数理解析研究所講究録 1451 巻 2005 年 199-206

Ramification of p-power torsions of an elliptic curve over a local field

東大数理　服部 新 (Shin HATTORI)
Department of Mathematical Sciences, University of Tokyo
shin-h@ms.u-tokyo.ac.jp

1 Introduction

K を完備離散付値体とする. K の剰余体 k が完全なとき, $G_K = \mathrm{Gal}(\bar{K}/K)$ の torsion な表現 ρ に対して ρ の導手 $f(\rho)$ が $f(\rho) = 1 + \sup(u \in \mathbb{Q}_{>0} \mid \rho(G_K^u) = 1)$ で定義される (ただし G_K^u は上付き分岐群). 一方 $\mathcal{O}_K$ 上の有限平坦群スキーム $\mathcal{G}$ に対しては $\mathcal{G}$ の導手 $c(\mathcal{G})$ と呼ばれる量が定義され, $\mathcal{G}$ の generic fiber が定めるガロア表現を $\rho_{\mathcal{G}}$ と書くと, $f(\rho_{\mathcal{G}}) \leq c(\mathcal{G})$ が成り立つ. 本稿の目的は $c(\mathcal{G})$ の上界を与えることによりこのようなガロア表現の導手をおさえることである. これに関連して $\mathcal{G}(\bar{K})$ と $\mathcal{G} \bmod \pi$-巾との関係についても述べる.

この研究に対し発表の機会を与えて頂いたことを心から感謝いたします.

2 有限平坦群スキームの導手

K を完備離散付値体, π を K の素元, e を K の絶対分岐指数, v を K の加法的付値で $v(\pi) = 1$ なものを K の分離閉包に自然に拡張したもの, とする. 一般に, A を $\mathcal{O}_K$ 上の有限平坦代数とするとき, $j \in \mathbb{Q}_{>0}$ に対して有限 G_K-加群 $F^j(A)$ が次のように定義される ([2]).

全射 $\rho : \mathcal{O}_K[T_1, \ldots, T_d] \to A$ を固定し, その核を I とする. $j = l/k$ と書くとき, K-algebra

$$A_K(\rho, k, l, A) = K \otimes_{\mathcal{O}_K} (\mathcal{O}_K[T_1, \ldots, T_d][I^k/\pi^l])^{\wedge}$$

(ただし $\wedge$ は π-進完備化) は K-affinoid algebra ([4]) になる. これが定める K-affinoid variety $X = X_K(\rho, l, k, A)$ の幾何学的連結成分 $\pi_0(X_{\bar{K}}) = \varprojlim_{K'/K:\text{有限次分離}} \pi_0(X \times_K K')$ を $F^j(A)$ とおく.

これは全射 $\mathcal{O}_K[T_1, \ldots, T_d] \to A$ や k, l のとりかたによらず A と j のみで定まる有限 G_K-加群になる. さらに $A \mapsto F^j(A)$ は関手

$$F^j : (\mathcal{O}_K \text{ 上の有限平坦代数の圏}) \to (\text{有限 } G_K\text{-加群の圏})$$

を定める.

また例えば $I = (f_1, \ldots, f_r)$ ならば, $X = \{z \in m_{\bar{K}} | v(f_1(z)) \geq j, \ldots v(f_r(z)) \geq j\}$. 従って $F(A) = \mathrm{Hom}_{\mathcal{O}_K - alg.}(A, \bar{K}) = \{z \in \bar{K} \mid f_1(z) = \ldots = f_r(z) = 0\}$ から $F^j(A)$ に自然な G_K-equivariant map があるが,

A が $\mathcal{O}_K$ 上 relative complete intersection なら $F(A) \to F^j(A)$ は全射 ([2, Proposition 6.2]).

とくに $\mathcal{G} = \mathrm{Spec}(A)$ が generic fiber が etale な $\mathcal{O}_K$ 上の有限平坦群スキームなら, geometric closed fiber が $\bar{k}[T_1, \ldots, T_r]/(T_1^{p^{n_1}}, \ldots, T_r^{p^{n_r}})$ という形をしているから, 自動的に relative complete intersection になり, 全射性が成立する. またこのときは関手性より $F^j(\mathcal{G})$ はG_K-加群の構造を持ち, $F(\mathcal{G}) = \mathcal{G}(\bar{K}) \to F^j(\mathcal{G})$ は G_K-加群の全射になることもわかる.

A の導手 $c(A) = c(\mathrm{Spec}(A))$ は,

$$c(A) = \inf(j \in \mathbb{Q}_{>0} \mid F(A) \simeq F^j(A))$$

で定義される量 ([2, Proposition 6.4]).

導手 $c(A)$ は A が monogenic なときには簡単に計算することができる.

