数理解析研究所講究録
第 572 巻 1985 年 180-200


# $\mathbb{Z}_p$ 拡大について

東大教養 藤崎 源二郎 (Genjiro Fujisaki)
東大 理 舘山 光一 (Koichi Tateyama)
都立大理 堀江 邦明 (Kuniaki Horie)

I．$p$を素数とする．有限次代数体$k$の拡大$K/k$に対し

1) $K/k$はGalois拡大であり，

2) Galois群 $Gal(K/k) \cong \mathbb{Z}_p$（$p$進整数環$\mathbb{Z}_p$の加法群と位相群として同型）

であるとき，$K/k$を$k$の$\mathbb{Z}_p$拡大であるという．$K/k$が$\mathbb{Z}_p$拡大であることと次のような中間体の列が（一意的に）存在することとは同値である：

$$k = k_0 \subset k_1 \subset \cdots \subset k_n \subset \cdots \subset K = \bigcup_{n \geq 0} k_n,$$

$$[k_n : k] = p^n, \quad k_n/k：\text{巡回拡大}.$$

$\mathbb{Z}_p$拡大$K/k$の中間体$k_n$のideal class群の$p$-Sylow群を$A_n$，$A_n$の位数を$p^{e_n}$とするとき次の定理が成り立つ．

定理（岩澤）　整数 $\lambda=\lambda(K/k,p)\geq 0$，$\mu=\mu(K/k,p)\geq 0$，$\nu$ が存在して，十分大きいすべての $n$ に対して

$$e_n=\lambda n+\mu p^n+\nu$$

が成り立つ．

以下，$p>2$ とする．$\mathbb{Z}_p$ 拡大 $K/k$ の中間体 $k_n$ がすべてCM体であるとすれば，

$$A_n=A_n^+\oplus A_n^-\quad,\quad A_n^\pm=\{a\in A_n\,|\,\bar{a}=a^{\pm1}\}$$

と分解され，$|A_n^\pm|=p^{e_n^\pm}$ とおけば，

$$e_n^\pm=\lambda^\pm n+\mu^\pm p^n+\nu^\pm\qquad(n\gg 0),$$

$$\lambda=\lambda^++\lambda^-,\ \mu=\mu^++\mu^-,\ \nu=\nu^++\nu^-$$

となる整数 $\lambda^\pm\geq 0$，$\mu^\pm\geq 0$，$\nu^\pm$ が存在する．

$k$ を1の原始 $p$ 乗根 $\zeta_p$ を含むCM体，$K/k$ を円分 $\mathbb{Z}_p$ 拡大とする．このとき，$k_n$ はすべてCM体である．$k$ および $k$ の最大実部分体 $k^+$ の類数をそれぞれ $h$，$h^+$ として $h^-=h/h^+$ とおく．

次の二つの定理が証明される．

定理1．$k$ をCM体 $\ni\zeta_p$，$K/k$ を円分 $\mathbb{Z}_p$ 拡大とするとき，次の二条件は同値である．

(1) $\lambda^- = \mu^- = 0$.

(2) 2a) $p \nmid h^-$ であり，かつ

2b) $p$ を割る $k^+$ の素 ideal はどれも $k$ において分解しない．

<u>定理2</u>． $k$ を CM 体 $\ni \zeta_p$，$K/k$ を円分 $\mathbb{Z}_p$ 拡大とする．このとき，$k_1/k$ が不分岐拡大でないならば次の二条件は同値である．

(1) $\lambda = \mu = 0$.

(2) 2a) $p \nmid h$ であり，かつ

2b) $p$ を割る $k^+$ の素 ideal はどれも $k$ において分解しない．

<u>定理2の系</u>． $k$ を CM 体 $\ni \zeta_p$，$K/k$ を円分 $\mathbb{Z}_p$ 拡大として，次のことを仮定する：$K/k$ に対して分岐する $k$ の素点は唯一つ存在してしかもそれは完全分岐である．このとき，

$$\lambda = \mu = 0 \iff p \nmid h \iff p \nmid h_n \quad (\forall n \geq 0).$$

($h_n$ は $k_n$ の類数)．

（藤崎源二郎）

# II. 2次体の λ-不変量

（館山光一）

## §1. Introduction

$p$ を素数とし $q = p$ $(p \neq 2)$ $= 4$ $(p = 2)$ とする。また $m$ を自然数とするとき. $\mu_m = \{\zeta \in \bar{\mathbb{Q}} : \zeta^m = 1\}$ とする。

$\mathbb{Q}(\mu_{p^\infty}) = \bigcup_{n=1}^{\infty} \mathbb{Q}(\mu_{p^n})$ とおくと. 位相群として.

