Vélu の公式とその応用

東北大・理　佐藤 篤 (Atsushi SATO)

E を完全体 k 上定義された楕円曲線, Γ を $E(\bar{k})$ の有限な部分群で $\mathrm{Gal}(\bar{k}/k)$-不変なものとする. このとき, k 上定義された楕円曲線 E^* と k 上定義された分離的な同種写像 $\lambda : E \to E^*$ で $\mathrm{Ker}\,\lambda = \Gamma$ となるようなものが k-同型の違いを除いて一意的に存在する (E^* は E/Γ とも書かれる). その証明の概略は次の通りである:

(i) 群 Γ は

$$T \cdot f = f \circ \tau_T \qquad \big(T \in \Gamma,\ f \in \bar{k}(E)\big)$$

により $\bar{k}(E)$ に作用する;

(ii) 上の作用に関して不変で, かつ k 上定義されているような函数全体のなす体

$$\bar{k}(E)^{\Gamma} \cap k(E)$$

を函数体とするような k 上の楕円曲線 E^* が存在する;

(iii) 自然な単射 $k(E^*) \to k(E)$ が引き起こす k 上の同種写像 $\lambda : E \to E^*$ は分離的で, $\mathrm{Ker}\,\lambda = \Gamma$ となっている.

E の Weierstrass 方程式と Γ が与えられたときに, 上で述べたような楕円曲線 E^* と同種写像 $\lambda : E \to E^*$ を具体的に与えるのが表題にある Vélu の公式である. 本稿の前半では, まず §1 で複素数体上の楕円曲線について簡単に復習した後, §2 と §3 で Vélu の原論文 [V] の解説を行う. Vélu の公式は, 体 k の標数が正でも使え, また一般的な形の Weierstrass 方程式を扱えることから, 有限体上定義された楕円曲線の間の同種写像を調べるのに用いられることが多いようである (例えば [L-M]). 本稿の後半では, §4 で Vélu の公式が与える同種写像の形に関する注意を述べ, それを用いて §5 で同種写像と離散付値による還元との関係を (特殊な場合について) 調べた後, §6 と §7 で代数的整数論への応用を述べる.

1 複素数体上の場合

Vélu の公式の解説に入る前に, k が複素数体 $\mathbb{C}$ の場合について, E と Γ から E^* と λ を与える方法を述べておく.

よく知られているように, E が $\mathbb{C}$ 上定義された楕円曲線の場合には, $\mathbb{C}$ 内の格子 L が存在して $E(\mathbb{C})$ は複素トーラス $\mathbb{C}/L$ と複素 Lie 群として同型になり, L に付随する Weierstrass の $\wp$-函数

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

がみたす微分方程式

$$\wp'_L(z)^2 = 4\wp_L(z)^3 - 60G_4(L)\,\wp_L(z) - 140G_6(L)$$

から E の方程式が得られる. ここで,

$$G_{2j}(L) = \sum_{\omega \in L-\{0\}} \frac{1}{\omega^{2j}} \qquad (j \geq 2)$$

は重さ $2j$ の Eisenstein 級数である. また, $E(\mathbb{C})$ の部分群 Γ には L を含むような格子 L^* が対応し, そのとき同種写像 $\lambda : E \to E^*$ には $\mathbb{C}/L$ から $\mathbb{C}/L^*$ への自然な写像が対応する:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L^*/L & \longrightarrow & \mathbb{C}/L & \longrightarrow & \mathbb{C}/L^* & \longrightarrow & 0 \\ & & \downarrow\wr & \circlearrowright & \downarrow\wr & \circlearrowright & \downarrow\wr & & \\ 0 & \longrightarrow & \Gamma & \longrightarrow & E(\mathbb{C}) & \xrightarrow{\lambda} & E^*(\mathbb{C}) & \longrightarrow & 0 \end{array}$$

(横の列は共に完全).

さて, L^* に付随する $\wp$-函数は L に付随する $\wp$-函数を用いて

$$\wp_{L^*}(z) = \wp_L(z) + \sum_{\omega^* \in L^*/L-\{0\}} \big(\wp_L(z+\omega^*) - \wp_L(\omega^*) \big) \tag{1.1}$$

と表せる. この式の両辺を微分して,

$$\wp'_{L^*}(z) = \sum_{\omega^* \in L^*/L} \wp'_L(z+\omega^*). \tag{1.2}$$

これら 2 式と $\wp$-函数の加法公式により, $\wp_{L^*}(z)$ と $\wp'_{L^*}(z)$ は $\wp_L(z)$, $\wp'_L(z)$, $G_4(L)$, $G_6(L)$ ならびに $\wp_L(\omega^*)$, $\wp'_L(\omega^*)$ $(\omega^* \in L^* - L)$ の有理式として表せることがわかる. それを具体

的に計算すれば, 同種写像 $\lambda : E \to E^*$ の代数的な表示が得られる. さらに

$$G_{2j}(L^*) = G_{2j}(L) + \frac{1}{(2j-1)!} \sum_{\omega^* \in L^*/L - \{0\}} \wp_L^{(2j-2)}(\omega^*)$$

より, $G_4(L^*)$ と $G_6(L^*)$ は $G_4(L)$, $G_6(L)$ ならびに $\wp_L(\omega^*)$, $\wp_L'(\omega^*)$ $(\omega^* \in L^* - L)$ の多項式として表せることがわかる. すなわち, E^* の方程式は E の方程式と Γ の座標から具体的に計算できる. なお,

$$\sum_{\omega^* \in L^*/L - \{0\}} \wp_L'(\omega^*) = 0$$

であるから, (1.2) は

$$\wp_{L^*}'(z) = \wp_L'(z) + \sum_{\omega^* \in L^*/L - \{0\}} \left(\wp_L'(z + \omega^*) - \wp_L'(\omega^*) \right) \tag{1.3}$$

と書いてもよい. また, 自明な式ではあるが,

$$\frac{d\wp_L}{\wp_L'}(z) = \frac{d\wp_{L^*}}{\wp_{L^*}'}(z) = dz \tag{1.4}$$

が成り立つことを注意しておく.

2 Vélu の公式

本節では, Vélu の公式を手短に述べ, いくつかの計算例を与える.

いま, E が方程式

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \qquad (a_i \in k) \tag{2.1}$$

により与えられているとする. まず, $g^x, g^y \in k(E)$ をそれぞれ

$$g^x = 3x^2 + 2a_2 x + a_4 - a_1 y, \qquad g^y = -2y - a_1 x - a_3 \tag{2.2}$$

によって定める. 以下, E 上の点 $Q \neq O$ に対して $x(Q)$, $y(Q)$, $g^x(Q)$, $g^y(Q)$ をそれぞれ x_Q, y_Q, g_Q^x, g_Q^y と略記することにし,

$$t_Q = \begin{cases} g_Q^x & \text{if } Q \in E[2] \\ 2g_Q^x - a_1 g_Q^y & \text{otherwise} \end{cases}, \qquad u_Q = (g_Q^y)^2$$

と置く. 次に, $(\Gamma - \{O\})/\pm 1$ の完全代表系 $S \subset \Gamma$ をとり,

$$t = \sum_{T \in S} t_T, \qquad w = \sum_{T \in S} (u_T + x_T t_T)$$

と置く. これらは S の選び方に依らず, また $t, w \in k$ となっている. さらに,

$$A_1 = a_1, \quad A_2 = a_2, \quad A_3 = a_3, \quad A_4 = a_4 - 5t, \quad A_6 = a_6 - (a_1^2 + 4a_2)t - 7w \tag{2.3}$$

と置く. 以上の記号の下で, Vélu の公式は次のように述べられる:

定理 2.1 (Vélu の公式) 楕円曲線 $E^* = E/\Gamma$ と $\mathrm{Ker}\,\lambda = \Gamma$ なる k 上定義された分離的な同種写像 $\lambda : E \to E^*$ はそれぞれ

$$Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6 \tag{2.4}$$

と

$$\begin{aligned} X &= x + \sum_{T \in S} \left(\frac{t_T}{x - x_T} + \frac{u_T}{(x - x_T)^2} \right), \\ Y &= y - \sum_{T \in S} \left(u_T \, \frac{2y + a_1x + a_3}{(x - x_T)^3} + t_T \, \frac{a_1(x - x_T) + y - y_T}{(x - x_T)^2} + \frac{a_1u_T - g_T^x g_T^y}{(x - x_T)^2} \right) \end{aligned} \tag{2.5}$$

により与えられる.

