数理解析研究所講究録
1026巻 1998年 43-62

楕円曲線の岩澤理論における木田の公式について

八森 祥隆 (Yoshitaka Hachimori)
(東大数理 博士課程2年)
松野 一夫 (Kazuo Matsuno)
(東大数理 博士課程1年)

1. 序

p を奇素数とし, 本稿を通じ固定しておく. $n \geqq 1$ に対し, μ_{p^n} を 1 の p^n 乗根のなす群とし, $\mu_{p^\infty} = \cup_n \mu_{p^n}$ とする. $\mathbb{Q}_\infty$ を $\mathbb{Q}(\mu_{p^\infty})$ の部分体で $\mathbb{Q}$ 上の Galois 群が $\mathbb{Z}_p$ に同型となる唯一の体とする. K を代数体とする. $K_\infty = K\mathbb{Q}_\infty$ とおく (円分 $\mathbb{Z}_p$-拡大). $n \geqq 0$ にたいし, K_n を K_∞/K の $[K_n : K] = p^n$ なる唯一の中間体とする.

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_\infty, \quad \cup_n K_n = K_\infty.$$

岩澤理論は, もともとは K_n のイデアル類群の n を動かしたときの変化を研究するものであった. その後, それと p 進 L 関数との深い関わりが発見された. それは岩澤主予想とよばれている ([Wa] Chap. 13, 15 参照).

岩澤理論は今やイデアル類群以外多くの対象について存在する. その中心にある哲学の1つは代数的なもの ("Selmer 群") と 解析的なもの ("p 進 L 関数") を結び付ける関係, "岩澤主予想" があるだろうというものである.

ここでは Mazur によって建設された楕円曲線の岩澤理論を扱う ([Maz], [Man1]). K を代数体とし, E を K 上の楕円曲線とする. E は更に p 上の全ての素点で good ordinary reduction をもつものとする. ここでイデアル類群のかわりになるものは E の Selmer 群である. まず理論の概観を復習しよう (詳しくは §7 参照). 考える代数的対象は $\mathrm{Sel}_{p^\infty}(E/K_\infty)$ の Pontrjagin dual $\mathfrak{X}_{E/K}$ (定義は §7.2) である. これには $\mathrm{Gal}(K_\infty/K)$ が作用するが, それをある程度記述するものとして "characteristic ideal" $\mathrm{char}_{\mathbb{Z}_p[[T]]}(\mathfrak{X}_{E/K})$ という, $\mathbb{Z}_p[[T]]$ の単項イデアルが定義される.

一方, 対応するべき p 進 L 関数は, K がアーベル体で E が $\mathbb{Q}$ 上の modular な楕円曲線であるという条件の下で, Mazur and Swinnerton-Dyer [M-SD] により構成されている. それは $\mathbb{Z}_p[[T]]$ の元である. (ここでは $f_{E/K}(T)$ と書く. 定義は §3 と §4.1.) これは E の Hasse-Weil L 関数の 1 での値を p 進的に補間したものとして特徴づけられる (定理 3.1 を見よ).

そして p 進 L 関数 が存在する条件の下では, "岩澤主予想" が定式化されている (§7.3 参照). それは, $\mathrm{char}_{\mathbb{Z}_p[[T]]}(\mathfrak{X}_{E/K})$ と $f_{E/K}(T)$ の生成するイデアルが一致するというものである. この岩澤主予想は現時点では未解決である.

さて, 岩澤理論でよく考える重要な不変量の1つとして λ, μ 不変量がある. $\mathfrak{X}_{E/K}$ に付随するλ, μ 不変量 $\lambda_{E/K}$, $\mu_{E/K}$ を考えることができる (§7.2). また, p 進 L 関数 $f_{E/K}(T)$ に対してもλ, μ 不変量 $\lambda_{E/K}^{p-L}$, $\mu_{E/K}^{p-L}$ (§4.1) が定義される. 岩澤主予想の下では, 特に $\lambda_{E/K} = \lambda_{E/K}^{p-L}$, $\mu_{E/K} = \mu_{E/K}^{p-L}$ となることに注意する (§7.3).

本稿で我々は次の状況を考える. L を K の有限次 Galois 拡大で, $[L:K]$ が p 巾であるものとする (p-拡大).

この時 $\mathfrak{X}_{E/K}$ と同様に, L に対しても $\mathfrak{X}_{E/L}$を考えることができる. そして 不変量 $\lambda_{E/L}$ が定まる. 今回我々が得た結果の一つは, $\lambda_{E/L}$ と $\lambda_{E/K}$ の間の関係式である (定理 8.1). それは次のような形になった.

$$\lambda_{E/L} = [L_\infty : K_\infty]\lambda_{E/K} + \sum_{w:split} (e_{L_\infty/K_\infty}(w) - 1) + 2 \sum_{w:good} (e_{L_\infty/K_\infty}(w) - 1).$$

但し $e_{L_\infty/K_\infty}(w)$ は分岐指数で, 最初の和では w は L_∞ の素点で E が split multiplicative reduction を持つもの, 2番目の和では w は L_∞ の p 上にない素点で E が good reduction を持ち, ある条件を満たすものを動く.

一方, L, K が共にアーベル体で E が $\mathbb{Q}$ 上 modular のときには p 進 L 関数 $f_{E/L}(T)$, $f_{E/K}(T)$ が定義され, $\lambda_{E/L}^{p-L}$ と $\lambda_{E/K}^{p-L}$ が定まる. 今回述べるもう一つの結果は$\lambda_{E/L}^{p-L}$ と $\lambda_{E/K}^{p-L}$ の間の関係式である (定理 4.1, 松野による).

ここで注目すべきことは定理 4.1 と 定理 8.1 の公式の形は E が $\mathbb{Q}$ 上 modular で L/K が共にアーベル体の時には一致するという事実である. このことは岩澤主予想を仮定すれば上に述べたことから当然成り立たなければならない事である. しかし岩澤主予想が未解決の現在そのことは自明でないことを注意しておく.

実はこういったことは代数体のオリジナルな (イデアル類群の) 岩澤理論においてすでに行なわれている. それは木田の公式とよばれている ([Ki]). 今回の結果はその類似である. ここで木田の公式について復習しておこう.

K を CM 体とする. K_+ を K の最大総実部分体とする. $A(K_n)$ を K_n のイデアル類群の p-part とする. norm map による逆極限を $X_K := \varprojlim A(K_n)$ とおく (これが楕円曲線で $\mathfrak{X}_{E/K}$ にあたる). X_K には自然に複素共役が作用しており, ± 1 倍の固有空間を $X_K^{\pm}$ とおくと, $X_K = X_K^+ \oplus X_K^-$ と分解される. ここでは X_K^- に注目する. X_K^- には付随する不変量 λ_K^-, $\mu_K^- \in \mathbb{Z}$ が定義される ([Wa], p. 286). 特に $\mu_K^- = 0$ であるときには $\mathbb{Z}_p$-module として, 次のようになる ([Wa] Cor. 13.29):

$$X_K^- \cong (\mathbb{Z}_p)^{\lambda_K^-}. \tag{1.1}$$

定理 1.1 ([Ki]). L/K を 有限次 Galois p-拡大で, 共に CM 体であるものとする. 更に K は μ_p を含むものとする. $\mu_K^- = 0$ とする. このとき $\mu_L^- = 0$ でかつ

$$2\lambda_L^- - 2 = [L_\infty : K_\infty](2\lambda_K^- - 2) + \sum_w (e_{L_\infty/K_\infty}(w) - 1)$$

が成り立つ. 但し $e_{L_\infty/K_\infty}(w)$ は分岐指数とし, w は L_∞ の素点で p 上になく, $L_\infty/L_{+\infty}$ で split するものを動く.

代数体と関数体の間には密接な類似がある. この場合 X_K^- は関数体における Jacobian の Tate module の類似と思える ([Iw1]). すると (1.1) を見れば λ_K^- は genus (の2倍) の類似であり, 定理 1.1 は 被覆に関する Riemann-Hurwitz の genus 公式の類似である.

一方, p 進 L 関数は, ここで必要な場合のみをいうと, p 進 ζ 関数 $\zeta_{K_+,p}(s)$ という, K_+ の Dedekind ζ 関数の負の整数点の値を補間した p 進解析関数が存在する (久保田-Leopoldt, Deligne-Ribet). 更に, ある巾級数 $g_{K_+}(T) \in \mathbb{Z}_p[[T]]$ と, ある $u \in \mathbb{Z}_p^\times$ により,

$$\zeta_{K_+,p}(s) = g_{K_+}(u^s - 1)/(u^s - 1)$$

となる (岩澤, Deligne-Ribet, cf. [Wil] Sect. I). これは楕円曲線における $f_{E/K}(T)$ にあたる. このとき $f_{E/K}(T)$ と同様, 付随する λ, μ 不変量が定義される.

そして K を定理 1.1 のものとした時, $g_{K_+}(T)$ と X_K^- は次のように深く関係する. X_K^- には自然に $\mathrm{Gal}(K_\infty/K)$ が作用するが, これにより $\mathrm{char}_{\mathbb{Z}_p[[T]]}(X_K^-)$ という $\mathbb{Z}_p[[T]]$ の単項イデアルが定義される (§7.1 参照). じつはそれが $g_{K_+}(T)$ の生成するイデアルに一致するのである (岩澤主予想, Mazur-Wiles, Wiles [Wil] Th'm 1.2, 1.4).

特に $g_{K_+}(T)$ に付随する λ, μ 不変量は λ_K^-, μ_K^- に一致する. 従って 定理 1.1 は それらに対しても当然成り立つ. 実際, Gras, Sinnott が p 進 L 関数の性質のみを使って定理 1.1 の別証明を与えた ([Si]). この結果が定理 4.1 に対応する事実である.

本稿の構成は Part I が p 進 L 関数に対する木田の公式で, Part II が Selmer 群に対する木田の公式である.

