楕円曲線のsecond [2]-descent の計算について

永田 雄一

2003年1月31日

序文

本論文は主等質空間を用いた [2]-Selmer 群上の Second [2]-descent が計算可能な skew-symmetric で双線形な pairing の構成およびそれを用いた計算に関する総合報告である. まず, K を完全体とし, E/K を K 上定義された楕円曲線とするとき E/K はすべての係数が K の元となる x, y を変数とした Weierstrass 方程式

$$E/K : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (a_i \in K)$$

で与えられることが知られており, E/K 上の点は無限遠点 O を単位元として Abel 群の群構造をもつ. このとき, 楕円曲線 E/K の K-有理点からなる集合 $E(K)$, すなわち Weierstrass 方程式の K-有理解を求めることを考えたい. $E(K)$ もまた E/K の部分群になるが, 特に K が代数体のとき次がよく知られている.

定理 0.0.1 (Mordell-Weil). ([16, Ⅷ Thm. 6.7] を参照.) K が代数体であれば $E(K)$ は有限生成 Abel 群である.

これより $E_{\mathrm{tors}}(K)$ を $E(K)$ のねじれ部分群としたとき $E(K) \cong E_{\mathrm{tors}}(K) \oplus \mathbb{Z}^r$ の形になり, $E(K)$ の生成元もしくは $E_{\mathrm{tors}}(K)$ と階数 r を求めることを考えるが, ここでは後者を考えることにする. 一般に階数 r を求めることは E_{tors} を求めるよりはるかに難しく, 任意に大きな階数 r をもつ楕円曲線が存在することは予想されているが未解決問題である. なお, ある $m \geq 2$ に対して $E(K)/mE(K)$ と $E_{\mathrm{tors}}(K)$ の群構造が分かれば階数 r が求まるが, $E(K)/mE(K)$ の群構造を直接求めることもまた難しく, それを計算できそうな群に埋め込むことを考える. ここで次がよく知られている.

命題 0.0.2. ([16, X Thm. 4.2] を参照.) 次の列は群の完全列である.

$$0 \longrightarrow E(K)/mE(K) \longrightarrow S^{(m)}(E/K) \longrightarrow Ш(E/K)[m] \longrightarrow 0. \tag{0.0.3}$$

上の命題中の $S^{(m)}(E/K)$ は $[m]$-Selmer 群と呼ばれ, この群は有限群であることが知られており, この群の計算は主等質空間のいたる所局所的な有理点をもつか否かに帰着し, これには主に Hensel の補題が用いられる. また, $Ш(E/K)$ は Shafarevich-Tate 群と呼ばれ, m 倍して 0 になるその部分群 $Ш(E/K)[m]$ が自明な群になりかつ $[m]$-Selmer 群が求まれば求めたい $E(K)/mE(K)$ が求まる. しかし, 代数体上定義された一般の楕円曲線に対して $Ш(E/K)[m]$ が自明な群になるとは限らない. よって, 次に $E(K)/mE(K)$ を含み, $[m]$-Selmer 群より小さい群を求めていくことによって $E(K)/mE(K)$ を評価することを考えたい. ここで, $m = 2, 4$ とすれば次の可換図式

$$\begin{array}{ccccc} E(K) & \longrightarrow & E(K)/4E(K) & \longrightarrow & E(K)/2E(K) \\ & & \downarrow & \circlearrowright & \downarrow \\ & & S^{(4)}(E/K) & \xrightarrow{f_2} & S^{(2)}(E/K) \end{array}$$

が成り立ち, この可換図式から群の包含列

$$E(K)/2E(K) \subset \mathrm{Im}(f_2) \subset S^{(2)}(E/K)$$

を得る. 一般に, $[m]$-Selmer 群から始めて, 上の完全列 (0.0.3) において m^n とすることによってそれより小さくかつ $E(K)/mE(K)$ を含むもので $E(K)/mE(K)$ を評価することが考えられる. ここでもし, Shafarevich-Tate 群が有限群であれば n を十分大きくすることによってその小さい群が $E(K)/mE(K)$ に一致する. しかし, Shafarevich-Tate 群の有限性は未解決問題である. よって, このようなやり方で $E(K)/mE(K)$ を評価できることは保証されていないが $E(K)/2E(K) = \mathrm{Im}(f_2)$ となる楕円曲線は存在する. そこで, $\mathrm{Im}(f_2)$ を計算することを考える. そのため, J. W. S. Cassels が主等質空間を用いて次を満たす双線形な pairing を構成した.

主定理 0.0.4 (Cassels, [6]). $S^{(2)} = S^{(2)}(E/K)$ とする. このとき, 主等質空間を用いて構成した双線形な pairing $\langle \cdot, \cdot \rangle : S^{(2)} \times S^{(2)} \to \{\pm 1\}$ は以下の 2 つを満たす.

(a) $\alpha \in S^{(2)}$ に対し, $\alpha \in \mathrm{Im}(f_2)$ となるための必要十分条件は任意の $\beta \in S^{(2)}$ に対して $\langle \alpha, \beta \rangle = 1$ となることである.

(b) $\alpha \in S^{(2)}$ に対し, $\langle \alpha, \alpha \rangle = 1$ である.

ここで $S^{(2)}$, $\mathrm{Im}(f_2)$ ともに $\mathbb{F}_2$-線型空間とみなすことができ, pairing の値は ± 1 と乗法的に書くことに注意する. この定理を言い換えると, (a) の必要十分性から $\alpha, \beta \in S^{(2)}$ に対し $\langle \alpha, \beta \rangle = -1$ となれば $\alpha, \beta \notin \mathrm{Im}(f_2)$ であり, また, (b) から $S^{(2)}$ の相異なる 2 つの $\mathbb{F}_2$-基底の pairing の値が分かればすべての pairing の値が分かる. これを用いて $E(K)/2E(K)$ が求まるときがある. 例えば有理数体 $\mathbb{Q}$ 上定義された楕円曲線

$$E/\mathbb{Q} : y^2 = x(x - 343)(x + 59049)$$

の $E(\mathbb{Q})$ の階数が 0 であり, $\mathbb{Q}$-有理点が $O, (0, 0), (343, 0), (-59049, 0)$ であることが計算できる. なお, この pairing は有名な Cassels pairing

$$Ш \times Ш \to \mathbb{Q}/\mathbb{Z}$$

の [2]-Selmer 群への引き戻しであり, Selmer 群, Shafarevich-Tate 群を定義する際に用いられる Galois cohomology を用いて (a), (b) を満たす [2]-Selmer 群上の pairing が [3] で構成されているが実際の計算は困難であった. そこで, Selmer 群, Shafarevich-Tate 群がともに主等質空間で解釈できることを手掛かりに Cassels は [6] で主定理の pairing を再構成している. ここで, もっとも簡単な場合の pairing $\langle \cdot, \cdot \rangle$ の構成を紹介する. まず, $K = \mathbb{Q}$ とし, $\mathbb{Q}$ 上定義された楕円曲線として

$$y^2 = (x - e_1)(x - e_2)(x - e_3) \quad (e_i \in \mathbb{Q})$$

とする. このとき [2]-Selmer 群を以下のようにして与えることができる. 今, 集合 KS を

$$\mathrm{KS} = \left\{ \Lambda = (b_1, b_2, b_3) \in \prod_{i=1}^{3} \mathbb{Q}^* \ ; \ b_1 b_2 b_3 \in \mathbb{Q}^{*2} \right\}$$

とし, $\Lambda = (b_1, b_2, b_3) \in \mathrm{KS}$ に対する C_Λ を

$$C_\Lambda : \left\{ H_i := b_{i+1} Z_{i+1}^2 - b_{i+2} Z_{i+2}^2 + (e_{i+1} - e_{i+2}) T^2 = 0 \ ; \ i = 1, 2, 3 \right\}$$

