

非 Galois 拡大体の岩澤理論

東大教養学部 片岡 俊孝

(Toshitaka Kataoka)

0.

この小論では、岩澤理論の代数的部分¹⁾、すなわち有限次代数体上の \mathbb{Z}_p -拡大での中間体の p -class group (= イデアル類群の Sylow p -subgroup) の振舞の記述・分析で p 進 L -函数²⁾と独立な部分を、基礎体上必しも Galois ではないが中間体の様子が \mathbb{Z}_p -拡大と同一である無限次拡大に、ゆるやかな制限の下で、拡張する。

このような拡大が特に CM 体からなる場合には、CM 体の \mathbb{Z}_p -拡大と同様のことが成立する。一般の場合には記述に準備を要するので、弱い形で結果を述べる。

以上の結果は、関連する岩澤加群 (= 必しも有限次ではない代数体上の最大不分岐アーベル p -拡大の Galois 群) の分析、ある種の非可換 2 次元 p -adic Lie 群 G の \mathbb{Z}_p

1) cf. Iwasawa [2]

2) cf. Iwasawa [1]

上の群環 $\mathbb{Z}_p[[G]]$ 上有限生成加群の考察等を基礎にして
 るが、その点にはふれない。

また、CM体の場合の p 進 L -函数との結びつきは不明である。

1.

p で素数、 k で体をあらわす。まず我々の考察対象とする拡大体を定義する。

(1.1) K/k が "twisted \mathbb{Z}_p -拡大

\Leftrightarrow
 def

k 上の Galois 拡大 L で、次の ①、② をみたすものが存在する。

① KL/L は \mathbb{Z}_p -拡大。

② $L \cap K = k$ 。

(1.2) (1.1) の拡大 K/k は、次のようにあらわされる。

(a) 任意の $n \in \mathbb{Z}_{>0}$ に対し、 $[k_n : k] = p^n$ となる K/k の中間体 k_n が一意的に存在する。

(b) $k = k_0 \subset k_1 \subset k_2 \subset \dots \subset k_n \subset \dots$

$$(1.2) \quad \bigcup_n k_n = K.$$

(1.3) 以下、次のように仮定あるいは定義する。

p : odd.

k : 有限次代数体.

Twisted \mathbb{Z}_p -拡大 K/k に対し、①, ②をみたす k の Galois 拡大 L の中で "最小のものが" 存在する。 L はつねにそのようなものをあらわすとする。

$$G = \text{Gal}(KL/k).$$

$$N = \text{Gal}(KL/L).$$

$$H = \text{Gal}(K/L).$$

$$\eta : \text{Gal}(KL/k) \xrightarrow{\psi} \text{Aut}_{\text{cont}}(N) = \mathbb{Z}_p^\times.$$

$$\begin{array}{ccc} \psi & & \psi \\ x \mapsto & \longrightarrow & (y \mapsto x^{-1}yx) \end{array}$$

L_0 : L/k の部分体で、 $[L_0:k]$ が p と素になる最大のもの。

$m_0 = [L_0:k]$. m_0 は $p-1$ の約数。

(1.4) 次の集合間に bijection がある。

$$\left\{ \begin{array}{l} \text{Twisted } \mathbb{Z}_p\text{-拡大 } k/k \text{ の} \\ k \text{ 上の isomorphism class} \end{array} \right\} \begin{array}{c} \text{1:1} \\ \longleftrightarrow \end{array} \left\{ \begin{array}{l} H^1(k, M) \text{ の直和因子で} \\ \mathbb{Z}_p \text{ と同型なもの} \end{array} \right\}$$

$$\begin{array}{ccc} \psi & & \psi \\ K & \longleftrightarrow & W = \text{Ker}(H^1(k, M) \rightarrow H^1(k, M)) \end{array}$$

ただし, M は, rank 1 の free \mathbb{Z}_p -加群で,
 $\text{Gal}(\bar{k}/k)$ の作用を η を経由して入れたもの。

2.

代数体 k に対して,

$C_k = (\text{compact}) p\text{-class group}$,

($\cong \text{Gal}(k^{nr}/k)$, k^{nr} は最大不分岐 p -ヘルム p -拡大 k).

(2.1) 以下 K/k は, Twisted \mathbb{Z}_p -拡大であるとし, 分岐に
 関する次の 2 条件が満たされていると仮定する。

(2.1.1) K/k で分岐する k の素点は有限個。

(2.1.2) L/L_0 で分岐する p 上の素点は, KL/L_0 でも分岐
 する。

L/k が有限次のときは, (2.1.1), (2.1.2) はともに
 満たされる。

有限 p -ヘルム群の列 $\{A_n\}$, $\{B_n\}$ に対し,

$$A_n \cong B_n$$

で, $\{\# \text{Ker } f_n\}$, $\{\# \text{Coker } f_n\}$ がともに bounded と存在

homomorphism の列 $\{f_n: A_n \rightarrow B_n\}$ が存在することを示す。

(2.2) 仮定 (2.1) の下で、次が成立する。

(a) $\dim_{\mathbb{Q}_p} C_K \otimes_{\mathbb{Z}_p} \mathbb{Q}_p < +\infty$ のとき、

$$C_{k_n} \approx \frac{(p^n - 1)}{m_0} \cdot A \oplus n \cdot (\# \text{Coker } \eta) B \oplus C/p^n C.$$

(b) $\dim_{\mathbb{Q}_p} C_K \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = +\infty$ のとき、

$$C_{k_n} \approx \frac{(p^n - 1)}{m_0} A \oplus n (\# \text{Coker } \eta) B \oplus C_n,$$

$$C_n \otimes_{\mathbb{Z}} \mathbb{Z}/p^n \approx n (\# \text{Coker } \eta) \cdot C/p^n C, \quad s \in \mathbb{Z}_{>0}.$$

