第3章

楕円曲線のreductionについて

加川 貴章 (早稲田大学 理工学部)

楕円曲線のreductionの基本的なことを羅列しておく. 証明を与える余裕は無いので, 必要があれば文献を参照されたい. いくつか例を載せておいたが, (我が師足立恒雄先生が常日頃言っておられるように) 任意の教科書に載っている例を再掲しても意味が無いと思うので, 日常の研究で出会った例で, テキストなどであまり見かけない例を中心にしてみた.

§1. 局所体上の楕円曲線のreduction

ここでは特に断らない限り次の記号を使う:

K	局所体,
v_K	K の正規離散付値,
$\mathcal{O}_K$	K の付値環,
$\mathfrak{p}_K$	K の最大イデアル,
π_K	$\mathcal{O}_K$ の素元の一つ, 即ち $\mathfrak{p}_K$ の生成元の一つ,
$k = \mathcal{O}_K/\mathfrak{p}_K$	$\mathcal{O}_K$ の剰余体 (有限体).

$a \in \mathcal{O}_K$ に対し, $\tilde{a} := a + \mathfrak{p}_K \in k$ とする.
また簡単のため, 変数変換

$$x = u^2X + r,\ y = u^3Y + u^2sX + t$$

を $[u, r, s, t]$ と略す. (別に標準的な記号というわけではない. 現に [6] では $T(r, s, t, u)$ になっている.)

§1.1. Reduction

E を Weierstraß方程式

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (a_1, a_2, a_3, a_4, a_6 \in K)$$

で K 上定義される楕円曲線, Δ をその方程式の判別式とする. 適当な変数変換で $a_i \in \mathcal{O}_K$ $(i = 1, 2, 3, 4, 6)$ と出来る (n を十分大きく取って $[u, r, s, t] = [\pi_K^n, 0, 0, 0]$ を考えればよい).

定義 1.1. 条件 $a_i \in \mathcal{O}_K$ $(i = 1, 2, 3, 4, 6)$ の下で $v_K(\Delta)$ が最小である E の K 上の定義方程式を, E の minimal な (Weierstraß) 方程式と言う.

命題 1.2. (1) K 上定義された任意の楕円曲線 E に対し, minimal な方程式が存在する. もとの方程式の係数が $\mathcal{O}_K$ に属していれば, minimal な方程式にうつす変換 $[u, r, s, t]$ において $u, r, s, t \in \mathcal{O}_K$ に取れる.

(2) E の 2 つの minimal な方程式は変数変換 $[u,r,s,t]$ ($u \in \mathcal{O}_K^\times$, $r,s,t \in \mathcal{O}_K$) でうつりあう. 特に $v_K(\Delta)$ は E の K-同型類に対し一意的に決まる.

Weierstraß方程式が minimal かどうかには, 係数 a_i と判別式 Δ と通常通り定義された c_4 を用いる簡単な判定条件

$$a_i \in \mathcal{O}_K \text{ かつ, } v_K(\Delta) < 12 \text{ または } v_K(c_4) < 4 \Longrightarrow \text{minimal}$$

がある. $\mathrm{char}(k) \neq 2,3$ の時は逆も言える ($y^2 = x^3 - 27c_4x - 54c_6$ で考えれば容易) ので, この時は minimal な方程式は容易に求まる. $\mathrm{char}(k)$ が 2 または 3 の時に minimal な方程式を求めるには Tate のアルゴリズムを使えばよい. (Tate のアルゴリズムについては [18] を参照されたい. [3], [15] も見よ. 実際に手でアルゴリズムに従った計算をするなら, 日本語で書かれた [19] が役に立つ.) Minimal かどうかの判定だけなら, 次の Kraus ([12]. [5] も見よ) の結果を使うとより簡単に出来る:

定理 1.3 (Kraus). $p = 2$ または 3 とし, K を $\mathbf{Q}_p$ の有限次拡大とする. $C_4, C_6 \in \mathcal{O}_K$ が

$$\frac{C_4^3 - C_6^2}{1728} \in \mathcal{O}_K \backslash \{0\}$$

を満たすとする. この時 $\mathcal{O}_K$ 係数の Weierstraß方程式で $c_4 = C_4$, $c_6 = C_6$ を満たすものが存在するための必要十分条件は, 次が成立することである:

(1) ($p = 2$ の時)
  (a) $C_4 \in \mathcal{O}_K^\times$ の時, $-C_6$ は mod 4 の平方数; または
  (b) $0 < v_K(C_4) < v_K(16)$ の時, 次のような $x \in \mathcal{O}_K$ が存在する: $P(X) = -X^6 + 3C_4X^2 + 2C_6$ とする時, $4x^2P(x) \equiv (x^4 - C_4)^2 \pmod{2^8}$, $16 \mid P(x)$, かつ $P(x)/16$ が mod 4 で平方数; または
  (c) $C_4 \equiv 0 \pmod{16}$ の時, $C_6 \equiv 8x^2 \pmod{32}$ となる $x \in \mathcal{O}_K$ が存在する.

(2) ($p = 3$ の時)
  (a) $C_6 \in \mathcal{O}_K^\times$; または
  (b) $0 < v_K(C_6) < v_K(27)$ かつ $x^3 - 3C_4x - 2C_6 \equiv 0 \pmod{27}$ であるような $x \in \mathcal{O}_K$ が存在する; または
  (c) $C_6 \equiv 0 \pmod{27}$.

系 1.4 (Mestre). p を 2 または 3 とする. $C_4, C_6 \in \mathbf{Z}_p$ が

$$\frac{C_4^3 - C_6^2}{1728} \in \mathbf{Z}_p \backslash \{0\}$$

を満たすとする. この時 $\mathbf{Z}_p$ 係数の Weierstraß方程式で $c_4 = C_4$, $c_6 = C_6$ を満たすものが存在するための必要十分条件は次が成立することである:

(1) ($p = 2$ の時) $C_6 \equiv -1 \pmod 4$; または $C_4 \equiv 0 \pmod{16}$, $C_6 \equiv 0, 8 \pmod{32}$.
(2) ($p = 3$ の時) $C_6 \not\equiv \pm 9 \pmod{27}$.

