

$\mathbb{Z}_p$ 拡大について

東大教養 藤崎 源一郎 (Genjiro Fujisaki)

東大理 館山 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 $\text{Gal}(K/k) \cong \mathbb{Z}_p$ (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 $\lambda = \lambda(K/k, p) \geq 0$, $\mu = \mu(K/k, p) \geq 0$, v が存在して, 十分大きいすべての n に対して

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

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 体であるとするば,

$$A_n = A_n^+ \oplus A_n^-, \quad A_n^\pm = \{a \in A_n \mid \bar{a} = a^{\pm 1}\}$$

と分解され, $|A_n^\pm| = p^{e_n^\pm}$ とおけば,

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

$$\lambda = \lambda^+ + \lambda^-, \quad \mu = \mu^+ + \mu^-, \quad v = v^+ + v^-$$

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

k を 1 の原始 p 乗根 ζ_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 体とする, 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.

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

$$(2) \text{ 2a) } p \nmid h^- \text{ であり,かつ}$$

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

定理 2. k を CM 体 $\mathfrak{O}_p$, 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.

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

$$(2) \text{ 2a) } p \nmid h \text{ であり,かつ}$$

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

定理 2 の系. k を CM 体 $\mathfrak{O}_p$, 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).

(藤崎源一郎)

II. λ -invariant of λ -extension.

(館山光一)

§ 1. Introduction

p is a prime $\neq 1$ $f = p$ ($p \neq 2$) $= 4$ ($p = 2$) $\neq 3$. f is
 m is a natural number $\neq 3$ $\neq 5$. $\mu_m = \{ \zeta \in \bar{\mathbb{Q}} : \zeta^m = 1 \}$ $\neq 3$.

$$\mathbb{Q}(\mu_{p^\infty}) = \bigcup_{n=1}^{\infty} \mathbb{Q}(\mu_{p^n}) \quad \text{is a } \mathbb{Q} \text{-extension.} \quad \text{Galois group } \neq 1.$$

$$\text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \cong \mathbb{Z}_p^\times. \quad \text{is a } \mathbb{Z}_p^\times \text{-extension.} \quad \mu = \mu_{p-1} \text{ ($p \neq 2$)} \quad \mu = \mu_4 \text{ ($p = 2$)}$$

$$\text{is a } \mathbb{Z}_p^\times \text{-extension.} \quad \mathbb{Z}_p^\times = \mu \times (1 + f \mathbb{Z}_p) \quad \text{is a } \mathbb{Z}_p^\times \text{-extension.} \quad \exists B_\infty \subset \mathbb{Q}(\mu_{p^\infty}) \text{ s.t.}$$

$$\text{Gal}(B_\infty/\mathbb{Q}) \cong 1 + f \mathbb{Z}_p \cong \mathbb{Z}_p \quad \text{is a } \mathbb{Z}_p \text{-extension.} \quad \text{Gal}(\mathbb{Q}(\mu_{p^\infty})/B_\infty) = \mu.$$

K is a finite extension of $\mathbb{Q}$. $K_\infty = K B_\infty$ $\neq 1$ $\neq 9$ part of K

$$K = K_0 \subset K_1 \subset K_2 \subset \dots \subset K_n \subset \dots \subset K_\infty = \bigcup K_n$$

$$[K_{m+1} : K_m] = p \quad \text{is a } p \text{-extension.} \quad K_m \text{ of } K_\infty \text{ is a } p \text{-extension.}$$

1. The following theorem is known.

Th. A (Iwasawa, [I, 1])

$$p^n \parallel h_n \quad \text{is a } p \text{-extension.} \quad \exists \lambda(K_\infty) \in \mathbb{N} \cup \{0\}. \quad \exists \mu(K_\infty) \in \mathbb{N} \cup \{0\}$$

$$\exists \nu(K_\infty/K) \in \mathbb{Z} \quad \text{s.t.}$$

$$e_n = \lambda(K_\infty)n + \mu(K_\infty)p^n + \nu(K_\infty/K) \quad (n \gg 0) //$$

R. Greenberg is K is totally real $\neq 3$. $\neq 9$.

λ, μ -invariant is related. The following conjecture is proposed. [CRJ].

