J. Math. Soc. Japan
Vol. 20, Nos. 1-2, 1968

On explicit formulas for the norm residue symbol

Dedicated to Professor Shôkichi Iyanaga on his 60th birthday

By Kenkichi IWASAWA*)

(Received Dec. 1, 1966)

Let p be an odd prime and let $\boldsymbol{Z}_p$ and $\boldsymbol{Q}_p$ denote the ring of p-adic integers and the field of p-adic numbers respectively. For each integer $n \geqq 0$, let $q_n = p^{n+1}$ and let Φ_n denote the local cyclotomic field of q_n-th roots of unity over $\boldsymbol{Q}_p$. We fix a primitive q_n-th root of unity ζ_n in Φ_n so that $\zeta_{n+1}^p = \zeta_n$, and put $\pi_n = 1 - \zeta_n$; π_n generates the unique prime ideal $\mathfrak{p}_n$ in the ring $\mathfrak{o}_n$ of local integers in Φ_n. Let $(\alpha, \beta)_n$ denote Hilbert's norm residue symbol in Φ_n for the power q_n and let

$$(\alpha, \beta)_n = \zeta_n^{[\alpha, \beta]_n}$$

with $[\alpha, \beta]_n$ in $\boldsymbol{Z}_p$, well determined mod q_n. The classical formulas for $[\alpha, \beta]_n$ state that

$$[\zeta_n, \beta]_n = q_n^{-1} T_n(\log \beta), \qquad \beta \in 1 + \mathfrak{p}_n, \quad n \geqq 0,$$

$$[\pi_n, \beta]_n = -q_n^{-1} T_n(\zeta_n \pi_n^{-1} \log \beta), \qquad \beta \in 1 + \mathfrak{p}_n, \quad n \geqq 0,$$

$$[\alpha, \beta]_0 = -q_0^{-1} T_0\left(\zeta_0 \alpha^{-1} \frac{d\alpha}{d\pi_0} \log \beta\right), \qquad \alpha \in 1 + \mathfrak{p}_0, \quad \beta \in 1 + \mathfrak{p}_0^2,$$

where T_n denotes the trace from Φ_n to $\boldsymbol{Q}_p$[1].

In a previous note [7], we have announced formulas for $[\alpha, \beta]_n$ which generalize the above formulas of Artin-Hasse. In the present paper, we shall prove those formulas and then discuss some related results.

As in the above, we retain most of the notations introduced in our earlier paper [6]. In particular, we denote by N_n the norm from Φ_n to $\boldsymbol{Q}_p$, and by $T_{n,m}$ and $N_{n,m}$ the trace and the norm, respectively, from Φ_m to Φ_n, $m \geqq n \geqq 0$; for an automorphism σ of the union Φ of all Φ_n, $n \geqq 0$, we denote by $\kappa(\sigma)$ the

---

*) The present research was supported in part by the National Science Foundation grant NSF-GP-4361.

1) See [1], [2], [5]. For the general theory of the norm residue symbol needed in the following, see [2], Chap. 12 or [4], II, § 11, § 19. It is to be noted that the symbol $(\alpha, \beta)_n$ in [2] is the inverse of the same symbol in [4]. Here we follow the definition of $(\alpha, \beta)_n$ in [2] as we did in [7].

unique p-adic unit such that $\zeta_n^\sigma=\zeta_n^{\kappa(\sigma)}$ for every $n\geqq 0$[2].

1. We shall first prove several elementary lemmas. For $n\geqq 0$, we denote by ν_n the normalized valuation on Φ_n such that $\nu_n(\pi_n)=1$.

LEMMA 1. *Let* $\mathfrak{d}_n$ *be the different of* $\Phi_n/\boldsymbol{Q}_p: \mathfrak{d}_n=q_n\mathfrak{p}_n^{-p^n}$. *Then*

$$T_n(\mathfrak{d}_n\log(1+\mathfrak{p}_n))\equiv 0 \qquad \bmod q_n\,.$$

PROOF. Since the multiplicative group $(1+\mathfrak{p}_n)/(1+\mathfrak{p}_n^2)$ is generated by the coset of ζ_n, we have $\log(1+\mathfrak{p}_n)=\log(1+\mathfrak{p}_n^2)$. We shall show that $T_n(\mathfrak{d}_n\log\alpha)\equiv 0 \bmod q_n$, or, equivalently, $\nu_n(q_n\log\alpha)\geqq 2p^n$, for any α in $1+\mathfrak{p}_n^2$. Let $\alpha=1-\beta$ with β in $\mathfrak{p}_n^2$ so that $\log\alpha=-\sum_{i=1}^{\infty}i^{-1}\beta^i$. It is sufficient to show $\nu_n(q_ni^{-1}\beta^i)\geqq 2p^n$ for $i\geqq 1$. Let p^e $(e\geqq 0)$ be the exact power of p dividing i. Then $\nu_n(q_ni^{-1}\beta^i)\geqq(n+1-e)(p-1)p^n+2i\geqq(n+1-e)(p-1)p^n+2p^e$. If $e\leqq n$, then clearly $(n+1-e)(p-1)p^n+2p^e\geqq(p-1)p^n\geqq 2p^n$. If $e>n$, then $(n+1-e)(p-1)p^n+2p^e=(2+2(p^{e-n}-1)-(e-n-1)(p-1))p^n\geqq 2p^n$ because $p^{e-n}-1=(1+p-1)^{e-n}-1\geqq(e-n)(p-1)$. Thus $\nu_n(q_ni^{-1}\beta^i)\geqq 2p^n$ in either case.

LEMMA 2.

i) $$q_m^{-1}T_m(\mathfrak{d}_m\log(1+\mathfrak{p}_n))\equiv 0 \bmod q_n\,,\qquad m\geqq 2n+1\,,$$

ii) $$q_m^{-1}T_m(\mathfrak{d}_m\log(1+\mathfrak{p}_n^{p^n}))\equiv 0 \bmod q_n\,,\qquad m\geqq n+1\,,$$

iii) $$q_m^{-1}T_m(\mathfrak{d}_m\log(1+\mathfrak{p}_n^{2p^n}))\equiv 0 \bmod q_n\,,\qquad m\geqq n\,.$$

PROOF. Clearly $T_{n,m}(\mathfrak{d}_m)=T_{n,m}(q_m\mathfrak{p}_0^{-1})$ is contained in $p^{m-n}q_m\mathfrak{p}_0^{-1}$, and if $m\geqq 2n+1$, the latter is contained in $p^{n+1}q_m\mathfrak{p}_0^{-1}=q_m\mathfrak{d}_n$. Hence, for $m\geqq 2n+1$, $q_m^{-1}T_m(\mathfrak{d}_m\log(1+\mathfrak{p}_n))=q_m^{-1}T_n(T_{n,m}(\mathfrak{d}_m)\log(1+\mathfrak{p}_n))$ is contained in $T_n(\mathfrak{d}_n\log(1+\mathfrak{p}_n))$, and i) follows from Lemma 1.

