

On the exponential series of formal groups

九大理 白谷克己 (Katsumi SHIRATANI)

§1. Introduction

Let p be an odd prime. In the prime cyclotomic field $\mathbb{Q}_p(\zeta_p)$ generated by a primitive p -th root ζ_p of unity over the p -adic rationals $\mathbb{Q}_p$, there are explicit formulas of Takagi for the reciprocity law.

Let $\mathfrak{f}_0 = (1 - \zeta_p)$ denote the prime ideal in $\mathbb{Q}_p(\zeta_p)$, and select a prime element $\tilde{\omega}$ such that

$$\tilde{\omega} = p^{-1}\sqrt{-p}, \quad \tilde{\omega} \equiv \zeta_p - 1 \pmod{\mathfrak{f}_0^2}.$$

Take Takagi basis κ_i ($1 \leq i \leq p$) as basis for the multiplicative group of the principal units U_1 modulo $\mathfrak{f}_0^{p+1}$ in $\mathbb{Q}_p(\zeta_p)$. Then the following formulas for the p -th norm residue symbol $(\ , \)$ hold.

$$(\kappa_i, \kappa_j) = 1 \quad \text{for } i+j \not\equiv 1 \pmod{p-1},$$

$$(\kappa_i, \kappa_j) = \zeta_p^{-i} \quad \text{for } i+j \equiv 1 \pmod{p-1},$$

$$(\tilde{\omega}, \kappa_i) = 1 \quad \text{for } i = 1, 2, \dots, p-1,$$

$$(\tilde{\omega}, \kappa_p) = \zeta_p.$$

For any principal unit $v \in U_1$ we have the congruence with some integers $t_i(v) \in \mathbb{Z}$, called the Takagi exponents,

$$v \equiv \kappa_1^{t_1(v)} \kappa_2^{t_2(v)} \dots \kappa_p^{t_p(v)} \pmod{\mathfrak{p}_0^{p+1}}.$$

Then it holds that for any $v, \mu \in U_1$

$$(v, \mu) = \zeta_p^{-\sum_{i=1}^{p-1} i t_i(v) t_{p-i}(\mu)},$$

$$(\hat{\omega}, v) = \zeta_p^{t_p(v)}.$$

These are called Takagi's formulas.

Now, the power series on indeterminate X

$$E(X) = e^{L(X)} = \prod_{(m,p)=1} (1-X^m)^{-\frac{\mu(m)}{m}}$$

with $L(X) = \sum_{\ell=0}^{\infty} \frac{1}{p^{\ell}} X^{p^{\ell}}$ is known as the Artin-Hasse exponential series, and $E(X) \in \mathbb{Z}_p[[X]]$ plays the central role in the proof for the complementary laws of reciprocity in the cyclotomic case [1]. Then we have the congruences

$$\kappa_i \equiv E((-1)^{i-1} \hat{\omega}^i) \pmod{\mathfrak{p}_0^{p+1}} \quad (1 \leq i \leq p).$$

For the details we refer to [6].

§2. Exponential series of the Lubin-Tate groups

Let k be a finite extension over $\mathbb{Q}_p$, and $\mathcal{O}$ the integer ring, $\mathfrak{f}$ the prime ideal, π a fixed prime element in k respectively. Let $q = p^c$ denote the number of the elements of the residue class field of k , namely, $\mathcal{O}/\mathfrak{f} = \text{GF}(q)$.

Let $f(X) \in \mathcal{O}[[X]]$ be a Frobenius power series belonging to the prime element π , namely

$$f(X) \equiv \pi X \pmod{\deg 2}, \quad f(X) \equiv X^q \pmod{\pi}$$

hold. Then there is a unique Lubin-Tate formal group $F = F_f$ attached to the series f , especially $f(X) = [\pi]_F(X)$ is an endomorphism of F .

Let $\Lambda_{f,m}$ denote the group of π^m division points in the algebraic closure k_s of k , and $L_{\pi,m} = k(\Lambda_{f,m})$ the field of π^m division points over k . Then we denote the integer ring, the prime ideal in $L_{\pi,m}$ by $\mathcal{O}_{m-1}$, $\mathfrak{f}_{m-1}$ respectively.

