[7] J. C. Lagarias, *On determining the 4-rank of the ideal class group of a quadratic field*, ibid. 12 (1980), 191–196.
[8] E. Lehmer, *On the quadratic character of some quadratic surds*, J. Reine Angew. Math. 250 (1971), 42–48.
[9] — *On some special quartic reciprocity laws*, Acta Arith. 21 (1972), 367–377.
[10] P. Morton, *On Rédei's theory of the Pell equation*, J. Reine Angew. Math. 307/308 (1979), 373–398.
[11] — *Density results for the 2-classgroups of imaginary quadratic fields*, ibid. 332 (1982), 156–187.
[12] — *Density results for the 2-classgroups and fundamental units of real quadratic fields*, Studia Sci. Math. Hungar. 17 (1982), 21–43.
[13] — *The quadratic number fields with cyclic 2-classgroups*, Pacific J. Math. 108 (1983), 165–175.
[14] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, PWN–Polish Scientific Publishers, Warszawa 1973.
[15] L. Rédei, *Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper I*, J. Reine Angew. Math. 180 (1939), 1–43.
[16] — *Die 2-Ringklassengruppe des quadratischen Zahlkörpers und die Theorie der Pellschen Gleichung*, Acta Math. Acad. Sci. Hungar. 4 (1953), 31–87.
[17] D. Shanks, *Gauss's ternary form reduction and the 2-Sylow subgroup*, Math. Comp. 25 (1971), 837–853.
[18] P. Stevenhagen, *Class groups and governing fields*, Ph.D. thesis, Univ. of California at Berkeley, 1988.
[19] — *Ray class groups and governing fields*, Academisch proefschrift, Universiteit van Amsterdam, 1989.

DEPARTMENT OF MATHEMATICS
WELLESLEY COLLEGE
Wellesley, Massachusetts, U.S.A.

Received on 4.11.1988 (1882)

ACTA ARITHMETICA
LV (1990)

Explicit reciprocity laws on relative Lubin–Tate groups

by

YUTAKA SUEYOSHI (Fukuoka)

§ 1. Introduction. In [6], E. de Shalit proved an explicit reciprocity law conjectured by R. F. Coleman [3, 4]. It gives an explicit formula for the norm residue symbol on fields generated by division points of Lubin–Tate formal groups, and generalizes the explicit reciprocity laws of Artin–Hasse, Iwasawa, Kudo and Wiles [1, 9, 12, 17]. In the present paper, we extend it to *relative Lubin–Tate formal groups* and give a refinement of the explicit formulas of Iwasawa, Kudo and Wiles.

Let p be a prime number, $k/\mathbf{Q}_p$ a finite extension, and q the number of elements in the residue field of k. Let d be a positive integer, k' the unramified extension of k of degree d, and φ the Frobenius automorphism of k'/k. Let $\mathfrak{o}$ and $\mathfrak{o}'$ denote the integer rings of k and k', respectively, and $\mathfrak{p}$ the maximal ideal of $\mathfrak{o}$. Let $v\colon k^\times \to \mathbf{Z}$ denote the normalized valuation of k, and let x be an element of k such that $v(x) = d$. Let $\pi \in k'$ be such that $N_{k'/k}\pi = x$, and take a power series $f \in \mathfrak{o}'[[X]]$ satisfying $f(X) \equiv \pi X \mod \deg 2$ and $f(X) \equiv X^q \mod \pi$. There exists a unique one-dimensional commutative formal group law (called a *relative Lubin–Tate formal group* [5]) $F_f \in \mathfrak{o}'[[X, Y]]$ such that $f \in \mathrm{Hom}(F_f, F_f^\varphi)$. We write $\underset{f}{+}$ for its addition. For $a \in \mathfrak{o}$ we denote by $[a]_f \in X\mathfrak{o}'[[X]]$ the endomorphism of F_f such that $[a]_f(X) \equiv aX \mod \deg 2$ and $[a]_f^\varphi \circ f = f \circ [a]_f$.

Let Ω denote the completion of the algebraic closure of k, and $\mathfrak{p}_\Omega$ the maximal ideal of the integer ring of Ω. Let W_f^i denote the set of all $\mathfrak{p}^i$-division points of $F_f(\mathfrak{p}_\Omega)$. The field $k_{x,i} = k'(W_f^i)$, $i \geq 1$, does not depend on the choices of π and f, and is an abelian extension over k with norm group $\langle x \rangle \times (1+\mathfrak{p}^i)$. Any element of $\tilde{W}_f^i = W_f^i - W_f^{i-1}$ is a prime element of $k_{x,i}$. The *Tate module*

$$W_f = \varprojlim_i W^i_{\varphi^{-i}(f)}$$

(the limit is taken with respect to the maps $\varphi^{-i}(f)$) of F_f is a free $\mathfrak{o}$-module of rank 1 by $[a]_f(\gamma) = ([a]_{\varphi^{-i}(f)}(\gamma_i))_i$ for $a \in \mathfrak{o}$ and $\gamma = (\gamma_i)_i \in W_f$, and

$$\tilde{W}_f = \varprojlim_i \tilde{W}^i_{\varphi^{-i}(f)}$$

is the set of all $\mathfrak{o}$-generators of W_f.