例 1.5. (1) E を

$$y^2 = x(x + 3^2)(x - 4^2)$$

で定義された楕円曲線とすると, $\Delta = 2^{12}\cdot 3^4\cdot 5^4$, $c_4 = 2^4\cdot 13\cdot 37$, $c_6 = 2^6\cdot 7\cdot 17\cdot 41$. この方程式は $\mathbf{Q}_2$ 上 minimal でない. 実際 $c_4 = 13\cdot 37$, $c_6 = 7\cdot 17\cdot 41$ なる $\mathbf{Z}_2$ 上の E の定義方程式の存在は系 1.4 よりわかる ($[u,r,s,t] = [2,4,1,4]$ なる変換で minimal な方程式 $y^2+xy+y = x^3+x^2-10x-10$, $\Delta = 3^4\cdot 5^4$ にうつる).

(2) (1) の曲線の twist である

$$E^{(-1)} : y^2 = x(x-3^2)(x+4^2)$$

は, $\Delta = 2^{12}\cdot 3^4\cdot 5^4$, $c_4 = 2^4\cdot 13\cdot 37$, $c_6 = -2^6\cdot 7\cdot 17\cdot 41$ であるにも関わらず $\mathbf{Q}_2$ 上 minimal である. 実際, $c_4 = 13\cdot 37$, $c_6 = -7\cdot 17\cdot 41$ である $\mathbf{Z}_2$ 係数の Weierstraß 方程式は系 1.4 より存在しない. ([1] の符号の取り方はおかしい. そこでは $E^{(-1)}$ を考えているが, 正しくは (1) の E を考えなくてはならない. [2] の符号の取り方も同様に間違っている.)

(3) $\mathbf{Q}_3$ 上定義された

$$E : y^2+xy+y = x^3-x^2+25x+1$$

は, $\Delta = -2\cdot 3^{12}$, $c_4 = -3^5\cdot 5$, $c_6 = -3^8$ であるが $\mathbf{Q}_3$ 上 minimal である. 実際, $c_4 = -3\cdot 5$, $c_6 = -3^2$ である $\mathbf{Z}_3$ 係数の Weierstraß 方程式が存在しないことは系 1.4 よりわかる.

系 1.4 の条件を満たす C_4, C_6 から Weierstraß 方程式を回復する方法は本文の最後に載せておいた.

注. Δ を minimal な方程式の判別式とする. $j(E)\in\mathcal{O}_K$ なら $v_K(\Delta) < 12+12v_K(2)+6v_K(3)$ が成り立つことも知られている.

定義 1.6. E を K 上定義された楕円曲線とする.

(1) E の minimal な方程式の係数を $\mathfrak{p}_K$ を法として考えた k 上の曲線 $\tilde{E}$ を E の reduction と言う:

$$\tilde{E} : y^2+\tilde{a}_1xy+\tilde{a}_3y = x^3+\tilde{a}_2x^2+\tilde{a}_4x+\tilde{a}_6.$$

(Reduction は方程式ごとではなく, E の K-同型類ごとに決めることに注意. また E の reduction $\tilde{E}$ は k 上の同型を除いて unique に定まる.)

(2) $\tilde{E}$ が特異点を持たない時, 即ち $\tilde{E}$ が楕円曲線である時, E は K 上 **good reduction** (または **stable reduction**) を持つと言う.

(3) $\tilde{E}$ が特異点を持つとき, E は K 上 **bad reduction** を持つと言う. より詳しく, $\tilde{E}$ が cusp を持つとき, **additive reduction** (または **unstable reduction**) を持つ, $\tilde{E}$ が node を持つとき, **multiplicative reduction** (または **semi-stable reduction**) を持つと言う. Node での接線の傾きが k の元の時 **split multiplicative reduction** を, そうでない時 **non-split multiplicative reduction** を持つと言う.

Multiplicative reduction について若干補足をしておく.

$$\tilde{E} : \tilde{f}(x,y) = y^2+\tilde{a}_1xy+\tilde{a}_3y-(x^3+\tilde{a}_2x^2+\tilde{a}_4x+\tilde{a}_6) = 0$$

を K 上定義された楕円曲線 E の reduction とする. E が K 上 multiplicative reduction を持つとし, (x_0, y_0) を $\tilde{E}$ の node とする. この時

$$f(x,y) - f(x_0,y_0) = \{(y-y_0) - \alpha(x-x_0)\}\{(y-y_0) - \beta(x-x_0)\} - (x-x_0)^3$$
$$(\alpha, \beta \in \bar{k},\ \alpha \neq \beta)$$

と書ける. (x_0, y_0) での接線は $(y-y_0) - \alpha(x-x_0) = 0$, $(y-y_0) - \beta(x-x_0) = 0$ であった. $\alpha, \beta \in k$ の時が split multiplicative reduction, $\alpha, \beta \notin k$ の時が non-split multiplicative reduction である.

注. Good reduction と multiplicative reduction を合わせて semi-stable と言うこともある.

注. $\tilde{E}$ が supersingular (ordinary) な楕円曲線の時, すなわち $\tilde{E}[p] = \{O\}$ $(\#\tilde{E}[p] = p)$ の時, E は supersingular (ordinary) reduction を持つと言う. これらも大事な概念だが, ここでは扱わない.

命題 1.7. E の minimal な方程式の判別式を Δ とし, c_4, c_6 をその方程式に付随する通常通りの量とする. また $\tilde{E}_{\mathrm{ns}}(\bar{k}) = \{P \in \tilde{E}(\bar{k}) \mid P \text{ は非特異}\}$ とおく.

(1) E が K 上 good reduction を持つことと $v_K(\Delta) = 0$ は同値である.

(2) E が K 上 multiplicative reduction を持つことと $v_K(\Delta) > 0$, $v_K(c_4) = 0$ は同値である. この時 $\tilde{E}_{\mathrm{ns}}(\bar{k}) \cong \bar{k}^\times$ である (multiplicative reduction の名前の由来).

(3) E が K 上 additive reduction を持つことと $v_K(\Delta) > 0$, $v_K(c_4) > 0$ は同値である. この時 $\tilde{E}_{\mathrm{ns}}(\bar{k}) \cong \bar{k}^+$ ($\bar{k}$ の加法群) である (additive reduction の名前の由来).