$\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \simeq \mathbb{Z}_p^\times$ 。また. $\mu = \mu_{p-1}$ $(p \neq 2)$ $\mu = \mu_4$ $(p = 2)$ とおくと. $\mathbb{Z}_p^\times = \mu \times (1 + q\mathbb{Z}_p)$ より $^\exists B_\infty \subset \mathbb{Q}(\mu_{p^\infty})$ s.t. $\mathrm{Gal}(B_\infty/\mathbb{Q}) \simeq 1 + q\mathbb{Z}_p \simeq \mathbb{Z}_p$ かつ $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/B_\infty) \simeq \mu$ 。

$k$ を有限次代数体. $k_\infty = kB_\infty$, とし その部分体を

$$k = k_0 \subset k_1 \subset k_2 \subset \cdots \subset k_n \subset \cdots \subset k_\infty = \bigcup k_n$$

$[k_{n+1} : k_n] = p$ とすると. $k_n$ の類数 $h_n$ に関して. 次の定理が知られている。

**Th. A** (Iwasawa. [I$_1$])

$p^{e_n} \| h_n$ とすると, $^\exists \lambda(k_\infty) \in \mathbb{N} \cup \{0\}$, $^\exists \mu(k_\infty) \in \mathbb{N} \cup \{0\}$, $^\exists \nu(k_\infty/k) \in \mathbb{Z}$ s.t.

$$e_n = \lambda(k_\infty) n + \mu(k_\infty) p^n + \nu(k_\infty/k) \qquad (n \gg 0) \quad //$$

R. Greenberg は $k$ が totally real のとき. この $\lambda$. $\mu$-invariant に関して. 次の予想を提出した ([R]).

Conj. (Greenberg). $k$ が totally real ならば $\lambda(k_\infty) = \mu(k_\infty) = 0$

この予想に関しては、ほとんど何もわかっていないと言っていい状態で、実例の計算がいくつか知られているだけである。$k$ が $\mathbb{Q}$ 上アーベルのときは、Ferrero - Washington の定理より $\mu = 0$ である。よって、$\lambda$- invariant が問題となる。ここでは、$k$ を実2次体とし、奇素数の場合に証明された小松-福田([K-F1])の Th 1. が $p = 2$ の場合も成立することを示し、$p$ が奇素数の場合は reflexion th. を利用し、特に、$p = 3$ のときは虚2次体の $\lambda$- invariant の計算を利用して Greenberg の予想の成立する例を示す。

§2. $p$ = odd

$k$ を実2次体、$K = k(\mu_p)$ $K_\infty = k(\mu_{p^\infty})$.

$K = K_0 \subset K_1 \subset \cdots \subset K_n \subset \cdots \subset K_\infty = \bigcup K_n$

$[K_{n+1} : K_n] = p$ とする。

$A_n$ を $K_n$ の ideal class group の $p$-Sylow 群とすると、自然に $Gal(K_\infty/B_\infty) = Gal(K/\mathbb{Q})$ - module となる。

$\Delta = Gal(K_\infty/B_\infty)$ とおくと、$\Delta$ の exponent が $p-1$ の約数であることより

$$A_n = \bigoplus_{\chi \in \hat{\Delta}} A_n(\chi)$$

$\hat{\Delta} = Hom(\Delta, \mu_{p-1})$. $A_n(\chi) = \{ a \in A_n : a^\sigma = a^{\chi(\sigma)} \quad \forall \sigma \in \Delta \}$

このとき Th. A と同様に、次が成立する。

$$|A_n(\chi)| = p^{e_n(\chi)} \qquad e_n(\chi) = \lambda(\chi)n + \nu(\chi) \qquad n \gg 0.$$

$\chi_0$ を $\Delta$ の trivial character、$\psi$ を $K^{\mathrm{Ker}(\psi)} = k$ なる character とすると、$\lambda(\chi_0) = \lambda(B_\infty) = 0$、$\lambda(\psi) = \lambda(k_\infty)$

ここで $\omega$ を Teichmüller character i.e. $\zeta^\sigma = \zeta^{\omega(\sigma)}$ $^\forall\zeta \in \mu_p$, $\sigma \in \Delta$.

$j$ を complex conjugation とすると、

Th. B (Iwasawa). $\chi \in \hat{\Delta}$, $\chi(j) = 1$ とすると、

$$\lambda(\chi) \leqq \lambda(\chi^{-1}\omega) \quad /\!/$$

$D_n$ を $p$ 上の prime の class で生成される $A_n$ の subgroup とする。$A_n$ と同様に、

$$D_n = \bigoplus_{\chi \in \hat{\Delta}} D_n(\chi) \qquad D_n(\chi) = D_n \cap A_n(\chi).$$

Th. 1. $\chi \in \hat{\Delta}$, $\chi(j) = 1$. $\lambda(\chi^{-1}\omega) \leqq 1$. かつ $D_0(\chi) = A_0(\chi)$

$$\Longrightarrow \lambda(\chi) = 0$$

Lemma 1. $\chi \in \hat{\Delta}$. $\chi(j) = 1$. $\lambda(\chi^{-1}\omega) \leqq 1$ ならば、$A_n(\chi)$ は cyclic group である。

