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.

$$Ш(E/K) \overset{\text{def}}{=} \mathrm{Ker}\left(H^1(G_K, E) \to \prod_v H^1(G_{K_v}, E) \right)$$

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 のトーサー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, Tate-Shafarevich 群の基礎的な事項について紹介するとともに, 楕円曲線 E/K を固定し, L/K を動かしたときの $Ш(E/L)$ の挙動について本講演 (2024 年 3 月 4 日) 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.

以下、断りのない限り K は全て代数体とする. 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. 代数体上での代数多様体の有理点の有無を判定するアルゴリズムは存在しない (Hilbert 第 10 問題の否定的解決) 一方で, その完備化 K_v 上での有理点の有無は判定することができる. 判定可能な局所的な体における有理点の有無で大域的な体における有理点の

* otheiio323.com@gmail.com

有無がわかるときに, 局所大域原理が成り立つというのである. 局所大域原理が成り立つ例として, 次が古典的に知られている.

定理 1.2. (Hasse–Minkowski の定理)
2 次形式 $aX^2+bY^2=Z^2(a,b\in K^\times)$ 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. 次の例の (3) のように, 最近になって見つかったものもある.

例 1.1.
(1) (Selmer, 1951) $3X^3+4Y^3+5Z^3=0$ 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.
(2) (Lind, 1940) $2y^2=x^4-17$ 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.
(3) (Han Wu 2022) [10] 任意の $\mathbb{Q}(\sqrt{-1})$ を含まない代数体 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.

上記 3 つの局所大域原理の反例には, 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 1.2. $S:3X^3+4Y^3+5Z^3=0$ 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, $\mathbb{Q}((\frac{3}{4})^{\frac{1}{3}})$ 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, 本稿で必要な事実を簡単に述べる.

命題 1.4. 標数が 2 または 3 でない体 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 $\mathbb{P}^2_K$ における射影閉包, $\{y^2=x^3+ax+b\}\cup\{\infty\overset{\text{def}}{=}(0,1,0)\}$ と K 上で同型である. 方程式 $y^2=x^3+ax+b$ を Weierstrass 方程式という. E の判別式を $\Delta_E=-16(4a^3+27b^2)$, E の j-不変量を $j(E)=1728\dfrac{4a^3}{4a^3+27b^2}$ で定義する.

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 とする. $P+Q$ を固定点 O と R を通る直線 L' と E との第 3 交点で与えれば, 固定点 O を単位元としてアーベル群をなす. 但し, $P=Q, R=O$ のときはそれぞれ L, L' をその点における E の接線として与える. ベズーの定理より, L' と E は重複を込めて必ず 3 点で交わることに注意する.

定理 1.6. 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,

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

($E(K)_{\mathrm{tor}}$ は有限アーベル群) とかける. $\mathrm{rank}(E/K)$ 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 $\phi : E_1 \to E_2$ であって, $\phi(O_{E_1}) = O_{E_2}$ を満たすもののことをいう．

定義 1.8. K を離散付値 v に関して完備な局所体とし, $E/K : y^2 = x^3 + ax + b$ を K 上の楕円曲線とする．π を K の整数環 O_K の素元とする．$k = O_K/(\pi)$ を O_K の剰余体とする．$x \mapsto u^2x, y \mapsto u^3y$ という変数変換を行うことで, $a, b \in O_K$ とできる．$a, b \in O_K$ の条件のもとで $v(\Delta_E)$ が最小のとき, Weilerstrass 方程式は最小であるという．今, Weierstrass 方程式は最小とする．楕円曲線 $\tilde{E}/k$ を次の方程式で定義する．

$$\tilde{E}/k : y^2 = x^3 + \tilde{a}x + \tilde{b}, \quad \tilde{a}_i := a_i \mod \pi$$

$\tilde{E}$ が非特異であるとき, E/K は π において良い還元 (good reduction) を持つといい, 特異点があるとき, E/K は π で悪い還元 (bad reduction) を持つという．

定義 1.9. 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のことをいう．

例 1.3. K を体とし, C/K を K 上の種数 1 の曲線とする．$C(\overline{K})$ は $\mathrm{Gal}(\overline{K}/K)$ 上の加群である．実際, $C(\overline{K})$ は固定点 O を単位元とするアーベル群をなし, $\mathrm{Gal}(\overline{K}/K)$ の $\overline{K}$ への作用を $x \mapsto \sigma x$ で表すことにすると, $\mathrm{Gal}(\overline{K}/K) \times C(\overline{K}) \to C(\overline{K})$ を $(\sigma, (x, y)) \mapsto (\sigma x, \sigma y), O \mapsto O$ で定めることができる．

定義 1.10. (ガロアコホモロジー) G をガロア群, 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 (有限群のときは離散位相に一致) を入れている．このとき,