例 2.2 ($\Gamma \cong \mathbb{Z}/2\mathbb{Z}$ の場合) E が位数 2 の k-有理点をもつとき, その方程式として

$$y^2 + axy = x^3 + bx^2 + cx \qquad \big(a, b, c \in k,\ c(a^4 + 8a^2b + 16b^2 - 64c) \neq 0\big) \tag{2.6}$$

なるものがとれて, $T_0 = (0, 0)$ が位数 2 の点を与える. 点 T_0 が生成する $E(k)$ の部分群を Γ と置くと, S としては $\{T_0 = (0, 0)\}$ がとれて,

$$\begin{gathered} a_1 = a, \quad a_2 = b, \quad a_3 = 0, \quad a_4 = c, \quad a_6 = 0; \\ g^x = 3x^2 + 2bx + c - ay, \quad g^y = -2y - ax; \\ g^x_{T_0} = c, \quad g^y_{T_0} = 0, \quad t_{T_0} = c, \quad u_{T_0} = 0; \\ t = c, \quad w = 0; \\ A_1 = a, \quad A_2 = b, \quad A_3 = 0, \quad A_4 = -4c, \quad A_6 = -a^2c - 4bc \end{gathered}$$

となる. 従って, 楕円曲線 E^* と同種写像 $\lambda : E \to E^*$ はそれぞれ

$$Y^2 + aXY = X^3 + bX^2 - 4cX - a^2c - 4bc \tag{2.7}$$

と

$$X = \frac{x^2 + c}{x}$$

(Y の方は省略) により与えられる. なお, (2.6), (2.7) の判別式はそれぞれ

$$\Delta = c^2(a^4 + 8a^2b + 16b^2 - 64c), \qquad \Delta^* = c(a^4 + 8a^2b + 16b^2 - 64c)^2$$

となる.

例 2.3 ($\Gamma \cong \mathbb{Z}/3\mathbb{Z}$ **の場合**) E が位数 3 の k-有理点をもつとき, その方程式として

$$y^2 + axy + by = x^3 \qquad \big(a, b \in k,\ b(a^3 - 27b) \neq 0\big) \tag{2.8}$$

なるものがとれて, $T_0 = (0, 0)$ が位数 3 の点を与える. 点 T_0 が生成する $E(k)$ の部分群を Γ と置くと, S としては $\{T_0 = (0, 0)\}$ がとれて,

$$\begin{gathered}
a_1 = a, \quad a_2 = 0, \quad a_3 = b, \quad a_4 = 0, \quad a_6 = 0; \\
g^x = 3x^2 - ay, \quad g^y = -2y - ax - b; \\
g^x_{T_0} = 0, \quad g^y_{T_0} = -b, \quad t_{T_0} = ab, \quad u_{T_0} = b^2; \\
t = ab, \quad w = b^2; \\
A_1 = a, \quad A_2 = 0, \quad A_3 = b, \quad A_4 = -5ab, \quad A_6 = -a^3b - 7b^2
\end{gathered}$$

となる. 従って, 楕円曲線 E^* と同種写像 $\lambda : E \to E^*$ はそれぞれ

$$Y^2 + aXY + bY = X^3 - 5abX - a^3b - 7b^2 \tag{2.9}$$

と

$$X = \frac{x^3 + abx + b^2}{x^2}$$

(Y の方は省略) により与えられる. なお, (2.8), (2.9) の判別式はそれぞれ

$$\Delta = b^3(a^3 - 27b), \qquad \Delta^* = b(a^3 - 27b)^3$$

となる.

例 2.4 ($\Gamma \cong \mathbb{Z}/5\mathbb{Z}$ **の場合**) E が位数 5 の k-有理点をもつとき, その方程式として

$$y^2 + (a + b)xy + ab^2y = x^3 + abx^2 \qquad \big(a, b \in k,\ ab(a^2 + 11ab - b^2) \neq 0\big) \tag{2.10}$$

なるものがとれて, $T_0=(0,0)$ が位数 5 の点を与える. 点 T_0 が生成する $E(k)$ の部分群を Γ と置くと, S としては $\{T_0=(0,0),\ [2]T_0=(-ab,a^2b)\}$ がとれて,

$$\begin{gathered}
a_1=a+b,\quad a_2=ab,\quad a_3=ab^2,\quad a_4=0,\quad a_6=0;\\
g^x=3x^2+2abx-(a+b)y,\quad g^y=-2y-(a+b)x-ab^2;\\
g^x_{T_0}=0,\quad g^y_{T_0}=-ab^2,\quad t_{T_0}=a^2b^2+ab^3,\quad u_{T_0}=a^2b^4;\\
g^x_{[2]T_0}=-a^3b,\quad g^y_{[2]T_0}=-a^2b,\quad t_{[2]T_0}=-a^3b+a^2b^2,\quad u_{[2]T_0}=a^4b^2;\\
t=-a^3b+2a^2b^2+ab^3,\quad w=2a^4b^2-a^3b^3+a^2b^4;\\
A_1=a+b,\quad A_2=ab,\quad A_3=ab^2,\quad A_4=5(a^3b-2a^2b^2-ab^3),\\
A_6=a^5b-10a^4b^2-5a^3b^3-15a^2b^4-ab^5
\end{gathered}$$

となる. 従って, 楕円曲線 E^* と同種写像 $\lambda:E\to E^*$ はそれぞれ

$$\begin{aligned}Y^2+(a+b)XY+ab^2Y=X^3+abX^2+5(a^3b-2a^2b^2-ab^3)X\\ +a^5b-10a^4b^2-5a^3b^3-15a^2b^4-ab^5\end{aligned}\tag{2.11}$$

と

$$X=\frac{x^5+2abx^4+(-a^3b+3a^2b^2+ab^3)x^3+(3a^3b^3+3a^2b^4)x^2+(a^4b^4+3a^3b^5)x+a^4b^6}{x^2(x+ab)^2}$$

(Y の方は省略) により与えられる. なお, (2.10), (2.11) の判別式はそれぞれ

$$\Delta=-a^5b^5(a^2+11ab-b^2),\qquad \Delta^*=-ab(a^2+11ab-b^2)^5$$

となる.

例 2.5 ($\Gamma\cong\mathbb{Z}/7\mathbb{Z}$ **の場合**) E が位数 7 の k-有理点をもつとき, その方程式として

$$\begin{gathered}y^2+(a^2+ab-b^2)xy+a^3b^2(a-b)y=x^3+ab^2(a-b)x^2\\ \big(a,b\in k,\ ab(a-b)(a^3+5a^2b-8ab^2+b^3)\neq 0\big)\end{gathered}\tag{2.12}$$

なるものがとれて, $T_0=(0,0)$ が位数 7 の点を与える. 点 T_0 が生成する $E(k)$ の部分群を Γ と置くと, S としては

$$\big\{T_0=(0,0),\ [2]T_0=\big(-ab^2(a-b),\,ab^3(a-b)^2\big),\ [3]T_0=\big(-a^2b(a-b),\,a^3b(a-b)^2\big)\big\}$$

がとれて,

$$a_1 = a^2 + ab - b^2, \quad a_2 = ab^2(a-b), \quad a_3 = a^3b^2(a-b), \quad a_4 = 0, \quad a_6 = 0;$$
$$g^x = 3x^2 + 2ab^2(a-b)x - (a^2+ab-b^2)y, \quad g^y = -2y - (a^2+ab-b^2)x - a^3b^2(a-b);$$
$$g^x_{T_0} = 0, \quad g^y_{T_0} = -a^3b^2(a-b),$$
$$t_{T_0} = a^3b^2(a-b)(a^2+ab-b^2), \quad u_{T_0} = a^6b^4(a-b)^2;$$
$$g^x_{[2]T_0} = -ab^3(a-b)^3(a+b), \quad g^y_{[2]T_0} = -ab^3(a-b)^2,$$
$$t_{[2]T_0} = -ab^3(a-b)^2(a^2-ab-b^2), \quad u_{[2]T_0} = a^2b^6(a-b)^4;$$
$$g^x_{[3]T_0} = -a^3b(a-b)^4, \quad g^y_{[3]T_0} = -a^2b(a-b)^3,$$
$$t_{[3]T_0} = -a^2b(a-b)^3(a^2-3ab+b^2), \quad u_{[3]T_0} = a^4b^2(a-b)^6;$$
$$t = -ab(a-b)(a^5 - 6a^4b + 8a^3b^2 - 6a^2b^3 + ab^4 + b^5),$$
$$w = a^2b^2(a-b)^2(2a^6 - 9a^5b + 15a^4b^2 - 8a^3b^3 + a^2b^4 - 2ab^5 + 2b^6);$$
$$A_1 = a^2 + ab - b^2, \quad A_2 = ab^2(a-b), \quad A_3 = a^3b^2(a-b),$$
$$A_4 = 5ab(a-b)(a^2-ab+b^2)(a^3 - 5a^2b + 2ab^2 + b^3),$$
$$A_6 = ab(a-b)\ (a^9 - 18a^8b + 76a^7b^2 - 182a^6b^3 + 211a^5b^4 - 132a^4b^5 + 70a^3b^6 - 37a^2b^7 + 9ab^8 + b^9)$$