Let $\mathfrak{p}_{x,i}$ denote the maximal ideal of the integer ring of $k_{x,i}$. Let $n \in N$, $\alpha \in F_f(\mathfrak{p}_{x,n})$ and $\beta \in k_{x,n}^{\times}$. Take any $\xi \in F_{\varphi^{-n}(f)}(\mathfrak{p}_\Omega)$ satisfying $\alpha = f^{\varphi^{-1}} \circ \ldots \circ f^{\varphi^{-n}}(\xi)$, and define a norm residue symbol on $k_{x,n}$ by

$$(\alpha, \beta)_{f,n} = \sigma_{x,n}(\beta)(\xi) \underset{\varphi^{-n}(f)}{-} \xi \in W^n_{\varphi^{-n}(f)},$$

where $\sigma_{x,n}(\beta) \in \mathrm{Gal}((k_{x,n})^{\mathrm{ab}}/k_{x,n})$ denotes the Artin symbol for β.

Let $\omega = (\omega_i)_i \in \tilde{W}_f$. Take any power series $s \in F_f(X\mathfrak{o}'[[X]])$ satisfying $\alpha = s(\omega_n)$ and define

$$\Theta^n_f s = \lambda_f \circ s - \frac{1}{\pi} \lambda^{\varphi}_f \circ s^{\varphi} \circ f^{\varphi^{-n}},$$

where $\lambda_f \colon F_f \xrightarrow{\sim} G_a$ denotes the unique logarithm map satisfying $\lambda_f(X) = X + \cdots$ Generalizing *Coleman's interpolation theorem* [2, Theorem 15; 5, Theorem 4], we see that there exists a power series $t \in \mathfrak{o}'((X))^{\times}$ such that $N_{k_{x,n}/k_{x,i}} \beta = t^{\varphi^{-i}}(\omega_i)$ for $1 \leqslant i \leqslant n$. Define

$$\delta_f t = \frac{1}{d\lambda_f/dX} \frac{dt/dX}{t} \in X^{-1}\mathfrak{o}'[[X]],$$

$$\langle s, t \rangle_{f,n} = T_{k'/k}\left(\frac{1}{\pi^{\varphi^{-1} + \ldots + \varphi^{-n}}} \left\{ \sum_{\gamma \in W^n_{\varphi^{-n}(f)}} ((\Theta^n_f s)(\delta_f t)^{\varphi^{-n}})(\gamma) + \frac{ds}{dX}(0)\left(1 - ((\mathcal{N}_f t)^{\varphi^{-1}}/t)^{\varphi^{-n}}(0)\right) \right\} \right) \in k,$$

where $\mathcal{N}_f \colon \mathfrak{o}'((X)) \to \mathfrak{o}'((X))$ denotes *Coleman's norm operator* [2, 5] associated with f. Our first result is (§ 3):

$$\langle s, t \rangle_{f,n} \in \mathfrak{o}; \qquad (\alpha, \beta)_{f,n} = [\langle s, t \rangle_{f,n}]_{\varphi^{-n}(f)}(\omega_n).$$

Using this formula, we deduce some explicit formulas under certain conditions on α and β (§ 4).

There are some different approaches to explicit reciprocity laws on Lubin–Tate groups. Vostokov [13–15] and Vostokov and Fesenko [16] gave an explicit formula for $(\alpha, \beta)_{f,n}$ on any field E *containing* division points W^n_f of a Lubin–Tate group by using a power series expansion for α with coefficients in the inertia subfield of E/k and a power series expansion for β with coefficients in the absolute inertia subfield of E. Kolyvagin [11] gave a generalization of the formulas of Artin–Hasse, Iwasawa and Wiles on any field containing division points for a wider class of formal groups.

§ 2. Analytical pairing $\langle s, t \rangle_{f,n}$. Let K denote the closure of the maximal unramified extension of k, and $\mathfrak{o}_K$ the integer ring of K. Let φ also denote the Frobenius automorphism of K/k. In this section, we extend the definition of $\langle s, t \rangle_{f,n}$ to power series with coefficients in $\mathfrak{o}_K$ and describe its properties.

Let π be a prime element of K. Take a power series $f \in \mathfrak{o}_K[[X]]$ satisfying $f(X) \equiv \pi X \mod \deg 2$ and $f(X) \equiv X^q \mod \pi$, and let $F_f \in \mathfrak{o}_K[[X, Y]]$ be the corresponding formal group law such that $f \in \mathrm{Hom}(F_f, F^{\varphi}_f)$ [10, Chap. IV]. For such an F_f we define $[a]_f$, $\underset{f}{+}$, W^i_f, W_f, $\tilde{W}^i_f$, $\tilde{W}_f$, λ_f, Θ^n_f and δ_f as in § 1.