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

を 0 次のガロアコホモロジー,

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

を 1 次のガロアコホモロジーという．

ただし,

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

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

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．

注意 1.11. アーベル群 N と M がアーベル群として同型でも, G 加群として同型でなければ, $H^1(G, N) \cong H^1(G, M)$ とは限らない．たとえば $\mathbb{Z}/2\mathbb{Z}$ が $\mathbb{Z}$ に自明に作用するとき $\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$ が -1 倍で作用するとき $\mathbb{Z}^-$ と表記することにすると, $\mathbb{Z}$ と $\mathbb{Z}^-$ はアーベル群としては同型だが $H^1(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) = 0$, $H^1(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}^-) \cong \mathbb{Z}/2\mathbb{Z}$ である．

定義 1.12. 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_K を K の絶対ガロア群とする.

$$Ш(E/K) \overset{\text{def}}{=} \mathrm{Ker}\left(\begin{array}{ccc} H^1(G_K, E) & \overset{\oplus_v \mathrm{res}_v}{\longrightarrow} & \bigoplus_{v \in M_K} H^1(G_{K_v}, E) \\ \cup & & \cup \\ [f] & \longmapsto & (\left[f\,|_{G_{K_v}} \right])_v \end{array} \right)$$

を楕円曲線 E/K の Tate-Shafarevich 群という. ここで, res$v : H^1(G_K, E) \to H^1(G_{K_v}, E), [f] \mapsto [f\,|_{G_{K_v}}]$ はガロアコホモロジーの制限写像である.

また, 正整数 n に対し, $Ш(E/K)[n] \overset{\text{def}}{=} \{[C] \in Ш(E/K) \mid n[C] = 0\}$ を Tate-Shafarevich 群 $Ш(E/K)$ 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トーサーの集合と思うことで Tate-Shafarevich 群は幾何的な解釈を得る. 定理 1.18のために, ここでは一般の体上でトーサーを定義する. なお, 標数 0 の場合にのみ興味がある場合は, 定義 1.17で十分である.

定義 1.13 (トーサー)**.** E/K を楕円曲線とする. E/K-トーサー (torsor, 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. 射 $\mu : C \times E \to C$ は K 上定義されていて, 次をみたす.

(a) $\overline{K}$ 上の同型 $\iota : C \to E$ が存在して, 次の図式を可換にする.

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

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 1.4. E/K 自身は E/K のトーサーである. 実際, $\mu(p, P) = p + P$ と定めればよい.

定義 1.14 (Weil-Châtelet 群)**.** E/K を楕円曲線とする.

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

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

E/K のトーサー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, $\mathrm{WC}(E/K)$ と表す. また, E/K を含む同値類を自明類という.

命題 1.15. E/K を楕円曲線とする. E/K のトーサー $(C/K, \mu)$ 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.
トーサー 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. $\phi : E \to C$ を $p \to \mu(P, p)$ で定めると, ϕ は K 上定義された同型射であることが確認でき, ϕ^{-1} は次の図式を可換にする.

$$\begin{array}{ccc} C \times E & \xrightarrow{\mu} & C \\ {\scriptstyle \phi^{-1}\times \mathrm{id}}\downarrow & & \downarrow{\scriptstyle \phi^{-1}} \\ E \times E & \xrightarrow[(P,Q)\mapsto P+Q]{} & E \end{array}$$

■

注意 1.16. K の標数が 0 のときはトーサーを次のように定義しても問題ない. すなわち,

定義 1.17. E/K-トーサー (C, μ) とは, K 上の曲線と K 上の射 $\mu : C \times E \to C$ の組であって, $C(\overline{K})$ 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. たとえばトーサーが E と $\overline{K}$ 上同型になるという, トーサーが本来満たすべき基本的な性質が成立しない. 実際, 作用が simply transitive であることより, $C(\overline{K})$ からとった点 p に対し, $E \to C, P \mapsto \mu(p, P)$ という射は分離次数は 1 だが, 次数が 1 とは限らない.

例 1.5. $p \neq 2, 3$ を素数とし, $E/\overline{\mathbb{F}}_p$ を $\overline{\mathbb{F}}_p$ 上の楕円曲線で $j(E) \notin \mathbb{F}_p$ となるものとする. $E^{(p)}$ を, E の Weierstrass 方程式の係数を p 乗して得られる楕円曲線とする. このとき, $E^{(p)}$ は $E^{(p)} \times E \to E^{(p)}$ を $(q, Q) \mapsto q + Q^p$ と定めることによって $E/\overline{\mathbb{F}}_p$-トーサーとなる. しかし, $j(E^{(p)}) = j(E)^p \neq j(E)$ となり, E と $E^{(p)}$ は $\overline{\mathbb{F}}_p$ 上同型にならない. $E^{(p)}(\overline{\mathbb{F}}_p)$ からとった点 q に対し, $E \to E^{(p)}, P \mapsto q + P^p$ という射は全単射だが, 逆写像が射ではなくなってしまっているのである.

