1/7

情性的素数における反円分 $\mathbb{Z}_p$-拡大上の plus/minus Selmer 群の非自明な指数有限 Λ-部分加群について (椎井亮太 / 九州大)

Contents

§1. BSD conj.

F : a number field (i.e. $F/\mathbb{Q}$: fin. ext.)

E : ellipic curve / F, $y^2 = x^3 + ax + b$ $(a, b \in F,\ 4a^3 - 27b^2 \neq 0)$

$E(F) := \{ (x, y) \in F^2 \mid y^2 = x^3 + ax + b \} \cup \{\infty\}$

$\rightsquigarrow$ $E(F)$ は アーベル群.

Theorem [Mordell-Weil]

$E(F)$ は 有限生成アーベル群 である. よって,

$$E(F) \simeq \mathbb{Z}^{\oplus r} \oplus E(F)_{tor}.$$

rank of E/F.

//

Hasse-Weil L-func. が E/F 上でも定義され, これは $L(E/F, s)$ が hol. on $\mathbb{C}$ であることが予想されている.

Conjecture [BSD]

① $r = \mathrm{ord}_{s=1} L(E/F, s)$

② Tate-Shafarevich 群 $Ш(E/F)$ は有限群であって,

ideal class gp の類似

$$\underbrace{\frac{L^{(r)}(E/F, 1)}{r!\ \Omega_{E/F} \mathrm{Reg}(E/F)}}_{\text{leading term}} = \sqrt{|\Delta_F|}\, \frac{\# Ш(E/F)}{(\# E(F)_{tor})^2} \prod c_v(E/F)$$

2. A brief of Iwasawa theory.

p: (odd) prime で固定する.

Purpose : The relation between arithmetic objects ($E(F)$, Selmer group) & analytic objects (L - func.) p-adically.

$x \in \mathbb{Q}^*$ を $x = p^r \frac{n}{m}$ ($r, m, n \in \mathbb{Z}$, $m \neq 0$, (p, m, n) は互いに素) で表示する.
このとき,

$$|x|_p := p^{-r}, \quad |0|_p := 0$$

と定める.

$\rightsquigarrow$ $d_p(x, y) := |x - y|_p$ は $\mathbb{Q}$ 上の距離となる.

特に, $d_p(x, y) \leq \max\{d_p(x, z), d_p(z, y)\}$ が成り立つ.

Definition

$\mathbb{Q}$ の $d_p(-,-)$ による完備化を $\mathbb{Q}_p$ とかいて, p進数体という.
これは, explicitには

$$\mathbb{Q}_p := \left\{ \sum_{n \gg -\infty} a_n p^n \;\middle|\; a_n \in \{0, 1, 2, \cdots, p-1\} \right\}.$$

また, $\mathbb{Z}_p := \left\{ \sum_{n=0}^{\infty} a_n p^n \in \mathbb{Q}_p \right\}$ を p進整数環という.

$\rightsquigarrow$ $\mathbb{Z}_p$, $\mathbb{Q}_p$ は様々な重要な性質をもつ.

Hensel's Lemma

$f(X) \in \mathbb{Z}[X]$ として, $a_0 \in \mathbb{Z}$ が $f(a_0) \equiv 0 \pmod p$ で $f'(a_0) \not\equiv 0 \pmod p$ となるようなものがあるとすれば,

$$\exists\, a \in \mathbb{Z}_p \text{ (s.t.) } f(a) = 0 \;\&\; a \equiv a_0 \pmod p.$$

e.g.

$a \in \mathbb{Z} \setminus \{0\}$, $x \in \mathbb{Z}$ with $x^2 \equiv a \pmod p$ $\Rightarrow$ $\sqrt{a} \in \mathbb{Z}_p$.

$f(X) = X^2 - a$ を考えて, Hensel の補題を使う.

$p = 5$, $a = -1$,
$\rightsquigarrow$ $x = 2$ が満たされる.
$\therefore$ $\sqrt{-1} \in \mathbb{Z}_5$.

Philosophy of Iwasawa theory

Consider a family of some objects, not each.

