\zeta)$. k/Q is tamely ramified abelian and $k=Q(\varpi)$ for $\varpi=\sqrt[p-1]{-p}$. We may fix ϖ by requiring $\zeta \equiv 1 + \varpi \pmod{\mathfrak{p}^2}$, where $\mathfrak{p}$ is of course the prime ideal of k . The ring of integers of Q and of k will be denoted Z and by $\mathfrak{o}$. If μ is a principal unit of k we define a polynomial $f(x)=f_\mu(x)$ of degree $\leq p-2$ and with coefficients in Q such that $f(1)=1$, $f(\zeta)=\mu$. Then using the logarithmic differential quotient

$$l_i(\mu) = \left[\frac{d^i \log f(e^x)}{dx^i} \right]_{x=0}$$

we have for two principal units μ, ν ,

$$\{\mu, \nu\} = \zeta^{\sum_{i=1}^{p-1} (-)^{i-1} l_i(\mu) l_{p-i}(\nu)},$$

where $\{\mu, \nu\}$ stands for the norm residue symbol.

The Kummer-Hilbert reciprocity law above has been derived from a global law (Hilbert [1, p. 413], Hasse [3, II, p. 110]), and recently Šafarevič [4] obtained a local proof. His proof is extremely complicated by the fact that he treats a much more general reciprocity law. Moreover Šafarevič and Kneser [5], who improved [4], could not avoid the norm residue symbol defined in extraneous sources to complete the most crucial point.

In the present paper we wish to show that the Kummer-Hilbert reciprocity law of k may be stated in a slightly different way.

THEOREM. *Let π be an arbitrary prime element of k . By using a polynomial $\text{Log}(1+x) = \sum_{i=1}^{p-1} (-)^{i-1} x^i / i$, define $l_i(\mu) \in Z$ for $i=1, \dots, p-1$ by*

$$\text{Log } \mu \equiv \sum_{i=1}^{p-1} \frac{l_i(\mu)}{i!} \pi^i \pmod{\mathfrak{p}^p}$$

where μ is a principal unit. Then a principal unit ν is a norm of the kummerian extension $k(\sqrt[p]{\mu})/k$ if and only if

$$\sum_{i=1}^{p-1} (-)^{i-1} l_i(\mu) l_{p-i}(\nu) \equiv 0 \pmod{p}.$$

In the proof we do not require any norm residue symbol defined in another source, but we need three major tools: the inverse function of the Artin-Hasse exponential function (in the form $\text{Log } \mu$), orthogonality relation of Stirling numbers, and Lagrange's formula for the inversion of power series. On the basis of the last formula we can define the residue $\text{Res } \omega d\alpha$ for $\alpha \in \mathfrak{p}$ and $\omega \in \mathfrak{o}$, resulting in

$$\sum_{i=1}^{p-1} (-)^{i-1} l_i(\mu) l_{p-i}(\nu) \equiv \text{Res}(\text{Log } \mu d \text{Log } \nu) \pmod{p}.$$

This shows clearly that the local reciprocity law itself bears a character of a residue formula on Riemann surfaces.

2. —Preliminary lemmas. —Our first concern is to evaluate the sum

$$U_{m,n} = (-)^n \sum_{\lambda} (-)^{\lambda} \binom{m}{p\lambda} \binom{\lambda}{n},$$

'in the realm of p ' i.e., in $\mathbb{Q}$. It is evident that $U_{m,n} = 0$ for $m < pn$, and $U_{pn,n} = 1$.

LEMMA 1. *We have $\sum_{\lambda \equiv a \pmod{p}} (-)^{\lambda} \binom{m}{\lambda} \equiv 0 \pmod{p^{\left[\frac{m-1}{p-1}\right]}}$ for a fixed integer a .*

Moreover if $n \geq 1$, then $U_{(p-1)n,0} \equiv (-p)^{n-1} \pmod{p^n}$.

PROOF. 1) With η running over p th roots of unity we have

$$\sum \eta^{-a} (1-\eta)^m = p \sum_{\lambda \equiv a \pmod{p}} (-)^{\lambda} \binom{m}{\lambda}.$$

But this number is $= S_{k/Q} \zeta^{-a} (1-\zeta)^m \in (p)^{1+\left[\frac{m-1}{p-1}\right]}$, since k/Q is tamely ramified of degree $p-1$.

2) In case $m = (p-1)n$ and $a=0$, $(1-\zeta)^{(p-1)n} \equiv (-\varpi)^{(p-1)n} \equiv (-p)^n \pmod{\mathfrak{p}^{(p-1)n+1}}$, and hence by 1) $S_{k/Q} (1-\zeta)^{(p-1)n} \equiv -(-p)^n \pmod{p^{n+1}}$, i.e., $U_{(p-1)n,0} \equiv (-p)^{n-1} \pmod{p^n}$.