Since $(1+\mathfrak{p}_n^{p^n})/(1+\mathfrak{p}_n^{p^n+1})$ is generated by the coset of ζ_0, we have $\log(1+\mathfrak{p}_n^{p^n})=\log(1+\mathfrak{p}_n^{p^n+1})=\mathfrak{p}_n^{p^n+1}$. Hence $q_m^{-1}T_m(\mathfrak{d}_m\log(1+\mathfrak{p}_n^{p^n}))=T_m(\mathfrak{p}_n)\equiv 0 \bmod p^m$, and ii) holds for $m\geqq n+1$. iii) can be proved similarly by using $\log(1+\mathfrak{p}_n^{2p^n})=\mathfrak{p}_n^{2p^n}=\mathfrak{p}_0^2$ and $T_m(\mathfrak{p}_0)\equiv 0 \bmod q_m$.

Let Λ denote the ring of formal power series in T with coefficients in $\boldsymbol{Z}_p: \Lambda=\boldsymbol{Z}_p[[T]]$. For any nonzero element ξ in $\mathfrak{o}_n$, there exists a power series $f(T)$ in Λ such that

$$\xi=f(\pi_n)\,,$$

$$f(T)=\sum_{i=s}^{\infty}a_iT^i\,,\qquad a_i\in\boldsymbol{Z}_p,\ s=\nu_n(\xi)\geqq 0\,.$$

Such $f(T)$ will be simply called a power series for ξ. Let

2) However, $(\alpha,\beta)_n$ in the formulas of [6], §3, is the inverse of the same symbol in the present paper. See the footnote 1).

$$\frac{d\xi}{d\pi_n} = f'(\pi_n),$$

$$\delta_n(\xi) = \frac{\zeta_n}{\xi} \frac{d\xi}{d\pi_n},$$

where $f'(T)$ denotes the formal derivative of $f(T)$ with respect to T. Since a power series for ξ such as $f(T)$ is not unique for ξ, $d\xi/d\pi_n$ and $\delta_n(\xi)$ are not uniquely determined by ξ. However we can prove the following lemma on the values taken by $\delta_n(\xi)$.

LEMMA 3. *The values of $\delta_n(\xi)$ which are obtained from all possible power series for ξ fulfil a residue class of $\mathfrak{p}_n^{-1} \bmod \mathfrak{d}_n$.*

PROOF. It is clear from the definition that $\delta_n(\xi_n)$ always belongs to $\mathfrak{p}_n^{-1}$. In general, let $f(T)$ and $g(T)$ be power series in Λ such that $f(\pi_n)=g(\pi_n)$. Then

$$f(T)=g(T)+u(T)d(T),$$

where $u(T)$ is a certain power series in Λ and $d(T)=\sum_{i=0}^{p-1}(1-T)^{ip^n}$ is the minimal polynomial of $\pi_n=1-\zeta_n$ over $\boldsymbol{Q}_p$[3]. Differentiating the both sides, we obtain

$$f'(\pi_n)=g'(\pi_n)+u(\pi_n)d'(\pi_n).$$

Since $\mathfrak{d}_n=(d'(\pi_n))$, it follows that

$$f'(\pi_n)\equiv g'(\pi_n) \qquad \bmod u(\pi_n)\mathfrak{d}_n.$$

Now, suppose that both $f(T)$ and $g(T)$ are power series for ξ. Then the coefficient of T^i vanishes for $0\leqq i<s=\nu_n(\xi)$ in both $f(T)$ and $g(T)$. Since $d(0)=p\neq 0$, the same holds for the coefficient of T^i in $u(T)$ for $0\leqq i<s$. Hence $\nu_n(u(\pi_n))\geqq s$ and it follows from the above congruence that

$$\zeta_n\xi^{-1}f'(\pi_n)\equiv\zeta_n\xi^{-1}g'(\pi_n) \qquad \bmod \mathfrak{d}_n.$$

On the other hand, let η be any element of $\mathfrak{d}_n=(d'(\pi_n))$. Then there is a power series $v(T)$ in Λ such that $\eta=\zeta_n v(\pi_n)d'(\pi_n)$. Let

$$h(T)=(1+v(T)d(T))f(T).$$

Then $h(T)$ is also a power series for ξ and $\zeta_n\xi^{-1}h'(\pi_n)=\zeta_n\xi^{-1}f'(\pi_n)+\eta$. Therefore the lemma is proved.

In the following, we regard $\delta_n(\xi)$ as a multi-valued function of $\xi\neq 0$ in $\mathfrak{o}_n$, representing any such value as described above.

LEMMA 4.

i) *For $\xi\neq 0$ and $\eta\neq 0$ in $\mathfrak{o}_0$,*

$$\delta_n(\xi\eta)\equiv\delta_n(\xi)+\delta_n(\eta) \qquad \bmod \mathfrak{d}_n.$$

ii) *For any $\xi\neq 0$ in $\mathfrak{o}_n$ and for any automorphism σ of Φ,*

3) See [2], p. 151.

$$\delta_n(\xi^\sigma)\equiv\kappa(\sigma)\delta_n(\xi)^\sigma \qquad \bmod \mathfrak{d}_n .$$

iii) *For $m\geqq n$ and for any unit ξ in $\mathfrak{o}_n$,*

$$\delta_m(\xi)\equiv p^{m-n}\delta_n(\xi) \qquad \bmod \mathfrak{d}_m .$$

PROOF. i) follows immediately from the fact that if $f(T)$ is a power series for ξ and $g(T)$ a power series for η, then $f(T)g(T)$ is a power series for $\xi\eta$. To prove ii), let

$$u(T)=1-(1-T)^{\kappa(\sigma)}=\kappa(\sigma)T+\cdots .$$

Then $u(T)$ is a power series for π_n^σ and

$$u'(\pi_n)=\kappa(\sigma)(1-\pi_n)^{\kappa(\sigma)-1}=\kappa(\sigma)\zeta_n^{\sigma-1} .$$

Let $f(T)$ be a power series for ξ. Then $f(u(T))$ is a power series for ξ^σ, and

$$\begin{aligned}\delta_n(\xi^\sigma)&=\zeta_n(\xi^\sigma)^{-1}f'(u(\pi_n))u'(\pi_n)=\zeta_n(\xi^{-1})^\sigma f'(\pi_n)^\sigma\kappa(\sigma)\zeta_n^{\sigma-1}\\ &=\kappa(\sigma)(\zeta_n\xi^{-1}f'(\pi_n))^\sigma=\kappa(\sigma)\delta_n(\xi)^\sigma .\end{aligned}$$