Definition

F_∞/F が $\mathbb{Z}_p$-extension $\overset{\text{def}}{\Longleftrightarrow}$ F_∞/F は (infinite) ガロア拡大 & $\mathrm{Gal}(F_\infty/F) \simeq \mathbb{Z}_p$.
(as Abelian groups)

$$\begin{array}{ccccccccc} \mathbb{Z}_p & \supset & p\mathbb{Z}_p & \supset & p^2\mathbb{Z}_p & \supset & \cdots & \supset & \{0\} \\ | & & | & & | & & & & | \\ F = F_0 & \subset & F_1 & \subset & F_2 & \subset & \cdots & \subset & F_\infty \end{array}$$

$\rightsquigarrow \mathrm{Gal}(F_n/F) \simeq \mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}$.

e.g.

$\mathbb{Q}(\mu_{p^\infty}) := \bigcup_n \mathbb{Q}(\mu_{p^n})$ (ここで, μ_{p^n} は単位元 1 の p^n 根からなる群)

$\rightsquigarrow \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \simeq \mathbb{Z}_p^\times \simeq (\mathbb{Z}/p\mathbb{Z})^\times \times \underbrace{(1+p\mathbb{Z}_p)}_{\simeq \mathbb{Z}_p}$

$\mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}) \simeq (\mathbb{Z}/p^n\mathbb{Z})^\times$

Hensel's Lemma ($f(x) = X^{p-1} - 1$)

(i) $\mathbb{Q}_\infty \subset \mathbb{Q}(\mu_{p^\infty})$: the subfield (s.t.) $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \simeq \mathbb{Z}_p$.

the cyclotomic $\mathbb{Z}_p$-ext. / $\mathbb{Q}$.

$F_\infty := F \cdot \mathbb{Q}_\infty$: the cyclotomic $\mathbb{Z}_p$-ext. / F. //

$\Lambda := \mathbb{Z}_p[[T]]$ として, M を コンパクトな $\mathbb{Z}_p$-mod で $\mathrm{Gal}(F_\infty/F) \curvearrowright M$: conti とする.

$\rightsquigarrow$ M は Λ-module の構造をもつ.

Theorem [str. theorem]

M: fin. gen. (cpt.) Λ-module. このとき完全列

$$0 \to (\text{fin.gp.}) \to M \xrightarrow{\varphi} \Lambda^{\oplus r} \oplus \left(\bigoplus_{i=1}^{s} \Lambda/(f_i) \right) \to (\text{fin.group}) \to 0 \quad : \text{exact as } \Lambda\text{-mod.}$$

を得る.

□ Selmer group

number field F に対して,

$$0 \to E(F) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to {}^{\exists}\mathrm{Sel}_p(E/F) \to Ш(E/F)[p^\infty] \to 0 \ : \text{exact.}$$

$G_F := \mathrm{Gal}(\overline{F}/F)$ ↻ $\mathrm{Sel}_p(E/F)$

$(p^\infty\text{-})$ Selmer group $/F$

For a $\mathbb{Z}_p$-ext F_∞/F に対して

$$\mathrm{Sel}_p(E/F_\infty) := \varinjlim_n \mathrm{Sel}_p(E/F_n)$$

↻ $\mathrm{Gal}(F_\infty/F)$

$\rightsquigarrow \mathrm{Sel}_p(E/F_\infty) \in \mathrm{Mod}\,\Lambda$.

M: top. Abel. gp とする. $M^\vee := \mathrm{Hom}_{\text{conti}}(M, \mathbb{Q}_p/\mathbb{Z}_p)$ を Pontryagin dual と呼ぶ.

"discrete" $\longleftrightarrow$ "cpt." "Submod of order n" $\longleftrightarrow$ "Submod with index n"

$(\mathbb{Q}_p/\mathbb{Z}_p)^{\oplus r} \longleftrightarrow \mathbb{Z}_p^{\oplus r}$

$\rightsquigarrow \mathrm{Sel}_p(E/F_\infty)^\vee$ は有限生成 (cpt.) Λ-mod となる.

str. thm. $\rightsquigarrow$

$$0 \to (\text{fin. gp.}) \to \mathrm{Sel}_p(E/F_\infty)^\vee \to \Lambda^{\oplus r} \oplus \left(\bigoplus_{i:\text{fin}} \Lambda/(f_i) \right) \to (\text{fin.gp.}) \to 0.$$

r: (Λ-corank of $\mathrm{Sel}_p(E/F_\infty)$)

$r=0$ のとき, $\mathrm{Sel}_p(E/F_\infty)$ を Λ-cotorsion と呼ぶ.
また, $\left(\prod_i f_i(T)\right) \in$ ideal Λ を characteristic ideal と呼ぶ.

