4.

楕円曲線の Mordell-Weil 群：descent 理論

吉川 祥[*1]（学習院大学）

4.1 イントロダクション

代数体上の楕円曲線で最も基本的な結果は次の Mordell-Weil の定理だろう．

定理 4.1.1. (Mordell-Weil) E を代数体 K 上の楕円曲線とする．このとき，E の K 有理点のなす群は有限生成アーベル群である．すなわち，自然数 r と有限アーベル群 T が存在して

$$E(K) \simeq \mathbb{Z}^r \oplus T \tag{4.1}$$

と表すことができる．

r を E の階数 (rank) とよび，T を E の捻じれ部分 (torsion part) とよぶ．捻じれ部分 T を決定することは比較的容易であるが，階数 r を決定することは一般には困難である．

本稿の目的は，個別の楕円曲線 E に対して，多くの場合にその階数 r を決定できるアルゴリズム (**2-descent**) を紹介することである．より詳しくは [3, Capter X] を見ていただきたい．

まず，次のことに注意しよう．(4.1) に $\mathbb{F}_2$ をテンソルすることで，

$$E(K)/2E(K) \simeq \mathbb{F}_2^r \oplus (T \otimes \mathbb{F}_2) \tag{4.2}$$

となる．(4.2) の次元を考えれば，

$$r = \dim_{\mathbb{F}_2}(E(K)/2E(K)) - \dim_{\mathbb{F}_2}(T \otimes \mathbb{F}_2)$$

[*1] This work was supported by JSPS KAKENHI Grant Number JP17H07074

である．T は計算できるので, r を計算するという問題は $\dim_{\mathbb{F}_2}(E(K)/2E(K))$ を計算するという問題に帰着する．

しかし，残念ながら $\dim_{\mathbb{F}_2}(E(K)/2E(K))$ を直接計算する方法は一般には知られていない．そこで, $E(K)/2E(K)$ を計算可能な有限集合 (Selmer 群) のなかに埋め込むことで, $E(K)/2E(K)$ の位数を上から抑える，というアプローチを採る．すなわち, $\dim_{\mathbb{F}_2}(E(K)/2E(K))$ の正確な大きさを求めるのではなく，より捉えやすい Selmer 群で妥協するというアイディアである．Selmer 群の大きさがどのくらい $E(K)/2E(K)$ から離れているかは Tate-Shafarevich 群と呼ばれる群（の 2-part）によって記述される．

4.1.1 絶対 Galois 群

F を体とする．このとき，F の絶対 Galois 群を $G_F := \mathrm{Gal}(\bar{F}/F) = \varprojlim_{F'/F} \mathrm{Gal}(F'/F)$ と定める．ただし，逆極限において $F'(\subset \bar{F})$ は F の有限次 Galois 拡大を走る．G_F は副有限群であることに注意しよう．p を素数とする．各埋め込み $i\colon \bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$ を決めるごとに, 単射準同形 $G_{\mathbb{Q}_p} \hookrightarrow G_{\mathbb{Q}}(g \mapsto g|_{\bar{\mathbb{Q}}})$ が定まる．i を取り換えると，この単射は $G_{\mathbb{Q}}$ の元による共役だけ変わる．以後，埋め込み i をひとつ固定し，単射 $G_{\mathbb{Q}_p} \hookrightarrow G_{\mathbb{Q}}$ （$g \mapsto g|_{\bar{\mathbb{Q}}}$）によって $G_{\mathbb{Q}_p}$ は $G_{\mathbb{Q}}$ の部分群だと考える．$\mathbb{Q}_p$ の最大不分岐拡大を $\mathbb{Q}_p^{\mathrm{ur}}$ と書く．$\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p$ は Galois 拡大であり，自然な同形

$$\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p) \simeq G_{\mathbb{F}_p}$$

がある．$G_{\mathbb{F}_p} \simeq \hat{\mathbb{Z}}$ である．また，p の惰性群を $I_{\mathbb{Q}_p} = \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p^{\mathrm{ur}})$ と定める．定義より，

$$1 \to I_{\mathbb{Q}_p} \to G_{\mathbb{Q}_p} \to \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p) \to 1$$