Finally, let ξ be a unit in $\mathfrak{o}_n$. Then ξ is also a unit in $\mathfrak{o}_m$ and every power series $g(T)$ such that $g(\pi_m)=\xi$ is a power series for ξ in $\mathfrak{o}_m$. Let $f(T)$ be a power series for ξ in $\mathfrak{o}_n$. Since $f(\pi_n)=\xi$, $\pi_n=1-(1-\pi_m)^{p^{m-n}}$, $f(1-(1-T)^{p^{m-n}})$ is a power series for ξ in $\mathfrak{o}_m$. Computing $d\xi/d\pi_m$ by means of this power series, we obtain immediately the formula in iii). Note that the both sides of the congruence in iii) are well determined mod $\mathfrak{d}_m$ because $\mathfrak{d}_m=p^{m-n}\mathfrak{d}_n$.

Let ξ now be an arbitrary element of the multiplicative group Φ_n^* of Φ_n, i.e., an arbitrary nonzero element of Φ_n. We write ξ in the form $\xi=\xi_1/\xi_2$ with $\xi_1\neq 0$, $\xi_2\neq 0$ in $\mathfrak{o}_n$, and define

$$\delta_n(\xi)=\delta_n(\xi_1)-\delta_n(\xi_2) .$$

By Lemma 4, i), we see that the values of $\delta_n(\xi)$ again fulfil a residue class of $\mathfrak{p}_n^{-1}$ mod $\mathfrak{d}_n$. Furthermore, i), ii) of Lemma 4 now hold for any ξ and η in Φ_n^*. Hence δ_n defines a so-called κ-homomorphism

$$\delta_n:\Phi_n^*\to\mathfrak{p}_n^{-1}/\mathfrak{d}_n .$$

δ_n is continuous in the sense that if $\xi\equiv 1 \bmod \mathfrak{p}_n^k$, $k\gg 0$, then $\delta_n(\xi)\equiv 0 \bmod \mathfrak{d}_n$.

LEMMA 5. *For $m\geqq n$ and for ξ in Φ_m^*,*

$$\delta_n(N_{n,m}(\xi))\equiv p^{-(m-n)}T_{n,m}(\delta_m(\xi)) \qquad \bmod \mathfrak{d}_n .$$

PROOF. Since $\mathfrak{d}_m=p^{m-n}\mathfrak{d}_n$, the both sides of the above are well determined mod $\mathfrak{d}_n$. By Lemma 4, i), it is sufficient to prove the lemma for $\xi\equiv\pi_m$ and for a unit ξ in $\mathfrak{o}_m$. Since

$$\begin{aligned}&N_{n,m}(\pi_m)=\pi_n , \qquad T_{n,m}(\zeta_m\pi_m^{-1})=p^{m-n}\zeta_n\pi_n^{-1} ,\\ &\delta_n(\pi_n)=\zeta_n\pi_n^{-1} , \qquad \delta_m(\pi_m)=\zeta_m\pi_m^{-1} ,\end{aligned}$$

the lemma holds for $\xi=\pi_m$. Let ξ be a unit in $\mathfrak{o}_m$. When σ ranges over all Galois automorphisms of Φ_m/Φ_n, we obtain from Lemma 4, ii), iii) that

$$p^{m-n}\delta_n(N_{n,m}(\xi))\equiv\delta_m(N_{n,m}(\xi))\equiv\sum_\sigma\delta_m(\xi^\sigma)$$

$$\equiv\sum_\sigma\kappa(\sigma)\delta_m(\xi)^\sigma \qquad \mathrm{mod}\ \mathfrak{d}_m\,.$$

Apply $p^{-(m-n)}T_{n,m}$ to the above. Since

$$T_{n,m}(\mathfrak{d}_m)=T_{n,m}(q_m\mathfrak{p}_0^{-1})=p^{m-n}q_m\mathfrak{p}_0^{-1}=p^{m-n}\mathfrak{d}_m\,,$$

we have

$$p^{m-n}\delta_n(N_{n,m}(\xi))\equiv p^{-(m-n)}\sum_\sigma\kappa(\sigma)T_{n,m}(\delta_m(\xi)) \qquad \mathrm{mod}\ \mathfrak{d}_m\,.$$

Here

$$\sum_\sigma\kappa(\sigma)\equiv\sum_{i=0}^{p^{m-n}-1}(1+iq_n)\equiv p^{m-n} \qquad \mathrm{mod}\ q_m\,.$$

Since ξ is a unit, $\delta_m(\xi)$ belongs to $\mathfrak{o}_m$. Hence $p^{-(m-n)}T_{n,m}(\delta_m(\xi))$ is in $\mathfrak{o}_n$, and we obtain from the above

$$p^{m-n}\delta_n(N_{n,m}(\xi))\equiv T_{n,m}(\delta_m(\xi)) \qquad \mathrm{mod}\ \mathfrak{d}_m\,,$$

which implies the congruence of the lemma.

2. For α in Φ_n^* and β in $1+\mathfrak{p}_n$, $n\geqq 0$, let

$$\langle\alpha,\beta\rangle_n=-q_n^{-1}T_n(\delta_n(\alpha)\log\beta)^{4)}\,.$$

Although the value of $\langle\alpha,\beta\rangle_n$ depends upon the choice of the value of $\delta_n(\alpha)$, it is, in certain cases, well determined modulo a high power of p.

LEMMA 6. *Let $m\geqq n$ and let α be an arbitrary element of Φ_m^*. In each one of the following three cases, the value of $\langle\alpha,\beta\rangle_m$ is well determined* mod q_n:

i) *$m\geqq 2n+1$ and β in $1+\mathfrak{p}_n$,*

ii) *$m\geqq n+1$ and β in $1+\mathfrak{p}_n^{p^n}$,*

iii) *$m\geqq n$ and β in $1+\mathfrak{p}_n^{2p^n}$.*

PROOF. Since $\delta_m(\alpha)$ is well determined mod $\mathfrak{d}_m$, the lemma follows immediately from Lemma 2.

In these three cases, we have

$$\langle\alpha_1\alpha_2,\beta\rangle_m\equiv\langle\alpha_1,\beta\rangle_m+\langle\alpha_2,\beta\rangle_m \qquad \mathrm{mod}\ q_n\,,$$

$$\langle\alpha,\beta_1\beta_2\rangle_m\equiv\langle\alpha,\beta_1\rangle_m+\langle\alpha,\beta_2\rangle_m \qquad \mathrm{mod}\ q_n\,,$$

for α, α_1, α_2 in Φ_m^* and β, β_1, β_2 in Φ_n satisfying respective conditions.