Part I は次のようになっている. §2 で p 進 L 関数の構成に必要な modular symbol についてまとめた. §3 では p 進 L 関数の定義と構成を復習する. §4 で引続き $f_{E/K}(T)$ の定義と, 付随する λ, μ 不変量の定義を復習した後, 主定理 (定理 4.1) を述べる. §5 では得られた公式を実例により検証する. §6 は証明の概略である. Part II は次の通りである. §7 では Selmer 群の岩澤理論を復習し, p 進 L 関数との関わり (岩澤主予想) について述べる. また, 付随する λ, μ 不変量の意味を復習する. §8 で主定理 (定理 8.1) を述べる. §9 は証明の概略である. §10 でいくつかの remark を述べる.

なお, 講演においては Part I を八森が, Part II を松野が担当した.

Part I. p 進 L 関数の木田の公式

2. Hasse-Weil L 関数 と modular symbol

E を $\mathbb{Q}$ 上の modular な楕円曲線とする. 対応する Hecke eigen normalized newform を $f(z) = \sum_n a_n e^{2\pi i z}$ $(a_n \in \mathbb{Z})$ とおき, その level を N とする. E の L 関数

$$L(E,s) = \sum_n a_n n^{-s}$$

はこのとき全 $s \in \mathbb{C}$-平面に解析接続され, $s = 1$ の軸を中心に関数等式をもつことはよく知られている ([Kna] Th'm 9.8).

ψ を Dirichlet 指標としたとき

$$L(E,\psi,s) := \sum_n \psi(n) a_n n^{-s}$$

とすると, 解析接続され関数等式が成り立つ ([Kna] Th'm 12.2). また, ψ の Gauss 和を

$$\tau(\psi) := \sum_{a\in\mathbb{Z}/m} \psi(a)\zeta_m^a$$

とおく (但し m は ψ の conductor). さらに, $\mathrm{sgn}(\psi)$ を $\psi(-1)$ の符号 ($\pm$) とする.

$H_1(E(\mathbb{C}),\mathbb{Z})$ には複素共役が作用しており, ± 1 倍で作用する部分群 $H_1(E(\mathbb{C}),\mathbb{Z})^{\pm}$ の生成元を $\gamma^{\pm}$ とする. ω_E を Neron differential とするとき, period を

$$\Omega_E^{\pm} = \int_{\gamma^{\pm}} \omega_E$$

と定義する. この時,

$$\frac{m}{\tau(\psi)} \frac{L(E,\psi,1)}{\Omega_E^{\mathrm{sgn}(\psi)}} \in \mathbb{Q}(\psi) \tag{2.1}$$

($\mathbb{Q}(\psi)$ は $\mathbb{Q}$ に ψ の値を全て付加した体) であることはよく知られている ([Man2] §4, §5).

2.1. **modular symbol について.** (2.1) は "modular symbol" とよばれる E が modular であることによって定義される関数

$$x_E^{\pm} : \mathbb{Q}\cup\{i\infty\} \longrightarrow \mathbb{Q}$$

により表すことができる (Manin, [Man2]). $x_E^{\pm}$ は次の式で定義されるものである:

$$\int_0^{\eta} -2\pi i f(z)dz = x_E^{+}(\eta)\Omega_E^{+} + x_E^{-}(\eta)\Omega_E^{-}.$$

重要なことは, これにより, L 関数の 1 での値が

$$\begin{cases} \dfrac{L(E,1)}{\Omega_E^{+}} = x_E^{+}(i\infty), \\ \dfrac{m}{\tau(\psi)} \dfrac{L(E,\psi,1)}{\Omega_E^{\mathrm{sgn}(\psi)}} = \displaystyle\sum_{a\in\mathbb{Z}/m} x_E^{\mathrm{sgn}(\psi)}(\frac{a}{m})\overline{\psi}(a) \quad (\text{if } \psi \neq 1) \end{cases} \tag{2.2}$$

と表されることである (cf. [Man2] §4,Th'm 4.2, §5, Th'm 5.5). また, その性質として次の Hecke 作用の公式が成り立つ (cf. [Man2] §3 Th'm 3.5). l を素数とする.

$$\begin{cases} a_l x_E^{\pm}(\eta) = x_E^{\pm}(l\eta) + \displaystyle\sum_{k=0}^{l-1} (x_E^{\pm}(\frac{\eta+k}{l}) - x_E^{\pm}(\frac{k}{l})) \quad (l\nmid N \text{ の時}), \\ a_l x_E^{\pm}(\eta) = \displaystyle\sum_{k=0}^{l-1} (x_E^{\pm}(\frac{\eta+k}{l}) - x_E^{\pm}(\frac{k}{l})) \quad (l|N \text{ の時}). \end{cases} \tag{2.3}$$

$x_E^{\pm}(\eta)$ の具体的計算も可能である: $\Gamma_0(N)\backslash SL_2(\mathbb{Z})$ (有限集合) の元 j にたいし

$$\xi^{\pm}(j) := x_E^{\pm}(\frac{a}{b}) - x_E^{\pm}(\frac{c}{d}) \quad \left(\text{但し } j \ni \begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)$$

とおくと, $x_E^{\pm}(\eta)$ の値は, η の連分数展開を用いることにより $\xi^{\pm}(j)$ たち の $\mathbb{Z}$-結合でかける. 故に有限個の $\xi(j)$ らを計算できればよく, これらのことは E (と f) が与えられれば実行可能である (Manin, [Man2] §1, §2, §3, §8). [St1] にはこれで (2.1) を計算した表がある.

3. p 進 L 関数

E を $\mathbb{Q}$ 上の modular な楕円曲線とする. E の conductor を N とする. 重要な仮定として 以下 E は p で good ordinary reduction をもつものとする ($p \nmid N$).

$n \geqq 1$ にたいし, μ_{p^n} を 1 の p^n 乗根のなす群とし, $\mu_{p^\infty} = \cup_n \mu_{p^n}$ とする. $\mathbb{Q}_\infty$ を $\mathbb{Q}(\mu_{p^\infty})$ の部分体で $\mathbb{Q}$ 上の Galois 群が $\mathbb{Z}_p$ に同型となる唯一の体とする. $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ とおく. また, Γ の生成元 γ_0 を 1 つ固定しておく. $\overline{\mathbb{Q}}(\subset \mathbb{C})$ から $\overline{\mathbb{Q}}_p$ への埋め込みを 1 つ fix しておく.

3.1. **p 進 L とは.** 上の仮定の下では, $a_p \not\equiv 0 \mod p$ なので, $T^2 - a_pT + p$ の根で $\mathbb{Z}_p^\times$ の元になるものが唯 1 つ存在するが, それを α とおく. χ を Dirichlet 指標とする. χ は上の埋め込みにより $\overline{\mathbb{Q}}_p$ に値をとるものと考える. $\mathcal{O}_\chi$ を $\mathbb{Z}_p$ に χ の値を全て付加した環とする. m を χ の conductor の p と素な部分とする.

E の (χ に付随する) p 進 L 関数 とは, 次のようなものである.

定理 3.1 ([M-SD], [St2] Th'm 4.4). $f_{E,\chi}(T) \in \frac{1}{c}\mathcal{O}_\chi[[T]]$ $(\exists c \in \mathbb{Z})$ で, 次をみたすものが唯一つ存在する: ϕ を Γ の有限位数の指標として任意にとる. これを Dirichlet 指標と同一視すると, $\chi\phi$ の conductor は ある n があって mp^n とかける. このとき,

$$f_{E,\chi}(\phi(\gamma_0) - 1) = \alpha^{-n}(1 - \chi\phi(p)\alpha^{-1})(1 - \overline{\chi\phi}(p)\alpha^{-1}) \times \frac{mp^n}{\tau(\overline{\chi\phi})} \frac{L(E, \overline{\chi\phi}, 1)}{\Omega_E^{\mathrm{sgn}(\chi)}}. \tag{3.1}$$

Rem . あとでは使わないが $\kappa : \Gamma \to \mathbb{Z}_p{}^\times$ を cyclotomic 指標としたとき

$$L_p(E, \overline{\chi}, s) := f_{E,\chi}(\kappa(\gamma_0)^{s-1} - 1)$$

と定義し, これを E の p 進 L 関数 と呼ぶことが多い.

Rem . 代数体の場合と異なり, χ の odd, even に関係なく $f_{E,\chi}(T) \neq 0$ である ([Ro] 参照).

3.2. **構成.** この構成は [St2] §4 による. $f_{E,\chi}(T)$ は 代数体の p 進 L 関数を構成するとき用いられた "Stickelberger element" ([Wa] §7.2) の類似 を構成することにより得られる. そのために modular symbol が必要となる. ここでは measure を用いて定義する. measure や distribution については [Wa] Chap. 12 を参照.

M を p と素な整数とし,

$$\mathbb{Z}_{p,M} := \varprojlim_n \mathbb{Z}/p^nM, \quad \mathbb{Z}_{p,M}^\times := \varprojlim_n (\mathbb{Z}/p^nM)^\times$$

とする. $\mathbb{Z}_{p,M}^\times$ は 標準的に $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty M})/\mathbb{Q})$ に同型であり,

$$\mathbb{Z}_{p,M}^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{pM})/\mathbb{Q}) \times \Gamma \tag{3.2}$$

と分解される. 以下これらを同一視する. $\mathbb{Z}_{p,M}^{\times}$ 上の $\mathbb{Q}_p$-valued distribution $\theta_{E,M}^{\pm}$ を次のように定める: $n \geqq 1$, $a \in \mathbb{Z}$, $(a, pM) = 1$ に対し,

$$\theta_{E,M}^{\pm}(a + p^n M\mathbb{Z}_{p,M}) := \alpha^{-n-1}(\alpha x_E^{\pm}(\frac{a}{p^n M}) - x_E^{\pm}(\frac{a}{p^{n-1}M}) + (1-\alpha)x_E^{\pm}(i\infty)). \tag{3.3}$$

これが distribution law を満たすことは (2.3) で $l = p$ とした式により示すことができる. 更にある (M に依らぬ) 定数 $c \in \mathbb{Z}$ があって $\theta_{E,M}^{\pm}$ は $\frac{1}{c}\mathbb{Z}_p$-valued measure となる.

