数理解析研究所講究録
第 721 巻 1990 年 131-141

円分体の単数のP進展開について

東工大　栗原文香　(Fumika Kurihara)

§0.　pを奇素数，ζ_1を1の原始p乗根．$\mathbb{Q}(\zeta_1)^+$を$\mathbb{Q}(\zeta_1)$の最大実部分体，$\pi = 1-\zeta_1$とする。このとき$\mathbb{Z}[\zeta_1]$の任意の元αで，$\mathbb{Z}$の元でなく，pと素なものは，

$$\alpha \equiv a + b\pi^c \pmod{\pi^{c+1}},\ a, b, c \in \mathbb{Z},\ p \nmid ab,\ c \not\equiv 0 \pmod{p-1}$$

と展開でき，cはαに対して一意的に決まることが知られている。L. Washingtonは論文 [10] で次を示した。

(I)　$\exists \{\eta_2, \eta_4, \cdots, \eta_{p-3}\}$: basis for the unit group mod $\{\pm 1\}$ of $\mathbb{Z}[\zeta_1]^+$

s.t. $\eta_i \equiv a_i + b_i \pi^{c_i} \pmod{\pi^{c_i+1}}$

with $c_i = i + (p-1)u_i'$ for some $u_i' \in \mathbb{Z}$, $0 \leq u_i' \leq u_i = v_p(L_p(1, \omega^i))$

ここで　v_p : p-adic valuation, $v_p(p) = 1$.

ω : Teichmüller character.

(II)　h : $\mathbb{Q}(\zeta_1)^+$の類数とすると，

$$v_p(h) = \sum_{\substack{i=2 \\ \text{even}}}^{p-3} (u_i - u_i')$$

以下の論説は、このWashingtonの結果のp巾への一般化に関するもので、詳しくは、J. Number Theory (1989) Vol.32 No.2, 226 - 253 に掲載されています。

§1. 単数のp進展開

p：奇素数を1つfixし、$n \geqq 0 \in \mathbb{Z}$，ζ_{n+1}：1の原始p^{n+1}乗根とする。K_{n+1}を$\mathbb{Q}(\zeta_{n+1})$の最大実部分体$\mathbb{Q}(\zeta_{n+1})^{+}$と$\mathbb{Q}$との中間体で指数$[\mathbb{Q}(\zeta_{n+1})^{+} : K_{n+1}] = d$が$p$と素なものとする。

$\pi_{n+1} = (1-\zeta_{n+1})(1-\zeta_{n+1}^{-1})$，$\pi = N_{\mathbb{Q}(\zeta_{n+1})^{+}/K_{n+1}}(\pi_{n+1})$とする。このとき、$K_{n+1} \ni {}^{\forall}\alpha$：integer，$\alpha \notin \mathbb{Z}$，$\alpha$：$p$と素 は、

$$\alpha \equiv a + b\pi^{c} \pmod{\pi^{c+1}},\ a, b, c \in \mathbb{Z},\ p \nmid ab,\ c \not\equiv 0 \left(\mathrm{mod}\ \frac{p^{n}(p-1)}{2d}\right)$$

と展開でき、cはαに対して一意的に決まる。今後この形の展開は特にことわらないが、すべて上の条件のものとする。

$E_{K_{n+1}}$：K_{n+1}の全単数群

$$r = \mathrm{rank}(E_{K_{n+1}}) = \frac{p^{n}(p-1)}{2d} - 1$$

としたとき、次が得られる。

Th. 1

$E_{K_{n+1}} \supset {}^{\forall}E$：finite index subgroupに対して

${}^{\exists}\{\eta_1, \eta_2, \cdots, \eta_r\}$：basis for $E/\{\pm 1\}$

s.t. $\eta_i^{p^n} \equiv a_i + b_i\pi^{c_i} \pmod{\pi^{c_i+1}}$ $\quad 1 \leq i \leq r$

with $c_i = i + \dfrac{p^{n}(p-1)}{2d} u_i$ for some $u_i \geqq 0 \in \mathbb{Z}$

Remarks.