という完全系列が存在する．

4.2 Selmer 群

必要な群のコホモロジーの知識は省略する．必要なまとめについては，例えば [3, Appendix B] または [2] を参照せよ．また，簡単のために楕円曲線は $\mathbb{Q}$ 上定義されたものを考えることにする．

E, E' を $\mathbb{Q}$ 上の楕円曲線とし, $\varphi\colon E \to E'$ を同種写像とする．$E[\varphi] = \ker\varphi$ とおく．このとき，$G_{\mathbb{Q}}$ 加群としての完全系列

$$0 \to E[\varphi](\bar{\mathbb{Q}}) \to E(\bar{\mathbb{Q}}) \xrightarrow{\varphi} E'(\bar{\mathbb{Q}}) \to 0$$

がある．各素点 $p \leq \infty$ についても同様に，$G_{\mathbb{Q}_p}$ 加群としての完全系列

$$0 \to E[\varphi](\bar{\mathbb{Q}}_p) \to E(\bar{\mathbb{Q}}_p) \xrightarrow{\varphi} E'(\bar{\mathbb{Q}}_p) \to 0$$

が得られる．これらから得られるコホモロジー長完全系列の一部をみることにより，可換図式

$$\begin{array}{ccccccc} 0 & \longrightarrow & E'(\mathbb{Q})/\varphi(E(\mathbb{Q})) & \longrightarrow & H^1(G_{\mathbb{Q}}, E[\varphi](\bar{\mathbb{Q}})) & \xrightarrow{i} & H^1(G_{\mathbb{Q}}, E(\bar{\mathbb{Q}})) \\ & & \downarrow & & \downarrow{\scriptstyle \alpha_p} & & \downarrow{\scriptstyle \beta_p} \\ 0 & \longrightarrow & E'(\mathbb{Q}_p)/\varphi(E(\mathbb{Q}_p)) & \longrightarrow & H^1(G_{\mathbb{Q}_p}, E[\varphi](\bar{\mathbb{Q}}_p)) & \xrightarrow{i_p} & H^1(G_{\mathbb{Q}_p}, E(\bar{\mathbb{Q}}_p)) \end{array}$$

が得られる．ここで，縦の写像 α_p, β_p は，$G_{\mathbb{Q}_p} \hookrightarrow G_{\mathbb{Q}}$ による制限写像を表す．

定義 4.2.1. 以上の設定のもと，

$$\mathrm{Sel}^{(\varphi)}(E/\mathbb{Q}) := \bigcap_{p \leq \infty} \ker(\beta_p \circ i) \subset H^1(G_{\mathbb{Q}}, E[\varphi](\bar{\mathbb{Q}}))$$

とおき (φ-)Selmer 群と呼ぶ．また，

$$Ш(E/\mathbb{Q}) := \bigcap_{p \leq \infty} \ker \beta_p \subset H^1(G_{\mathbb{Q}}, E(\bar{\mathbb{Q}}))$$

とおき Shafarevich-Tate 群と呼ぶ．

注意 4.2.2. (1) 定義により完全系列

$$0 \to E(\mathbb{Q})/\varphi(E'(\mathbb{Q})) \to \mathrm{Sel}^{(\varphi)}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})$$

がある．

(2) 注意 4.2.4 において，Selmer 群が原理的に計算可能であることを見る．(1) の完全系列で特に重要なことは，E の階数を知るために重要な群 $E(\mathbb{Q})/\varphi(E'(\mathbb{Q}))$ が計算可能な群（Selmer 群）に含まれているという点である．そして，2 つの群の差が Tate-Shafarevich 群という群で記述されているということも重要である．

(3) E を体 K 上の楕円曲線とする．E-torsor(もしくは E の主等質空間) の同形類からなる集合（実は群になる）を $\mathrm{WC}(E/K)$ と書き，Weil-Châtelet 群という．詳しい定義や性質は [3, Chapter X §3] を見られたい．特に重要な事実として，自然な同形 $\mathrm{WC}(E/K) \xrightarrow{\simeq} H^1(G_K, E(\bar{K}))$ の存在が挙げられる（[3, X Theorem 3.6]）．

