数理解析研究所講究録
第 797 巻 1992 年 141-152

Lubin-Tate 群による高木の公式

九大理・末吉 豊 (Yutaka Sueyoshi)

§1. 序

p を奇素数とし、$\mathbb{Q}_p$ を有理 p 進数体とする。ζ で 1 の原始 p 乗根を表わし、$\mathbb{Q}_p(\zeta)$ を素円体とする。$a, b \in \mathbb{Q}_p(\zeta)^\times$ に対し、$(a,b) := \sqrt[p]{b}^{\,\sigma_a - 1}$, $\sigma_a \in Gal(\mathbb{Q}_p(\zeta)^{ab}/\mathbb{Q}_p(\zeta))$ で p-th Hilbert symbol を定義する。ここで、$\mathbb{Q}_p(\zeta)^{ab}$ は $\mathbb{Q}_p(\zeta)$ の最大アーベル拡大を表わし、σ_a はアルティン記号である。$\sqrt[p-1]{-p} \in \mathbb{Q}_p(\zeta)$ を $\sqrt[p-1]{-p} \equiv \zeta - 1 \mod (\zeta-1)^2$ をみたすようにとる。このとき、$\mathrm{mod}\ \mathbb{Q}_p(\zeta)^{\times p}$ で explicit に定められた $\mathbb{Q}_p(\zeta)^\times$ の主単数 $\kappa_1, \cdots, \kappa_p$ が存在して、$\{\sqrt[p-1]{-p}, \kappa_1, \cdots, \kappa_p\}$ が $\mathbb{Q}_p(\zeta)^\times/\mathbb{Q}_p(\zeta)^{\times p}$ の 1 組の底を代表し(高木の底とよばれる)、次の explicit formulas が成り立つ。

<u>高木の公式</u>([8])

$$\left(\sqrt[p-1]{-p}\,,\ \kappa_i\right) = \begin{cases} \zeta & (i = p), \\ 1 & (\text{その他}), \end{cases} \qquad (\text{補充法則})$$

$$(\kappa_j,\ \kappa_i) = \begin{cases} \zeta^{-j} & (i+j = p), \\ 1 & (\text{その他}). \end{cases} \qquad (\text{一般法則})$$

この公式は、白谷先生（[5]）により、Lubin-Tate群の素分点を付加した体の場合に一般化された。その証明には、Iwasawa-Wiles公式（[2, 3, 11]）及びde Shalit公式（[1]）を用いている。ここでは、Vostokov公式（[9, 10]）を用いて素巾分点の体の場合に得られた結果を述べる。詳しくは、[7]をご覧下さい。

§2. $k_n^\times$ 及び $F(\mathfrak{p}_n)$ の生成元

p を奇素数とし、$k/\mathbb{Q}_p$ を有限次拡大とする。$\mathcal{O}$ を k の整数環，$\mathfrak{p}$ を $\mathcal{O}$ の素イデアルとする。π を k の素元とし、$F(X, Y) \in \mathcal{O}[[X, Y]]$ を π に属する Lubin-Tate 群すなわち、F は1次元可換形式群で π に付随する F の endomorphism $[\pi]_F$ が

$$\begin{cases} [\pi]_F(X) \equiv X^q & \bmod \pi, \\ [\pi]_F(X) \equiv \pi X & \bmod \deg 2 \end{cases}$$

をみたすとする。ここで、$q = p^f$ は k の剰余体 $\mathcal{O}/\mathfrak{p}$ の元の個数を表わす。k_A で k の代数閉包を表わし、$v_n \in k$ を F の原始 π^n-分点として、$k_n := k(v_n)$ とおく。$\mathfrak{p}_n$ を k_n の整数環の素イデアルとし、$F(\mathfrak{p}_n)$ で付随する formal module を表わす。

$\alpha \in k_n^\times$, $\beta \in F(\mathfrak{p}_n)$ に対し、一般化された Hilbert symbol が

$$(\alpha, \beta)_n^F := \rho^{\sigma_\alpha} \underset{F}{-} \rho \quad , \rho \in k_A \ , [\pi^n](\rho) = \beta, \ \sigma_\alpha \in Gal(k_n^{ab}/k_n)$$

で定義される（[11]）。

$\lambda_F : F \xrightarrow{\sim} G_a$ を F の logarithm で $\lambda_F'(0) = 1$ をみたすものとし、