ここに、 A, B, C は有限生成 \mathbb{Z}_p -加群で、

A, B は torsion, C は torsion-free であるものをあらわす。

L/k が有限次るときは、(a) が自動的に成立し、 $B=0$ である。 L/k が無限次で (b) をみたすものが存在する。 L/k が無限次るときは、(a), (b) のどちらが成立するかを一般的に決めるのは困難であると思われるが、次のような特殊な場合には、(a) が成立する。

(2.3) (2.1) を仮定し、 L/k が無限次であるとする。 k で

k と異なり、 L_0 を含む L の有限次の部分体をあらわす。

このとき、 k の twisted \mathbb{Z}_p -拡大 k' で次の2条件をみたすものが存在する。

$$(2.3.1) \quad K'L = KL.$$

(2.3.2) K' は、 k 上の twisted \mathbb{Z}_p -拡大 k' と k' との合成体ではない。

このとき、 K'/k' に対しては、(2.2) の (a) が成立する。すなわち $\dim_{\mathbb{Q}_p} C_{K'} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p < +\infty$. さらに、整数 $\lambda, \mu \geq 0, \nu$ が存在して、

$$\# C_{k'_n} = p^{e_n}, \quad e_n = \lambda n + \mu p^n + \nu$$

が、十分大きな n での整数 n に対して成立する。

ただし、 k'_n は $[k'_n : k'] = p^n$ とする K'/k' の中間体。

(2.3) のような K'/k' として例えは"次のようなものが"ある。

$$k' = k(\zeta), \quad K = \bigcup_n k'_n, \quad k'_n = k'(\sqrt[p^n]{\zeta \alpha}).$$

ここで、 ζ は、1 の p 乗根で k に含まれない

もの、 α は $k^x \setminus (k^x)^p / \mu_{p^\infty}$ の元。 $\zeta \alpha$ の p^n 乗根 $\sqrt[p^n]{\zeta \alpha}$ は、

$$(\sqrt[p^{i+1}]{\zeta \alpha})^p = \sqrt[p^i]{\zeta \alpha}, \quad i > 0, \text{ をみたすように定める。}$$

3.

この § では、 K/k を CM 体の Twisted \mathbb{Z}_p -拡大とする。

(3.1) 上の仮定の下で、 KL , L はともに CM 体である。

(3.2) さらに以下を仮定する。

(3.2.1) $KL(\mathcal{M}_p) > K(\mathcal{M}_{p^\infty})$.

(3.2.2) K/L で分解する K の素点 \mathfrak{p} について条件 (2.1) が成立。

(3.2.3) $C_L^- (= \ker(C_L \rightarrow C_{L^+}))$ は有限生成。

(3.3) 次のように F, F' を定める。

(3.3.1) $F: \mathbb{Z}_{\geq 0} \rightarrow \mathbb{N}$,

$$F(x) = \max\{1, x-t+1\} \cdot \# \text{Coker } \eta_x$$

ただし、

$$t = \min\{n \in \mathbb{Z}_{\geq 0} \mid 1+p^{n+1}\mathbb{Z}_p \subset \text{Im } \eta\}, \text{Im } \eta \text{ が有限のとき}$$

は、 $t = \infty$ 。

$$\eta_x: H \xrightarrow{\eta} \mathbb{Z}_p^x \rightarrow (\mathbb{Z}/p^{x+1})^x.$$

(3.3.2)

$$F'(x) = \begin{cases} F(x) & \text{if } x \leq t, \\ F(x)-1 & \text{if } x > t. \end{cases}$$

(3.4) $\lambda = \dim_{\mathbb{Q}_p} C_K^- \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ とおく。次のような条件を

みたす $n \in \mathbb{Z}_{\geq 0}$ に対し、(3.4.1), (3.4.2) が成立する。

" L/L^+ で分解し、 KL/L で分岐する素点 \mathfrak{p} は、 $KL/K_n L$ で完全分岐する。"

(3.4.1) $\exists \lambda \text{ ord}_p \# C_{k_{n+1}/k_n}^- < F'(n)$ が成立すれば”

次の (1) ~ (3) が成立する。

(1) $\lambda = \text{ord}_p \# C_{k_{n+1}/k_n}^-$.

(2) 任意の $m \geq n$ に対し, $\text{ord}_p \# C_{k_m/k_n}^- = \lambda(m-n)$

が成立する。

(3) $C_{k,i}^- = \text{Ker}(C_{k,i}^- \rightarrow C_{k,i}^-)$, $i \geq 0$ とおく。任意の自然数 $m \geq n$ に対し,

$$p C_{k,m}^- = C_{k,m+1}^-$$

が成立する。

(3.4.2) $\exists \lambda \text{ ord}_p C_{k_{n+1}/k_n}^- \geq F'(n)$ なら

$$\lambda \geq F'(n)$$

である。

関数 F' は F 以上に良くするとはできない。また、 F' を F に置きかえて成立する場合があるか、一般的にそうできるかどうかは不明である。

$$C_{k_m/k_n}^- = \text{Ker}(C_{k_m}^- \rightarrow C_{k_n}^-) \text{ である。}$$

証明には、木田の公式 (Kida [3]) を用いた。

文献

- [1] Iwasawa, K., Lectures on p -adic L -functions, Ann. of Math. Studies No. 74
- [2] Iwasawa, K., On \mathbb{Z}_p -extensions of algebraic number fields, Ann. of Math., 98, 246-326, 1973
- [3] Kida, Y., \mathbb{Q} -extensions of CM-fields and cyclotomic invariants, J. Number theory, 12, 519-528, 1980