となる. 従って, 楕円曲線 E^* は

$$\begin{aligned} &Y^2 + (a^2+ab-b^2)XY + a^3b^2(a-b)Y \\ &\quad = \ X^3 + ab^2(a-b)X^2 \\ &\qquad +5ab(a-b)(a^2-ab+b^2)(a^3-5a^2b+2ab^2+b^3)X \\ &\qquad +ab(a-b)\ (a^9 - 18a^8b + 76a^7b^2 - 182a^6b^3 + 211a^5b^4 \\ &\qquad\qquad -132a^4b^5 + 70a^3b^6 - 37a^2b^7 + 9ab^8 + b^9) \end{aligned} \tag{2.13}$$

により与えられる ($\lambda : E \to E^*$ の表示は省略). なお, (2.12), (2.13) の判別式はそれぞれ

$$\Delta = -a^7b^7(a-b)^7(a^3+5a^2b-8ab^2+b^3), \qquad \Delta^* = -ab(a-b)(a^3+5a^2b-8ab^2+b^3)^7$$

となる.

3 公式の証明

まず初めに, 証明の方針を述べる.

各 $Q \in E(\bar{k})$ に対し,

$$\mathrm{ord}_Q : \bar{k}(E) \longrightarrow \mathbb{Z} \cup \{\infty\}$$

を Q に付随する正規化された加法付値とする. このとき, E の方程式 (2.1) を与えることと, 条件

$$\begin{aligned} &\mathrm{ord}_O(x) = -2, \quad \mathrm{ord}_O(y) = -3, \quad \frac{y^2}{x^3}(O) = 1; \\ &\mathrm{ord}_Q(x) \geq 0, \quad \mathrm{ord}_Q(y) \geq 0 \qquad \text{if } Q \in E(\bar{k}) - \{O\} \end{aligned} \tag{3.1}$$

をみたす $x, y \in k(E)$ を与えることとは同等である.

さて, $z = -x/y$ と置くと $\mathrm{ord}_O(z) = 1$ であるから, x, y を z によって点 O の近傍で Laurent 展開することができる:

$$\begin{aligned} x &= z^{-2} - \alpha_1 z^{-1} - \alpha_2 - \alpha_3 z - \alpha_4 z^2 - \alpha_5 z^3 - \alpha_6 z^4 - \cdots, \\ y &= -\frac{x}{z} = -z^{-3} + \alpha_1 z^{-2} + \alpha_2 z^{-1} + \alpha_3 + \alpha_4 z + \alpha_5 z^2 + \alpha_6 z^3 + \cdots \end{aligned} \qquad (\alpha_i \in k). \tag{3.2}$$

これを (2.1) に代入し, 0 次までの係数を比較することにより,

$$\begin{aligned} &\alpha_1 = a_1, \quad \alpha_2 = a_2, \quad \alpha_3 = a_3, \quad \alpha_4 = a_1 a_3 + a_4, \\ &\alpha_5 = a_2 a_3 + a_1^2 a_3 + a_1 a_4, \quad \alpha_6 = a_1^2 a_4 + a_1^3 a_3 + a_2 a_4 + 2a_1 a_2 a_3 + a_3^2 + a_6 \end{aligned} \tag{3.3}$$

を得る. これより, a_1, a_2, a_3, a_4, a_6 は $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_6$ で表せることがわかる.

ところで, 以上の議論は E^* に対しても適用できる. すなわち, E^* の方程式 (2.4) を得るためには, 条件

$$\begin{aligned} &\mathrm{ord}_O(X) = -2, \quad \mathrm{ord}_O(Y) = -3, \quad \frac{Y^2}{X^3}(O) = 1; \\ &\mathrm{ord}_Q(X) \geq 0, \quad \mathrm{ord}_Q(Y) \geq 0 \qquad \text{if } Q \in E(\bar{k}) - \Gamma \end{aligned} \tag{3.4}$$

をみたす $X, Y \in \bar{k}(E)^\Gamma \cap k(E)$ を構成し, X の $Z = -X/Y$ による点 O の近傍での Laurent 展開 (の初めの方) を計算すればよい. また, 上の X, Y を x, y の有理式で表せば, 同種写像 $\lambda : E \to E^*$ の形がわかることになる.

以上の準備の下で, Vélu の公式は次のようにして示される:

[定理 2.1 の証明] まず, $X, Y \in \bar{k}(E)$ を

$$X = x + \sum_{T \in \Gamma - \{O\}} (x \circ \tau_T - x_T), \qquad Y = y + \sum_{T \in \Gamma - \{O\}} (y \circ \tau_T - y_T) \tag{3.5}$$

により定める (*cf.* (1.1), (1.3)). このとき, 明らかに $X, Y \in \bar{k}(E)^{\Gamma} \cap k(E)$. また, (3.1) を使うと X, Y が条件 (3.4) をみたすことも容易にわかる.

次に, 上の X, Y を x, y の有理式で表すために,

$$x_{-Q} = x_Q, \quad y_{-Q} = g_Q^y + y_Q, \quad g_{-Q}^x = g_Q^x - a_1 g_Q^y, \quad g_{-Q}^y = -g_Q^y$$

や

$$x \circ \tau_Q - x_Q = \frac{g_Q^x}{x - x_Q} + \frac{g_Q^y (y - y_Q)}{(x - x_Q)^2},$$

$$y \circ \tau_Q - y_{-Q} = -\frac{a_1 g_Q^x}{x - x_Q} - \frac{(g_Q^x + a_1 g_Q^y)(y - y_Q)}{(x - x_Q)^2} - \frac{g_Q^y (y - y_Q)^2}{(x - x_Q)^3}$$

等を使って (3.5) を変形すると, (2.5) なる表示が得られる. なお, $t, w \in k$ であることは

$$t = \sum_{T \in \Gamma - \{O\}} g_T^x, \qquad w = \sum_{T \in S} (g_T^y)^2 + \sum_{T \in \Gamma - \{O\}} x_T g_T^x$$

から直ちに従う.

最後に, X の $Z = -X/Y$ による O の近傍での Laurent 展開を計算するために, (2.5) に (3.2) を代入すると

$$\begin{aligned} X &= z^{-2} - \alpha_1 z^{-1} - \alpha_2 - \alpha_3 z \\ &\quad -(\alpha_4 - t) z^2 - (\alpha_5 - \alpha_1 t) z^3 - (\alpha_6 - \alpha_1^2 - \alpha_2 t - w) z^4 - \cdots, \\ Y &= -z^{-3} + \alpha_1 z^{-2} + \alpha_2 z^{-1} + \alpha_3 + (\alpha_4 + t) z + \alpha_5 z^2 + (\alpha_6 + \alpha_2 t + 2w) z^3 + \cdots \end{aligned}$$

が得られる. これより

$$Z = -\frac{X}{Y} = z + 2tz^5 + 3\alpha_1 t z^6 + (4\alpha_1^2 t + 4\alpha_2 t + 3w) z^7 + \cdots \tag{3.6}$$

となり, これを逆に解いて,

$$z = Z - 2tZ^5 - 3\alpha_1 t Z^6 - (4\alpha_1^2 t + 4\alpha_2 t + 3w) Z^7 + \cdots.$$

以上より

$$\begin{aligned} X &= Z^{-2} - \alpha_1 Z^{-1} - \alpha_2 - \alpha_3 Z \\ &\quad -(\alpha_4 - 5t) Z^2 - (\alpha_5 - 5\alpha_1 t) Z^3 - (\alpha_6 - 6\alpha_1^2 t - 9\alpha_2 t - 7w) Z^4 - \cdots \end{aligned}$$

となることがわかり, (3.3) に注意して

$$\alpha_1 = A_1, \quad \alpha_2 = A_2, \quad \alpha_3 = A_3, \quad \alpha_4 - 5t = A_1 A_3 + A_4,$$

$$\alpha_6 - 6\alpha_1^2 t - 9\alpha_2 t - 7w = A_1^2 A_4 + A_1^3 A_3 + A_2 A_4 + 2A_1 A_2 A_3 + A_3^2 + A_6$$

を解くと (2.3) を得る. □

注意 3.1 (3.5) は

$$X+\sum_{T\in\Gamma-\{O\}}x_T=\sum_{T\in\Gamma}x\circ\tau_T,\qquad Y+\sum_{T\in\Gamma-\{O\}}y_T=\sum_{T\in\Gamma}y\circ\tau_T$$

とも書ける. これより, $P\in E^*(\bar{k})-\{O\}$ に対して

$$X_P+\sum_{T\in\Gamma-\{O\}}x_T=\sum_{Q\in\lambda^{-1}(P)}x_Q,\qquad Y_P+\sum_{T\in\Gamma-\{O\}}y_T=\sum_{Q\in\lambda^{-1}(P)}y_Q$$

が成り立つことがわかる. ここで X_P, Y_P はそれぞれ $X(P), Y(P)$ の略記である.