さて, ψ を $\mathbb{Z}_{p,M}^{\times}$ の位数有限な指標とする. ψ は (必ずしも primitive でない) Dirichlet 指標と同一視できる. この ψ に対し,

$$f_{E,M,\psi}(T) := \int_{\mathbb{Z}_{p,M}^{\times}} \psi(x)(1+T)^{\iota(<x>)} d\theta_{E,M}^{\mathrm{sgn}(\psi)}(x) \tag{3.4}$$

とおく. 但し $<>$ は (3.2) での Γ への projection とし, ι は, $\iota : \Gamma \to \mathbb{Z}_p$ で, $\gamma \in \Gamma$ に対し $\gamma = \gamma_0^{\iota(\gamma)}$ となるものと定義する.

そこで, χ を 定理 3.1 のものとし, m を χ の conductor の p と素な部分とする. χ は $\mathbb{Z}_{p,m}^{\times}$ の指標と同一視される.

$$f_{E,\chi}(T) := f_{E,m,\chi}(T) \tag{3.5}$$

と定義する. これが求めたものであるのは,

$$\begin{aligned} f_{E,\chi}(\phi(\gamma_0) - 1) &= \int_{\mathbb{Z}_{p,m}^{\times}} \chi(x)\phi(x) d\theta_{E,m}^{\mathrm{sgn}(\chi)}(x) \\ &= \sum_{a \in (\mathbb{Z}/p^n m)^{\times}} \chi\phi(a)\theta_{E,m}^{\mathrm{sgn}(\chi)}(a + p^n m\mathbb{Z}_{p,m}) \end{aligned}$$

となり, (2.2), (2.3) らにより, これが (3.1) の右辺となるためである.

予想 3.1. $\theta_{E,M}^{\pm}$ は $\mathbb{Z}_p$-valued ($c = 1$ にとれる. [St2] §4 Conj. IV). 従って任意の χ で $f_{E,\chi}(T) \in \mathcal{O}_{\chi}[[T]]$.

Rem . 有限個を除く (good ordinary な) p で予想は成り立つ. ([St2] Th'm 4.6). §5 における例ではこの予想は全て正しい.

4. 木田の公式

4.1. **$f_{E/K}(T)$ の定義と付随する不変量.** まず巾級数に対する λ, μ 不変量の定義を復習する. 一般に $\mathcal{O}$ を $\mathbb{Q}_p$ の有限次拡大の整数環とする. π を $\mathcal{O}$ の素元とする. $g(T) = \sum_n a_n T^n (\neq 0) \in \mathcal{O}[[T]]$ にたいし, それに付随する λ, μ 不変量とは

$$\begin{cases} \mu = \mu_{g(T)} := \max\{m \mid \pi^m | g(T)\}, \\ \lambda = \lambda_{g(T)} := \min\{n \mid \pi \nmid (a_n/\pi^{\mu})\} \end{cases} \tag{4.1}$$

と定義されるものであった.

以下, 予想 3.1 を仮定する. 上に述べたようにこれはほとんど成り立つ条件である. K をアーベル体とする. [M-SD] p.52 に従い, K 上の E の p 進 L 関数 $f_{E/K}(T)$ とその λ,

μ 不変量を定義する. 以下 K を次の条件 C1(E,K) を満たすものとする.

C1(E,K) : S を E が additive reduction をもつ素数全体の集合とする. 任意の K の素点で S 上にあるものにおいて, 再び E は additive reduction をもつ.

Rem . これは E が semi-stable ならどんな K でも成り立つ条件である. また, $K/\mathbb{Q}$ で additive prime が分岐しなければ成り立つ.

$K\cap\mathbb{Q}_\infty=\mathbb{Q}$ のときには

$$f_{E/K}(T):=\prod_{\chi} f_{E,\chi}(T)$$

とおく. ここで χ は $\mathrm{Gal}(K/\mathbb{Q})$ の指標全体を動く. これは $\mathbb{Z}_p[[T]]$ の元となる. 次に, $K\cap\mathbb{Q}_\infty\neq\mathbb{Q}$ のときには ある n があって $[K\cap\mathbb{Q}_\infty:\mathbb{Q}]=p^n$ となっている. そして

$$g((1+T)^{p^n}-1)=\prod_{\chi} f_{E,\chi}(T)$$

なる $g(T)\in\mathbb{Z}_p[[T]]$ が存在する. そこで $f_{E/K}(T):=g(T)$ と定義する.

$$\text{(4.2)}\qquad \begin{cases} \lambda_{E/K}^{p-L}: &= \lambda_{f_{E/K}(T)}(=\sum_\chi \lambda_{f_{E,\chi}(T)}),\\ \mu_{E/K}^{p-L}: &= \mu_{f_{E/K}(T)} \end{cases}$$

とおく. これらの不変量の意味については §7.3 で述べる.

4.2. **木田の公式.** K を条件 C1(E,K) を満たすアーベル体とする. L/K を p-拡大とし, L はアーベル体で, C1(E,L) を満たすものとする.

Rem . $p\geqq 5$ ならば, K が C1(E,K) を満たすなら 自動的に L は C1(E,L) を満たす.

$\lambda_{E/L}^{p-L}$, $\lambda_{E/K}^{p-L}$ らを(4.2) で定義したものとする.

定理 4.1 ([Mat]). $\mu_{E/K}^{p-L}=0$ とする. このとき $\mu_{E/L}^{p-L}=0$ でかつ

$$\lambda_{E/L}^{p-L}=[L_\infty:K_\infty]\lambda_{E/K}^{p-L}+\sum_{w:split}(e_{L_\infty/K_\infty}(w)-1)+2\sum_{w:good}(e_{L_\infty/K_\infty}(w)-1)$$

が成り立つ. 但し $e_{L_\infty/K_\infty}(w)$ は分岐指数で, 最初の和では w は L_∞ の素点で E が split multiplicative reduction を持つものを動き, 2 番目の和では w は L_∞ の p 上にない素点で E が good reduction を持ち, $E(L_{\infty,w})\supset E_p$ (E_p は p 等分点の群) なるものを動くものとする.

Rem . 有限個を除く (good ordinary な) p で$\mu_{E/K}^{p-L}=0$ が予想されている. ([St2] p. 95). 実際多くの実例がある (cf. §5).

5. 計算例

$\lambda_{E,\chi}$ や $\mu_{E,\chi}$ は序に挙げた代数体の場合の計算例 (例えば [DFKS]) の方法と同様にして計算することができる. それには次の合同式をみる:

$$\text{(5.1)}\qquad f_{E,\chi}(T)\equiv\sum_{a\in(\mathbb{Z}/mp^{n+1})^\times}\chi(a)\theta_{E,m}^{\mathrm{sgn}(\chi)}(a+p^{n+1}\mathbb{Z}_{p,m})(1+T)^{t(a)}\mod\omega_n.$$

TABLE 1. 木田の公式

(1) $p=3$, $E=X_0(11)$,

$K=\mathbb{Q}(\sqrt{13})$
$\lambda_{E/K}^{p-L}=1$, $\mu_{E/K}^{p-L}=0$

l	$\chi(l)$	a_l	g	$\lambda_{E/L}^{p-L}$	λ_1	λ_ψ	λ_χ	$\lambda_{\chi\psi}$
7	-1	-2	1	7	0	0	1	3
13	0	4	1	3	0	0	1	1
19	-1	0	1	3	0	0	1	1
31	-1	7	1	7	0	0	1	3
37	-1	3	1	3	0	0	1	1
43	1	-6	2	3	0	0	1	1
61	1	12	2	3	0	0	1	1
67	-1	-7	1	7	0	2	1	1
73	-1	4	3	15	0	0	1	7
79	1	-10	2	11	0	2	1	3
97	-1	-7	1	7	0	2	1	1

$K=\mathbb{Q}(\sqrt{19})$
$\lambda_{E/K}^{p-L}=1$, $\mu_{E/K}^{p-L}=0$

l	$\chi(l)$	a_l	g	$\lambda_{E/L}^{p-L}$	λ_1	λ_ψ	λ_χ	$\lambda_{\chi\psi}$
7	-1	-2	1	7	0	0	1	3
13	-1	4	1	7	0	0	1	3
19	0	0	1	3	0	0	1	1
31	1	7	2	3	0	0	1	1
37	-1	3	1	3	0	0	1	1
43	-1	-6	1	3	0	0	1	1
61	1	12	2	3	0	0	1	1
67	1	-7	2	11	0	2	1	3
73	1	4	6	3	0	0	1	1
79	1	-10	2	11	0	2	1	3
97	-1	-7	1	7	0	2	1	1

(2) $p=7$, $E=37A$,

$K=\mathbb{Q}(\sqrt{-11})$,
$\lambda_{E/K}^{p-L}=5$, $\mu_{E/K}^{p-L}=0$

l	$\chi(l)$	a_l	g	$\lambda_{E/L}^{p-L}$	λ_1	λ_ψ	λ_χ	$\lambda_{\chi\psi}$
29	-1	6	1	35	1	1	4	4
43	-1	2	1	47	1	3	4	4
71	1	9	2	59	1	3	4	6

$K=\mathbb{Q}(\sqrt{6})$,
$\lambda_{E/K}^{p-L}=3$, $\mu_{E/K}^{p-L}=0$

l	$\chi(l)$	a_l	g	$\lambda_{E/L}^{p-L}$	λ_1	λ_ψ	λ_χ	$\lambda_{\chi\psi}$
29	1	6	2	21	1	1	2	2
43	1	2	2	45	1	3	2	4
71	1	9	2	45	1	3	2	4

但し, $t(a)$ は $t(a)\equiv\iota(<a>) \mod (p^n)$, $0\leqq t(a)<p^n$, $\omega_n=(1+T)^{p^n}-1$ とする. すると $\lambda_{\omega_n}=p^n$ なので, 例えばある n と k で (5.1) の右辺の T^k の係数が p で割れないものが存在すれば, その最小の k が λ 不変量となり $\mu=0$ となる. $\theta_{E,m}^{\pm}$ は (3.3) で定義され, $x_E^{\pm}(a)$ は §2.1 でのべたように Manin により具体的に計算する方法が与えられている. 従って E が与えられればこれらの不変量は計算可能である. (例えば [M-SD] の最後に表が載っている.)