Now, for any $\alpha \in F(\mathfrak{f}_n)$, $\beta \in L_{\pi,n+1}^\times$ take an element $\gamma \in k_s$ such that $[\pi^{n+1}]_F(\gamma) = \alpha$, and define the norm residue symbol $(\alpha, \beta)_n^F$ due to Wiles [5], [7] as follows :

$$(\alpha, \beta)_n^F = \sigma_{\beta} \gamma - \gamma \in \Lambda_{f,n+1}, \quad \sigma_{\beta} = (\beta, L_{\pi,n+1}^{ab}/L_{\pi,n+1}) ,$$

where $L_{\pi,n+1}^{ab}$ means the maximal abelian extension of $L_{\pi,n+1}$ and $\sigma_{\beta} \in G(L_{\pi,n+1}^{ab}/L_{\pi,n+1})$ denotes the Artin map in local class field theory.

There is the isomorphism $\lambda_F : F \xrightarrow{\sim} G_a$ from the group F to the additive formal group G_a over k satisfying $\lambda_F'(0) = 1$. This power series $\lambda_F(X) \in k[[X]]$ is called the logarithm of F and is explicitly given by a formula

$$\lambda_F(X) = \lim_{n \rightarrow \infty} \frac{1}{\pi^n} [\pi^n]_F(X) .$$

The inverse power series $e_F : G_a \xrightarrow{\sim} F$ with $e_F'(0) = 1$ is called the exponential series of F .

Now, we define an exponential series $E_F(X)$ as follows :

$$E_F(X) = e_F(L(X)) \quad \text{with} \quad L(X) = \sum_{\ell=0}^{\infty} \frac{1}{\pi^\ell} X^{q^\ell} .$$

Then we see $E_F(X) \in k[[X]]$, but more precisely $E_F(X) \in X\mathcal{O}[[X]]$. This fact depends on the generalization of the Dieudonné-Dwork lemma.

Lemma 1. It is necessary and sufficient for a power series $P(X) \in Xk[[X]]$ to belong to $X\mathcal{O}[[X]]$ that $P(X^q)_{\overline{F}[\pi]_F}(P(X))$ has all the coefficients divisible by π , namely

$$P(X^q)_{\overline{F}[\pi]_F}(P(X)) \in X\pi\mathcal{O}[[X]] .$$

The Dieudonné-Dwork lemma is a special case of Lemma 1 for the multiplicative group G_m and $\mathcal{O} = \mathbb{Z}_p$.

By the definition of $E_F(X)$ we have directly

$$E_F(X^q)_{\overline{F}[\pi]_F}(E_F(X)) = e_F(-\pi X) ,$$

and we know $e_F(\pi X) \in X\pi\mathcal{O}[[X]]$. Consequently we conclude from Lemma 1 that

$$E_F(X) \in X\sigma[[X]].$$

§3. Complementary laws

We consider the basic formal group ξ attached to $f(X) = \pi X + X^q$.

For each $n \geq 0$ we take a prime element $u_n \in \Lambda_{f,n+1}$ in $L_{\pi,n+1}$ such as $[\pi]_{\xi}(u_n) = u_{n-1}$, $[\pi]_{\xi}(u_0) = 0$.

It holds from the Iwasawa-Wiles formula [2], [5], [7] that for any $i \geq 1$

$$(E_{\xi}(u_n^i), u_n)_{\xi}^{\xi} = \left[\frac{1}{\pi^{n+1}} T_n \left(\frac{\lambda_{\xi}(E_{\xi}(u_n^i))}{\lambda_{\xi}(u_n) u_n} \right) \right]_{\xi}(u_n),$$

where T_n denotes the trace with respect to $L_{\pi,n+1}/k$.