注意 3.2 (3.2) と (3.3) を用いると, 方程式 (2.1) に付随する E 上の不変微分

$$\omega(x,y)=\frac{dx}{-g^y}=\frac{dy}{g^x}$$

は z によって

$$\omega(x,y)=(1+a_1z+\cdots)dz$$

なる形に表されることがわかる. 同様に, $G^X, G^Y\in k(E^*)$ をそれぞれ

$$G^X=3X^2+2A_2X+A_4-A_1Y,\qquad G^Y=-2Y-A_1X-A_3 \tag{3.7}$$

によって定めると, 方程式 (2.4) に付随する E^* 上の不変微分

$$\omega(X,Y)=\frac{dX}{-G^Y}=\frac{dY}{G^X}$$

は Z によって

$$\omega(X,Y)=(1+A_1Z+\cdots)dZ$$

なる形に表される. ここで, $\omega(X,Y)$ は E 上の正則微分ともみなせて, (2.3) と (3.6) より

$$\omega(X,Y)=(1+a_1z+\cdots)dz$$

なる形に表せることに注意すると,

$$\omega(X,Y)=\omega(x,y)$$

が成り立つことがわかる (*cf.* (1.4)).

4　いくつかの注意

以下, 楕円曲線 $E^* = E/\Gamma$ 上の点 $P \neq O$ に対して $X(P), Y(P), G^X(P), G^Y(P)$ をそれぞれ X_P, Y_P, G^X_P, G^Y_P と略記する.

4.1　G^X, G^Y と g^x, g^y との関係

(3.7) で定めた $G^X, G^Y \in k(E^*)$ は (2.2) で定めた $g^x, g^y \in k(E)$ を用いて

$$G^X = m\, g^x + n(g^y)^2, \qquad G^Y = m\, g^y$$

なる形に表される. ここで,

$$m = 1 - \sum_{T\in S}\left(\frac{t_T}{(x-x_T)^2} + \frac{2u_T}{(x-x_T)^3}\right), \quad n = \sum_{T\in S}\left(\frac{t_T}{(x-x_T)^3} + \frac{3u_T}{(x-x_T)^4}\right) \in k(E).$$

これらの等式は, 注意 3.2 で述べた

$$\frac{dx}{-g^y} = \frac{dy}{g^x} = \frac{dX}{-G^Y} = \frac{dY}{G^X}$$

と

$$dX = m\, dx, \qquad dY = -ng^y\, dx + m\, dy$$

から容易に導かれる.

4.2　X と x との関係

同種写像 λ の次数 $\sharp\Gamma$ を l と置くとき, (2.5) の初めの式は k-係数の多項式

$$I(x) = x^l - \Big(\sum_{T\in\Gamma-\{O\}} x_T\Big)x^{l-1} + \cdots,$$

$$J(x) = \prod_{T\in\Gamma-\{O\}}(x-x_T) = x^{l-1} - \Big(\sum_{T\in\Gamma-\{O\}} x_T\Big)x^{l-2} + \cdots$$

を用いて

$$X = \frac{I(x)}{J(x)}$$

なる形に書き直せる. $[k(x):k(X)]$ は $[k(E):k(E^*)] = l$ に一致するから, $I(x)$ と $J(x)$ は共通因子をもたない.

いま, P を $[2]P \neq O$ なる $E^*(\bar{k})$ 内の点とする. このとき, 任意の $Q \in \lambda^{-1}(P)$ に対して

$$Q \neq O, \qquad J(x_Q) \neq 0, \qquad I(x_Q) - X_P J(x_Q) = 0$$

が成り立つ. ここで, $[2]P \neq O$ なる仮定より

$$\sharp\{x_Q\ ;\ Q \in \lambda^{-1}(P)\} = \sharp\lambda^{-1}(P) = l$$

となることがわかるから,

$$I(x) - X_P J(x) = \prod_{Q \in \lambda^{-1}(P)} (x - x_Q)$$

を得る.

4.3 λ から生じる体の拡大

P を $[2]P \neq O$ なる $E^*(\bar{k})$ 内の点とし, 体

$$k(P) = k(X_P, Y_P), \qquad k\big(\lambda^{-1}(P)\big) = k\big(x_Q,\, y_Q\ ;\ Q \in \lambda^{-1}(P)\big)$$

をそれぞれ K, K' と置く. 同種写像 λ は k 上定義されているから, K は K' の部分体となる. 以下, 体 k の標数が 2 でないと仮定して, 拡大 K'/K に関する注意を述べる.

まず, 標数が 2 でないことより,

$$K = k(X_P, G_P^Y), \qquad K' = k\big(x_Q,\, g_Q^y\ ;\ Q \in \lambda^{-1}(P)\big).$$

また, §4.1 で述べたことより, 任意の $Q \in \lambda^{-1}(P)$ に対して

$$G_P^Y = m_Q g_Q^y$$

が成り立つ. ただし, m_Q は $m(Q)$ の略記である ($m \in k(E)$ は任意の $Q \in \lambda^{-1}(P)$ で正則であることに注意). 従って, $[2]P \neq O$ ($i.e.$, $G_P^Y \neq 0$) なる仮定より

$$m_Q \neq 0, \qquad g_Q^y = m_Q^{-1} G_P^Y \in k(x_Q, G_P^Y)$$

となり, 次を得る:

$$K' = K\big(x_Q\ ;\ Q \in \lambda^{-1}(P)\big).$$

よって, §4.2 で述べたことより, K' は多項式 $I(x) - X_P J(x)$ の K 上の最小分解体になる.

5　還元写像との関係

本節では, 体 k の離散的な加法付値 v をひとつ固定し, その付値環, 付値イデアル, 剰余体をそれぞれ $\mathcal{O}_v$, $\mathfrak{p}_v$, κ_v で表す. また, l を素数とし, E を k 上の楕円曲線で位数 l の k-有理点 T_0 をもつようなものとする. このとき, E の方程式

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{5.1}$$

で

$$a_1,\ a_2,\ a_3,\ a_4,\ a_6,\ x_{T_0},\ y_{T_0} \in \mathcal{O}_v$$

なるものがとれる. このような方程式をひとつ固定し, それに関する E の $\mathfrak{p}_v$ を法とする還元を

$$E(k) \longrightarrow (E \bmod \mathfrak{p}_v)(\kappa_v), \qquad Q \longmapsto Q \bmod \mathfrak{p}_v \tag{5.2}$$

とする. この還元写像を用いて, $E(k)$ の部分集合 $\mathcal{E}_0(k;\mathfrak{p}_v)$, $\mathcal{E}_1(k;\mathfrak{p}_v)$ をそれぞれ

$$\begin{aligned}
\mathcal{E}_0(k;\mathfrak{p}_v) &= \{Q \in E(k)\ ;\ Q \bmod \mathfrak{p}_v \in (E \bmod \mathfrak{p}_v)_{\mathrm{ns}}(\kappa_v)\}\,,\\
\mathcal{E}_1(k;\mathfrak{p}_v) &= \{Q \in E(k)\ ;\ Q \bmod \mathfrak{p}_v = O \bmod \mathfrak{p}_v\}
\end{aligned}$$

により定める. このとき, 明らかに $\{O\} \subset \mathcal{E}_1(k;\mathfrak{p}_v) \subset \mathcal{E}_0(k;\mathfrak{p}_v)$. また, 次も容易にわかる:

補題 5.1 (i) $Q \in E(k) - \{O\}$ に対し,

$$Q \in \mathcal{E}_1(k;\mathfrak{p}_v) \iff x_Q \notin \mathcal{O}_v \iff y_Q \notin \mathcal{O}_v.$$

(ii) $Q \in E(k) - \mathcal{E}_1(k;\mathfrak{p}_v)$ に対し,

$$Q \notin \mathcal{E}_0(k;\mathfrak{p}_v) \iff g_Q^x \equiv g_Q^y \equiv 0 \pmod{\mathfrak{p}_v}.$$

注意 5.2 点 $Q \in E(k)$ が $\mathcal{E}_0(k;\mathfrak{p}_v)$ に入るか否かは, その x-座標 x_Q の $\mathfrak{p}_v$ を法とする合同条件だけで定まる. より正確には, 方程式 (5.1) の判別式を Δ とするとき:

(i) $\Delta \not\equiv 0 \pmod{\mathfrak{p}_v}$ ならば, $\mathcal{E}_0(k;\mathfrak{p}_v) = E(k)$.

