2.

体上の楕円曲線の一般論

工藤 桃成[*1]（九州大学マス・フォア・インダストリ研究所）

本稿は 2017 年 8 月 28 日（月）から 9 月 1 日（金）の期間に開催された第 25 回整数論サマースクール「楕円曲線とモジュラー形式の計算」における著者の講演「体上の楕円曲線の一般論」（8 月 28 日（月）14:00〜15:15，15:30〜16:05）の内容を纏めたものである．講演では，楕円曲線の定義や性質及び関連する概念について概説した．特に，本講演の次の講演以降で重要となる事項（楕円曲線の有理点のなす群の構造，モジュラー曲線の定義など）について重点的に解説した．

2.1　本稿の構成

講演では，

- 本サマースクールにおける楕円曲線に関連する話題を学ぶための準備
- 体上の楕円曲線に関して，よく知られている結果の復習，特に計算に関連する話題の紹介・導入

を目的とし，楕円曲線の定義や性質及び関連する概念について概説した．具体的には次の五つの項目（本稿の各節に対応）であった：

[*1] 講演時の所属：九州大学大学院数理学府

§1 楕円曲線の定義
§2 楕円曲線の有理点のなす群（Mordell-Weil 群）の構造
§3 複素数体上の楕円曲線
§4 楕円曲線の同種・同型
§5 本講演の次の講演以降で重要となる概念の導入（2 次元 Galois 表現，モジュラー曲線）

2.2 楕円曲線の定義

本節では，三次の射影平面曲線として楕円曲線を定義する．以下 K を体とし，記号 $\mathbf{A}^n(K)$ で K 上の n 次元アファイン空間 K^n を表す．

2.2.1 射影空間

定義 2.2.1 (射影空間)．集合 $\mathbf{A}^n(K) \smallsetminus \{(0,\dots,0)\}$ の二元 $(a_1,\dots,a_n)$, $(b_1,\dots,b_n)$ に対して，関係 $\sim$ を次で定める：ある $\lambda \in K^\times$ が存在して，$(b_1,\dots,b_n) = (\lambda a_1,\dots,\lambda a_n)$ を満たすとき $(a_1,\dots,a_n) \sim (b_1,\dots,b_n)$ と定義する．このとき，$\sim$ は集合 $\mathbf{A}^n(K) \smallsetminus \{(0,\dots,0)\}$ における同値関係である．商集合 $(\mathbf{A}^n(K) \smallsetminus \{(0,\dots,0)\})/\sim$ を体 K 上の n 次元射影空間 **(projective n-space)** と呼び，$\mathbf{P}^n(K)$ と書く．集合 $\mathbf{A}^n(K) \smallsetminus \{(0,\dots,0)\}$ の元 $(a_1,\dots,a_n)$ の $\mathbf{P}^n(K)$ における同値類を $[a_1 : \cdots : a_n]$ と書く．特に $n = 1$ のとき，$\mathbf{P}^1(K)$ を射影直線 **(projective line)** と呼び，$n = 2$ のとき，$\mathbf{P}^2(K)$ を射影平面 **(projective plane)** と呼ぶ．

$C_1 = \{[a : b : c] : c \neq 0\}$, $C_0 = \{[a : b : 0] : a, b \in K\} = \{[1 : b : 0] : b \in K\} \cup \{[0 : 1 : 0]\}$ とする．このとき，全単射 $C_1 \cong \mathbf{A}^2(K)$, $C_0 \cong \mathbf{A}^1(K) \cup \{\mathcal{O}\} \cong \mathbf{P}^1(K)$ が成り立つ．ここで $\mathcal{O} := [0 : 1 : 0]$ を無限遠点 **(point at infinity)** と呼ぶ．

斉次多項式 $G(x,y,z) \in K[x,y,z]$ に対して，$G_x(x,y,z)$, $G_y(x,y,z)$, $G_z(x,y,z)$ をそれぞれ x, y, z に関する $G(x,y,z)$ の偏微分多項式とする．射影平面曲線 $C : G(x,y,z) = 0$ 上の点 $[a : b : c] \in \mathbf{P}^2(\overline{K})$ が

$$G_x(a,b,c) = G_y(a,b,c) = G_z(a,b,c) = 0$$

を満たすとき，点 $[a : b : c]$ は C の特異点 **(singular point)** である，または C は点 $[a : b : c]$ で特異である，という．そうでないとき，C は点 $[a : b : c]$ で非特異 **(non-singular)** であるという (この定義は well-defined であることに注意せよ)．曲線 C 上の全ての点が非特異であるとき，C を非特異代数曲線という．

2.2.2 Weierstrass の標準形

次のアファイン三次曲線

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.1}$$

を考える．ここで $a_i \in K$ $(i = 1, 2, 3, 4, 6)$ とする．(2.1) を **Weierstrass** の標準形と呼ぶ．体 K の標数が 2 でないとき，変数変換

$$(x, y) \mapsto \left(x, \frac{y - a_1x - a_3}{2}\right), \tag{2.2}$$

すなわちアファイン変換

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -\frac{a_1}{2} & \frac{1}{2} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} 0 \\ -\frac{a_3}{2} \end{bmatrix}$$

によって

$$\tilde{E} : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 \tag{2.3}$$

の形に変換される．ここで,

$$b_2 = a_1^2 + 4a_2, \qquad b_4 = a_1a_3 + 2a_4, \qquad b_6 = a_3^2 + 4a_6$$

である．さらに，体 K の標数が 2 でも 3 でもないとき，$\tilde{E}$ は変数変換

$$(x, y) \mapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108}\right), \tag{2.4}$$

すなわちアファイン変換

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} \frac{1}{36} & 0 \\ 0 & \frac{1}{108} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} -\frac{3b_2}{36} \\ 0 \end{bmatrix}$$

によって

$$E' : y^2 = x^3 - 27c_4x - 54c_6 \tag{2.5}$$

の形となる．ここで,

$$c_4 = b_2^2 - 24b_4, \qquad c_6 = -b_2^3 + 36b_2b_4 - 216b_6$$

である．そこで予め

$$E : y^2 = x^3 + ax + b \tag{2.6}$$

を考えることも多い．

定義 2.2.2 (判別式). (2.1) の形のアファイン三次曲線 E に対して,

$$\Delta(E) := -b_2^2 b_8 + 9b_2 b_4 b_6 - 8b_4^3 - 27b_6^2 \in K$$

をアファイン三次曲線 E の判別式 **(discriminant)** という. ここで b_2, b_4, b_6 は上において定義したものであり,

$$b_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2$$

とする.

上の記号の下, 計算によって次の補題を示すことができる：

補題 2.2.3. 1. 体 K 上のアファイン三次曲線 $E : y^2 = x^3 + ax^2 + bx + c$ $(a, b, c \in K)$ に対して,

$$\Delta(E) = 16(-a^2(4ac - b^2) + 18abc - 4b^3 - 27c^2) \in K$$

である. ここで,

$$D = -a^2(4ac - b^2) + 18abc - 4b^3 - 27c^2$$

は三次多項式 $f(x) = x^3 + ax^2 + bx + c$ の判別式である.

2. 体 K 上のアファイン三次曲線 $E : y^2 = x^3 + ax + b$ $(a, b \in K)$ に対して,

$$\Delta(E) = 16(-4a^3 - 27b^2) \in K$$

である. ここで,

$$D = -4a^3 - 27b^2$$

は三次多項式 $f(x) = x^3 + ax + b$ の判別式である.

補題 2.2.4. 標数が 2 でない体 K 上のアファイン三次曲線 $E : y^2 = x^3 + ax^2 + bx + c$ $(a, b, c \in K)$ が非特異曲線であるための必要十分条件は $\Delta(E) \neq 0$ である.

証明. はじめに, $f(x) = x^3 + ax^2 + bx + c$, $F(x, y) = y^2 - f(x)$ とする. このとき,

$$f'(x) = 3x^2 + 2ax + b, \qquad F_x(x, y) = -f'(x), \qquad F_y(x, y) = 2y$$

であることに注意する. 曲線 $E : F(x, y) = 0$ 上の点 (x_0, y_0) が E の特異点であることの必要十分条件は, $F_x(x_0, y_0) = F_y(x_0, y_0) = 0$ であり, これは $2y_0 = 0$ かつ $f'(x_0) = 0$ に同値である. さらにこれは, $y_0 = 0$ かつ $f(x_0) = f'(x_0) = 0$ に同値である. 従って, 曲線 $E : F(x, y) = 0$ の特異点として考えられるものは $(x_0, 0)$ $(x_0 \in \overline{K})$ の形の点であり, これが曲線 E の特

異点であることの必要十分条件は，f が（$\overline{K}$ において） x_0 を重根に持つことである．ここで三次多項式 $f(x) = x^3+ax^2+bx+c$ の判別式は $D = \frac{1}{16}\Delta(E)$ を満たすので，三次曲線 $E : y^2 = x^3 + ax^2 + bx + c$ が非特異曲線であるための必要十分条件は $\Delta(E) \neq 0$ である． □

定義 2.2.5 (楕円曲線). (2.1) の形の方程式で定義される非特異アファイン平面曲線を $\mathbf{P}^2(\overline{K})$ 内に斉次化して得られる非特異射影平面曲線

$$E : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

を K 上の楕円曲線 **(elliptic curve)** という．なお，$F(x, y) = y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6)$ とし，$G(x, y, z)$ を $F(x, y)$ の z に関する斉次化とするとき，

$$\begin{aligned} E &= \{[a : b : c] \in \mathbf{P}^2(\overline{K}) : G(a, b, c) = 0\} \\ &= \{[a : b : 1] \in \mathbf{P}^2(\overline{K}) : F(a, b) = 0\} \cup \{[0 : 1 : 0]\} \end{aligned}$$

である．このことから，「体 K 上の楕円曲線」といった場合，(2.1) の形の方程式で定義される非特異アファイン平面曲線と，無限遠点 $\mathcal{O} = [0 : 1 : 0]$ とを合わせたものと解釈できる．

注意 2.2.6. 体 K の標数が 2 であるとき，$y^2 = f(x) = x^3 + ax^2 + bx + c$ の形 (特に，(2.3) または (2.6) の形) の方程式で定義されるアファイン平面曲線 E は $\mathbf{A}^2(\overline{K})$ において特異点を持つ．実際，$F(x, y) = y^2 - f(x)$ とするとき，一変数多項式 $f'(x) = 3x^2 + 2ax + b$ の ($\overline{K}$ における) 根を x_0，元 $f(x_0) = x_0^3 + ax_0^2 + bx_0 + c$ の平方根の 1 つを y_0 とすると，$F(x_0, y_0) = y_0^2 - f(x_0) = 0$, $F_x(x_0, y_0) = -f'(x_0) = 0$, $F_y(x_0, y_0) = 2y_0 = 0$ より $(x_0, y_0) \in \mathbf{A}^2(\overline{K})$ は E の特異点である．