[9, §2 ; 4, §1] に従って 2つの巾級数

$$\begin{cases} E_F(X) := \lambda_F^{-1}\left(\sum_{\ell=0}^{\infty} \dfrac{X^{q^\ell}}{\pi^\ell}\right) \in X\mathcal{O}[[X]], \\ E(X) := 1 + E_{\mathbb{G}_m}(X) = \exp\left(\sum_{m=0}^{\infty} \dfrac{X^{p^m}}{p^m}\right) \in 1 + X\mathbb{Z}_p[[X]] \end{cases}$$

を定義する。$E(X)$ は Artin-Hasse-Šafarevič の関数として知られている。F_0 を basic Lubin-Tate 群 i.e. $[\pi]_{F_0}(X) = X^q + \pi X$ に付随する Lubin-Tate 群とし、$u_n := (\lambda_{F_0}^{-1} \circ \lambda_F)(v_n)$ を F_0 の原始 π^n-分点とすると、$k_n = k(v_n) = k(u_n)$ である。$\mathcal{R}$ を $\mathcal{O}/\mathfrak{p}$ の乗法的代表系とし、e を $k/\mathbb{Q}_p$ の分岐指数とする。次のようにおく。

$$R_1 := \left\{ E(\theta u_n^j) \;\middle|\; \theta \in \mathcal{R},\ 1 \leqq j < \frac{pe(q-1)q^{n-1}}{p-1}\ (p \nmid j) \text{ or } j = \frac{pe(q-1)q^{n-1}}{p-1} \right\},$$

$$R_2 := \left\{ E_F(u_n^i) \;\middle|\; 1 \leqq i < q^n\ (q \nmid i) \right\} \cup \{\kappa\}.$$

但し、ここで

$$\kappa := \lambda_F^{-1}\left(\sum_{\ell=0}^{\infty} \frac{1}{\pi^\ell} [\pi^n]_{F_0}(u_n^{q^\ell})\right)$$

は [9, Proposition 1] で定義されている $F(\mathfrak{p}_n)$ の π^n-primary element である (i.e. κ の $[\pi^n]_F$-分点は k_n 上に不分岐拡大を生成する)。

[4, §1] により、R_1 は $k_n^\times$ の主単数群 $1 + \mathfrak{p}_n$ の $\mathbb{Z}_p$-生成系をなす。また、[9, §4, Proposition 3 及び Remark] により、R_2 は $\mathcal{O}/(\pi^n)$-module $F(\mathfrak{p}_n)/[\pi^n]_F(F(\mathfrak{p}_n))$ の 1 組の底を代表する。更に [9, Proposition 1] により、

$$(1) \qquad \begin{cases} (u_n, \kappa)_n^F = (\lambda_F^{-1} \circ \lambda_{F_0})((u_n, \kappa)_n^{F_0}) = v_n, \\ (E(\theta u_n^j), \kappa)_n^F = 0 \qquad (\forall E(\theta u_n^j) \in R_1) \end{cases}$$

が成り立つ。

特に $k=\mathbb{Q}_p$, $n=1$, $\pi=p$, $F=\mathbb{G}_m=X+Y+XY$ とすると、$v_1=\zeta-1$, $u_1=\sqrt[p-1]{-p}$ となり、

$$\left\{\sqrt[p-1]{-p},\ E(u_1^i)^{(-1)^{i-1}}\ (1\leqq i\leqq p-1),\ \exp\Big(\sum_{\ell=0}^{\infty}\frac{1}{p^\ell}[p]_{F_0}(u_1^{p^\ell})\Big)\right\}$$

が mod $\mathbb{Q}_p(\zeta)^{\times p}$ で高木の底と一致する([6, Theorem 3.1])。これについては§4も参照して下さい。

白谷先生の公式は次のように述べられる。

<u>Shiratani の公式</u>([5, Theorem 1 及び Theorem 2])

(2)
$$(u_n, E_F(u_n^i))_n^F = \begin{cases} v_n & (i=q^n), \\ 0 & (1\leqq i<q^n), \end{cases} \qquad (\text{補充法則})$$

$$(E(u_1^j), E_F(u_1^i))_1^F = \begin{cases} [j]_F(v_1) & (i+p^m j=q,\ {}^{\exists}m\geqq 0), \\ 0 & (\text{その他}). \end{cases} \qquad (\text{一般法則})$$