(4) $\xi \in H^1(G_{\mathbb{Q}}, E[\varphi](\bar{\mathbb{Q}}))$ に対して，ξ を

$$i\colon H^1(G_{\mathbb{Q}}, E[\varphi](\bar{\mathbb{Q}})) \to H^1(G_{\mathbb{Q}}, E(\bar{\mathbb{Q}})) = \mathrm{WC}(E/\mathbb{Q})$$

で送って得られる E-torsor（の同形類）を C_ξ と書く．このとき，Selmer 群 $\mathrm{Sel}^{(\varphi)}(E/\mathbb{Q})$ は

$$\mathrm{Sel}^{(\varphi)}(E/\mathbb{Q}) = \{\xi \in H^1(G_{\mathbb{Q}}, E[\varphi](\bar{\mathbb{Q}})) \mid p \in S \text{ に対して } C_\xi(\mathbb{Q}_p) \neq \emptyset\}$$

と記述される．また，$E(\mathbb{Q})/\varphi(E'(\mathbb{Q}))$ は

$$E(\mathbb{Q})/\varphi(E'(\mathbb{Q})) = \{\xi \in H^1(G_{\mathbb{Q}}, E[\varphi](\bar{\mathbb{Q}})) \mid C_\xi(\mathbb{Q}) \neq \emptyset\}$$

と記述される．

さて，Selmer 群の性質で最も基本的なものは有限性である．これを保証するのが次の定理である．この定理はさらに，Selmer 群を計算可能な有限集合の部分集合としてとらえるという意味でも有用である．

定理 4.2.3. [3, X Theorem 4.2, Lemma 4.3, Corollary 4.4] $\varphi\colon E \to E'$ を $\mathbb{Q}$ 上の楕円曲線の間の同種写像とし，$S(\ni \infty)$ を $\mathbb{Q}$ の素点からなる有限集合とする．また，

$$H^1(G_{\mathbb{Q}}, E[\varphi]; S) := \{\xi \in H^1(G_{\mathbb{Q}}, E[\varphi](\bar{\mathbb{Q}})) \mid p \notin S \text{ に対して} \xi|_{I_{\mathbb{Q}_p}} \text{は自明 } \}$$

とおく．（すなわち，S の外で不分岐なコホモロジー類全体のなす部分群である．）
(1) $H^1(G_{\mathbb{Q}}, E[\varphi]; S)$ は有限集合である．
(2) S が $\{\infty\} \cup \{p|\ p \text{ は } \deg\varphi \text{ を割る.}\} \cup \{p|\ E, E' \text{は } p \text{ で悪い還元を持つ.}\}$ を含むとする．このとき，$\mathrm{Sel}^{(\varphi)}(E/\mathbb{Q}) \subset H^1(G_{\mathbb{Q}}, E[\varphi]; S)$ である．

証明．(1) のみ，簡単な場合（$E = E', \varphi = [2], E[2](\bar{\mathbb{Q}}) \subset E(\mathbb{Q})$）の証明の概略を述べる．$E[2](\bar{\mathbb{Q}}) \subset E(\mathbb{Q})$ により，$G_{\mathbb{Q}}$ 加群としての同形

$$f\colon E[2] \xrightarrow{\simeq} (\mathbb{Z}/(2))^{\oplus 2} = \mu_2^{\oplus 2}$$

がある．（ここで $\mu_2 = \{\pm 1\}$ は 1 の 2 乗根のなす群を表す．）したがって，素点 p に対し，以下の可換図式において横方向の射は Kummer 理論から同形である．

$$\begin{array}{ccc} H^1(G_{\mathbb{Q}}, E[2](\bar{\mathbb{Q}})) & \xrightarrow[\delta]{\simeq} & (\mathbb{Q}^\times/(\mathbb{Q}^\times)^2)^{\oplus 2} \\ {\scriptstyle R_p}\downarrow & & \downarrow{\scriptstyle R'_p} \\ H^1(I_{\mathbb{Q}_p}, E[2](\bar{\mathbb{Q}})) & \xrightarrow[\delta_p]{\simeq} & (\mathbb{Q}_p^{\mathrm{ur}\,\times}/(\mathbb{Q}_p^{\mathrm{ur}\,\times})^2)^{\oplus 2} \end{array}$$