Proof) $A_n^- = \bigoplus_{\chi(j)=-1} A_n(\chi) \qquad A_\infty^- = \varinjlim A_n^-$

M を $K_\infty$ 上 $p$ の外で不分岐な max. CM. ab. $p$-extension とする。このとき、

$$\mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Gal}(M/K_\infty),\ \mu_{p^\infty}) \simeq A_\infty^- \qquad ([I_3])$$

$\Delta$ の自然な action より

$$\mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Gal}(M/K_\infty)(\chi),\ \mu_{p^\infty}) \simeq \varinjlim A_n(\chi^{-1}\omega)$$

L を M の $K_\infty$ 上不分岐な最大の部分体とすると、

$$\mathrm{Gal}(M/K_\infty) \twoheadrightarrow \mathrm{Gal}(L/K_\infty) \simeq \varprojlim_{\text{norm}} A_n^+ \ , \qquad A_n^+ = \bigoplus_{\chi(-1)=1} A_n(\chi)$$

$\lambda(\chi^{-1}\omega) = 0$ とすると、Th. B より、$\lambda(\chi) = 0$ である。

$\lambda(\chi^{-1}\omega) = 1$ とすると、$A_\infty(\chi^{-1}\omega) \simeq \mathbb{Q}_p/\mathbb{Z}_p$ (abel 群として)。

$\therefore\ \mathrm{Gal}(M/K_\infty)(\chi) \simeq \mathbb{Z}_p$ (top. gp として)

故に、$\mathrm{Gal}(M/K_\infty)(\chi) \twoheadrightarrow \mathrm{Gal}(L/K_\infty)(\chi) \twoheadrightarrow A_n(\chi)$

より、$A_n(\chi)$ は cyclic group である。//

Lemma. 2. G を order $p$ の cyclic group. $\sigma$ を generator とする。

$$\Rightarrow (1-\sigma)^{p-1} - (1+\sigma+\cdots+\sigma^{p-1}) = pu, \qquad u \in \mathbb{Z}_p[G]^\times$$

Proof)
$$X^{p-1} - \frac{(X+1)^p - 1}{X} = -\sum_{i=1}^{p-1}\binom{p}{i}X^{i-1}$$
$$= -X\sum_{i=2}^{p-1}\binom{p}{i}X^{i-2} - p$$

$\binom{p}{i} \equiv 0 \ (p) \quad i \neq 0, p$ より

$$X^{p-1} - \{1 + (1+X) + \cdots + (1+X)^{p-1}\} = p(1 + Xg(X)) \qquad g(X) \in \mathbb{Z}[X].$$

故に、$X = \sigma - 1$ とすると、$\sigma - 1 \in$ max. ideal of $\mathbb{Z}_p[G]$.

$\mathbb{Z}_p[G]$ は local ring より. $1+(\sigma-1)g(\sigma-1)$ は $\mathbb{Z}_p[G]$ の unit である。//

Proof of Th.1) まず Induction で $A_n(x) = D_n(x)$ を示す。

$A_{n-1}(x) = D_{n-1}(x)$ を仮定し. $G = Gal(K_n/K_{n-1}) = \langle\sigma\rangle$

とする。 $A_n(x)^{1-\sigma} \neq 1$ とすると. $\exists a \in A_n(x)$. s.t.

$1 \neq a^{1-\sigma} \in A_n(x)^{1-\sigma} \cap A_n(x)^G$. $\therefore$ $a^{(1-\sigma)^2} = 1$.

故に $a^{(1-\sigma)^{p-1}} = 1$. よって. Lemma 2. より.

$a^{(1-\sigma)^{p-1}} \cdot a^{1+\sigma+\cdots+\sigma^{p-1}} = a^{pu}$ $u \in \mathbb{Z}_p[G]^\times$

$\therefore$ $a^{pu} = a^{1+\sigma+\cdots+\sigma^{p-1}}$.

$N_{K_n/K_{n-1}}(a) \in A_{n-1}(x) = D_{n-1}(x)$ より $\exists d \in D_n(x)$ s.t.

$N_{K_n/K_{n-1}}(ad^{-1}) = 1$. $b = ad^{-1}$ とすると.

$b^{1-\sigma} = a^{1-\sigma}$. $\therefore$ $b^{(1-\sigma)^2} = 1$. $b^{1-\sigma} \neq 1$.

$\Longrightarrow$ $b^{(1-\sigma)^{p-1}} = 1$ $\therefore$ $b^{pu} = b^{1+\sigma+\cdots+\sigma^{p-1}} = 1$.

$c = b^u$ とすると. $c^{1-\sigma} \neq 1$. $c^p = 1$.