LEMMA 2. 1) *In general $\text{ord}_p U_{m,n} \geq \left[\frac{m-n-1}{p-1}\right] - n$.*

2) *If in particular $0 < n < p^{i+1}$ and $\text{ord}_p m \geq i+h$ then*

$$\text{ord}_p U_{m,n} \geq \left[\frac{m-n-1}{p-1}\right] - n + h.$$

PROOF. 1) The Faà di Bruno's formula on successive derivative reads :

$$\frac{d^n f}{dx^n} = \sum_{\alpha} \frac{n!}{(1!)^{\alpha_1} (2!)^{\alpha_2} \cdots a_1! a_2! \cdots} \left(\frac{d\xi}{dx}\right)^{\alpha_1} \left(\frac{d^2\xi}{dx^2}\right)^{\alpha_2} \cdots \frac{d^a f}{d\xi^a},$$

for $f=f(x)$, $\xi=\xi(x)$, with $a=a_1+a_2+\dots$; the summation extends over all partitions $\alpha: n=1a_1+2a_2+\dots$ of n .

By taking $x=\xi^p$, $f=x^\lambda=\xi^{p\lambda}$, and comparing coefficients of $x^{\lambda-n}$ we find

$$(\lambda)_n = \sum_{\alpha} \frac{n!}{(1!)^{a_1} (2!)^{a_2} \dots a_1! a_2! \dots} \left(\left(\frac{1}{p} \right)_1 \right)^{a_1} \left(\left(\frac{1}{p} \right)_2 \right)^{a_2} \dots (p\lambda)_a,$$

$$p^n \binom{\lambda}{n} = \sum_{\alpha} \frac{1}{(1!)^{a_1} (2!)^{a_2} \dots a_1! a_2! \dots} (1-p)^{a_2} ((1-p)(1-2p))^{a_3} \dots \binom{p\lambda}{a}.$$

We note moreover that

$$\sum_{\lambda} (-)^{\lambda} \binom{m}{p\lambda} \binom{p\lambda}{a} = \binom{m}{a} \sum_{\lambda} (-)^{\lambda} \binom{m-a}{p\lambda-a} = \binom{m}{a} p^{\left[\frac{m-a-1}{p-1} \right]} z$$

by Lemma 1, with an integer z . Thus if we put $p^n \binom{\lambda}{n}$ above in the definition of $p^n U_{m,n}$ the contribution C_{α} therein of a partition α has the ordinal in p : $\text{ord}_p C_{\alpha} \geq \text{ord}_p \binom{m}{a} + \left[\frac{m-a-1}{p-1} \right] - \sum_i a_i \text{ord}_p(i!)$, where

$$\sum_i a_i \text{ord}_p(i!) \leq \sum_i a_i \frac{i-1}{p-1} = \frac{n-a}{p-1}. \quad \text{Hence } \text{ord}_p C_{\alpha} \geq \text{ord}_p \binom{m}{a} + \left[\frac{m-a-1}{p-1} \right] - \left[\frac{n-a}{p-1} \right] \geq \left[\frac{m-n-1}{p-1} \right], \text{ independently of } \alpha. \quad \text{This means that } \text{ord}_p U_{m,n} \geq \left[\frac{m-n-1}{p-1} \right] - n.$$

2) If $0 < n < p^{i+1}$ and $\text{ord}_p m \geq i+h$ then $0 < a < p^{i+1}$ for any partition α and $\binom{m}{a}$ is divisible by p^h , since a is not divisible by p^{i+1} . Hence

$$\text{ord}_p U_{m,n} \geq \left[\frac{m-n-1}{p-1} \right] - n + h.$$

LEMMA 3. 1) If $pn \leq m < p(n+1)$, then $U_{m,n} \equiv 1 \pmod{p}$. 2) If $m > n$, then $U_{pm,n} \equiv 0 \pmod{p^2}$.

PROOF 1) Let $m = pn + r$, $0 \leq r < p$, $n = \left[\frac{m}{p} \right]$. Then since $\binom{m}{pc} \equiv \binom{n}{c} \pmod{p}$ in general, we have $U_{m,n} \equiv \binom{n}{n} \equiv 1 \pmod{p}$.

2) Similarly it is well known (cf. Artin-Hasse [2, p. 161]) that $\binom{pm}{p\lambda} \equiv \binom{m}{\lambda} \pmod{p^2}$, hence $U_{pm,n} \equiv (-)^n \sum_{\lambda} (-)^{\lambda} \binom{m}{\lambda} \binom{\lambda}{n} \equiv 0 \pmod{p^2}$, for $m < n$.

3. —The trace σ_m .—If the principal unit $\mu \equiv 1 \pmod{\mathfrak{p}^v}$, then μ is primary and any ν is a norm of $k(\sqrt[p]{\mu})/k$, whereas $\text{Log } \mu \equiv 0 \pmod{\mathfrak{p}^v}$. Thus our Theorem is trivially true.