与えられる $\mathbb{P}^3$ の 3 つ 2 次曲面の intersection とすると, この C_Λ は $E/\mathbb{Q}$ と $\overline{\mathbb{Q}}$ 上同型であり, 特に $E/\mathbb{Q}$ の主等質空間となる. さらに, 集合 FD を

$$\mathrm{FD} = \{ \Lambda \in \mathrm{KS} \ ; \ \text{各 } v \in M_\mathbb{Q} \text{ に対し, } C_\Lambda(\mathbb{Q}_v) = \emptyset \}$$

としたとき $S^{(2)} \cong \mathrm{FD}/\mathrm{KS}^2$ となる. よって, $S^{(2)}$ と同型なこの $\mathrm{FD}/\mathrm{KS}^2$ 上の pairing $\langle \cdot, \cdot \rangle$ を以下のようにして構成する. まず, $\alpha = \{\Lambda\} \in \mathrm{FD}/\mathrm{KS}^2$ に対する C_Λ において, 各 $i (i = 1, 2, 3)$ に対し Q_i を円錐曲線 $Y_i : \{H_i = 0\} \subset \mathbb{P}^2$ の $\mathbb{Q}$-有理点として取り, さらに添え字を mod 3 で与えたとき

$$L_i := a_{i+1} Z_{i+1} + a_{i+2} Z_{i+2} + aT \quad (a_{i+1}, a_{i+2}, a \in \mathbb{Q})$$

を $L_i = 0$ が Q_i における Y_i の接線となるように取る. また, FD の与え方から各 $v \in M_\mathbb{Q}$ に対して $L_i(Q_v) \neq 0$ となる C_Λ 上の $\mathbb{Q}_v$-有理点を取る. これより, $\alpha = \{\Lambda\}, \beta = \{(c_1, c_2, c_3)\} \in \mathrm{FD}/\mathrm{KS}^2$ に対する $\langle \alpha, \beta \rangle$ を

$$\langle \alpha, \beta \rangle = \prod_{v \in M_\mathbb{Q}} \prod_{i=1}^{3} (L_i(Q_v), c_i)_v$$

(但し, $(\cdot, \cdot)_v$ を Hilbert 記号とする) とする. 実際, これが主定理の性質 (a), (b) を満たすこととなる.

以上でこの修士論文の大まかな流れを述べたが, 最後に楕円曲線に関する基礎的事項, 特に主等質空間に関して書いたつもりである. それらに関しては [4],[16],[5] を参考にして書いた.

末筆になりましたが, この 3 年間, セミナー等で御指導して頂きました雪江明彦教授には本当に心から感謝します. また, 幾つか助言を頂きました佐藤篤助手, 森田康夫教授に感謝します. そして, 共に学び, 時に良き相談相手となってくれた友人たち, 数学に志そうと思うきっかけになった高校時代の高橋直文先生, 陰ながら支えてくれた母親と親戚の方々にも感謝します. 最後に, 3 年前に他界した父に冥福を祈ります.

平成 15 年 1 月 31 日

目次

1 準備

この修士論文でよく使う記号の定義と幾つかの事実を引用する. まず, よく用いる記号として次を定義する.

記号 1.0.5. R を環としたとき, R^* を R の可逆元全体からなる集合とすれば, R^* は環 R の積を演算として群をなす. 特に R が体であれば, $R^* = R \setminus \{0\}$ である. また, 正の整数 n に対し, 集合 $(R^*)^n$ を

$$(R^*)^n := \{a^n \in R^* \ ; \ a \in R^*\}$$

とすれば $(R^*)^n$ は R^* の部分群である.

次に K を完全体としたとき次を定義する.

定義 1.0.6. K を完全体とする. このとき, n 次元射影空間 $\mathbb{P}^n$ に対し

$$\mathbb{P}^n(K) = \{[X_0 : X_1 : \cdots : X_n] \in \mathbb{P}^n \ ; \ \text{各 } i \text{ に対し, } X_i \in K\}$$

とし, 点 $P \in \mathbb{P}^n(K)$ を K-有理点という (Affine 空間に対しても同様に定義する). また, 代数多様体 C が K 係数の幾つかの代数方程式の共通零点で与えられているならば, C は K 上定義されているといい, C/K と書く. さらに $C \subset \mathbb{P}^n$ ならば $C(K) = C \cap \mathbb{P}^n(K)$ とおく.

次に K が大域体のとき以下の記号を定義しておく.

記号 1.0.7 (大域体と局所体). K を代数体とするとき, 以下の記号を定義する.

- M_K : K の自明でない付値 v の同値類からなる集合,
- R : K の整数環,
- K_v : $v \in M_K$ で完備化した体,
- R_v : K_v の付値環,
- R_v^*(または U_{K_v}) : R_v の単数群,
- k_v : K_v の剰余体.
- $\mathrm{ord}_v(x)$: $x \in K_v$ における正規化付値

次に述べる Hasse-Minkovski の定理は Selmer 群上の pairing $\langle \cdot, \cdot \rangle$ の構成の際に用いる. また後で述べる Selmer 群, Shafarevich-Tate 群を与える動機付けともなる.

定理 1.0.8 (Hasse-Minkovski). ([1, 1 §1 Thm. 1] より引用.) K を代数体とし, f を係数がすべて K の元となる非退化 2 次形式とする. このとき, f が K で 0 を表現するための必要十分条件は各 $v \in M_K$ に対し f が K_v で 0 を表現することである.

注 1.0.9. 以下を注意として与える.

(1) 定理の特別な場合を代数幾何の言葉で言い換えれば次である. C/K を K 上定義された非特異 2 次曲線としたとき, C が K-有理点をもつための必要十分条件は各 $v \in M_K$ に対し C が K_v-有理点をもつことである.

(2) (1) と同様のことは非特異 3 次曲線において必ずしも成立しない. 一般に, 代数体 K に関するある命題が各 $v \in M_K$ に対して, K_v に関する命題として同時に成り立つことに帰着できるならば, その命題に関して Hasse の原理が成り立つという. 特に非特異 3 次曲線における K-有理点の存在性に関して Hasse の原理が成立しないものが存在する. 詳細は節 2.5 で述べる.

次に述べる Hensel の補題は主定理を用いた計算で用いる.

補題 1.0.10 (Hensel). ([16, X exer. 10.12] より引用.) R を離散付値 v で完備な環とする. このとき, $f(x_1, \dots, x_n) \in R[x_1, \dots, x_n]$ に対して次を満たす $(a_1, \dots, a_n) \in R^n$ が存在すれば, f は R^n で根をもつ.

$$v(f(a_1, \dots, a_n)) > 2v\left(\frac{\partial f}{\partial x_i}(a_1, \dots, a_n)\right) \quad (\text{ある } 1 \leq i \leq n). \tag{1.0.11}$$

次に述べる Hilbert 記号は Selmer 群上の paring $\langle \cdot, \cdot \rangle$ の構成に用いる.

定義 1.0.12 (Hilbert 記号). K を代数体とし, K_v を $v \in M_K$ での完備体とする. このとき, $\alpha, \beta \in K_v^*$ に対し $(\alpha, \beta)_{K_v}$ を以下で定義する. $(\cdot, \cdot)_{K_v}$ は Hilbert 記号と呼ばれる.

$$(\alpha, \beta)_{K_v} := \begin{cases} 1 & (\alpha x^2 + \beta y^2 - z^2 \text{が} \prod_{i=1}^3 K_v \text{で自明でない根をもつとき}) \\ -1 & (\text{それ以外のとき}). \end{cases}$$

以下ヒルベルト記号の性質を述べる. これらは主定理の証明および主定理を用いた計算で用いる.

命題 1.0.13 (Hilbert 記号の諸性質). (詳細は [1, 1 §6] または [18, 第 8 章 §8.2] を参照.) 以下の 4 つが成り立つ.