定理 4.1 を実例により確かめたい. そこで次の条件 (A) を満たす L/K を考える.

(A) K を 2 次体とし, l を $l\equiv 1(p)$ なる E が good reduction をもつ素数 (即ち $l\nmid N$) とする. M_l を conductor l の $\mathbb{Q}$ 上 p 次 cyclic 拡大体とする. $L=KM_l$ とおく.

(A) の状況で, 次の場合に $\lambda_{E/K}^{p-L}$, $\lambda_{E/L}^{p-L}$ を計算機で計算した. (**Table 1**, 計算には Pari-Gp を用いた). いずれも予想 3.1 は成り立つ. またいずれも $\mu_{E/K}=0$ である.

- $p=3$, $E=X_0(11)$, $K=\mathbb{Q}(\sqrt{13})$, $\mathbb{Q}(\sqrt{19})$, $0<l<100$.
- $p=7$, $E=37A$, $K=\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{6})$, $0<l<100$.

但し, $37A$ は $y^2+y=x^3-x$ で定義される導手 37 の楕円曲線とする.

$\lambda_{E/K}^{p-L}$, $\lambda_{E/L}^{p-L}$ は指標ごとに$\lambda_{E,\chi}$ を計算して足し合わせる. 表においては$\lambda_{E,\chi}$ らをλ_1, λ_ψ, λ_χ, $\lambda_{\chi\psi}$ により表示した. ここで 1 は自明な指標, χ は K の指標, ψ は M_l の指標で自明でないものとする. これらが実際計算機を用いて計算した部分である. これを用いて $\lambda_{E/K}^{p-L}$, $\lambda_{E/L}^{p-L}$ は次の式で計算される.

$$\lambda_{E/K}^{p-L} = \lambda_1 + \lambda_\chi,\ \lambda_{E/L}^{p-L} = \lambda_1 + (p-1)\lambda_\psi + \lambda_\chi + (p-1)\lambda_{\chi\psi}.$$

一方, 定理 4.1 によれば (A) の状況では木田の公式は次の (5.2) のようになるはずである ($\mu_{E/K} = 0^{p-L}$ を仮定する). 但し, $g = \#\{w : \text{primes of } L_\infty \text{ over } l\}$ とする. また, (5.2) の条件は $E(L_{\infty,w})$ が p 等分点を含むかどうかの条件を a_l の条件に言いかえたものである.

$$\lambda_{E/L}^{p-L} = p\lambda_{E/K}^{p-L} + \begin{cases} & \chi(l) = -1 \text{ and } a_l \equiv \pm 2(p) \\ 2(p-1)g & \cdots \text{ または} \\ & \chi(l) = 0 \text{ or } 1, \text{ and } a_l \equiv 2(p), \\ 0 & \cdots \text{ otherwise.} \end{cases} \tag{5.2}$$

表の $\lambda_{E/K}^{p-L}$, $\lambda_{E/L}^{p-L}$ が (5.2) を満たすことを確かめよう. 例えば $p = 3$, $E = X_0(11)$, $K = \mathbb{Q}(\sqrt{13})$, $l = 7$ のとき, 表の値は $\lambda_{E/K}^{p-L} = 1$, $\lambda_{E/L}^{p-L} = 7$. 一方, (5.2) は, $\chi(l) = -1$ かつ $a_l \equiv -2(3)$ であるから上の場合となる. この時 $g = 1$ であるから

$$\lambda_{E/L}^{p-L} = 3\lambda_{E/K}^{p-L} + 4$$

となる. 表の値はこれを満たす. 表の他の場合も同様に確かめることができる.

Rem . λ_1, λ_ψ, λ_χ, $\lambda_{\chi\psi}$ らの計算例により, §6 の Lem. 6.2+6.4 も確かめられる.

6. 証明の概略

ここでは場合を限定して証明する. 詳細は [Mat] 参照. 証明は [Si] の方針に従う (Lem. 6.2, Lem. 6.4) が, Lem. 6.4 は [Si] の方法ではできないので Hecke 作用を用いた別の方針 (Lem. 6.3) で示す. まず次の補題がある.

Lemma 6.1. $K \subset L \subset M$ をいずれもアーベル体で M/K が p-拡大とする. M/K, L/K, M/L いずれか 2 つで定理 4.1 が正しければ, 残りの 1 つも正しい.

このことから $p \nmid [K : \mathbb{Q}]$ の場合を示せば十分である. さらに

(i) $L \subset K_\infty$
(ii) $p \nmid [K : \mathbb{Q}]$ かつ $L \cap K_\infty = K$

の場合を示せば十分. ここでは (ii) のみ示す. このとき L' で $\mathbb{Q}$ 上 p-拡大 かつ $L = KL'$ なるものがある. 更に簡単のため特に次の場合に限定して示す.

- L' は $\mathbb{Q}$ 上 p 次 cyclic で conductor が素数 l ($L' = M_l$). 更に l は K の conductor と素で E は l で good reduction をもつ (即ち $l \nmid N$).

定義 (4.2) と仮定により次のようにかける.

$$\begin{cases} \lambda_{E/K}^{p-L} : & = \sum_\chi \lambda_{E,\chi}, \\ \lambda_{E/L}^{p-L} : & = \sum_\chi \sum_\psi \lambda_{E,\chi\psi}. \end{cases} \tag{6.1}$$

但し χ は $K/\mathbb{Q}$ の指標, ψ は $L'/\mathbb{Q}$ の指標を走り, $\lambda_{E,\chi} := \lambda_{f_{E,\chi}(T)}$, $\lambda_{E,\chi\psi} := \lambda_{f_{E,\chi\psi}(T)}$ などと定義する. そこで$\lambda_{E,\chi}$ と $\lambda_{E,\chi\psi}$ ($\psi \neq 1$) を比べることを考える. χ の conductor を

m とする. ψ の conductor は l であり, 仮定より (m,l)=1 である. (3.5) の定義に戻れば $f_{E,\chi}(T)=f_{E,m,\chi}(T)$, $f_{E,\chi\psi}(T)=f_{E,ml,\chi\psi}(T)$ である. χ は $\mathbb{Z}_{p,ml}^{\times}$ の指標ともみなせるから, (3.4) により $f_{E,ml,\chi}(T)$ が定義できる. (ψ は *even* なので $\mathrm{sgn}(\chi)=\mathrm{sgn}(\chi\psi)$ であることを注意しておく.)

$f_{E,ml,\chi}(T)$ の λ, μ 不変量を $\lambda_{E,ml,\chi}$, $\mu_{E,ml,\chi}$ とする.

Lemma 6.2 ([Si] Prop. 2.1). $\mu_{E,ml,\chi}=0 \Leftrightarrow \mu_{E,\chi\psi}=0$. 更にそのとき

$$\lambda_{E,ml,\chi}=\lambda_{E,\chi\psi}.$$

次に $\lambda_{E,\chi}$ と $\lambda_{E,ml,\chi}$ を比べる. 次の補題が必要である. φ を 自然な射影 $\mathbb{Z}_{p,ml}^{\times}\to\mathbb{Z}_{p,m}^{\times}$ とする. 次は §2.1 (2.3) より導かれる.

Lemma 6.3. U を $\mathbb{Z}_{p,m}^{\times}$ の open subset とする. この時

$$\varphi(\theta_{E,ml}^{\pm})(U)(:=\theta_{E,ml}^{\pm}(\varphi^{-1}(U)))=a_l\theta_{E,m}^{\pm}(U)-\theta_{E,m}^{\pm}(l^{-1}U)-\theta_{E,m}^{\pm}(lU).$$

Rem . [M-SD] §8 Lem. 2 にこの補題が書いてあるが間違っていると思われる. l が bad $(l\mid N)$ の場合にも上のような公式がある ((2.3) を使う). それにより以下の議論と同様にして l が bad のときの公式も示せる.

次に a を $p^{a+1}|l-1$ なる最大の整数とする. 次のようにおく. 但し $\mathfrak{p}$ は $\mathcal{O}_\chi$ の p 上の素イデアルとする.

$$g_\chi(l):=\begin{cases}0 & \cdots\ \chi(l)+\chi(l)^{-1}\not\equiv a_l \mod \mathfrak{p},\\ 2a & \cdots\ \chi(l)=\pm1 \text{ and } a_l\equiv\pm2 \mod p \text{ (複号同順)},\\ a & \cdots\ \text{otherwise.}\end{cases}$$

Lemma 6.4. $\mu_{E,ml,\chi}=\mu_{E,\chi}$ かつ$\lambda_{E,ml,\chi}=\lambda_{E,\chi}+g_\chi(l)$.

(略証). χ は conductor m なので $x\in\mathbb{Z}_{p,ml}^{\times}$ に対し

$$\chi(x)(1+T)^{\iota(<x>)}=\chi(\varphi(x))(1+T)^{\iota(<\varphi(x)>)}.$$

である (φ は上で定義した射影). 故に

$$f_{E,ml,\chi}(T)=\int_{\mathbb{Z}_{p,ml}^{\times}}\chi(x)(1+T)^{\iota(<x>)}d\theta_{E,ml}^{\mathrm{sgn}(\chi)}(x)=\int_{\mathbb{Z}_{p,m}^{\times}}\chi(y)(1+T)^{\iota(<y>)}\varphi(\theta_{E,ml}^{\mathrm{sgn}(\chi)})(y)$$

となり, 補題 6.3 により

$$=\int_{\mathbb{Z}_{p,m}^{\times}}(a_l\chi(y)(1+T)^{\iota(<y>)}-\chi(l^{-1}y)(1+T)^{\iota(<l^{-1}y>)}-\chi(ly)(1+T)^{\iota(<ly>)})d\theta_{E,m}^{\mathrm{sgn}(\chi)}(y)$$

$$=(a_l-\chi(l)^{-1}(1+T)^{-\iota(<l>)}-\chi(l)(1+T)^{\iota(<l>)})\int_{\mathbb{Z}_{p,m}^{\times}}\chi(y)(1+T)^{\iota(<y>)}d\theta_{E,m}^{\mathrm{sgn}(\chi)}(y)$$

$$=(a_l-\chi(l)^{-1}(1+T)^{-\iota(<l>)}-\chi(l)(1+T)^{\iota(<l>)})f_{E,m,\chi}(T)$$

となる. よって $(a_l-\cdots)$ の部分が $\lambda=g_\chi(l)$, $\mu=0$ となることをみれば良い. (証終)

更に χ を $\mathrm{Gal}(K/\mathbb{Q})$ の指標全体を走らせた時, 次の補題がある.