$F=\mathbb{G}_m$ とおけば高木の公式が得られる。(2) は仮定 $q>2n$ の下で証明されたが、§3で述べる Vostokov 公式を用いれば一般に証明できる。以下で $n\geqq 2$ のときの一般法則を与える。

§3. 一般法則

以下で $(E(\theta u_n^j), E_F(u_n^i))_n^F$, $n\geqq 2$ を計算する。

$$(E(\theta u_n^j), E_F(u_n^i))_n^F = (\lambda_F^{-1}\circ\lambda_{F_0})\big((E(\theta u_n^j), E_{F_0}(u_n^i))_n^{F_0}\big)$$

に注意すれば、$F=F_0$ のときに計算できればよいことがわかる。

一般に $\alpha\in k_n^{\times}$, $\beta\in F_0(\mathfrak{p}_n)$ に対し、

$$\begin{cases} \alpha = u_n^a \cdot \eta \cdot \varepsilon(u_n), \quad a \in \mathbb{Z}, \ \eta \in \mathcal{R}, \ \varepsilon(X) \in 1 + X\mathcal{O}_T[[X]], \\ \beta = B(u_n), \quad B(X) \in X\mathcal{O}[[X]] \end{cases}$$

とかく。ここで、$\mathcal{O}_T$ は $K/\mathbb{Q}_p$ の惰性体 T の整数環を表わす。

$A(X) := X^a \cdot \eta \cdot \varepsilon(X)$ とおき、

$$\Phi(X) := -\frac{1}{\pi}\left\{ \log \varepsilon(X) - \frac{1}{q} \log \varepsilon(X^q) \right\} \frac{d}{dX}\left(\lambda_{F_0} \circ B(X^q)\right) + \left\{ \lambda_{F_0} \circ B(X) - \frac{1}{\pi} \lambda_{F_0} \circ B(X^q) \right\} A^{-1} \frac{dA}{dX} \quad \in \mathcal{O}[[X]]$$

と定義するとき、

<u>Vostokovの公式</u>（[10, Theorem 4]）

$$(\alpha, \beta)_n^{F_0} = \left[\mathrm{res}_X \, \Phi/[\pi^n]_{F_0} \right]_{F_0}(u_n).$$

但し、

$$\begin{cases} \Phi/[\pi^n]_{F_0} \in \mathcal{O}\{X\} := \left\{ \varphi(X) = \sum_{i=-\infty}^{\infty} a_i X^i \ \middle| \ a_i \in \mathcal{O}, \ a_i \to 0 \ (i \to -\infty) \right\}, \\ \mathrm{res}_X \, \varphi(X) := a_{-1}, \quad \varphi(X) = \sum_{i=-\infty}^{\infty} a_i X^i \in \mathcal{O}\{X\}. \end{cases}$$

が成り立つ。[9, §1]により、$\varphi(X) = \sum_{i=-\infty}^{\infty} a_i X^i \in \mathcal{O}\{X\}$ が $\mathcal{O}\{X\}$ で可逆であるための必要十分条件は、a_i が $\mathcal{O}$ の単元となるような i が存在することであり、i_0 をそのような i の最小値とし、$\varphi(X) = a_{i_0} X^{i_0}(1 + \psi(X))$ とかくと、$1/\varphi = a_{i_0}^{-1} X^{-i_0}(1 - \psi + \psi^2 - \cdots)$ となる。従って特に $[\pi^n]_{F_0}(X) = X^{q^n} + \cdots + \pi^n X$ は $\mathcal{O}\{X\}$ において可逆であり、$\Phi/[\pi^n]_{F_0}$ は意味をもつ。

さて、$\alpha = E(\theta u_n^j)$, $\beta = E_{F_0}(u_n^i)$ とすれば

$$\begin{cases} A(X) = \varepsilon(X) = E(\theta X^j) = \exp\left(\sum_{m=0}^{\infty} \theta^{p^m} \frac{X^{p^m j}}{p^m} \right) \in 1 + X\mathcal{O}_T[[X]], \\ B(X) = E_{F_0}(X^i) = \lambda_{F_0}^{-1}\left(\sum_{l=0}^{\infty} \frac{X^{q^l i}}{\pi^l} \right) \in X\mathcal{O}[[X]] \end{cases}$$

