

楕円曲線の Tate-Shafarevich 群の体拡大における挙動について

東北大学 大学院 理学研究科 数学専攻
志賀明日香 (Asuka Shiga) *

概要

Igor Shafarevich(1923-2017) は, 代数体 K 上の楕円曲線 E/K に対し, ガロアコホモロジーを用いて次のアーベル群を定義した.

$$\text{III}(E/K) \stackrel{\text{def}}{=} \ker \left\{ H^1(G_K, E) \rightarrow \prod_v H^1(G_{K_v}, E) \right\}$$

ただし K_v は K の素点 v における K の完備化であり, G_K, G_{K_v} はそれぞれ K, K_v の絶対ガロア群である. この群は今日では Tate-Shafarevich 群と呼ばれ, E の K 有理点全体のなす群 $E(K)$ の構造を決定する上で重要な役割を果たす. また, E/K の torsor における局所大域原理が成り立つことの障害になっているという点でも, 数論的に重要な群と見做されている.

本稿では, 1 導入 において Tate-Shafarevich 群の基礎的な事項について紹介するとともに, 2 主定理 において, 楕円曲線 E/K を固定し, L/K を動かしたときの $\text{III}(E/L)$ の挙動について本講演で話す予定の結果を述べる.

1 導入

本稿を通してキーワードになるのは局所と大域である. まずは局所大域原理について解説する.

定義 1.1. K を代数体とし, M_K を K の素点全体の集合とする. K_v を K の $v \in M_K$ における完備化とする. X/K を K 上定義された代数多様体とする.

X/K において局所大域原理が成り立つとは

$$X(K_v) \neq \emptyset, \forall v \in M_K \implies X(K) \neq \emptyset$$

が成り立つときのことをいう.

K は大域的な体と呼ばれる体の 1 つであり, K_v は局所的な体と呼ばれる体の一部である. 局所的な体たちで有理点を持てば, 大域的な体で有理点が存在するという理想的な状況が, 局所大域原理が成り立つということである. 次の例が古典的に知られている.

* otheio323.com@gmail.com

定理 1.2. (Hasse-Minkovski の定理) K を代数体とし, $a, b \in K^\times$ とする. $aX^2 + bY^2 = Z^2$ において局所大域原理が成り立つ.

上記は種数が 0 の場合であるが, 種数が 1 の場合は反例がある. 局所大域原理にどのような反例があるかという問題は, 古くから考えられてきた. 次の例 1. (3) のように, 最近になって見つかったものもある.

例 1.

(1) $3X^3 + 4Y^3 + 5Z^3 = 0$ はすべての素数 p に対する \mathbb{Q}_p および \mathbb{R} で解を持つが, \mathbb{Q} に解を持たない. (Selmer, 1961)

(2) $2y^2 = x^4 - 17$ はすべての素数 p に対する \mathbb{Q}_p および \mathbb{R} で解を持つが, \mathbb{Q} に解を持たない. (Lind, 1950)

(3) 任意の代数体 K に対して, ある $p, q \in K$ が存在して, $qy^2 = x^4 - p$ はすべての K の素点 v に対して K_v で解を持つが, K に解を持たない (Han Wu 2022)[10].

上記 3 つの反例は, 全て楕円曲線が関係している.

定義 1.3. K 上の楕円曲線 E とは, K 上の種数 1 の非特異射影代数曲線であって, 固定点 $O_E \in E(K)$ を持つもののことである.

例 2. $S : 3X^3 + 4Y^3 + 5Z^3 = 0$ は種数 1 の代数曲線であるが, $S(\mathbb{Q}) = \emptyset$ なので, \mathbb{Q} 上の楕円曲線ではないが, $\mathbb{Q}(\left(\frac{3}{4}\right)^{\frac{1}{3}})$ 上は楕円曲線である.

楕円曲線とガロアコホモロジーに関して, 本稿で必要な事項を述べる.

命題 1.4. K 上の楕円曲線は, $y^2 = x^3 + ax + b$ (ただし, $a, b \in K, 4a^3 + 27b^2 \neq 0$) の \mathbb{P}_K^2 における射影閉包, $\{y^2 = x^3 + ax + b\} \cup \{\infty \stackrel{\text{def}}{=} (0, 1, 0)\}$ と K 上で同型である.