Lemma 6.5. $\sum_{\chi} g_\chi(l) = \begin{cases} 0 & \text{if } E(K_{\infty,v}) \not\supset E_p, \\ 2\#\{K_\infty \text{ の } l \text{ 上の素点 }\} & \text{if } E(K_{\infty,v}) \supset E_p. \end{cases}$

但し v は K_∞ 上の l 上の (任意の) 素点で, E_p は E の p 等分点のなす群とする.

(略証). l の Frobenius の E_p への作用の固有値を $\alpha, \beta \in \overline{\mathbb{F}}_p$ とおく. $\alpha+\beta \equiv a_l \mod p$ である. さらに $l \equiv 1 \mod p$ だったから $\beta = \alpha^{-1}$ である. $\mathcal{O}$ を $\mathbb{Z}_p$ に 1 の $[K:\mathbb{Q}]$ 乗根を付加した環, $\mathfrak{p}'$ をその素イデアルとする. ($\mathcal{O} \supset \mathcal{O}_\chi$ である.) $\mathcal{O}/\mathfrak{p}' \hookrightarrow \overline{\mathbb{F}}_p$ を一つ定めておく. 従って $g_\chi(l)$ の定義より

$$g_\chi(l) \neq 0 \Leftrightarrow a_l \equiv \chi(l) + \chi(l)^{-1} \mod \mathfrak{p}$$
$$\Leftrightarrow \alpha = \chi(l) \text{ or } \chi(l)^{-1} \text{ in } \overline{\mathbb{F}}_p$$

$K/\mathbb{Q}$ の l の分解指数を f とおけば $\chi(l)$ は 1 の f 乗根を値としてもつが, χ が動く時 f 乗根のそれぞれを $[K:\mathbb{Q}]/f$ 回ずつとる. (f は p と素であるから $\chi(l)$ を $\mod \mathfrak{p}$ して $\overline{\mathbb{F}}_p$ へいってもそれぞれを $[K:\mathbb{Q}]/f$ 回ずつとることに注意.) 上の同値性よりもし $\alpha^f \neq 1$ ならば $\sum_\chi g_\chi(l) = 0$. もし $\alpha^f = 1$ ならば $g_\chi(l) \neq 0$ となる χ の数は$\alpha = \pm 1$ なら $[K:\mathbb{Q}]/f$ 個, $\alpha^f \neq \pm 1$ なら $2[K:\mathbb{Q}]/f$ 個 である. 従っていずれにせよ $\sum_\chi g_\chi(l) = 2a[K:\mathbb{Q}]/f$ となる. この右辺は $2\#\{K_\infty$ の l 上の素点 $\}$ に一致する. あとは $\alpha^f = 1$ と $E(K_{\infty,v}) \supset E_p$ の同値性をいえばよい. これは $\alpha^f = 1$ と $[K_v(E_p) : K_v]$ が p 巾であることの同値性と $K_{\infty,v}/K_v$ が最大不分岐 p-拡大であることから分かる. (証終)

さて証明であるが, (6.1) より,

$$\lambda_{E/L}^{p-L} = \sum_\chi \sum_\psi \lambda_{E,\chi\psi}$$
$$= \sum_\chi \lambda_{E,\chi} + \sum_{\psi\neq 1}(\sum_\chi \lambda_{E,\chi\psi}) = \lambda_{E/K}^{p-L} + \sum_{\psi\neq 1}(\sum_\chi \lambda_{E,\chi\psi})$$

となり, 補題 6.2, 6.4 と $\psi \neq 1$ なる ψ の数が $p-1$ 個であることから

$$= \lambda_{E/K}^{p-L} + (p-1)(\lambda_{E/K}^{p-L} + \sum_\chi g_\chi(l))$$
$$= p\lambda_{E/K}^{p-L} + (p-1)\sum_\chi g_\chi(l)$$
$$= p\lambda_{E/K}^{p-L} + \begin{cases} 0 & \text{if } E(K_{\infty,v}) \not\supset E_p \\ 2\#\{K_\infty \text{ の } l \text{ 上の素点 }\} & \text{if } E(K_{\infty,v}) \supset E_p \end{cases}$$

$[L_\infty : K_\infty] = p$ なので 分岐する素点は不分解. このとき分岐指数は p. さらに分岐する素点 は l 上の素点のみだったことに注意する. 故に

$$\#\{K_\infty \text{ の } l \text{ 上の素点 }\} = \#\{L_\infty \text{ の } l \text{ 上の素点 }\}$$

である. また, w を L_∞ の l 上の素点とし, v を K_∞ への制限としたとき, $K_{\infty,v}(E_p)/K_{\infty,v}$ は不分岐であり, $L_{\infty,v}/K_{\infty,v}$ は完全分岐であることから, $E(K_{\infty,v}) \supset E_p$ と $E(L_{\infty,v}) \supset E_p$ は同値である. 以上より上の式はこの L/K に対する定理 4.1 の公式に一致する.

Part II. Selmer 群の木田の公式

7. 楕円曲線の岩澤理論

この章では, 楕円曲線の岩澤理論を復習する. [Man1], [Ku] を参考文献として挙げておく.

p を奇素数とする. $\mathbb{Q}_\infty$ を §3 の始めで定義した $\mathbb{Q}$ 上の $\mathbb{Z}_p$-拡大とする. K を有限次代数体とするとき, $K_\infty = K\mathbb{Q}_\infty$ とおく (円分 $\mathbb{Z}_p$-拡大). $\Gamma := \mathrm{Gal}(K_\infty/K)$ とおく. $\Gamma \cong \mathbb{Z}_p$ (位相アーベル群として) である. $n \geqq 0$ にたいし, K_n を K_∞/K の $[K_n : K] = p^n$ なる唯一の中間体とする.

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_\infty, \quad \cup_n K_n = K_\infty.$$

Γ の生成元 γ_0 を固定しておく. M を compact な $\mathbb{Z}_p$-module で Γ が連続に作用しているものとする. このとき M は自然に $\mathbb{Z}_p[[\Gamma]]$-module となる. 更に

$$\mathbb{Z}_p[[\Gamma]] \cong \mathbb{Z}_p[[T]] \quad (\gamma_0 \rightsquigarrow T+1)$$

という同型 ([Wa] Th'm 7.1) により $\mathbb{Z}_p[[T]]$-module の構造が入ることはよく知られている.

7.1. **$\mathbb{Z}_p[[T]]$ 上の加群に付随する不変量.** 最初に $\mathbb{Z}_p[[T]]$ 上の加群について復習し, 付随する不変量を定義する. 一般に $\mathcal{O}$ を $\mathbb{Q}_p$ の有限次拡大体 k の整数環とする. M を有限生成 $\mathcal{O}[[T]]$-torsion $\mathcal{O}[[T]]$-module とする. このとき次の kernel, cokernel 有限な $\mathcal{O}[[T]]$-module の準同型がある ([Wa] Th'm 13.12).

$$M \to \oplus_i \mathcal{O}[[T]]/(g_i(T))^{m_i}. \tag{7.1}$$

但し, $g_i(T)$ は $\mathcal{O}[[T]]$ の素元で, $m_i \in \mathbb{Z}$, $\geqq 1$ とする. $g(T) := \prod_i g_i(T)^{m_i}$ の生成する $\mathcal{O}[[T]]$ の 単項 ideal は上の準同型のとり方によらず定まる. これを M の characteristic ideal と呼び

$$\mathrm{char}_{\mathcal{O}[[T]]}(M)$$

と書く. その生成元 (つまり $g(T)$) に対し (4.1) で定義した λ, μ 不変量を

$$\lambda_M := \lambda_{g(T)}, \quad \mu_M := \mu_{g(T)}$$

とおくと, $g(T)$ の取り方によらず定まる. (7.1) から, M との関係は次のようになる ([Wa] §13.4 の最後参照).

$$\begin{cases} \lambda_M = \dim_k(M \otimes_{\mathcal{O}} k), \\ \mu_M = 0 \Leftrightarrow M \text{ は有限生成 } \mathcal{O}\text{-module}. \end{cases} \tag{7.2}$$

7.2. **Selmer 群.** K を一般の有限次代数体, E を K 上 の楕円曲線とする. 重要な仮定として, 以下 E は K の p 上の全ての素点で good ordinary reduction を持つものとする.