ととれるから、

$$(E(\theta u_n^j),\ E_F(u_n^i))_n^F = (\lambda_F^{-1}\circ\lambda_{F_0})\big((E(\theta u_n^j),\ E_{F_0}(u_n^i))_n^{F_0}\big)$$

$$= [\mathrm{res}_X\ \Phi/[\pi^n]_{F_0}]_F(v_n),$$

(3) $$\Phi(X) = -\sum_{m=0}^{f-1}\sum_{\ell=0}^{\infty}\frac{q^{\ell+1} i\,\theta^{p^m}}{p^m\pi^{\ell+1}}X^{p^m j+q^{\ell+1}i-1} + \sum_{m=0}^{\infty} j\,\theta^{p^m}X^{i+p^m j-1}$$

を得る。 $1/[\pi^n]_{F_0}$ を $n=2,3$ について計算すると、

$$[\pi^2]_{F_0}(X) = (X^q+\pi X)^q+\pi(X^q+\pi X) \equiv X^{q^2}+\pi X^q \qquad \mathrm{mod}\ \pi^2,$$

$$1/[\pi^2]_{F_0} \equiv X^{-q^2}(1-\pi X^{-q^2+q}) \qquad \mathrm{mod}\ \pi^2,$$

$$[\pi^3]_{F_0}(X) \equiv (X^{q^2}+\pi X^q)^q+\pi(X^{q^2}+\pi X^q)$$

$$\equiv X^{q^3}+q\pi X^{q^3-q^2+q}+\pi X^{q^2}+\pi^2X^q \qquad \mathrm{mod}\ \pi^3,$$

$$1/[\pi^3]_{F_0} \equiv X^{-q^3}(1-q\pi X^{-q^2+q}-\pi X^{-q^3+q^2}-\pi^2X^{-q^3+q}+\pi^2X^{-2q^3+2q^2})$$

$$\mathrm{mod}\ \pi^3.$$

従って、 $\mathrm{res}_X\ \Phi/[\pi^n]_{F_0}$, $n=2,3$ を計算して次を得る。

<u>命題 1</u> $E(\theta u_n^j)\in R_1$, $E_F(u_n^i)\in R_2$ $(q\nmid i)$ とするとき、

$n=2,3$ について

$$(E(\theta u_2^j),\ E_F(u_2^i))_2^F = \begin{cases} [-p\theta]_F(v_2) & (e=f=1,\ j=p^2,\ i=p-1), \\ [j\theta^{p^m}]_F(v_2) & (i+p^m j = q^2,\ {}^\exists m\geqq 0), \\ [-j\theta^{p^m}]_F(v_1) & (i+p^m j = 2q^2-q,\ {}^\exists m\geqq 0), \\ 0 & (\text{その他}). \end{cases}$$

$$\begin{cases} [-p^2\theta+\frac{p^2(p-1)}{\pi}\theta]_F(v_3) & (e=f=1,\ j=p^3,\ i=p-1), \\ [-p\theta]_F(v_2) & (e=f=1,\ j=p^3,\ i=p^2-1), \end{cases}$$

$$
(E(\theta u_3^j),\ E_F(u_3^i))_3^F = \begin{cases} [2p^2\theta]_F(v_3) & (e=f=1,\ j=p^3,\ i=2p-2), \\ [j\theta^{p^m}]_F(v_3) & (i+p^m j = q^3,\ \exists m \geqq 0), \\ [-jp\,\theta^{p^m}]_F(v_2) & (e=f=1,\ i+j=p^3+p^2-p), \\ [-j\theta^{p^m}]_F(v_2) & (i+p^m j = 2q^3-q^2,\ \exists m \geqq 0), \\ [-j\theta^{p^m}]_F(v_1) & (i+p^m j = 2q^3-q,\ \exists m \geqq 0), \\ [j\theta^{p^m}]_F(v_1) & (i+p^m j = 3q^3-2q^2,\ \exists m \geqq 0), \\ 0 & (\text{その他}). \end{cases}
$$

一般の n について次が成り立つ。

<u>定理 1</u>　$E(\theta u_n^j) \in R_1$, $E_F(u_n^i) \in R_2$ $(q \nmid i)$ とするとき.