By the way we have $\lambda_{\xi}(E_{\xi}(u_n^i)) = L(u_n^i) \in L_{\pi,n+1}$, because we have in general $\lambda_F(X) = \sum_{m=1}^{\infty} \frac{c_m}{m} X^m$ with $c_m \in \sigma$. Thus we have

$$(E_{\xi}(u_n^i), u_n)_{\xi}^{\xi} = \left[\frac{1}{\pi^{n+1}} T_n \left(\frac{L(u_n^i)}{\lambda_{\xi}(u_n) u_n} \right) \right]_{\xi}(u_n).$$

Lemma 2. Assume $\ell \geq 2n + 2$. Then we have

$$\frac{1}{\pi^{\ell}} T_n \left(\frac{u_n^{iq^{\ell}-1}}{\lambda_{\xi}(u_n)} \right) \equiv 0 \pmod{\pi^{2(n+1)}}.$$

This can be obtained by virtue of the different $\mathfrak{D}_n$ equal to $\mathfrak{D}_n^{q^n((n+1)(q-1)-1)} \sim \pi^{n+1} u_0^{-1} \sigma_n$.

Lemma 3. We have

$$T_n\left(\frac{u_n^r}{\lambda_\xi(u_n)}\right) = \begin{cases} 0 & \text{for } 0 \leq r \leq q^{n-2}, \\ -\pi^n & \text{for } r = q^{n-1}. \end{cases}$$

Especially

$$\frac{1}{\pi^\ell} T_n\left(\frac{u_n^{iq^\ell-1}}{\lambda_\xi(u_n)}\right) = 0 \quad \text{for } iq^\ell < q^n,$$

$$\frac{1}{\pi^n} T_n\left(\frac{u_n^{q^n-1}}{\lambda_\xi(u_n)}\right) = -1.$$

These formulas come out from Euler's identity, Lagrange's interpolation formula for polynomials. The next lemma follows similarly from the same and noticing the minimal basis of $L_{\pi,n+1}/L_{\pi,n}$ to be $1, u_n, \dots, u_n^{q-1}$. $T_{n,n-1}$ denotes the trace with respect to $L_{\pi,n+1}/L_{\pi,n}$.

Lemma 4. Assume $n \geq 1$. Then we have

$$T_{n,n-1}\left(\frac{u_n^r}{\lambda_\xi(u_n)}\right) = \begin{cases} 0 & \text{for } 0 \leq r \leq q-2, \\ \frac{\pi}{\lambda_\xi(u_{n-1})} & \text{for } r = q-1, \end{cases}$$

$$T_{n,n-1}\left(\frac{u_n^r}{\lambda_\xi(u_n)}\right) = \frac{\pi}{\lambda_\xi(u_{n-1})} \sum_{\substack{s_0, r_1 \geq 0 \\ (q-1)(s_0+1)+r_1=r}} (-1)^{s_0-r_1} \binom{s_0}{r_1} u_{n-1}^{r_1} \pi^{s_0-r_1} \quad \text{for } r \geq q.$$

Now, by a repeated use of Lemma 4 we see

$$T_{n,0}\left(\frac{u_n^r}{\lambda'_\xi(u_n)}\right) = \sum (-1)^{s_0+\dots+s_{n-1}-r_1-\dots-r_n} \begin{pmatrix} s_0 \\ r_1 \end{pmatrix} \begin{pmatrix} s_1 \\ r_2 \end{pmatrix} \dots \begin{pmatrix} s_{n-1} \\ r_n \end{pmatrix} \pi^{n+(s_0+\dots+s_{n-1})-(r_1+\dots+r_n)} \frac{u_0^{r_n}}{\lambda'_\xi(u_0)}$$

where the summation is taken over the integers $s_i, r_i \geq 0$ satisfying $(q-1)(s_i+1) + r_{i+1} = r_i$ ($0 \leq i \leq n-1$), $r_0 = r$.

Therefore, after noticing that $T_0(u_0^{r_n}) = 0$ for $r_n \not\equiv 0 \pmod{q-1}$ and $r_n \equiv r \pmod{q-1}$, we have

$$(E_\xi(u_n^i), u_n)_n^\xi = 0 \quad \text{for} \quad i \not\equiv 1 \pmod{q-1}.$$

In the sequel we compute $(E_\xi(u_n^i), u_n)_n^\xi$ for the cases $i \equiv 1 \pmod{q-1}$.