$D_n(x) \neq 1$ とすると. $c \notin D_n(x)$ より. $A_n(x)$ が cyclic に反する。 $D_n(x) = 1$ とすると. $A_n(x)$ が cyclic より. $c$ の生成する cyclic が $A_n(x)$ の unique な order $p$ の subgroup である。しかし これは $c^{1-\sigma} \neq 1$ に反する。

$\therefore$ $A_n(x)^{\sigma-1} = 1$ i.e. $A_n(x) = A_n(x)^G$.

$i_m : A_{m-1} \longrightarrow A_m$ を canonical な map とする。

$s(G) = \sum_{\sigma \in G} \sigma$ は $A_m(\chi)^G$, $D_m(\chi)$ に $p$ 乗写像として作用する。また

$$A_m(\chi)^{s(G)} = i_m(D_{m-1}(\chi))$$
$$D_m(\chi)^{s(G)} = i_m(D_{m-1}(\chi)) .$$

$A_m(\chi)^G$, $D_m(\chi)$ は共に cyclic で、$p$ 乗の order が同じである。 $\therefore\ D_m(\chi) = A_m(\chi) = A_m^G(\chi)$。

$\chi(j) = 1$ のとき $|D_m(\chi)|$ = bounded は well-known である。

([G]). //

§3. $\lambda(\chi^{-1}\omega)$ $(p \neq 2)$

以下 $\chi = \psi$ : $k$ を定義する character ($K^{\mathrm{Ker}\chi} = k$)

$\chi$, $\omega$ 共に自然に Dirichlet character と同一視することができる。 $L_p(s, \chi)$ を $p$-adic Dirichlet $L$-function とする。

このとき $\exists\, G(T) \in \mathbb{Z}_p[[T]]$ s.t. $L_p(s, \chi) = G((1+p)^s - 1)$ ([$I_3$])

Weierstrass' preparation より $\exists\, u(T) \in \mathbb{Z}_p[[T]]^\times$, $\exists\, f(T) \in \mathbb{Z}_p[T]$

s.t. $G(T) = u(T) f(T)$ $\quad f(T) \equiv T^{\deg(f)} \mod p$.

Mazur-Wiles ([M-W]) の定理より $\deg f = \lambda(\chi^{-1}\omega)$

従って $G(T) = \sum_{n=0}^{\infty} a_n T^n$ とすると

$$\lambda(\chi^{-1}\omega) \leqq 1 \iff a_1 \not\equiv 0 \ (p)$$

ここで $L_p(1, \chi) - L_p(0, \chi) = G(p) - G(0)$

$$= a_1 p + a_2 p^2 + \cdots$$

$\therefore \quad a_1 \not\equiv 0 \mod p \iff L_p(1,\chi) - L_p(0,\chi) \not\equiv 0 \mod p^2$.

ここで. $L_p(s,\chi)$ の special value を用いると.

$$L_p(0,\chi) = -(1-\chi\omega^{-1}(p))B_{1,\chi\omega^{-1}}$$

$$L_p(1,\chi) = -\left(1-\frac{\chi(p)}{p}\right)\frac{\tau(\chi,\zeta)}{f}\sum_{a=1}^{f}\chi(a)\log_p(1-\zeta^{-a})$$

ここで. $B_{1,\chi\omega^{-1}}$ は. generalized Bernoulli number

$f$ は. $\chi$ の conductor, $\tau(\chi,\zeta)$ は. Gauss の和.

$\zeta$ : primitive $f$-th root of 1. $\log_p$ : Iwasawa logarithm

また. $L(s,\chi)$ を. complex の $L$-function とすると.

$$L(1,\chi) = \frac{2h\log\varepsilon}{\sqrt{d}}$$

$\varepsilon > 1$ : fundamental unit

$$= -\frac{\tau(\chi,\zeta)}{f}\sum\chi(a)\log(1-\zeta^{-a})$$

$h$ : class number of $k$.

$d$ : discriminant of $k$.

$f = d$, $\tau(\chi) = \sqrt{d}$ に注意すると $\quad (\zeta = e^{\frac{2\pi i}{f}})$

$$2h\log\varepsilon = -\sum\chi(a)\log(1-\zeta^{-a})$$

$\chi(a) = \pm 1, 0$ より $\quad \varepsilon^{2h} = \dfrac{1}{\prod(1-\zeta^{-a})^{\chi(a)}}$

ここで $\mathbb{Q}(\zeta) \hookrightarrow \mathbb{Q}_p(\zeta)$ の embedding を $\rho$ とすると.

$$2h\log_p\rho(\varepsilon) = -\sum\chi(a)\log_p\rho(1-\zeta^{-a})$$

$$\therefore \quad L_p(1,\chi) = \left(1-\frac{\chi(p)}{p}\right)\rho(\sqrt{d})\cdot 2h\log_p\rho(\varepsilon)$$