定理 1.5. 楕円曲線 E/K を $\{(x, y) \mid y^2 = x^3 + ax + b\} \cup \{\infty\}$ とする. $P, Q \in E(K)$ に対して, P と Q を通る直線 L と E との第 3 交点を $R \in E(K)$ とする. $P + Q$ を ∞ と R を通る直線 L' と E との第 3 交点で与えれば, $E(K)$ は固定点 ∞ を単位元としてアーベル群をなす.

定理 1.6. (Mordel-Weil の定理, 証明は [9] を参照) K が代数体のとき, 群 $E(K)$ は有限生成なアーベル群である. よって,

$$E(K) \cong \mathbb{Z}^{\text{rank}(E/K)} \times E(K)_{\text{tor}}$$

($E(K)_{\text{tor}}$ は有限アーベル群) とかける. $\text{rank}(E/K)$ を E/K のランクという.

定義 1.7. E_1, E_2 をそれぞれ O_{E_1}, O_{E_2} を単位元とする楕円曲線とする. E_1 から E_2 への isogeny とは, 定数でない射 $\phi : E_1 \rightarrow E_2$ であって, $\phi(O_{E_1}) = O_{E_2}$ を満たすものをいう.

定義 1.8. G を群とし, M をアーベル群とする. M が G 加群であるとは, G が M に作用し, 作用の分配則が成り立つものをいう.

例 3. K を体とし, C/K を K 上の種数 1 の曲線とする. $C(\overline{K})$ は $\text{Gal}(\overline{K}/K)$ 上の加群である. 実際, $C(\overline{K})$ は固定点を単位元とするアーベル群をなし, $\text{Gal}(\overline{K}/K)$ の \overline{K} への作用を $x \mapsto \sigma x$ で表すことにすると, $\text{Gal}(\overline{K}/K) \times C(\overline{K}) \rightarrow C(\overline{K})$ を $(\sigma, (x, y)) \mapsto (\sigma x, \sigma y)$ で定めることができる.

定義 1.9. K を体, $G = \text{Gal}(\overline{K}/K)$ をその絶対ガロア群, M を G 上の加群とする. 今, M に G は連続に作用しているとする. ただし, M には離散位相, G には Krull 位相を入れている.

$$H^0(G, M) = M^G \stackrel{\text{def}}{=} \{m \in M \mid \forall \sigma \in G, \sigma m - m = 0\}$$

$$H^1(G, M) \stackrel{\text{def}}{=} Z^1(G, M)/B^1(G, M)$$

ただし,

$$Z^1(G, M) \stackrel{\text{def}}{=} \{f : G \rightarrow M : \text{連続写像} \mid f(\sigma\tau) = f(\sigma) + \sigma f(\tau), \forall \sigma, \tau \in G\}$$

$$B^1(G, M) \stackrel{\text{def}}{=} \{f : G \rightarrow M : \text{連続写像} \mid \exists m \in M, \forall \sigma \in G, f(\sigma) = \sigma m - m\}$$

とする.

$Z^1(G, M)$ の元を 1-コサイクル, $B^1(G, M)$ の元を 1-コバウンダリという. 1-コサイクル f に対して, コホモロジーにおける剰余類を $[f]$ と書くことにする.

定義 1.10. K を代数体とし, M_K を K の素点全体の集合とする. $v \in M_K$ に対し, K_v を K の v における完備化とする. G_L を K の絶対ガロア群とする.

$$\text{III}(E/K) \stackrel{\text{def}}{=} \ker \left\{ H^1(G_K, E(\overline{K})) \rightarrow \prod_{v \in M_K} H^1(G_{K_v}, E(\overline{K}_v)) \right\}$$

を楕円曲線 E/K の Tate-Shafarevich 群という. また, 正整数 n に対し, $\text{III}(E/K)[n] \stackrel{\text{def}}{=} \{[C] \in \text{III}(E/K) \mid n[C] = 0\}$ を Tate-Shafarevich 群 $\text{III}(E/K)$ の n -part という.