① c_i, u_i はEに対して一意的に決まり basis のとり方によらない。今後Eに対して Th.1 のようにして決まる c_i. u_i を $c_i(E)$. $u_i(E)$ と書くことにする。

② $E_{k_{n+1}} \supset^{\forall} E \supset^{\forall} E'$: finite index subgroups に対して

$$c_i(E) \leq c_i(E'), \quad u_i(E) \leq u_i(E') \quad \text{for } {}^{\forall}i$$

が成り立つ。

§2. The Main Theorem

Th. 2 (the main theorem)

$E_{k_{n+1}} \supset^{\forall} E \supset^{\forall} E'$: finite index subgroups に対して.

$$v_p([E:E']) = \sum_{i=1}^{r} (u_i(E') - u_i(E))$$

ただし v_p : p-adic valuation , $v_p(p) = 1$.

証明の概略

$$v_p([E:E']) = v_p(R_p(E'^{p^n})) - v_p(R_p(E^{p^n}))$$

なので. $v_p(R_p(E^{p^n}))$ を計算する。ここで. 次のようなEの subgroup E_r を作る。

${}^{\forall}M \in \mathbb{Z}$: 十分大　1つ fix する

$m_1, m_2, \cdots, m_r \in \mathbb{Z}$

s.t. $m_i + u_i(E) \equiv 0 \pmod{p^M}$, $0 \ll m_1 \ll \cdots \ll m_r$ をとる.

このとき．

$$E \supset E_r = \langle \eta'_1, \eta'_2, \cdots, \eta'_r \rangle$$

$$\text{s.t. (i)} \quad \eta_i'^{p^n} \equiv a_i + b_i \pi^{c_i} \pmod{P^M}$$

$$\text{with} \quad c_i = c_i(E) + \frac{p^n(p-1)}{2d} m_i$$

$$= i + \frac{p^n(p-1)}{2d}(m_i + u_i(E))$$

$$\text{(ii)} \quad v_p([E : E_r]) = \sum_{i=1}^{r} m_i$$

ここで．$Gal(K_{n+1}/\mathbb{Q}) = \{\sigma_j\}_{1 \leq j \leq r+1}$ とすると．

$$R_p(E_r^{p^n}) = \det(\log_p \eta_i'^{p^n \sigma_j})_{1 \leq i, j \leq r}$$

$$\equiv \det(\log_p(a_i + b_i \pi^{\sigma_j c_i}))_{1 \leq i, j \leq r} \pmod{P^M}$$

となる。v_pでの値を実際に計算すると．

$$v_p(\det(\log_p(a_i + b_i \pi^{\sigma_j c_i}))_{1 \leq i, j \leq r})$$

$$= \sum_{i=1}^{r} m_i + \sum_{i=1}^{r} u_i(E) + \delta(K_{n+1})$$

（ここで $\delta(K_{n+1})$ は K_{n+1} のみによりEによらない定数．）

となる。従って．Mが十分大であることから

$$v_p(R_p(E^{p^n})) = v_p(R_p(E_r^{p^n})) - \sum_{i=1}^{r} m_i$$

$$= \sum_{i=1}^{r} u_i(E) + \delta(K_{n+1})$$

となり定理が証明される。

E_{n+1} : $\mathbb{Q}(\zeta_{n+1})^+$の全単数群

C_{n+1} : $\mathbb{Q}(\zeta_{n+1})^+$の円単数群

$C_{K_{n+1}} = N_{\mathbb{Q}(\zeta_{n+1})^+/K_{n+1}}(C_{n+1})$ とする。

このとき、次が得られる。

Cor.

$h_{K_{n+1}}$: K_{n+1} の類数　としたとき、

$$v_p(h_{K_{n+1}}) = \sum_{i=1}^{r} \left(u_i(C_{K_{n+1}}) - u_i(E_{K_{n+1}}) \right)$$

Th.1, Th.2, Cor は最初に述べた Washington の結果の P 巾への拡張になっています。

§3. $u_i(E_{n+1})$, $u_i(C_{n+1})$ の性質

ここでは $K_{n+1} = \mathbb{Q}(\zeta_{n+1})^+$ とする。従って、$\pi = \pi_{n+1}$, $r = r_{n+1} = \frac{p^n(p-1)}{2} - 1$ とする。

(1) p-adic L-function との関係

簡単な計算より、

$$\sum_{i=1}^{r} u_i(C_{n+1}) = rn + v_p\left(p^n \prod_{\chi}{}' L_p(1,\chi)\right)$$