注. 従って E が multiplicative reduction を持てば, $v_K(j) = -v_K(\Delta) < 0$ (乗法付値の言葉で言えば $|j| = |\Delta|^{-1} > 1$) である.

例 1.8. (1) $\mathbf{Q}_3$ 上定義された楕円曲線

$$E : y^2 = x(x+3^2)(x-4^2)$$

は non-split multiplicative reduction を持つ. E が $\mathbf{Q}_5$ 上定義されていると思った時は split multiplicative reduction を持つ. また, $\mathbf{Q}_2$ 上の楕円曲線と思った時は good reduction を持つ.

(2) $\mathbf{Q}_3$ (または $\mathbf{Q}_5$) 上定義された楕円曲線

$$E : y^2 = x(x-3^2)(x+4^2)$$

は split multiplicative reduction を持つ. E を $\mathbf{Q}_2$ 上の楕円曲線と思った時は additive reduction を持つ. (mod 2 すると $y^2 = x^2(x+1)$ となるので, $\mathbf{Q}_2$ 上 multiplicative reduction を持つように見えるかもしれないが, $(y-x)^2 = x^3$ と書けば additive reduction を持つのがわかるであろう.)

Stable 等の名前は次に由来する:

定理 1.9 (semi-stable reduction theorem). E を K 上定義された楕円曲線とする.

(1) L/K が不分岐拡大ならば, E の K 上の reduction の種類と, L 上の reduction の種類は等しい.

(2) L/K を有限次拡大とする. E が K 上 good reduction, または multiplicative reduction を持つならば, E は L 上同じ種類の reduction を持つ.

(3) K のある有限次拡大体 L において, E は L 上 good reduction か (split) multiplicative reduction を持つ.

この定理の証明の方針は次の通りである.

(1) L/K が不分岐なら $v_K(c_4) = v_L(c_4)$, $v_K(\Delta) = v_L(\Delta)$ であるから主張は自明である.

(2) $v_K(\Delta) = 0$ ($v_K(c_4) = 0$) なら, L/K がどんな拡大でも $v_L(\Delta) = 0$ ($v_L(c_4) = 0$) だから, K 上 good (multiplicative) reduction を持てば L 上でもそのままである.

(3) $\mathrm{char}(k) \neq 2$ の時, 標準形 $y^2 = x(x-1)(x-\lambda)$ ($\lambda \neq 0, 1$) を使えば, 十分大きな体 L で $v_L(c_4) = 0$ または $v_L(\Delta) = 0$ と出来ることが示せる. $\mathrm{char}(k) = 2$ の時は Deuring normal form $y^2 + \alpha xy + y = x^3$ ($\alpha^3 = 27$) を使えば同様に証明できる.

定義 1.10. K 上定義された楕円曲線 E が, K のある有限次拡大体上で good reduction を持つとき, E は **potential good reduction を持つ**と言う.

命題 1.11. K 上定義された楕円曲線 E が potential good reduction を持つことと, $j(E) \in \mathcal{O}_K$ は同値である.

これの証明もそんなに難しくない. 然るべき体 L 上で good reduction を持てば, E は $c_4 \in \mathcal{O}_L$, $\Delta \in \mathcal{O}_L^\times$ なる方程式で定義されるから, $j(E) = c_4^3/\Delta \in K \cap \mathcal{O}_L = \mathcal{O}_K$ である. 逆に ($\mathrm{char}(k) \neq 2$ の時) $E : y^2 = x(x-1)(x-\lambda)$ ($\lambda \neq 0, 1$, λ は K のある有限次拡大体 L の元) とした時, $j(E) = 2^8(\lambda^2 - \lambda + 1)^3/(\lambda(\lambda-1))^2$ であるから, $j(E) \in \mathcal{O}_K$ より $\lambda \in \mathcal{O}_L$, $\lambda \not\equiv 0, 1 \pmod{\mathfrak{p}_L}$ がすぐわかる. これは E が L 上 good reduction を持つことを意味する. ($\mathrm{char}(k) = 2$ の時はやはり Deuring normal form を使う.)

§1.2. 有限位数の点

$P \in E(K)$ とする. P を斉次座標で $P = (x : y : z) \in \mathbf{P}^2(K)$ ($x, y, z \in K$) と書いた時, π_K の適当な冪を掛けて $x, y, z \in \mathcal{O}_K$ で, いずれか一つは $\mathcal{O}_K$ の単数に取れる. この時 P の reduction $\tilde{P} \in \tilde{E}(k)$ を $\tilde{P} = (\tilde{x} : \tilde{y} : \tilde{z})$ で定義する. $P \in E(K)$ に reduction $\tilde{P} \in \tilde{E}(k)$ を対応させることにより reduction map が得られる:

$$\tilde{}: E(K) \to \tilde{E}(k),\ P \mapsto \tilde{P}.$$

定理 1.12. E を K 上定義された楕円曲線とする. また $p = \mathrm{char}(k)$ とする.

(1) $v_K(p) < p - 1$ かつ E が K 上 good reduction を持てば, reduction map $E(K)_{\mathrm{tors}} \to \tilde{E}(k)$ は単射準同型である. ここに $E(K)_{\mathrm{tors}} = \{P \in E(K) \mid P \text{ は有限位数}\}$.

(2) m を p と互いに素 (即ち $v_K(m) = 0$) な自然数とする. E が K 上 good reduction を持てば, reduction map $E(K)[m] \to \tilde{E}(k)$ は単射準同型である.