2.3 Mordell-Weil 群 $E(K)$

前節に引き続き K を体とする．本節では，体 K 上の楕円曲線 E に対して，E の点（と無限遠点のなす）集合

$$E(K) := \{(a, b) \in \mathbf{A}^2(K) : E(a, b) = 0\} \cup \{\mathcal{O}\}$$

に加法アーベル群の構造を入れる．さらに，$E(K)$ の有限生成性を示す Mordell-Weil の定理を紹介し，(ある条件下において) $E(K)$ の計算方法を与える．

2.3.1 Mordell-Weil 群の群演算

■一般形 Weierstrass 標準形　体 K 上の楕円曲線

$$E : y^2 + a_1xy + a_3y = f(x) = x^3 + a_2x^2 + a_4x + a_6$$

の 2 点 $P, Q \in E(K)$ に対して，和 $P + Q \in E(K)$ を次で定義する：

- $P = \mathcal{O}$ (resp. $Q = \mathcal{O}$) のとき $P + Q = Q$ (resp. $P + Q = P$)．ここで $\mathcal{O}$ は無限遠点である．
- $P \neq \mathcal{O}$ かつ $Q \neq \mathcal{O}$ かつ $P \neq Q$ のとき：$P = (x_1, y_1)$, $Q = (x_2, y_2)$ と書いたとき
  1. $x_1 \neq x_2$ ならば,

$$\begin{aligned} x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \\ y_3 &= -(\lambda x_3 + \nu) - a_1x_3 - a_3 \end{aligned}$$

として $P + Q = (x_3, y_3)$ と定義する．ここで,

$$\begin{aligned} \lambda &= (y_2 - y_1)/(x_2 - x_1), \\ \nu &= y_1 - \lambda x_1 \\ &= (y_1x_2 - y_2x_1)/(x_2 - x_1) \end{aligned}$$

とする．点 (x_3, y_3) は，P と Q を通る直線 $\ell : y = \lambda x + \nu$ と E との第三の交点 (x_3, y_3') と同じ x 座標を持つような E 上の点で，(x_3, y_3') と異なる点に他ならない；直線 $y = \lambda x + \nu$ と曲線 $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ との交点の x 座標は，方程式

$$(\lambda x + \nu)^2 + a_1x(\lambda x + \nu) + a_3(\lambda x + \nu) = x^3 + a_2x^2 + a_4x + a_6$$

の解である．この方程式を整理すると,

$$x^3 + (a_2 - \lambda^2 - a_1\lambda)x^2 + (a_4 - 2\lambda\nu - a_1\nu - a_3\lambda)x + a_6 - \nu^2 - a_3\nu$$

であるので, 解と係数の関係から $x_1 + x_2 + x_3 = -(a_2 - \lambda^2 - a_1\lambda)$ である．従って，P と Q を通る直線 $\ell : y = \lambda x + \nu$ と E との第三の交点の x 座標 は $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$ で与えられる．その y 座標は $y_3' = \lambda x_3 + \nu$ である．さらに, x 座標が x_3 であるような E の点の y 座標は, y に関する方程式 $y^2 + (a_1x_3 + a_3)y - f(x_3) = 0$ の解である．従って, 解と係数の関係により $y_3 + y_3' = -(a_1x_3 + a_3)$ であるので，$y_3 = -y_3' - a_1x_3 - a_3 = -(\lambda x_3 + \nu) - a_1x_3 - a_3$ を得る．

2. $x_1 = x_2$ かつ $y_1 \neq y_2$ ならば，$P + Q = \mathcal{O}$ と定義する．この場合は $Q = (x_2, y_2) = (x_1, -y_1 - a_1x_1 - a_3)$ であることに注意する；y_1, y_2 はともに y に関する方程式 $y^2 + (a_1x_1 + a_3)y - f(x_1) = 0$ の解である．従って，解と係数の関係により $y_1 + y_2 = -(a_1x_1 + a_3)$ であるので，$y_2 = -y_1 - a_1x_1 - a_3$ を得る．

- $P \neq \mathcal{O}$ かつ $Q \neq \mathcal{O}$ かつ $P = Q$ のとき：$P = (x_1, y_1)$, $Q = (x_2, y_2)$ と書いたとき
  1. $2y_1 + a_1x_1 + a_3 = 0$ ならば，$P + Q = \mathcal{O}$ と定義する．
  2. $2y_1 + a_1x_1 + a_3 \neq 0$ ならば，

$$\begin{aligned} x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 = \lambda^2 + a_1\lambda - a_2 - 2x_1, \\ y_3 &= -(\lambda x_3 + \nu) - a_1x_3 - a_3 \end{aligned}$$

として $P + Q = (x_3, y_3)$ と定義する．ここで，

$$\begin{aligned} \lambda &= (f'(x_1) - a_1y_1)/(2y_1 + a_1x_1 + a_3), \\ \nu &= y_1 - \lambda x_1 \\ &= (-x_1^3 + a_4x_1 + 2a_6 - a_3y_1)/(2y_1 + a_1x_1 + a_3) \end{aligned}$$

である．これは，楕円曲線 E の $P = Q$ における接線 $\ell : y = \lambda x + \mu$ と E とのもう一つの交点 (x_3, y_3') と同じ x 座標を持つような E 上の点で，(x_3, y_3') と異なる点に他ならない．さらに計算すると，

$$\begin{aligned} x_3 &= \frac{x_1^4 + (-a_1a_3 - 2a_4)x_1^2 + (-2a_3^2 - 8a_6)x_1}{(2y_1 + a_1x_1 + a_3)^2} \\ &\quad + \frac{a_1a_3a_4 - a_1^2a_6 - a_2a_3^2 + a_4^2 - 4a_2a_6}{(2y_1 + a_1x_1 + a_3)^2}, \\ y_3 &= -(\lambda x_3 + y_1 - \lambda x_1) - a_1x_3 - a_3 \end{aligned}$$

の形となる．

■標数 $\neq 2$ の場合　標数が 2 でない体 K 上の楕円曲線

$$E : y^2 = x^3 + ax^2 + bx + c$$

の 2 点 $P, Q \in E(K)$ に対して，和 $P + Q \in E(K)$ を次で定義する：

- $P = \mathcal{O}$ (resp. $Q = \mathcal{O}$) のとき $P + Q = Q$ (resp. $P + Q = P$)．ここで $\mathcal{O}$ は無限遠点である．
- $P \neq \mathcal{O}$ かつ $Q \neq \mathcal{O}$ かつ $P \neq Q$ のとき：$P = (x_1, y_1)$, $Q = (x_2, y_2)$ と書いたとき

1. $x_1 \neq x_2$ ならば,

$$\begin{aligned} x_3 &= \lambda^2 - a - x_1 - x_2, \\ y_3 &= -(\lambda x_3 + \nu) \end{aligned}$$

として $P + Q = (x_3, y_3)$ と定義する．ここで,

$$\begin{aligned} \lambda &= (y_2 - y_1)/(x_2 - x_1), \\ \nu &= y_1 - \lambda x_1 \\ &= (y_1 x_2 - y_2 x_1)/(x_2 - x_1) \end{aligned}$$

とする．これは，P と Q を通る直線 $\ell : y = \lambda x + \nu$ と E との第三の交点 (x_3, y_3') を x 軸に関して対称移動して得られる点 $(x_3, -y_3') \in E(K)$ に他ならない．

2. $x_1 = x_2$ かつ $y_1 \neq y_2$ ならば，$P + Q = \mathcal{O}$ と定義する．この場合は $Q = (x_2, y_2) = (x_1, -y_1)$ であることに注意する．

- $P \neq \mathcal{O}$ かつ $Q \neq \mathcal{O}$ かつ $P = Q$ のとき：$P = (x_1, y_1)$, $Q = (x_2, y_2)$ と書いたとき

1. $y_1 = y_2 = 0$ ならば，$P + Q = \mathcal{O}$ と定義する．
2. $y_1 = y_2 \neq 0$ ならば,

$$\begin{aligned} x_3 &= \lambda^2 - a - x_1 - x_2 = \lambda^2 - a - 2x_1, \\ y_3 &= -(\lambda x_3 + \nu) \end{aligned} \tag{2.7}$$

として $P + Q = (x_3, y_3)$ と定義する．ここで,

$$\begin{aligned} \lambda &= f'(x_1)/(2y_1), \\ \nu &= y_1 - \lambda x_1 \\ &= (-x_1^3 + a_4 x_1 + 2a_6)/(2y_1) \end{aligned}$$

である．これは, 楕円曲線 E の $P = Q$ における接線 $\ell : y = \lambda x + \mu$ と E とのもう一つの交点 (x_3, y_3') を x 軸に関して対称移動して得られる点 $(x_3, -y_3')$ に他ならない．さらに計算すると,

$$\begin{aligned} x_3 &= \frac{x_1^4 - 2bx_1^2 - 8cx_1 + b^2 - 4ac}{4(x_1^3 + ax_1^2 + bx_1 + c)}, \\ y_3 &= -(\lambda x_3 + y_1 - \lambda x_1) \end{aligned} \tag{2.8}$$

の形となる．

次の命題の証明は省略する．

命題 2.3.1. 上記の二項演算によって，$E(K)$ は $\mathcal{O}$ を加法単位元とするアーベル群をなす．特に，点 $P = (x, y) \in E(K) \setminus \{\mathcal{O}\}$ の逆元は $-P = (x, -y - a_1 x - a_3)$ で与えられる．

定義 2.3.2 (Mordell-Weil 群). 体 K 上の楕円曲線 E に対して，加法アーベル群 $E(K)$ を **Mordell-Weil 群**という．群 $E(K)$ の元を E の K **有理点 (K-rational point)** と呼ぶ（ただし，無限遠点 $\mathcal{O}$ も有理点と取り決めている）．

例 2.3.3. 有理数体 $K=\mathbb{Q}$ 上の楕円曲線 $E: y^2=x^3-43x+166$ を考える．E 上の点 $P=(3,8)$ について，上記の群演算によって $2P, 3P, 4P, 8P$ を計算すると，$2P=(-5,-16), 3P=(11,-32), 4P=(11,32,1), 8P=(3,8)=P$ である．従って $7P=\mathcal{O}$ であり，7 は素数であるので P の位数（2.3.2 節で定義）は 7 である．

注意 2.3.4. 本稿では Mordell-Weil 群 $E(K)$ における加法およびスカラー倍をアファイン座標で表された点に対して定義しているが，射影座標や **Jacobian** 座標と呼ばれる座標で表された点に対しても加法およびスカラー倍を定義することが可能であり，座標系の間の変換も可能である（本稿では取り扱わない）．演算の計算量という観点では，射影座標や Jacobian 座標を用いた方がアファイン座標より効率的である．アファイン座標以外の座標によって表された点の演算については，例えば [3, 1 章] を参照とする．