(i) $\begin{cases} (E(\theta u_n^j),\ E_F(u_n^i))_n^F = [j\theta^{p^m}]_F(v_n) & (i+p^m j = q^n,\ \exists m \geqq 0), \\ (E(\theta u_n^j),\ E_F(u_n^i))_n^F \in \{[c]_F(v_{n-1}) \mid c \in \mathcal{O}\} & (\text{その他}). \end{cases}$

(ii) $p \nmid j$ かつ $q \nmid i + p^m j$, $0 \leqq {}^\forall m \leqq f-1$ あるいは $i + p^{f-1} j < q^n$ のいずれかの条件が成り立てば,

$$(E(\theta u_n^j),\ E_F(u_n^i))_n^F = 0 .$$

(証明の概略)　$[\pi^n]_{F_0}(X) = \sum_{s=1}^{q^n} a_s X^s$ $(a_{q^n} = 1)$ とかくとき. n についての induction により容易に. $q \nmid s$ ならば $a_s \equiv 0 \bmod \pi^n$ がわかる。従って $1/[\pi^n]_{F_0} = X^{-q^n} \sum_{s=0}^{\infty} b_s X^{-s}$ $(b_0 = 1)$ とかくとき、$q \nmid s$ ならば $b_s \equiv 0 \bmod \pi^n$ が成り立つ。従って (3) より、

$$
(4) \qquad \mathrm{res}_X\, \Phi/[\pi^n]_{F_0} \equiv \sum_{\substack{q \mid s \\ s \geqq 0}} \Bigl(- \sum_{\substack{p^m j + q^{\ell+1} i = q^n + s \\ 0 \leqq m \leqq f-1,\ \ell \geqq 0}} \frac{q^{\ell+1} i\, \theta^{p^m}}{p^m \pi^{\ell+1}} + \sum_{\substack{i + p^m j = q^n + s \\ m \geqq 0}} j\theta^{p^m} \Bigr) b_s \quad \bmod \pi^n
$$

となる。(4) の右辺を条件に従って計算することにより、定理の式を得る。

§4. 高木公式の一般化

$k=\mathbb{Q}_p$, $\pi=p$, $F=\mathbb{G}_m$, $u_n=\zeta_n-1$, $k_n=\mathbb{Q}(\zeta_n)$ (ζ_n : 1の原始 p^n 乗根) とおく。$a, b\in k_n^\times$ に対し、$(a,b)_n := \sqrt[p^n]{b}^{\,\sigma_a-1}$ により、p^n-th Hilbert symbol を表わす。

$$\varepsilon_i := \begin{cases} E(u_n^i) & (1\leqq i<p^n,\ p\nmid i), \\ \exp\left(\sum_{l=0}^{\infty} \frac{1}{p^l}[p^n]_{F_0}(u_n^{p^l})\right) & (i=p^n) \end{cases}$$

と定義すれば、$R:=\{u_n, \varepsilon_1, \cdots, \varepsilon_{p^n}\}$ は $\mathbb{Z}_p/(p^n)$-module $k_n^\times/k_n^{\times p^n}$ の1組の底を代表する。特に $n=1$ のとき、§2 で述べたように、

$$\kappa_i \equiv \varepsilon_i^{(-1)^{i-1}} \mod \mathbb{Q}_p(\zeta_1)^{\times p} \qquad (1\leqq i\leqq p)$$

となり、R は高木の底と本質的に同じである。(1), (2) より、

$$(u_n, \varepsilon_i)_n = \begin{cases} \zeta_n & (i=p^n), \\ 1 & (\text{その他}) \end{cases} \qquad (\text{補充法則})$$

を得る。一般法則については、$i=p^n$ のとき、(1) より、

(5) $$(\varepsilon_j, \varepsilon_{p^n}) = 1 \qquad (\forall \varepsilon_j\in R)$$