Now let μ be a principal unit, $\mu = 1 - \beta$, $\text{ord}_{\mathfrak{p}} \beta = s$ with $1 \leq s \leq p-1$. It is well known that $k(\sqrt[p]{\mu})/k$ is completely ramified with the ramification number $v = p - s$ (cf. Hasse [3, I, p. 75]). Choose the least nonnegative solution c, d of $cs - dp = 1$. Let τ be an arbitrary prime element of k , and let $M = \sqrt[p]{\mu}$, $K = k(\sqrt[p]{\mu})$. Then $\Pi = (1 - M)^c \tau^{-d}$ is a prime element of K . We define

$$\gamma = N_{K/k} \Pi, \quad \sigma_m = S_{K/k} \Pi^m.$$

Note that $\gamma = \beta^c \tau^{-dp}$. And if $\beta \equiv \tau^s \xi^{-1} \pmod{\mathfrak{p}}$ for a $(p-1)$ th root of unity ξ , we have $\beta \equiv \tau^s \xi^d \pmod{\mathfrak{p}^v}$.

We fix the meanings of the notations above throughout the rest of this paper. Our next concern is to evaluate σ_m/m modulo $\mathfrak{p}^{v+1}$.

LEMMA 4. We have

$$\frac{\sigma_m}{m} \equiv \frac{p}{m} \tau^{-dm} \beta^{\left[\frac{cm}{p}\right]} \pmod{\mathfrak{p}^{v+1}},$$

except the case $v=1$, $m=p$, where we have instead $\sigma_p/p \equiv 2\tau \pmod{\mathfrak{p}^2}$.

PROOF. 1) We consider σ_m first:

$$\begin{aligned} \sigma_m &= \tau^{-dm} S_{K/k} (1 - M)^{cm} = \tau^{-dm} \sum_{\lambda} (-)^{\lambda} \binom{cm}{\lambda} S_{K/k} M^{\lambda} = p \tau^{-dm} \sum_{\lambda} (-)^{\lambda} \binom{cm}{p\lambda} \mu^{\lambda} \\ &= p \tau^{-dm} \sum_{\lambda} \sum_t (-)^{\lambda} \binom{cm}{p\lambda} \binom{\lambda}{l} (-\beta)^l = p \tau^{-dm} \sum_l \beta^l U_l = \sum T_l, \end{aligned}$$

with $U_l = U_{cm, l}$ of §2. Using $r = cm - pl \geq 0$ we have $\text{ord}_{\mathfrak{p}}(\tau^{-dm} \beta^l) = -dm + sl = \frac{m - sr}{p}$, $\text{ord}_{\mathfrak{p}} U_l \geq \left[\frac{cm - l - 1}{p - 1} \right] - l = \left[\frac{r - 1}{p - 1} \right]$ by Lemma 2, and especially if $r \neq 0$, i.e., if $r \geq p$ then

$$\text{ord}_{\mathfrak{p}}(T_l) \geq \frac{m - sr}{p} + (p - 1) \left(\left[\frac{r - 1}{p - 1} \right] + 1 \right) \geq \frac{m - sr}{p} + r = \frac{vr + m}{p} > v.$$

Hence only the term T_l with $r=0$ is significant. In that case $l = \left[\frac{cm}{p} \right]$ and

$U_l \equiv 1 \pmod{p}$ by Lemma 3. Hence $\sigma_m \equiv p \tau^{-dm} \beta^{\left[\frac{cm}{p}\right]} \pmod{\mathfrak{p}^{v+1}}$.

2) Let $m=pm'$, $r=pr'$ in 1). Then $p^{-1}\sigma_m=\tau^{-dm}\sum_l\beta^l U_l=\sum_l T_l'$, say with

$$\text{ord}_p(T_l') \geq m' - sr' + (p-1)\left(r' + \left\lceil \frac{r'-1}{p-1} \right\rceil\right)$$

by the result in 1). Assume $r' \neq 0$, i.e., $r' \geq 1$ then the last number

$$\geq m' - sr' + (p-1)r' = \begin{cases} vr' + m' - r' \\ vm' + (v-1)(r' - m') \end{cases} \geq v$$

The equality sign can only be valid for $m'=r'=1$ or for $v=1$, $m'=1$. In either case, if moreover $l=c-r'>0$, then $U_l=U_{pc,l}$ is divisible by p as seen from Lemma 2, 2), since of course $l < c \leq p-1$. This means that the term with both $l>0$ and $r>0$ are negligible in the sum for $p^{-1}\sigma_m$.

If $r'=1$, $l=0$, then $c=l+r'=1$ and $U_0=U_{p,0}=0$. Hence $T_0=0$.

If $v=1$, $m'=1$, then $s=p-1$, $c=p-1$ and $U_0=U_{p(p-1),0} \equiv p^{p-1} \pmod{p^p}$, by Lemma 1.