(a) $(\cdot, \cdot)_{K_v}$ は K_v^*/K_v^{*2} 上の双線形, 非退化, 対称的な 2 次形式である.

(b) $\alpha, \beta \in K$ に対し, 有限個を除いたすべての $v \in M_K$ で $[\alpha, \beta]_v = 1$ であり,

$$\prod_{v \in M_K} (\alpha, \beta)_{K_v} = 1 \tag{1.0.14}$$

が成り立つ. これを積公式という.

(c) L/K_v を有限次拡大とする. このとき, $\alpha \in L,\ \beta \in K_v$ に対し,

$$(\alpha, \beta)_L = \big(N_{L/K_v}(\alpha), \beta\big)_{K_v} \tag{1.0.15}$$

が成り立つ.

(d) $\alpha, \beta \in U_{K_v}$ に対し, $(\alpha, \beta)_{K_v} = 1$ である.

次で与える命題は Application おける Hilbert 記号の計算で用いる.

命題 1.0.16. ([14, Ⅲ Thm. 1] より引用.) $K = \mathbb{Q}$ のとき, 各 $v \in M_{\mathbb{Q}}$ に対する Hilbert 記号を簡略化のため $(\cdot, \cdot)_v$ とする. このとき, $v = \infty$ であれば $\alpha, \beta \in \mathbb{R}$ に対し

$$(\alpha, \beta)_\infty = \begin{cases} 1 & (\alpha > 0 \text{ または} \beta > 0 \text{ のとき}) \\ -1 & (\alpha, \beta < 0 \text{ のとき}) \end{cases}$$

であり, それ以外については $\alpha, \beta \in Q_v$ に対し $\alpha = p_v^a u_1, \beta = p_v^b u_2$(ある $u_1, u_2 \in \mathbb{Z}_v^*$) とすれば,

$$(\alpha, \beta)_v = \begin{cases} (-1)^{ab(p-1)/2} \left(\frac{u_1}{p_v}\right) \left(\frac{u_2}{p_v}\right) & (v \neq 2 \text{ のとき}) \\ (-1)^{\left\{2(u_1-1)(u_2-1) + a\left(u_2^2-1\right) + b\left(u_1^2-1\right)\right\}/8} & (v = 2 \text{ のとき}) \end{cases}$$

となる (但し, $(\frac{u}{p_v})$ は Legendre 記号である).

2 楕円曲線概論

この節では, 楕円曲線を定義してその諸性質について簡単に述べた後, Mordell-Weil の定理について解説し, Selmer 群と Shafarevich-Tate 群を用いた Mordell-Weil 群の計算について述べる.

2.1 定義と諸性質

以下 K を完全体, $\overline{K}$ をその代数的閉包とし, $G_{\overline{K}/K} = \mathrm{Gal}(\overline{K}/K)$ とする.

定義 2.1.1 (楕円曲線). 種数 1 の曲線 E とその曲線上の固定点 O との対 (E, O) を楕円曲線とする. また, $O \in \mathbb{P}^n(K)$ であり E が K 上定義されているならば, その楕円曲線は K 上定義されているといい, この意味で E/K と書く.

上で楕円曲線の定義を述べたが, 任意の楕円曲線 (E, O) に対して, E は Aff^2 におけるある非特異曲線

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.1.2}$$

$$(Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3) \tag{2.1.3}$$

(下の曲線は $x = X/Z,\ y = Y/Z$ で斉次化したもの) に同型で, しかもこの同型写象によりその固定点 O が無限遠点 ∞(斉次座標で表すと $[0:1:0]$) に写ることが Riemann-Roch の定理よりいえる (詳細は [16, Ⅲ Thm. 3.1] を参照). 逆に定義から明らかに (2.1.2) または (2.1.3) で与えられる非特異曲線は固定点 O を ∞ とすれば楕円曲線である. ちなみに (2.1.2) あるいは (2.1.3) を Weierstrass 方程式といい, これより楕円曲線の議論はすべて Weierstrass 方程式で行われてよい. ここで, 楕円曲線の例とそうでない例を述べる.

例 2.1.4. 次の (a)∼(d) は楕円曲線であるが, (e)∼(h) はそうではない. ちなみに, (e), (f) はともに $(0,0)$ を特異点として持ち, その特異点はそれぞれ node, cusp である (node, cusp については命題 2.1.6 の (b) で述べる).

(a) $E_1/\mathbb{Q} : y^2 + y = x^3 - x + 1$

(b) $E_2/\mathbb{Q} : y^2 = (x - 12)(x - 45/32)(x - 123/22)$

(c) $E_3/\mathbb{Q} : y^2 = x^4 + 1$

(d) $E_4/\mathbb{Q}_p : y^2 = x^3 + x$

(e) $C_1/\mathbb{Q} : y^2 = x^3 + x^2$

(f) $C_2/\mathbb{Q} : y^2 = x^3$

(g) $C_3/\mathbb{F}_{13} : y^2 + y = x^3 - x + 1$

(h) $C_4/\mathbb{Q} : y^4 = x^4 + 1$.

楕円曲線の諸性質を述べる前に, その際に用いられる Weierstrass 方程式について幾つか述べておく.

記号 2.1.5. Weierstrass 方程式 (2.1.2) に対し, 以下の記号を定義する.

$$
\begin{aligned}
&b_2 := a_1^2 + 4a_2,\ b_4 := 2a_4 + a_1a_3, \qquad b_6 := a_3^2 + 4a_6,\\
&b_8 := a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,\\
&c_4 := b_2^2 - 24b_4,\ c_6 := -b_2^3 - 24b_4, \qquad c_6 := -b_2^3 + 36b_2b_4 - 216b_6,\\
&\Delta := -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \qquad j := c_4^3/\Delta,\\
&\omega := dx/(2y + a_1x + a_3) = dy/(3x^2 + 2a_2x + a_4 - a_1y).
\end{aligned}
$$

命題 2.1.6 (Weierstrass 方程式の性質). (詳細は [16, Ⅲ] を参照.) Weierstrass 方程式において以下の 4 つが成り立つ.

(a) Weierstrass 方程式 (2.1.2) は $\mathrm{ch}\,(K) \neq 2, 3$ であれば, $y^2 = x^3 - 27c_4x - 54c_6$ に同型である.

(b) Weierstrass 方程式で与えられた曲線は, $\Delta \neq 0$ であれば非特異で楕円曲線となるが, $\Delta = 0$ であれば, 1 点のみを特異点としてもち, $c_4 \neq 0$ であれば特異点で異なる 2 本の接線をもち (このときの特異点を node という), $c_4 = 0$ であれば特異点で接線は 2 重に接している (このときの特異点を cusp という).

(c) Weierstrass 方程式から Weierstrass 方程式への, O を動かさない変換は次の形で与えられる.