2.3.2 位数が小さい点の決定

ここでは，位数 2 または 3 の点を決定する方法を与える．簡単のため体 K の標数は 2 でないとし，$E: y^2=f(x)=x^3+ax^2+bx+c$ $(a,b,c\in K)$ の形の場合で考える．また，$E(K)$ の元 P に対して $nP=\mathcal{O}$ となる自然数 n が存在するとき，そのような n のうち最小なものを $\mathrm{ord}(P)$ と書き，これを P の位数と呼ぶ．$nP=0$ となる自然数が存在しないとき，$\mathrm{ord}(P)=\infty$ と定める．整数 $m\in\mathbb{Z}$ に対して，

$$E(K)[m] := \{P\in E(K) : mP=\mathcal{O}\}$$

と定める．$K=\overline{K}$ のときは，$E(K)[m]$ を単に $E[m]$ とも書く．

■位数 2 の点　$P\in E(K)[2]$ とし，$P\neq\mathcal{O}$ とする．$P=(x,y)$ $(x,y\in K)$ と書く．$2P=\mathcal{O}$ より，$P=-P$ であるので，$y=-y$ である．従って $y=0$ である．点 $P=(x,0)$ は E 上の点であるから，$f(x)=0$ より，x は f の根である．その可能性としては高々 3 個であるが，E は非特異であるので，f は代数閉包 $\overline{K}$ 上で重根を持たない．よって，$2P=\mathcal{O}$ となる元は（$\mathcal{O}$ と合わせて）4 個である．$\mathcal{O}$ 以外の残りの 3 つ（位数 2 の点）は，f の $\overline{K}$ における相異なる 3 つの根を x_1, x_2, x_3 としたとき，$(x_1,0), (x_2,0), (x_3,0)$ で与えられる．

例 2.3.5. $E : y^2 = x^3 + 8$ とする．$x^3 + 8 = (x+2)(x^2 - 2x + 4)$ であるので，

$$E(\mathbb{C})[2] = \{\mathcal{O}, (-2, 0), (\alpha, 0), (\beta, 0)\}$$

である．ここで $\alpha = 1 + \sqrt{-3}$, $\beta = 1 - \sqrt{-3}$ とする．

例 2.3.6. $E : y^2 = (x-1)(x-2)(x-3)$ とする．このとき，

$$E(\mathbb{R})[2] = \{\mathcal{O}, (1, 0), (2, 0), (3, 0)\}$$

である．

■位数 3 の点　$P \in E(K)[3]$ とし，$P \neq \mathcal{O}$ とする．$3P = \mathcal{O}$ より，$2P = -P$ であるので，$x(2P) = x(-P) = x(P)$，従って (2.7) より

$$\frac{f'(x)^2}{4y^2} - a - 2x = x \tag{2.9}$$

である．ここで，点 Q に対してその x 座標を $x(Q)$ と書く．(2.9) を整理すると，

$$2f''(x)f(x) - f'(x)^2 = 0 \tag{2.10}$$

となる．(2.10) の左辺を $\psi_3(x)$ と書く．

命題 2.3.7. 体 K の標数が 2 でも 3 でもないとき，$\psi_3(x)$ は（$\overline{K}$ において）相異なる 4 つの根を持つ．

証明. まず，$f'''(x) = 6$ であり，$\psi_3'(x) = 2f'''(x)f(x) + 2f''(x)f'(x) - 2f'(x)f''(x) = 2f'''(x)f(x) = 12f(x)$ である．従って，もし $\psi_3(x)$ がある元 $\alpha \in \overline{K}$ を重根に持つならば，$\psi_3'(\alpha) = 12f(\alpha) = 0$ より $f(\alpha) = 0$ である．また，$\psi_3(\alpha) = 2f''(\alpha)f(\alpha) - f'(\alpha)^2 = -f'(\alpha)^2 = 0$ であるので，$f'(\alpha) = 0$ が成り立つ．ゆえに α は f の重根となり，これは $E : y^2 = f(x)$ の非特異性に矛盾する．従って，$\psi_3(x)$ は（$\overline{K}$ において）重根を持たない．　□

注意 2.3.8. 計算によって

$$\psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + b^2 - 4ac \tag{2.11}$$

がわかる．

従って，$\mathrm{ord}(P) = 3$ となる元は次の 8 つである：$\psi_3(x)$ の $\overline{K}$ における相異なる 4 つの根を x_1, x_2, x_3, x_4 としたとき，(x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4), $(x_1, -y_1)$, $(x_2, -y_2)$, $(x_3, -y_3)$, $(x_4, -y_4)$．ここで，$P = (x, y)$ が位数 3 の点であれば，$-P = (x, -y)$ も位数 3 の点であることに注意する．よって，$3P = \mathcal{O}$ となる元は $\mathcal{O}$ と合わせて 9 個である．

命題 2.3.9. E を体 K 上の楕円曲線とする．このとき，

$$\#\{P \in E(\overline{K}) : \mathrm{ord}(P)|3\} = 9$$

である．

より一般に，次が成り立つ（証明略）：

定理 2.3.10. 体 K 上の楕円曲線 E と整数 $n \in \mathbb{Z}_{>0}$ に対し

$$E[n] = \{P \in E(\overline{K}) : \mathrm{ord}(P)|n\} \cong \mathbb{Z}_n \times \mathbb{Z}_n$$

である．ここで $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ としている．従って，$\#\{P \in E(\overline{K}) : \mathrm{ord}(P)|n\} = n^2$ である．

例 2.3.11. 実数体 $\mathbb{R}$ 上の楕円曲線 $E : y^2 = f(x) = ax^2 + bx + c$ (ただし $a, b, c \in \mathbb{R}$) に対して，$E(\mathbb{R})[3]$ を求めてみよう．まず，計算により

$$\frac{d^2y}{dx^2} = \frac{2f''(x)f(x) - f'(x)^2}{4yf(x)} = \frac{\psi_3(x)}{4yf(x)}.$$

である．従って，点 $P = (x, y) \in E$ の位数が 3 であることは，$P \neq \mathcal{O}$ かつ P は E の変曲点であることに同値である．

ここで, $\psi_3(x)$ はちょうど 2 つの相異なる実根を持つことに注意する．実際，$\psi_3'(x) = 12f(x)$ であるので，$\psi_3'(x)$ と $f(x)$ の根は一致する．そこでまず, $f(x)$ が相異なる 3 つの実根 $\beta_1 < \beta_2 < \beta_3$ を持つ場合を考える（f は重根を持たないので, $f'(\beta_i) \neq 0$ であることに注意する）．この場合, 4 次関数 $y = \psi_3(x)$ は $x = \beta_i$ で停留点をとるが, $\psi_3(\beta_i) = 2f''(\beta_i)f(\beta_i) - f'(\beta_i)^2 = -f'(\beta_i)^2 < 0$ であるので, $y = \psi_3(x)$ のグラフは x 軸と異なる 2 点で交わる．次に $f(x)$ がただ 1 つの実根 β を持つ場合を考える．この場合，4 次関数 $y = \psi_3(x)$ は $x = \beta$ で停留点をとるが, $\psi_3(\beta) = -f'(\beta)^2 < 0$ であるので, $y = \psi_3(x)$ のグラフは x 軸と異なる 2 点で交わる．以上から $\psi_3(x)$ は相異なる 2 つの実根 α_1, α_2 を持つ．また，$\psi_3'(\alpha_1) < 0$ (resp. $\psi_3'(\alpha_1) > 0$) に注意すると，$f(\alpha_1) = \frac{1}{12}\psi_3'(\alpha_1) < 0$ (resp. $f(\alpha_2) = \frac{1}{12}\psi_3'(\alpha_2) > 0$) である．

従って，$y^2 = f(\alpha_1)$ が実解 y を持たないことに注意すると，$E(\mathbb{R})$ における位数 3 の点は $(\alpha_2, \pm\sqrt{f(\alpha_2)})$ であり，ゆえに $E(\mathbb{R})[3] \cong \mathbb{Z}/3\mathbb{Z}$ である．

2.3.3 Mordell-Weil の定理

ここでは Mordell-Weil 群 $E(K)$ の構造について，よく知られている結果をいくつか述べる．次の定理 2.3.12 が示すように，$E(K)$ は有限生成アーベル群であり，特に K が有限体であるとき $E(K)$ は 2 つの巡回群の直和に分解する．

定理 2.3.12 (Mordell-Weil). 代数体 K 上の楕円曲線 E に対して，アーベル群 $E(K)$ は有限生成であり，

$$E(K) \cong \mathbb{Z}^r \oplus G$$

の形に書ける．ここで G は有限群である．有限群 G は $E(K)$ の捩れ部分 (torsion part) であるので，以降 $G = E(K)_{\mathrm{tors}}$ と書く．

定義 2.3.13. 定理 2.3.12 における非負整数 r を楕円曲線 E の階数 **(rank)** と呼ぶ.

命題 2.3.14. 有限体 $K = \mathbb{F}_q$ 上の楕円曲線 E に対して，アーベル群 $E(\mathbb{F}_q)$ は巡回群または二つの巡回群の直和

$$E(\mathbb{F}_q) \cong C \times C'$$

の形に書ける．ここで $\#C | \#C'$ かつ $\#C' | q-1$ である．

問題 2.3.15. 与えられた K と K 上の楕円曲線 E について, 有理点 $P \in E(K)$ を見つける（効率的）アルゴリズムは存在するか？

問題 2.3.16. 与えられた K と K 上の楕円曲線 E について，$E(K)$ の階数を求める（効率的）アルゴリズムは存在するか？

問題 2.3.17. 与えられた K について，$E(K)$ の階数の上限は存在するか？ cf. $K = \mathbb{Q}$：Elkies によって階数 ≥ 28 の楕円曲線が見つけられた（注：$= 28$ かどうかは未解決).

2.3.4 Mordell-Weil の定理の証明

ここでは $K = \mathbb{Q}$ の場合における Mordell-Weil の定理（定理 2.3.12）を証明する．証明のポイントは次の二つである：

(1) 剰余群 $E(K)/2E(K)$ は有限である (**second descent**, **2-descent**).
(2) 有理点の高さを導入し，剰余群 $E(K)/2E(K)$ の有限個の完全代表系を用いて，Fermat の無限降下法 **(infinite descent, ∞-descent)** を適用する．

(1) は弱 **Mordell** の定理とも呼ばれる．著者の講演では (2) のみを紹介し，(1) については 2 日目の吉川祥氏（学習院大学）の講演に譲った．以下ではまず，有理数・有理点の高さを定義する．楕円曲線の有理点の高さとして，ナイーブ高さと標準高さの二種類を定義する．

■有理点の高さ

定義 2.3.18 (有理数の高さ). 0 でない有理数 $x = \frac{m}{n}$ $(m, n \in \mathbb{Z},\ n \neq 0,$ $\gcd(m,n) = 1)$ に対して, x の**高さ (height)** $H(x)$ を $H(x) := \max\{|m|, |n|\}$ と定義する. また, $H(0) := 0$ と定める.