The field $K_i = K(W^i_f)$, $i \geqslant 1$, does not depend on the choices of π and f. Let $\omega = (\omega_i)_i \in \tilde{W}_f$. As in [6, § 2], we define

$$M^n_f = \left\{ t \in \mathfrak{o}_K((X))^{\times} \,\middle|\, (\mathcal{N}_f t)^{\varphi^{-1}}/t \in 1 + \frac{\pi}{X} f^{\varphi^{n-2}} \circ \ldots \circ f(X)\mathfrak{o}_K[[X]] \right\}$$
$$= \left\{ t \in \mathfrak{o}_K((X))^{\times} \,\middle|\, t^{\varphi^{-i}}(\omega_i) = N_{K_{i+1}/K_i}(t^{\varphi^{-i-1}}(\omega_{i+1})),\ 1 \leqslant i < n \right\}$$

for $n \geqslant 1$ and put

$$M^{\infty}_f = \bigcap_{n=1}^{\infty} M^n_f = \{ t \in \mathfrak{o}_K((X))^{\times} \mid \mathcal{N}_f t = t^{\varphi} \}.$$

For $s \in F_f(X\mathfrak{o}_K[[X]])$ and $t \in M^n_f$ we define

$$\langle s, t \rangle^1_{f,n} = \sum_{i=0}^{d-1} \left\{ \frac{1}{\pi^{\varphi^{-1} + \ldots + \varphi^{-n}}} \sum_{\gamma \in W^n_{\varphi^{-n}(f)}} ((\Theta^n_f s)(\delta_f t)^{\varphi^{-n}})(\gamma) \right\}^{\varphi^i},$$

$$\langle s, t \rangle^2_{f,n} = \sum_{i=0}^{d-1} \left\{ \frac{1}{\pi^{\varphi^{-1} + \ldots + \varphi^{-n}}} \frac{ds}{dX}(0)\left(1 - ((\mathcal{N}_f t)^{\varphi^{-1}}/t)^{\varphi^{-n}}(0)\right) \right\}^{\varphi^i},$$

$$\langle s, t \rangle_{f,n} = \langle s, t \rangle^1_{f,n} + \langle s, t \rangle^2_{f,n} \in K.$$

Remark 1. (i) Since $\lambda_f = \lim_{n \to \infty} f^{\varphi^{n-1}} \circ \ldots \circ f/\pi^{\varphi^{n-1} + \ldots + 1}$, we obtain $\Theta^n_f s \in X\mathfrak{o}_K[[X]]$ as in [2, Lemmas 20 and 21]. Using the properties of *Coleman's trace operator* $\mathcal{S}_f$ [2], we see that

$$\langle s, t \rangle^1_{f,n} = \sum_{i=0}^{d-1} \left\{ \frac{1}{\pi^{\varphi^{-1} + \ldots + \varphi^{-n}}} \left(\mathcal{S}^n_{\varphi^{-n}(f)}((\Theta^n_f s)(\delta_f t)^{\varphi^{-n}})\right)(0) \right\}^{\varphi^i} \in \mathfrak{o}_K,$$

where $\mathcal{S}^n_{\varphi^{-n}(f)} = \mathcal{S}_{\varphi^{-1}(f)} \circ \ldots \circ \mathcal{S}_{\varphi^{-n}(f)}$. On the other hand, by the definition of M^n_f, we have $\langle s, t \rangle^2_{f,n} \in \mathfrak{o}_K$. If f, s and t have coefficients in $\mathfrak{o}'$, then $\langle s, t \rangle_{f,n} \in \mathfrak{o}$.

(ii) $\langle s, t \rangle_{f,n} \mod \pi^n$ is $\mathfrak{o}$-linear in s and linear in t.

(iii) Let U_K denote the unit group of $\mathfrak{o}_K$. Let π' be another prime element of K. We define

$$\mathfrak{o}_K(\pi, \pi') = \{ \eta \in \mathfrak{o}_K \mid \eta^{\varphi}\pi = \eta\pi' \}, \qquad U_K(\pi, \pi') = U_K \cap \mathfrak{o}_K(\pi, \pi').$$

Then $U_K(\pi, \pi') \neq \emptyset$ and $\mathfrak{o}_K(\pi, \pi) = \mathfrak{o}$ by [10, Lemma 3.11]. If $\pi, \pi' \in k'$ and $N_{k'/k}\pi = N_{k'/k}\pi'$, then $\mathfrak{o}_K(\pi, \pi') \subset \mathfrak{o}'$ by the same lemma. Take a power series

$f' \in \mathfrak{o}_K[[X]]$ satisfying $f'(X) \equiv \pi' X \bmod \deg 2$ and $f'(X) \equiv X^q \bmod \pi$. For $\eta \in \mathfrak{o}_K(\pi, \pi')$ there exists a unique power series $\theta = [\eta]_{f,f'} \in \mathrm{Hom}(F_f, F_{f'})$ such that $\theta(X) \equiv \eta X \bmod \deg 2$ and $\theta^\varphi \circ f = f' \circ \theta$ [10, Proposition 3.12]. In particular, $f = [\pi]_{f,\varphi(f)}$. The assertion of [5, Theorem 2] also holds for $[\eta]_{f,f'}$. Let $\eta \in U_K(\pi, \pi')$, then θ: $W_f \ni (\gamma_i)_i \to (\theta^{\varphi^{-i}}(\gamma_i))_i \in W_{f'}$ is an $\mathfrak{o}$-module isomorphism. Put

$$\bar{s} = \theta \circ s \circ (\theta^{\varphi^{-n}})^{-1} \in F_{f'}(X\mathfrak{o}_K[[X]]), \quad \bar{t} = t \circ \theta^{-1} \in M^n_{f'}.$$

Then $\Theta^n_f s = \eta^{-1}(\Theta^n_{f'}\bar{s}) \circ \theta^{\varphi^{-n}}$, $\delta_f t = \eta(\delta_{f'}\bar{t}) \circ \theta$, $\mathcal{N}_f t = (\mathcal{N}_{f'}\bar{t}) \circ \theta^\varphi$ and therefore $\langle s, t \rangle_{f,n} = \langle \bar{s}, \bar{t} \rangle_{f',n}$.