上の定理は global field 上の楕円曲線の torsion subgroup を求めるのに役立つ．このうち (1) は有名な事実にも関わらず, [14] には出ていない．(1) のつもりで (2) ([14], Chapter VII の Proposition 3.1) を引用している人が多いようだが, これは明らかな間違いである．

例 1.13. Silverman の本 [14] (の最初の頃のもの) に出ている

$$E : y^2 + y = x^3 - x + 1$$

の torsion subgroup を求める例 (Chapter VII の Example 3.3.1) は間違っている (最近売られているものは直っている)．実際そこでは $\tilde{E}(\mathbf{F}_2) = \{O\}$ から定理 1.12 (2) を使って torsion-free であることを導いているが, これでは位数が 2 冪でない点が存在しないことが言えただけである．

(2) は Mordell–Weil の定理の証明にも使われることを注意しておく．

§1.3. Néron–Ogg–Shafarevich の criterion

定義 1.14. $\bar{K}$ を K の代数的閉包, Σ を $\mathrm{Gal}(\bar{K}/K)$ が作用する集合とする．惰性群 $I \subset \mathrm{Gal}(\bar{K}/K)$ が Σ に自明に作用する (しない) 時, Σ は不分岐である (分岐する) という．

E が K 上 good reduction を持つ時, $\mathrm{char}(k)$ と素な $m \in \mathbf{N}$ に対し, $E[m]$ が不分岐であることが定理 1.12 (2) から次のように従う．

必要なら体を拡大して $E[m] \subset E(K)$ としてよい．$P \in E[m]$, σ を惰性群の元とする．惰性群は剰余体に自明に作用するから $\widetilde{P^\sigma - P} = \tilde{P}^\sigma - \tilde{P} = O$. $P^\sigma - P \in E(K)[m]$ であること, E は K' 上 good reduction を持つこと (定理 1.9 (2)) から定理 1.12 (2) が使えて, $P^\sigma = P$ が得られる．

実はこれの逆を含めたより詳しい結果が成り立つ:

定理 1.15 (Néron–Ogg–Shafarevich の criterion). E を K 上定義された楕円曲線とする時, 次の 4 条件は同値である．

(1) E は K 上 good reduction を持つ．
(2) $\mathrm{char}(k)$ と素な全ての自然数 m に対し, $E[m]$ は不分岐である．
(3) $\mathrm{char}(k)$ と異なるある (全ての) 素数 l に対し, Tate 加群 $T_l(E)$ は不分岐である．
(4) $\mathrm{char}(k)$ と素な無限に多くの自然数 m に対し, $E[m]$ は不分岐である．

これから得られることとして次がある:

系 1.16. K 上定義された楕円曲線 E, E' が K 上 isogenous ならば, E, E' は K 上共に good reduction を持つか, 共に bad reduction を持つかのどちらかである．

証明. $\phi : E \to E'$ を K 上定義された $\phi(E) = \{O_{E'}\}$ でない isogeny, $m \geq 2$ を $\mathrm{char}(k)$ とも $\deg \phi$ とも素な整数とする．$\phi : E[m] \to E'[m]$ は $\mathrm{Gal}(\bar{K}/K)$-加群としての同型写像である．よって $E[m], E'[m]$ は共に不分岐であるか, 共に分岐するかである．故に主張は定理

1.15 の (1), (4) の同値性から従う.

§2. 代数体上の楕円曲線の reduction

ここでは特に断らない限り次の記号を使う:

K 有限次代数体,
$\mathcal{O}_K$ K の整数環,
$K_\mathfrak{p}$ K の素イデアル $\mathfrak{p}$ における完備化,
$v_\mathfrak{p}$ K の素イデアル $\mathfrak{p}$ における正規離散付値.

§2.1. $\mathfrak{p}$ における reduction

定義 2.1. E を K 上定義された楕円曲線とする. また $\mathfrak{p}$ を K の素イデアルとする.

(1) E の定義方程式が $K_\mathfrak{p}$ 上定義されていると思った時に minimal である時, その方程式は $\mathfrak{p}$ において minimal であると言う.

(2) E を $K_\mathfrak{p}$ 上定義された楕円曲線と思った時の reduction を E の $\mathfrak{p}$ における **reduction** (**reduction modulo $\mathfrak{p}$**) と言い, $E_\mathfrak{p}$ と書くことにする (これも別に標準的な記号というわけではない. $\tilde{E}$ では $\mathfrak{p}$ がわからないので, こっちの方がいいと思うのだが).

(3) E が $K_\mathfrak{p}$ 上 good reduction を持つ時, E は $\mathfrak{p}$ において good reduction を持つと言う. Bad reduction, additive reduction など, 他の場合も同様に言う.

(4) E が $\mathfrak{p}$ において good (bad) reduction を持つ時, $\mathfrak{p}$ を E に対する **good (bad) prime** と言う.

Weierstraß方程式が全ての素イデアルにおいて同時に minimal である時, その方程式は global minimal であるという. Global minimal な方程式の判別式の素因子は bad prime のみである. そんな方程式が存在すれば, 一気に reduction が出来て便利なのだが, global minimal な方程式は必ずしも存在しない. 以下で存在するかどうかを判定する方法を与える.

E を K 上定義された楕円曲線, Δ をその定義方程式の判別式とする. 素イデアル $\mathfrak{p}$ に対し, $\Delta_\mathfrak{p}$ を $\mathfrak{p}$ において minimal である E の定義方程式の判別式とし, $\Delta = u_\mathfrak{p}^{12}\Delta_\mathfrak{p}$ ($u_\mathfrak{p} \in K^\times$) とする. この時 E の minimal discriminant $\mathcal{D}_{E/K}$ を全素イデアルに渡る積

$$\mathcal{D}_{E/K} = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(\Delta_\mathfrak{p})}$$

で定義する. また分数イデアル $\mathfrak{a}_\Delta$ を

$$\mathfrak{a}_\Delta = \prod_\mathfrak{p} \mathfrak{p}^{-v_\mathfrak{p}(u_\mathfrak{p})}$$

で定義する. 両者は次の関係で結ばれている:

$$\mathcal{D}_{E/K} = (\Delta)\mathfrak{a}_\Delta^{12}.$$

補題 2.2. $\mathfrak{a}_\Delta$ の属するイデアル類は E の K-同型類のみで決まる (Δ によらない).

実際, $\Delta = u^{12}\Delta'$ ならば, $\mathfrak{a}_{\Delta'} = (u)\mathfrak{a}_{\Delta}$ であることが容易に示せる.

定義 2.3. $\mathfrak{a}_{\Delta}$ の属するイデアル類を $\bar{\mathfrak{a}}_{E/K}$ と書き, E/K の Weierstraß class と呼ぶ.

命題 2.4. E の global minimal な方程式が存在することと, Weierstraß class $\bar{\mathfrak{a}}_{E/K}$ が単位類であることは同値である.