が成り立ち、一般の i, j について次が成り立つ。

<u>命題 2</u> $1\leqq i, j<p^n$, $p\nmid i$, $p\nmid j$ とするとき、$n=2, 3, 4$ について

$$
(\varepsilon_j, \varepsilon_i)_2 = \begin{cases} \zeta_2^{\,j} & (i+j = p^2), \\ \zeta_1^{-j} & (i+j = 2p^2 - p), \\ 1 & (\text{その他}). \end{cases}
$$

$$
(\varepsilon_j, \varepsilon_i)_3 = \begin{cases} \zeta_3^{\,j} & (i+j = p^3), \\ \zeta_1^{-j} & (i+j = p^3 + p^2 - p), \\ \zeta_2^{-j} & (i+j = 2p^3 - p^2), \\ \zeta_1^{-j} & (i+j = 2p^3 - p), \\ 1 & (\text{その他}). \end{cases}
$$

$$
(\varepsilon_j, \varepsilon_i)_4 = \begin{cases} \zeta_4^{\,j} & (i+j = p^4), \\ \zeta_1^{-j} & (i+j = p^4 + p^2 - p), \\ \zeta_2^{-j} & (i+j = p^4 + p^3 - p^2), \\ \zeta_1^{-j} & (i+j = p^4 + p^3 - p), \\ \zeta_1^{-\frac{p-1}{2}j} & (i+j = p^4 + 2p^3 - 2p^2), \\ \zeta_3^{-j} & (i+j = 2p^4 - p^3), \\ \zeta_1^{-j} & (i+j = 2p^4 - p^3 + p^2 - p), \\ \zeta_2^{-j} \cdot \zeta_1^{2j} & (i+j = 2p^4 - p^2), \\ \zeta_1^{-j} & (i+j = 2p^4 - p), \\ 1 & (\text{その他}). \end{cases}
$$

高木の底の特徴づけ([8, §1; 6, §3])が次のように一般化される。$\eta \in V := \{\eta \in \mathbb{Z}_p^{\times} \mid \eta^{p-1} = 1\}$ に対し、$\sigma_\eta \in \mathrm{Gal}(\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p)$ を

$\zeta_n^{\sigma_\eta} = \zeta_n^{\eta}$ で定義する。$H := \{\sigma_\eta \mid \eta \in V\} \subseteq Gal(\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p)$ とおく。
$U := 1 + \mathfrak{P}_n$ を $\mathbb{Q}_p(\zeta_n)^\times$ の主単数群とする。

$$1_i := \frac{1}{p-1} \sum_{\eta \in V} \eta^{-i} \sigma_\eta \in \mathbb{Z}_p[H] \qquad (1 \leq i \leq p-1)$$

と定義すると、

$$1 = \sum_{i=1}^{p-1} 1_i \ , \quad 1_i \cdot 1_j = \delta_{ij} 1_i \quad (\delta_{ij} : \text{Kronecker のデルタ記号})$$

が成り立ち、1_i $(1 \leq i \leq p-1)$ は群環 $\mathbb{Z}_p[H]$ の原始直交巾等元である。従って U は $\mathbb{Z}_p[H]$-module として次の直積分解をもつ。

$$U = A^{(1)} \times \cdots \times A^{(p-1)},$$

$$A^{(i)} := U^{1_i} = \{ \varepsilon \in U \mid \varepsilon^{\sigma_\eta} = \varepsilon^{\eta^i} \ , \ ^\forall \eta \in V \}.$$

Artin-Hasse logarithm $\lambda_a(X) := \sum_{\ell=0}^{\infty} \frac{X^{p^\ell}}{p^\ell}$ に付随する Lubin-Tate 群を F_a とする。$\eta \in V$ とすると $\lambda_a \circ [\eta]_{F_a}(X) = \eta \lambda_a(X) = \lambda_a(\eta X)$ が成り立つから、$[\eta]_{F_a}(X) = \eta X$ を得る。一方、よく知られているように([11, Lemma 20])、$[\eta]_{F_0}(X) = \eta X$ である。従って

$$\sigma_\eta(u_n) = ((\lambda_{F_0}^{-1} \circ \log)(\zeta_n))^{\sigma_\eta} = (\lambda_{F_0}^{-1} \circ \log)(\zeta_n^\eta) = \eta u_n,$$