LEMMA 7. *Let $l\geqq m\geqq n$. Let α be an element of Φ_l^*, and β an element*

---

4) The symbol $\langle\alpha,\beta\rangle_n$ here is completely different from the same symbol defined in [**6**], §1, p. 52.

of $1+\mathfrak{p}_n$. *Suppose that* β *and* m *satisfy one of the three conditions in Lemma* 6. *Then*

$$\langle N_{m,l}(\alpha), \beta\rangle_m \equiv \langle \alpha, \beta\rangle_l \qquad \bmod q_n .$$

PROOF. By Lemma 5,

$$\delta_m(N_{m,l}(\alpha)) \equiv p^{-(l-m)}T_{m,l}(\delta_l(\alpha)) \qquad \bmod \mathfrak{d}_m .$$

Multiply the both sides of the above by $-\log\beta$ and apply $q_m^{-1}T_m$. The congruence of the lemma then follows immediately from Lemma 2.

For $n\geqq 0$, $i\geqq 1$, let

$$\eta_i^{(n)} = 1-\pi_n^i .$$

For any $k\geqq 0$, the elements $\eta_i^{(n)}$, $i\geqq k$, generate the compact multiplicative group $1+\mathfrak{p}_n^k$ topologically. We shall next prove a key lemma for such $\eta_i^{(n)}$.

LEMMA 8. *For* $i\geqq 1$, $j\geqq((n+2)(p-1)+1)p^{n-1}$,

$$[\eta_i^{(n)}, \eta_j^{(n)}]_n = \langle \eta_i^{(n)}, \eta_j^{(n)}\rangle_n .$$

PROOF. Since n is fixed throughout the following proof, we shall write η_i for $\eta_i^{(n)}$, $i\geqq 1$. By Lemma 6, iii) $\langle\eta_i, \eta_j\rangle_n$ is well determined mod q_n. Hence it is sufficient to prove the lemma for the following particular value of $\delta_n(\eta_i)$:

$$\delta_n(\eta_i) = -\zeta_n \sum_{r=1}^{\infty} i\pi_n^{ir-1} .$$

Since

$$\log \eta_j = -\sum_{s=1}^{\infty} s^{-1}\pi_n^{js} ,$$

we have

$$\langle \eta_i, \eta_j\rangle_n = -q_n^{-1} \sum_{r,s\geqq 1} is^{-1}T_n(\zeta_n \pi_n^{ir+js-1})$$

$$= -q_n^{-1} \sum_{\substack{r,s\geqq 1\\(r,s)=1}} \sum_{u=1}^{\infty} i(us)^{-1}T_n(\zeta_n\pi_n^{u(ir+js)-1}) .$$

On the other hand, it is known that

$$[\eta_i, \eta_j]_n = \sum_{\substack{r,s\geqq 1\\(r,s)=1}} (ir'+js')[\pi_n, \eta_{ir+js}]_n ,$$

where for each pair r, s, the integers r', s' are chosen so that $rs'-sr'=1$[5]. Using Artin-Hasse's formula

$$[\pi_n, \beta]_n = -q_n^{-1}T_n(\zeta_n\pi_n^{-1}\log\beta) , \qquad \beta\in 1+\mathfrak{p}_n ,$$

we obtain

5) See [**3**].

$$[\eta_i, \eta_j]_n = -q_n^{-1} \sum_{\substack{r,s\geq 1\\(r,s)=1}} (ir'+js')T_n(\zeta_n \pi_n^{-1} \log \eta_{ir+js})$$

$$= q_n^{-1} \sum_{\substack{r,s\geq 1\\(r,s)=1}} \sum_{u=1}^{\infty} (ir'+js')u^{-1}T_n(\zeta_n \pi_n^{u(ir+js)-1}) .$$

Since $rs'-sr'=1$, we see that

$$[\eta_i, \eta_j]_n - \langle \eta_i, \eta_j \rangle_n = q_n^{-1} \sum_{\substack{r,s\geq 1\\(r,s)=1}} \sum_{u=1}^{\infty} s'(ir+js)(us)^{-1}T_n(\zeta_n \pi_n^{u(ir+js)-1}) .$$

However

$$\begin{aligned} q_n^{-1} \sum_{u=1}^{\infty} (ir+js)u^{-1}T_n(\zeta_n \pi_n^{u(ir+js)-1}) &= -q_n^{-1}(ir+js)T_n(\zeta_n \pi_n^{-1} \log \eta_{ir+js}) \\ &= (ir+js)[\pi_n, \eta_{ir+js}]_n \\ &= [\pi_n^{ir+js}, 1-\pi_n^{ir+js}]_n \\ &\equiv 0 \qquad \bmod q_n^{6)} . \end{aligned}$$

Hence

$$[\eta_i, \eta_j]_n - \langle \eta_i, \eta_j \rangle_n$$

$$\equiv q_n^{-1} \sum_{r,s}{}' \sum_{u=1}^{\infty} s'(ir+js)(us)^{-1}T_n(\zeta_n \pi_n^{u(ir+js)-1}) \qquad \bmod q_n ,$$

where the outer sum on the right is taken over all pairs of integers $r, s \geq 1$ with $(r, s)=1$ and with s divisible by p. We shall next show that each term on the right hand side of the above is divisible by q_n.

With r, s, and u fixed, let p^e be the exact power of p dividing us. Then $e \geq 1$ by the assumption on s. Since $j \geq ((n+2)(p-1)+1)p^{n-1}$, we have

$$\begin{aligned} \nu_n(q_n^{-1}(us)^{-1}\zeta_n \pi_n^{u(ir+js)-1}) &= u(ir+js)-1-(n+1+e)(p-1)p^n \\ &\geq ((n+2)(p-1)+1)p^{n-1+e}-(n+1+e)(p-1)p^n . \end{aligned}$$

For real x, let $f(x)=((n+2)(p-1)+1)p^{n-1+x}-(n+1+x)(p-1)p^n$. Then $f(1)=p^n$ and $f'(x) \geq 0$ for $x \geq 1$. Hence $f(x) \geq p^n$ for $x \geq 1$. Since $e \geq 1$, it follows that

$$\nu_n(q_n^{-1}(us)^{-1}\zeta_n \pi_n^{u(ir+js)-1}) \geq p^n$$

so that

$$q_n^{-1}s'(ir+js)(us)^{-1}T_n(\zeta_n \pi_n^{u(ir+js)-1}) \equiv 0 \qquad \bmod q_n .$$

Thus we obtain

$$[\eta_i, \eta_j]_n \equiv \langle \eta_i, \eta_j \rangle_n \qquad \bmod q_n ,$$

and the lemma is proved. Note that $[\eta_i, \eta_j]_n$ is a p-adic integer, determined only mod q_n. Note also that if $j > ((n+1)(p-1)+1)p^n$, then η_j is a q_n-th power of an element in $1+\mathfrak{p}_n^{p^n+1}$ and the equality of the lemma can be verified immedi-

6) In general, $(\alpha, 1-\alpha)_n=1$.

ately because both sides are simply zero.