ガロアコホモロジーによる定義を見ているだけではよくわからないが, ガロアコホモロジーを torsor の集合と思うことで Tate-Shafarevich 群は幾何的な解釈を得る.

定義 1.11 (tosor). E/K を楕円曲線とする. E/K の torosor(トーサー, もしくは principle homogeneous space(主等質空間)) とは, 次をみたす組 (C, μ) のことである.

1. C/K は滑らかな曲線である.
2. $\mu : C \times E \rightarrow C$ は K 上定義されていて, 次をみたす.
 - (a) \overline{K} 上の同型 $\iota : C \rightarrow E$ が存在して, 次の図式を可換にする.

$$\begin{array}{ccc} C \times E & \xrightarrow{\mu} & C \\ \iota \times id \downarrow & & \downarrow \iota \\ E \times E & \xrightarrow{(P, Q) \mapsto P+Q} & E \end{array}$$

この図式から, μ は次の 3つの性質を満たすことに注意する.

- (b) 任意の C の点 p に対し, $\mu(p, O) = p$ が成り立つ.
- (c) 任意の C の点 p と任意の E の点 P, Q に対し, $\mu(\mu(p, P), Q) = \mu(p, P+Q)$ が成り立つ.
- (d) 任意の C の点 p, q に対し, $\mu(p, P) = q$ をみたす E の点 P が一意に存在する.

例 4. E/K 自身は E/K の torsor である. 実際, $\mu(p, P) = p + P$ と定めればよい.

定義 1.12 (Weil-Châtelet 群). E/K を楕円曲線とする.

E/K の torsor $(C/K, \mu), (C'/K, \mu')$ が同値であるとは, 次の図式を可換にする K 上の同型 $\theta: C \rightarrow C'$ が存在することをいう.

$$\begin{array}{ccc} C \times E & \xrightarrow{\mu} & C \\ \theta \times id \downarrow & & \downarrow \theta \\ C' \times E & \xrightarrow{\mu'} & C' \end{array}$$

E/K の torsor 全体の集合をこの同値関係で割ったものを E/K の Weil-Châtelet 群といい, $WC(E/K)$ と表す. また, E/K を含む同値類を自明類という.

命題 1.13. E/K を楕円曲線とする. E/K の torsor $(C/K, \mu)$ が自明類に含まれることは, C が K -有理点をもつことと同値である.

Proof.

torsor C/K が自明類に含まれるとき, ある K 上の同型 $\theta: E \cong C$ が存在する. $\theta(O) \in C(K)$ となり, C は K 有理点を持つ.

逆に, $C(K) \neq \emptyset$ のとき, $(C/K, \mu)$ が自明類に含まれることを示そう. $P \in C(K)$ を 1 つ取って固定する. $\phi: C \rightarrow E$ を $p \rightarrow \mu(p, P)$ で定めると, ϕ は K 上で定義された射である. 定義 1.11 より, 同型写像 $\iota: C \rightarrow E$ が存在する. E 上の平行移動 $\tau: E \rightarrow E, Q \mapsto Q + \mu(p, P) - \iota(p)$ で定義すると, $\phi = \tau \circ \iota$ であるから, ϕ は同型射である. よって K 上の同型 $\phi: C \rightarrow E$ が存在し, 次の図式を可換にする.

$$\begin{array}{ccc} C \times E & \xrightarrow{\mu} & C \\ \phi \times id \downarrow & & \downarrow \phi \\ E \times E & \xrightarrow{(P, Q) \mapsto P+Q} & E \end{array}$$

■

注意 1.14. K の標数が 0 のときは torsor を次のように定義しても問題ない. すなわち,

定義 1.15. E/K の torsor (C, μ) とは, K 上の曲線と K 上の射 $\mu: C \times E \rightarrow C$ の組であって, $C(\bar{K})$ に simply transitive な作用を誘導するものである.

ただし, 正標数のときは上記の定義では不十分である. たとえば torsor が twist になるという基本的な性質も成立しない. 実際, 作用が simply transitive であることより, $C(\bar{K})$ からとった点 p に対し, $E \rightarrow C, P \mapsto \mu(p, P)$ という射は分離次数は 1 だが次数が 1 とは限らない.