(iv) Suppose that $f \in \mathfrak{o}'[[X]]$, $N_{k'/k}\pi = x$ and that s, t have coefficients in $\mathfrak{o}'$. Let $\gamma_j \in \tilde{W}^j_{\varphi^{-n}(f)}$ for $0 \leqslant j \leqslant n-1$ ($\gamma_0 = 0$). Write

$$v = (\mathcal{N}_f t)^{\varphi^{-1}}/t = 1 + \pi^{\varphi^{n-1}} f^{\varphi^{n-2}} \circ \ldots \circ f(X) w(X)/X$$

with some $w \in \mathfrak{o}'[[X]]$. Then, as in the proof of [4, Lemma 13], we see from $\mathcal{S}_f(\delta_f t) = \pi\delta_{\varphi(f)}(\mathcal{N}_f t) = \pi(\delta_f t + \delta_f v)^\varphi$ [2, p. 115] that

$$\langle s, t \rangle^1_{f,n} = T_{k'/k}\Bigg(\frac{1}{\pi^{\varphi^{-1}+\ldots+\varphi^{-n}}}\Big\{\sum_{\gamma \in W^n_{\varphi^{-n}(f)}} ((\lambda_f \circ s)(\delta_f t)^{\varphi^{-n}})(\gamma)$$

$$- \sum_{\gamma \in W^{n-1}_{\varphi^{-n}(f)} - \{0\}} ((\lambda_f \circ s)(\delta_f v)^{\varphi^{-n}})(\gamma)\Big\}\Bigg).$$

Since $(\delta_f v)^{\varphi^{-n}}(\gamma) = \pi^{\varphi^{-1}+\ldots+\varphi^{-n}} w^{\varphi^{-n}}(\gamma)/\gamma$ for $\gamma \in W^{n-1}_{\varphi^{-n}(f)} - \{0\}$ and since

$$\langle s, t \rangle^2_{f,n} = -T_{k'/k}\Bigg(\Big(\frac{\lambda_f \circ s}{X} w^{\varphi^{-n}}\Big)(0)\Bigg),$$

we obtain

$$\langle s, t \rangle_{f,n} = T_{k_{x,n}/k}\Bigg(\frac{1}{\pi^{\varphi^{-1}+\ldots+\varphi^{-n}}} \lambda_f \circ s(\omega_n)(\delta_f t)^{\varphi^{-n}}(\omega_n)\Bigg)$$

$$- \sum_{j=0}^{n-1} T_{k_{x,j}/k}\Bigg(\Big(\frac{\lambda_f \circ s}{X} w^{\varphi^{-n}}\Big)(\gamma_j)\Bigg).$$

Put $\alpha = s(\omega_n) \in F_f(\mathfrak{p}_{x,n})$ and let $\langle \alpha, t \rangle_{f,n}$ denote the first term of the right-hand side of this equality. Since

$$T_{k_{x,j}/k}\Bigg(\Big(\frac{\lambda_f \circ s}{X} w^{\varphi^{-n}}\Big)(\gamma_j)\Bigg) \in \mathfrak{o} \quad [17, \text{Lemma } 11],$$

we have $\langle \alpha, t \rangle_{f,n} \in \mathfrak{o}$. In particular, if $t \in M^\infty_f \cap \mathfrak{o}'((X))^\times$, then $w = 0$ and we have $\langle \alpha, t \rangle_{f,n} = \langle s, t \rangle_{f,n} \in \mathfrak{o}$. In this case, since $\mathcal{S}_f(\delta_f t) = \pi\delta_{\varphi(f)}(\mathcal{N}_f t) = \pi(\delta_f t)^\varphi$, we have $\langle \alpha, t \rangle_{f,i} = \langle \alpha, t \rangle_{f,n}$ for $i \geqslant n$.

§ 3. The Coleman–de Shalit formula in the relative case. Let x, π, f and ω be as in § 1. Let $\alpha \in F_f(\mathfrak{p}_{x,n})$ and $b = (\beta_i)_i \in B_x = \varprojlim_i k^\times_{x,i}$ (the limit is taken with respect to the norm maps). Then the symbol $(\alpha, b)_f = ((\alpha, \beta_i)_{f,i})_{i \geqslant n}$ defines an element of W_f. We write $(\alpha, b)_{f,i} = (\alpha, \beta_i)_{f,i}$ for $i \geqslant n$. Let $t \in M^\infty_f \cap \mathfrak{o}'((X))^\times$ be such that $\beta_i = t^{\varphi^{-i}}(\omega_i)$ for all $i \geqslant 1$ [7, Theorem 2.2]. By Remark 1(iv), we define $\langle \alpha, b \rangle_\omega = \langle \alpha, t \rangle_{f,i} \in \mathfrak{o}$ with $i \geqslant n$, and define $[\alpha, b]_\omega = [\langle \alpha, b \rangle_\omega]_f(\omega) \in W_f$. We denote by $[\alpha, b]_{\omega,i}$ the ith component of $[\alpha, b]_\omega$.