LEMMA 9. *Let* $m \geqq 3n+1$. *Then*

$$[N_{n,m}(\alpha), \beta]_n = \langle \alpha, \beta \rangle_m, \qquad \alpha \in \Phi_m^*, \ \beta \in 1+\mathfrak{p}_n.$$

PROOF. We first note that $\langle \alpha, \beta \rangle_m$ is well determined mod q_n by Lemma 6, i). Let $k=((m-2n)(p-1)+1)p^m$. It follows from $m \geqq 3n+1$, $p \geqq 3$ that $k \geqq ((m+2)(p-1)+1)p^{m-1}$. Since β is in $1+\mathfrak{p}_n$, β^{p^n} is contained in $1+\mathfrak{p}_n^{p^n}$, and $\beta^{p^{m-n}}$ in $1+p^{m-2n}\mathfrak{p}_n^{p^n}=1+\mathfrak{p}_m^k$. Hence $\beta^{p^{m-n}}$ is the limit of a sequence of certain products of $\eta_j^{(m)}$, $j \geqq ((m+2)(p-1)+1)p^{m-1}$. Therefore it follows from Lemma 8 that

$$[\eta_i^{(m)}, \beta^{p^{m-n}}]_m = \langle \eta_i^{(m)}, \beta^{p^{m-n}} \rangle_m, \qquad i \geqq 1.$$

Using the well known properties of the norm residue symbol, we then have

$$\begin{aligned}(N_{n,m}(\eta_i^{(m)}), \beta)_n &= (\eta_i^{(m)}, \beta)_m^{p^{m-n}} = (\eta_i^{(m)}, \beta^{p^{m-n}})_m \\ &= \zeta_m^{[\eta_i^{(m)}, \beta^{p^{m-n}}]_m} = \zeta_m^{\langle \eta_i^{(m)}, \beta^{p^{m-n}} \rangle_m} \\ &= \zeta_m^{p^{m-n}\langle \eta_i^{(m)}, \beta \rangle_m}.\end{aligned}$$

Since the first term of the above is a q_n-th root of unity,

$$q_n p^{m-n} \langle \eta_i^{(m)}, \beta \rangle_m \equiv 0 \qquad \text{mod } q_m.$$

Therefore $\langle \eta_i^{(m)}, \beta \rangle_m$ is a p-adic integer, and the last term of the above equalities can be written as $\zeta_n^{\langle \eta_i^{(m)}, \beta \rangle_m}$. Hence

$$[N_{n,m}(\eta_i^{(m)}), \beta]_n = \langle \eta_i^{(m)}, \beta \rangle_m, \qquad i \geqq 1.$$

Since $1+\mathfrak{p}_m$ is topologically generated by $\eta_i^{(m)}$, $i \geqq 1$, it follows that the lemma holds for any α in $1+\mathfrak{p}_m$.

If α is an element of the group V of $(p-1)$-*st* roots of unity in Φ_m, then $[N_{n,m}(\alpha^{p-1}), \beta]_n = \langle \alpha^{p-1}, \beta \rangle_m = 0$ so that $[N_{n,m}(\alpha), \beta]_n = \langle \alpha, \beta \rangle_m = 0$. Hence the lemma again holds for such α. Let $\alpha = \pi_m$. Then $N_{n,m}(\alpha) = \pi_n$ and $q_m^{-1}T_{n,m}(\delta_m(\alpha)) = q_m^{-1}T_{n,m}(\zeta_m \pi_m^{-1}) = q_n^{-1}\zeta_n \pi_n^{-1}$. Hence the equality of the lemma in this case is nothing but the formula of Artin-Hasse. Since the group Φ_m^* is generated by π_m, V, and $1+\mathfrak{p}_m$, the lemma is completely proved.

We are now able to prove the main result of the paper. For each $n \geqq 0$, let Φ_n' denote the intersection of all $N_{n,m}(\Phi_m^*)$, $m \geqq n$. Then

$$\Phi_n^* = U_0 \times \Phi_n', \qquad \Phi_n' = N_{n,m}(\Phi_m'), \qquad m \geqq n,$$

with $U_0 = 1+p\boldsymbol{Z}_p$[7]. It follows in particular that for each α in Φ_n' and for any $m \geqq n$, there exists an element α' in Φ_m' such that $\alpha = N_{n,m}(\alpha')$. Any such α'

7) See [6], § 2, Proposition 9.

will be denoted by $N_{n,m}^{-1}(\alpha)$.

THEOREM 1. *For α in Φ_n', β in $1+\mathfrak{p}_n$,*

$$[\alpha, \beta]_n = \langle N_{n,m}^{-1}(\alpha), \beta\rangle_m$$

for any $m \geqq 2n+1$. More explicitly,

$$(\alpha, \beta)_n = \zeta_n^{-q_m^{-1}T_m(\zeta_m \alpha'^{-1}(d\alpha'/d\pi_m)\log \beta)}$$

with $\alpha' \in \Phi_m'$, $N_{n,n}(\alpha')=\alpha$, $m \geqq 2n+1$.

PROOF. Let $l \geqq m$, $3n+1$ and $\alpha''=N_{m,l}^{-1}(\alpha')$ so that $\alpha'=N_{m,l}(\alpha'')$, $\alpha=N_{n,l}(\alpha'')$. By Lemma 9,

$$[\alpha, \beta]_n = \langle \alpha'', \beta\rangle_l,$$

and by Lemma 7,

$$\langle \alpha', \beta\rangle_m \equiv \langle \alpha'', \beta\rangle_l \mod q_n.$$

Hence

$$[\alpha, \beta]_n = \langle \alpha', \beta\rangle_m.$$

Let $\alpha=\zeta_n$. Then $N_{n,m}^{-1}(\alpha)=\zeta_m$. Since $\delta_m(\zeta_m)=\zeta_m\zeta_m^{-1}(d\xi_m/d\pi_m)=-1$, the theorem gives us the first formula of Artin-Hasse:

$$[\zeta_n, \beta]_n = q_n^{-1}T_n(\log \beta), \qquad \beta \in 1+\mathfrak{p}_n.$$