F を K の拡大体とする. $0 \leqq m \leqq \infty$ に対し E の F 上の p^m-Selmer 群とは,

$$\mathrm{Sel}_{p^m}(E/F) := \mathrm{Ker}(H^1(F, E_{p^m}) \to \prod_v H^1(F_v, E))$$

と定義される群である. ここで, E_{p^m} は E の p^m 等分点のなす群とする. 一般にアーベル群 A に対し A_{p^m} で p^m 倍写像の kernel を表す ($A_{p^\infty} = \cup_m A_{p^m}$). $\mathrm{Sel}_{p^\infty}(E/F)$ は次のような完全列をもつ. 但し $Ш(E/F)$ は Tate-Shafarevich 群である.

$$0 \to E(F) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_{p^\infty}(E/F) \to Ш(E/F)_{p^\infty} \to 0.$$

K_∞ 上の p^∞-Selmer 群 $\mathrm{Sel}_{p^\infty}(E/K_\infty)$ を考える. 自然な inclusion $E_{p^m} \to E_{p^{m+1}}$ と restriction により

$$\mathrm{Sel}_{p^\infty}(E/K_\infty) \cong \varinjlim_n \varinjlim_m \mathrm{Sel}_{p^m}(E/K_n)$$

である. これには Γ が作用しており, その Pontrjagin dual

$$\mathfrak{X}_{E/K} := \mathrm{Hom}(\mathrm{Sel}_{p^\infty}(E/K_\infty), \mathbb{Q}_p/\mathbb{Z}_p)$$

は $\gamma \in \Gamma$ が $\phi \in \mathfrak{X}_{E/K}$ に, $(\gamma\phi)(s) = \phi(\gamma^{-1}s)$ と作用するものとして, Γ が連続に作用する compact $\mathbb{Z}_p$-module となる. これにより, $\mathfrak{X}_{E/K}$ には §7 の始めに述べたように $\mathbb{Z}_p[[T]]$-module の構造が入る. さらに,

定理 7.1 ([Man1] Th'm 4.5). $\mathfrak{X}_{E/K}$ は有限生成 $\mathbb{Z}_p[[T]]$-module となる.

次が予想されている.

予想 7.1 (Mazur). $\mathfrak{X}_{E/K}$ は更に $\mathbb{Z}_p[[T]]$-torsion であろう.

Rem . 次の場合に予想は正しい.

- $\mathrm{Sel}_{p^\infty}(E/K)$ が有限 (Mazur, [Man1] cor. 2.7).
- E が modular で K が アーベル体 (Rubin, 加藤).

$M = \mathfrak{X}_{E/K}$ にたいし上の予想を認めれば, §7.1 で定義した λ, μ 不変量が定義できる.

$$\lambda_{E/K} := \lambda_{\mathfrak{X}_{E/K}}, \quad \mu_{E/K} := \mu_{\mathfrak{X}_{E/K}} \tag{7.3}$$

と定義する. (7.2) よりこれらは次の意味をもつ.

$$\begin{cases} \mu_{E/K} = 0 & \Leftrightarrow \mathrm{Sel}_{p^\infty}(E/K_\infty) \text{ は cofinitely generated } \mathbb{Z}_p\text{-module.} \\ \mu_{E/K} = 0 & \text{のとき } \lambda_{E/K} = \mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(E/K_\infty). \end{cases} \tag{7.4}$$

Rem . 有限次代数体 K_n の段階では $Ш$ は有限と予想されているので, $\mathrm{Sel}_{p^\infty}(E/K_n)$ の $\mathbb{Z}_p$-corank は $E(K_n)$ の rank に一致すると予想される. しかし, $\mathrm{Sel}_{p^\infty}(E/K_\infty)$ ではその $\mathbb{Z}_p$-corank ($= \lambda_{E/K}$) は $E(K_\infty)$ の rank より真に大きいこともあると思われる. ($Ш$ が無限ということ.)

7.3. <u>岩澤主予想</u>. ここで特に K がアーベル体で E が $\mathbb{Q}$ 上の modular な楕円曲線であるときを考える. この時 §4.1 で定義した "解析的な" p 進 L 関数 $f_{E/K}(T)$ がある. これと上の "代数的" な $\mathfrak{X}_{E/K}$ との関係を述べる. 次が予想されている.

予想 7.2 (岩澤主予想, [M-SD] §9 conj. 3). (予想 3.1, 予想 7.1 が成り立ち更に)

$$\mathrm{char}_{\mathbb{Z}_p[[T]]}(\mathfrak{X}_{E/K}) = (f_{E/K}(T)).$$

これらの予想の下 (4.2) で定義した不変量らは次のような関係をもつ.

$$\lambda_{E/K} = \lambda_{E/K}^{p-L},\ \mu_{E/K} = \mu_{E/K}^{p-L}. \tag{7.5}$$

より詳しく $\mathfrak{X}_{E/K}$ を見る事が出来る: K を first kind (conductor が p^2 で割れない) とし, χ を $\mathrm{Gal}(K/\mathbb{Q})$ の 指標とする. $\mathrm{Sel}_{p^\infty}(E/K)$ には Δ が作用しているので $\mathfrak{X}_{E/K}$ は (上の Γ の作用と同様にして) Δ-module となる. そこで $\mathfrak{X}_{E/K}$ のχ-quotient

$$(\mathfrak{X}_{E/K})_\chi := \mathfrak{X}_{E/K} \otimes_{\mathbb{Z}_p[\Delta]} \mathcal{O}_\chi$$

($\mathcal{O}_\chi$ は χ を通じて $\mathbb{Z}_p[\Delta]$-module とみなす) は自然に $\mathcal{O}_\chi[[T]]$-module となる. $[K:\mathbb{Q}]$ が p と素なら $(\mathfrak{X}_{E/K})_\chi$ は $\mathfrak{X}$ の $\mathbb{Z}_p[[T]]$-module としての直和因子である.

予想 7.3 (岩澤主予想, [M-SD] §9 conj. 3). $\mathrm{char}_{\mathcal{O}_\chi[[T]]}((\mathfrak{X}_{E/K})_\chi) = (f_{E,\chi}(T))$.

予想 7.3 が全ての χ で成り立てば 予想 7.2 が成り立つ.

Rem . 加藤により, 次が示されている.

$$\mathrm{char}_{\mathcal{O}_\chi[[T]]}((\mathfrak{X}_{E/K})_\chi) \ni p^n f_{E,\chi}(T) \quad (\exists n).$$

8. 木田の公式

K を一般の有限次代数体, E を K 上 の楕円曲線とする. L/K を 有限次 Galois p-拡大で次の条件 C2(E,L/K) を満たすものとする.

C2(E,L/K) : S を E が additive reduction をもつ K の素点全体の集合とする. 任意の L の素点で S 上にあるものにおいて, 再び E は additive reduction をもつ.

Rem . この時全ての素点で reduction type が変わらない. $p \geqq 5$ の時 任意の L は自動的に C2(E,L/K) を満たす. E が semi-stable なら 任意の L/K で C2(E,L/K) は成り立つ. また, L/K で additive prime が分岐しないなら成り立つ.

E を L 上の楕円曲線とも思えるから, §7.2 で K を全て L と置き換えることにより $\mathfrak{X}_{E/L}$ が定義され, $\mathrm{Gal}(L_\infty/L)$ の作用で $\mathbb{Z}_p[[T]]$-module とみなせ, $\lambda_{E/L}$, $\mu_{E/L}$ などを (7.3) と同じく定義することができる.

定理 8.1 ([HM]). $\mathfrak{X}_{E/K}$ が $\mathbb{Z}_p[[T]]$-torsion でかつ $\mu_{E/K} = 0$ と仮定する. このとき $\mathfrak{X}_{E/L}$ も $\mathbb{Z}_p[[T]]$-torsion でかつ $\mu_{E/L} = 0$ が成り立つ. 更に

$$\lambda_{E/L} = [L_\infty : K_\infty]\lambda_{E/K} + \sum_{w:split} (e_{L_\infty/K_\infty}(w) - 1) + 2 \sum_{w:good} (e_{L_\infty/K_\infty}(w) - 1)$$

が成り立つ. 但し $e_{L_\infty/K_\infty}(w)$ は分岐指数で, 最初の和では w は L_∞ の素点で E が split multiplicative reduction を持つものを動き, 2 番目の和では w は L_∞ の p 上にない素点で E が good reduction を持ち, $E(L_{\infty,w}) \supset E_p$ (E_p は p 等分点の群) なるものを動くものとする.

Rem . K, L が共にアーベル体で E が $\mathbb{Q}$ 上の modular な楕円曲線であるとき, 定理 8.1 の公式の形は定理 4.1 のそれに一致する. それは予想 7.2 と (7.5) によれば成り立つべきことだが, 予想は現時点で未解決だからそのことは自明でない.

Rem . K がアーベル体で E が $\mathbb{Q}$ 上の modular な楕円曲線のときには, 岩澤主予想を仮定すれば, $\mu_{E/K} = \mu_{E/K}^{p-L}$ であるから, 定理 4.1 の後の Rem. と同じく, 有限個を除く (good ordinary な) p で $\mu_{E/K} = 0$ であると予想できる.

9. 証明

ここでは証明の概略を示す. 詳細は [HM] 参照.

9.1. **準備.** まず, 証明に必要な事実を列挙する. F を有限次代数体とする. S を F の素点の有限集合で p 上の素点と無限素点を全て含むものとする. F の任意の拡大体 F' に対し S の上の素点全体を $S(F')$ とかくことにする. F_S で F の S の外不分岐最大拡大を表す. $F_\infty \subset F_S (= F_{\infty, S(F_\infty)})$ である.

定理 9.1 (cohomological dimension).

(i) ([Hab] Prop. 7) $\mathrm{cd}_p(\mathrm{Gal}(F_S/F_\infty)) \leqq 2$.

(ii) (cf. [Se] Chap. II) v を F_∞ の任意の素点とする. $\mathrm{cd}_p(\mathrm{Gal}(\overline{F}_{\infty,v}/F_{\infty,v})) = 1$.

E を F 上の楕円曲線とする. F_∞ の p 巾分点について次の結果がある.

定理 9.2 ([Im]). $E(F_\infty)_{p^\infty}$ は有限.

次は Tate local duality などよりの帰結である.

定理 9.3 ([Man1] p.34, [Se] Chap II Prop. 16). v を F の任意の有限素点とし, $v|l$ とする. このとき

$$E(F_v) \cong \mathbb{Z}_l^{[F_v:\mathbb{Q}_l]} \oplus (\text{finite}), \quad H^2(F_v, E) = 0.$$

S をさらに E が bad reduction をもつ素点を全て含むとする. すると

$$0 \to \mathrm{Sel}_{p^\infty}(E/F_\infty) \to H^1(F_S/F_\infty, E_{p^\infty}) \xrightarrow{\varphi} \prod_{v \in S(F_\infty)} H^1(F_{\infty,v}, E)_{p^\infty}$$

という完全列がある. 次の事実はそれ自体重要であり, 証明の鍵でもある.