Theorem [Greenberg '97]

E/F が good ordinary at $\forall \mathfrak{p} | p$ of F. であり, F_∞/F が cyclic $\mathbb{Z}_p$-ext とする.

もし, $\mathrm{Sel}_p(E/F_\infty)$ が Λ-cotorsion なら $\mathrm{Sel}_p(E/F_\infty)$ は

有限指数の非自明な $\mathrm{Sel}_p(E/F_\infty)$ の Λ-submod は存在しない.

Corollary

先の仮定において, $\#\mathrm{Sel}_p(E/F) < \infty$ ならば, $\mathrm{Sel}_p(E/F_\infty)$ は Λ-cotorsion であって,

更に f_E が characteristic ideal of $\mathrm{Sel}_p(E/F_\infty)$ が生成元のとき

$$f_E(0) \sim \left(\prod_{\mathfrak{p}|p} \#\hat{E}(\mathbb{F}_\mathfrak{p}) \right) \cdot \frac{\#\mathrm{Sel}_p(E/F_\infty)}{(\# E(F)_{\mathrm{tor}})^2} \prod_{v \nmid \infty} C_v(E/F)$$

up to $\mathbb{Z}_p$-unit.

(もし, 岩澤の Main conj が成り立っていたら….)

$\rightsquigarrow$ $f_E(0) \overset{\mathrm{IMC}}{\sim}$ the const. term of p-adic L-func. of E.

$\shortparallel$

$L(E/F, 1)$

$\rightsquigarrow$ "p-part" of BSD-conj. が成り立つ. //

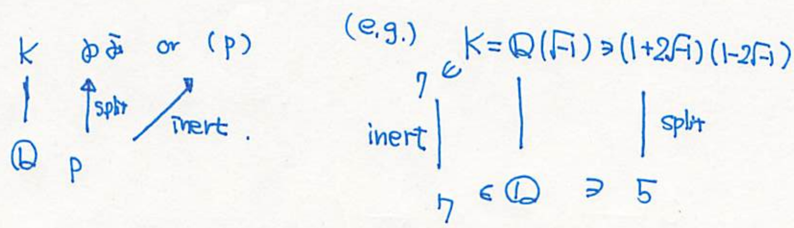
K : 虚2次体.

Situation

① K_∞/K : 反円分 $\mathbb{Z}_p$-拡大.

② p is inert in $K/\mathbb{Q}$.

③ E : super singular red. at p.



<u>Theorem</u>

- $p \geq 5$: prime
- K : img. quad. field (s.t.) p : inert in $K/\mathbb{Q}$
  $p \nmid h_K$
- K_∞/K : anti-cyclotomic $\mathbb{Z}_p$-ext.
- F/K : fin. ext. (s.t.) $\begin{cases} p : \text{splits completely in } F/K \\ p \nmid [F:K] \end{cases}$
- $F_\infty := F \cdot K_\infty$
- E/F : ellipic curve with good supersingulan at $^\forall \mathfrak{p} | p$ of F
  & $\hat{E} \simeq_{/\mathcal{O}_\mathfrak{p}}$ the L-T formal gp. with ht $= 2$ & parameter $-p$

このとき,

$\mathrm{Sel}_p^\pm(E/F_\infty)$: Λ-cotorsion

$\Rightarrow$ $\mathrm{Sel}_p^\pm(E/F_\infty)$ has no non-trivial Λ-submodule / finite index.

先に $\# \mathrm{Sel}_p(E/F) < \infty$ ならば,

① $\mathrm{Sel}_p^\pm(E/F_\infty)$ は Λ-cotorsion,

② $f_E^\pm$ が $\mathrm{Sel}_p^\pm(E/F_\infty)$ の character ideal の生成元ならば

$$f_E^\pm(0) \underset{\substack{\uparrow \\ \text{up to } \mathbb{Z}_p\text{-unit.}}}{\sim} \# \mathrm{Sel}_p(E/F) \cdot \prod_{v \nmid \infty} C_v(E/F)$$

//