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 1.18. (F.K.Schmidt 1931, [8] 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, $\mathrm{WC}(E/\mathbb{F}_q) = 0$.

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, C の自己射 $f : C \to C$ を $f(P) = Fr_q(P) - Fr_q(P_0)$ で定める.

$1-f$ は閉体上の isogeny だから全射であり, ある $P_1 \in C(\overline{F}_q)$ 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 $\mathrm{WC}(E/\mathbb{F}_q)$ の自明な元である. ■

次の命題によって, $\mathrm{WC}(E/K)$ に群構造が入る.

命題 1.19 ([8] の X, Theorem 3.6)**.** 楕円曲線 E/K に対し, 次は全単射である.

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

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 1.13の (d) よりただ 1 つ存在する.

注意 1.20.

命題 1.19より, $Ш(E/K) \cong \mathrm{Ker}\left(\mathrm{WC}(E/K) \to \prod_{v \in M_K} \mathrm{WC}(E/K_v)\right)$ と特徴付けることができる. また, 命題 1.15より, $Ш(E/K)$ とは局所的に有理点を持つ E のトーサーの同型類の集合だと理解できる. つまり, $Ш(E/K)$ は局所大域原理が成り立つトーサーで代表される元 (つまり, 楕円曲線)1 つと, その他の局所大域原理が成り立たないトーサーで代表される元たちからなる集合である. すなわち,

$$\begin{aligned} Ш(E/K) &= \{\text{local に有理点を持つ } E/K\text{-トーサーの同型類の集合 }\} \\ &= \{[E/K]\} \bigcup \left\{ [C/K] \;\middle|\; \begin{array}{l} C\text{: } E/K\text{-トーサー s.t. } C(K) = \emptyset, \\ C(K_v) \neq \emptyset, \forall v \in M_K \end{array} \right\} \end{aligned}$$

である.

$\#Ш(E/K)$ 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, $Ш(E/K)$ 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 1.21. 定理 1.18と Hensel の補題より, $Ш(E/K) = \mathrm{Ker}\left(H^1(G_K, E) \to \bigoplus_{v \in M_K} H^1(G_{K_v}, E)\right)$ である. 実際, トーサー C/K が v で良い還元を持つ場合, 有限体上の種数 1 の曲線は常に有理点を持つため, Hensel の補題によって C は K_v-有理点を持ち, $H^1(G_{K_v}, E)$ におけるその像は命題 1.15より自明類に含まれるからである。

例 1.6. $\overline{\mathbb{Q}}$ 上の同型 $\phi : C \to E$ を $\mu : C \times E \to C : (p, P) \mapsto \phi^{-1}(\phi(p) + P)$ が $\mathbb{Q}$ 上定義されるように適切に定めることによって, 次のことが確認できる.
(1) $[3X^3 + 4Y^3 + 5Z^3 = 0] \in Ш(E : X^3 + Y^3 + 60Z^3 = 0/\mathbb{Q})$
(2) $[2y^2 = x^4 - 17] \in Ш(E : y^2 = x^3 + 17x/\mathbb{Q})$

注意 1.22. $[2y^2 = x^4 + 17] \in Ш(E : y^2 = x^3 + 17x/\mathbb{Q})$ と書いたとき, 正確には $2y^2 = x^4 - 17$ を $\mathbb{P}^3$ に埋め込んでできた射影曲線を表している. 単に $\mathbb{P}^2$ の中で射影閉包を取っても, $[0:1:0]$ が特異

点になってしまい, 非特異射影曲線であるトーサーとしては採用できない. そこで, 特異点を無くすために 2 つの非特異な affine curve, $C_0 : 2y^2 = x^4 - 17$ と $C_1 : 2v^2 = 1 - 17u^4$ を $u = \frac{1}{x}, v = \frac{y}{x^2}$ で貼り合わせる. つまり, 重み付き射影空間 $\mathbb{P}(1,2,1)$ に $i : C_0 \to \mathbb{P}(1,2,1)$ を $(x,y) \mapsto [x : y : 1]$, $v : C_1 \to \mathbb{P}(1,2,1)$ を $(u,v) \mapsto (1,u,v)$ で $\mathbb{P}(1,2,1)$ に埋め込み, $C = i(C_0) \bigcup v(C_1)$ で $\mathbb{P}(1,2,1)$ における曲線を定義する. 無限遠点は $[\sqrt{2} : 1 : 0]$ であり, 基礎体が $\mathbb{Q}$ の場合は無限遠点はない. $\mathbb{P}(1,2,1)$ は $\mathbb{P}^3$ に, $(x,y,z) \mapsto (x^2, xz, z^2, y)$ によって埋め込まれることに注意する. C は C_0 と双有理同値だから同じ種数 $g(C)$ である. $C_0 \to \mathbb{P}^1$ を $[x,y,z] \mapsto (x,y)$ とし, リーマンフルヴィッツの公式を使うと $g(C) = 1$ がわかる.