Th. 2. $\quad \lambda(\chi^{-1}\omega) \leqq 1$ if and only if

$$-(1-\chi\omega^{-1}(p))B_{1,\chi\omega^{-1}} \not\equiv 2h\left(1-\frac{\chi(p)}{p}\right)\rho(\sqrt{d})\log_p\rho(\varepsilon) \mod p^2$$

Cor. $p = 3$ のとき $\lambda(\chi^{-1}\omega) \leqq 1$

$$\Longleftrightarrow \frac{(1-\chi\omega^{-1}(p))h^-}{w} \not\equiv (1-\frac{\chi(p)}{p})\, h\, p(\sqrt{d})\log_p \rho(\varepsilon) \mod p^2.$$

$h^-$ : $\mathbb{Q}(\sqrt{-d})$ の class number
$w$ : $\mathbb{Q}(\sqrt{-d})$ の 1 の巾根の数 //

Rem) 小松-福田の Th. 2 の仮定 (1). (2). (3) から. 上の定理を用いることにより, $\lambda(\chi^{-1}\omega) \leqq 1$ を導くことができる。

§4. $p = 2$.

この § では小松-福田の Th. 1 が. $p = 2$ で成立することを示す。以下 $p$ は素数で $k$ で分解するものとする。

更に. $G = Gal(k_n/k) = \langle\sigma\rangle$ . $\mathcal{E}_k$ : $k$ の $p$-unit group

$r = r_p(k) = \mathrm{Min}\{\mathrm{ord}_{\mathfrak{p}} \log_{\mathfrak{p}} \alpha : \alpha \in \mathcal{E}_k\}$. $(p) = \mathfrak{p}\mathfrak{p}'$ $(\mathfrak{p} \neq \mathfrak{p}')$

$\log_{\mathfrak{p}}$ : $k^\times \hookrightarrow k_{\mathfrak{p}}^\times \simeq \mathbb{Q}_p$ 上の Iwasawa logarithm とする。

Th. 3 $D_0 = A_0$, $p^r = q$ $\Longrightarrow$ $\lambda(k_\infty) = 0$

$$\nu(k_\infty/k) = \mathrm{ord}_p\left(\frac{|A_0|}{q}\log_{\mathfrak{p}} \varepsilon\right)$$

Lemma. ${}_N A_n = \{a \in A_n : N_{k_n/k}(a) \in D_0\} \supsetneq D_n$

$$n \gg 0 \Longrightarrow [{}_N A_n : A_n^{1-\sigma} D_n] = \frac{p^r}{q}$$

Proof) $B_n = A_n/D_n$ $\quad {}_NB_n = \mathrm{Ker}\{N_{k_n/k} : B_n \longrightarrow B_0\}$ とおく.

$k_n/k$ is totally ramified より $[{}_NA_n : A_n^{1-\sigma}D_n] = [{}_NB_n : B_n^{1-\sigma}]$

また. 次の 2つの exact sequence より

$$0 \longrightarrow B_n^G \longrightarrow B_n \xrightarrow{1-\sigma} B_n^{1-\sigma} \longrightarrow 0$$

$$0 \longrightarrow {}_NB_n/B_n^{1-\sigma} \longrightarrow B_n/B_n^{1-\sigma} \longrightarrow B_0 \longrightarrow 0$$

$[{}_NB_n : B_n^{1-\sigma}] = \dfrac{|B_n^G|}{|B_0|}$ 。この order は. よく知られている (cf.[?])

$$\frac{|B_n^G|}{|B_0|} = \frac{[k_n : k]}{(\mathcal{E}_k : \mathcal{E}_k \cap N_{k_n/k}k_n^\times)}$$

Hasse の norm theorem より

$$0 \longrightarrow \mathcal{E}_k \cap Nk_n^\times \longrightarrow \mathcal{E}_k \longrightarrow k_{\mathfrak{z}}^\times/Nk_{\mathfrak{z}_n}^\times \times k_{\mathfrak{z}'}^\times/k_{\mathfrak{z}_n'}^\times \quad \text{(exact)}$$

ここで. $\mathfrak{z}_n$. $\mathfrak{z}_n'$ は. $k_n$ の $\mathfrak{z}$. $\mathfrak{z}'$ 上の prime で. $k_{\mathfrak{z}_n}$. $k_{\mathfrak{z}_n'}$ は. それぞれの completion である。 $U_{\mathfrak{z}}$. $U_{\mathfrak{z}_n}$ を local unit gp とすると

$$k_{\mathfrak{z}}^\times/Nk_{\mathfrak{z}_n}^\times \simeq U_{\mathfrak{z}}/NU_{\mathfrak{z}_n} \simeq \frac{1+\mathfrak{z}\mathbb{Z}_p}{1+\mathfrak{z}p^n\mathbb{Z}} \qquad (\mathfrak{z}' \text{ も同様})$$