Next, let $\alpha=\pi_n$. Using the equalities for π_n and π_m given in the proof of Lemma 5, we see immediately that Theorem 1 in this case gives us the second formula of Artin-Hasse:

$$[\pi_n, \beta]_n = -q_n^{-1}T_n(\zeta_n\pi_n^{-1}\log \beta), \qquad \beta \in 1+\mathfrak{p}_n.$$

3. In Theorem 1, if $\beta-1$ is divisible by a higher power of $\mathfrak{p}_n$, then the formula $[\alpha, \beta]_n=\langle N_{n,m}^{-1}(\alpha), \beta\rangle_m$ holds with a smaller m. The proof of the theorem shows that

$$[\alpha, \beta]_n = \langle N_{n,n+1}^{-1}(\alpha), \beta\rangle_{n+1} \qquad \alpha \in \Phi_n', \ \beta \in 1+\mathfrak{p}_n^{p^n},$$

$$[\alpha, \beta]_n = \langle \alpha, \beta\rangle_n, \qquad \alpha \in \Phi_n', \ \beta \in 1+\mathfrak{p}_n^{2p^n},$$

We shall next prove that the second equality holds not only for α in Φ_n' but also for arbitrary α in Φ_n^*. Since $\Phi_n^*=U_0\times\Phi_n'$, it is sufficient to prove it for α in $U_0=1+p\mathbf{Z}_p$.

For integers $a \geqq 1$, $n \geqq 0$, let

$$s_n(a) = p^{-n}\sum_{\substack{0\leqq i\leqq a\\ p^n \mid i}}(-1)^i i\binom{a}{i} = \sum_{0\geqq kp^n\leqq a}(-1)^k k\binom{a}{kp^n}.$$

Using

$$\binom{a}{kp^n} \equiv \binom{ap}{kp^{n+1}} \qquad \bmod p^{8)},$$

one sees immediately that

$$s_n(a) \equiv s_{n+1}(ap) \qquad \bmod p.$$

Let $a>0$, $(a, p)=1$, $n>0$. Then $kp^n \leqq a$ implies $kp^n \leqq a-1$. Hence

$$\begin{aligned} s_n(a) &= \sum_{0 \leqq kp^n \leqq a-1} (-1)^k \frac{a}{a-kp^n} k\binom{a-1}{kp^n} \\ &\equiv \sum_{0 \leqq kp^n \leqq a-1} (-1)^k k\binom{a-1}{kp^n} \qquad \bmod p, \end{aligned}$$

namely,

$$s_n(a) \equiv s_n(a-1) \qquad \bmod p.$$

LEMMA 10. *Let* $a \geqq 2p^n$, $n \geqq 0$. *Then*

$$s_n(a) \equiv 0 \qquad \bmod p.$$

PROOF. We use induction on n. For $n=0$,

$$\begin{aligned} s_0(a) &= \sum_{k=0}^{a} (-1)^k k\binom{a}{k} = \sum_{k=1}^{a} (-1)^k a\binom{a-1}{k-1} \\ &= -a(1-1)^{a-1} = 0. \end{aligned}$$

Let $n>0$ and $a=bp+c$, $b \geqq 0$, $p>c \geqq 0$. Then we have $bp \geqq 2p^n$, and we see from the above remarks and from the induction assumption on $s_{n-1}(b)$, $b \geqq 2p^{n-1}$ that

$$s_n(a) \equiv s_n(bp) \equiv s_{n-1}(b) \equiv 0 \qquad \bmod p.$$

LEMMA 11. *Let* $a \geqq 2p^n$, $n \geqq 0$. *Then*

$$T_n(a\zeta_n\pi_n^{a-1}) \equiv 0 \qquad \bmod p^{2n+1}.$$

PROOF. Since

$$T_n(\zeta_n^i) = \begin{cases} 0, & p^n \nmid i, \\ -p^n, & p^n \mid i, \quad p^{n+1} \nmid i, \\ p^{n+1}-p^n, & p^{n+1} \mid i, \end{cases}$$

and since

$$a\zeta_n\pi_n^{a-1} = \sum_{i=0}^{a-1} (-1)^i a\binom{a-1}{i}\zeta_n^{i+1} = -\sum_{i=0}^{a} (-1)^i i\binom{a}{i}\zeta_n^i,$$

we obtain by Lemma 10

8) See [1], Hilfssatz 2.

$$T_n(a\zeta_n\pi_n^{a-1}) = p^n \sum_{\substack{0\leqq i\leqq a \\ p^n | i}} (-1)^i i\binom{a}{i} - p^{n+1} \sum_{\substack{0\leqq i\leqq a \\ p^{n+1} | i}} (-1)^i i\binom{a}{i}$$

$$\equiv p^{2n}s_n(a) \qquad \mathrm{mod}\ p^{2n+1}$$

$$\equiv 0 \qquad \mathrm{mod}\ p^{2n+1}\,.$$

LEMMA 12. *For any ξ in $1+\mathfrak{p}_n^{2p^n}$,*

$$T_n(\delta_n(\xi)) \equiv 0 \qquad \mathrm{mod}\ p^{2n+1}\,.$$

PROOF. Note first that since $T_n(\mathfrak{d}_n)\equiv 0 \bmod p^{2n+1}$, $T_n(\delta_n(\xi))$ is well determind $\bmod p^{2n+1}$ (for any ξ in Φ_n^*). For the proof of the lemma, it suffices to show that for each $a\geqq 2p^n$, there exists an element ξ_a such that $\nu_n(\xi_a-1)=a$ and $T_n(\delta_n(\xi_a))\equiv 0 \bmod p^{2n+1}$. Let $b=ap-(p-1)p^n$ and let

$$\alpha = 1-\pi_n^{ap}\,, \qquad \beta = \exp(p^{-1}\log\alpha)\,.$$

We see from $ap>p^{n+1}$ that β is defined, $\alpha=\beta^p$, and $\nu_n(\beta-1)\geqq b$. Let $f(T)$ be a power series for $\beta-1$ and let

$$(1+f(T))^p = 1+g(T)\,.$$

Then the coefficient of T^i vanishes for $0\leqq i<b$ in both $f(T)$ and $g(T)$. Since $g(\pi_n)=-\pi_n^{ap}$, $ap\geqq b$, we obtain from the proof of Lemma 3 that

$$g'(\pi_n) = p(1+f(\pi_n))^{p-1}f'(\pi_n) \equiv -ap\pi_n^{ap-1} \qquad \mathrm{mod}\ \mathfrak{p}_n^b\mathfrak{d}_n\,.$$