(ここで $\prod_{\chi}{}'$: mod p^{n+1} の nontrivial even Dirichlet characters)

が得られる。ここで、$n=0$ のときは Washington の結果より、

$$u_k(C_1) = v_p(L_p(1,\omega^{2k})) \quad \text{for } 1 \leq k \leq \frac{p-3}{2}$$

(ω: Teichmüller character)

が成り立つ。これより、$n>0$ で次が成り立つかということが自然に考えられる。

$$\begin{cases} \displaystyle\sum_{i\equiv k \pmod{\frac{p-1}{2}}} U_i(C_{n+1}) = v_p\Big(\prod_{\psi} L_p(1, \omega^{2k}\psi)\Big) + np^n \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{for } 1 \le k \le \frac{p-3}{2} \\ \displaystyle\sum_{i\equiv 0 \pmod{\frac{p-1}{2}}} U_i(C_{n+1}) = v_p\Big(p^n {\prod_{\psi}}' L_p(1, \psi)\Big) + n(p^n-1) \end{cases}$$

（ただし．$\prod_{\psi}$：mod p^{n+1} の Dirichlet characters s.t. $\psi^{p^n}=1$ の積
$\prod'_{\psi}$：上のもので nontrivial なものの積）

これらが成り立つかどうかについては．まだ完全にはわかっていないが．ある特殊な場合については次が言える．

Th.4 の Cor.

for $1 \le k \le \frac{p-3}{2}$;

$v_p(L_p(1, \omega^{2k})) = 0$

$$\Rightarrow \sum_{i\equiv k \pmod{\frac{p-1}{2}}} U_i(C_{n+1}) = v_p\Big(\prod_{\psi} L_p(1, \omega^{2k}\psi)\Big) + np^n$$
$$= np^n$$

・$v_p(L_p(1. \omega^{2k})) \neq 0$ なる k については $\sum_{i\equiv k \pmod{\frac{p-1}{2}}} U_i(C_{n+1})$ の値はよくわかっていない。

・$\sum_{i\equiv 0 \pmod{\frac{p-1}{2}}} U_i(C_{n+1})$ の値についてもよくわかっていないが．

$$\sum_{i\equiv 0 \pmod{\frac{p-1}{2}}} (U_i(C_{n+1}) - U_i(E_{n+1})) = 0$$

が成り立つ。

(2) $U_i(E_n)$ と $U_{ip}(E_{n+1})$ の関係

次が成り立つ。

(i) $U_{ip}(E_{n+1}) \leq U_i(E_n) + 1$ for $\forall i = 1, \cdots, r_n$

(ii) $i \not\equiv 0 \pmod{\frac{p-1}{2}}$ なる i について.

if $U_{ip}(E_{n+1})$ があまり大きくない

($U_{ip}(E_{n+1}) \leq n-1$ なら十分)

$\Rightarrow U_i(E_n) \leq U_{ip}(E_{n+1})$

(3) $\lambda = 0$ となるための条件

λ: $\mathbb{Q}(\zeta_1)^+$ の cyclotomic $\mathbb{Z}_p$-extension の Iwasawa λ-invariant とする.

<u>**Def.**</u>

$E_{n+1} \supset {}^\forall E$: finite index subgroup とする

for each $i = 1, 2, \cdots, r_{n+1}$;

$U_i(E)$: normal $\overset{\text{def}}{\Leftrightarrow}$ $U_i(E) = (U_i(E_{n+1})$ のとりうる最小の値 $)$

ここで. $U_i(E_{n+1})$ のとりうる最小の値とは. だいたい.