ただし，縦方向の射は $I_{\mathbb{Q}_p} \hookrightarrow G_{\mathbb{Q}}$ から得られる制限写像を表す．定義により

$$H^1(G_{\mathbb{Q}}, E[\varphi]; S) = \bigcap_{p \notin S} \ker R_p$$

であるが，上の図式の同形射によって，これは

$$\bigcap_{p \notin S} \ker R'_p = \mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$$

と同一視される．ただし $\mathbb{Q}(S,2)$ は

$$\begin{aligned} \mathbb{Q}(S,2) &= \{a \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \mid p \notin S \text{ に対して } \mathrm{val}_p(a) \equiv 0 \bmod 2\} \\ &\simeq \{\prod_{p \in S} p^{\epsilon(p)} \mid\ \epsilon(p) = 0 \text{ または } 1\} \end{aligned}$$

とおいた．$\mathbb{Q}(S,2)$ は明らかに有限なので，$H^1(G_{\mathbb{Q}}, E[\varphi]; S)$ も有限となる．

□

注意 4.2.4. (1) 定理 4.2.3(1) の証明から推測できるように，$H^1(G_{\mathbb{Q}}, E[\varphi]; S)$ は原理的に計算可能である．
(2) S を定理 4.2.3 (2) のようにとる．注意 4.2.2 の (3) と定理 4.2.3 の (2) により，

$$\mathrm{Sel}^{(\varphi)}(E/\mathbb{Q}) = \{\xi \in H^1(G_{\mathbb{Q}}, E[\varphi]; S) \mid p \in S \text{ に対して } C_\xi(\mathbb{Q}_p) \neq \emptyset\}$$
$$E(\mathbb{Q})/\varphi(E'(\mathbb{Q})) = \{\xi \in H^1(G_{\mathbb{Q}}, E[\varphi]; S) \mid C_\xi(\mathbb{Q}) \neq \emptyset\}$$

が成り立つ．注意 4.2.2(3) との違いは，$\mathrm{Sel}^{(\varphi)}(E/\mathbb{Q})$ や $E(\mathbb{Q})/\varphi E'(\mathbb{Q})$ を含んでいる集合が $H^1(G_{\mathbb{Q}}, E[\varphi]; S)$ に変わった点である．すなわち，$\mathrm{Sel}^{(\varphi)}(E/\mathbb{Q})$ や $E(\mathbb{Q})/\varphi E'(\mathbb{Q})$ が，計算可能な集合 $H^1(G_{\mathbb{Q}}, E[\varphi]; S)$ の部分集合として具体的な条件で切り出せたことを示している．さらに，$\mathrm{Sel}^{(\varphi)}(E/\mathbb{Q})$ を切り出している条件 $C_\xi(\mathbb{Q}_p) \neq \emptyset$ は Hensel の補題により有限のプロセスで成否を確認することが可能である．したがって，$\mathrm{Sel}^{(\varphi)}(E/\mathbb{Q})$ は原理的に計算可能となる．しかし，$E(\mathbb{Q})/\varphi E'(\mathbb{Q})$ を切り出している条件 $C_\xi(\mathbb{Q}) \neq \emptyset$ は曲線の $\mathbb{Q}$ 有理点の存在問題であり，種数 1 なので局所大域原理が成り立たず，これを計算するアルゴリズムは一般には知られていない．

4.3 descent(降下)

ここでも E を $\mathbb{Q}$ 上の楕円曲線とする．この節では E の 2-Selmer 群を求める手法を紹介する．注意 4.2.4 で述べたように，2-Selmer 群を計算可能な集合として具体的に捉え，$E(\mathbb{Q})/2E(\mathbb{Q})$ をその中の部分集合として捉えることが重要である．2-Selmer 群は，$E[2](\mathbb{Q})$ の位数 (1, 2, または 4) が大きければ大きいほどを容易に計算が可能である．