(ii) $\Delta \equiv 0 \pmod{\mathfrak{p}_v}$ ならば, $Q \in E(k)$ が $\mathcal{E}_0(k;\mathfrak{p}_v)$ に属さないためには, $x_Q \in \mathcal{O}_v$ かつ

$$\begin{cases}
f(x_Q) \equiv f'(x_Q) \equiv 0 \pmod{\mathfrak{p}_v} & \text{if } 2 \not\equiv 0 \pmod{\mathfrak{p}_v}\\
x_Q^2 \equiv a_4 \pmod{\mathfrak{p}_v} & \text{if } 2 \equiv a_1 \equiv 0 \pmod{\mathfrak{p}_v}\\
x_Q \equiv a_3/a_1 \pmod{\mathfrak{p}_v} & \text{if } 2 \equiv 0,\ a_1 \not\equiv 0 \pmod{\mathfrak{p}_v}
\end{cases}$$

が成り立つことが必要かつ十分. ここで,

$$f(x) = 4x^3 + (a_1^2 + 4a_2)x^2 + 2(a_1a_3 + 2a_4)x + a_3^2 + 4a_6.$$

方程式 (5.1) は極小とは限らないから, $\mathcal{E}_0(k;\mathfrak{p}_v)$ や $\mathcal{E}_1(k;\mathfrak{p}_v)$ は E, k や v から一意的に定まっているわけではない. しかしながら, 次が成り立つことが確かめられる:

補題 5.3 集合 $\mathcal{E}_0(k;\mathfrak{p}_v)$ は $E(k)$ の部分群で, 還元写像 (5.2) を $\mathcal{E}_0(k;\mathfrak{p}_v)$ に制限したものは準同型. また, その核は $\mathcal{E}_1(k;\mathfrak{p}_v)$ に一致する.

点 T_0 が生成する $E(k)$ の部分群を Γ と置く. Γ の位数 l は素数であるから, その部分群である $\Gamma \cap \mathcal{E}_0(k;\mathfrak{p}_v)$ や $\Gamma \cap \mathcal{E}_1(k;\mathfrak{p}_v)$ は $\{O\}$ または Γ に一致する. ところが $x_{T_0}, y_{T_0} \in \mathcal{O}_v$ より $T_0 \notin \mathcal{E}_1(k;\mathfrak{p}_v)$ であるから, $\Gamma \cap \mathcal{E}_1(k;\mathfrak{p}_v)$ は $\{O\}$ でなければならない. 従って, 全ての $T \in \Gamma - \{O\}$ に対して

$$x_T,\ y_T,\ g_T^x,\ g_T^y,\ t_T,\ u_T \in \mathcal{O}_v$$

が成り立つ.

いま, k 上の楕円曲線 $E^* = E/\Gamma$ の方程式

$$Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6 \tag{5.3}$$

と k 上の同種写像 $\lambda : E \to E^*$ を Vélu の公式により定める. このとき $a_i \in \mathcal{O}_v$ と上で述べたことより

$$A_1,\ A_2,\ A_3,\ A_4,\ A_6 \in \mathcal{O}_v$$

となることがわかる. 方程式 (5.3) に関する E^* の $\mathfrak{p}_v$ を法とする還元を

$$E^*(k) \longrightarrow (E^* \bmod \mathfrak{p}_v)(\kappa_v), \qquad P \longmapsto P \bmod \mathfrak{p}_v$$

とし, $E^*(k)$ の部分集合 $\mathcal{E}_0^*(k;\mathfrak{p}_v)$, $\mathcal{E}_1^*(k;\mathfrak{p}_v)$ を上と同様に定める. このとき, E^* に対しても, 補題 5.1, 注意 5.2 ならびに補題 5.3 と同様のことが言える.

以上の記号と仮定の下で, 次が成り立つ:

命題 5.4 P を $\lambda^{-1}(P) \subset E(k)$ なる $\mathcal{E}_0^*(k;\mathfrak{p}_v)$ 内の点とするとき, $\lambda^{-1}(P)$ 内の少なくともひとつの点は $\mathcal{E}_0(k;\mathfrak{p}_v)$ に含まれる:

$$\lambda^{-1}(P) \cap \mathcal{E}_0(k;\mathfrak{p}_v) \neq \emptyset.$$

[証明] $P=O$ のときは明らかなので, 以下 $P\neq O$ とする. 先に述べたように $\Gamma\cap\mathcal{E}_0(k;\mathfrak{p}_v)$ は $\{O\}$ または Γ に一致するので, それぞれの場合に分けて考える.

(i) $\Gamma\cap\mathcal{E}_0(k;\mathfrak{p}_v)=\Gamma$ の場合. このときには, より強く $\lambda^{-1}(P)\subset\mathcal{E}_0(k;\mathfrak{p}_v)$ が成り立つ. 実際, 仮に $Q\in\lambda^{-1}(P)-\mathcal{E}_0(k;\mathfrak{p}_v)$ が存在したとすると,

$$x_Q, y_Q\in\mathcal{O}_v,\quad g_Q^x\equiv g_Q^y\equiv 0\ (\mathrm{mod}\ \mathfrak{p}_v).$$

また, $\Gamma\subset\mathcal{E}_0(k;\mathfrak{p}_v)$ より,

$$x_Q\not\equiv x_T\ (\mathrm{mod}\ \mathfrak{p}_v)\quad \text{if } T\in\Gamma-\{O\}.$$

従って (2.5) より $X_P, Y_P\in\mathcal{O}_v$ となるが, §4.1 で述べたことより

$$G_P^X\equiv G_P^Y\equiv 0\ (\mathrm{mod}\ \mathfrak{p}_v)$$

となることもわかるから, $P\notin\mathcal{E}_0^*(k;\mathfrak{p}_v)$. これは矛盾.

(ii) $\Gamma\cap\mathcal{E}_0(k;\mathfrak{p}_v)=\{O\}$ の場合. このときには全ての $T\in\Gamma-\{O\}$ に対して

$$g_T^x\equiv g_T^y\equiv t_T\equiv u_T\equiv 0\ (\mathrm{mod}\ \mathfrak{p}_v)$$

となるから, $t\equiv w\equiv 0\ (\mathrm{mod}\ \mathfrak{p}_v)$. 従って,

$$A_1=a_1,\quad A_2=a_2,\quad A_3=a_3,\quad A_4\equiv a_4\ (\mathrm{mod}\ \mathfrak{p}_v),\quad A_6\equiv a_6\ (\mathrm{mod}\ \mathfrak{p}_v).$$

いま, 仮に $\lambda^{-1}(P)\cap\mathcal{E}_0(k;\mathfrak{p}_v)=\emptyset$ とすると, 全ての $Q\in\lambda^{-1}(P)$ と $T\in\Gamma-\{O\}$ は $\mathfrak{p}_v$ を法として $E\bmod\mathfrak{p}_v$ の (高々 1 個しか存在しない) 特異点に還元されることになるから,

$$x_Q, y_Q\in\mathcal{O}_v,\quad x_Q\equiv x_T\ (\mathrm{mod}\ \mathfrak{p}_v),\quad y_Q\equiv y_T\ (\mathrm{mod}\ \mathfrak{p}_v)$$

が成り立たなければならない. 従って, 注意 3.1 で述べた

$$X_P+\sum_{T\in\Gamma-\{O\}}x_T=\sum_{Q\in\lambda^{-1}(P)}x_Q,\qquad Y_P+\sum_{T\in\Gamma-\{O\}}y_T=\sum_{Q\in\lambda^{-1}(P)}y_Q$$

より, $X_P, Y_P\in\mathcal{O}_v$ ならびに

$$X_P\equiv x_Q\ (\mathrm{mod}\ \mathfrak{p}_v),\qquad Y_P\equiv y_Q\ (\mathrm{mod}\ \mathfrak{p}_v)$$

が任意の $Q\in\lambda^{-1}(P)$ に対して成り立つことがわかる. よって $P\notin\mathcal{E}_0^*(k;\mathfrak{p}_v)$ となるが, これは矛盾. □

注意 5.5 上の証明より, $\Delta\equiv 0\ (\mathrm{mod}\ \mathfrak{p}_v)$ ならば $\Delta^*\equiv 0\ (\mathrm{mod}\ \mathfrak{p}_v)$ となることがわかる.