Conj. (Greenberg). K is totally real is $\neq 3$. $\lambda(K_\infty) = \mu(K_\infty) = 0$

この予想に関しては、ほとんど何もわかっていないと言、
 ている状態で、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 p -ヘルムの場合は、Ferreiro-Washington の
 定理より $\mu = 0$ である。よ、 λ -invariant の問題と
 なる。ここでは、 K が実 2 次体とし、奇素数の場合に証明さ
 した。小松-福田 (JK-FJ) の Th.1. の $p=2$ の場合も成り立つ
 ことを示し、 p が奇素数の場合は、reflection th. を利用し、
 特に $p=3$ のときは、虚 2 次体の λ -invariant の計算を利用し、
 Greenberg の予想の成り立つ例を示す。

§ 2. $p = \text{odd}$

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

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

$[K_{n+1} : K_n] = p$ とする。

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

$\Delta = \text{Gal}(K_\infty/B_\infty)$ とし、 Δ の exponent は $p-1$ の
 約数であることに注意。

$$A_n = \bigoplus_{x \in \Delta} A_n(x)$$

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

$\therefore a \in \mathfrak{z}$. Th. A と同様に、次の成立する。

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

$x_0 \in \Delta$ a trivial character. $\psi \in K^{K_n(\psi)} = k$ である。

character である。 $\lambda(x_0) = \lambda(\beta_\infty) = 0$. $\lambda(\psi) = \lambda(k_\infty)$

$\therefore \therefore \omega$ is Teichmüller character i.e. $\gamma^* = \gamma^{\omega(\gamma)}$ $\gamma \in \mu_p$

$$\sigma \in \Delta.$$

j is complex conjugation である。

Th. 8. (Iwasawa). $x \in \hat{\Delta}$. $x(j) = 1$ である。

$$\lambda(x) \leq \lambda(x^{-1}\omega) \quad //$$

D_n is $p \nmid n$ prime a class である。生成する。 A_n is subgroup である。 A_n と同様に。

$$D_n = \bigoplus_{x \in \hat{\Delta}} D_n(x) \quad D_n(x) = D_n \cap A_n(x).$$

Th. 1. $x \in \hat{\Delta}$, $x(j) = 1$. $\lambda(x^{-1}\omega) \leq 1$. $\therefore D_0(x) = A_0(x)$

$$\implies \lambda(x) = 0$$

Lemma 1. $x \in \hat{\Delta}$. $x(j) = 1$. $\lambda(x^{-1}\omega) \leq 1$ である。 $A_n(x)$

is cyclic group である。

$$\text{Proof. } A_n = \bigoplus_{x(j)=-1} A_n(x) \quad A_\infty = \varprojlim A_n$$

$M \in K_\infty$ 上 p 外 τ_2 不分歧 τ_2 max. CM. ab. p -extension
 $\tau_2 \nmid 3$. $\tau_2 \nmid 3$.

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

Δ の自然 τ_2 action 2)

$$\text{Hom}_{\mathbb{Z}_p}(\text{Gal}(M/K_\infty)(x), \mu_{p^\infty}) \cong \varprojlim A_n(x^{-1}\omega)$$

$L \in M$ の K_∞ 上 不分歧 τ_2 最大の部分体 $\tau_2 \nmid 3$ である。

$$\text{Gal}(M/K_\infty) \longrightarrow \text{Gal}(L/K_\infty) \cong \varprojlim_{n \geq 1} A_n^+ \quad A_n^+ = \bigoplus_{x \neq 1} A_n(x)$$

$$\lambda(x^{-1}\omega) = 0 \quad \tau_2 \nmid 3 \quad \text{Th. B より} \quad \lambda(x) = 0 \quad \tau_2 \nmid 3$$