It then follows from $b\geqq 2p^{n+1}-(p-1)p^n > (p-1)p^n = \nu_n(p)$ that

$$\frac{f'(\pi_n)}{1+f(\pi_n)} \equiv -\frac{a\pi^{ap-1}}{1-\pi_n^{ap}} \qquad \mathrm{mod}\ \mathfrak{d}_n$$

so that

$$\delta_n(\beta) \equiv -\sum_{i=1}^{\infty} a\zeta_n\pi_n^{api-1} \qquad \mathrm{mod}\ \mathfrak{d}_n\,.$$

Let

$$\xi_a = (1-\pi_n^a)\beta^{-1}\,.$$

Then $\nu_n(\beta-1)\geqq b>a$ implies $\nu_n(\xi_a-1)=a$. We also see from the above that

$$\delta_n(\xi_a) \equiv \delta_n(1-\pi_n^a)-\delta_n(\beta)$$

$$\equiv -\sum_{i=1}^{\infty} a\zeta_n\pi_n^{ai-1} + \sum_{i=1}^{\infty} a\zeta_n\pi_n^{api-1}$$

$$\equiv -\sum_{\substack{i=1 \\ (i,p)=1}}^{\infty} a\zeta_n\pi_n^{ai-1} \qquad \mathrm{mod}\ \mathfrak{d}_n$$

so that

$$T_n(\delta_n(\xi_a)) \equiv -\sum_{\substack{i=1 \\ (i,p)=1}}^{\infty} T_n(a\zeta_n\pi_n^{ai-1}) \qquad \mathrm{mod}\ p^{2n+1}\,.$$

However, it follows from Lemma 11 that if $(i, p)=1$, then

$$T_n(a\zeta_n\pi_n^{ai-1})=i^{-1}T_n(ai\zeta_n\pi_n^{ai-1})\equiv 0 \qquad \mod p^{2n+1}.$$

Hence $T_n(\delta_n(\xi_a))\equiv 0 \mod p^{2n+1}$, and the lemma is proved.

THEOREM 2. *For any α in Φ_n^* and any β in $1+\mathfrak{p}_n^{2p^n}$, $n\geqq 0$,*

$$[\alpha, \beta]_n=\langle \alpha, \beta\rangle_n,$$

namely

$$(\alpha, \beta)_n=\zeta_n^{-q_nT_n(\zeta_n\alpha^{-1}(d\alpha/d\pi_n))\log\beta}.$$

PROOF. As noted earlier, we need only to prove the theorem for α in U_0. Since $\delta_n(\alpha)=0$ in this case, we have to show

$$(\alpha, \beta)_n=1, \qquad \alpha\in U_0,\ \beta\in 1+\mathfrak{p}_n^{2p^n}.$$

Let

$$\beta=\xi\eta, \qquad \xi\in U_0,\ \eta\in\Phi_n'.$$

Then $(\alpha, \xi)_n=1$ because both α and ξ are powers of $1+p$ with exponents in Z_p and $(1+p, 1+p)_n=1$. Since η is in Φ_n' and α in $1+\mathfrak{p}_n^{2p^n}$, we know that

$$[\eta, \alpha]_n=\langle\eta, \alpha\rangle_n=-q_n^{-1}T_n(\delta_n(\eta)\log\alpha)$$
$$=-q_n^{-1}\log\alpha T_n(\delta_n(\eta))$$

with $\log\alpha$ in pZ_p. On the other hand, it follows from $\beta\equiv 1 \mod \mathfrak{p}_n^{2p^n}$, $\xi\equiv 1 \mod p$ that $\eta\equiv 1 \mod \mathfrak{p}_n^{2p^n}$. Hence $T_n(\delta_n(\eta))\equiv 0 \mod p^{2n+1}$ by Lemma 12. Therefore $[\eta, \alpha]_n\equiv 0 \mod q_n$, $(\eta, \alpha)_n=1$, and

$$(\alpha, \beta)_n=(\alpha, \xi)_n(\alpha, \eta)_n=(\alpha, \xi)_n(\eta, \alpha)_n^{-1}=1.$$

Hence the theorem is proved.

Obviously Theorem 2 is a generalization of the third formula stated in the introduction. We also note that as the proof of the theorem indicates, Lemma 12 is equivalent with the fact that the conductor of the abelian extension $\Phi_n((1+p)^{q_n^{-1}})/\Phi_n$ is a divisor of $\mathfrak{p}_n^{2p^n}$.

4. For $n\geqq 0$, let X_n denote the set of all elements ξ in Φ_n such that

$$T_n(\xi\log(1+\mathfrak{p}_n))\equiv 0 \qquad \mod Z_p.$$

$\mathfrak{X}_n$ is a compact subgroup of the additive group of Φ_n. As we saw in [6], the compact modules $\mathfrak{X}_n$, $n\geqq 0$, play important roles in the theory of cyclotomic fields. In Proposition 14 of that paper, we proved that for each $n\geqq 0$, there exists a unique map

$$\phi_n:\Phi_n'\rightarrow\mathfrak{X}_n/q_n\mathfrak{X}_n$$

such that

$$(\alpha, \beta)_n=\zeta_n^{T_n(\phi_n(\alpha)\log\beta)},$$

for any α in Φ_n' and β in $1+\mathfrak{p}_n$. It was also proved that ψ_n is a surjective κ-homomorphism.

THEOREM 3. *For* $m \geqq 2n+1$,

$$\psi_n(\alpha) = -q_m^{-1} T_{n,m}(\delta_m(N_{n,m}^{-1}(\alpha))), \qquad \alpha \in \Phi_n'.$$

PROOF. Let $\psi_n'(\alpha)$ denote the right hand side of the above. By Theorem 1,

$$[\alpha, \beta]_n = T_n(\psi_n'(\alpha) \log \beta), \qquad \beta \in 1+\mathfrak{p}_n.$$

This shows that $\psi_n'(\alpha)$ is contained in $\mathfrak{X}_n$ and is well determined mod $q_n \mathfrak{X}_n$ for any choice of the value of $\delta_m(N_{n,m}^{-1}(\alpha))$. Hence we abtain a map

$$\psi' : \Phi_n' \rightarrow \mathfrak{X}_n / q_n \mathfrak{X}_n$$

such that

$$(\alpha, \beta)_n = \zeta_n^{T_n(\psi'_n(\alpha) \log \beta)}, \qquad \alpha \in \Phi_n',\ \beta \in 1+\mathfrak{p}_n.$$

The uniqueness of ψ_n then implies $\psi_n' = \psi_n$.