有限体上では, 種数 1 の曲線は自動的に有理点を持つ.

定理 1.16. (F.K.Schmidt 1931, [9] の演習問題 10.6 も参照)

E/\mathbb{F}_q を有限体 \mathbb{F}_q 上定義された楕円曲線とする. このとき, $WC(E/\mathbb{F}_q) = 0$.

Proof. 種数 1 の曲線 C に対し, $C(\mathbb{F}_q) \neq \emptyset$ を示せばよい. Fr_q を C の q 乗 Frobenius 写像とする. Fr_q のままでは固定点を固定点に移すとは限らず isogeny とは言えないので, 平行移動することで isogeny にしてしまおう.

$P_0 \in C(\overline{\mathbb{F}}_q)$ を任意に固定し, $f \in \text{End}(C)$ を $f(P) = Fr_q(P) - Fr_q(P_0)$ と定める. さらに, $1 - f$ は閉体上の isogeny だから全射であり, ある $P_1 \in C$ が存在して, $(1 - f)(P_1) = Fr_q(P_0)$. よって, $Fr_q(P_1) = f(P_1) + Fr_q(P_0) = P_1$ より, $P_1 \in C(\mathbb{F}_q)$. よって C は \mathbb{F}_q 有理点を持つので $WC(E/\mathbb{F}_q)$ の自明な元である. ■

次の命題によって, $WC(E/K)$ に群構造が入る.

命題 1.17 ([9] の X, Theorem 3.6). 楕円曲線 E/K に対し, 次は全単射である.

$$\begin{array}{ccc} WC(E/K) & \longrightarrow & H^1(G_{\overline{K}/K}, E) \\ \downarrow & & \downarrow \\ [C/K] & \longmapsto & [\sigma \mapsto \sigma p - p] \end{array}$$

ここで, p は任意に取った $C(\overline{K})$ の点であり, $\sigma p - p$ は $\mu(p, Q) = \sigma p$ となる点 $Q \in E$ を表すものとする. このような Q は定義 1.6 の (d) よりただ 1 つ存在する.

注意 1.18. 命題 1.17 より, $\text{III}(E/K) \cong \ker(WC(E/K) \rightarrow \prod_v WC(E/K_v))$ と特徴付けることができる. また, 命題 1.13 より, $\text{III}(E/K)$ とは局所的に有理点を持つ E の主等質空間の同型類の集合だと理解できる. つまり, $\text{III}(E/K)$ は局所大域原理が成り立つ主等質空間で代表される元 1 つと, その他の局所大域原理が成り立たない主等質空間で代表される元たちからなる集合である. すなわち,

$$\begin{aligned} \text{III}(E/K) &= \{ \text{local に有理点を持つ } E/K\text{-torsor の同型類の集合} \} \\ &= \{ [E/K] \} \cup \left\{ [C/K] \mid \begin{array}{l} C: E/K\text{-torsor s.t. } C(K) = \emptyset, \\ C(K_v) \neq \emptyset, \forall v \in M_K \end{array} \right\} \end{aligned}$$

である.

$\#\text{III}(E/K)$ が 1 のとき, 全ての主等質空間で局所大域原理が成り立ち, 1 より大きくなればなるほど, 局所大域原理を満たさない主等質空間が増えていくのであるから, $\text{III}(E/K)$ の大きさはまさに局所大域原理の成り立たなさを定量的に評価していると言える.

注意 1.19. 定理 1.16 と Hensel の補題より, $\text{III}(E/K) = \ker \{ H^1(G_K, E) \rightarrow \bigoplus_v H^1(G_{K_v}, E) \}$ である.

例 5. $\overline{\mathbb{Q}}$ 上の同型 $\phi: C \rightarrow E$ を適切に定めると, $\mu: C \times E \rightarrow C$ を $\phi^{-1}(\phi(p) + P)$ で定めることによって, 次のことが確認できる.