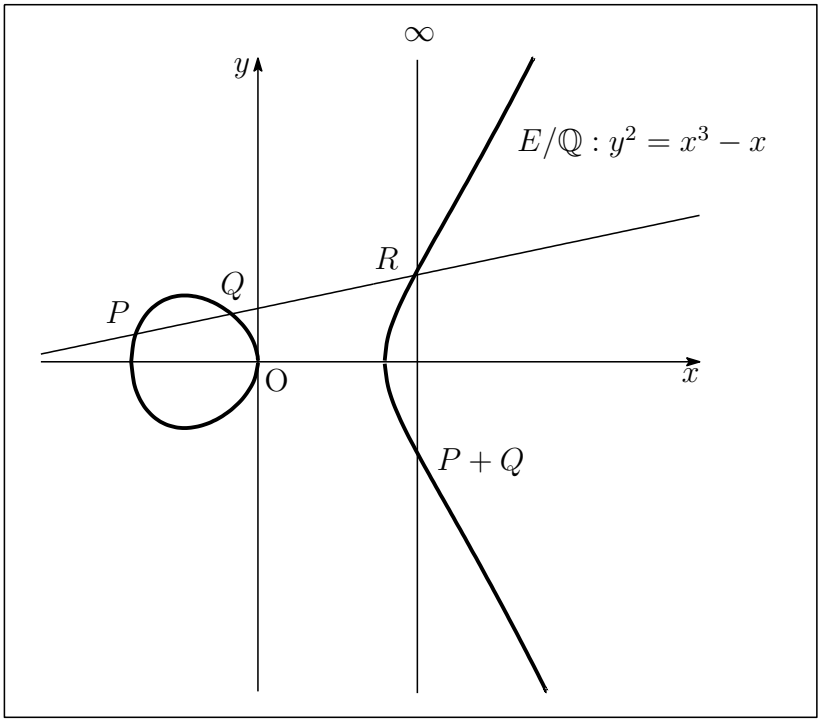
$$x = u^2x' + r, \quad y = u^3y' + u^2sx' + t \qquad (\text{ある } u, r, s, t \in \overline{K}). \tag{2.1.7}$$

(d) j, ω はそれぞれ, E の j-invariant, E の Weierstrass 方程式に付随する invariant differential といい, 変数変換 (2.1.7) に対して j は不変で, ω は定数倍を除いて不変である.

次に楕円曲線の諸性質について幾つか述べるが, もっともよく知られているものの 1 つに複素解析の言葉を用いれば, $\mathbb{C}$ 上の楕円曲線 E はある 1 次元複素トーラス $\mathbb{C}/\Lambda$ (Λ は $\mathrm{rank}_{\mathbb{Z}}\Lambda = 2$ となる $\mathbb{C}$ の離散部分群) に解析的同型であることがあげられ, トーラスの穴の数が種数に対応している. 実際, E は次の弦と接線の方法による演算で群をなし, その演算は任意の $\overline{K}$ で成り立つ.

命題 2.1.8 (弦と接線の方法と E の群構造). ([16, Ⅲ §2] を参照.) $P, Q \in E$ に対して, $P + Q$ を P と Q を通る直線 L と E との第 3 交点を R としたときの, 固定点 O と R を通る直線 L' と E との第 3 交点で与えれば, 固定点 O を単位元として Abel 群をなす (但し, $P = Q$, $R = O$ のときはそれぞれ L, L' をその点における E の接線として与え

る). なお, このとき $P+Q+R=O$ であり, 以上を $\mathbb{R}^2$ のグラフで表すと下の図のようになる.



これより $P \in E$ と整数 $m > 0$ に対して $[m]P$ を P の m 個の和とし, $[0]P = O$, $[-m]P = [m](-P)$ とする. また, E/K を K 上定義された楕円曲線とすれば, 次で与える命題から $P \in E(K)$ に対して, $[m]P \in E(K)$ となるため $E(K)$ もまた Abel 群である. 特に K が代数体であれば $E(K)$ は有限生成となる (Mordell-Weil の定理). これについては後で触れることにする.

命題 2.1.9 (加法公式). (詳細は [16, Ⅲ §2] を参照.) E を Weierstrass 方程式 (2.1.2) で与えれば, 以下の 3 つが成り立つ.

(a) $P_0 = (x_0, y_0) \in E$ に対して, $-P_0$ は

$$-P_0 = (x_0,\ -y_0 - a_1x_0 - a_3) \tag{2.1.10}$$

で与えられる.

(b) $P_1 = (x_1, y_1),\ P_2 = (x_2, y_2) \in E$ に対し, $P_3 = (x_3, y_3) := P_1 + P_2$ は $P_1 \neq -P_2$ であれば,

$$P_3 = (\lambda^2 + a_1\lambda - a_2 - x_1 - x_2,\ -(\lambda + a_1)x_3 - \nu - a_3) \tag{2.1.11}$$

で与えられる (但し, λ, ν はそれぞれ,

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & (x_1 \neq x_2 \text{ のとき}) \\ \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & (x_1 = x_2 \text{ のとき}) \end{cases}$$

$$\nu = \begin{cases} \dfrac{y_1x_2 - y_2x_1}{x_2 - x_1} & (x_1 \neq x_2 \text{ のとき}) \\ \dfrac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} & (x_1 = x_2 \text{ のとき}) \end{cases}$$

とする).

(c) (b) から, $P = (x, y) \in E$ の 2 倍 $[2]P$ の x 座標 $x([2]P)$ は

$$x([2]P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6} \tag{2.1.12}$$

で与えられ, これを 2 倍公式という.

ここで, E 上の関数を構成する際に用いる有名な Abel の定理を述べる. 代数幾何の言葉を用いるが, 後で因子類群を使うことも考えて K 上定義された曲線 C/K に対して幾つかの記号を定義する.

定義 2.1.13 (因子群と因子類群). C/K を K 上定義された代数曲線とする. このとき, C の関数体 $\overline{K}(C)$ に対し,

$$K(C) = \{f \in \overline{K}(C)\ ;\ f \text{ は } G_{\overline{K}/K} \text{ の作用で不変}\}$$

とする. また, 整数係数の C 上の点の形式和

$$D = \sum_{p \in C} n_p(P)$$

を C の divisor といい (但し, n_p は有限個の点を除いて 0 となる整数として取る), C の divisor からなる群を C の因子群といい $\mathrm{Div}(C)$ と書く. さらに, 2 つの divisor D_1, D_2 に対しある $f \in \overline{K}(C)^*$ が存在して $D_1 - D_2 = \mathrm{div}(f)$ となるならば (但し, $\mathrm{div}(f)$ は f の divisor であり, この divisor を principal divisor という), D_1 と D_2 は線形同値といい, $D_1 \sim D_2$ と書くことにする. すると明らかに関係 $\sim$ は同値関係であり, この関係よる $\mathrm{Div}(C)$ の商集合を C の因子類群といい $\mathrm{Pic}(C)$ と書く. 以上より, $D \in \mathrm{Div}(C)$ に対し

$$\deg\ D = \sum_{p \in C} n_p$$

を D の degree といい, $G_{\overline{K}/K}$ の $\mathrm{Div}(C)$ への作用を $\sigma \in G_{\overline{K}/K}$ と $D = \sum_{p \in C} n_p(p)$ に対し

$$D^\sigma = \sum_{p \in C} n_p(p^\sigma)$$

で定めたとき, 以下の 4 つの記号を定義する.

- $\mathrm{Div}^0(C) := \{D \in \mathrm{Div}(C)\ ;\ \deg\ D = 0\}$,
- $\mathrm{Pic}^0(C) := \{\{D\} \in \mathrm{Pic}(C)\ ;\ \deg\ D = 0\}$,
- $\mathrm{Div}^0_K(C) := \left\{D \in \mathrm{Div}^0(C)\ ;\ \text{各}\,\sigma \in G_{\overline{K}/K}\,\text{に対し},\, D^\sigma = D\right\}$,
- $\mathrm{Pic}^0_K(C) := \left\{\{D\} \in \mathrm{Pic}^0(C)\ ;\ \text{各}\,\sigma \in G_{\overline{K}/K}\,\text{に対し},\, D^\sigma = D\right\}$.

このとき, divisr $D \in \mathrm{Div}^0(C)$ が $D \in \mathrm{Div}^0_K(C)$ ならば D は K 上定義されているという ($\mathrm{Pic}^0(C)$ に対しても同様に定義する).