定理 9.4 ([Pe] Prop 4.6). 予想 7.1 が成り立つ ($\mathfrak{X}_{E/F}$ が $\mathbb{Z}_p[[T]]$-torsion) ならば, φ は全射. さらに $H^2(F_S/F_\infty, E_{p^\infty}) = 0$.

9.2. **証明の方針.** 証明の方針は [Iw2] の最後に示されている Herbrand 商の計算による証明を踏襲する. これは CM 楕円曲線の場合の [Mi] でも用いられた. (§10 最後の Rem. 参照). しかし, 今の場合, Selmer 群を何らかの形で体の言葉 (乗法群や単数群) になおす方法 (類体論など) がなく, [Iw2], [Mi] とは全く別の方法で示さねばならない. 次の補題が成り立つ.

Lemma 9.1. $K \subset L \subset M$ で M/K が p-拡大であるとする. M/K, L/K, M/L いずれか 2 つで定理 8.1 が正しければ, 残りの 1 つも正しい.

故に L/K が p 次 cyclic 拡大の場合に証明すれば十分である. $L \subset K_\infty$ の時は $L_\infty = K_\infty$ なので, $\mathfrak{X}_{E/L} = \mathfrak{X}_{E/K}$, 故に $\lambda_{E/L} = \lambda_{E/K}$, $\mu_{E/L} = p\mu_{E/K}$, となり定理は明らか. よって $L \cap K_\infty = K$ の場合を示せばよい. $G := \mathrm{Gal}(L_\infty/K_\infty)$ とおく. $G \cong \mathbb{Z}/p$ である. S を K の素点の有限集合で, p 上の素点と無限素点, E が bad reduction をもつ素点, さらには L/K で分岐する素点を全て含むものとする. すると $K_S \supset L_\infty$ であり, $L_{S(L)} = K_S$ である. $\mathrm{Sel}_{p^\infty}(E/L_\infty)$ には G が作用している.

Proposition 9.1. restriction map

$$\mathrm{Sel}_{p^\infty}(E/K_\infty) \to \mathrm{Sel}_{p^\infty}(E/L_\infty)^G$$

は kernel, cokernel 有限である.

証明はここでは省略するが,

$$H^i(G, E(L_\infty)_{p^\infty}) \ (i = 1, 2), \quad H^1(\mathrm{Gal}(L_{\infty,w}/K_{\infty,v}), E(L_{\infty,w})) \ (\forall v \in S(K_\infty))$$

らが有限集合である事実が証明に必要であることを注意しておく. これらのことは前者は後の Lem 9.2, 後半は Lem 9.3 とその後の Rem. を参照されたい. 系として次がわかる.

Cororally 9.1. $\mathfrak{X}_{E/K}$ が $\mathbb{Z}_p[[T]]$-torsion でかつ $\mu_{E/K} = 0$ と仮定する. このとき $\mathfrak{X}_{E/L}$ は $\mathbb{Z}_p[[T]]$-torsion でかつ $\mu_{E/L} = 0$. 更にこのとき

$$\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}(E/L_\infty)^G) = \lambda_{E/K}.$$

Proof. §7 (7.4) により, "$\mathfrak{X}_{E/K}$ が $\mathbb{Z}_p[[T]]$-torsion かつ $\mu_{E/K} = 0$" は $\mathrm{Sel}_{p^\infty}(E/K_\infty)$ が $\mathbb{Z}_p$-cofinitely generated であることを意味する. 従って Prop. より $\mathrm{Sel}_{p^\infty}(E/L_\infty)^G$ もそうであり, 従って $(\mathfrak{X}_{E/L})_G$ (G-coinvariant) は有限生成 $\mathbb{Z}_p$-module. このことから $\mathfrak{X}_{E/L}$ は有限生成 $\mathbb{Z}_p[G]$-module となる. (それは $\mathbb{Z}_p[G]$ が compact 局所環であり compact 群 $\mathfrak{X}_{E/L}$ に連続に作用している. これより compact 局所環に関する "Nakayama の lemma" が使えるため. [Wa],Lem. 13.16 の証明参照.) よって特に $\mathfrak{X}_{E/L}$ は有限生成 $\mathbb{Z}_p$-module. 故に再び (7.2) より $\mathfrak{X}_{E/L}$ は $\mathbb{Z}_p[[T]]$-torsion でかつ $\mu_{E/L} = 0$. (7.4) より $\lambda_{E/K} = \mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}(E/K_\infty))$ だから最後の式がでる. □

これにより定理の前半がわかった. M を cofinitely generated $\mathbb{Z}_p$-module で G が作用しているものとする. このときある α, β, γ があって次の cokernel 有限な単射がある (cf. [Iw2],p. 285).

$$M \to (\mathbb{Q}_p/\mathbb{Z}_p)^\alpha \oplus (\mathbb{Q}_p/\mathbb{Z}_p)[G]^\beta \oplus (I_G)^\gamma. \tag{9.1}$$

但し I_G は $\mathbb{Z}_p[G]$ の augumentation ideal の Pontrjagin dual とする. 次は容易にわかる.

$$\alpha + \beta = \mathrm{corank}_{\mathbb{Z}_p} M^G, \ \gamma - \alpha = h(M).$$

但し, $h(M)$ は M の Herbrand 商, 即ち

$$h(M) := \dim_{\mathbb{F}_p} H^2(G, M) - \dim_{\mathbb{F}_p} H^1(G, M)$$

とおく. 従って,

$$\text{(9.2)} \qquad \mathrm{corank}_{\mathbb{Z}_p}(M) = \alpha + p\beta + (p-1)\gamma = p(\mathrm{corank}_{\mathbb{Z}_p}(M^G)) + (p-1)h(M)$$

がわかる. $M = \mathrm{Sel}_{p^\infty}(E/L_\infty)$ とおけば, 上のことが使えて、$\mathrm{corank}_{\mathbb{Z}_p}(M) = \lambda_{E/L}$ であり, Cor. 9.1 より $\mathrm{corank}_{\mathbb{Z}_p} M^G = \lambda_{E/K}$ がわかる. あとは $h(M)$ が計算できればよい. それには, 定理 9.4 による完全列

$$0 \to \mathrm{Sel}_{p^\infty}(E/L_\infty) \to H^1(K_S/L_\infty, E_{p^\infty}) \to \prod_{v \in S(K_\infty)} (\prod_{w|v} H^1(L_{\infty,w}, E)_{p^\infty}) \to 0$$

を使う. 但し, 素点の有限集合 S は Prop. 9.1 の直前でとったものとする. $S(K_\infty)$ は有限集合である. これにより,

$$h(\mathrm{Sel}_{p^\infty}(E/L_\infty)) = h(H^1(K_S/L_\infty, E_{p^\infty})) - \sum_{v \in S(K_\infty)} h(\prod_{w|v} H^1(L_{\infty,w}, E)_{p^\infty})$$

と (右辺の各項がもし有限なら) 計算される. 次に右辺を計算する.

9.3. Herbrand 商の計算.

9.3.1. *global part.*

Lemma 9.2. $H^i(G, H^1(K_S/L_\infty, E_{p^\infty}))$ $(i = 1, 2)$ は有限, 更に $h(H^1(K_S/L_\infty, E_{p^\infty})) = 0$.

Proof. 定理 9.1, 9.4 より $H^i(K_S/L_\infty, E_{p^\infty}) = H^i(K_S/K_\infty, E_{p^\infty}) = 0$ $(i \geqq 2)$. 故に Hochschild-Serre spectral sequence ([Iw2] p.282 参照) により

$$H^i(G, H^1(K_S/L_\infty, E_{p^\infty})) \cong H^i(G, E(L_\infty)_{p^\infty}).$$

定理 9.2 より右辺は有限であり, $h(E(L_\infty)_{p^\infty}) = 0$. □

9.3.2. *local part I.* 次に local な方の計算をする. $v \in S(K_\infty)$ が L_∞/K_∞ で分解するなら $L_{\infty,w} = K_{\infty,v}$ である. 従って $H^i(G, \prod_{w|v} H^1(L_{\infty,w}, E)_{p^\infty}) = 0$. 故に不分解のときのみ考えれば良い. w を $L_{\infty,w}$ の v 上の唯一の素点とする. この時 $G = \mathrm{Gal}(L_{\infty,w}/K_{\infty,v})$ となる. まず $v \nmid p$ の場合を考える. このとき不分解なのは v が L_∞/K_∞ で分岐するときのみであることを注意しておく. また,

$$\text{(9.3)} \qquad H^1(L_{\infty,w}, E)_{p^\infty} \cong H^1(L_{\infty,w}, E_{p^\infty})$$

が分かる ($v \nmid p$ と定理 9.3 による). 定理 9.1 (ii) と Hochschild-Serre により

$$\text{(9.4)} \qquad H^i(G, H^1(L_{\infty,w}, E_{p^\infty})) \cong H^i(G, E(L_{\infty,w})_{p^\infty})$$

となる. ここで次の命題を用いる.

Proposition 9.2. $l \neq p$ とし, $[F_v : \mathbb{Q}_l] < \infty$ とする. F_v が μ_p を含むとする. $F_{v,\infty} := F_v(\mu_{p^\infty})$ とおく ($F_{v,\infty}/F_v$ は $\mathbb{Z}_p$-拡大). E/F_v を楕円曲線とする. このとき $E(F_v) \cap E_p = 0$ なら $E(F_{v,\infty})_{p^\infty} = 0$. そうでなければ,

$$E(F_{v,\infty})_{p^\infty} \cong \begin{cases} (\mathbb{Q}_p/\mathbb{Z}_p)^2 & E \text{ は good reduction をもつ,} \\ \mathbb{Q}_p/\mathbb{Z}_p \oplus (\text{finite}) & E \text{ は split multiplicative reduction をもつ,} \\ (\text{finite}) & \text{その他.} \end{cases}$$

Rem . split multiplicative なら常に $E(F_v) \cap E_p \neq 0$ である.