$A = \mathcal{O}_K[T]/(f(T))$ を $\mathcal{O}_K$ 上の有限平坦 monogenic な代数で, $A \otimes_{\mathcal{O}_K} K$ が separable なものとする. $z_1, \ldots, z_d$ を $f(T)$ の根とするとき, 次のことを仮定する.

- $f(T + z_i)$ の Newton polygon は i によらない. (この polygon を P とおく)

この仮定は A が K の有限次分離拡大の整数環のときに, また $\mathrm{Spec}(A)$ が群スキームになるときにも満たされる. 後者の場合, zero section を $T = 0$ ととっておけば, P は $f(T)$ の Newton polygon になる.

さてこのとき, P の頂点を $(d_1, f_1), (d_2, f_2), \ldots, (d_{r-1}, f_{r-1}), (d_r, f_r)$, ただし $1 = d_1 < d_2 < \ldots < d_r = d$, $f_1 > f_2 > \ldots > f_r = 0$ とする. P の

m-番目の辺の傾きの絶対値を $s_m = (f_m - f_{m+1})/(d_{m+1} - d_m)$, y-切片を $t_m = d_{m+1}s_m + f_{m+1}$ とおく. 次に, $s > 0$ に対して $F(A)$ 上の同値関係 $\sim_s$ を,

$$z \sim_s w \Leftrightarrow v(z-w) \geq s$$

で定義する. 最後に P の Herbrand 関数 $\varphi_P(s)$ を,

$$\varphi_P(s) = (Y = -sX + t \text{ が } P \text{ と交わるような } t \text{ の inf})$$

で定める. このとき,

Theorem 1. $F^{\varphi_P(s)}(A) = F(A)/\sim_s$. つまり, $t_m < a \leq t_{m-1} \Rightarrow F^a(A) = F(A)/\sim_{s_{m-1}}$. とくに $c(A) = s_1 + f_1 = \sup_{j\neq i} v(z_j - z_i) + \sum_{j\neq i} v(z_j - z_i)$.

さらに, $\mathcal{G} = \mathrm{Spec}(A)$ が群スキームのときはこの関係を上付き分岐群と下付き分岐群の対応と類似した形で書くことができる. つまり,

$$\mathcal{G}_s(\bar{K}) = \{z \in \mathcal{G}(\bar{K}) \mid v(z) \geq s\},$$

$$\mathcal{G}^t(\bar{K}) = \mathrm{Ker}(F(\mathcal{G}) = \mathcal{G}(\bar{K}) \to F^t(\mathcal{G})),$$

$\mathcal{G}_s$ や $\mathcal{G}^t$ をこれらの $\mathcal{G}$ のなかでの schematic closure,

とすると, $\mathcal{G}^{\varphi_P(s)} = \mathcal{G}_s$.

例.

- $c(\mu_{p^n}) = ne + e/(p-1)$.
- $c(\mathcal{G}(r)) = pr/(p-1)$, ただし $\mathcal{G}(r)$ は $T^p = \pi^r T$ で定義される Raynaud $\mathbb{F}_p$-スキーム ([7]).
- $c(\mathcal{G}(r_1, r_2)) = p(r_1 + pr_2)/(p^2-1)$, ただし $\mathcal{G}(r_1, r_2), r_1 \leq r_2$, は ${T_1}^p = \pi^{r_1}T_2, {T_2}^p = \pi^{r_2}T_1$ で定義される Raynaud $\mathbb{F}_{p^2}$-スキーム.

Remark 2. K' を K の完備離散付値体としての拡大, $e(K'/K)$ を分岐指数とするとき, $c(A \otimes_{\mathcal{O}_K} \mathcal{O}_{K'}) = e(K'/K)c(A)$ が成り立つ.

Remark 3. K の剰余体 k が完全とは限らないときにも, 上付き分岐群 G_K^j が,

K 上の etale algebra L に対し $j > c(\mathcal{O}_L) \Leftrightarrow G_K^j$ が $\mathrm{Hom}_{K-alg.}(L, \bar{K})$ に trivial に作用,

という条件で定義され, k が完全なときは古典的な上付き分岐群 $G_{K,cl}^j$ を 1 ずらしたもの $G_{K,cl}^{(j)} = G_{K,cl}^{j-1}$ と一致する ([2, Definition 3.4]).

また A が $\mathcal{O}_K$ 上 relative complete intersection のとき, B を A の $A \otimes_{\mathcal{O}_K} K$ のなかでの整閉包とすると, 図式

$$\begin{array}{ccc} F(B) & \longrightarrow & F^j(B) \\ \| & & \downarrow \\ F(A) & \longrightarrow & F^j(A) \end{array}$$

が可換なので縦の矢印も全射であり,

$$j > c(A) \Rightarrow G_K^j \text{ が } F(A) \text{ に自明に作用},$$

が成り立つ.