注 2.1.14 (K 上定義された divisor). K 上定義された divisor D は必ずしも K-有理点のみの形式和とは限らない. 例えば楕円曲線

$$E/\mathbb{Q} : y^2 = x^3 - 67 = \left(x - \sqrt[3]{67}\right)\left(x - \sqrt[3]{67}\zeta_3\right)\left(x - \sqrt[3]{67}\zeta_3^2\right)$$

に対し (但し, ζ_3 は 1 の原始 3 乗根とする), 次で与える divisor D_0, D_1, D_2, D_3 はそれぞれ $\mathbb{Q}, \mathbb{Q}\left(\sqrt[3]{67}\right), \mathbb{Q}\left(\sqrt[3]{67}\zeta_3\right), \mathbb{Q}\left(\sqrt[3]{67}\zeta_3^2\right)$ 上定義されている.

$$D_0 = 2\left(\left(\left(\sqrt[3]{67}, 0\right)\right) + \left(\left(\sqrt[3]{67}\zeta_3, 0\right)\right) + \left(\left(\sqrt[3]{67}\zeta_3^2, 0\right)\right) - 3(O)\right) \tag{2.1.15}$$

$$D_1 = 2\left(\left(\left(\sqrt[3]{67}, 0\right)\right) - (O)\right), \tag{2.1.16}$$

$$D_2 = 2\left(\left(\left(\sqrt[3]{67}\zeta_3, 0\right)\right) - (O)\right), \tag{2.1.17}$$

$$D_3 = 2\left(\left(\left(\sqrt[3]{67}\zeta_3^2, 0\right)\right) - (O)\right). \tag{2.1.18}$$

次に divisor に関して幾つか述べるが, それらは主定理の pairing $\langle \cdot, \cdot \rangle$ を構成する際に用いられる. なお, $\mathrm{Pic}^0(C)$ は下の命題の (a) から代表元による演算により群をなすことがいえ, 単位元は同値関係 $\sim$ の与え方からすべての principal divisor のみを含む同値類となる.

命題 2.1.19. K 上定義された代数曲線 C/K に対し, 以下の 3 つが成り立つ.

(a) $f \in \overline{K}(C)^*$ に対し $\deg(\mathrm{div}(f)) = 0$ であり, $\mathrm{div}(f) = 0$ となるための必要十分条件は $f \in \overline{K}^*$ となることである (詳細は [16, Ⅱ Prop. 3.1] または [9, Ⅱ Cor. 6.10] を参照).

(b) C の種数が 0 であれば C 上の任意の 2 点 P, Q に対して 2 つ divisor$(P), (Q)$ は線形同値であり逆も成立する (詳細は [9, Ⅱ Ex. 6.10, Ⅳ Ex. 1.3,5] を参照).

(c) (a) と定義から完全列

$$1 \longrightarrow \overline{K}^* \longrightarrow \overline{K}(C)^* \xrightarrow{\text{div}} \text{Div}^0(C) \longrightarrow \text{Pic}^0(C) \longrightarrow 1$$

を得る (div は $f \in \overline{K}(C)^*$ に対し, f の divisor $\text{div}(f)$ を対応させる写像). さらに次の列もまた完全列である ([16, Ⅱ Exer. 2.13] より引用).

$$1 \longrightarrow K^* \longrightarrow K(C)^* \xrightarrow{\text{div}} \text{Div}_K^0(C) \longrightarrow \text{Pic}_K^0(C) \tag{2.1.20}$$

これより Abel の定理について述べる.

定理 2.1.21 (Abel). ([16, Ⅲ Cor. 3.5] を参照.) E を楕円曲線とする. このとき, $D = \sum_{P \in E} n_p(P) \in \text{Div}(E)$ に対して, D が principal となるための必要十分条件は

$$\sum_{P \in E} n_p = 0 \text{ かつ } \sum_{P \in E} [n_p]P = O \tag{2.1.22}$$

を満たすことである (但し, 上の一番右側の和は E 上の演算である).

注 2.1.23. 上で与えた divisor(2.1.15)〜(2.1.16) は Abel の定理から principal divisor である.

この Abel の定理を用いて構成される Weil pairing について述べておく. これは, 代数体 K 上定義されたある場合の楕円曲線 E/K に対する $E(K)/mE(K)$ の計算に用いられる. ちなみにこの pairing は双線形, 交代的で, 非退化な $E[m]$ 上の pairing となる.

定義 2.1.24 (Weil pairing). $m \in \mathbb{Z}^*$ とする. 今, $T \in E[m]$ に対して, Abel の定理から,

$$\text{div}(f) = m(T) - m(O), \qquad \text{div}(g) = [m]^*(T) - [m]^*(O)$$

であって ($[m]^*$ は [m] 倍写像によって引き起こされる Divisor の引き戻し), $f \circ [m] = g^m$ を満たす $f, g \in \overline{K}(E)^*$ を取ることができ, これにより, 上の T と $S \in E[m]$ による pairing を

$$e_m(S, T) := \frac{g(X+S)}{g(X)} \quad (X \in E) \tag{2.1.25}$$

で与える. これを Weil pairing という.

上の定義において, f, g, S の取り方から, $X \in E$ の取り方に寄らないことと, $e_m \in \mu_m$(μ_m は K^* の単元の m 乗根からなる集合) がいえる. よって e_m は $E[m] \times E[m]$ から μ_m への pairing となり, 次の命題で述べる性質をもつ.

命題 2.1.26 (Weil pairing の性質). ([16, Ⅲ §8] を参照.) E/K を K 上定義された楕円曲線とするとき, 次の 2 つが成り立つ.

(a) Weil pairing は双線形, 交代的, 非退化, Galois 不変な pairing である.

(b) 非退化性と後で述べる注 2.1.39 から, $e_m(S,T)$ が原始 m 乗根となる $S,T \in E[m]$ が存在し, 特に $E[m] \subset E(K)$ ならば, $\mu_m \subset K^*$ となる.

次に楕円曲線間のある写像 (isogeny) とその諸性質について述べた後, dual isogeny について述べる. この dual isogeny もまた $E(K)/mE(K)$ の計算に利用されるが, Weil pairing を使った方法では計算できない楕円曲線 E/K に対する $E(K)/mE(K)$ が計算可能となる. しかし, この方法でも一般の代数体上定義された楕円曲線に対して計算できるわけではない. ちなみに isogeny は $\mathbb{C}$ 上においては, 複素トーラス $\mathbb{C}/\Lambda_1$ から複素トーラス $\mathbb{C}/\Lambda_2$ への正則写像に相当する.

定義 2.1.27 (isogeny). E_1, E_2 を楕円曲線とする. このとき, E_1 から E_2 への射 ϕ であって $\phi(O) = O$ を満たすものを E_1 から E_2 へ isogeny という. さらに,

$$\mathrm{Hom}(E_1, E_2) := \{\phi : E_1 \to E_2 \ ; \ \phi\text{は isogeny}\}$$

とし, $\mathrm{End}(E_1) := \mathrm{Hom}(E_1, E_1)$ とし, $\mathrm{End}(E_1)$ の元であって自己同型なものからなる集合を $\mathrm{Aut}\,(E_1)$ とする

注 2.1.28. 以下を注意として与える.

(1) 定義で使われる射という言葉は代数幾何の言葉であり, 定義の詳細は [16, I §3] あるいは [9, I §4] を参照. しかし, 大まかに言えば射とは有理多項式で与えられる変数変換のことである.

(2) isogeny は群の準同型である.

(3) ϕ_1, ϕ_2 を E_1 から E_2 への isogeny とすれば,

$$\begin{aligned} \phi_1 + \phi_2 : E_1 \ni P \mapsto \phi_1(P) + \phi_2(P) \in E_2, \\ -\phi_1 : E_1 \ni P \mapsto -\phi_1(P) \in E_2 \end{aligned} \tag{2.1.29}$$

もまたともに E_1 から E_2 への isogeny となる. よって $\mathrm{Hom}(E_1, E_2)$ は $\mathbb{Z}$-加群であり, さらに $\mathrm{End}(E_1)$ は合成を積として環をなし, $\mathrm{Aut}\,(E_1)$ は合成を演算として群をなす.

(4) (3) より, 特に $m \in \mathbb{Z}$ に対し, m 倍写像 $[m] : E_1 \ni P \mapsto [m]P \in E_1$ もまた isogeny である.

(5) 変数変換 (2.1.7) も当然 isogeny である.