実際 E が global minimal な方程式で定義されていれば $\mathfrak{a}_{\Delta} = (1)$ が容易にわかり, 逆に $\mathfrak{a}_{\Delta} = (u^{-1})$ とする時, E を global minimal な方程式にうつす $[u, r, s, t]$ の u がこの u に取れるのである.

例 2.5. (1) K の類数が 1 ならば, K 上定義された全ての楕円曲線は global minimal な方程式で定義され得る.

(2) K 上定義された楕円曲線 E が K の全素イデアルで good reduction を持つ (everywhere good reduction を持つ) 時, すなわち $\mathcal{D}_{E/K} = (1)$ である時, K の類数が 6 と素ならば global minimal な方程式で定義され得る. ([7], [8], [9], [11] 等で "類数が 6 と素" がしばしば仮定されているのはこれが理由である.)

例 2.6. $K = \mathbf{Q}(\sqrt{26})$, $(2) = \mathfrak{p}^2$ とすると, K のイデアル類群は $\mathfrak{p}$ の類で生成される位数 2 の巡回群である (特に $\mathfrak{p}$ は単項イデアルではない). $\varepsilon = 5 + \sqrt{26}$ を K の基本単数とし,

$$E : y^2 = x^3 - (1 + \sqrt{26})x^2 + (26 + 4\sqrt{26})x - (232 + 46\sqrt{26})$$

とする. $c_4 = -2^4\varepsilon^2$, $\Delta = -2^6\varepsilon^6$ ($\varepsilon = 5 + \sqrt{26}$ は K の基本単数) なので, minimal でない可能性があるのは $\mathfrak{p}$ の所だけである. 実際に minimal でないことは $[u, r, s, t] = [u_{\mathfrak{p}}, r_{\mathfrak{p}}, s_{\mathfrak{p}}, t_{\mathfrak{p}}] = [\sqrt{26}, \sqrt{26}, 1, 26 + \sqrt{26}]$ により $\mathfrak{p}$ における minimal な方程式

$$y^2 + \frac{\sqrt{26}}{13}xy + \frac{1 + \sqrt{26}}{13}y = x^3 + \frac{-1 + \sqrt{26}}{13}x^2 - \frac{107 + 9\sqrt{26}}{13^3}, \ \Delta = -\frac{\varepsilon^6}{13^6}$$

にうつることからわかる. よって $\mathcal{D}_{E/K} = (1)$ (everywhere good reduction) で, $\bar{\mathfrak{a}}_{E/K}$ は $\mathfrak{p}$ の類であり, これは単位類ではない. 従って E は global minimal な方程式では定義されない.

一方 E の twist

$$E^{(2)} : y^2 = x^3 - 2(1 + \sqrt{26})x^2 + 4(26 + 4\sqrt{26})x - 8(232 + 46\sqrt{26})$$

の判別式は $\Delta = -2^{12}\varepsilon^6$ (イデアルで言うと $(\Delta) = \mathfrak{p}^{24}$) であり, global minimal な方程式

$$y^2 + (1 - \varepsilon)xy - \varepsilon y = x^3 - \varepsilon x^2, \ \Delta = -\varepsilon^6$$

で定義される ($\bar{\mathfrak{a}}_{E/K}$ は $\mathfrak{p}^2 = (2)$ の類, 即ち単位類であることに注意).

§2.2. 導手

K 上定義された楕円曲線 E の導手 $N_{E/K}$ を

$$N_{E/K} = \prod_{\mathfrak{p}} \mathfrak{p}^{f_{\mathfrak{p}}(E/K)}$$

で定義する．ここに積は K の全素イデアルをわたり，指数 $f_{\mathfrak{p}}(E/K) \in \mathbf{N} \cup \{0\}$ は，Galois 表現または Néron model を用いて定義される．正確なところは省略する ([15] を見よ) が，結果として次のようになることが知られている:

$$f_{\mathfrak{p}}(E/K) = \begin{cases} 0 & (E \text{ が } \mathfrak{p} \text{ において good reduction を持つ時}), \\ 1 & (E \text{ が } \mathfrak{p} \text{ において multiplicative reduction を持つ時}), \\ 2+\delta_{\mathfrak{p}} & (E \text{ が } \mathfrak{p} \text{ において additive reduction を持つ時}). \end{cases}$$

$\delta_{\mathfrak{p}}$ は 0 以上の整数で，$\delta_{\mathfrak{p}} \leq 6v_{\mathfrak{p}}(2) + 3v_{\mathfrak{p}}(3)$ を満たすことが知られている．特に $(\mathfrak{p}, 6) = 1$ ならば $\delta_{\mathfrak{p}} = 0$ だから，2 でも 3 でもない素数の上にある素イデアル $\mathfrak{p}$ に対する $f_{\mathfrak{p}}$ の決定は容易である．2, 3 を割る素イデアル $\mathfrak{p}$ の場合の $f_{\mathfrak{p}}$ の決定は Tate のアルゴリズム ([18]. [3], [15], [19] も見よ) で出来る．

$N_{E/K}$ の素因子は bad prime のみであることを注意しておく．また，全素イデアルで高々 semi-stable であることと $N_{E/K}$ が square-free であることは同値である．

例 2.7. (1) 例 1.5, 1.8 より，$E : y^2 = x(x+3^2)(x-4^2)$ は導手 $3 \cdot 5$ である．

(2) 例 1.5, 1.8 より，$E^{(-1)} : y^2 = x(x-3^2)(x+4^2)$ の導手は $2^f \cdot 3 \cdot 5$ $(f \geq 2)$ の形であるが，f はすぐにはわからない．(Tate のアルゴリズムによれば $f = 4$ である.)