また. $N_{k/\mathbb{Q}}(u) = \pm p^r$. $u \in \mathcal{E}_k$: $r \in \mathbb{Z}$ より. $\mathcal{E}_k$ の image は. cyclic group である。 $k_{\mathfrak{z}}^\times$ における. Iwasawa log. を $\log_{\mathfrak{z}}$ とすると. $k_{\mathfrak{z}}^\times \xrightarrow{\log_{\mathfrak{z}}} \mathfrak{z}\mathbb{Z}_p$ induces

$$k_{\mathfrak{z}}^\times/Nk_{\mathfrak{z}_n}^\times \xrightarrow{\sim} \frac{1+\mathfrak{z}\mathbb{Z}_p}{1+\mathfrak{z}p^n\mathbb{Z}_p} \xrightarrow{\sim} \frac{\mathfrak{z}\mathbb{Z}_p}{\mathfrak{z}p^n\mathbb{Z}_p}$$

$\therefore$ $\mathcal{E}_k$ の image の order が $p^{r_0}$

$\iff$ $\mathrm{Min}\{\mathrm{ord}_p \log_\mathfrak{g} \alpha : \alpha \in \mathcal{E}_k\} = \mathrm{ord}_p\, \mathfrak{g} p^{n-r_0}$ $(n \gg 0)$

i.e. $p^r = \mathfrak{g} p^{n-r_0}$

$\therefore$ $\dfrac{|B_n^G|}{|B_0|} = \dfrac{p^n}{p^{r_0}} = p^{n-r_0} = \dfrac{p^r}{\mathfrak{g}}$ //

Proof of Th.3) Lemma より. $p^r = \mathfrak{g}$ ならば. $n \gg 0$ のとき

${}_N A_n = A_n^{1-\sigma} D_n$. $A_0 = D_0$ より. ${}_N A_n = A_n$.

$\therefore$ $A_n = A_n^{1-\sigma} D_n = (A_n^{1-\sigma} D_n)^{1-\sigma} D_n = A_n^{(1-\sigma)^2} D_n = \cdots = A_n^{(1-\sigma)^{p^N}} D_n$

$N \gg 0$ とすると. $A_n = D_n. = A_n^G$

Lemma の証明と同様に. $|A_n^G| = \dfrac{p^{m_0}}{\mathfrak{g}} |A_0|$ $m_0 = \mathrm{ord}_p \log_\mathfrak{g} \varepsilon$ //

Rem). $p$ が $k$ で分解しない場合. $D_0 = A_0 \Rightarrow \lambda(k_\infty) = 0$ は. 容易に示すことができる。

計算例) 1] $p = 2$, $k = \mathbb{Q}(\sqrt{m})$ $m \in \mathbb{N}$.

$1 < m < 100$, $m \neq 51, 65, 85$ $\Rightarrow \lambda(k_\infty) = 0$

( $m = 51, 65, 85$ のとき. $A_0 \neq D_0$ )

2] $p = 3$. $\lambda = \lambda(\mathbb{Q}_\infty(\sqrt{m}))$. $\lambda^- = \lambda(\mathbb{Q}_\infty(\sqrt{-3m}))$ $m \in \mathbb{N}$.

( [K-F] を参照. ).

| $m$ | $\lambda^-$ | $\lambda$ | $m$ | $\lambda^-$ | $\lambda$ |
|---|---|---|---|---|---|
| 103 | $\geqq 2$ | ? | 607 | 1 | 0 |
| 106 | 1 | 0 | 679 | $\geqq 2$ | ? |
| 139 | $\geqq 2$ | ? | 727 | $\geqq 2$ | ? |
| 253 | 1 | 0 | 745 | 1 | 0 |
| 295 | 1 | 0 | 787 | 1 | 0 |
| 397 | 1 | 0 | 790 | $\geqq 2$ | ? |
| 418 | 1 | 0 | 886 | 1 | 0 |
| 454 | 1 | 0 | 994 | 1 | 0 |
| 505 | $\geqq 2$ | ? | | | |

References


[K-F]. T. Fukuda - K. Komatsu, On $\mathbb{Z}_p$-extensions of real quadratic fields. (Preprint)

[$I_1$] K. Iwasawa, On Γ-extensions of algebraic number field, Bull. Amer. Math. Soc. 65 (1959). pp. 183-226

[$I_2$] , Lectures on p-adic L-functions

[$I_3$]. On $\mathbb{Z}_\ell$-ex. of algebraic number fields. Ann of Math. 98.