例 2.3.19. $H(1) = 1$. $H(39/40) = 40$.

補題 2.3.20. 自然数 $k \in \mathbb{Z}_{\geq 1}$ に対して,

$$\#\{x \in \mathbb{Q} : H(x) \leq k\} \leq 2k^2 + k$$

が成り立つ. 従って集合 $\{x \in \mathbb{Q} : H(x) \leq k\}$ は有限集合である.

証明. $H(x) \leq k$ を満たす有理数 x の個数を勘定する. $x = \frac{m}{n}$ $(m, n \in \mathbb{Z},$ $n \neq 0,$ $\gcd(m,n) = 1)$ とし, $H(x) \leq k$ とする. $n > 0$ としてよい. まず, $0 \leq |m| < n$ の場合を考える. この場合, $n = H(x)$ であるので, n の候補は $1, 2, \ldots, k$ である. n の候補それぞれに対して, m の候補は $n-1, \ldots, 1, 0, -1, \ldots, -(n-1)$ の $2(n-1)+1$ 個である. 従って, $0 \leq |m| < n$ の場合において $H(x) \leq k$ を満たす有理数 x の個数は,

$$\sum_{i=1}^{k} 2\left((i-1)+1\right) = 2\sum_{i=1}^{k} i - \sum_{i=1}^{k} 1 = k^2$$

以下である. 次に, $0 < n \leq |m|$ の場合を考える. この場合, $|m| = H(x)$ であるので, m の候補は $-k, \ldots -1, 1, \ldots, k$ である. m の候補それぞれに対して, n の候補は $1, \ldots, |m|$ の $|m|$ 個である. 従って, $0 < n \leq |m|$ の場合において $H(x) \leq k$ を満たす有理数 x の個数は,

$$2\sum_{i=1}^{k} i = k^2 + k$$

以下である. 従って, $H(x) \leq k$ を満たす有理数 x の個数は $k^2 + (k^2 + k) = 2k^2 + k$ 以下である. □ □

定義 2.3.21 (有理点の高さ). 有理数体 $K = \mathbb{Q}$ 上の楕円曲線 E について, 有理点 $P = (x, y) \in E(\mathbb{Q})$ の**高さ (height)** $H(P)$ を $H(P) := H(x) \in \mathbb{Z}_{\geq 0}$ と定義する. 無限遠点 $\mathcal{O}$ に対しては, $H(\mathcal{O}) := 1$ と定義する. また, $h(P) := \log H(P)$ を有理点 P の**対数的高さ (logarithmic height)** と呼ぶ.

注意 2.3.22. 関数 $P \mapsto h(P)$ を**ナイーブ高さ関数**ともいう. これに対して**標準高さ関数** $P \mapsto \hat{h}(P)$ はナイーブ高さ関数を用いて次のように定義される: $\hat{h}(P) := \lim_{n\infty} 4^{-n} h(2^n P)$.

有理数体 $K = \mathbb{Q}$ 上の楕円曲線 E について, 次の 3 性質が成り立つ (証明略):

(i) 任意の実数 $M \geq 0$ に対して，集合 $\{P \in E(\mathbb{Q}) : h(P) \leq M\}$ は有限集合である．

(ii) 任意の P_0 に対して，ある定数 k_0 が存在して，任意の $P \in E(\mathbb{Q})$ に対して

$$h(P + P_0) \leq 2h(P) + k_0$$

が成り立つ．

(iii) ある定数 k が存在して，任意の $P \in E(\mathbb{Q})$ に対して

$$h(2P) \geq 4h(P) - k$$

が成り立つ．

上記の 3 性質を用いて，$K = \mathbb{Q}$ の場合における定理 2.3.12 を証明する．

■$K = \mathbb{Q}$ の場合における定理 2.3.12 の証明　本小節冒頭で言及したように，$[E(\mathbb{Q}) : 2E(\mathbb{Q})]$ が有限であることは認める．そこで $n := [E(\mathbb{Q}) : 2E(\mathbb{Q})]$ とし，$Q_1, \ldots, Q_n \in E(\mathbb{Q})$ を剰余群 $E(\mathbb{Q})/2E(\mathbb{Q})$ の完全代表系とする．$P \in E(\mathbb{Q})$ を任意の有理点とする．このとき，ある $1 \leq i_1 \leq n$ と $P_1 \in E(\mathbb{Q})$ が存在して，$P - Q_{i_1} = 2P_1$ の形に書ける．P_1 についても P と同様にして，ある $1 \leq i_2 \leq n$ と $P_2 \in E(\mathbb{Q})$ が存在して，$P_1 - Q_{i_2} = 2P_2$ の形に書ける．これを繰り返して，

$$P_{j-1} - Q_{i_j} = 2P_j$$

なる P_j, Q_{i_j} を得る．特に，任意の $m \geq 1$ に対して

$$P = Q_{i_1} + 2Q_{i_2} + \cdots + 2^{m-1}Q_{i_m} + 2^m P_m$$

となる．よって $P \in \langle P_m, Q_i \rangle_{1 \leq i \leq n}$ を得る．もし $P_m = \mathcal{O}$ ならば $P \in \{Q_1, \ldots, Q_n\}$ である．任意の m に対して $P_m \neq \mathcal{O}$ と仮定する．性質 (ii) によって，各 $1 \leq i \leq n$ についてある k_i が存在して，任意の $P' \in E(\mathbb{Q})$ に対して

$$h(P' - Q_i) \leq 2h(P') + k_i$$

が成り立つ．そこで $k_0 := \max\{k_1, \ldots, k_n\}$ とすると，任意の $P' \in E(\mathbb{Q})$ と任意の $1 \leq i \leq n$ に対して

$$h(P' - Q_i) \leq 2h(P') + k_0$$

が成り立つ．性質 (iii) により，ある k が存在して，任意の j に対して

$$h(2P_j) \geq 4h(P_j) - k$$

が成り立つ．従って

$$4h(P_j) \leq h(2P_j) + k = h(P_{j-1} - Q_{i_j}) + k \leq 2h(P_{j-1}) + k_0 + k \quad (2.12)$$

であり，

$$h(P_j) \leq \frac{1}{2}h(P_{j-1}) + \frac{1}{4}(k_0 + k) = \frac{3}{4}h(P_{j-1}) - \frac{1}{4}(h(P_{j-1}) - (k_0 + k))$$

ここで，ある m に対して $h(P_m) \leq k_0 + k$ である．なぜならば，もし任意の m に対して $h(P_m) > k_0 + k$ ならば，(2.12) より

$$h(P_j) < \frac{3}{4}h(P_{j-1})$$

を満たすので，点列 $P, P_1, P_2, \ldots$ はナイーブ高さが狭義単調減少するような相異なる点の無限列である．従って集合 $\{P' \in E(\mathbb{Q}) : h(P') \leq h(P)\}$ は無限集合となるがこれは性質 (i) に反する．いま，ある整数 $a_1, \ldots, a_n$ によって

$$P = a_1Q_1 + \cdots + a_nQ_n + 2^mP_m$$

の形に書けており $h(P_m) \leq k_0 + k$ である．ここで k_0 は E と $Q_1, \ldots, Q_n$ のみに，k は E のみにそれぞれ依存する定数であることに注意する．性質 (i) によって

$$\{Q_1, \ldots, Q_n\} \cup \{R \in E(\mathbb{Q}) : h(R) \leq k_0 + k\}$$

は有限集合であり，これは $E(\mathbb{Q})$ を生成する．

注意 2.3.23. 上で見たように，もし $E(\mathbb{Q})/2E(\mathbb{Q})$ の完全代表系が計算でき，さらに定数 k を具体的に求めることができれば，高さの不等式を満たす有理点を総当たりで探索することで $E(\mathbb{Q})$ の生成元を（理論上）計算することができる．さらに，生成元のなかから独立な生成元を求めることができれば，E の階数も（理論上）計算することができる．これらの計算については，2.3.6 節で紹介する．

2.3.5 Torsion part の計算

前節で Mordell-Weil 群 $E(K)$ は有限生成アーベル群になることを見た．ここでは，$K = \mathbb{Q}$ のときに $E(\mathbb{Q})$ の捩れ部分 $E(\mathbb{Q})_{\mathrm{tors}}$ を具体的に計算する方法を与える．

体 $K = \mathbb{Q}$ 上の楕円曲線 $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ を考える．係数 a, b, c を整数 a_1, a_2, b_1, b_2, c_1, c_2 によって $a = a_1/a_2$, $b = b_1/b_2$, $c = c_1/c_2$ と書く．a, b, c のいずれかが整数でない有理数の場合，$d = a_2b_2c_2$ とし，変数変換 $X = d^2x$, $Y = d^3y$ によって E は

$$Y^2 = X^3 + d^2aX^2 + d^4bX + d^6c$$

を定義方程式とする楕円曲線と同型となる．ここで d^2a, d^4b, d^6c は全て整数である．これを踏まえ以下では，楕円曲線 E の定義方程式の係数が全て整数の場合を考える．

定理 2.3.24 (Nagell-Lutz, 1930's). 有理数体 $\mathbb{Q}$ 上の楕円曲線 $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ を考える．ただし係数 a, b, c は全て整数であると仮定する．このとき，$P = (x, y) \in E(\mathbb{Q})_{\mathrm{tors}} \setminus \{\mathcal{O}\}$ ならば，$x, y \in \mathbb{Z}$ であり，

1. $y = 0$ ならば P の位数は 2 である．
2. $y \neq 0$ ならば $y^2 | D$ である．

ここで，

$$D := -27c^3 - 4a^3c - 4b^3 + a^2b^2 + 18abc = \frac{1}{16}\Delta(E)$$

は三次多項式 $f(x)$ の判別式である．

計算によって，次の補題 2.3.25 を示すことができる：

補題 2.3.25. $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ を体 K 上の楕円曲線とする．D を三次多項式 $f(x)$ の判別式とし，α_1, α_2, α_3 を $\overline{K}$ における $f(x)$ の根とする．このとき，

1. $D = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2$,
2. $D = r(x)f(x) + s(x)f'(x)$, ここで

$$\begin{aligned} r(x) &= (18b - 6a^2)x - (4a^3 - 15ab + 27c), \\ s(x) &= (2a^2 - 6b)x^2 + (2a^3 - 7ab + 9c)x + (a^2b + 3ac - 4b^2) \end{aligned}$$

が成り立つ．

補題 2.3.26. 有理数体 $\mathbb{Q}$ 上の楕円曲線 $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ を考える．ただし係数 a, b, c は全て整数であると仮定する．このとき，E 上の点 $P = (x, y)$ について，P と $2P$ が整数点（すなわち，P と $2P$ の x 座標と y 座標は全て整数である）ならば，$y = 0$ または $y | D$ が成り立つ．