したがって, $c(\mathcal{G})$ を押さえることにより, $\mathcal{O}_K$ 上の有限平坦群スキームにのびるガロア表現の導手を押さえることができる. 有限平坦群スキームの導手は係数拡大と可換なので, 都合のよい体まで base change することによって上界が容易に求まる. これは Fontaine の結果 ([6]) の別証明と剰余体が非完全の場合への一般化を与えている.

Theorem 4. K を混標数 $(0, p)$ の完備離散付値体, $\mathcal{G}$ を $\mathcal{O}_K$ 上の有限平坦群スキームで p^n で消えるもの, とするとき,

$$c(\mathcal{G}) \leq ne + e/(p-1)$$

が成り立つ. とくに $j > ne + e/(p-1)$ なら上付き分岐群 G_K^j は $\mathcal{G}(\bar{K})$ に自明に作用.

Proof. 両辺は係数拡大で分岐指数倍されるだけだから, K をとりかえて, G_K が $\mathcal{G}(\bar{K})$ に自明に作用かつ $\zeta_{p^n} \in K$, としてもよい. このとき $\mathcal{G}$ の minimal prolongation $\mathcal{M}$ は μ_{p^m}, $m \leq n$, の直和であり, 図式

$$\begin{array}{ccc} F(\mathcal{G}) & \longrightarrow & F^j(\mathcal{G}) \\ \| & & \downarrow \\ F(\mathcal{M}) & \longrightarrow & F^j(\mathcal{M}) \end{array}$$

が可換だから縦の矢印も全射であり, $c(\mathcal{G}) \leq c(\mathcal{M}) \leq ne + e/(p-1)$ となる.

□

古典的な分岐理論というのは, 法π-巾の世界から generic fiber の情報を取り出す, といった意味を持っていたが, われわれの導手 $c(A)$ もそのようなものと解釈することができる. $F^j(A)$ の定義をよくみてみると, j が整数でべつの整数 N よりも小さいならば, $F^j(A)$ は $I + \pi^N$ にしかよらないことがわかる. つまり I として ρ のかわりに全射 $\mathcal{O}_K[T_1, \ldots, T_d] \to A/\pi^N$ の核を取ってもよい. したがってこのとき,

$$F^j(A) \text{ は } A/\pi^N \text{ にしかよらない.}$$

(このことは一般の $j \in \mathbb{Q}_{>0}$ でも成り立つことが示せる.) とくに, $N > c(A)$ となる整数 N をとれば,

$$F(A) \text{ は } A/\pi^N \text{ にしかよらない}$$

ことがわかる. さらに $\mathcal{G} = \mathrm{Spec}(A)$ が $\mathcal{O}_K$ 上の有限平坦群スキームのときは,

$$\text{有限 } G_K\text{-加群 } \mathcal{G}(\bar{K}) \text{ は群スキーム } \mathcal{G} \bmod \pi^N \text{ にしかよらない}$$

ことが示せる.

Remark 5. $\mathcal{G}$ と $\mathcal{G}'$ を, n-truncated Barsotti-Tate 群で, $\mathcal{O}_K$ 上の $(n+1)$-truncated Barsotti-Tate 群の p^n-torsion として書けるもの, とする. このとき,

$$\mathcal{G} \simeq \mathcal{G}' \bmod p^{n+1} \Leftrightarrow \mathcal{G} \simeq \mathcal{G}'$$

が成り立つ. 証明には Brueil 加群 ([5]) を使う. つまりこの場合 $N = e(n+1)$ ととってしまえばいいが, これは $ne + e/(p-1)$ よりも大きい値だから, generic fiber の同型を与えるためにはわれわれの $c(\mathcal{G})$ で十分. また場合によっては $c(\mathcal{G})$ よりもかなり小さな法π-巾で generic fiber が決まってしまうこともあるが, 逆に $c(\mathcal{G})$ が sharp な場合もある. これらについては後述.

3 例：楕円曲線の場合

K を混標数 $(0,p)$ の完備離散付値体とします. E を $\mathcal{O}_K$ 上の楕円曲線, $[p](X) = px + \ldots + c_p X^p + \ldots$ を E の原点での formal completion の p 倍公式, $f = v(c_p)$ とおくと, $E[p^n]$ の導手は次のように $E[p]$ にしかよらない形で計算できる.

Theorem 6.

$$c(E[p^n]) = \begin{cases} ne + (e-f)/(p-1) & if\, f < pe/(p+1), \\ ne + e/(p^2-1) & if\, f \geq pe/(p+1). \end{cases}$$

Proof. $f = 0$(E が ordinary) の場合は, K を有限次拡大すると $E[p^n]$ はスキームとして μ_{p^n} の disjoint union になるので $c(E[p^n]) = c(\mu_{p^n}) = ne + e/(p-1)$. $f > 0$(E が supersingular) の場合は $E[p^n]$ が monogenic なので定理 1 より $c(E[p^n]) = ne + s$, ただし $s = sup_{z \neq 0 \in E[p^n](\bar{K})} v(z)$. 下付き分岐群 $E[p^n]_s$ は p-群だから位数 p の元を含み, $s = sup_{z \neq 0 \in E[p](\bar{K})} v(z)$ でもあるから, $f < pe/(p+1)$ ならば $s = (e-f)/(p-1)$, $f \geq pe/(p+1)$ ならば $s = e/(p^2-1)$ になるのは $[p](X)$ の Newton polygon からわかる. □

例.