THEOREM 1. $(\alpha, b)_f = [\alpha, b]_\omega$.

Proof. It suffices to prove $(\alpha, b)_{f,i} = [\alpha, b]_{\omega,i}$ for all i ($\geqslant n$) $\in d\mathbf{Z}$. Fix such an i and put $\alpha_j = [x^{(j-i)/d}]_f(\alpha)$ for j ($\geqslant i$) $\in d\mathbf{Z}$. Then, since $(\alpha, b)_{f,i} = (\alpha_j, b)_{f,j}$ and $[\alpha, b]_{\omega,i} = [\alpha_j, b]_{\omega,j}$, it is enough to show $(\alpha_j, b)_{f,j} = [\alpha_j, b]_{\omega,j}$ for sufficiently large j. However, this can be proved in a similar way to [6, § 3].

Remark 2. In the case where p is *odd*, Theorem 1 was proved by Imada [8], by computing $(\alpha, b)_f$ for $f(X) = \pi X + X^q$.

THEOREM 2. *Let* α, β, s *and* t *be as in* § 1. *Then*

$$(\alpha, \beta)_{f,n} = [\langle s, t \rangle_{f,n}]_{\varphi^{-n}(f)}(\omega_n).$$

Proof. We prove the theorem by translating the proof of [6, Theorem 1] to relative Lubin–Tate groups. Since both sides of the equality are linear in β, we may assume that β is a prime element of $k_{x,n}$. Put $\pi' = N_{k_{x,n}/k'}\beta$, $x' = N_{k'/k}\pi'$ and $u = x'/x$. Then $u \in 1 + \mathfrak{p}^n$ and $k_{x',i} = k_{x,i}$ for $0 \leqslant i \leqslant n$. Take a power series $f' \in \mathfrak{o}'[[X]]$ satisfying $f'(X) \equiv \pi' X \bmod \deg 2$ and $f'(X) \equiv X^q \bmod \pi$. Let $\eta \in U_K(\pi, \pi')$ and put

$$\theta = [\eta]_{f,f'} \in X\mathfrak{o}_K[[X]]^\times, \quad \omega' = (\omega'_i)_i = \theta(\omega) \in \tilde{W}_{f'}, \quad \varphi' = \varphi^d.$$

Since $\eta^{\varphi'-1} = u$, we have $\theta^{\varphi'} = \theta \circ [u]_f = [u]_{f'} \circ \theta$. Put

$$\bar{s} = \theta \circ s \circ (\theta^{\varphi^{-n}})^{-1} \in F_{f'}(X\mathfrak{o}_K[[X]]).$$

Then $\bar{s}^{\varphi'} = [u]_{f'} \circ \bar{s} \circ [u^{-1}]_{\varphi^{-n}(f')}$. It is easy to see from [10, Lemma 3.11] (or from [6, Lemma]) that there exists a power series $h \in F_{f'}(X\mathfrak{o}_K[[X]])$ such that $\bar{s} = h^{\varphi'} -_{f'} h$. Therefore we have

$$(h^{\varphi'} -_{f'} h)^{\varphi'} = ([u]_{f'} \circ h \circ [u^{-1}]_{\varphi^{-n}(f')})^{\varphi'} -_{f'} [u]_{f'} \circ h \circ [u^{-1}]_{\varphi^{-n}(f')}.$$

Put

$$s' = h^{\varphi'} -_{f'} [u]_{f'} \circ h \circ [u^{-1}]_{\varphi^{-n}(f')} \in F_{f'}(X\mathfrak{o}'[[X]]),$$

$$\alpha' = s'(\omega'_n) \in F_{f'}(\mathfrak{p}_{x,n}).$$

Then $\theta^{\varphi^{-n}}((\alpha, \beta)_{f,n}) = (\alpha', \beta)_{f',n}$ [6, Lemma 1]. Since $N_{k_{x',n}/k}\beta = x'$, there exists some $b' = (\beta'_i)_i \in B_{x'}$ such that $\beta = \beta'_n$. Let $t' \in M^\infty_{f'} \cap X\mathfrak{o}'[[X]]^\times$ be such that

$\beta_i' = t'^{\varphi^{-i}}(\omega_i')$ for all $i \geq 1$. Then, from the above and Theorem 1, we have $(\alpha, \beta)_{f,n} = [\langle s', t'\rangle_{f',n}]_{\varphi^{-n}(f)}(\omega_n)$. So, we must show $\langle s, t\rangle_{f,n} \equiv \langle s', t'\rangle_{f',n} \bmod \pi^n$. Put $\bar{t} = t \circ \theta^{-1} \in M_{f'}^n \cap X\mathfrak{o}_K[[X]]^\times$. By Remark 1(iii), we only need to show $\langle \bar{s}, \bar{t}\rangle_{f',n} \equiv \langle s', t'\rangle_{f',n} \bmod \pi^n$, or equivalently,

$$\langle \bar{s} -_{\!F'} s', \bar{t}\rangle_{f',n} \equiv \langle s', t'/\bar{t}\rangle_{f',n} \bmod \pi^n.$$