6　代数体の不分岐巡回拡大の構成

以下, k は有限次代数体であるものとし, その整数環を $\mathfrak{O}_k$ で表す. また, l を素数とし, E を k 上の楕円曲線で位数 l の k-有理点 T_0 をもつようなものとする. このとき, E の方程式

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{6.1}$$

で

$$a_1,\ a_2,\ a_3,\ a_4,\ a_6,\ x_{T_0},\ y_{T_0} \in \mathfrak{O}_k$$

なるものがとれる. このような方程式をひとつ固定しておく. 点 T_0 が生成する $E(k)$ の部分群を Γ と置くと, 全ての $T \in \Gamma - \{O\}$ に対して $x_T, y_T \in \mathfrak{O}_k$ が成り立つ. 従って, k 上の楕円曲線 $E^* = E/\Gamma$ の方程式

$$Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6 \tag{6.2}$$

と k 上の同種写像 $\lambda : E \to E^*$ を Vélu の公式により定めるとき,

$$A_1,\ A_2,\ A_3,\ A_4,\ A_6 \in \mathfrak{O}_k$$

となる. また, §4.2 で定めた多項式 $I(x), J(x)$ の係数は全て $\mathfrak{O}_k$ に属する.

いま, $\mathfrak{O}_k$-係数の 3 次式 $F(X)$ を

$$F(X) = 4X^3 + (A_1^2 + 4A_2)X^2 + 2(A_1A_3 + 2A_4)X + A_3^2 + 4A_6$$

によって定め, $\xi \in k$ に対して $K_\xi = k\big(\sqrt{F(\xi)}\big)$ と置く. E^* の方程式 (6.2) は左辺を平方完成して

$$(G^Y)^2 = F(X)$$

と変形できるから, $X_P = \xi \in k$ なる $P \in E^*(\bar{k}) - \{O\}$ に対して K_ξ は $k(P)$ に一致する. また, 各 $\xi \in k$ に対し, k-係数の l 次式 $\Lambda_\xi(x)$ を

$$\Lambda_\xi(x) = I(x) - \xi J(x)$$

により定める. さらに, 方程式 (6.1), (6.2) の判別式をそれぞれ Δ, Δ^* とし, k における Δ の素因子 (注意 5.5 より, Δ^* の素因子でもある) $\mathfrak{p}$ に対し, 条件

$$\begin{cases} F(\xi) \equiv F'(\xi) \equiv 0 \pmod{\mathfrak{p}} & \text{if } 2 \not\equiv 0 \pmod{\mathfrak{p}} \\ \xi^2 \equiv A_4 \pmod{\mathfrak{p}} & \text{if } 2 \equiv A_1 \equiv 0 \pmod{\mathfrak{p}} \\ \xi \equiv A_3/A_1 \pmod{\mathfrak{p}} & \text{if } 2 \equiv 0,\ A_1 \not\equiv 0 \pmod{\mathfrak{p}} \end{cases}$$

をみたす $\xi \in \mathcal{O}_{k,\mathfrak{p}}$ のなす集合を $\mathcal{X}_{\mathrm{bad}}(k;\mathfrak{p})$ とする. ここで, $\mathcal{O}_{k,\mathfrak{p}}$ は $\mathfrak{p}$ における $\mathcal{O}_k$ の局所化を表す.

以上の記号と仮定の下で, 次が成り立つ:

定理 6.1 Ξ を次の 3 つの条件をみたす $\xi \in k$ のなす集合とする:

(C0) $F(\xi) \neq 0$.

(C1) $\Lambda_\xi(x)$ は k 上既約.

(C2) k における Δ の全ての素因子 $\mathfrak{p}$ に対して $\xi \notin \mathcal{X}_{\mathrm{bad}}(k;\mathfrak{p})$.

このとき, $X_P \in \Xi$ なる任意の $P \in E^*(\bar{k}) - \{O\}$ に対し, $k\big(\lambda^{-1}(P)\big)/k(P)$ は全ての有限素点で不分岐な l 次巡回拡大.

この定理と類体論により, 直ちに次が得られる:

系 6.2 任意の $\xi \in \Xi$ に対し, 体 K_ξ の類数は l で割り切れる.

例 6.3 (例 2.2 の続き) 例 2.2 において $a, b, c \in \mathcal{O}_k$ とすると,

$$F(X) = 4X^3 + (a^2 + 4b)X^2 - 16cX - 4a^2c - 16bc.$$

例 6.4 (例 2.3 の続き) 例 2.3 において $a, b \in \mathcal{O}_k$ とすると,

$$F(X) = 4X^3 + a^2X^2 - 18abX - 4a^3b - 27b^2.$$

[Sa 1] で述べた結果は, この例において $a = 0$ としたものに当たる.

例 6.5 (例 2.4 の続き) 例 2.4 において $a, b \in \mathcal{O}_k$ とすると,

$$\begin{aligned} F(X) = 4X^3 + (a^2 + 6ab + b^2)X^2 + 2(10a^3b - 19a^2b^2 - 9ab^3)X \\ +4a^5b - 40a^4b^2 - 20a^3b^3 - 59a^2b^4 - 4ab^5. \end{aligned}$$

例 6.6 (例 2.5 の続き) 例 2.5 において $a, b \in \mathcal{O}_k$ とすると,

$$\begin{aligned} F(X) = 4X^3 &+ (a^4 + 2a^3b + 3a^2b^2 - 6ab^3 + b^4)X^2 \\ &+2ab(a-b)(10a^5 - 59a^4b + 81a^3b^2 - 61a^2b^3 + 10ab^4 + 10b^5)X \\ &+ab(a-b)\ (4a^9 - 72a^8b + 304a^7b^2 - 727a^6b^3 + 843a^5b^4 \\ &\qquad -528a^4b^5 + 280a^3b^6 - 148a^2b^7 + 36ab^8 + 4b^9). \end{aligned}$$

それでは, 定理 6.1 の証明を与える. そのアイデアは Weak Mordell-Weil Theorem の証明 (例えば [Sil] の Chapter VIII, §1 を見よ) や本田平氏の論説 [Ho] の §3 に基づく. 方針は [Sa 1] と同様だが, 以前は特殊な楕円曲線に対して直接的な計算をしていたところを命題 5.4 で置き換えたものになっている.

以下, $X_P = \xi \in \Xi$ なる $P \in E^*(\bar{k}) - \{O\}$ をひとつ固定し, $K = k(P)$ $(= K_\xi)$, $K' = k\big(\lambda^{-1}(P)\big)$ と置く. このとき:

補題 6.7 (i) K'/K は l 次巡回拡大.

(ii) 任意の $Q \in \lambda^{-1}(P)$ に対し, $K' = K(Q)$.

(iii) 写像

$$\iota : \mathrm{Gal}(K'/K) \longrightarrow \Gamma, \qquad \sigma \longmapsto Q^\sigma - Q$$

(Q は $\lambda^{-1}(P)$ 内の任意の点) は群の同型.

[証明] まず, $\Gamma \subset E(k) \subset E(K)$ と $P \in E^*(K)$ より, K'/K が Galois 拡大であること, 任意の $Q \in \lambda^{-1}(P)$ に対して $K' = K(Q)$ が成り立つこと, ならびに ι が ($Q \in \lambda^{-1}(P)$ の選び方に依らず) 群の単射準同型であることは明らか.

さて, 群 Γ の位数 l は素数であるから, $\mathrm{Im}\,\iota$ は $\{O\}$ または Γ に一致する. また, 仮定 (C0) と §4.3 の最後で述べたことより, K' は $\Lambda_\xi(x)$ の K 上の最小分解体である. 従って, 仮定 (C1) より $\mathrm{Im}\,\iota = \Gamma$ となり, 主張を得る. □

いま, 体 K の素イデアル $\mathfrak{P}$ を任意にとり, それが K'/K で不分岐であることを示す. 拡大次数 $[K' : K] = l$ は素数であるから, $\mathfrak{P}$ は K'/K で不分解であるとしてよい. K' における $\mathfrak{P}$ の (ただひとつの) 素因子を $\mathfrak{P}'$ とし, その剰余体を κ' とする. 方程式 (6.1) に関する E の $\mathfrak{P}'$ を法とする還元を

$$E(K') \longrightarrow (E \bmod \mathfrak{P}')(\kappa'), \qquad P \longmapsto P \bmod \mathfrak{P}'$$