[F]. B. Ferrero, The cyclotomic $\mathbb{Z}_2$-ex. of imag. quadratic fields, Amer. J. Math (1980)

[G]. R. Greenberg, The Iwasawa inv. of totally real number fields. Amer. J. Math (1976)

## III. λ⁻不変量について

(堀江邦明)

各(有限次)CM体 $k$ に対し、

$$\lambda_p^-(k_\infty/k) = \lambda_p(k_\infty/k) - \lambda_p((k^+)_\infty/k^+)$$

とおく。ここに $k^+$ は $k$ の最大総実部分体である。この値は、素数 $p$ を固定している以上、体 $k$ にしかよらぬから単に $\lambda_k^-$ と書いて、$k$ の(または $k_\infty$ の)λ⁻不変量と呼んだりする。

<u>注意</u> 一般に、$K/k$ をCM体 $k$ の $\mathbb{Z}_p$-拡大とするとき、"$K$ のλ⁻不変量が自然に定義される" 即ち $K$ がCM体となるのは、Leopoldt予想の下では $K = k_\infty$ の場合に限るのである。然も、$k$ が $\mathbb{Q}$ 上のAbel拡大のときLeopoldt予想の成立つことが証明されているのであった。

そこでGreenbergの予想なども考え合わせると、$k$ を特に虚のAbel体に限っても、そのλ⁻不変量が取る値(の分布)を調べるのは興味深いことである。以下に簡単な考察の結果をいくつか述べよう。

円分体の全体のなす族を $C$ で表わす。$C$ の任意の部分族 $S$ と、各 $x > 3$ に対し、$S(x)$ で導手が $x$ 以下の $S$ に属する円

分体の全体を表わす。このとき、もし比 $|S(x)|/|C(x)|$ が $x \to \infty$ で収束するならば、

$$d(S) = \lim_{x \to \infty} \frac{|S(x)|}{|C(x)|}$$

と定める。この値が定義される限り、$0 \leqq d(S) \leqq 1$ であり、明らかに $d(C) = 1$ となる。一方、$C$ の有限部分族 $F$ に対しては常に $d(F) = 0$ である。

いま自然数 $N$ を一つ固定し、$C'$ で $\lambda_k^- \geqq N$ を満たす円分体の全体を表わそう。

<u>命題 1.</u> $$d(C') = 1 .$$

これは、λ-不変量に関する Riemann-Hurwitz の公式（木田の公式）、及び Landau が素数定理を拡張するときに用いた解析的計算法によって示すことが出来る（[3]）。従って、直ちに次を得る。

<u>系</u> $P$ を素数の有限集合、$C^*$ を $\lambda_q^-(k_\infty/k) \geqq N$ $(\forall q \in P)$ なる円分体の全体とするとき、

$$d(C^*) = 1 .$$

次に、$X$ を

$$\Gamma_0(p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \pmod p \right\}$$

に付随した modular 曲線、$g$ を X の種数、J を X の Jacobi 多様体とする。このとき、X 従って J の定義体として $\mathbb{Q}$ が取れる。$J_p$ で J の $p$ 等分点全体の成す有限群を表わせば

$$J_p \cong (\mathbb{Z}/p\mathbb{Z})^g .$$

$\mathbb{Q}$ に $J_p$ の点の affine 座標をすべて添加した代数体を $\mathbb{K}$ とすると、これは $\mathbb{Q}$ 上の Galois 拡大となり、有限群 $Gal(\mathbb{K}/\mathbb{Q})$ は $J_p$ に自然に作用するから、その有限体 $\mathbb{Z}/p\mathbb{Z}$ 上の表現

$$R : Gal(\mathbb{K}/\mathbb{Q}) \longrightarrow GL_{2g}(\mathbb{Z}/p\mathbb{Z})$$

を得る。

一方、$\mathfrak{S} = \mathfrak{S}_2(\Gamma_0(p))$ で $\Gamma_0(p)$ に属する 2 次の尖点形式の全体を表わせば、これは $\mathbb{C}$ 上 $g$ 次元の線型空間をなす。いま Hecke 作用素 $T_n$ $(n = 1, 2, \cdots)$ を $\mathfrak{S}$ の線型変換で各 $f = f(z) \in \mathfrak{S}$ を

$$f|T_n = n \sum_{(a,d)} \sum_{b=1}^{d} f\left(\frac{az+b}{d}\right) d^{-2} \in \mathfrak{S}$$

に写すものとして定義する。但し、上の $(a,d)$ は自然数の対で $ad = n$, $(a,p) = 1$ となるもの全部に渡るのである。従って $T_n$ は ($\mathfrak{S}$ の基底を定めたとき) $g$ 次行列を定めるが、その跡を

$$\mathrm{tr}(T_n)$$

と書こう。よく知られているように、この値は有理整数である。

さて、$p$ を割らない $\mathbb{K}$ の各素 ideal $\mathfrak{q}$ は $\mathbb{K}/\mathbb{Q}$ で不分岐であるから、$\mathfrak{q}$ の $\mathbb{K}/\mathbb{Q}$ に関する唯一の Frobenius 置換を $\sigma_{\mathfrak{q}}$ と書くことにする。このとき、$\mathfrak{q}$ で割られる素数を $q$ とすると、いわゆる modular 対応の合同関係式によって、

$$(1) \qquad \mathrm{tr}(R(\sigma_{\mathfrak{q}})) \equiv \mathrm{tr}(T_q) \mod p$$