証明. $y \neq 0$ とする．このとき，P の位数は 2 ではないので $2P \neq \mathcal{O}$ である．$2P = (X, Y)$ $(X, Y \in \mathbb{Z})$ と書く．$\lambda = f'(x)/(2y)$ とすると，(2.7) より $\lambda^2 = 2x + X + a$ である．x, X, a は全て整数であるので，λ^2 も整数である．λ は有理数であるので，λ は整数となる．従って $y | f'(x)$ である．また，$y^2 = f(x)$ より $y | f(x)$ である．ゆえに，y は $D = r(x)f(x) + s(x)f'(x)$ を割りきる． □

例 2.3.27. 有理数体 $\mathbb{Q}$ 上の楕円曲線 $E : y^2 = f(x) = x^3 + 4x$ について，$E(\mathbb{Q})_{\mathrm{tors}}$ を計算する．まず，位数 1 の点は無限遠点 $\mathcal{O}$ である．次に位数 2 の点は $(x, 0)$ (x は $f(x)$ の根) の形であるので，

$$E(\mathbb{C})[2] = \{\mathcal{O}, (0, 0), (2i, 0), (-2i, 0)\}$$

である．$(x, y) \in E(\mathbb{Q})$ を位数 3 以上の点とする．$D = -4 \cdot 4^3 = -256 = -2^8$ であるので，定理 2.3.24 より，y の可能性としては $y = \pm 1, \pm 2, \pm 4, \pm 8, \pm 16$ である．それぞれを $y^2 = x^3 + 4x$ に代入することで x が求まり，

$$E(\mathbb{Q})_{\mathrm{tors}} = \{\mathcal{O}, (0,0), (2,4), (2,-4)\}$$

である．点 $(2, \pm 4)$ の位数は 4 であるので，$E(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/4\mathbb{Z}$ である．

Nagell-Lutz の定理によって，E の捩れ元の y 座標（の絶対値）の上界がわかる．しかし判別式 D の値は E（の定義方程式の係数）に依存する．Mazur によって証明された次の定理 2.3.28 は，$K = \mathbb{Q}$ の場合に E の捩れ元の個数の上界を E に依らない形で与えている：

定理 2.3.28 (Mazur, 1997)．E を有理数体 $K = \mathbb{Q}$ 上の楕円曲線とする．このとき，$E(\mathbb{Q})_{\mathrm{tors}}$ は次のいずれかと同型である：

1. $\mathbb{Z}/m\mathbb{Z}$ $(1 \leq m \leq 12,\ m \neq 11)$.
2. $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}$ $(1 \leq m \leq 4)$.

問題 2.3.29. 与えられた K と K 上の楕円曲線 E について，$E(K)_{\mathrm{tors}}$ の元の位数の上界は存在するか？ cf. $K = \mathbb{Q}$ の場合は Mazur により解決（定理 2.3.28）．他の K (e.g., $K = \mathbb{Q}(\sqrt{2})$ など) についてはどうだろうか？

2.3.6 Free part の計算

ここでは，$K = \mathbb{Q}$ のときに $E(\mathbb{Q})$ の自由部分 $E(\mathbb{Q})_{\mathrm{fr}}$ を計算する方法を説明する．ここで与える計算法は古典的かつ基本的なものであり, [1, Chapter 3] において説明されているアイデアに基づくものである．具体的には，$E(\mathbb{Q})/2E(\mathbb{Q})$ の完全代表系 $Q_1, \ldots, Q_n$ および $E(\mathbb{Q})$ の階数 r が与えられたときに，次のようにして $E(\mathbb{Q})$ の独立な生成元を求める．

Step 0. （探索ステップにおける高さの上界 B の決定）前処理として，$Q_1, \ldots, Q_n$ から Step 1 における高さの上界 B を計算する．また，$k := 0$, $\mathcal{P} := \emptyset$, $\mathcal{L} := \emptyset$ とする．

Step 1. （有理点探索）$h(P) \leq B$ を満たす有理点 $P \in E(\mathbb{Q})$ を探索する．ただし, Step 2 の計算過程で出現した有理点, すなわち $P \in \mathcal{L}$ なるものは除外してよい．存在しなければ, $\mathcal{P}$ が $E(\mathbb{Q})_{\mathrm{fr}}$ の基底である．見つかった有理点を $P_{k+1} := P$ とする．

Step 2. （高さ対を用いた独立性判定と部分群拡張）高さ対によって構成される行列から, $P_1, \ldots, P_k, P_{k+1}$ が $\mathbb{Z}$ 上で一次独立かどうかを判定する．一次独立である場合, $\mathcal{P} := \mathcal{P} \cup \{P_{k+1}\}$ として $\mathcal{P}$ を更新する．も

し P_{k+1} が $P_1, \ldots, P_k$ の $\mathbb{Z}$ 上の線形和で書けるなら, $\langle P_1, \ldots, P_k \rangle_{\mathbb{Z}} = \langle P_1, \ldots, P_k, P_{k+1} \rangle_{\mathbb{Z}}$ であるので $\mathcal{P}$ の更新はしない．もしある $k > 1$ に対して kP が $P_1, \ldots, P_k$ の $\mathbb{Z}$ 上の線形和で書けるなら, 有理点 $R_1, \ldots, R_k \in E(\mathbb{Q})$ で $\langle R_1, \ldots, R_k \rangle_{\mathbb{Z}}$ が $\langle \mathcal{P} \rangle_{\mathbb{Z}}$ より真に大きくなるものを構成し, $\mathcal{P} := \{R_1, \ldots, R_k\}$ として $\mathcal{P}$ を更新する．なお, $R_1, \ldots, R_k$ の構成過程で生じる, $\langle R_1, \ldots, R_k \rangle_{\mathbb{Z}}$ の生成元は $\mathcal{L}$ に追加して記録しておく．$\mathcal{P}$ を更新した後, Step 1 に戻る．

上記における各ステップの詳細は後述する．まず, 最終的に得られる $\mathcal{P}$ が $E(\mathbb{Q})_{\mathrm{fr}}$ の基底であることを保障するために，以下にいくつかのよく知られた事実を述べる：

補題 2.3.30 (Cremona)．実数 $B > 0$ を集合

$$S = \{P \in E(\mathbb{Q}) : \hat{h}(P) \leq B\}$$

が $E(\mathbb{Q})/2E(\mathbb{Q})$ の完全代表系を含むようにとる．このとき，S は $E(\mathbb{Q})$ を生成する．

定理 2.3.31 (Silverman, Simon)．ある定数 B' が存在して，任意の $P \in E(\mathbb{Q})$ に対して,

$$h(P) - \hat{h}(P) \leq B'$$

を満たす.

定理 2.3.31 における定数 B' は次のように決定される．実数 x に対して, $\log^+(x) := \log(\max\{1, |x|\})$ と定める．

命題 2.3.32 ([1], Proposition 3.5.1)．$\mathbb{Z}$ 上の楕円曲線 E に対して,

$$\mu(E) = \frac{1}{6}(\log|\Delta(E)| + \log^+(j(E))) + \log^+(b_2/12) + \log(2^*)$$

と定義する．ただし $b_2 \neq 0$ (resp. $b_2 = 0$) のとき $2^* = 2$ (resp. $2^* = 1$) とする．このとき，任意の $P \in E(\mathbb{Q})$ に対して

$$-\frac{1}{12}h(j(E)) - \mu(E) - 1.922 \leq \hat{h}(P) - h(P) \leq \mu(E) + 2.14$$

が成り立つ．ここで $j(E)$ は E の j 不変量であり，$h(j(E))$ はその高さである.

定義 2.3.33 (高さ対)．有理数体 $K = \mathbb{Q}$ 上の楕円曲線 E の K 有理点 $P, Q \in E(\mathbb{Q})$ に対して,

$$\hat{h}(P, Q) := \frac{1}{2}(\hat{h}(P + Q) - \hat{h}(P) - \hat{h}(Q))$$

を P と Q の高さ対 **(height pairing)** という．これは, 標準高さ関数 $P \mapsto \hat{h}(P)$ を $E(\mathbb{Q})$ 上の二次形式とみたときの, 付随する対称双線形形式であり, 特に $\hat{h}(P,P) = \hat{h}(P)$ である．

補題 2.3.34. 有理数体 $K = \mathbb{Q}$ 上の楕円曲線 E の K 有理点 $P_1, \ldots, P_k, P_{k+1}$ に対して，$k \times k$ 行列 $M_k = (\hat{h}(P_i, P_j))_{1 \le i,j \le k}$ および $(k+1) \times (k+1)$ 行列 $M_{k+1} = (\hat{h}(P_i, P_j))_{1 \le i,j \le k+1}$ を考える．もし $\det(M_k) \neq 0$ であるならば, ある $c_1, \ldots, c_{k+1} \in \mathbb{R}$ $(c_{k+1} \neq 0)$ が存在して,

$$c_1 P_1 + \cdots + c_k P_k + c_{k+1} P_{k+1} = 0 \ \text{ in } \ E(\mathbb{R})/E(\mathbb{R})_{\mathrm{tors}} \cong E(\mathbb{R})_{\mathrm{fr}}$$

が成り立つ.

証明. $\det(M_k) \neq 0$ より, $M_k = {}^tM_k$ を係数行列とする連立 1 次方程式

$${}^tM_k \mathbf{x} = \begin{bmatrix} \hat{h}(P_1,P_1) & \cdots & \hat{h}(P_k,P_1) \\ \vdots & \ddots & \vdots \\ \hat{h}(P_1,P_k) & \cdots & \hat{h}(P_k,P_k) \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_k \end{bmatrix} = \begin{bmatrix} \hat{h}(P_{k+1},P_1) \\ \vdots \\ \hat{h}(P_{k+1},P_k) \end{bmatrix}$$

は $\mathbb{R}$ 上で一意的な解を持ち, それは Cramer の公式によって $x_i = \dfrac{\det(A_i)}{\det(M_k)}$ で与えられる．ここで A_i は

$$\begin{bmatrix} \hat{h}(P_1,P_1) & \cdots & \hat{h}(P_{i-1},P_1) & \hat{h}(P_{k+1},P_1) & \hat{h}(P_{i+1},P_1) & \cdots & \hat{h}(P_k,P_1) \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ \hat{h}(P_1,P_k) & \cdots & \hat{h}(P_{i-1},P_k) & \hat{h}(P_{k+1},P_k) & \hat{h}(P_{i+1},P_k) & \cdots & \hat{h}(P_k,P_k) \end{bmatrix}$$

とする．また, M_{k+1} の i 行と $k+1$ 列を取り除いて得られる部分行列は

$$\begin{bmatrix} \hat{h}(P_1,P_1) & \cdots & \hat{h}(P_1,P_k) \\ \vdots & & \vdots \\ \hat{h}(P_{i-1},P_1) & \cdots & \hat{h}(P_{i-1},P_k) \\ \hat{h}(P_{i+1},P_1) & \cdots & \hat{h}(P_{i+1},P_k) \\ \vdots & & \vdots \\ \hat{h}(P_{k+1},P_1) & \cdots & \hat{h}(P_{k+1},P_k) \end{bmatrix}$$