Hence $p^{-1}\sigma_{pm'} \equiv \tau^{-dpm'} \beta^{cm'} \pmod{p^{v+1}}$ unless $s=p-1$, $m'=1$, in which case $p^{-1}\sigma_p \equiv \tau^{-p(p-2)}(p^{p-1} + \beta^{p-1}) \equiv 2\tau \pmod{p^2}$, as is easily verified.

3) Let $m=p^e m''$ with $e \geq 2$ and $r=pr'$ in 1). Then $p^{-e}\sigma_m = p^{-e+1}\tau^{-dm} \sum_l \beta^l U_l = \sum_l T_l''$ with

$$\text{ord}_p(T_l'') \geq p^{e-1}m'' - sr' + (p-1)\left(r' + \left\lceil \frac{r'-1}{p-1} \right\rceil - e + 1\right).$$

It is easy to see that this is $> v$ for $r' \neq 0$, except the case $e=2$, $m''=r'=1$. But since $U_{p^2c, pc-1} \equiv 0 \pmod{p^2}$ by Lemma 3, 2) we know that only T''_{pc} is significant. I.e., $p^{-e}\sigma_m \equiv p^{-e+1}\tau^{-dm} \beta^{\frac{cm}{p}} \pmod{p^{v+1}}$ for $\text{ord}_p m \geq 2$.

The considerations 1)~3) prove the Lemma completely, since the terms T_l, T_l', T_l'' with $r=0$ are displayed in the proposition.

LEMMA 4'. 1) If either $m \not\equiv p \pmod{s}$ or $m > v$ then $\sigma_m \equiv 0 \pmod{p^{v+1}}$, while if $m = p - js$, $j > 0$ then $\sigma_{p-js} \equiv -\xi^{(j-1)d} \gamma^v \pmod{p^{v+1}}$.

2) If $m > v$ then $p^{-1}\sigma_{pm} \equiv 0 \pmod{p^{v+1}}$, while $p^{-1}\sigma_{pm} \equiv \gamma^m \pmod{p^{v+1}}$ for $m \leq v$ if $v \neq 1$. If $v=m=1$ we have instead $p^{-1}\sigma_p \equiv 2\gamma \pmod{p^2}$.

3) For $e \geq 2$ we have $p^{-e}\sigma_{p^e m} \equiv 0 \pmod{p^{v+1}}$ except the case $e=2$, $m=1$, where $p^{-2}\sigma_{p^2} \equiv \frac{\gamma^p}{p} \pmod{p^{v+1}}$.

PROOF. This is almost a restatement of Lemma 4. We only prove the first part of 1). By Proof 1) of Lemma 4 we have

$\text{ord}_{\mathfrak{p}}(T[\frac{ms}{p}]) - v = s - 1 - \frac{rs - m}{p} \geq 0$, since $\frac{rs - m}{p} < \frac{rs}{p} < s$. The equality sign is valid if and only if $p - m = s(p - r)$, i.e., $p - m$ is a positive multiple of s .

We have immediately

LEMMA 5. *We have*

$$\begin{aligned} \log N_{K/k}(1 - \Pi^m) &\equiv 0 & (\text{mod } \mathfrak{p}^{v+1}) & \text{ for } m > v, \\ \log N_{K/k}(1 - \Pi^m) &\equiv -\gamma^m & (\text{mod } \mathfrak{p}^{v+1}) & \text{ for } m \not\equiv p \pmod{s}, v \geq m \geq 2, \\ \log N_{K/k}(1 - \Pi^m) &\equiv -\gamma^m + \xi^{(j-1)d}\gamma^v & (\text{mod } \mathfrak{p}^{v+1}) & \text{ for } m = p - js, m \geq 2, \\ \log N_{K/k}(1 - \Pi) &\equiv -\gamma - \frac{\gamma^p}{p} & (\text{mod } \mathfrak{p}^{v+1}) & \text{ for } p \not\equiv 1 \pmod{s}, \\ \log N_{K/k}(1 - \Pi) &\equiv -\gamma - \frac{\gamma^p}{p} + \xi^{(j-1)d}\gamma^v & (\text{mod } \mathfrak{p}^{v+1}) & \text{ for } 1 = p - js, v \neq 1, \\ \log N_{K/k}(1 - \Pi) &\equiv 0 & (\text{mod } \mathfrak{p}^2) & \text{ for } v = 1. \end{aligned}$$

4. —**The function** $\text{Log } \varepsilon$. —We define polynomials $\text{Log}(1+x) =$

$$\sum_{i=1}^{p-1} (-)^{i-1} x^i / i \text{ and } \text{Exp } x = \sum_{i=0}^{p-1} \frac{x^i}{i!}. \text{ It is evident that } \text{Log}(\text{Exp } x) \equiv x,$$

$\text{Exp}(\text{Log}(1+x)) \equiv 1+x \pmod{x^p}$ in the polynomial ring $Q[x]$. Similarly $\text{Log}(1+x+y+xy) \equiv \text{Log}(1+x) + \text{Log}(1+y)$, $\text{Exp}(x+y) \equiv \text{Exp } x \cdot \text{Exp } y \pmod{\mathfrak{m}}$, in $Q[x, y]$ where $\mathfrak{m}$ is the ideal consisting of elements of total degree $\geq p$.