$$\lambda(x^{-1}\omega) = 1 \quad \tau_2 \nmid 3 \quad A_\infty(x^{-1}\omega) \cong \mathbb{Z}_p \quad (\text{abel 群 } \tau_2 \nmid 3)$$

$$\therefore \text{Gal}(M/K_\infty)(x) \cong \mathbb{Z}_p \quad (\text{top. gp } \tau_2 \nmid 3)$$

$$\text{故に} \quad \text{Gal}(M/K_\infty)(x) \longrightarrow \text{Gal}(L/K_\infty)(x) \longrightarrow A_n(x)$$

$$\text{より} \quad A_n(x) \text{ は cyclic group } \tau_2 \nmid 3 \quad "$$

Lemma. 2. G は order p の cyclic group. σ は generator $\tau_2 \nmid 3$.

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

$$\begin{aligned} \text{Proof) } X^{p-1} - \frac{(X+1)^p - 1}{X} &= - \sum_{i=1}^{p-1} \binom{p}{i} X^{i-1} \\ &= -X \sum_{i=2}^{p-1} \binom{p}{i} X^{i-2} - p \end{aligned}$$

$$\binom{p}{i} \equiv 0 \pmod{p} \quad i \neq 0, p \quad \text{2)}$$

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

$$\text{故に} \quad X = \sigma - 1 \quad \tau_2 \nmid 3 \quad \sigma - 1 \in \text{max. ideal of } \mathbb{Z}_p[G]$$

$\mathbb{Z}_p[G]$ is local ring 2). $1 + (p-1) \neq 0$ 2). $\mathbb{Z}_p[G]$ is unit
 1. 2. 3. //

Proof of Th. 1) 3. Induction 1. $A_m(x) = D_m(x)$ 2. 3.

$$A_{m-1}(x) = D_{m-1}(x) \quad \text{is fixed 1.} \quad G = \text{Gal}(K_n/K_{n-1}) = \langle \sigma \rangle$$

$$1 \neq a^{1-\sigma} \in A_m(x)^{1-\sigma} \neq 1 \quad \text{2. 3. 2.} \quad \exists a \in A_m(x) \quad \text{s.t.}$$

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

$$\text{6. 2. 1.} \quad a^{(1-\sigma)^{p-1}} = 1. \quad \text{5. 2. Lemma 2. 2. 1.}$$

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

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

$$N_{K_n/K_{n-1}}(a) \in A_{m-1}(x) = D_{m-1}(x) \quad \text{2. 1.} \quad \exists d \in D_m(x) \quad \text{s.t.}$$

$$N_{K_n/K_{n-1}}(ad^{-1}) = 1. \quad b = ad^{-1} \quad \text{2. 3. 2.}$$

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

$$\Rightarrow b^{(1-\sigma)^{p-1}} = 1. \quad \therefore b^{pu} = b^{1+\sigma+\dots+\sigma^{p-1}} = 1.$$

$$c = b^u \quad \text{2. 3. 2.} \quad c^{1-\sigma} \neq 1. \quad c^p = 1.$$

$$D_m(x) \neq 1 \quad \text{2. 3. 2.} \quad c \notin D_m(x) \quad \text{2. 1.} \quad A_m(x) \text{ is}$$

$$\text{cyclic 1. 2. 3.} \quad D_m(x) = 1 \quad \text{2. 3. 2.} \quad A_m(x) \text{ is cyclic}$$

$$\text{2. 1.} \quad c \text{ is a generator 2. 3. cyclic 1. 2.} \quad A_m(x) \text{ is unique T. 2. order } p$$

$$\text{a subgroup 2. 3. 2.} \quad |x| = n. \quad c^{1-\sigma} \neq 1 \quad \text{1. 2. 3.}$$

$$\therefore A_m(x)^{\sigma-1} = 1 \quad \text{i.e.} \quad A_m(x) = A_m(K)^G.$$

$i_m : A_{m-1} \longrightarrow A_m$ is a canonical is map etc.