(1) $[3X^3 + 4Y^3 + 5Z^3 = 0] \in \text{III}(E: X^3 + Y^3 + 60Z^3 = 0/\mathbb{Q})$

(2) $[2y^2 = x^4 - 17] \in \text{III}(E: y^2 = x^3 + 17x/\mathbb{Q})$

2 主定理

導入において解説した Tate-Shafarevich 群と局所大域原理の関係 (注意 1.18) を踏まえ、本講演では、以下の問を考える。

問. 代数体上の楕円曲線 E/K を固定する. L/K を体の拡大としたとき, $\text{III}(E/L)$ の位数は $\text{III}(E/K)$ の位数と比べてどう増減するか.

この問は言い換えると、体拡大による局所大域原理の反例の個数の増減を調べていることになる。体を拡大すると、局所大域原理の反例が有理点を持ち、局所大域原理の反例が減少するように思える一方、上げた体上で新たな局所大域原理の反例が増える可能性もあり、その挙動は複雑である。

例 6. $[C : 2y^2 = x^4 - 2] \in \text{III}(E : y^2 = x^3 + 17x/\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ であり, $C(\mathbb{Q}) \neq \emptyset$ であるから, $[C]$ は $\text{III}(E : y^2 = x^3 + 17x/\mathbb{Q})$ の非自明な元である. ここで, 体を \mathbb{Q} から $\mathbb{Q}(\sqrt{-34})$ に拡大すると, $(0, \sqrt{-\frac{17}{2}}) \in C(\mathbb{Q}(\sqrt{-34}))$ であり, 命題 1.13 より $\text{III}(E/\mathbb{Q}(\sqrt{-34}))$ において $[C] = 0$ となる. しかし, このとき $\text{III}(E/\mathbb{Q}(\sqrt{-34}))[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ であり, $\mathbb{Q}(\sqrt{-34})$ 上で C は局所大域原理の反例ではなくなったにも関わらず, $\mathbb{Q}(\sqrt{-34})$ 上では局所大域原理の反例となる E/\mathbb{Q} の torsor が少なくとも 3 つ存在することがわかる. 一方で, $\text{III}(E/\mathbb{Q}(\sqrt{-2}))[2] = 0, \text{III}(E/\mathbb{Q}(\sqrt{-37}))[2] = 0$ のように, III の 2-part を自明化する 2 次体も存在する.

固定した E/K に対して, $\text{III}(E/L)$ の位数を $\text{III}(E/K)$ の位数より減らそうとするのか, 増やそうとするのかによって, 選択するべき L/K は大きく異なる.

増やす方向性について, Clark は任意の整数 r に対して, p 次拡大 L/K があって, $\text{III}(E/L)$ は位数 r の元を少なくとも p 個持つということを示した [2]. Matsuno は $K = \mathbb{Q}, p = 2$ の場合に Clark の別証明を与えた [5]. 一方で, \mathbb{Q} 上の $\text{III}(E_D/\mathbb{Q})$ をいくらでも大きくできることが Rohlich によって知られている [3]. すなわち, 任意の整数 r と任意の \mathbb{Q} 上の楕円曲線 E/\mathbb{Q} に対し, ある平方因子を持たない整数 D が存在し, $\#\text{III}(E_D/\mathbb{Q}) \geq r$ とできる. ただし, $E/K : y^2 = x^3 + Ax + B$ と書いたとき, $E_D/K : Dy^2 = x^3 + Ax + B$ を E/K の D による 2 次の twist という. 筆者は, [4] の結果のもと, それぞれいくらでも大きくできる $\#\text{III}(E/\mathbb{Q}(\sqrt{D}))$ と $\#\text{III}(E_D/\mathbb{Q})$ の比がいくらでも大きくできることを明らかにした. すなわち,

定理 2.1. 任意の整数 r と任意の楕円曲線 E/\mathbb{Q} に対して, ある 2 次体 $K = \mathbb{Q}(\sqrt{D})$ が存在して,

$$\#\text{III}(E/\mathbb{Q}(\sqrt{D})) \geq r\#\text{III}(E_D/\mathbb{Q})$$

が成り立つ.

証明においては, 次の完全列が重要な役割を果たす.