We define $\text{Log } \varepsilon$ for a principal unit ε and $\text{Exp } \alpha$ for a non-unit α of k by the above polynomials, taken mod $\mathfrak{p}^p$. Thus we have

$$\text{Log}(\text{Exp } \alpha) \equiv \alpha, \text{Exp}(\text{Log } \varepsilon) \equiv \varepsilon,$$

$\text{Log}(\varepsilon \varepsilon_1) \equiv \text{Log } \varepsilon + \text{Log } \varepsilon_1$, $\text{Exp}(\alpha + \alpha_1) \equiv \text{Exp } \alpha \cdot \text{Exp } \alpha_1 \pmod{\mathfrak{p}^p}$ for principal units $\varepsilon, \varepsilon_1$ and non-units α, α_1 .

Moreover if $\text{ord}_{\mathfrak{p}} \alpha > 1$ or $\text{ord}_{\mathfrak{p}}(\varepsilon - 1) > 1$ then we have

$$\text{Log } \varepsilon \equiv \log \varepsilon, \text{Exp } \alpha \equiv e^{\alpha} \pmod{\mathfrak{p}^p},$$

as is readily seen. These functions $\text{Exp } \alpha$ and $\text{Log } \varepsilon$ are nothing but the Artin-Hasse exponential function and its inverse reduced mod $\mathfrak{p}^p$, in truth.

The following Lemma is of some interest in itself.

LEMMA 6. $\zeta \equiv \text{Exp } \varpi$, $\varpi \equiv \text{Log } \zeta$, $(\text{mod } \mathfrak{p}^p)$.

PROOF. It is sufficient to prove $(\text{Exp } \varpi)^p \equiv 1 \pmod{\mathfrak{p}^{2p-1}}$. For indeed $\zeta^{-1} \text{Exp } \varpi \equiv 1 \pmod{\mathfrak{p}^2}$ and from $(1 + \varpi^2 z)^p \equiv 1 \pmod{\mathfrak{p}^{2p-1}}$ it follows $\varpi^2 z \equiv 0 \pmod{\mathfrak{p}^p}$, i.e., $\zeta \equiv \text{Exp } \varpi \pmod{\mathfrak{p}^p}$. Now by definition $\text{Exp } x = 1 + xg(x)$ for

a polynomial $g(x)$, and $(\text{Exp } x)^p = 1 + pxg(x) + \cdots + x^p g(x)^p = 1 + ph(x) + x^p g(x)^p$, say. Since $(\text{Exp } \varpi)^p \equiv 1 + ph(\varpi) + \varpi^p \pmod{\mathfrak{p}^{2p-1}}$, we have to evaluate $h(\varpi) \pmod{\mathfrak{p}^p}$. But $h(x) \equiv \frac{1}{p}(e^{px} - 1) \pmod{x^p}$ when considered in the ring $Q\langle x \rangle$ of formal power series. Hence $h(\varpi) \equiv \varpi \pmod{\mathfrak{p}^p}$, i.e., $(\text{Exp } \varpi)^p \equiv 1 + p\varpi + \varpi^p \equiv 1 \pmod{\mathfrak{p}^{2p-1}}$.

It is important to know $\text{Log } N_{K/k}(1 - \Pi)$. If $v \neq 1$, then it is well known that $N_{K/k}(1 - \Pi) \equiv 1 - \gamma \pmod{\mathfrak{p}^2}$. Thus if $\gamma \equiv t\varpi \pmod{\mathfrak{p}^2}$, with $1 \leq t \leq p-1$, then $\zeta^{-t} N_{K/k}(1 - \Pi) \equiv 1 \pmod{\mathfrak{p}^2}$ and hence $\text{Log } N_{K/k}(1 - \Pi) \equiv \text{Log}(\zeta^{-t} N_{K/k}(1 - \Pi)) + t\varpi \equiv \log(\zeta^{-t} N_{K/k}(1 - \Pi)) + t\varpi \equiv \log N_{K/k}(1 - \Pi) + t\varpi \pmod{\mathfrak{p}^p}$. But $\gamma \equiv t\varpi$

$(\text{mod } \mathfrak{p})$ entails $\gamma^p \equiv t^p \varpi^p \pmod{\mathfrak{p}^{p+1}}$, i.e., $t\varpi \equiv -\frac{\gamma^p}{p} \pmod{\mathfrak{p}^p}$. This means that $\text{Log } N_{K/k}(1 - \Pi) \equiv \log N_{K/k}(1 - \Pi) - \frac{\gamma^p}{p} \pmod{\mathfrak{p}^p}$, for $v \neq 1$. If $v = 1$ on the contrary we have simply $N_{K/k}(1 - \Pi) \equiv 0 \pmod{\mathfrak{p}^2}$.