$S(G) = \sum_{\sigma \in G} \sigma$ is $A_m(X)^G$, $D_m(X)$ is p -adic image etc. (作用)

etc. $A_m(X)^{S(G)} = i_m(D_{m-1}(X))$

$D_m(X)^{S(G)} = i_m(D_{m-1}(X))$.

$A_m(X)^G$, $D_m(X)$ is cyclic p -adic order etc.

同 (1) etc. $D_m(X) = A_m(X) = A_m^G(X)$.

$X(j)=1$ etc. $|D_m(X)| = \text{bounded}$ is well-known etc.

([G]). //

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

以下 $X = \psi$: K is defined character ($K^{K_X} = K$)

X, ω is naturally Dirichlet character etc. (view etc.)

etc. $L_p(s, X)$ is p -adic Dirichlet L -function etc.

etc. $G(T) \in \mathbb{Z}_p[[T]]$ s.t. $L_p(s, X) = G((1+p)^s - 1)$ ([I3])

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

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

Mazur-Wiles ([M-W]) 9 theorem etc. $\deg f = \lambda(X^{-1}\omega)$

従, $G(T) = \sum_{n=0}^{\infty} a_n T^n$ etc.

$\lambda(X^{-1}\omega) \leq 1 \iff a_1 \neq 0 \pmod{p}$

etc. $L_p(1, X) - L_p(0, X) = G(p) - G(0)$

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

$$\therefore a_1 \not\equiv 0 \pmod{p} \iff L_p(1, \chi) - L_p(0, \chi) \not\equiv 0 \pmod{p^2}.$$

$\therefore \therefore L_p(s, \chi)$ is special value & 用 $\therefore \exists \epsilon$.

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

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

$\therefore \therefore B_{1, \chi\omega^{-1}}$ is generalized Bernoulli number

f is χ a conductor, $\tau(\chi, \zeta)$ is Gauss's $\neq 0$.

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

$\exists \epsilon$: $L(s, \chi)$ is complex $\circ$ L-function & $\exists \exists \epsilon$.

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

$\epsilon > 1$: fundamental unit

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

h : class number of K .

d : discriminant of K .

$$f = d, \quad \tau(\chi) = \sqrt{d} \quad \text{注意 } \exists \exists \epsilon \quad (\zeta = e^{\frac{2\pi i}{f}})$$

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

$$\chi(a) = \pm 1, 0 \quad \therefore \quad \epsilon^{2h} = \frac{1}{\prod (1 - \zeta^{-a})^{\chi(a)}}$$

$\therefore \therefore \mathbb{Q}(\zeta) \hookrightarrow \mathbb{Q}_p(\zeta)$ is embedding & $p \nmid f \exists \exists \epsilon$.

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

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

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

$$-(1 - \chi\omega^{-1}(p)) B_{1, \chi\omega^{-1}} \not\equiv 2h (1 - \frac{\chi(p)}{p}) \rho(\sqrt{d}) \log_p \rho(\epsilon) \pmod{p^2}$$

Cor. $p = 3$ のとき $\lambda(x^{\omega}) \leq 1$

$$\Leftrightarrow \frac{(1-x\omega^2\varphi)h^-}{w} \equiv (1-\frac{x\varphi}{p})h\rho(\sqrt{d})\log_p\rho(\varepsilon) \pmod{p^2}$$

h^- : $\mathbb{Q}(\sqrt{-d})$ の class number

w : $\mathbb{Q}(\sqrt{-d})$ の 1 の中根の数 //

Rem) 小松-福田の Th. 2 の仮定 (1), (2), (3) から, 上の定理を用い

て $\lambda(x^{\omega}) \leq 1$ を導くことができる。

§4. $p = 2$

この § では, 小松-福田の Th. 1 から, $p = 2$ で成り立つことを示す。以下 p は素数で, k で分解するものとする。

$\bar{k} = G = \text{Gal}(\bar{k}/k) = \langle \sigma \rangle$, $E_k : k$ の p -unit group

$$r = r_p(k) = \min \{ \text{ord}_f \log_f \alpha : \alpha \in E_k \} \quad (p) = f f' \quad (f \neq f')$$