注意 1.23. $Ш(E/\mathbb{Q})$ の 4 つの元は知られている. 参考文献 [8] の Proposition 6.5(a) より,
$Ш(E : y^2 = x^3 + 17x/\mathbb{Q}))[2]$ の非自明な元は

$$[y^2 + 1 = 68x^4], [y^2 = -34x^2 + 2], [y^2 = -34x^4 - 2]$$

の 3 つであり, Lind の反例 $2y^2 = x^4 - 17$ は $y^2 = -34x^4 + 2$ と同型である.

2 講演内容

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 1.20) 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, $Ш(E/L)$ の位数は $Ш(E/K)$ 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 2.1. $[C : 2y^2 = x^4 - 2] \in Ш(E : y^2 = x^3 + 17x/\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ であり, $C(\mathbb{Q}) \neq \emptyset$ であるから, $[C]$ は $Ш(E : y^2 = x^3 + 17x/\mathbb{Q})$ 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 1.15より $Ш(E/\mathbb{Q}(\sqrt{-34}))$ において $[C] = 0$ となる. しかし, このとき $Ш(E/\mathbb{Q}(\sqrt{-34}))[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 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 $E/\mathbb{Q}$ のトーサーが少なくとも 3 つ存在することがわかる. 一方で, $Ш(E/\mathbb{Q}(\sqrt{-2}))[2] = 0, Ш(E/\mathbb{Q}\sqrt{-37}))[2] = 0$ のように, Ш 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, $Ш(E/L)$ の位数を $Ш(E/K)$ 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, $Ш(E/L)$ 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 [1]. Matsuno は $K = \mathbb{Q}, p = 2$ の場合に Clark の別証明を与えた [4]. 一方で, $\mathbb{Q}$ 上の $Ш(E_D/\mathbb{Q})$ 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 [2]. 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, $\#Ш(E_D/\mathbb{Q}) \geq r$ 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, [3] の結果のもと, それぞれいくらでも大きくできる $\#Ш(E/\mathbb{Q}(\sqrt{D}))$ と $\#Ш(E_D/\mathbb{Q})$ 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,

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

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 ([5] を参照)**.** E/K を代数体 K 上の楕円曲線とする. $Ш(E/K)$ の有限性を仮定すると, 次の完全列がある.

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

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, $X \overset{\text{def}}{=} \operatorname{coker}(H^1(G_K, E)[2] \to \bigoplus_v H^1(G_{K_v}, E)[2]))$ の位数を上から評価することによって, [1] 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 (2024 年 3 月 4 日) のところ $\#X \leq \#\mathrm{Sel}^2(E/K)$(ただし, $\mathrm{Sel}^2(E/K)$ は 2-Selmer 群とする) であり $\#Ш(E/\mathbb{Q}(\sqrt{D}))[2]$ が $\#Ш(E_D/\mathbb{Q})[2]$ 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, この問は代数体の 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うことができる.

[6] 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 $Ш(E/K)[2] \neq 0$ 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.

$Ш(E/K)[2] = 0$ もしくは $Ш(E/K)[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 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 $K(S, 2) \overset{\text{def}}{=} \left\{ b \in K^\times/K^{\times 2} \mid v(b) \equiv 0 \mod 2, \forall v \notin S \right\}$ を小さくしつつ, Selmer 群の元に対応する E/K-トーサー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 $Ш(E/K)[2] = 0$ とは出来ないのではないかと予想している.

参考文献

[1] P. L. Clark and S. Sharif, Period, index and potential Sha. Algebra and Number Theory 4 (2010), No. 2, 151-174.

[2] 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.

[3] V. A. Kolyvagin, Finiteness of $E(Q)$ and Ш(E/Q) for a class of Weil curves, Math.USSR Izvestiya 32 (1989), 523-541.

[4] K. Matsuno, Elliptic curves with large Tate-Shafarevich groups over a number field, Math. Research Letters 16 (2009), no. 3, 449–461

[5] J. S. Milne,Arithmetic Duality Theorems, Perspectives in Mathematics, Vol. 1, Academic Press, New York, 1986.

[6] 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.

[7] D. Qiu, Shafarevich-Tate groups of elliptic curves upon quadratic extension and several applications, 2014, arXiv:1003.4393v2

[8] J. H. Silverman, The arithmetic of elliptic curves, Springer, 2nd edition 2009.

[9] J. H. Silverman, Errata, Corrections, and Addenda to The Arithmetic of Elliptic Curves 2nd Edition, 2nd Printing (2015)

[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.