Now we can state Lemma 5 in a neater form.

LEMMA 5'. *We have*

$$\begin{aligned} \text{Log } N_{K/k}(1 - \Pi^m) &\equiv 0 && \pmod{\mathfrak{p}^{v+1}} \quad \text{for } m > v, \\ \text{Log } N_{K/k}(1 - \Pi^m) &\equiv -\gamma^m && \pmod{\mathfrak{p}^{v+1}} \quad \text{for } m \equiv p \pmod{s}, \quad m \leq v, \\ \text{Log } N_{K/k}(1 - \Pi^m) &\equiv -\gamma^m + \xi^{(j-1)d} \gamma^v && \pmod{\mathfrak{p}^{v+1}} \quad \text{for } m = p - js. \end{aligned}$$

5. —A canonical mapping. —By the mapping $\varepsilon \rightarrow \text{Log } \varepsilon \pmod{\mathfrak{p}^{v+1}}$ the multiplicative group $\varepsilon/\varepsilon^{(v+1)}$, where $\varepsilon^{(v+1)} = 1 + \mathfrak{p}^{v+1}$, is mapped isomorphically onto the additive group $\mathfrak{p} - \mathfrak{p}^{v+1}$, since $v+1 \leq p$. The image $\mathfrak{N}$ of the norm group of K/k is determined in Lemma 5' above. Hence:

A principal unit ν is a norm of $k(\sqrt[p]{\mu})/k$ if and only if $\text{Log } \nu$ is reduced to 0 by applying the 'rules'

$$\begin{aligned} \gamma^m &\sim \xi_0 \gamma^v && \text{for } m = p - js, \quad j > 0, \\ \gamma^m &\sim 0 && \text{for other } m\text{'s}. \end{aligned}$$

Of course $\alpha \sim 0$ is here to denote $\alpha \in \mathfrak{N}$.

It is natural to ask for a prime element ϑ such that $\vartheta \sim \vartheta^2 \sim \cdots \sim \vartheta^{v-1} \sim 0$.

LEMMA 7. *In order that a prime element $\vartheta = \gamma(1 + \cdots)$ satisfies the relations $\vartheta \sim \vartheta^2 \sim \cdots \sim \vartheta^{v-1} \sim 0$ it is necessary and sufficient that*

$$\vartheta \equiv \gamma \left(\frac{\text{Log } \mu}{-\beta} \right)^{\alpha} \pmod{\mathfrak{p}^{v+1}}.$$

PROOF. We prove only the sufficiency part of the Lemma since this only will be used in the sequel. But the necessity part is interesting because it explains the intrusion of the function $\text{Log } \mu$ in our problem.

It is easy to see that $\mathfrak{J}^h \sim 0$ for $h \neq p - js$. If $h = p - js$, $j > 1$ then

$$\mathfrak{J}^{p-js} \equiv \gamma^{p-js} \left(\frac{\text{Log } \mu}{-\beta} \right)^{p-j} \pmod{\mathfrak{p}^p}.$$

Now $\left(\frac{\text{Log}(1-x)}{-x} \right)^{p-j} \equiv \left(\frac{\log(1-x)}{-x} \right)^{p-j} \pmod{x^{p-2}Q\langle x \rangle}$ in the ring $Q\langle x \rangle$ of formal power series and in general

$$\frac{(\log(1-x))^m}{m!} = \sum_{n=1}^{\infty} \frac{S_n^m}{n!} (-x)^n,$$

with the *Stirling numbers* S_n^m of the first kind. Hence

$$\begin{aligned} \mathfrak{J}^{p-js} &\equiv (p-j)! \gamma^{p-js} \sum_{\lambda=1}^{j-1} \frac{S_{p-j+\lambda}^{p-j}}{(p-j+\lambda)!} (-\beta)^\lambda \equiv (p-j)! \sum_{\lambda=1}^{j-1} (-)^\lambda \xi^{d\lambda} \frac{S_{p-j+\lambda}^{p-j}}{(p-j+\lambda)!} \gamma^{p-(j-\lambda)s} \\ &\sim (-)^{p-j} (p-j)! \xi^{(j-1)d} \left(\sum_{\lambda=1}^{p-j} (-)^\lambda \frac{S_\lambda^{p-j}}{\lambda!} \right) \gamma^v \sim 0. \end{aligned}$$