$\log_f : k^* \hookrightarrow k_f^* \simeq \mathbb{Q}_p$ は Iwasawa logarithm とする。

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

$$\nu(k_\infty/k) = \text{ord}_p \left(\frac{|A_0|}{f} \log_f \varepsilon \right)$$

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

$$n \gg 0 \Rightarrow [{}_N A_n : A_n^{-r} D_n] = \frac{p^r}{f}$$

Proof) $B_m = A_m/D_m$ $N B_m = \text{Ker } (N_{k_m/k} : B_m \longrightarrow B_0)$ $\epsilon \text{ } m < r$.

k_m/k is totally ramified $\therefore [N A_m : A_m^{-\sigma} D_m] = [N B_m : B_m^{-\sigma}]$

また、次の exact sequence $\therefore$

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

$$0 \longrightarrow N B_m / B_m^{1-\sigma} \longrightarrow B_m / B_m^{1-\sigma} \longrightarrow B_0 \longrightarrow 0$$

$$[N B_m : B_m^{1-\sigma}] = \frac{|B_m^G|}{|B_0|} \quad \therefore \text{the order is } f < \infty \text{ since } f \text{ is finite (CFI)}$$

$$\frac{|B_m^G|}{|B_0|} = \frac{[k_m : k]}{(\epsilon_k : \epsilon_k \cap N_{k_m/k} k_m^{\times})}$$

Hasse's norm theorem $\therefore$

$$0 \longrightarrow \epsilon_k \cap N k_m^{\times} \longrightarrow \epsilon_k \longrightarrow \frac{k_j^{\times}}{N k_{j_m}^{\times}} \times \frac{k_{j'}^{\times}}{k_{j'_m}^{\times}} \quad (\text{exact})$$

$\therefore \therefore$ j, j' is k_m or j, j' is a prime $\therefore k_{j_m}, k_{j'_m}$ is

k or k is a completion $\therefore$ $\exists$ $\mathcal{O}_j, \mathcal{O}_{j_m}$ is local unit gp $\therefore$ $\exists$ $\therefore$

$$\frac{k_j^{\times}}{N k_{j_m}^{\times}} \cong \frac{\mathcal{O}_j}{N \mathcal{O}_{j_m}} \cong \frac{1 + \mathfrak{p} \mathbb{Z}_p}{1 + \mathfrak{p}^n \mathbb{Z}_p} \quad (j' \text{ is same})$$

$\exists \epsilon. N_{k/k}(u) = \pm p^r. \quad u \in \epsilon_k. \quad r \in \mathbb{Z} \text{ is } \therefore \epsilon_k \text{ is image}$

is cyclic group $\therefore$ $\exists$ $k_j^{\times} = \therefore \therefore \exists$ Iwasawa log. ϵ log $\therefore$

$\epsilon \exists \exists \epsilon. \quad k_j^{\times} \xrightarrow{\log} \mathbb{Z}_p \text{ induces}$

$$\frac{k_j^{\times}}{N k_{j_m}^{\times}} \xrightarrow{\sim} \frac{1 + \mathfrak{p} \mathbb{Z}_p}{1 + \mathfrak{p}^n \mathbb{Z}_p} \xrightarrow{\sim} \frac{\mathfrak{p} \mathbb{Z}_p}{\mathfrak{p}^n \mathbb{Z}_p}$$

$\therefore \xi_k$ の image の order は p^{r_0}

$$\Leftrightarrow \min \{ \text{ord}_p \log_g \alpha : \alpha \in \xi_k \} = \text{ord}_p g p^{n-r_0} \quad (n \gg 0)$$

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

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

Proof of Th. 3) Lemma 2). $p^r = g$ ならば $n \gg 0$ かつ

$$n A_n = A_n^{1-\sigma} D_n, \quad A_0 = D_0 \quad \text{より} \quad n A_n = A_n$$