$p^{n-e} \| i \Rightarrow (U_i(E_{n+1})$ のとりうる最小の値$) = e$

for $0 \leq e \leq n$ となっている。

Th. 6

for each k . $(1 \leq k \leq \frac{p-3}{2})$;

if $\exists n_k \in \mathbb{Z}$

s.t. (i) $n_k \geq U_k(C_1) = v_p(L_p(1, \omega^{2k}))$

$$\left.\begin{array}{l}\text{(ii)} \quad i \equiv k \pmod{\frac{p-1}{2}} \\ U_i(C_{n_k}) : \text{not normal}\end{array}\right\} \text{なる } i \text{ について.}$$

$U_i(E_{n_k}) \geq U_k(C_1)$

$\Rightarrow \; n = 0$

これは. $n = 0$ となるための. $U_i(E_{n+1})$ についての十分条件であるが. 次の特別な場合については. 必要十分条件が得られる。

Cor.

for each k $(1 \leq k \leq \frac{p-3}{2})$;

if $U_k(C_1) = v_p(L_p(1, \omega^{2k})) \leq 1$

$\Rightarrow \left[\, n = 0 \iff U_{kp^n}(E_{n+1}) \geq U_k(C_1) \text{ for some } n \geq 0 \,\right]$

Remarks (Th. 6 について)

① if $v_p(L_p(1, \omega^{2k})) = 0$

$\Rightarrow \forall i$ s.t. $i \equiv k \pmod{\frac{p-1}{2}}$ について.

$u_i(C_{n+1})$: normal for $\forall n \geq 0$

が言える。従って、このような k については無条件。

② $v_p(L_p(1, \omega^{2k})) > 0$ なる k について.

for $\forall n \geq 0$; $u_i(C_{n+1})$: not normal なる

i ($i \equiv k \pmod{\frac{p-1}{2}}$) は必ずある。また.

$p^{n-e} \| i$ $(0 \leq e \leq n)$ ⇒ だいたい $u_i(E_{n+1}) \geq e$

なので. Th.6 の条件(ii) は.

$$\left.\begin{array}{l} i \equiv k \pmod{\frac{p-1}{2}}, \\ p^{n-u_k(C_1)} \mid i \\ u_i(C_{n+1}) : \text{not normal} \end{array}\right\}$$ なる i についての条件と

なる。

<u>Remark</u> (Cor について)

(2)の $u_i(E_n)$ と $u_{ip}(E_{n+1})$ の関係より.

$$\begin{array}{l} u_k(C_1) \\ \ \ \ \rotatebox{90}{$\leq$} \\ u_k(E_1) \leq u_{kp}(E_2) \leq \cdots \leq u_{kp^n}(E_{n+1}) \leq \cdots \end{array}$$

が成り立つ。

$\lambda = 0 \iff u_{kp^n}(E_{n+1}) \geq u_k(C_1)$ for some $n \geq 0$

であるが.

$(1 \leq k \leq \frac{p-3}{2})$

Vandiver conj が成立 ⇔ $u_k(C_1) = u_k(E_1)$ for each k

なので "Vandiver conj ⇒ $\lambda = 0$" も直ちにわかる。

« References »

1. J. Coates : p-adic L-functions and Iwasawa's theory, in "Algebraic Number Fields" (A. Fröhlich, Ed.) pp. 269-353, Durham Symposium, 1975, Academic Press, New York / London, 1977.

2. P. Dénes, : Über irreguläre Kreiskörper, Publ. Math. Debrecen 3 (1953), 17-23.

3. P. Dénes : Über Grundeinheitssysteme der irregulären Kreiskörper von besonderen Kongruenzeigenschaften, Publ. Math. Debrecen 3. (1954), 195-204.

4. P. Dénes : Über den zweiten Faktor der Klazzenzahl und den Irreguläritatsgrad der irregulären Kreiskörper, Publ. Math. Debrecen 4. (1956), 163-170.

5. R. Gold : Rational Coates-Wiles series, Illinois J. Math. 28 (1984), 379-382

6. R. Greenberg : On the Iwasawa invariants of totally real number fields, Amer. J. Math. 98 (1976), 263-284.

7. H. Hasse : "Über die Klassenzahl abelscher Zahlkörper", Akademie-Verlag, Berlin, 1952.

8. K. Iwasawa : Lecture on p-adic L-functions, in "Annals of Math. Studies" Vol. 74, Princeton Univ. Press, Princeton, NJ, 1972.

9. W. Sinnott : On the Stickelberger ideal and the circular units of an abelian field, Invent. Math. 62 (1980), 181-234.

10. L. Washington : Units of irregular cyclotomic fields, Illinois.J. Math. 23 (1979), 635-647.

11. L. Washington : "Introduction to Cyclotomic Fields", Springer-Verlag, New York, 1982.