例 2.1.30 (dual isogeny). ([16, Ⅲ Ex. 4.5] より引用.) $\mathrm{ch}\,(K) \neq 2$ とし, $a, b \in K$ を $b \neq 0$ かつ $a^2 - 4b \neq 0$ として取ってくれば, 2 つの K 上定義された楕円曲線

$$E_1/K : y^2 = x^3 + ax^2 + bx, \tag{2.1.31}$$
$$E_2/K : Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X \tag{2.1.32}$$

において次の ϕ, $\hat{\phi}$ はともに degree 2 の isogeny であり, $\hat{\phi} \circ \phi = \phi \circ \hat{\phi} = [2]$ となる.

$$\phi : E_1 \to E_2 \quad (x, y) \mapsto \left(\frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2} \right),$$
$$\hat{\phi} : E_2 \to E_1 \quad (X, Y) \mapsto \left(\frac{Y^2}{4X^2}, \frac{Y\{(a^2 - 4b) - X^2\}}{8X^2} \right).$$

dual isogeny について述べる前に, 自己準同型環 $\mathrm{End}(E)$ と自己同型群 $\mathrm{Aut}\,(E)$ の構造にについて述べておく. ここで, $\mathrm{Hom}(E_1, E_2)$ がねじれのない $\mathrm{rank}_{\mathbb{Z}}\mathrm{Hom}(E_1, E_2) \leq 4$ となる $\mathbb{Z}$-自由加群であることが知られており, $\mathrm{End}(E)$ および $\mathrm{Aut}\,(E)$ は次の命題で与えられた構造を持つ. ちなみに $\mathbb{C}$ 上において $\mathrm{End}(E)$ は複素トーラスの自己正則環に同型であり, それは $\mathbb{Z}$ またはある虚 2 次体の order に同型である.

命題 2.1.33 (End と Aut の構造). ([16, Ⅲ Cor. 9.4, Thm. 10.1] を参照.) E/K を楕円曲線とする. このとき $\mathrm{End}(E)$ は次の 3 つのいずれかに同型である.

(a) $\mathbb{Z}$.

(b) $\mathbb{Q}$ 上のある虚 2 次体の order.

(c) $\mathbb{Q}$ 上のある四元環の order.

さらに, $\mathrm{Aut}\,(E)$ は位数が 24 を割る有限群であり, 以下のように分類される.

$$\mathrm{Aut}\,(E) = \begin{cases} 2 & (j(E) \neq 0, 1728 \text{ のとき}) \\ 4 & (j(E) = 1728 \text{ かつ } \mathrm{ch}\,(K) \neq 2, 3 \text{ のとき}) \\ 6 & (j(E) = 0 \text{ かつ } \mathrm{ch}\,(K) \neq 2, 3 \text{ のとき}) \\ 12 & (j(E) = 1728 = 0 \text{ かつ } \mathrm{ch}\,(K) = 3 \text{ のとき}) \\ 24 & (j(E) = 1728 = 0 \text{ かつ } \mathrm{ch}\,(K) = 2 \text{ のとき}). \end{cases} \tag{2.1.34}$$

注 2.1.35. 以下を注意として与える.

(1) $\mathrm{ch}\,(K) = 0$ であれば Lifshetz の原理から $\mathrm{End}(E)$ は (c) と同型ではない ([16, Ⅵ Thm. 6.1] を参照). よって, (a) と同型でなければ (b) と同型である. このとき, E は虚数乗法をもつまたは CM をもつという. この名前は $\mathbb{C}$ 上の E に対応するトーラスを定める lattice Λ において, $\alpha\Lambda \subset \Lambda$ となる $\alpha \in \mathbb{C} \setminus \mathbb{R}$ が存在していることに由来する.

(2) K が有限体ならば, $\mathrm{End}(E) \neq \mathbb{Z}$ である.

次に dual isogeny の定義と諸性質の説明に入る. dual isogeny の性質から, $E(K)$ のねじれ部分群 $E(K)_{\mathrm{tors}}$ の構造を得ることもできる.

定義 2.1.36 (dual isogeny). E_1, E_2 を楕円曲線とし, $\phi : E_1 \to E_2$ を degree m の定値ではない isogeny とする. このとき, [16, Ⅲ Thm. 6.1] より $\phi' \circ \phi = [m]$ を満たす isogeny $\phi' : E_2 \to E_1$ が唯 1 つ存在しており, この ϕ' を ϕ の dual isogeny といい, $\hat{\phi}$ と書く.

注 2.1.37. 定義から, 例 2.1.30 において, $\hat{\phi}(\phi)$ は $\phi(\hat{\phi})$ の dual isogeny である.

命題 2.1.38 (dual isogeny の性質). ([16, Ⅲ Thm. 6.2] を参照.) $\phi : E_1 \to E_2$ を isogeny とするとき, 以下の 4 つが成立する.

(a) $m = \deg\phi$ とすれば E_1 上 $\hat{\phi} \circ \phi = [m]$ であり, E_2 上 $\phi \circ \hat{\phi} = [m]$ である.

(b) 各 $m \in \mathbb{Z}$ に対して $\hat{[m]} = [m]$ であり, $\deg[m] = m^2$ となる.

(c) $\deg\hat{\phi} = \deg\phi$ である.

(d) $\hat{\hat{\phi}} = \phi$ である.

$m \in \mathbb{Z} \setminus \{0\}$ に対して $E[m] := \{P \in E(\overline{K}) \ ; \ [m]P = O\}$ とし, $P \in E[m]$ を m-torsion point という. このとき, $E[m]$ について次の系を得る. ちなみに $\mathbb{C}$ 上であれば, E に同型な複素トーラスが $\mathbb{C}/\Lambda$ で与えられることから $E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ であるため, $E(\mathbb{C})$ のねじれ部分群 $E(\mathbb{C})_{\mathrm{tors}}$ は $(\mathbb{Q}/\mathbb{Z}) \times (\mathbb{Q}/\mathbb{Z})$ に同型である.

系 2.1.39. 以下の 2 つが成り立つ.

(a) $m \in \mathbb{Z} \setminus \{0\}$ に対し, $\mathrm{ch}\,(K) = 0$ であるか, または m が $\mathrm{ch}\,(K)$ と互いに素であれば,

$$E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}).$$

が成り立つ.

(b) $\mathrm{ch}\,(K) = p$ のとき,

$$E[p^e] \cong \{O\} \qquad (e = 1, 2, \dots)$$

であるか, または

$$E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z} \qquad (e = 1, 2, \dots)$$

となる.

例 2.1.40 (位数 2 の元). $\mathrm{ch}\,(K) \neq 2$ のとき, $\overline{K}$ 上重根を持たない 3 次多項式 $f(x) \in K[x]$ に対し, $e_i (i = 1, 2, 3)$ を f の $\overline{K}$ における 3 根とし, 楕円曲線 E/K を

$$E/K : y^2 = f(x) = (x - e_1)(x - e_2)(x - e_1)$$

として与える. このとき (2.1.10) より, $P = (x, y) \in E$ に対して, $[2]P = O$ となることと $y = 0$ であることは必要十分であることから

$$E[2] = \{O, (e_1, 0), (e_2, 0), (e_3, 0)\} \cong (\mathbb{Z}/2\mathbb{Z})^2$$

を得る. ここで, 一般に $\mathrm{ch}\,(K) \neq 2$ である体 K 上定義された楕円曲線 E/K は下の形の Weierstrass 方程式で与えられた楕円曲線 E' に $\overline{K}$ 上同型であり, この方程式は Legendre 形式といわれる.

$$E' : y^2 = x(x - 1)(x - \lambda) \quad (\lambda \in \overline{K} \setminus \{0, 1\}).$$

2.2 Galois cohomology

Mordell-Weil の定理を中心とした代数体上の楕円曲線について述べる前に, そこでよく用いられる Galois cohomology について述べるが, 始めに Abel 群の Galois cohomology について述べる. 以下 K を完全体, $\overline{K}$ をその代数的閉包とし, $G_{\overline{K}/K} = \mathrm{Gal}(\overline{K}/K)$ とする.