4.3.1 $|E[2](\mathbb{Q})| = 4$ のとき

この場合，Complete 2-descent と呼ばれる手法を使う．仮定により、E の定義方程式を

$$y^2 = (x - e_1)(x - e_2)(x - e_3)$$

$(e_1, e_2, e_3 \in \mathbb{Q})$ にとることができる。S を定理 4.2.3 (2) のようにとると、定理 4.2.3 (1) の証明により

$$H^1(G_{\mathbb{Q}}, E[2]; S) \simeq \mathbb{Q}(S,2)^{\oplus 2}$$

が成り立つ。このとき、注意 4.2.4 により、Selmer 群と $E(\mathbb{Q})/2E(\mathbb{Q})$ は次のように記述される：

$$\mathrm{Sel}^{(2)}(E/\mathbb{Q}) = \{b = (b_1, b_2) \in \mathbb{Q}(S,2)^{\oplus 2} \mid \ p \in S \text{ に対して } C_b(\mathbb{Q}_p) \neq \emptyset\}$$
$$E(\mathbb{Q})/2E(\mathbb{Q}) = \{b = (b_1, b_2) \in \mathbb{Q}(S,2)^{\oplus 2} \mid \ C_b(\mathbb{Q}) \neq \emptyset\}.$$

ここで、C_b は b を

$$\mathbb{Q}(S,2) \simeq H^1(G_{\mathbb{Q}}, E[2]; S) \to H^1(G_{\mathbb{Q}}, E(\bar{\mathbb{Q}})) = \mathrm{WC}(E/\mathbb{Q})$$

で送って得られる E-torsor である。

注意 4.3.1. C_b は具体的には次の方程式で定まる $\mathbb{P}^3_{\mathbb{Q}}$ 内の曲線として与えられる（[3, X Proposition 1.4]）：

$$b_1 z_1^2 - b_2 z_2^2 = (e_2 - e_1) z_0^2$$
$$b_1 z_1^2 - b_1 b_2 z_3^2 = (e_3 - e_1) z_0^2$$

4.3.2 $|E[2](\mathbb{Q})| = 2$ のとき

この場合，descent via 2-isogeny とよばれる手法を使う．E の定義方程式を

$$y^2 = x^3 + ax^2 + bx$$

にとることができる．$(0,0)$ が位数 2 の $\mathbb{Q}$ 有理点である．上記の定義方程式に対し，新たな楕円曲線 E' を

$$Y^2 = X^3 - 2aX + (a^2 - 4b)$$

で定義する．このとき，E と E' の間には以下の次数 2 の同種写像が存在する ([3, III Example 4.5])．

$$\varphi\colon E \to E',\ (x,y) \mapsto (X,Y) = \left(\frac{y^2}{x^2}, \frac{y(b-x)}{x^2}\right)$$

$$\hat{\varphi}\colon E' \to E,\ (X,Y) \mapsto (x,y) = \left(\frac{Y^2}{4X^2}, \frac{Y(a^2 - 4b - X^2)}{8X^2}\right)$$

この φ について、$E[\varphi](\bar{\mathbb{Q}}) = E[2](\mathbb{Q})$ が成り立つ．φ が $E(\mathbb{Q})/2E(\mathbb{Q})$ を知るのに有用な理由は次の命題による．

命題 4.3.2. [3, Remark 4,7] 次の完全系列がある：

$$0 \to \frac{E'[\hat{\varphi}](\mathbb{Q})}{\varphi(E[2](\mathbb{Q}))} \to \frac{E'(\mathbb{Q})}{\varphi(E(\mathbb{Q}))} \to \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \to \frac{E(\mathbb{Q})}{\hat{\varphi}(E'(\mathbb{Q}))} \to 0.$$

命題の完全系列において，$E'[\hat{\varphi}](\mathbb{Q})/\varphi(E[2](\mathbb{Q}))$ を計算することは容易である．したがって，あとは $E'(\mathbb{Q})/\varphi(E(\mathbb{Q}))$ と $E(\mathbb{Q})/\hat{\varphi}(E'(\mathbb{Q}))$ の位数が分かれば所望の $E(\mathbb{Q})/2E(\mathbb{Q})$ の位数が分かる．すくなくとも，$\mathrm{Sel}^{(\varphi)}(E/\mathbb{Q})$ や $\mathrm{Sel}^{(\hat{\varphi})}(E'/\mathbb{Q})$ を計算することで，$E(\mathbb{Q})/2E(\mathbb{Q})$ の位数が上からおさえられる．