- $K = \mathbb{Q}_5(5^{1/20})$, $E : y^2 = x^3 + \pi_K x + 1$, $E' : y^2 = x^3 + \pi_K(1 + 5\pi_K^5)x + 1$, とすると $c(E[5]) = 24.25$ であり, $E[5](\bar{K}) \simeq E'[5](\bar{K})$.
- $K = \mathbb{Q}_5(5^{1/20})$, $E : y^2 = x^3 + \pi_K^{11} x + 1$, $E' : y^2 = x^3 + \pi_K^{11}(1 + 5\pi_K^3)x + 1$, とすると $c(E[5]) = 22.75$ であり, $E[5](\bar{K}) \simeq E'[5](\bar{K})$. このときは $\mathcal{O}_K$ 上の群スキームとしても $E[5] \simeq E'[5]$.
- $K = \mathbb{Q}_5(5^{1/6})$, $E : y^2 = x^3 + \pi_K x + 1$, $E' : y^2 = x^3 + \pi_K(1 + 5\pi_K^2)x + 1$, とすると $c(E[5]) = 7.25$, $E[5](\bar{K}) \simeq E'[5](\bar{K})$. このときも $\mathcal{O}_K$ 上の群スキームとしても $E[5] \simeq E'[5]$.

また $\mathcal{G}^{j+} = \cup_{j'>j} \mathcal{G}^{j'}$ とおくと次のことが成り立つ.

Theorem 7. $f < p^2 e/p^n(p+1)$ のとき, $E[p^n]^{pe/p^n(p-1)+}$ は $\mathbb{Z}/p^n$ 上階数 1 の自由部分群スキーム. $n = 1$ のときは *canonical subgroup* と一致.

最後に, $\mathcal{G}$ の generic fiber を決める法 π-巾のなかで $c(\mathcal{G})$ が sharp なものかどうか, についての話をします. 簡単のために $K = K^{nr}$ とする.

$\mathcal{G}$ を $\mathbb{Z}/p^n$ の μ_{p^n} による $\mathcal{O}_K$ 上の有限平坦群スキームとしての extension とする.

$$\mathrm{Ext}_{\mathcal{O}_K-grp.}(\mathbb{Z}/p^n, \mu_{p^n}) = \mathcal{O}_K^{\times}/(\mathcal{O}_K^{\times})^{p^n}$$

であることから,

$$\text{すべてのこのような}\mathcal{G}\text{に対して}\mathcal{G}(\bar{K})\text{が}\mathcal{G}\bmod\pi^N\text{で決まる} \Leftrightarrow$$
$$N \geq ne + e/(p-1)$$

が従う. したがって, 導手の評価 $c(\mathcal{G}) \leq ne + e/(p-1)$ は ($\zeta_p \in K$ かどうかで1ずれるにせよ) 「ほとんど」 sharp であることがわかる (一方, $\mathcal{G}$ を supersingular reduction を持つ楕円曲線の p-torsion, に限ると, $f > e/2$ のときは $\bmod p$ がガロア表現を決めることが示せる).

参考文献

[1] A. Abbes and A. Mokrane, Sous-groupes canoniques et cycles évanescents p-adiques pour les variétés abéliennes, Publ. Math. IHES 99 (2004) 117-162.

[2] A. Abbes and T. Saito, Ramification of local fields with imperfect residue fields I, Amer. J. Math. 124 (2002) 879-920.

[3] A. Abbes and T. Saito, Ramification of local fields with imperfect residue fields II, Documenta Math. Extra volume: Kazuya Kato's Fiftieth Birthday (2003) 5-72.

[4] S. Bosch, U. Güntzer, R. Remmert, Non-Archimedean Analysis, A Series of Comprehensive Studies in Mathematics 261, Springer-Verlag (1984)

[5] C. Breuil, Groupes p-divisibles, groupes finis et modules filtrés, Ann. of Math. (2) 152 (2000) 489-549.

[6] J.-M. Fontaine, Il n'y a pas de variété abélienne sur $\mathbb{Z}$, Inv. Math. 81 (1985) no. 3 515-538.

[7] M. Raynaud, Schémas en groupes de type $(p, ..., p)$, Bull. Soc. Math. France 102 (1974) 241-280.

[8] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Inv. Math. 15 (1972) no.4 259-331.