First, from Lemma 4 for $iq^\ell \geq q^n$

$$\begin{aligned} (*) \quad & \frac{1}{\pi^\ell} T_n\left(\frac{u_n^{iq^\ell-1}}{\lambda'_\xi(u_n)}\right) \\ &= \sum_{j_1, \dots, j_n} (-1)^{j_0-n-1} \begin{pmatrix} j_0-1-j_1 \\ j_1(q-1) \end{pmatrix} \begin{pmatrix} j_1-1-j_2 \\ j_2(q-1) \end{pmatrix} \dots \begin{pmatrix} j_{n-1}-1-j_n \\ j_n(q-1) \end{pmatrix} \pi^{j_0-(q-1)(j_1+\dots+j_n)-\ell}, \end{aligned}$$

where $j_0 = \frac{iq^\ell-1}{q-1}$ and j_m runs over the integers satisfying

$$\frac{q^{n-m}-1}{q-1} \leq j_m \leq \frac{1}{q} (j_{m-1} - 1).$$

Here we can find easily the minimum of all the exponents of π , when ℓ and $j_1, \dots, j_n$ run over the possible ranges under the assumption $1 \leq i \leq q^{n+1}-1, i \equiv 1 \pmod{q-1}$. The minimum exponent

becomes $t + s_q(\frac{i-q^t}{q-1})$, where t means the non-negative integer such that $q^t \leq i < q^{t+1}$ and $s_q(x)$ denotes the sum of the coefficients of the canonical q -expansion of x .

Consequently, under the condition $q > 2n + 2$ we have a congruence

$$\frac{1}{\pi^{n+1}} T_n(\frac{L(u_n^i)}{\lambda_\xi(u_n)u_n}) \equiv \frac{1}{\pi^{n+1}} A_0^{(i)} \pi^{t+s_q(\frac{i-q^t}{q-1})} \pmod{\pi^{n+1}},$$

where $A_0^{(i)} \in \mathbb{Z}$ is the sum of all coefficients of terms with the exponent $t + s_q(\frac{i-q^t}{q-1})$ of π in the formulas $(*)_\ell$, $n-t \leq \ell \leq n$.

After a simple observation we see that there are two terms with coefficients not zero to be considered, namely in the cases $\ell = n-t$, $n-t+1$. Furthermore, these coefficients cancel out. Thus we obtain

$$(E_\xi(u_n^i), u_n)_n^\xi = 0 \quad \text{for } 1 \leq i \leq q^{n+1} - 1.$$

Because there is the isomorphism $\phi : \xi \xrightarrow{\sim} F$, $\phi'(0) = 1$ and $(\alpha, \beta)_n^F = \phi(\phi^{-1}(\alpha, \beta)_n^\xi)$ holds, we obtain, by denoting $v_n = \phi(u_n)$, the following

Theorem 1. Under the assumption $q > 2n + 2$ we have

$$\begin{aligned} (E_F(u_n^i), u_n)_n^F &= 0 \quad \text{for } 1 \leq i \leq q^{n+1} - 1, \\ (E_F(u_n^{q^{n+1}}), u_n)_n^F &= v_n. \end{aligned}$$

The second formula follows from the fact that $E_\xi(u_n^q) = [\pi]_\xi(E_\xi(u_n)) \bar{e}_\xi(\pi u_n)$, and repeatedly $E_\xi(u_n^{q^{n+1}}) = [\pi^{n+1}]_\xi(E_\xi(u_n)) \bar{e}_\xi(\pi^{n+1} u_n + \pi^n u_n^q + \dots + \pi u_n^{q^n})$, and from Lemma 3, namely $(E_\xi(u_n^{q^{n+1}}), u_n)_n^\xi = u_n$.

§4. Explicit formulas in prime division fields

In this section we give a generalization of Takagi's formulas stated in Introduction.