であるので, 行列 M_{k+1} の $(i, k+1)$ 余因子を a_i とすると $a_i = (-1)^{i+k+1}(-\det({}^tA_i)) = (-1)^{i+k}\det(A_i)$ $(i < k)$ である．また, $a_k = (-1)^{2k+1}\det({}^tA_k) = -\det(A_k)$ であり, $a_{k+1} = (-1)^{2k+2}\det(M_k) = \det(M_k)$ であることに注意する．任意の $1 \le j \le k$ について

$$x_1 \hat{h}(P_1,P_j) + \cdots + x_k \hat{h}(P_k,P_j) = \hat{h}(P_{k+1},P_j)$$

であるので,

$$\sum_{i=1}^{k-1} (-1)^{i+k} a_i \hat{h}(P_i,P_j) - a_k \hat{h}(P_k,P_j) - a_{k+1}\hat{h}(P_{k+1},P_j) = 0 \quad (2.13)$$

である．そこで c_i を (2.13) の左辺における $\hat{h}(P_i, P_j)$ の係数とすると，

$$c_1\hat{h}(P_1, P_j) + \cdots + c_k\hat{h}(P_k, P_j) + c_{k+1}\hat{h}(P_{k+1}, P_j) = 0$$

が成り立つ．いま，

$$\begin{aligned}\hat{h}\left(\sum_{i=1}^{k+1} c_iP_i\right) &= \hat{h}\left(\sum_{i=1}^{k+1} c_iP_i, \sum_{i=1}^{k+1} c_iP_i\right) = \hat{h}\left(\sum_{i=1}^{k+1} c_iP_i, \sum_{j=1}^{k+1} c_jP_j\right) \\ &= \sum_{j=1}^{k+1} c_j\hat{h}\left(\sum_{i=1}^{k+1} c_iP_i, P_j\right) = \sum_{j=1}^{k+1} c_j\left(\sum_{i=1}^{k+1} c_i\hat{h}(P_i, P_j)\right) = 0\end{aligned}$$

である．標準高さが 0 である点はねじれ点であるので，$\sum_{i=1}^{k+1} c_iP_i \in E(\mathbb{R})_{\mathrm{tors}}$ となり，従って

$$c_1P_1 + \cdots + c_kP_k + c_{k+1}P_{k+1} = 0 \ \text{ in } \ E(\mathbb{R})/E(\mathbb{R})_{\mathrm{tors}} \cong E(\mathbb{R})_{\mathrm{fr}}$$

となる． □

補題 2.3.35. 有理数体 $K = \mathbb{Q}$ 上の楕円曲線 E の K 有理点 $P_1, \ldots, P_k$ に対して，$k \times k$ 行列 $M_k = (\hat{h}(P_i, P_j))_{1 \le i,j \le k}$ を考える．このとき，$\det(M_k) \neq 0$ ならば $P_1, \ldots, P_k$ は $\mathbb{Z}$ 上で一次独立である．

■Step 0. 探索ステップにおける高さの上界 B の決定　命題 2.3.32 における記号を用いる．既に得られている Q_i たちから $h(Q_i)$ を計算し，

$$B_+ := \mu(E) + 2.14, \quad B_- := -\frac{1}{12}h(j(E)) - \mu(E) - 1.922,$$
$$B := B_+ + \max_{1 \le i \le n} h(Q_i)$$

とする．このとき

$$T := \{P \in E(\mathbb{Q}) : h(P) \le B - B_-\}$$

とすると，命題 2.3.32 により

$$\{Q_1, \ldots, Q_n\} \subset S := \{P \in E(\mathbb{Q}) : \hat{h}(P) \le B\} \subset T$$

である．従って補題 2.3.30 より S および T は $E(\mathbb{Q})$ を生成する．最終的に得られる $\mathcal{P}$ は一次独立であり，かつ $E(\mathbb{R})/E(\mathbb{R})_{\mathrm{tors}}$ において $\langle \mathcal{P} \rangle_{\mathbb{Z}} = \langle T \rangle_{\mathbb{Z}}$ を満たすので，これは $E(\mathbb{Q})_{\mathrm{fr}}$ の基底を与える．

■Step 1. 有理点探索　補題 2.3.20 に基づいて有理数 x で $H(x) \le B$ を満たすものを探索し，それを x 座標に持つ点 $P = (x, y) \in E(\mathbb{Q})$ が存在するかを確認する (E の定義方程式に x を代入して得られる y に関する二次方程式が $\mathbb{Q}$ 上で解を持つかを確認する)．

■Step 2. 高さ対を用いた独立性判定　高さ対 $\hat{h}(P_i, P_{k+1})$ $(i \leq k+1)$ を計算することで，$(k+1)$ 次正方行列 $M_{k+1} := (\hat{h}(P_i, P_j))_{1 \leq i,j \leq k+1}$ を得る．さらに $\det(M_{k+1})$ を計算する．

$\det(M_{k+1}) \neq 0$ の場合，補題 2.3.35 により $P_1, \ldots, P_k, P_{k+1}$ は $\mathbb{Z}$ 上で一次独立であり，$\langle \mathcal{P} \rangle_{\mathbb{Z}} \subset \langle P_1, \ldots, P_k, P_{k+1} \rangle_{\mathbb{Z}}$ かつ $P_{k+1} \notin \langle \mathcal{P} \rangle_{\mathbb{Z}}$ である．そこで $\mathcal{P} := \mathcal{P} \cup \{P_{k+1}\}$ として $\mathcal{P}$ を更新する．注意として，既に $k = r$ であれば $\det(M_{k+1}) \neq 0$ にはなり得ない．

$\det(M_{k+1}) = 0$ の場合，補題 2.3.34 により

$$a_1 \hat{h}(P_1, P_{k+1}) + \cdots + a_k \hat{h}(P_k, P_{k+1}) + a_{k+1} \hat{h}(P_{k+1}, P_{k+1}) = 0$$

なる等式を得る．ここで $a_i \in \mathbb{R}$ $(1 \leq i \leq k+1)$, $a_{k+1} \neq 0$ である．これらの a_i に対して，

$$a_1 P_1 + \cdots + a_k P_k + a_{k+1} P_{k+1} = 0 \ \text{ in } \ E(\mathbb{R})/E(\mathbb{R})_{\text{tors}}$$

である．各係数 a_i を有理数で近似し，分母を払うことで

$$b_1 P_1 + \cdots + b_k P_k + b_{k+1} P_{k+1} = 0 \ \text{ in } \ E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$$

の形 (ただし $b_i \in \mathbb{Z}$, $\gcd(b_1, \ldots, b_k, b_{k+1}) = 1$) の等式を得る．$a_{k+1} \neq 0$ より $b_{k+1} \neq 0$ であることに注意する．このとき，群 $\langle \mathcal{P} \rangle_{\mathbb{Z}}$ の，$\langle P_1, \ldots, P_k, P_{k+1} \rangle_{\mathbb{Z}}$ の部分群としての指数は $|b_{k+1}|$ の正の約数であることに注意する．もし，$|b_{k+1}| = 1$ ならば，$\langle \mathcal{P} \rangle_{\mathbb{Z}} = \langle P_1, \ldots, P_k, P_{k+1} \rangle_{\mathbb{Z}}$ であるので $\mathcal{P}$ の更新はしない．

$|b_{k+1}| > 1$ とする．また，$i := k+1$ とする．いま，$\gcd(b_1, \ldots, b_k, b_{k+1}) = 1$ であるので，ある $1 \leq j \leq k+1$ で $j \neq i$ なる添え字が存在して b_j は b_i で割り切れない．このような b_j を 1 つとる (b_1, b_2, b_3, ... と順に b_i で割っていけば求めることができる)．整数 q_j と r_j によって $b_j = b_i q_j + r_j$ と表す．ただし $0 < r_j < |b_i|$ である．このとき，

$$b_j P_j + b_i P_i = (b_i q_j + r_j) P_j + b_i P_i = r_j P_j + b_i (q_j P_j + P_i)$$

である．そこで $b'_j := r_j$, $b'_\ell := b_\ell$ $(1 \leq \ell \leq k+1, \ell \neq j)$, $P'_i := q_j P_j + P_i$, $P'_m := P_m$ $(1 \leq m \leq k+1, m \neq i)$ とすることで，関係式

$$b'_1 P'_1 + \cdots + b'_k P'_k + b'_{k+1} P'_{k+1} = 0 \ \text{ in } \ E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$$

を得る．注意として，b'_ℓ たちは全て整数，$|b'_j| < b_j$，$\langle P_1, \ldots, P_k, P_{k+1} \rangle_{\mathbb{Z}} = \langle P'_1, \ldots, P'_k, P'_{k+1} \rangle_{\mathbb{Z}}$ である．

このような操作を有限回繰り返すことで，点 $R_1, \ldots, R_k, R_{k+1} \in E(\mathbb{Q})$ および整数 $c_1, \ldots, c_k, c_{k+1}$ で関係式

$$c_1 R_1 + \cdots + c_k R_k + c_{k+1} R_{k+1} = 0 \ \text{ in } \ E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$$

を満たし，かつ，ある i について $c_i = 1$, さらに $\langle P_1, \ldots, P_k, P_{k+1}\rangle_{\mathbb{Z}} = \langle R_1, \ldots, R_k, R_{k+1}\rangle_{\mathbb{Z}}$ を満たすものを得る．添え字を付け替えて $c_{k+1} = 1$, 従って R_{k+1} は $R_1, \ldots, R_k$ の $\mathbb{Z}$ 上の線形和で書けるとしてよい．いま, $\langle \mathcal{P}\rangle_{\mathbb{Z}} \subset \langle P_1, \ldots, P_k, P_{k+1}\rangle_{\mathbb{Z}} = \langle R_1, \ldots, R_k\rangle_{\mathbb{Z}}$ であり, 群 $\langle \mathcal{P}\rangle_{\mathbb{Z}}$ の, $\langle P_1, \ldots, P_k, P_{k+1}\rangle_{\mathbb{Z}}$ の部分群としての指数は 2 以上であるので, $\langle R_1, \ldots, R_k\rangle_{\mathbb{Z}}$ は群 $\langle \mathcal{P}\rangle_{\mathbb{Z}}$ より真に大きい $E(\mathbb{Q})$ の部分群である．そこで $\mathcal{P} := \{R_1, \ldots, R_k\}$ として $\mathcal{P}$ を更新する．

注意 2.3.36. 実用的な計算の観点では, 高さの上界 B が大きすぎると探索ステップのコストおよびループ回数が増大するといった事態が生じ, 現実的な時間で計算が終了するかはわからない．このため, 有理点探索の高速化, より小さい上界 B の設定, あるいはループごとに上界 B を更新する, などといった様々な工夫がなされている (e.g. [5]).