(6)
$$\varepsilon_j^{\sigma_\eta} = ((\exp \circ \lambda_a)(u_n^j))^{\sigma_\eta} = (\exp \circ \lambda_a)(\eta^j u_n^j) = \varepsilon_j^{\eta^j} \quad (p \nmid j),$$

$$\varepsilon_{p^n}^{\sigma_\eta} = \left(\exp\left(\sum_{\ell=0}^{\infty} \frac{1}{p^\ell} [p^n]_{F_0}(u_n^{p^\ell})\right)\right)^{\sigma_\eta} = \exp\left(\sum_{\ell=0}^{\infty} \frac{1}{p^\ell} [p^n]_{F_0}(\eta^{p^\ell} u_n^{p^\ell})\right)$$
$$= \exp\left(\eta \sum_{\ell=0}^{\infty} \frac{1}{p^\ell} [p^n]_{F_0}(u_n^{p^\ell})\right) = \varepsilon_{p^n}^{\eta} = \varepsilon_{p^n}^{\eta^{p^n}}$$

が成り立つ、

$$A^{(i)} = \langle \varepsilon_j \in R \mid j \equiv i \mod p-1 \rangle \qquad (1 \leq {}^\forall i \leq p-1)$$

が得られる。これは高木の底の特徴づけの一般化を与える。

注: 高木の底 $\{\kappa_1, \cdots, \kappa_p\}$ は次の条件で特徴づけられている

([8, §1 ; 6, §3])。

(i) $\kappa_i^{\sigma_n} \equiv \kappa_i^{\eta^i} \mod U^p \quad (1 \leqq \forall i \leqq p,\ \forall \eta \in V)$,

(ii) $\kappa_i \equiv 1-(1-\zeta)^i \mod (1-\zeta)^{i+1} \quad (1 \leqq \forall i \leqq p)$,

(iii) $\kappa_1 \equiv \zeta \mod U^p$.

これにより、$\kappa_1, \cdots, \kappa_p$ は mod U^p で一意的に定まる。

定理 2　$\varepsilon_i, \varepsilon_j \in R$ とするとき、

$$(\varepsilon_j, \varepsilon_i)_n = \begin{cases} \zeta_n^j & (i+j=p^n), \\ 1 & (i+j \not\equiv p \mod p(p-1) \text{ 又は } i+j<p^n). \end{cases}$$

（証明）第１の式は定理１(i)から得られる。$j=p^n$ 又は $i=p^n$ のときは、第２の式は(5)から従う。$p \nmid j$, $p \nmid i$ とする。$\eta \in V$ に対し、(6)より

$$(\varepsilon_j, \varepsilon_i)_n^{\eta} = (\varepsilon_j, \varepsilon_i)_n^{\sigma_n} = (\varepsilon_j^{\eta^j}, \varepsilon_i^{\eta^i})_n = (\varepsilon_j, \varepsilon_i)_n^{\eta^{i+j}}$$

となるから、

$$i+j \not\equiv 1 \mod p-1 \text{ ならば } (\varepsilon_j, \varepsilon_i)_n = 1$$

となる。一方、定理１(iii)より

$$i+j \not\equiv 0 \mod p \text{ 又は } i+j<p^n \text{ ならば } (\varepsilon_j, \varepsilon_i)_n = 1$$

である。これらにより第２の式を得る。

References

[1] E. de Shalit, The explicit reciprocity law in local class field theory, Duke Math. J. 53(1986), 163-176.

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

[3] K. Iwasawa, Local Class Field Theory, Oxford University Press, New York, 1986.

[4] I. R. Šafarevič, A general reciprocity law, Mat. Sb. 26(68) (1950), 113-146; English transl. in Amer. Math. Soc. Transl. (2) 4(1968), 73-106.

[5] K. Shiratani, On the exponential series of formal groups, RIMS Kokyuroku 658(1988), 85-95.

[6] K. Shiratani and M. Ishibashi, On explicit formulas for the norm residue symbol in prime cyclotomic fields, Mem. Fac. Sci. Kyushu Univ. Ser. A 38(1984), 203-231.

[7] Y. Sueyoshi, A generalization of Takagi's explicit formulas by Lubin-Tate groups, preprint.

[8] T. Takagi, On the law of reciprocity in the cyclotomic corpus, Proc. Phys.-Math. Soc. Japan 4(1922), 173-182.

[9] 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.

[10] S. V. Vostokov, Symbols on formal groups, Izv. Akad. Nauk SSSR Ser. Mat. 45(1981), 985-1014; English transl. in Math. USSR-Izv. 19(1982), 261-284.

[11] A. Wiles, Higher explicit reciprocity laws, Ann. of Math. 107(1978), 235-254.