$E'(\mathbb{Q})/\varphi(E(\mathbb{Q}))$ や $\mathrm{Sel}^{(\varphi)}(E/\mathbb{Q})$ に関する具体的な記述は以下のようにして得られる．素点の有限集合 S を定理 4.2.3 (2) のようにとる．すると，定理 4.2.3 (1) の証明と同様にして，同一視

$$H^1(G_{\mathbb{Q}}, E[\varphi]; S) \simeq \mathbb{Q}(S, 2)$$

が得られる．したがって，注意 4.2.4(2) により，

$$\begin{aligned}\mathrm{Sel}^{(\varphi)}(E/\mathbb{Q}) &= \{d \in \mathbb{Q}(S,2) \mid \text{すべての } p \in S \text{ に対して } C_d(\mathbb{Q}_p) \neq \emptyset\} \\ E'(\mathbb{Q})/\varphi(E(\mathbb{Q})) &= \{d \in \mathbb{Q}(S,2) \mid C_d(\mathbb{Q}) \neq \emptyset\}\end{aligned}$$

となる．ただし，C_d は $d \in \mathbb{Q}(S,2)$ を

$$\mathbb{Q}(S,2) \simeq H^1(G_{\mathbb{Q}}, E[\varphi]; S) \to H^1(G_{\mathbb{Q}}, E(\bar{\mathbb{Q}})) = \mathrm{WC}(E/\mathbb{Q})$$

で送って得られる E-torsor である．$\hat{\varphi}$ についても同様の議論を行うことで，$\mathrm{Sel}^{(\hat{\varphi})}(E'/\mathbb{Q})$ と $E(\mathbb{Q})/\hat{\varphi}(E'(\mathbb{Q}))$ に関する同様の記述が得られる．

注意 4.3.3. C_d は $\mathbb{P}^2_{\mathbb{Q}}$ 内の曲線として次の定義方程式で与えられる：

$$C_d \colon dw^2 = d^2 - 2adz^2 + (a^2 - 4b)z^4.$$

4.3.3 $|E[2](\mathbb{Q})| = 1$ のとき

この場合，general 2-descent と呼ばれる手法を使う．ここで述べるものは [1] を参考にしたかなり大雑把な説明である．より詳しく知りたい場合は，[4] を参照せよ．

仮定により，E の定義方程式は $y^2 = f(x)$ （$f(x) \in \mathbb{Q}[x]$ は既約 3 次式）と書ける．$f(x)$ の根の一つを θ とかき，$L = \mathbb{Q}(\theta)$ とおく．このとき，写像

$$\begin{aligned} f \colon E(\mathbb{Q})/2E(\mathbb{Q}) &\hookrightarrow L^\times/(L^\times)^2 \\ 0 &\mapsto 1 \bmod (L^\times) \\ (x,y)(\neq 0) &\mapsto x - \theta \bmod (L^\times)\end{aligned}$$

は群の単射準同形を定める．L の素点の有限集合 S を適当にとることにより，f は

$$T := L(S,2) \cap \ker(N_{L/\mathbb{Q}}) \subset L^\times/(L^\times)^2$$

を経由する．ただし，

$$L(S,2)=\{a\in L^\times/(L^\times)^2 \mid v\notin S \text{ に対して } \mathrm{val}_v(a)\equiv 0 \bmod 2\}$$

とおき，$N_{L/\mathbb{Q}}\colon L^\times/(L^\times)^2\to\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ をノルム写像とした．