First, the formula of de Shalit reads as follows [2] :

For $\alpha \in F(\mathfrak{p}_n)$, $\beta \in L_{\pi, n+1}^\times$ take a power series $h \in X_0[[X]]$ such that $\alpha = h(v_n)$ and the Coleman power series $g(X) \in X_0[[X]]$ with $\beta = g(v_n)$. Then it holds that

$$(\alpha, \beta)_n^F = \left[\frac{1}{\pi^{n+1}} \left\{ \sum_{v \in \Lambda_{f, n+1}} \left(\lambda_F \circ h - \frac{\lambda_F \circ h \circ [\pi]_F}{\pi} \right) \delta g(v) + \frac{dh}{dX}(0) \left(1 - \frac{Ng}{g} \right)(0) \right\} \right]_F(v_n),$$

where Ng denotes Coleman's norm operator of g and δg means the logarithmic derivative of g , namely $(\delta g)(X) = \frac{1}{\lambda_F(X)} \frac{1}{g(X)} \frac{d}{dX} g(X)$.

By making use of de Shalit formula we obtain the following

Lemma 5. For $i \geq q$ or $j \geq q$ or $i \not\equiv 1 \pmod{(j, q-1)}$

we have

$$\frac{1}{\pi} T_0 \left(\frac{L(u_0^i) j u_0^{j-1}}{\lambda_\xi'(u_0) (1-u_0^j)} \right) \equiv 0 \pmod{\pi}.$$

For $q = i + mj$, $1 \leq m \leq q - 1$, $1 \leq i, j$

$$\frac{1}{\pi} T_0 \left(\frac{L(u_0^i) j u_0^{j-1}}{\lambda_{\xi}^i(u_0) (1-u_0^j)} \right) \equiv \begin{cases} 0 & (\text{mod } \pi) & (i = 1) , \\ j & (\text{mod } \pi) & (i \geq 2) . \end{cases}$$

Thus we have under the condition $q = i + mj$

$$(E_{\xi}(u_0^i), 1-u_0^j)_0^{\xi} = [-j]_{\xi}(u_0) \quad \text{for } i \geq 1 .$$

From this lemma we obtain

$$(E_{\xi}(u_0^i), E(u_0^j))_0^{\xi} = [j]_{\xi}(u_0) \quad \text{for } q = i + p^a j ,$$

$$(E_{\xi}(u_0^i), E(u_0^j))_0^{\xi} = 0 \quad \text{otherwise.}$$

Herein $E(X)$ is the ordinary Artin-Hasse exponential series in Introduction.

Finally, for any Lubin-Tate group F isomorphic to ξ over $\mathcal{O}$ belonging to the prime π we obtain the following

Theorem 2. We have

$$(E_F(u_0^i), E(u_0^j))_0^F = [j]_F(v_0) \quad \text{if } q = i + p^a j, p^a | q ,$$

$$(E_F(u_0^i), E(u_0^j))_0^F = 0 \quad \text{otherwise ,}$$

$$(E_F(u_0^i), u_0)_0^F = 0 \quad \text{if } 1 \leq i \leq q - 1 ,$$

$$(E_F(u_0^q), u_0)_0^F = v_0 .$$

In particular, in the case where $k = \mathbb{Q}_p$, $q = p$, $F = G_m$, $\pi = p$ and necessarily $v_0 = \zeta_p^{-1} - 1$, $u_0 = -\tilde{\omega}$, the formulas in Theorem 2 coincide just with Takagi's formulas quoted in Introduction.

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] E. de Shalit, The explicit reciprocity law in local class field theory, Duke Math. J., 53(1986), 163-176.
- [3] J. Dieudonné, On the Artin-Hasse exponential series, Proc. Amer. Math. Soc., 8(1957), 210-214.
- [4] K. Iwasawa, On explicit formulas for the norm residue symbol, J. Math. Soc. Japan, 20(1968), 151-164.
- [5] K. Iwasawa, Local class field theory, Oxford Univ. press, 1986.
- [6] K. Shiratani and M. Ishibashi, On explicit formulas for the norm residue symbol in prime cyclotomic fields, Mem. Fac. Scie., Kyushu Univ., 38(1984), 203-231.
- [7] A. Wiles, Higher explicit reciprocity law, Ann. Math., 107(1978), 235-254.