定義 2.2.1 ($G_{\overline{K}/K}$-加群). A を Abel 群とする. このとき, Kull 位相による位相群としての $G_{\overline{K}/K}$ が離散位相による A に連続的に作用しているならば A を $G_{\overline{K}/K}$-加群という.

例 2.2.2. $\overline{K}^+$,$\overline{K}^*$ はともに自然な作用により $G_{\overline{K}/K}$-加群であり, K 上定義された楕円曲線もまた各点の成分への作用によってひき起こされる作用により $G_{\overline{K}/K}$-加群となる.

定義 2.2.3 ($0^{\mathrm{th}}, 1^{\mathrm{th}}$-cohomology(abelian case)). A を $G_{\overline{K}/K}$-加群とする. このとき

$$H^0(K, A) := A^{G_{\overline{K}/K}} = \{P \in A\ ;\ \text{各}\, \sigma \in G_{\overline{K}/K}\ \text{に対し}, P^\sigma = P\}$$

を $G_{\overline{K}/K}$-加群 A の 0^{th}-cohomology という. さらに連続写像 $\xi : G_{\overline{K}/K} \to A$ であって, 各 $\sigma, \tau \in G_{\overline{K}/K}$ に対し,

$$\xi_{\sigma\tau} = \xi_\sigma^\tau + \xi_\tau$$

を満たすものを 1-cocycle といい, 1-cocycle からなる集合を $Z^1(K, A)$ とする. また, $a \in A$ に対し写像

$$G_{\overline{K}/K} \ni \sigma \mapsto a^\sigma - a \in A$$

は連続写像であり 1-cocycle となるがこの形の写像を coboundary といい, coboundary からなる集合を $B(K,A)$ とする. このとき, A が Abel 群であることから, $Z^1(K,A)$, $B(K,A)$ はともに群であり, 剰余群 $H^1(K,A) := Z(K,A)/B(K,A)$ を 1^{th}-cohomology という.

ここで, 楕円曲線における弱有限生成定理の証明および, Selmer 群, Shafarevich-Tate 群の定義にも用いられる長完全列について述べる.

命題 2.2.4. (詳細は [16, B Prop. 2.3] を参照.) $G_{\overline{K}/K}$-加群としての短完全列

$$0 \longrightarrow A \xrightarrow{\phi} B \xrightarrow{\psi} C \longrightarrow 0 \tag{2.2.5}$$

において, $c \in C^{G_{\overline{K}/K}} = H^0(K,C)$ に対し, $\psi(b) = c$ となる $b \in B$ を取ることによって得られる 1-cocycle

$$\xi : G_{\overline{K}/K} \ni \sigma \mapsto b^\sigma - b \in A$$

を対応させることによって引き起こされる写像

$$\delta : H^0(K,C) \ni c \mapsto \{\xi\} \in H^1(K,A)$$

を connecting homomorphism という. これによって次の長完全列が存在する.

$$\begin{array}{l} 0 \longrightarrow H^0(K,A) \longrightarrow H^0(K,B) \longrightarrow H^0(K,C) \xrightarrow{\delta} \\ \qquad H^1(K,A) \longrightarrow H^1(K,B) \longrightarrow H^1(K,C) \longrightarrow \cdots \end{array} \tag{2.2.6}$$

次に述べる命題の (b) は Hilbert の定理 90 と呼ばれ, その次の系が主定理の補題の証明に用いられる.

命題 2.2.7. (詳細は [15, X §§1-3] を参照.) K を体とするとき次の 3 つが成り立つ.

(a) $H^1(K, \overline{K}^+) = 0$ である.

(b) $H^1(K, \overline{K}^*) = 0$ である.

(c) $\mathrm{ch}\,(K) = 0$ であるかまたは $(\mathrm{ch}\,(K), m) = 1$ のとき, μ_m を 1 の m 乗根からなる $\overline{K}^*$ の部分群とすれば

$$H^1(K, \mu_m) \cong K^*/(K^*)^m$$

が成り立つ.

系 2.2.8. (詳細は [15, p. 151] を参照.) L/K を有限次巡回拡大とし, σ を $\mathrm{Gal}(L/K)$ の生成元とする. このとき, $\alpha \in K^*$ に対し $\mathrm{N}_{L/K}(\alpha) = 1$ を満たすならば $\alpha = \sigma(\beta)/\beta$ となる $\beta \in L^*$ が存在する.

最後に非可換群 A における Galois cohomology を定義する.

定義 2.2.9 ($0^{\text{th}}, 1^{\text{th}}$-cohomology(non-abelian case)). Kull 位相による位相群としての $G_{\overline{K}/K}$ が離散位相による非可換群 A に連続的に作用しているとする. このとき

$$H^0(K,A) := A^{G_{\overline{K}/K}} = \{P \in A\ ;\ \text{各}\ \sigma \in G_{\overline{K}/K}\ \text{に対し},\ P^\sigma = P\}$$

を A の 0^{th}-cohomology という. さらに連続写像 $\xi : G_{\overline{K}/K} \to A$ であって, 各 $\sigma, \tau \in G_{\overline{K}/K}$ に対し,

$$\xi_{\sigma\tau} = \xi_\sigma^\tau \xi_\tau$$

を満たすものを 1-cocycle という. またさらに 2 つの 1-cocycle ξ, ζ が次を満たすとき cohomologous という. ある $P \in A$ が存在し, 各 $\sigma \in G_{\overline{K}/K}$ に対し

$$P^\sigma \xi_\sigma = \zeta_\sigma P$$

が成り立つ. これにより 1-cocycle からなる集合 H に同値関係を入れることができ, この関係による H の商集合を $H^1(K,A)$ とし, A の 1^{th}-cohomology という.

注 2.2.10. $H^0(K,A)$ は群であるが $H^1(K,A)$ は群ではないことに注意しておく.

2.3 Mordell-Weil の定理とそれに関連した話題

いよいよ, Mordell-Weil の定理およびその周辺について述べる. 一般に, 不定方程式の整数解および有理数解を求める問題は Diophantus 問題といい, Fermat の最終定理そして Mordell-Weil の定理もそれに関連した話題の 1 つである. 今, $E/\mathbb{Q}$ を楕円曲線としたとき, $E(\mathbb{Q})$ は, $E/\mathbb{Q}$ を与える不定方程式の有理数解からなる集合のことであり, 前にも話したように, Abel 群であり, Mordell-Weil の定理はそれが有限生成であることを主張している. しかも, それは一般の代数体 K に対しても成り立つ. よって, その生成元 (もしくは $E(K)$ のねじれ部分群 $E(K)_{\text{tors}}$ および free part の rank) を求めることに主眼が置かれることとなる. ここでは, その定理とその弱有限生成定理, そして $E(K)_{\text{tors}}$ について述べる. 以下 K は代数体としておく.

定理 2.3.1 (Mordell-Weil の有限生成定理). (詳細は [16, VIII] を参照.) E/K を楕円曲線とする. このとき $E(K)$ は有限生成 Abel 群である. 従って,

$$E(K) \cong E(K)_{\text{tors}} \oplus \mathbb{Z}^r \tag{2.3.2}$$

という形になる. このとき $\text{rank}E(K) = r$ とする.

注 2.3.3. 以下を注意として与える.

(1) 一般の E/K に対して $E(K)$ を求める algorithm は今のところ知られていない.

(2) 任意に大きい r をもつ楕円曲線が存在することが予想されており, rank 問題といわれているが, 2000 年の段階で ([12] を参照), $r \geq 24$ となる楕円曲線が存在することがわかっている.