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

$$n \gg 0 \text{ かつ } \exists \varepsilon. \quad A_n = D_n = A_n^G$$

$$\text{Lemma の証明と同様に} \quad |A_n^G| = \frac{p^{m_0}}{g} |A_0| \quad m_0 = \text{ord}_p \log_g g //$$

Rem). p は k で分解しない場合 $D_0 = A_0 \Rightarrow \lambda(k_\infty) = 0$ であることは容易に

示すことはできる。

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

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

$$(m = 51, 65, 85 \text{ のときは } A_0 \neq D_0)$$

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

([K-F] を参照)。

m	λ^-	λ	m	λ^-	λ
103	≥ 2	?	607	1	0
106	1	0	679	≥ 2	?
139	≥ 2	?	727	≥ 2	?
253	1	0	745	1	0
295	1	0	787	1	0
397	1	0	790	≥ 2	?
418	1	0	886	1	0
454	1	0	994	1	0
505	≥ 2	?			

References

- [K-F]. T. Fukuda, - K. Komatsu, On $\mathbb{Z}_p$ -extensions of real quadratic fields. (Preprint)
- [I₁] K. Iwasawa, On Γ -extensions of algebraic number field,
Bull. Amer. Math. Soc. 65 (1959). pp. 183 - 226
- [I₂] , Lectures on p -adic L -functions
- [I₃] . On $\mathbb{Z}_2$ -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 λ_k と書いて、 k の(または k_∞ の) λ -不変量と呼んだりする。

注意 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 -不変量を取る値(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 $\mathcal{C}$ で表わす。 $\mathcal{C}$ の任意の部分族 $\mathcal{S}$ と、各 $x \geq 3$ に対し、 $\mathcal{S}(x)$ で導手が x 以下の $\mathcal{S}$ 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 $x \rightarrow \infty$ で収束するならば、

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

と定める。この値が定義される限り、 $0 \leq d(S) \leq 1$ 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 $\lambda_k \geq N$ を満たす円分体の全体を表わそう。

命題 1. $d(C') = 1$.

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を用いた、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。

系 P を素数の有限集合、 C^* を $\lambda_g(k_\infty/k) \geq N$ ($\forall g \in P$) なる円分体の全体とするとき、

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

次に、 X を

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

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 K とすると、これは $\mathbb{Q}$ 上の Galois 拡大となり、有限群 $\text{Gal}(K/\mathbb{Q})$ 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

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

を得る。

一方、 $\mathcal{S} = \mathcal{S}_2(\Gamma_0(p))$ 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 ($n=1, 2, \dots$) を $\mathcal{S}$ の線型変換で各 $f = f(z) \in \mathcal{S}$ を

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

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 ($\mathcal{S}$ の基底を定めたとき) g 次行列を定めるが、その跡を

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

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 K の各素 ideal $\mathfrak{q}$ は $K/\mathbb{Q}$ で不分裂であるから、 $\mathfrak{q}$ の $K/\mathbb{Q}$ 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、

$$(1) \quad \text{tr}(R(\sigma_{\mathfrak{q}})) = \text{tr}(T_q) \pmod{p}$$

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、

$$(2) \quad \text{tr}(T_q) + q + 1 = \sum_k c_k \cdot h_k.$$

ここに h 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 h 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 h で、 $\lambda_k = 0$ となるものが無数に存在する。

以下、 $p \geq 5$ の場合の命題の証明を手短かに述べよう。

l を $\text{mod } p$ での正の最小平方非剰余とすると、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

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

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 K の素 ideal $\mathfrak{q}$ を選べば

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

但し l は l の上にある 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

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

更に、 K は $\mathbb{Q}$ の p 分体を含むから

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

従って、(3) により

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

を得る。このとき (2) を見れば、 $p \geq 5$ としたから、

$$a_k \not\equiv 0 \pmod{p}, \quad p \text{ は } k \text{ で不分解}$$

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、 $p \geq 5$ 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

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

で定める。 $|T| = \frac{1}{2}(p-2)(p-1)$ 。

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

特に $p \geq 3$ ならば $|T| \geq 1$ 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 II (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.