Since $\bar{s} -_{\!F'} s' \in X^2\mathfrak{o}_K[[X]]$, we have $\langle \bar{s} -_{\!F'} s', \bar{t}\rangle_{f',n}^2 = 0$ and the term corresponding to $\gamma = 0$ in $\langle \bar{s} -_{\!F'} s', \bar{t}\rangle_{f',n}^1$ is 0. Since $u \equiv 1 \bmod \pi^n$, we have

$$\Theta_{f'}^n(\bar{s} -_{\!F'} s')(\gamma) = (u-1)(\Theta_{f'}^n h)(\gamma) \quad \text{for } \gamma \in W_{\varphi^{-n}(f')}^n - \{0\}.$$

Using $\delta_{f'}\bar{t} = X^{-1} + \ldots$ and [2, Lemma 6], we see that

$$\begin{aligned}
\langle \bar{s} -_{\!F'} s', \bar{t}\rangle_{f',n} &= \langle \bar{s} -_{\!F'} s', \bar{t}\rangle_{f',n}^1 \\
&= \sum_{i=0}^{d-1} \left\{ \frac{u-1}{\pi'^{\varphi^{-1}+\ldots+\varphi^{-n}}} \sum_{\gamma \in W_{\varphi^{-n}(f')}^n - \{0\}} \big((\Theta_{f'}^n h)(\delta_{f'}\bar{t})^{\varphi^{-n}}\big)(\gamma) \right\}^{\varphi^i} \\
&\equiv -\sum_{i=0}^{d-1} \left\{ \frac{u-1}{\pi'^{\varphi^{-1}+\ldots+\varphi^{-n}}} \left(\frac{dh}{dX}(0) - \frac{\varphi^{-n}(\pi')}{\pi'} \frac{dh}{dX}(0)^{\varphi} \right) \right\}^{\varphi^i} \bmod \pi^n \\
&= \frac{u-1}{\pi'^{\varphi^{-1}+\ldots+\varphi^{-n}}} \frac{ds'}{dX}(0).
\end{aligned}$$

Put $r = t'/\bar{t} \in \mathfrak{o}_K[[X]]^\times$. Since $\delta_f r \in \mathfrak{o}_K[[X]]$, the term corresponding to $\gamma = 0$ in $\langle s', r\rangle_{f',n}^1$ is 0. Since $r^{\varphi^{-i}}(\omega_i') = 1$, $1 \leq i \leq n$, we may write

$$r(X) = 1 + f'^{\varphi^{n-1}} \circ \cdots \circ f'(X) y(X)/X, \qquad y \in \mathfrak{o}_K[[X]].$$

Then $(\delta_{f'} r)^{\varphi^{-n}}(\gamma) = \pi'^{\varphi^{-1}+\ldots+\varphi^{-n}} y^{\varphi^{-n}}(\gamma)/\gamma$ for $\gamma \in W_{\varphi^{-n}(f')}^n - \{0\}$. Therefore, by [2, Lemma 6], we see that

$$\begin{aligned}
\langle s', r\rangle_{f',n}^1 &= \sum_{i=0}^{d-1} \left\{ \sum_{\gamma \in W_{\varphi^{-n}(f')}^n - \{0\}} \left(\frac{\Theta_{f'}^n s'}{X} y^{\varphi^{-n}} \right)(\gamma) \right\}^{\varphi^i} \\
&\equiv -\sum_{i=0}^{d-1} \left\{ \left(\frac{ds'}{dX}(0) - \frac{\varphi^{-n}(\pi')}{\pi'} \frac{ds'}{dX}(0)^{\varphi} \right) y^{\varphi^{-n}}(0) \right\}^{\varphi^i} \bmod \pi^n.
\end{aligned}$$

On the other hand, since $(\mathcal{N}_{f'} r)(0) = r(0) = 1 + \pi'^{\varphi^{n-1}+\ldots+1} y(0)$, we have

$$\langle s', r\rangle_{f',n}^2 \equiv \sum_{i=0}^{d-1} \left\{ \frac{ds'}{dX}(0) \left(y^{\varphi^{-n}}(0) - \frac{\varphi^{-n-1}(\pi')}{\varphi^{-1}(\pi')} y^{\varphi^{-n-1}}(0) \right) \right\}^{\varphi^i} \bmod \pi^n.$$

Hence, using $r(0) = (t'/\bar{t})(0) = (t'/t)(0)\eta \in \eta \cdot k'^\times$, we see that

$$\begin{aligned}
\langle s', r\rangle_{f',n} &\equiv \frac{\varphi^{-n-1}(\pi')}{\varphi^{-1}(\pi')} \frac{ds'}{dX}(0)\big(y^{\varphi^{-n-1+d}}(0) - y^{\varphi^{-n-1}}(0)\big) \bmod \pi^n \\
&\equiv \frac{1}{\pi'^{\varphi^{-1}+\ldots+\varphi^{-n}}} \frac{ds'}{dX}(0)\big(r^{\varphi^{-n-1+d}}(0)/r^{\varphi^{-n-1}}(0) - 1\big) \bmod \pi^n \\
&= \frac{u-1}{\pi'^{\varphi^{-1}+\ldots+\varphi^{-n}}} \frac{ds'}{dX}(0).
\end{aligned}$$

Thus we obtain the desired congruence and conclude the proof.