定理 2.2 ([6] を参照). E/K を代数体 K 上の楕円曲線とする. $\text{III}(E/K)$ の有限性を仮定すると, 次の完全列がある.

$$0 \rightarrow \text{III}(E/K) \rightarrow H^1(G_K, E) \rightarrow \bigoplus_v H^1(G_{K_v}, E) \rightarrow \widehat{E(K)}^* \rightarrow 0$$

ただし, $\widehat{E(K)}$ は $E(K)$ の副有限完備化であり, $\widehat{E(K)}^*$ は $\widehat{E(K)}$ の Pontryagin 双対である.

また, $X \stackrel{\text{def}}{=} \text{coker}(H^1(G_K, E)[2] \rightarrow \bigoplus_v H^1(G_{K_v}, E)[2])$ の位数を上から評価することによって, [2] の $K = \mathbb{Q}, p = 2$ の別証明を与えることができる. しかし, 筆者の知る最良の評価は現在のところ $\#X \leq \#\text{Sel}^2(E/K)$ (ただし, $\text{Sel}^2(E/K)$ は 2-Selmer 群とする) であり $\#\text{III}(E/\mathbb{Q}(\sqrt{D}))[2]$ が $\#\text{III}(E_D/\mathbb{Q})[2]$ と比べてもいくらでも大きくできるのかについては証明に至っておらず今後の課題である.

減らす方向性について, Tate-Shafarevich 群が代数体のイデアル類群の楕円曲線類似であることを考えると, この間は代数体の Hilbert 類体の楕円曲線類似が存在するか否かを問う問題であると言える.

[7] で予想されるランクの有界性を認めれば, ある楕円曲線が存在して, 任意の 2 次体 K に対して $\text{III}(E/K)[2] \neq 0$ が成り立つことがわかる.

筆者は具体的な楕円曲線について次のことを明らかにした.

命題 2.3. p を奇素数とし, $E : y^2 = x^3 + px$ を楕円曲線とする.

$\text{III}(E/K)[2] = 0$ もしくは $\text{III}(E/K)[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ となる虚 2 次体 K が無数に存在する.

この命題の証明は, K のイデアル類群の 2-part を自明化することによって体の Selmer 群 $K(S, 2) \stackrel{\text{def}}{=} \{b \in K^\times / K^{\times 2} \mid v(b) \equiv 0 \pmod{2}, \forall v \notin S\}$ を小さくしつつ, Selmer 群の元に対応する E/K -torsor が有理点を持たないようにするかランクを大きくすることによって行う. ただし, S は $2, p$ の上にある K の素点全体からなる集合である.

しかし, Magma による計算から $p = 257$ の場合については $\text{III}(E/K)[2] = 0$ とは出来ないのではないかと予想している.

参考文献

- [1] J.Bednarski, T.Ciurca, D.Gallo Supervised by L.Mann PROMYS, 2-Torsion in Ideal Class-Groups Europe 2017.
- [2] P. L. Clark and S. Sharif, Period, index and potential III, 2008, arXiv:0811.3019
- [3] J. Hoffstein and W. Luo. Nonvanishing of L-series and the combinatorial sieve. Math. Res. Lett., 4(2-3):435-444, 1997. With an appendix by David E. Rohrlich.
- [4] V.A.Kolyvagin, Finiteness of $E(Q)$ and $\text{III}(E/Q)$ for a class of Weil curves, Math.USSR Izvestiya 32 (1989), 523-541.
- [5] K. Matsuno, Elliptic curves with large Tate-Shafarevich groups over a number field, Math. Research Letters 16 (2009), no. 3, 449-461
- [6] J. S. Milne, Arithmetic Duality Theorems, Perspectives in Mathematics, Vol. 1, Academic Press, New York, 1986.
- [7] J. Park, B. Poonen, J. Voight, and M. Wood, A heuristic for boundedness of ranks of elliptic curves, J. Eur. Math. Soc. 21, (2019) 2859-2903.
- [8] D.Qiu, Shafarevich-Tate groups of elliptic curves upon quadratic extension and several applications, 2014, arXiv:1003.4393v2
- [9] J. H. Silverman, The arithmetic of elliptic curves, Springer, 2nd edition 2009.
- [10] H.Wu, On genus 1 curve violating Hasse principle, 2022, arXiv:2112.02470.
- [11] H.Yu, On Tate-Shafarevich groups over Galois extensions, Israel J. Math. 141 (2004), 211-220.