さて，$E(\mathbb{Q})/2E(\mathbb{Q})$ を T からどのように切り出すかについて大まかな方針を述べる：すなわち，$\delta=a+b\theta+c\theta^2\in L^\times$ が与えられたとして，$\bar{\delta}=\delta \bmod (L^\times)^2\in T$ が $E(\mathbb{Q})/2E(\mathbb{Q})$ に属するか否かを調べる方法を述べる．

f によって $E(\mathbb{Q})/2E(\mathbb{Q})$ を T の部分集合とみなしているので，

$$x-\theta=\delta z^2 \tag{4.3}$$

を満たす $z=u+v\theta+w\theta^2\in L^\times$（$u,v,w\in\mathbb{Q}$）と $x\in\mathbb{Q}$ が存在するか否かが問題となる．ここで u,v,w を未知数と考えて

$$\begin{aligned}\delta z^2&=(a+b\theta+c\theta^2)(u+v\theta+w\theta^2)\\&=q_0(u,v,w)-q_1(u,v,w)\theta+q_2(u,v,w)\theta^2\end{aligned}$$

（q_0,q_1,q_2 は u,v,w に関する二次形式）と表示する．すると，(4.3) をみたす $x,z=u+v\theta+w\theta^2$ が存在するかどうかは，

$$x=q_0(u,v,w), 1=q_1(u,v,w), 0=q_2(u,v,w)$$

の有理数解 x,u,v,w の存在問題と同値である．x は $1=q_1(u,v,w),0=q_2(u,v,w)$ の解を用いて $x=q_0(u,v,w)$ と置けばよいので，結局 $\bar{\delta}\in E(\mathbb{Q})/2E(\mathbb{Q})$ かどうかは

$$1=q_1(u,v,w),\quad 0=q_2(u,v,w) \tag{4.4}$$

の有理数解の存在問題に帰着する．

まず，$0=q_2(u,v,w)$ の解を見付けることは常に可能であることが知られる．その解のひとつを $(u_0.v_0,w_0)$ とし $z_0=u_0+v_0\theta+w_0\theta^2$ とおく．

次に，(4.3) の代わりに，z_0 を用いて (4.3) を修正した方程式

$$x-\theta=\delta z_0^2(u'+v'\theta+w'\theta^2)^2 \tag{4.5}$$

を考える．すなわち，（(4.3) ではなく！）(4.5) の有理数解 x,u',v',w' の存在問題を考える．(4.3) から (4.4) を導いたのと同様にして，(4.5) から適当な二次形式 $Q_1(u',v',w'),Q_2(u',v',w')$ に関する方程式

$$1=Q_1(u',v',w'),\quad 0=Q_2(u',v',w') \tag{4.6}$$

が得られ, (4.6) の有理数解の存在問題に帰着される．方程式 $0 = Q_2(u', v', w')$ の解は，($0 = q_2(u, v, w)$ のときよりも強く）3 変数でパラメトライズされることが分かる．その解をパラメータ X, Y, Z を用いて $u' = u'(X, Y, Z), v' = v'(X, Y, Z), w' = w'(X, Y, Z)$ と書き $Q_1(u', v', w')$ に代入すれば，方程式 $1 = Q_1(u', v', w')$ は $\mathbb{P}^2$ 内の種数 1 の曲線 $C = C_{\bar{\delta}}$ を定める．この C について，$C(\mathbb{Q}) \neq \emptyset$ であることと $\bar{\delta} \in E(\mathbb{Q})/2E(\mathbb{Q})$ であることが同値となる．また,

$$\mathrm{Sel}^{(2)}(E/\mathbb{Q}) = \{\bar{\delta} \in T \mid \text{各素点 } p \text{ に対して } C(\mathbb{Q}_p) \neq \emptyset\}$$

であることも分かる.

参考文献

[1] 木田雅成，長尾孝一，楕円曲線の *Moedell-Weil* 群について，日本応用数理学会論文誌，Vol. 13, No.2 2003, pp. 257-271.

[2] J. S. Milne, *Elliptic Curves*, available at http://www.jmilne.org/math/Books/ectext5.pdf

[3] J. H. Silverman, *The arithmetic of elliptic curves*, Vol. 106. Springer Science & Business Media, 2009.

[4] D. Simon, *Computing the rank of elliptic curves over number fields*, LMSJ. Comput. Math. 5(2002), 7-17(electronic).