The fact used above that $\sum (-)^\lambda S_\lambda^{p-j}/\lambda! \equiv 0 \pmod{p}$ is a special case of the *orthogonality relation of the Stirling numbers* of the first and the second kinds. Indeed with the *Stirling numbers*

$$\mathfrak{S}_n^m = \frac{\Delta^m 0^n}{m!} = \frac{1}{m!} \sum_{\lambda} (-)^{m-\lambda} \binom{m}{\lambda} \lambda^n$$

of the second kind the orthogonality relation

$$\sum_{\lambda} \mathfrak{S}_{\lambda}^m S_n^{\lambda} = \sum_{\lambda} S_{\lambda}^m \mathfrak{S}_n^{\lambda} = \delta_{m,n}$$

holds, as is well known. Moreover in particular

$$\mathfrak{S}_{p-1}^{\lambda} \equiv \frac{(-1)^{\lambda}}{\lambda!} \sum_{\kappa=1}^{\lambda} (-)^{\kappa} \binom{\lambda}{\kappa} \equiv \frac{(-1)^{\lambda-1}}{\lambda!} \pmod{p}.$$

We have seen that ν is a norm of K/k if and only if $\text{Log } \nu \equiv$

$$\sum_{i=1}^{v-1} a_i \mathfrak{J}^i \pmod{\mathfrak{p}^{v+1}}, \text{ with } a_i \in Z.$$

6. —The differential in k . —Let π be an arbitrary prime element of k and α a non-unit. If $\alpha \equiv \sum_{i=1}^{p-1} \frac{a_i \pi^i}{i!} \pmod{\mathfrak{p}^p}$, with $a_i \in Z$, we write $a_i \equiv D_{\pi}^i \alpha$ ($i=1, \dots, p-1$). Moreover we define $\frac{d\alpha}{d\pi} \equiv \sum_{i=0}^{p-2} \frac{a_{i+1}}{i!} \pi^i$. These are to be taken modulo p . We define $D_{\pi}^0 \alpha = 0$. Let ν be a unit, $\nu \equiv \sum_{i=0}^{p-2} \frac{c_i \pi^i}{i!} \pmod{\mathfrak{p}^{p-1}}$ with

$c_i \in Z$. We define $D_\pi^i v \equiv c_i$, for $i=0,1,\dots, p-2$ and $\frac{dv}{d\pi} = \sum_{i=0}^{p-3} \frac{c_{i+1}}{i!} \pi^i$. The operators D_π^i are additive and carry $\mathfrak{p}-\mathfrak{p}\mathfrak{p}$ or $\mathfrak{o}-\mathfrak{p}\mathfrak{o}$ into $Z-\mathfrak{p}Z$. Especially $D_\pi = D_\pi^1$ is a derivation :

$$D_\pi(\alpha\beta) \equiv \alpha D_\pi \beta + \beta D_\pi \alpha \pmod{p};$$

and more generally the Leibnitz' formula

$$D_\pi^m(\alpha\beta) \equiv \sum_{i=0}^m \binom{m}{i} D_\pi^i \alpha D_\pi^{m-i} \beta \pmod{p}$$

is valid. Note further that

$$(1) \quad D_\pi^{m+i}(\alpha\pi^i) \equiv (m+i)_i D_\pi^m \alpha \pmod{p}$$

and that

$$(2) \quad D_\pi^m \frac{d\alpha}{d\pi} \equiv D_\pi^{m+1} \alpha \pmod{p}.$$

These formulas are valid for values of m and i , for which the left-hand side members are defined.

We need the important

LEMMA 8 (Lagrange's formula for inversion of power series). *If π and θ are prime elements and $\alpha \in \mathfrak{o}$, then for the m for which $D_\theta^m \alpha$ is defined,*

$$D_\theta^m \alpha \equiv D_\pi^{m-1} \left(\frac{d\alpha/d\pi}{d\pi/d\theta} \right)^m \pmod{p}.$$

PROOF. If $\alpha \equiv a_0 + a_1 \pi + \dots$ with $a_i \in \mathfrak{o}$, then $D_\theta^1 \alpha \equiv a_1 \frac{\pi}{\theta} \equiv \frac{d\alpha}{d\pi} \frac{\pi}{\theta} \pmod{p}$.

This furnishes the case $m=1$. Assume therefore $m \geq 1$ and the validity of the proposition for lesser values of m . It is sufficient to prove for

$\alpha = \pi^l$ with $1 \leq l \leq m$. Now $D_\theta^m \pi^l = D_\theta^m (\theta^l \phi^l)$ with $\phi = \frac{\pi}{\theta}$ and by using Leib-

nitz' formula $D_\theta^m \pi^l \equiv \sum_i \binom{m}{i} D_\theta^i \theta^l D_\theta^{m-i} \phi^l \equiv (m)_i D_\theta^{m-i} \phi^l \pmod{p}$. This is $\equiv m! \phi^m$

$\pmod{p}$ for $l=m$, while the right-hand side member is the same. If $l < m$,

then by induction hypothesis we have $(m)_i D_\theta^{m-i} \phi \equiv (m)_i D_\pi^{m-i-1} \left(\frac{d\phi^l}{d\pi} \phi^{m-l} \right)$

$$\equiv (m)_i l D_\pi^{m-i-1} \left(\frac{d\phi}{d\pi} \phi^{m-1} \right) \equiv (m-1)_{i-1} l D_\pi^{m-i} \phi^m \equiv D_\pi^{m-1} (l \pi^{l-1} \phi^m) \equiv D_\pi^{m-1} \left(\frac{d\pi^l}{d\pi} \cdot \phi^m \right)$$

$\pmod{p}$, using (1) and (2).