とし, $E(K')$ の部分集合 $\mathcal{E}_0(K';\mathfrak{P}')$, $\mathcal{E}_1(K';\mathfrak{P}')$ を §5 と同様に定める. $\mathfrak{P}'$ は K'/K で不分解としているから, これらは $\mathrm{Gal}(K'/K)$-不変な $E(K')$ の部分群である. 従って, $I_{\mathfrak{P}'/\mathfrak{P}}$ を $\mathfrak{P}'/\mathfrak{P}$ の惰性群とするとき, 任意の $Q \in \mathcal{E}_0(K';\mathfrak{P}')$ と任意の $\sigma \in I_{\mathfrak{P}'/\mathfrak{P}}$ に対して

$$Q^\sigma - Q \in \mathcal{E}_1(K';\mathfrak{P}')$$

が成り立つ. 特に $Q \in \lambda^{-1}(P) \cap \mathcal{E}_0(K'; \mathfrak{P}')$ — 仮定 (C0), (C2) と命題 5.4 により, この集合は空ではない! — とすると,

$$Q^\sigma - Q \in \Gamma \cap \mathcal{E}_1(K'; \mathfrak{P}')$$

が全ての $\sigma \in I_{\mathfrak{P}'/\mathfrak{P}}$ に対して成り立つことがわかる. ここで, $\Gamma \cap \mathcal{E}_1(K'; \mathfrak{P}') = \{O\}$ であったから, 点 Q は $\sigma \in I_{\mathfrak{P}'/\mathfrak{P}}$ の作用で不変ということになる. よって, $K' = K(Q)$ より, 惰性群 $I_{\mathfrak{P}'/\mathfrak{P}}$ は単位元のみからなることがわかる. すなわち, $\mathfrak{P}$ は K'/K で不分岐となり, これで定理 6.1 が示せた.

注意 6.8 l が奇素数ならば, K'/K は全ての無限素点で不分岐でもある.

7 集合 Ξ の密度

本節では, §6 で定めた集合 Ξ が高さ函数に関して体 k の中で正の密度をもつことを示し, さらに $k = \mathbb{Q}$ の場合にはその密度を具体的に求める. 以下, $d-1$ 次元射影空間上の k-有理点 $P \in \mathbb{P}^{d-1}(k)$ に対し, その k に関する乗法的な高さを $H_k(P)$ で表す (高さの定義や基本的な性質については, 例えば [Hin-Sil] の Part B を見よ). このとき, Schanuel が [Sch] で示したように, 具体的に書ける正の定数 $C_{d,k}$ が存在して $B \to \infty$ のとき

$$\sharp\left\{P \in \mathbb{P}^{d-1}(k)\ ;\ H_k(P) \le B\right\} = C_{d,k}B^d + \begin{cases} O(B\log B) & \text{if } d=2,\ k=\mathbb{Q} \\ O\left(B^{d-1/[k:\mathbb{Q}]}\right) & \text{otherwise} \end{cases} \tag{7.1}$$

なる漸近公式が成り立つ. 以下では, $\mathbb{P}^1(k) = k \cup \{\infty\}$ とみなして, 実変数 $B > 0$ の函数

$$\sharp\{\xi \in \Xi\ ;\ H_k(\xi) \le B\}$$

の漸近的な挙動を求めることを考える.

さて, 集合 $\Xi \subset k$ は (C0)–(C2) なる 3 つの条件で定義されているが, 条件 (C0) をみたさない $\xi \in k$ は高々 3 個であるから, これについては無視してよい. また, 条件 (C1) をみたさない $\xi \in k$ の個数は次のように評価される:

補題 7.1 $B \to \infty$ のとき,

$$\sharp\{\xi \in k\ ;\ \Lambda_\xi(x) \text{ は } k \text{ 上可約},\ H_k(\xi) \le B\} \asymp B^{2/l}.$$

[証明] まず, $F(\xi)\neq 0$ なる $\xi\in k$ に対して次の条件は同値であることを示す:

(a) $\Lambda_\xi(x)$ は k 上可約.

(b) $\Lambda_\xi(x)$ は k 内に根をもつ.

(b)$'$ ξ は $J(\zeta)\neq 0$ なる $\zeta\in k$ によって $\xi=I(\zeta)/J(\zeta)$ と表される.

(b) から (a) が従うことは明らかで, (b) と (b)$'$ が同値であることは容易にわかるから, (a) から (b) が従うというのがここでの主張である. $l=2$ ならばこの主張は自明であるから, 以下しばらく $l\neq 2$ とする. さて, 補題 6.7 の証明と同様にして, $F(\xi)\neq 0$ なる $\xi\in k$ に対して次の条件は同値であることがわかる:

(A) $\Lambda_\xi(x)$ は K_ξ 上可約.

(B) $\Lambda_\xi(x)$ は K_ξ 上で 1 次式の積に分解される.

ここで, (a) から (A) が従うことは明らか. また, K_ξ/k は高々 2 次の拡大で, $\Lambda_\xi(x)$ の次数 l は奇数としているから, (B) が成り立てば (b) も成り立たなければならない. よって, ($l\neq 2$ ならば) $F(\xi)\neq 0$ なる $\xi\in k$ に対して上に挙げた 5 つの条件は全て同値であることが示せた.

条件 (a), (b)$'$ の同値性より, 次の漸近公式が得られる:

$$\sharp\{\xi\in k\ ;\ \Lambda_\xi(x)\text{ は }k\text{ 上可約},\ H_k(\xi)\le B\}\asymp\sharp\big\{\zeta\in k\ ;\ H_k\big(I(\zeta)/J(\zeta)\big)\le B\big\}.$$

ここで, $I(x)/J(x)$ は次数 l の有理式であるから, k 上

$$H_k\big(I(\,\cdot\,)/J(\,\cdot\,)\big)\asymp H_k(\,\cdot\,)^l$$

となることが高さの性質よりわかる. よって, 漸近公式 (7.1) より主張を得る. □

続いて条件 (C2) を吟味する. 集合 $\mathfrak{X}_{\rm bad}(k;\mathfrak{p})\subset\mathcal{O}_{k,\mathfrak{p}}$ は Δ の k における各素因子 $\mathfrak{p}$ に対して定義されていたが, 剰余体上の適当な有理点 $\xi_\mathfrak{p}\in\mathbb{P}^1(\mathcal{O}_k/\mathfrak{p})-\{\infty\}$ を用いて

$$\mathfrak{X}_{\rm bad}(k;\mathfrak{p})=\big\{\xi\in\mathbb{P}^1(k)\ ;\ \xi\bmod\mathfrak{p}=\xi_\mathfrak{p}\big\}$$

と表せる (特に空ではない) ことがその定義よりわかる. このように, 射影空間上の有理点で, 有限個の素イデアルに対して還元の先を指定されたものの高さに関する分布は次のようになる:

補題 7.2 $\mathfrak{p}_1,\dots,\mathfrak{p}_r$ を有限次代数体 k の相異なる素イデアルとするとき, 各 $(P_1,\dots,P_r)\in\mathbb{P}^{d-1}(\mathcal{O}_k/\mathfrak{p}_1)\times\cdots\times\mathbb{P}^{d-1}(\mathcal{O}_k/\mathfrak{p}_r)$ に対し, $B\to\infty$ のとき

$$\sharp\big\{P\in\mathbb{P}^{d-1}(k)\ ;\ P\bmod\mathfrak{p}_1=P_1,\dots,P\bmod\mathfrak{p}_r=P_r,\ H_k(P)\le B\big\}\asymp B^d.$$

k が有理数体 $\mathbb{Q}$ の場合には, より精密に

$$\sharp\left\{P \in \mathbb{P}^{d-1}(\mathbb{Q})\ ;\ P \bmod p_1 = P_1,\ \dots,\ P \bmod p_r = P_r,\ H_{\mathbb{Q}}(P) \le B\right\}$$
$$= \left(\prod_{i=1}^{r} \frac{p_i - 1}{p_i^d - 1}\right) \frac{2^{d-1}}{\zeta(d)}\, B^d + \begin{cases} O(B \log B) & \text{if } d = 2 \\ O(B^{d-1}) & \text{otherwise} \end{cases}.$$

ここで, p_i は $\mathfrak{p}_i$ を生成する素数で, $\zeta(\,\cdot\,)$ は Riemann のゼータ函数を表す.