§ 4. Some explicit formulas. Let x, π, f, α, β and ω be as in § 1. Let $m \geq n$ and suppose that $\beta = N_{k_{x,m}/k_{x,n}}\beta'$, $\beta' \in k_{x,m}^\times$. Take *any* power series $t \in \mathfrak{o}'((X))^\times$ satisfying $\beta' = t^{\varphi^{-m}}(\omega_m)$. We define

$$\langle \alpha, t\rangle_{f,m} = T_{k_{x,m}/k}\left(\frac{1}{\pi^{\varphi^{-1}+\ldots+\varphi^{-m}}} \lambda_f(\alpha)(\delta_f t)^{\varphi^{-m}}(\omega_m) \right) \in k.$$

Let $t' \in M_f^m \cap \mathfrak{o}'((X))^\times$ be such that $\beta' = t'^{\varphi^{-m}}(\omega_m)$. We have $\langle \alpha, t'\rangle_{f,m} \in \mathfrak{o}$ by Remark 1(iv).

THEOREM 3. *If* (a) $m \geq 2n$, *or* (b) $m \geq n+l$ *and* $\alpha \in F_f(\mathfrak{p}_{x,n}^{q^{n-1-l}+1})$, *for some* l $(0 \leq l \leq n-1)$, *then*

$$(\alpha, \beta)_{f,n} = [\langle \alpha, t'\rangle_{f,m}]_{\varphi^{-n}(f)}(\omega_n).$$

Proof. Take a power series $s \in F_f(X\mathfrak{o}'[[X]])$ satisfying $\alpha = s(\omega_m)$. By Theorem 2, we have

$$(\alpha, \beta)_{f,n} = f^{\varphi^{-n-1}} \circ \ldots \circ f^{\varphi^{-m}}((\alpha, \beta')_{f,m}) = [\langle s, t'\rangle_{f,m}]_{\varphi^{-n}(f)}(\omega_n).$$

Write $(\mathcal{N}_f t')^{\varphi^{-1}}/t' = 1 + \pi^{\varphi^{m-1}} f^{\varphi^{m-2}} \circ \ldots \circ f(X) w(X)/X$, $w \in \mathfrak{o}'[[X]]$. Let $\gamma_j \in \tilde{W}_{\varphi^{-m}(f)}^j$ for $0 \leq j < m$. By Remark 1(iv), we have

$$\langle s, t'\rangle_{f,m} = \langle \alpha, t'\rangle_{f,m} - \sum_{j=0}^{m-1} T_{k_{x,j}/k}\left(\left(\frac{\lambda_f \circ s}{X} w^{\varphi^{-m}} \right)(\gamma_j) \right).$$

We estimate the second term of the right-hand side of this equality. By the assumption of the theorem, we may assume that $s \in X^{q^{m-n}}\mathfrak{o}'[[X]]$ in case (a) and $s \in X^{q^{m-n}(q^{n-1-l}+1)}\mathfrak{o}'[[X]]$ in case (b). Since $s \in X^2\mathfrak{o}'[[X]]$ in both cases, we have

$$T_{k'/k}\left(\left(\frac{\lambda_f \circ s}{X} w^{\varphi^{-m}} \right)(\gamma_0) \right) = 0.$$

Let $\mathscr{L}$ be the $\mathfrak{o}_K[[X]]$-submodule of $K[[X]]$ spanned by $\{X^{q^i}/\pi^i\}_{i=0}^{\infty}$. Then $\lambda_f \in \mathscr{L}$ [17, Lemma 4]. Using this and the inequality $(q^i-1)/(q-1) \geq i$ for $i \in \mathbf{Z}$, we estimate the other terms. Let $1 \leqslant j < m$. In case (a), we see that

$$v\left(\left(\frac{\lambda_f \circ s}{X} w^{\varphi^{-m}}\right)(\gamma_j)\right) \geqslant \min_{i \geqslant 0} v((\gamma_j^{q^{m-n}})^{q^i}/\pi^i) - v(\gamma_j)$$

$$= \min_{i \geqslant 0}\left(\frac{q^{m-n+i}}{q^{j-1}(q-1)} - i\right) - \frac{1}{q^{j-1}(q-1)} \geqslant n - \left(j - \frac{1}{q-1}\right).$$

Similarly, we obtain the same estimate in case (b). Since the different of $k_{x,j}/k$ is $\mathfrak{p}^{j-1/(q-1)}$, we obtain

$$T_{k_{x,j}/k}\left(\left(\frac{\lambda_f \circ s}{X} w^{\varphi^{-m}}\right)(\gamma_j)\right) \equiv 0 \mod \pi^n$$

in both cases and conclude the proof.