Now it is immediate to prove our main Theorem. Indeed we have only to evaluate $D_{\vartheta}^{\nu} \text{Log } \nu \pmod{p}$. Let π be an arbitrary prime element. Then by using Lemmas 7, 8 and (1) above we have

$$\begin{aligned}
D_{\vartheta}^{p-s} \text{Log } \nu &\equiv D_{\pi}^{p-s-1} \left(\frac{d}{d\pi} \nu \left(\frac{\pi}{\vartheta} \right)^{p-s} \right) \equiv D_{\pi}^{p-s-1} \left(\frac{d}{d\pi} \text{Log } \nu \left(\frac{\pi}{\gamma} \right)^{p-s} \frac{\text{Log } \mu}{-\beta} \right) \\
&\equiv -\xi^{-d} D_{\pi}^{p-s-1} \left(\frac{d}{d\pi} \text{Log } \nu \frac{\text{Log } \mu}{\pi^s} \right) \equiv -\xi^{-d} \sum_{i=1}^{p-s} \frac{D_{\pi}^i \text{Log } \nu}{(i-1)!} D_{\pi}^{p-s-1} \left(\pi^{i-1} \frac{\text{Log } \mu}{\pi^s} \right) \\
&\equiv -\xi^{-d} \sum_{i=1}^{p-s} \frac{D_{\pi}^i \text{Log } \nu}{(i-1)!} \frac{(p-s-1)!}{(p-i)!} D_{\pi}^{p-i} \text{Log } \mu \\
&\equiv (p-s-1)! \xi^{-d} \sum_{i=1}^{p-1} \binom{p-1}{i-1} D_{\pi}^i \text{Log } \nu D_{\pi}^{p-i} \text{Log } \mu \\
&\equiv -(p-s-1)! \xi^d \sum_{i=1}^{p-1} (-)^{i-1} D_{\pi}^i \text{Log } \mu D_{\pi}^{p-i} \text{Log } \nu \\
&\equiv (-)^s s! \xi^{-d} \sum_{i=1}^{p-1} (-)^{i-1} D_{\pi}^i \text{Log } \mu D_{\pi}^{p-i} \text{Log } \nu.
\end{aligned}$$

This completes proof of our Theorem.

The fact that the last expression does not depend on the choice of π originates in a residue formula. Indeed we see readily, by using Lemma 8, that $D_{\pi}^{p-1} \omega \frac{d\alpha}{d\pi} \pmod{p}$ is independent of π , for $\alpha \in \mathfrak{p}$ and $\omega \in \mathfrak{o}$. We define by this the symbol $\text{Res } \omega d\alpha \pmod{p}$. Then we have $\text{Res } d\alpha \equiv 0 \pmod{p}$. The expression for $D_{\vartheta}^{\nu} \text{Log } \nu$ above may be written as $(-)^s s! \xi^{-d} \text{Res} (\text{Log } \mu d \text{Log } \nu) \pmod{p}$, explaining the above mentioned “invariance”, together with the “skew symmetry” of the underlying norm residue symbol.

In conclusion it may be noted that Kummer used as the uniformizing prime element π the prime element ϖ , and Šafarevič [4] the prime element $\zeta-1$, when interpreted by our method. The distinction is quite parallel to that which exists between the Šafarevič E -function and the F -function of Dwork [6].

References.

- [1] D. HILBERT, *Die Theorie der algebraischen Zahlkörper*, Jber. d. Deut. Math.-Ver., 4 (1897), 175-546.
- [2] E. ARTIN und H. HASSE, *Die beiden Ergänzungssätze zum Reziprozitätsgesetz der l^n -ten Potenzreste im Körper der l^n -ten Einheitswurzeln*, Abh. Math. Sem., Hamburg. Univ., 4 (1928), 146-162.
- [3] H. HASSE, *Bericht über neuere Untersuchungen und Probleme aus der Theorie*

der algebraischen Zahlkörper, Berlin, Teil I, Ia, II. 1927, 1930.

- [4] I. R. ŠAFAREVIČ, *A general reciprocity law*, Amer. Math. Soc. Transl., Ser. 2, 4 (1956), 13–106.
- [5] M. KNESER, *Zum expliziten Reziprozitätsgesetz von I.R. Šafarevič*, Math. Nachr., 6 (1952), 89–96.
- [6] B. DWORK, *Norm residue symbol in local number fields*, Abh. Math. Sem., Univ. Hamburg, 22 (1958), 180–190.