[証明] 各 $\boldsymbol{P} = (P_1, \dots, P_r) \in \prod_i \mathbb{P}^{d-1}(\mathcal{O}_k/\mathfrak{p}_i)$ に対して

$$\mathbb{P}^{d-1}(k; \boldsymbol{P}) = \left\{P \in \mathbb{P}^{d-1}(k)\ ;\ P \bmod \mathfrak{p}_1 = P_1,\ \dots,\ P \bmod \mathfrak{p}_r = P_r\right\}$$

と置くと, $\mathbb{P}^{d-1}(k)$ の分割

$$\mathbb{P}^{d-1}(k) = \coprod_{\boldsymbol{P}} \mathbb{P}^{d-1}(k; \boldsymbol{P})$$

が得られる. いま, $\boldsymbol{P}^0 \in \prod_i \mathbb{P}^{d-1}(\mathcal{O}_k/\mathfrak{p}_i)$ を任意に固定する. このとき, Chinese Remainder Theorem を用いると, 各 $\boldsymbol{P} \in \prod_i \mathbb{P}^{d-1}(\mathcal{O}_k/\mathfrak{p}_i)$ に対し, $\mathbb{P}^{d-1}(k; \boldsymbol{P}) = f_{\boldsymbol{P}}\big(\mathbb{P}^{d-1}(k; \boldsymbol{P}^0)\big)$ となるような k 上定義された射影変換 $f_{\boldsymbol{P}}$ が存在することがわかる. このとき

$$\sharp\left\{P \in \mathbb{P}^{d-1}(k)\ ;\ H_k(P) \le B\right\} = \sum_{\boldsymbol{P}} \sharp\left\{P \in \mathbb{P}^{d-1}(k; \boldsymbol{P}^0)\ ;\ H_k\big(f_{\boldsymbol{P}}(P)\big) \le B\right\}$$

となるが, $\mathbb{P}^{d-1}(k)$ 上

$$H_k\big(f_{\boldsymbol{P}}(\,\cdot\,)\big) \asymp H_k(\,\cdot\,)$$

が成り立つから, 漸近公式 (7.1) より

$$\sharp\left\{P \in \mathbb{P}^{d-1}(k; \boldsymbol{P}^0)\ ;\ H_k(P) \le B\right\} \asymp B^d$$

を得る. $k = \mathbb{Q}$ の場合については [Sa 2] を見よ. □

以上をまとめて, 次を得る:

定理 7.3 $B \to \infty$ のとき,

$$\sharp\{\xi \in \Xi\ ;\ H_k(\xi) \le B\} \asymp B^2.$$

$k = \mathbb{Q}$ の場合には,

$$\sharp\{\xi \in \Xi\ ;\ H_{\mathbb{Q}}(\xi) \le B\} = \left(\prod_{i=1}^{r} \frac{p_i}{p_i + 1}\right) \frac{12}{\pi^2}\, B^2 + O(B \log B).$$

ここで, $p_1, \dots, p_r$ は Δ の相異なる素因数.

系 7.4 集合 Ξ は体 k の中で高さ函数 H_k に関して次の意味で正の密度をもつ:

$$\liminf_{B\to\infty} \frac{\sharp\{\xi\in\Xi\ ;\ H_k(\xi)\le B\}}{\sharp\{\xi\in k\ ;\ H_k(\xi)\le B\}} > 0.$$

$k=\mathbb{Q}$ の場合には, Ξ の k における密度は Δ の相異なる素因数 $p_1,\dots,p_r$ を用いて次のように表される:

$$\lim_{B\to\infty} \frac{\sharp\{\xi\in\Xi\ ;\ H_{\mathbb{Q}}(\xi)\le B\}}{\sharp\{\xi\in\mathbb{Q}\ ;\ H_{\mathbb{Q}}(\xi)\le B\}} = \prod_{i=1}^{r}\frac{p_i}{p_i+1}.$$

注意 7.5 K を k の拡大体とするとき,

$$\sharp\{\xi\in\Xi\ ;\ K_\xi=K,\ H_k(\xi)\le B\} \asymp (\log B)^r$$

となるような $r\in\mathbb{Z}_{\ge 0}$ が存在することが示せるから, Ξ を添字集合とする k の (高々 2 次の) 拡大体の族 $\{K_\xi\}_{\xi\in\Xi}$ は無限族であることがわかる.

系 6.2 と系 7.4 より, 体 $K_\xi=k\big(\sqrt{F(\xi)}\big)$ の類数が l で割り切れるような $\xi\in k$ の全体は k の中で高さ函数 H_k に関して次の意味で正の密度をもつことがわかる:

$$\liminf_{B\to\infty} \frac{\sharp\big\{\xi\in k\ ;\ l\mid h_{K_\xi},\ H_k(\xi)\le B\big\}}{\sharp\{\xi\in k\ ;\ H_k(\xi)\le B\}} > 0.$$

$k=\mathbb{Q}$ の場合には, 密度が具体的に下から評価できて,

$$\liminf_{B\to\infty} \frac{\sharp\big\{\xi\in\mathbb{Q}\ ;\ l\mid h_{K_\xi},\ H_{\mathbb{Q}}(\xi)\le B\big\}}{\sharp\{\xi\in\mathbb{Q}\ ;\ H_{\mathbb{Q}}(\xi)\le B\}} \ge \prod_{i=1}^{r}\frac{p_i}{p_i+1}$$

となる. つまり, 雑な言い方をすれば, 無作為に選ばれた $\xi\in\mathbb{Q}$ に対し, 体 K_ξ の類数は $\prod_i p_i/(p_i+1)$ 以上の "確率" で l で割り切れるということになる. 最後に, 係数の絶対値の大きさの割りには "確率" が高くなるような $F(X)$ の例を挙げておく.

例 7.6 (例 6.3 の続き) 例 2.2 と例 6.3 において $a=9,\ b=4,\ c=-1$ とすると,

$$F(X)=4X^3+97X^2+16X+388,\qquad \Delta=9473.$$

従って, $\xi\in\mathbb{Q}$ に対し, 体 $\mathbb{Q}\big(\sqrt{4\xi^3+97\xi^2+16\xi+388}\big)$ の類数は

$$\frac{9473}{9473+1}=0.9998\cdots$$

以上の "確率" で 2 で割り切れる.

例 7.7 (例 6.4 の続き) 例 2.3 と例 6.4 において $a = 4,\ b = 1$ とすると,

$$F(X) = 4X^3 + 16X^2 - 72X - 256, \qquad \Delta = 37.$$

従って, $\xi \in \mathbb{Q}$ に対し, 体 $\mathbb{Q}\big(\sqrt{4\xi^3 + 16\xi^2 - 72\xi - 256}\big)$ の類数は

$$\frac{37}{37+1} = 0.9736\cdots$$

以上の "確率" で 3 で割り切れる.

例 7.8 (例 6.5 の続き) 例 2.4 と例 6.5 において $a = 1,\ b = -1$ とすると,

$$F(X) = 4X^3 - 4X^2 - 40X - 79, \qquad \Delta = -11.$$

従って, $\xi \in \mathbb{Q}$ に対し, 体 $\mathbb{Q}\big(\sqrt{4\xi^3 - 4\xi^2 - 40\xi - 79}\big)$ の類数は

$$\frac{11}{11+1} = 0.9166\cdots$$

以上の "確率" で 5 で割り切れる.

例 7.9 (例 6.6 の続き) 例 2.5 と例 6.6 において $a = 1,\ b = 2$ とすると,

$$F(X) = 4X^3 - 15X^2 - 832X - 4184, \qquad \Delta = -2^7 \cdot 13.$$

従って, $\xi \in \mathbb{Q}$ に対し, 体 $\mathbb{Q}\big(\sqrt{4\xi^3 - 15\xi^2 - 832\xi - 4184}\big)$ の類数は

$$\frac{2}{2+1} \cdot \frac{13}{13+1} = 0.6190\cdots$$

以上の "確率" で 7 で割り切れる.

参考文献

[Hin-Sil] M. Hindry and J. H. Silverman, *Diophantine Geometry: An Introduction*, Graduate Texts in Math. **201**, Springer, New York, 2000.

[Ho] 本田 平, Abel 多様体と代数的整数論, 数学の歩み **8** (1961), 262–270.

[L-M] R. Lercier and F. Morain, Algorithms for computing isogenies between elliptic curves, in *Computational Perspectives on Number Theory* (D. A. Buell and J. T. Teitebaum eds.), AMS/IP Studies in Advanced Math. **7**, 1998, pp. 77–96.

[Sa 1] 佐藤 篤, Rational points on quadratic twists on an elliptic curve, 仙台数論小研究集会 1998 報告集, 1999, pp. 13–28.

[Sa 2] A. Sato, Counting rational points on projective space with certain congruent conditions, preprint.

[Sch] S. H. Schanuel, Heights in number fields, Bull. Soc. Math. France **107** (1979), 433–449.

[Sil] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math. **106**, Springer, New York, 1985.

[V] J. Vélu, Isogénies entre courbes elliptiques, C. R. Acad. Sc. Paris **273** (1971), 238–241.

980-8578 仙台市青葉区荒巻字青葉
東北大学大学院理学研究科数学専攻
E-mail: atsushi@math.tohoku.ac.jp