THEOREM 4. *If* (a) $m \geqslant 2n$, *or* (b) $m \geqslant n+l$ *and* $\alpha \in F_f(\mathfrak{p}_{x,n}^{2q^{n-1-l}})$ *for some* l $(0 \leqslant l \leqslant n-1)$, *then* $\langle \alpha, t \rangle_{f,m} \in \mathfrak{o}$ *and we have an explicit formula*

$$(\alpha, \beta)_{f,n} = [\langle \alpha, t \rangle_{f,m}]_{\varphi^{-n}(f)}(\omega_n).$$

Proof. Write $t' = tz$ with $z \in \mathfrak{o}'[[X]]^\times$. Then, by Theorem 3, we only need to show

$$\langle \alpha, z \rangle_{f,m} = T_{k_{x,m}/k}\left(\frac{1}{\pi^{\varphi^{-1}+\dots+\varphi^{-m}}} \lambda_f(\alpha)(\delta_f z)^{\varphi^{-m}}(\omega_m)\right) \equiv 0 \mod \pi^n.$$

Since $z^{\varphi^{-m}} - 1$ can be divided by $f^{\varphi^{-1}} \circ \dots \circ f^{\varphi^{-m}} / f^{\varphi^{-2}} \circ \dots \circ f^{\varphi^{-m}}$ in $\mathfrak{o}'[[X]]$, we have $v((\delta_f z)^{\varphi^{-m}}(\omega_m)) \geqslant m - 1/(q-1)$. Then, using the inequalities $(q^i - 1)/(q-1) \geqslant i$ for $i \geqslant 0$ and $(q^i - 1)/(q-1) \geqslant i/q$ for $i < 0$, we obtain

$$v(\lambda_f(\alpha)(\delta_f z)^{\varphi^{-m}}(\omega_m)/\pi^{\varphi^{-1}+\dots+\varphi^{-m}}) \geqslant n - \left(m - \frac{1}{q-1}\right)$$

in both cases and conclude the proof.

Remark 3. Theorem 4 is a refinement of Wiles' formulas [17, Theorems 1 and 23]. In particular, in the *Hilbert symbol* case ($k = \boldsymbol{Q}_p$, $x = p^d$, $f(X) = 1 - (1-X)^p$, $F_f(X, Y) = X + Y - XY$ and $(1 - \zeta_i)_i \in \tilde{W}_f$), we obtain an explicit formula

$$((1-\alpha)^{1/p^n})^{\sigma_{k,n}(\beta)-1} = \zeta_n^w,$$

$$w = -T_m(\log(1-\alpha) \cdot \zeta_m \cdot (dt/dX)^{\varphi^{-m}}(1-\zeta_m)/\beta')/p^m,$$

where ζ_i denotes a primitive p^ith root of unity satisfying $\zeta_{i+1}^p = \zeta_i$, and $T_m = T_{k_{x,m}/k}$. This formula is a refinement of the explicit formulas of Iwasawa [9, Theorems 1 and 2] and Kudo [12, Theorems 1′ and 2′].

References

[1] 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. Univ. Hamburg 6 (1928), 146–162.

[2] R. F. Coleman, *Division values in local fields*, Invent. Math. 53 (1979), 91–116.

[3] — *The arithmetic of Lubin-Tate division towers*, Duke Math. J. 48 (1981), 449–466.

[4] — *The dilogarithm and the norm residue symbol*, Bull. Soc. Math. France 109 (1981), 373–402.

[5] E. de Shalit, *Relative Lubin-Tate groups*, Proc. Amer. Math. Soc. 95 (1985), 1–4.

[6] — *The explicit reciprocity law in local class field theory*, Duke Math. J. 53 (1986), 163–176.

[7] — *Iwasawa Theory of Elliptic Curves with Complex Multiplication*, Academic Press, London 1987.

[8] T. Imada, *Relative Lubin-Tate groups and the explicit reciprocity law* (in Japanese), Master's thesis, Kyushu Univ., 1988.

[9] K. Iwasawa, *On explicit formulas for the norm residue symbol*, J. Math. Soc. Japan 20 (1968), 151–165.

[10] — *Local Class Field Theory*, Oxford University Press, New York 1986.

[11] V. A. Kolyvagin, *Formal groups and the norm residue symbol*, Izv. Akad. Nauk SSSR Ser. Mat. 43 (1979), 1054–1120; English transl. in Math. USSR-Izv. 15 (1980), 289–348.

[12] A. Kudo, *On Iwasawa's explicit formula for the norm residue symbol*, Mem. Fac. Sci. Kyushu Univ. Ser. A 26 (1972), 139–148.

[13] S. V. Vostokov, *A norm pairing in formal modules*, Izv. Akad. Nauk SSSR Ser. Mat. 43 (1979), 765–794; English transl. in Math. USSR-Izv. 15 (1980), 25–51.

[14] — *Symbols on formal groups*, ibid. 45 (1981), 985–1014; English transl. in Math. USSR-Izv. 19 (1982), 261–284.

[15] — *The Hilbert symbol for Lubin-Tate formal groups I*, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. 114 (1982), 77–95; English transl. in J. Soviet Math. 27 (1984), 2885–2901.

[16] S. V. Vostokov and I. B. Fesenko, *The Hilbert symbol for Lubin-Tate formal groups II*, ibid. 132 (1983), 85–96; English transl. in J. Soviet Math. 30 (1985), 1854–1862.

[17] A. Wiles, *Higher explicit reciprocity laws*, Ann. of Math. 107 (1978), 235–254.

DEPARTMENT OF MATHEMATICS
KYUSHU UNIVERSITY 33
Fukuoka 812, Japan

Received on 5.12.1988
and in revised form on 10.3.1989 (1890)