Proof. $E(F_v) \cap E_p = 0$ のときは $F_{v,\infty}/F_v$ は p-拡大だからいえる (p-群の性質, [Man1] Lem 3.5 の議論参照). そうでないとする. 簡単のため good reduction の場合のみ示す. $F_{v,n}$ を n 番目の中間体とする. $F_{v,\infty}/F_v$ は不分岐だから norm map $E(F_{v,n+1}) \to E(F_{v,n})$ は全射 ([Man1] p. 32). $l \neq p$ より, 定理 9.3 を見れば, $E(F_{v,n+1})_{p^\infty} \to E(F_{v,n})_{p^\infty}$ も全射が分かる. よって $E(F_{v,\infty})_{p^\infty}$ は無限群. 従って任意の m にたいし ある n があって $E(F_{v,n})_{p^\infty}$ は位数 p^m の点を含む. 故に適当に基底をとることにより $\mathrm{Gal}(\overline{F}_v/F_{v,n})$ の E_{p^m} への作用の行列は $\begin{pmatrix} 1 & b(\sigma) \\ 0 & d(\sigma) \end{pmatrix}$ と書ける. Weil pairing により $1 \times d(\sigma)$ は $\mathrm{Gal}(\overline{F}_v/F_{v,n})$ の μ_{p^m} への作用を定める. 今 n を m より大きくとれば仮定より $F_{v,n} \supset \mu_{p^m}$ であるから $d(\sigma) \equiv 1$ でなければならない. さらに m を大きくすれば $F_{v,\infty}/F_v$ は不分岐最大 p-拡大だから $b(\sigma) \equiv 0$ とできる. 故に $E(F_{v,\infty}) \supset E_{p^m}$ である. m は任意だったので示された. □

$v \nmid p$ であり, L_w/K_v は分岐しているので, $L_w \supset K_v \supset \mu_p$ である. 故に $K_{\infty,v} = K_v(\mu_{p^\infty})$, $L_{\infty,w} = L_w(\mu_{p^\infty})$ である. 従って命題が使えて, 次が分かる (C2(E, L/K) の条件はここで使う).

$$h(H^1(L_{\infty,w}, E)) = h(E(L_{\infty,w})_{p^\infty}) = \begin{cases} -2 & E(L_{\infty,w}) \supset E_p,\ w \text{ で good,} \\ -1 & w \text{ で split multiplicative,} \\ 0 & \text{その他.} \end{cases} \tag{9.5}$$

9.3.3. *local part II.* まず v を 任意の有限素点とする. ここでも L_∞/K_∞ で不分解のときのみ考える. G は p 群ゆえ, $H^i(G, H^1(L_{\infty,w}, E)_{p^\infty}) = H^i(G, H^1(L_{\infty,w}, E))$ に注意する. 定理 9.1, 9.3 と Hochschild-Serre により,

$$H^i(G, H^1(L_{\infty,w}, E)) \cong H^i(G, E(L_{\infty,w}))\ (i = 1, 2) \tag{9.6}$$

となる. 次の補題は証明を略すが [CoGr] Th'm 3.1 が key となる.

Lemma 9.3. $v|p$ のとき $H^i(G, E(L_{\infty,w}))$ は有限. 更に $h(E(L_{\infty,w})) = 0$.

Rem . $v \nmid p$ なら, (9.3), (9.4), (9.6) により

$$H^1(G, E(L_{\infty,w})) \cong H^1(G, E(L_{\infty,w})_{p^\infty}).$$

よってこれは §9.3.2 により有限集合である.

9.4. まとめ. Lemma 9.2, 式 (9.5), Lemma 9.3 と, L_∞/K_∞ で分岐する素点は不分解であることから, 次が分かる.

$$\begin{aligned} h(\mathrm{Sel}_{p^\infty}(E/L_\infty)) &= -\sum_{v\in S(K_\infty),L_\infty\text{で分岐}} h(H^1(L_{\infty,w},E)) \\ &= 2\#\{w\in S(L_\infty):\ w\nmid p, L_\infty/K_\infty\text{で分岐, good, } E(L_{\infty,w})\supset E_p\} \\ &\quad +\#\{w\in S(L_\infty):\ L_\infty/K_\infty\text{で分岐, split mult.}\}. \end{aligned}$$

分岐指数は p だから (9.2) で $M=\mathrm{Sel}_{p^\infty}(E/L_\infty)$ としたものに Cor. 9.1 と上式を代入すれば, 定理 8.1 の式を得る.

10. Some Remarks

Rem . $E(K)_p=0$ であるとする. このときには, $\mathrm{Sel}_{p^\infty}(E/L_\infty)$ は 定理の条件の下 $\mathbb{Z}_p$-cofree となることを示すことができる. 故に (9.1) は同型にとることができる. 更に (9.1) の $\alpha=0$ を示すことができ, $\mathbb{Z}_p[G]$-module としての構造も決定することができる.

Rem . より一般の p 進表現に対しても, Greenberg の Selmer 群 ([Gre] p. 98) を使って §9.2 と同様の議論を考えることができる. しかし §9.3 の local な計算にあたるところは一般に計算が困難であり, 定理 8.1 のような形で公式を得ることはいまのところ出来ていない. ただ, もともとの木田の公式 (定理 1.1) はこの方法で示すことが出来る. 詳細はここでは省略する.

Rem . なお, CM 楕円曲線 の岩澤理論という, CM 楕円曲線に対する本稿で考えた岩澤理論とは別の岩澤理論の枠組があって, それに対する木田の公式が [Win], [Mi] では Selmer 群, [Ai] では p 進 L 関数に対して得られている. しかし, この枠組は考えている Selmer 群や $\mathbb{Z}_p$-拡大が今回のものと全く別のものであり, CM 楕円曲線に限っても今回の結果とは直接結びつかないことを指摘しておく. (証明法も異なる.)

References

[Ai] Aiba, A.: *"On p-adic L-functions attached to elliptic curves with complex multiplication and the Riemann-Hurwitz genus formula"*, Bull. Fac. Sci. Ibaraki Univ. **22** (1990), 23–28.

[CoGr] Coates, J. and Greenberg, R.: *"Kummer theory for abelian varieties over local fields"*, Invent. Math. **124** (1996), 129–174.

[DFKS] Dummit, D., Ford, D., Kisilevsky, H., and Sands, J.: *"Computation of Iwasawa Lambda Invariants for Imaginary Quadratic Fields"*, J. Number theory **37** (1991), 100–121.

[Gre] Greenberg, R: *"Iwasawa theory for p-adic representations"*, Adv. Studies in Pure Math. **17** (1989), 97–137.

[Hab] Haberland, K.: *"Galois cohomology of algebraic number fields"*, VEB, Deutsher Verlag der Wiss., Berlin, (1978).

[HM] Hachimori, Y. and Matsuno, K.: *"An analogue of Kida's formula for the Selmer groups of elliptic curves"*, in preparation.

[Im] Imai, H.: *"A note on the rational points of abelian varieties with values in cyclotomic $\mathbb{Z}_p$-extensions"*, Proc. Japan Acad. **51** (1975),12–16.

[Iw1] 岩澤 健吉: "代数体と関数体のある類似について", 数学 **15** (1963),65–67.

[Iw2] Iwasawa, K.: *"Riemann-Hurwitz formula and p-adic Galois representations for number fields"*, Tohoku Math. J. **33** (1981),263–288.

[Ki] Kida, Y.: *"l-extensions of CM-fields and cyclotomic invariants"*, J. Number Theory **12** (1980), 519–528.

[Kna] Knapp, A. W.: *"Elliptic curves"*, Math. Notes 40, Princeton Univ. Press (1992).

[Ku] 栗原 将人: "岩澤理論の一般化についての概説", R.I.M.S. 講究録 **925** (1995), 53–65.

[Man1] Manin, J. I.: *"Cyclotomic Fields and Modular Curves"*, Russian Math. surveys **26** (1971), 7–78.

[Man2] Manin, J. I.: *"Parabolic Points and Zeta Functions of Modular Elliptic Curves"*, Math. USSR-Izv. **6** (1972), 19–64.

[Mat] 松野 一夫: "楕円曲線の岩澤理論における木田の公式について", 東大修論 (1997).

[Maz] Mazur, B.: *"Rational Points of Abelian Varieties with Values in Towers of Number Fields"*, Invent. Math. **18** (1972), 183–266.

[Mi] Michel, A: *"Une formule de Riemann-Hurwitz pour le groupe de Selmer d'une courbe elliptique"*, Ann. Inst. Fourier Grenoble **43** (1993), 57–84.

[M-SD] Mazur, B. and Swinnerton-Dyer, P.: *"Arithmetic of Weil Curves"*, Invent. Math. **25** (1974), 1–61.

[Pe] Perrin-Riou, B.: *"Théorie d'Iwasawa et hauteurs p-adiques (cas des variétés abéliennes)"*, Séminaire de Théorie des Nombres, Paris 1990/91, Birkhäuser. (1993), 203-222.

[Ro] Rohrlich, D.: *"On L-functions of elliptic curves and cyclotomic towers"*, Invent. Math. **75** (1984), 409–423.

[Se] Serre, J.-P.: *"Cohomologie Galoisienne"*, L.M.N. 5, Springer (1973).

[Si] Sinnott, W.: *"On p-adic L-functions and the Riemann-Hurwitz genus formula"*, Compositio Math.**53** (1984), 3–17.

[St1] Stevens, G.: *"Arithmetic on Modular Curves"*, Progr. in Math.**20** Birkhäuser (1982).

[St2] Stevens, G.: *"Stickelberger elements and modular parametrizations of elliptic curves"*, Invent. Math. **98** (1989), 75–106.

[Wa] Washignton, L. C.: *"Introduction to Cyclotomic Fields"* 2nd ed., G.T.M. no.83, Springer, New York (1997).

[Wil] Wiles, A: *"The Iwasawa conjecture for totally real fields"*, Ann. of Math. **131** (1990), 493–540.

[Win] Wingberg, K: *"A Riemann-Hurwitz formula for the Selmer group of an elliptic curve with complex multiplication"*, Comment. Math. Helvetici **63** (1988), 587–592.