となることが分る（以上の議論については、例えば [2] を参照されたい）。

一方、Eichler の跡公式及び Kronecker の類数関係式によれば、

$$(2) \qquad \mathrm{tr}(T_q) + q + 1 = \sum_{k} c_k h_k .$$

ここに $k$ は $\mathbb{Q}(\sqrt{a^2-4q})$ $(a \in \mathbb{Z},\ a^2 < 4q)$ なる形の虚2次体で、$p$ がそこで分解しないようなもの全体を走り、各 $h_k$ は $k$ の類数を表わし、各 $c_k$ は $12c_k$ が整数となるような $0$ 以上の有理数である。

**命題 2.** 虚2次体 $k$ で、$\lambda_k = 0$ となるものが無数に存在する。

以下、$p \geqq 5$ の場合の命題の証明を手短かに述べよう。$l$ を $\mathrm{mod}\ p$ での正の最小平方非剰余とするとき、これは

$p$と異なる素数であるが、$q=l$ に対する(2)式を特に考察して

(3) $$tr(T_l)+l+1 \not\equiv 0 \pmod{p}$$

を導くことが出来る。

次に、$r$を勝手な素数とする。このとき、Tchebotareff の密度定理から分るように、次の性質(i),(ii)を満たす素数 $q \neq p$ が存在する。

(i) $q$ の上にある $\mathbb{K}$ の素ideal $\mathfrak{q}$ を選べば

$$\sigma_{\mathfrak{q}} = \sigma_{\mathfrak{l}} .$$

但し $\mathfrak{l}$ は $l$ の上にある $\mathbb{K}$ の素idealの一つ。

(ii) $q$ は $\mathbb{Q}(\sqrt{-1})$ と $\mathbb{Q}(\sqrt{-2})$ のいずれでも素(remains prime)。また $p$ と異なる各奇素数 $v \leq r$ に対して、$q$ は $\mathbb{Q}(\sqrt{v^*})$ でも素。但し $v^*=\left(\frac{-1}{v}\right)v$。

さて、(1)と(i)から

$$tr(T_q) \equiv tr(T_l) \pmod{p}.$$

更に、$\mathbb{K}$は円の$p$分体を含むから

$$q \equiv l \pmod{p}.$$

従って、(3)により

$$tr(T_q)+q+1 \not\equiv 0 \pmod{p}$$

を得る。このとき(2)を見れば、$p \geq 5$としたから、

$t_k \not\equiv 0 \pmod{p}$, $p$は$k$で不分解

となる虚2次体$k$が存在しなければならない。よく知られているように、このような$k$は

$$\lambda_k^- = 0$$

を満たす([1])。然も、(ii)と$l$の取り方とから、$k$の導手は$r$より大きいことが分る。かくして、$p \geqq 5$に対し、命題2は証明されたことになる。

尚$p=3$のときも、Gierster, Hurwitzによる類数関係式を用いれば、上とほぼ同様の議論をして命題の証明が出来る。

$p=2$の場合は例外的で、Gaußの種の理論と[1]とから明らかである。

最後にもう一つ結果を述べるために、自然数の有限集合$T$を

$$T = \{ a + b(p-1) \mid a, b \in \mathbb{Z},\ 1 \leqq a \leqq p-2,\ 0 \leqq b \leqq a-1 \}$$

で定める。$|T| = \frac{1}{2}(p-2)(p-1)$.

命題3. $k$を虚Abel体とするとき、もし$p$が拡大次数$[k_\infty : \mathbb{Q}_\infty]$を割り切れば、$\lambda_k^-$は$T$に属する数にはなり得ない。

特に$p > 2$ならば$T \ni 1$であるから、$p \mid [k_\infty : \mathbb{Q}_\infty]$となる虚Abel体$k$に対して常に$\lambda_k^- \neq 1$なのである。逆に、

例えば $p=3$ の場合などは、1以外の非負整数 $n$ を与えたとき $\lambda_k=n$ を満たす虚の6次Abel体 $k$ は無数に存在することが分る。

謝辞 この節の内容を研究するに当たり、山本芳彦先生には特にお世話になりました。ここに改めてお礼申し上げます。

参考文献

[1] 岩澤健吉：A note on class numbers of algebraic number fields, Abh. Math. Sem. Univ. Hamburg, 20 (1956), 257-258.

[2] 志村五郎：保型関数と整数論 I, II, 数学 11 (1960), 193-205, 13 (1961), 65-80.

[3] 代数的整数論研究集会報告集, 1984年, 於 京都大学数理解析研究所, 11-22.