E と E' が K 上 isogenous である時，E と E' の導手を構成する素イデアルは等しい (系 1.16)．より強く次のことが成り立つ．

定理 2.8. 代数体 K 上定義された楕円曲線 E, E' が K 上 isogenous である時，E の導手と E' の導手は等しい．

与えられた導手を持つ楕円曲線 (の K-同型類) は有限個である．より一般に，S を K の素イデアルの有限集合とする時，S の外 good reduction を持つ楕円曲線は有限個である．またそれらは effective に求まる (Shafarevich)．それらをすべて尽くして K-isogeny class に分解することは大事な作業である．しかし effective に求まることと実際に求まることの gap は極めて大きい (この差異は例えば [7], [8], [9] 等を見ていただければわかると思う)．次の命題 (Néron–Ogg–Shafarevich の criterion を代数体の言葉で言い換えたもの) は実際に決定する時の第一歩目として大事な役割を果たす:

命題 2.9. E を代数体 K 上定義された楕円曲線とする．n を自然数とし，$K(E[n])$ を $E[n]$ の全ての点の x 座標と y 座標を K に添加した体とする．この時 $K(E[n])/K$ で分岐しうる素点は，無限素点，n の素因子，及び bad prime のみである．

例 2.10. $\mathbf{Q}$ 上導手 (1) の楕円曲線 (全ての素数で good reduction を持つ楕円曲線，と言っても同じ) が存在しないことを示す．(これは今日ではもちろん Wiles の定理に含まれている.)

そのような楕円曲線が存在するとし，それを E とする．E が位数 2 の有理点を持たないとすると，$\mathbf{Q}(E[2])/\mathbf{Q}(\sqrt{\Delta})$ は 2 の外不分岐な 3 次巡回拡大である ($E : y^2 = f(x)$ $(f(x) \in \mathbf{Z}[x]$ は三次式) とした時，$\mathbf{Q}(E[2])$ は $f(x)$ の最小分解体であること，及び $\mathbf{Q}(\sqrt{\Delta}) = \mathbf{Q}(\sqrt{\mathrm{disc}(f)})$ であることに注意)．しかし $\mathbf{Q}(\sqrt{\Delta}) = \mathbf{Q}, \mathbf{Q}(\sqrt{-1})$ はこのような拡大を持ち得ないことが

類体論でわかる. よって E は次のような方程式で定義される:

$$E : y^2 = x^3 + ax^2 + bx,\ \Delta = \pm 2^{12} = 2^4 b^2 (a^2 - 4b).$$

$\pm 2^8 = b^2(a^2 - 4b)$ を満たす $a, b \in \mathbf{Z}$ は $(a, b) = (0, \pm 4), (\pm 6, 8)$ のみで, 得られる楕円曲線はそれぞれ

$$\begin{aligned}
y^2 &= x^3 + 4x, & c_4 &= -2^6 3,\ c_6 = 0,\ \Delta = -2^{12},\\
y^2 &= x^3 - 4x, & c_4 &= 2^6 3,\ c_6 = 0,\ \Delta = 2^{12},\\
y^2 &= x^3 + 6x^2 + 8x, & c_4 &= 2^6 3,\ c_6 = 0,\ \Delta = 2^{12},\\
y^2 &= x^3 - 6x^2 + 8x, & c_4 &= 2^6 3,\ c_6 = 0,\ \Delta = 2^{12}.
\end{aligned}$$

(下の三つは $\mathbf{Q}$ 上同型である. これは $x^3 - 4x = (x-2)x(x+2)$, $x^3 + 6x^2 + 8x = x(x+2)(x+4)$, $x^3 - 6x^2 + 8x = (x-4)(x-2)x$ と書けばわかるであろう.) これらがすべて minimal であること, 即ち 2 で bad reduction を持つことは系 1.4 よりわかる.

[17] では, 上と同じような議論で, K が虚二次体で E の K 上の導手が自明ならば, E は global minimal な方程式で定義されないことが示されていて, その帰結として K の類数が 6 と素ならば導手が自明な楕円曲線が存在しないことが得られている. [4] は実二次体上導手が自明でかつ位数 2 の K-有理点ががある場合を考えている (上と同じように $\Delta = 2^{12}u = 2^4 b^2(a^2 - 4b)$ $(u \in \mathcal{O}_K^\times)$ を考えるわけだが, 実二次体の場合は単数群が無限であることから有理数体, 虚二次体の場合と違う困難が生じて面白い).

$\mathbf{Q}$ 上 everywhere good reduction を持つ楕円曲線はないが, 多くの実二次体上に例がある. 例えば先の $\mathbf{Q}(\sqrt{26})$ 上の例など. 他にも [4], [5], [7], [8], [9], [10], [11], [20] などに沢山出ている. しかし実二次体上 everywhere good reduction を持ち, しかも判別式が ± 1 の楕円曲線を筆者は知らない. Connell ([5]) も見たことがないと言っている.

問. そういう楕円曲線を見付けるか, 非存在を証明せよ.

§2.3. Reduction と isogeny

定理 2.11. 代数体 K 上定義された楕円曲線 E, E' に対し,

$$\begin{aligned}
&E, E' \text{ が } K \text{ 上 isogenous である}\\
\Longleftrightarrow\ &K \text{ の全ての素イデアル } \mathfrak{p} \text{ に対し } \#E_{\mathfrak{p}}(\mathcal{O}_K/\mathfrak{p}) = \#E'_{\mathfrak{p}}(\mathcal{O}_K/\mathfrak{p}).
\end{aligned}$$

定理の主張のうち $\Rightarrow$ は有限体上の楕円曲線の結果から従い, 比較的容易である. 他方逆向きは Faltings の結果による深いものである.

例 2.12. (1) 導手 $1225 = 5^2 7^2$ (であることを確かめよ) の曲線

$$\begin{aligned}
E &: y^2 + xy + y = x^3 + x^2 - 8x + 6,\\
E' &: y^2 + xy + y = x^3 + x^2 - 208083x - 36621194
\end{aligned}$$

を考える．素数 p を小さな方から走らせて $\#E_{(p)}(\mathbf{F}_p)$, $\#E'_{(p)}(\mathbf{F}_p)$ を求めると，一致し続けることが見て取れる．実は E と E' の間には $\mathbf{Q}$ 上定義された 37 次の isogeny が存在することが知られている (cf. [13])．

(2) $K=\mathbf{Q}(\sqrt{26})$ とし，例 2.6 の E, $E^{(2)}$ を考える．5 を割る K の素イデアル $\mathfrak{p}_5$ に対し，$\#E_{\mathfrak{p}_5}(\mathcal{O}_K/\mathfrak{p}_5)=7$, $\#E^{(2)}_{\mathfrak{p}_5}(\mathcal{O}_K/\mathfrak{p}_5)=5$ であるから，E と $E^{(2)}$ は K 上 isogenous ではない (定理 2.11)．またさらに $\#E_{\mathfrak{p}_7}(\mathcal{O}_K/\mathfrak{p}_7)=45$($\mathfrak{p}_7$ は 7 を割る K の素イデアル) であるから，定理 1.12 (1) より $E(K)_{\mathrm{tors}}=\{O\}$ がわかる．(なお $E^{(2)}(K)_{\mathrm{tors}}$ は $(8+2\sqrt{26}, 20+4\sqrt{26})$ で生成される位数 5 の巡回群である.)