For $m \geqq n \geqq 0$, let $\mathfrak{X}_{n,m}$ denote the set of all elements of the form

$$q_m^{-1} T_{n,m}(\delta_m(\xi))$$

with ξ ranging over Φ_m^* and with $\delta_m(\xi)$ taking all possible values of the multi-valued $\delta_m(\xi)$. $\mathfrak{X}_{n,m}$ is a subgroup of the additive group of Φ_n, containing the open subgroup $q_m^{-1} T_{n,m}(\mathfrak{d}_m) = q_n^{-1} \mathfrak{d}_n$. Since $\Phi_m^* = U_0 \times \Phi_m'$ and $\delta_m(U_0) \equiv 0 \mod \mathfrak{d}_m$, we have

$$\mathfrak{X}_{n,m} = q_m^{-1} T_{n,m}(\delta_m(\Phi_m')) = q_m^{-1} T_{n,m}(\delta_m(N_{n,m}^{-1}(\Phi_n'))).$$

Let $m \geqq 2n+1$. Since $\psi_n : \Phi_n' \rightarrow \mathfrak{X}_n / q_n \mathfrak{X}_n$ is surjective, it follows from Theorem 3 that

$$\mathfrak{X}_n = \mathfrak{X}_{n,m} + q_n \mathfrak{X}_n.$$

However, $\mathfrak{X}_n$ is a profinite p-group and $\mathfrak{X}_{n,m}$ is an open subgroup of $\mathfrak{X}_n$. Hence we obtain from the above that $\mathfrak{X}_n = \mathfrak{X}_{n,m}$ for $m \geqq 2n+1$.

THEOREM 4. *For any* $m \geqq n$,

$$\mathfrak{X}_n = \mathfrak{X}_{n,m}.$$

In particular, $\mathfrak{X}_n = \mathfrak{X}_{n,n}$, *and* $\mathfrak{X}_n$ *consists of all elements of the form*

$$q_n^{-1} \delta_n(\alpha) = q_n^{-1} \zeta_n \alpha^{-1} (d\alpha / d\pi_n), \qquad \alpha \in \Phi_n^*.$$

PROOF. It is sufficient to show that $\mathfrak{X}_{n,m} = \mathfrak{X}_{n,n}$ for $m \geqq n$. By Lemma 5,

$$q_m^{-1} T_{n,m}(\delta_m(\xi)) \equiv q_n^{-1} \delta_n(N_{n,m}(\xi)) \qquad \mod q_n^{-1} \mathfrak{d}_n$$

for any ξ in Φ_m^*. Since $q_n^{-1} \mathfrak{d}_n$ is contained in $\mathfrak{X}_{n,n}$, we see that $\mathfrak{X}_{n,m}$ is a subgroup of $\mathfrak{X}_{n,n}$.

Let ξ be a unit of $\mathfrak{o}_n$ and let $\delta_n(\xi)$ be fixed. By Lemma 4, iii), one value of $\delta_m(\xi)$ is given by $p^{m-n} \delta_n(\xi)$. Hence $q_n^{-1} \delta_n(\xi) = q_m^{-1} T_{n,m}(\delta_m(\xi))$ is contained in

$\mathfrak{X}_{n,m}$. On the other hand, since

$$q_n^{-1}\delta_n(\pi_n) = q_n^{-1}\zeta_n\pi_n^{-1} = q_m^{-1}T_{n,m}(\delta_m(\pi_m)),$$

$q_n^{-1}\delta_n(\pi_n)$ is also contained in $\mathfrak{X}_{n,m}$. Therefore $\mathfrak{X}_{n,n}$ is a subgroup of $\mathfrak{X}_{n,m}$.

In [**6**], the compact module $\mathfrak{X}_n$ was explicitly described as follows[9]: Let G_n denote the Galois group of $\Phi_n/\boldsymbol{Q}_p$ and let

$$\mu_n = q_n^{-1}\zeta_n\pi_n^{-1}$$

$$\theta_n = q_n^{-1}\sum_{i=0}^{n}\zeta_i^{-1}.$$

Then the elements θ_n^σ, $\sigma \in G_n$, form a normal basis of Φ_n over $\boldsymbol{Q}_p$, and $\mathfrak{X}_n$ consists of all elements of the form

$$\sum_\sigma c_\sigma\mu_n^\sigma + \sum_\sigma d_\sigma\theta_n^\sigma$$

with arbitrary p-adic integers c_σ and d_σ satisfying $\sum_\sigma d_\sigma = 0$.

We like to note here that a similar description of the compact module $\log(1+\mathfrak{p}_n)$ can be given as follows: Let

$$\lambda_n = p^{-n}\sum_{i=0}^{n}p^i\pi_i.$$

Then the elements λ_n^σ, $\sigma \in G_n$, also form a normal basis of Φ_n over $\boldsymbol{Q}_p$, and $\log(1+\mathfrak{p}_n)$ consists of all elements of the form

$$ap + \sum_\sigma a_\sigma\lambda_n^\sigma$$

with arbitrary p-adic integers a and a_σ satisfying

$$\sum_\sigma \kappa(\sigma)a_\sigma \equiv 0 \qquad \bmod q_n\text{[10]}.$$

The proof is obtained easily from the result on $\mathfrak{X}_n$ stated above and from the fact that if we put

$$\theta_n' = p^{-n}(-1+\sum_{i=0}^{n}p^i\zeta_i),$$

then we have

$$T_n(\theta_n^\sigma\theta_n'^\tau) = \begin{cases} 1, & \sigma = \tau, \\ 0, & \sigma \neq \tau,\ \sigma, \tau \in G_n. \end{cases}$$

Princeton University

9) See [**6**], § 1, Theorem 1.

10) For σ in G_n, $\kappa(\sigma)$ is defined in the obvious manner. It is a p-adic integer well determined mod q_n.

Bibliography

[1] E. Artin and H. Hasse, Die beiden Ergänzungssätze zum Reziprozitätsgesetz der l^n-ten Potenzrests im Körper der l^n-ten Einheitswurzeln, Abh. Math. Sem. Univ. Hamburg, **6** (1928), 146–162.

[2] E. Artin and J. Tate, Class field theory, Lecture notes at Princeton University, 1951–1952.

[3] H. Hasse, Zum expliziten Reziprozitätsgesetz, Abh. Math. Sem. Univ. Hamburg, **7** (1930), 52–63.

[4] H. Hasse, Bericht über die neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, I, Ia, II, Leipzig und Berlin, 1930.

[5] H. Hasse, Zum expliziten Reziprozitätsgesetz, Arch. Math., **13** (1962), 479–485.

[6] K. Iwasawa, On some modules in the theory of cyclotomic fields, J. Math. Soc. Japan, **16** (1964), 42–82.

[7] K. Iwasawa, Some results in the theory of cyclotomic fields, Proc. Symposia in Pure Math., Amer. Math. Soc., **8** (1965), 66–69.