2.4 複素数体上の楕円曲線

本節では複素数体 $\mathbb{C}$ 上の楕円曲線の性質を（証明なしに）述べる．

2.4.1 複素数平面内の格子と複素数体上の楕円曲線

複素数体 $\mathbb{C}$ 上の楕円曲線は，$\mathbb{C}$ 内の格子と呼ばれる離散部分群 Λ による商空間 $\mathbb{C}/\Lambda$（これはトーラス）に同型であり，さらにリーマン面に同型である．また，この逆も成り立つ．本小節ではこれらの事実を復習する．

定義 2.4.1 (格子). 複素数平面 $\mathbb{C}$ における**格子 (lattice)** とは，$\mathbb{R}$ 上線形独立な二つの複素数 ω_1, ω_2 の $\mathbb{Z}$ 上の線形結合全体からなる集合のことである．

注意 2.4.2. 格子 $\Lambda \subset \mathbb{C}$ と $m \in \mathbb{Z}_{\geq 1}$ に対して, $(1/m)\Lambda := \{(1/m)\omega : \omega \in \Lambda\}$ は格子であり，Λ を部分格子として含む．写像 $(1/m)\Lambda \to \mathbb{C}/\Lambda\ ;\ (1/m)\omega \mapsto (1/m)\omega + \Lambda$ は同型 $(1/m)\Lambda/\Lambda \cong (\mathbb{C}/\Lambda)_m$ を誘導する．ここで $(\mathbb{C}/\Lambda)_m$ は $\mathbb{C}/\Lambda$ の m ねじれ部分群である．また，$(1/m)\Lambda/\Lambda \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ であるので，$(\mathbb{C}/\Lambda)_m \cong (1/m)\Lambda/\Lambda \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ が成り立つ．

以下，$\Lambda = \langle \omega_1, \omega_2\rangle_{\mathbb{Z}}$ を ω_1, ω_2 で張られる複素数平面 $\mathbb{C}$ 内の格子とするとき，ω_1 と ω_2 の順序を付け替えて $\Im(\omega_2/\omega_1) > 0$ と仮定してよい；もし $\Im(\omega_1/\omega_2) \leq 0$ かつ $\Im(\omega_2/\omega_1) \leq 0$ ならば ω_1/ω_2 および ω_2/ω_1 の虚部は 0 であることが従い，ω_1 は ω_2 の実数倍で書けてしまう．

次の三つの命題 (命題 2.4.3 – 2.4.5) の証明は省略する．

命題 2.4.3. 複素数平面 $\mathbb{C}$ における格子 Λ に対して，商空間 $\mathbb{C}/\Lambda$ はリーマン面をなす．

命題 2.4.4. 複素数平面 $\mathbb{C}$ における二つの格子 Λ, Λ' に対して，商空間 $\mathbb{C}/\Lambda$, $\mathbb{C}/\Lambda'$ は同相（位相的に同型）である．これらがリーマン面として同型となるための必要十分条件は，ある $\alpha \in \mathbb{C}^\times$ が存在して $\Lambda' = \alpha\Lambda$ となることである．

命題 2.4.5.
1. 複素数体 $\mathbb{C}$ 上の楕円曲線 E に対して，ある格子 $\Lambda(E) = \langle\omega_1, \omega_2\rangle_{\mathbb{Z}} \subset \mathbb{C}$ が存在して，$E(\mathbb{C}) \cong \mathbb{C}/\Lambda(E)$ となる．
2. 任意の格子 $\Lambda \subset \mathbb{C}$ に対して，$\mathbb{C}$ 上のある楕円曲線 E が存在して，$E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ となる．

命題 2.4.6. 複素数体 $\mathbb{C}$ 上の楕円曲線 E と $m \in \mathbb{Z}_{\geq 1}$ に対して，

$$E_m(\mathbb{C}) := \{P \in E(\mathbb{C}) : mP = \mathcal{O}\} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

である．

証明. 命題 2.4.5 (1) により，ある格子 $\Lambda(E) \subset \mathbb{C}$ が存在して $E(\mathbb{C}) \cong \mathbb{C}/\Lambda(E)$ が成り立つ．従って，$E_m(\mathbb{C}) \cong (\mathbb{C}/\Lambda(E))_m \cong (1/m)\Lambda(E)/\Lambda(E) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ である． □

注意 2.4.7. 命題 2.4.6 の証明において，格子 Λ の基底を $\{\omega_1, \omega_2\}$ とするとき，

$$\left\{\frac{a}{m}\omega_1 + \frac{b}{m}\omega_2 : 0 \leq a, b \leq m-1\right\} \cong E_m(\mathbb{C})$$

であることに注意する．

定義 2.4.8. 複素数平面 $\mathbb{C}$ 上の有理型関数 $f(z)$ が格子 $\Lambda \subset \mathbb{C}$ に関する楕円関数 **(elliptic function)** であるとは，任意の $z \in \mathbb{C}$ と任意の $w \in \Lambda$ に対して $f(z+w) = f(z)$ が成り立つことである．

定義 2.4.9 (Weierstrass のペー関数). 複素数平面 $\mathbb{C}$ における格子 Λ に対して，

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \smallsetminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$$

と定め，これを格子 Λ に関する **Weierstrass のペー関数 (Weierstrass's $\wp$ function)** という．

注意 2.4.10. Weierstrass のペー関数は ω_1, ω_2 を基本周期対に持つ二重周期関数である．

Weierstrass のペー関数を用いることで，$\mathbb{C}/\Lambda$ に同型となる $\mathbb{C}$ 上の楕円曲線 E を構成できる．関数 $\wp(z)$ の $z = 0$ におけるローラン展開は

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) G_{2k+2}(\Lambda) z^{2k}$$

で与えられる．ここで，

$$G_{2k}(\Lambda) = \sum_{\omega \in \Lambda \smallsetminus \{0\}} \frac{1}{\omega^{2k}}$$

である．$G_{2k}(\Lambda)$ は $k > 1$ に対して絶対収束することが知られている．さらに

$$g_2(\Lambda) := 60G_4(\Lambda) = 60 \sum_{\omega \in \Lambda \smallsetminus \{0\}} \frac{1}{\omega^4},$$
$$g_3(\Lambda) := 140G_6(\Lambda) = 140 \sum_{\omega \in \Lambda \smallsetminus \{0\}} \frac{1}{\omega^6}$$

とおくことで

$$\wp(z) = z^{-2} + \frac{1}{20} g_2(\Lambda) z^2 + \frac{1}{28} g_3(\Lambda) z^4 + O(z^6)$$

となる．$g_2(\Lambda)$ と $g_3(\Lambda)$ を格子 Λ のモジュラー不変量と呼ぶ．また，$\Delta(\Lambda) := g_2^3 - 27g_3^2$ をモジュラー判別式 **(modular discriminant)** という．Weierstrass のペー関数は次の微分方程式を満たすことが知られている：

$$\wp'(z)^2 = 4\wp(z)^2 - g_2(\Lambda)\wp(z) - g_3(\Lambda).$$

命題 2.4.11. 複素数平面 $\mathbb{C}$ における格子 Λ に対して，

1. 多項式 $4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ は $\mathbb{C}$ 上で相異なる三つの根を持つ．
2. E を $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ で定義される $\mathbb{C}$ 上の楕円曲線とする．このとき，

$$\mathbb{C}/\Lambda \to E(\mathbb{C}) \subset \mathbf{P}^2(\mathbb{C}) \ ; \ z + \Lambda \mapsto [\wp(z) : \wp'(z) : 1]$$

は（群）同型写像である．

証明. (例えば) [4, Lemma 3.6, Corollary 3.9] を参照とする． □

$\Lambda' = \alpha\Lambda$ のとき，上のようにして構成される 2 つの楕円曲線 $\mathbb{C}/\Lambda$ と $\mathbb{C}/\Lambda'$ は同型となる．実際，$g_4(\Lambda) = \alpha^4 g_4(\alpha\Lambda)$ かつ $g_6(\Lambda) = \alpha^6 g_6(\alpha\Lambda)$ であり，二つの楕円曲線の j 不変量 (2.5.1 節参照) は等しい．

2.5 楕円曲線の同種・同型

本節では，楕円曲線の同種という概念を導入し，2 つの楕円曲線が同型かどうかを判定する量として j 不変量を定義する．

2.5.1 同種写像

定義 2.5.1 (楕円曲線の同種写像). 体 K 上の 2 つの楕円曲線 E_1, E_2 が**同種 (isogenous)** であるとは，次を満たすような定値でない写像 $\phi : E_1 \to E_2$ が存在するときをいう：

1. ϕ は有理関数である．すなわち，$P = (x, y) \in E_1$ に対して，$\phi(P) \in E_2$ の各座標が x, y の有理式で書ける．
2. ϕ は加法に関する準同型である．すなわち，$P, Q \in E_1$ に対して，$\phi(P + Q) = \phi(P) + \phi(Q)$ を満たす．

このとき ϕ を E_1 の**同種写像 (isogeny)** という．全単射な同種写像を**同型写像 (isomorphism)** という．E_1 から E_2 への同型写像が存在するとき E_1 と E_2 は**同型 (isomorphic)** であるといい，$E_1 \cong E_2$ と書く．

方程式 (2.1) で与えられる K 上の楕円曲線

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

を考える．ここで $a_i \in K$ $(i = 1, 2, 3, 4, 6)$ とする．そこで

$$b_2 = a_1^2 + 4a_2, \qquad b_4 = a_1a_3 + 2a_4, \qquad b_6 = a_3^2 + 4a_6,$$
$$c_4 = b_2^2 - 24b_4, \qquad c_6 = -b_2^3 + 36b_2b_4 - 216b_6$$

としたことを思い出そう．

定義 2.5.2. 方程式 (2.1) で与えられる K 上の楕円曲線 E に対して，$j(E) = \frac{c_4^3}{\Delta(E)}$ と定義し，これを E の j **不変量 (j-invariant)** という．方程式 (2.6) で与えられる K 上の楕円曲線 E' に対して，$j(E') = -12^3 \cdot \frac{(4a)^3}{\Delta(E')}$ である．

命題 2.5.3. 体 K 上の楕円曲線 E_1, E_2 に対して，$j(E_1) = j(E_2)$ と $E_1 \cong E_2$ (over $\overline{K}$) は同値である．

2.5.2 虚数乗法を持つ楕円曲線

K を体とし，E を K 上の楕円曲線とする．E から E への K 準同型写像全体のなす環を $\mathrm{End}_K(E)$ と書き，これを E の K **自己準同型環**と呼ぶ．このとき，

$$\mathbb{Z} \to \mathrm{End}_K(E)\ ;\ m \mapsto ([m] : P \mapsto mP) \tag{2.14}$$

なる単射によって $\mathrm{End}_K(E)$ は $\mathbb{Z}$ を部分環として含む．

定義 2.5.4 (虚数乗法). 写像 (2.14) が全単射でない，すなわち $\mathrm{End}_K(E)$ が $\mathbb{Z}$ より真に大きくなるとき, E は K 上で**虚数乗法 (Complex Multiplication, CM)** を持つという．E が $\overline{K}$ 上で虚数乗法を持つときは，単に E は虚数乗法を持つという．

例 2.5.5. 標数が 2 でない体 K 上の楕円曲線 $E : y^2 = x^3 + x$ を考える．代数閉包 $\overline{K}$ における -1_K の平方根の一つを i とする．自己準同型環 $\mathrm{End}(E)$ は

$$[i]_E : (x, y) \mapsto (-x, iy)$$

を含む．ここで写像

$$\mathbb{Z}[i] \to \mathrm{End}(E)\ ;\ m + ni \mapsto [n] + [n] \cdot [i]_E$$

は単射準同型である（K の標数が 0 のときは上の写像は全単射である）．従って E は虚数乗法を持つ.