(3) $E: y^2=x^3-27$ の torsion subgroup $E(\mathbf{Q})_{\mathrm{tors}}$ を求めたいとする．E の判別式は $-2^4\cdot 3^9$ だから，$p\geq 5$ なら定理 1.12 (1) が使える．$\#E_{(p)}(\mathbf{F}_p)$ を求めると以下のようになる:

$$\begin{aligned}
&\#E_{(5)}(\mathbf{F}_5)=6, && \#E_{(7)}(\mathbf{F}_7)=12, && \#E_{(11)}(\mathbf{F}_{11})=12,\\
&\#E_{(13)}(\mathbf{F}_{13})=12, && \#E_{(17)}(\mathbf{F}_{17})=18, && \#E_{(19)}(\mathbf{F}_{19})=12,\\
&\#E_{(23)}(\mathbf{F}_{23})=24, && \#E_{(29)}(\mathbf{F}_{29})=30, && \#E_{(31)}(\mathbf{F}_{31})=36, \ \ldots
\end{aligned}$$

全部 6 の倍数ですね．実は $\#E_{(p)}(\mathbf{F}_p)$ は 5 以上のどんな素数 p に対しても 6 の倍数である (これは，E が $E': y^2=x^3+1$ と $\mathbf{Q}$ 上 isogenous なこと，$E'(\mathbf{Q})_{\mathrm{tors}}\cong \mathbf{Z}/6\mathbf{Z}$ であること，および定理 2.11 から従う．ちなみに $E'=E/\langle(3,0)\rangle$ である.) 従って reduction を用いただけでは $\#E(\mathbf{Q})_{\mathrm{tors}}\mid 6$ 以上の情報は得られない．にも関わらず $\#E(\mathbf{Q})_{\mathrm{tors}}=2$ だから，torsion group を求めるのに $E_{(p)}(\mathbf{F}_p)$ を求めるだけでは一般には不十分である．[14] や [16] に出ている例では，いくつかの素数 p に対し $E_{(p)}(\mathbf{F}_p)$ を見るだけで $E(\mathbf{Q})_{\mathrm{tors}}$ が求まる例ばかりなので，reduction curve を見るだけで $E(k)_{\mathrm{tors}}$ が求まると勘違いされている方もいるようである．注意していただきたい．

問題. $K=\mathbf{Q}(\sqrt{7})$ とし，$\varepsilon=8+3\sqrt{7}$ を K の基本単数とする．

$$\begin{aligned}
&E_1: y^2+xy=x^3+4\varepsilon x^2-4\varepsilon x-(\varepsilon^3+2\varepsilon), && \Delta=\varepsilon^{-9},\\
&E_2: y^2+xy=x^3+4\varepsilon x^2+(6\varepsilon-80\varepsilon^2)x-(3044-48513\varepsilon), && \Delta=\varepsilon^{3},\\
&E_3: y^2+xy=x^3+4\varepsilon x^2+\varepsilon x, && \Delta=\varepsilon^{6}
\end{aligned}$$

とする時，$E_1(K)_{\mathrm{tors}}\cong\mathbf{Z}/2\mathbf{Z}$, $E_2(K)_{\mathrm{tors}}\cong\mathbf{Z}/4\mathbf{Z}$, $E_3(K)_{\mathrm{tors}}\cong\mathbf{Z}/2\mathbf{Z}\oplus\mathbf{Z}/2\mathbf{Z}$ であることを示せ．(E_1, E_2, E_3 は K 上 isogenous であることが示せるから，$\#(E_i)_{\mathfrak{p}}(\mathcal{O}_K/\mathfrak{p})$ $(i=1,2,3)$ は全ての素イデアル $\mathfrak{p}$ に対して等しい．従って定理 1.12 を用いただけでは $\#(E_i)_{\mathfrak{p}_7}(\mathcal{O}_K/\mathfrak{p}_7)=8$, $\#(E_i)_{\mathfrak{p}_{19}}(\mathcal{O}_K/\mathfrak{p}_{19})=20$ ($\mathfrak{p}_7$, $\mathfrak{p}_{19}$ はそれぞれ 7, 19 を割る K の素イデアル) からわかる $\#E_i(K)_{\mathrm{tors}}\leq 4$ 以上の情報は得られない.)

注. 上の E_1, E_2, E_3 に対し $(E_i)_{\mathfrak{p}_{19}}(\mathcal{O}_K/\mathfrak{p}_{19})\cong\mathbf{Z}/20\mathbf{Z}$ $(i=1,2)$, $(E_3)_{\mathfrak{p}_{19}}(\mathcal{O}_K/\mathfrak{p}_{19})\cong\mathbf{Z}/10\mathbf{Z}\oplus\mathbf{Z}/2\mathbf{Z}$ ($\mathfrak{p}_{19}$ は 19 を割る K の素イデアル) がわかる．よって K 上 isogenous なら $\#E(\mathcal{O}_K/\mathfrak{p})$ は一致する (定理 2.11) が，群構造までは一般には一致しない．

§3. Appendix 1: ソフトウェア

楕円曲線の計算をするためのソフトは沢山ある．筆者がよく使っているものを以下に挙げておく (その後に書いた URL より ftp で入手可能．但し Apecs は有料のソフト MAPLE

が必要. Upecs は UBASIC を必要とするが, UBASIC は free). 他にも Lidia 等色々あるようだが, 使ったことが無いしよく知らないので省略する.