命題 2.5.6. E を体 K 上の楕円曲線とする．このとき，次のいずれかが成り立つ：

1. $\mathrm{End}_K(E) \cong \mathbb{Z}$,
2. $F := \mathrm{End}_K(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ は虚二次体，従って $\mathrm{End}_K(E) \cong \mathcal{O}_F$,
3. $\mathrm{End}_K(E)$ は $\mathbb{Q}$ 上の四元数代数の整環に同型である.

ただし，体 K の標数が 0 の場合は (1) または (2), 標数が正の場合は (2) または (3) に限る.

2.6 本講演の次の講演以降で重要となる事項の導入

本節では本講演の次の講演以降で重要となった事項（2 次元 Galois 表現, モジュラー曲線の定義）を導入する.

2.6.1 2 次元 Galois 表現

ここでは 2 次元 Galois 表現の概念を簡単に紹介する．動機や有用性などは 2 日目以降の吉川祥氏（学習院大学）の講演に譲るものとした.

体 K の分離閉包 (separable closure) を K^s と書き，$G_K := \mathrm{Gal}(K^s/K)$ とする．E を体 K 上の楕円曲線とするとき，G_K は $E[N]$ に $(\sigma, P) \mapsto \sigma(P)$ ($\sigma \in G_K$, $P \in E[N]$) によって作用する．この作用は法 N での表現

$$\rho_{E,N} : G_K \to \mathrm{Aut}(E[N])$$

を誘導する．ここで $\mathrm{Aut}(E[N])$ は群 $E[N]$ の自己同型群である．もし

$\mathrm{char}(K)$ が N を割り切らないならば $\mathrm{Aut}(E[N]) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ が成り立つ.

例 2.6.1. 有理数体 $K = \mathbb{Q}$ 上の楕円曲線 $E : y^2 = x^3 - x$ について,

$$\rho_{E,2}(\sigma) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{2.15}$$

が任意の $\sigma \in G_K$ に対して成り立つ. 実際, $y^2 = x^3 - x = x(x+1)(x-1)$ であるから, $E(\mathbb{Q})[2] = \{\mathcal{O}, (-1,0), (0,1), (1,0)\} \cong \mathbb{F}_2^2$ であり, $E[2] := E(\overline{\mathbb{Q}})[2]$ の $\mathcal{O}$ でない元の x 座標と y 座標はともに有理数である. 従って, 任意の $P \in E[2]$ に対して $\sigma(P) = P$, 特に $E[2]$ の $\mathbb{F}_2$ 上ベクトル空間としての基底 $\{P_1, P_2\}$ について $\sigma(P_1) = 1 \cdot P_1 + 0 \cdot P_2$ かつ $\sigma(P_2) = 0 \cdot P_1 + 1 \cdot P_2$ を満たすので, (2.15) が成り立つ.

素数 ℓ と ℓ^n 等分点の集合の族 $\{E[\ell^n]\}_n$ および写像

$$E[\ell^{n+1}] \to E[\ell^n] \ ; \ P \mapsto \ell P$$

が定める逆系 $\{E[\ell^{n+1}] \to E[\ell^n] \ ; \ P \mapsto \ell P\}_n$ に対して,

$$T_\ell(E) := \varprojlim_n E[\ell^n] \cong \mathbb{Z}_\ell^{\oplus 2}, \quad V_\ell(E) := T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$$

と定義する. ここで $\mathbb{Z}_\ell$, $\mathbb{Q}_\ell$ はそれぞれ ℓ 進整数環, ℓ 進有理数体を表す. $T_\ell(E)$ は自由 $\mathbb{Z}_\ell$ 加群であり, $V_\ell(E)$ は $\mathbb{Q}_\ell$ ベクトル空間である.

定義 2.6.2. $T_\ell(E)$ を E の ℓ 進 **Tate 加群 (ℓ-adic Tate module)**, $V_\ell(E)$ を E の ℓ 進有理 **Tate 加群 (ℓ-adic rational Tate module)** と呼ぶ.

E を体 K 上の楕円曲線とすると, G_K は $V_\ell(E)$ に作用する. この作用は ℓ 進表現

$$\rho_{E,\ell^\infty} : G_K \to \mathrm{Aut}(V_\ell(E))$$

を誘導する. ここで $\mathrm{Aut}(V_\ell(E))$ は群 $V_\ell(E)$ の自己同型群である. もし $\mathrm{char}(K) \neq \ell$ ならば $V_\ell(E) \cong \mathbb{Q}_\ell^2$ (群同型), $\mathrm{Aut}(V_\ell(E)) \cong \mathrm{GL}_2(\mathbb{Q}_\ell)$ が成り立つ.

2.6.2 モジュラー曲線

ここではモジュラー曲線の定義や楕円曲線との関係を簡単に紹介する. 動機や有用性などは 2 日目以降の木村巌氏（富山大）の講演に譲るものとした.

$\mathbb{H} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ を $\mathbb{C}$ の上半平面とし,

$$\begin{aligned} \mathrm{SL}_2(\mathbb{Z}) &:= \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{Mat}_2(\mathbb{Z}) : ad - bc = 1 \right\} \\ &= \{A \in \mathrm{GL}_2(\mathbb{Z}) : \det(A) = 1\} \end{aligned}$$

を有理整数環 $\mathbb{Z}$ 上の二次特殊線形群とする．ここで $\mathrm{Mat}_2(\mathbb{Z})$ は $\mathbb{Z}$ の元を成分に持つ二次正方行列全体のなす集合である．特殊線形群 $\mathrm{SL}_2(\mathbb{Z})$ はモジュラー群 **(modular group)** とも呼ばれ，

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} z = \frac{az+b}{cz+d} \quad \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}),\ z \in \mathbb{H} \right)$$

なる一次分数変換によって $\mathbb{H}$ に作用する．自然数 $N > 0$ に対して，$\mathrm{SL}_2(\mathbb{Z})$ の部分群 $\Gamma(N), \Gamma_1(N), \Gamma_0(N)$ を次で定義する：

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \bmod N \right\},$$
$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \bmod N \right\},$$
$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \bmod N \right\}.$$

このとき，$\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N)$ であり，これらは全て $\mathrm{SL}_2(\mathbb{Z})$ の離散部分群である．

定義 2.6.3 (合同部分群)．モジュラー群 $\mathrm{SL}_2(\mathbb{Z})$ の部分群 Γ が合同部分群 **(congruence subgroup)** であるとは，ある自然数 $N > 0$ に対して $\Gamma(N) \subset \Gamma$ を満たすことである．そのような自然数 N のうち最小なものを合同部分群 Γ のレベルという．合同部分群は $\mathrm{SL}_2(\mathbb{Z})$ の離散部分群であり，上半平面 $\mathbb{H}$ に真性不連続に **(properly discontinuously)** 作用する：任意のコンパクト部分集合 $K_1, K_2 \subset \mathbb{H}$ に対して，集合 $\{\gamma \in \Gamma : (\gamma \cdot K_1) \cap K_2 \neq \emptyset\}$ は有限集合である．

注意 2.6.4. 自然数 $N > 0$ に対して，$\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N)$ であり，これらは全て $\mathrm{SL}_2(\mathbb{Z})$ におけるレベル N の合同部分群である．

定義 2.6.5 (モジュラー曲線)．レベル N の合同部分群 $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ に対して $Y(\Gamma) := \Gamma \setminus \mathbb{H}$ をレベル N の（非コンパクト）モジュラー曲線と呼ぶ．

注意 2.6.6. $Y(\Gamma)$ はリーマン面の構造を持つ．$Y(\Gamma)$ にカスプと呼ばれる有限個の点を付け加えることによってコンパクトなリーマン面 $X(\Gamma)$ を構成することができる．これをコンパクト化された (レベル N の) モジュラー曲線と呼ぶ．

謝辞

2017 年度第 25 回整数論サマースクール「楕円曲線とモジュラー形式の計算」主催者並びにプログラム責任者の皆様方に感謝申し上げます．また，九州大学大学院数理学府の学生である馬渕圭史氏，横田祐貴氏には本講演の予行発

表にお付き合いいただき，多くの助言やコメントをいただきました．併せて御
礼申し上げます．

参考文献

[1] J. Cremona, *Algorithms for modular elliptic curves*, second edition, Cambridge University Press, Cambridge, 1997.

[2] J. S. Milne, *Elliptic Curves*, BookSurge Publishers, ISBN: 1-4196-5275-5, 2006.

[3] 伊豆哲也, 楕円曲線暗号入門, 2010, available at `http://researchmap.jp/mulzrkzae-42427/# 42427`

[4] J. S. Milne, *Elliptic Curves*, BookSurge Publishing, 2006 (電子版: `http://www.jmilne.org/math/Books/ectext5.pdf`)

[5] S. Siksek, *Infinite descent on elliptic curves*, Rocky Mountain J. Math., **25**, 1995, no. 4, pp. 1501–1538.

[6] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **151**, Springer-Verlag, New York, 1994.

[7] J. H. Silverman, *The arithmetic of elliptic curves*, Corrected reprint of the 1986 original, Graduate Texts in Mathematics, **106**, Springer-Verlag, New York, 1992.

[8] J. H. Silverman, *The difference between the Weil height and the canonical height on elliptic curves*, Math. Comp., **55**, 1990, no. 192, pp. 723–743.

[9] J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, UTM, 1992.

[10] D. Simon, *Computing the rank of elliptic curves over number fields*, LMS JCM, **5**, 2002, pp. 7–17.

[11] 横山俊一, 計算する立場からの楕円曲線論入門, 山形大学理学部数理科学科 2014 年度後期「数理情報特選 F/数理科学特別講義 E」講義資料, available at `http://www2.math.kyushu-u.ac.jp/s̃-yokoyama/Yamagata2014.html`

[12] 横山俊一, 楕円曲線の計算にみる数論システムの進展状況, 数理解析研究所講究録, **1785**, pp. 57–66, 2012.