Apecs	`ftp://math.mcgill.ca/pub/apecs`
Upecs	`ftp://math.mcgill.ca/pub/upecs`
mrank, mwrank	`ftp://euclid.ex.ac.uk/pub/cremona`
SIMATH	`ftp://ftp.math.uni-sb.de/pub/simath`
PARI/GP	`ftp://megrez.math.u-bordeaux.fr/pub/pari`

本文中にしばしば出てきた Tate のアルゴリズムは, 有理数体上でならば mrank, mwrank 以外のどれでも実行できる (mrank, mwrank はそれぞれ, 有理数体上定義された楕円曲線の rank, Mordell-Weil 群を計算するためのものである). 二次体上の Tate のアルゴリズムは SIMATH で実行できるが, bug が沢山あり中々思ったように動いてくれない (SIMATH の製作者達へは, 筆者や電気通信大の木田雅成さんが度々報告し, version up の度に直してもらっている. が, まだ bug が大分残っている). 梅垣氏の program (cf. [19]) は任意の代数体 (類数も任意) で Tate のアルゴリズムを実行してくれて, bug らしきものに出会ったことはない. 製作者の苦労が伺われる.

類数 1 の 2 次体上の場合に global minimal な方程式を求めるアルゴリズム (定理 1.3 を用いる) は Apecs に入っている

§4. Appendix 2: C_4, C_6 から曲線を復元する方法

$C_4, C_6 \in \mathbf{Z}$ が系 1.4 の条件 (1), (2) を満たすとする. この時 $c_4 = C_4, c_6 = C_6$ なる $\mathbf{Z}$ 係数の Weierstraß 方程式は次のようにして得られる (cf. [6]):

$$
\begin{aligned}
b_2 &= -c_6 \bmod 12 \in \{-5, \ldots, 6\};\\
b_4 &= (b_2^2 - c_4)/24;\\
b_6 &= (-b_2^3 + 36 b_2 b_4 - c_6)/216;\\
a_1 &= b_2 \bmod 2 \in \{0, 1\};\\
a_3 &= b_6 \bmod 2 \in \{0, 1\};\\
a_2 &= (b_2 - a_1)/4;\\
a_4 &= (b_4 - a_1 a_3)/2;\\
a_6 &= (b_6 - a_3)/4.
\end{aligned}
$$

例 1.5 (1) の場合は, これを使えば直ちに $c_4 = 13 \cdot 37$, $c_6 = 7 \cdot 17 \cdot 41$ なる $\mathbf{Z}$ 上の方程式 $y^2 + xy + y = x^3 + x^2 - 10x - 10$ が得られるが, 同 (2) の場合は, $c_4 = 13 \cdot 37$, $c_6 = -7 \cdot 17 \cdot 41$ なる方程式は $y^2 + xy + y = x^3 - (3/2)x^2 - 10x + (19/2)$ となり, $\mathbf{Z}$ 上の方程式ではなくなってしまう. 同 (3) の場合は, $c_4 = -3 \cdot 5$, $c_6 = -3^2$ なる方程式を求めようとすると $b_6 = -1/3$ となってしまう. 例 2.10 で $c_4 = \pm 12$, $c_6 = 0$ (従って $\Delta = \pm 1$) なる $\mathbf{Z}$ 上の方程式があるかどうか調べると, $b_4 = \mp 1/2$ となってしまい矛盾する.

系 1.4 の条件は, 上の計算が破綻しないための条件だったのである.

参考文献

[1] N. Adachi, On Pythagorean elliptic curves, *Proc. Japan Acad.* **70A** (1994), 226–229.

[2] N. Adachi, An application of Frey's idea to exponential Diophantine equations *Proc. Japan Acad.* **70A** (1994), 261–263.

[3] H. Cohen, *A Course in Computational Algebraic Number Theory*, G. T. M. **138**, Springer, 1986.

[4] S. Comalada, Elliptic curves with trivial conductor over quadratic fields, *Pacific J. Math.* **144** (1990), 233–258.

[5] I. Connell, Elliptic curve handbook, `ftp://math.mcgill.ca/pub/ECH1` より ftp で入手可能.

[6] J. E. Cremona, *Algorithms for Modular Elliptic Curves* (2nd ed.), Cambridge Univ. Press, 1997.

[7] T. Kagawa, Determination of elliptic curves with everywhere good reduction over $\mathbf{Q}(\sqrt{37})$, *Acta Arith.* **83** (1998), 253–269.

[8] 加川 貴章, 実二次体上至る所 good reduction を持つ楕円曲線, 研究集会「代数学と計算」

[9] T. Kagawa, Determination of elliptic curves with everywhere good reduction over real quadratic fields, *Arch. Math.*, to appear.

[10] 木田 雅成, 実二次体のあらゆる素点で good reduction を持つ楕円曲線の計算, 仙台数論小研究集会.

[11] M. Kida and T. Kagawa, Nonexistence of elliptic curves with good reduction everywhere over real quadratic fields, *J. Number Theory* **66** (1997), 201–210.

[12] A. Kraus, Quelques remarques à propos des invariants c_4, c_6 et Δ d'une courbe elliptique, *Acta Arith.* **54** (1989), 75–80.

[13] B. Mazur and P. Swinnerton-Dyer, Arithmetic of Weil curves, *Invent. Math.* **25** (1974), 1–61.

[14] J. H. Silverman, *The Arithmetic of Elliptic Curves*, G. T. M. 106, Springer, 1986.

[15] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, G. T. M. 151, Springer, 1994.

[16] J. H. シルヴァーマン, J. テイト (足立恒雄, 小松啓一, 木田雅成, 田谷久雄訳) 「楕円曲線論入門」シュプリンガー, 1995.

[17] R. J. Stroeker, Reduction of elliptic curves over imaginary quadratic number fields, *Pacific J. Math.* **108** (1983), 451–463.

[18] J. Tate, Algorithm for determining the type of a singular fibre in an elliptic pencil, in *Modular Functions of One Variable IV*, Lecture Notes in Math. no. 476, Springer, 1975, 33–52.

[19] 梅垣敦紀, 代数体上の楕円曲線の計算, 研究集会「代数学と計算」

[20] A. Umegaki, A construction of everywhere good $\mathbf{Q}$-curves with p-isogeny, *Tokyo J. Math.* **21** (1998), 183–200.