Mordell-Weil の定理は次に述べる弱有限生成定理および降下定理とその定理中で述べられている高さが $E(K)$ に対して与えられるためいえる.

定理 2.3.4 (弱有限生成定理). ([16, VⅢ §1] を参照.) E/K を楕円曲線とする. このとき, 2 以上の各整数 m に対し $E(K)/mE(K)$ は有限群である.

定理 2.3.5 (降下定理). ([16, VⅢ Prop. 3.1] を参照.) Abel 群 A に対し, height function と呼ばれる以下の 3 つを満たす関数 $h : A \to \mathbb{R}$ が存在しているとする.

(a) $Q \in A$ に対し, 各 $P \in A$ において

$$h(P+Q) \leq 2h(P) + C_1$$

を満たす非負定数 $C_1 = C_1(A, Q)$ が存在する.

(b) 2 以上のある整数 m に対し, 各 $P \in A$ において

$$h(mP) \geq m^2 h(P) - C_2$$

を満たす非負定数 $C_2 = C_2(A)$ が存在する.

(c) 任意定数 $C_3 (\geq 0)$ に対し, 集合

$$\{P \in A \ ; \ h(P) \leq C_3\}$$

は有限集合である.

このとき, (b) における m に対し, A/mA が有限群であれば A は有限生成 Abel 群である.

補題 2.3.6. ([16, VⅢ §§4-6, Ex. 8.18] を参照.) E/K を楕円曲線とする. このとき, 2 以上の各整数 m に対する $E(K)$ 上の height function が存在する.

注 2.3.7. 上の定理と補題の 3 つについて以下の注意を与える.

(1) 弱有限生成定理は Kummer pairing ($E(K) \times G_{\overline{K}/K}$ から $E[m]$ へのある双線形な pairing) の kernel の考察と代数的整数論 (類数の有限性と Dirichlet の単数定理) からいえる. なおここで用いられる Kummer pairing は, E の m 倍による自明な $G_{\overline{K}/K}$-加群としての短完全列

$$0 \longrightarrow E[m] \longrightarrow E \xrightarrow{[m]} E \longrightarrow 0 \tag{2.3.8}$$

から得られる Galois cohomology の長完全列

$$0 \longrightarrow E(K)[m] \longrightarrow E(K) \xrightarrow{[m]} E(K) \xrightarrow{\delta} H^1(K, E[m]) \longrightarrow H^1(K, E) \xrightarrow{[m]'} H^1(K, E) \longrightarrow \cdots \tag{2.3.9}$$

(但し, $[m]'$ は $[m]$ によって引き起こされたものであり, δ は connecting homomorphism である) の connecting homomorphism δ で与えることもできる.

(2) 降下定理とその周辺の議論から, $E(K)/mE(K)$ の完全代表系が求まれば, 有限回の操作により $E(K)$ の生成元が求まることがいえる. もしくは $E(K)/mE(K)$ の群構造 (または位数) と $E(K)_{\mathrm{tors}}$ から $\mathrm{rank}E(K)$ が求まる. 従って, $E(K)/mE(K)$ の完全代表系, もしくは群構造 (または位数) と $E(K)_{\mathrm{tors}}$ を求めればよい. 実際の $E(K)/mE(K)$ の計算は, 可換図式 (2.3.9) の connecting homomorphism δ によって引き起こされる単射準同型 $\delta : E(K)/mE(K) \to H^1(K, E[m])$ の image を計算することとなる.

(3) 補題 2.3.6 において, 楕円曲線 $E/\mathbb{Q}$ を

$$E/\mathbb{Q} : y^2 = x^3 + Ax + B \qquad (A, B \in \mathbb{Z})$$

で与えたときの $E(\mathbb{Q})$ 上の height function は次で与えられ, 一般の代数体 K においてもほぼ同様に与えられる.

$$h_x : E(\mathbb{Q}) \to \mathbb{R}$$

$$h_x(P) = \begin{cases} \log H(x(P)) & (P \neq O \text{ のとき}) \\ 0 & (P = O \text{ のとき}) \end{cases}$$

(但し, H は $t \in \mathbb{Q}$ に対し $t = p/q$ を既約分数としたとき,

$$H(t) = \max\{|p|, |q|\}$$

で与える).

次に $E(K)$ を求める段階に入る. これが楕円曲線論の主題であった. 注 2.3.7 で, ある 2 以上の整数 m で $E(K)/mE(K)$ を求めればよいことを述べたが, まず $E(K)_{\mathrm{tors}}$ について述べる.

定理 2.3.10 (Luts-Nagell). $E/\mathbb{Q}$ を次の Weierstrass 方程式

$$y^2 = x^3 + Ax + B \qquad (A, B \in \mathbb{Z})$$

で与えられた楕円曲線とする. このとき, $P \in E(\mathbb{Q})_{\mathrm{tors}} \setminus \{O\}$ に対し, 次の 2 つが成り立つ.

(a) $x(P),\ y(P) \in \mathbb{Z}$ である.

(b) $P \in E[2]$ でなければ, $\mathbb{Z}$ において $y(P) \mid 4A^3 + 27B^2$ となる.

注 2.3.11. 以下を注意として与える.

(1) 上の定理は必要十分条件ではないが, $E(\mathbb{Q})_{\mathrm{tors}}$ の元を求める 1 つの方法を与える.

(2) 一般の代数体 K における $E(K)_{\mathrm{tors}}$ の元については, (a) の類似として, $P \in E(K)_{\mathrm{tors}}$ の位数がある素数のべきでなければ $x(P),\ y(P) \in R$ (但し, R は K の整数環) となることが知られている.

定理 2.3.10 で, $E(\mathbb{Q})_{\mathrm{tors}}$ の元はすべて整数点となることを述べたが, $E/\mathbb{Q}$ の整数点については次に述べる Siegel の定理により有限個しかないことがいえ, しかもその次で与える Mazur の定理から $E(\mathbb{Q})_{\mathrm{tors}}$ は 15 通りしかないことが知られている.

定理 2.3.12 (Siegel). S を K の無限素点を含む $M_{\mathbb{Q}}$ の任意の有限部分集合とする. このとき, $\deg f \geq 3$ であって $\overline{K}$ 上重根を持たない $f(x) \in K[x]$ に対して, $y^2 = f(x)$ を満たす S-整数解 (x, y) は高々有限個しかない.

定理 2.3.13 (Mazur). $E/\mathbb{Q}$ を楕円曲線とするとき $E(\mathbb{Q})_{\mathrm{tors}}$ は次で与える 15 個の群の 1 つに同型であり, しかもその 15 個それぞれに同型となる $\mathbb{Q}$ 上定義された楕円曲線が存在する.

$$\begin{aligned} &\mathbb{Z}/N\mathbb{Z} \qquad (1 \leq N \leq 10 \text{ または } N = 12) \\ &\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} \qquad (1 \leq N \leq 4). \end{aligned}$$

次に $E(K)/mE(K)$ の群構造もしくは位数を考えることになるのだが, 注 2.3.7 で述べたように $E(K)/mE(K)$ を $H^1(K, E[m])$ に埋め込んで計算または評価することを考えるが, $H^1(K, E[m])$ のままでは大き過ぎるため $H^1(K, E[m])$ より小さい群であって $E(K)/mE(K)$ を評価できそうな群を考える必要がある. その群は Selmer 群と呼ばれ, 節 2.5 で詳しく述べる.

2.4 主等質空間

Selmer 群と Shafarevich-Tate 群を定義する前にそれらの群を解釈する際に必要な E/K の主等質空間を定義し, その諸性質について幾つか述べる. 代数幾何の言葉を用いることにすれば, それは Jacobi 多様体が E/K となる K 上定義された種数 1 の曲線である (特にこの曲線は固定点を考えていないため必ずしも楕円曲線ではない). 以下 K は完全体とする.

定義 2.4.1 (主等質空間). E/K を K 上定義された楕円曲線とする. このとき, K 上定義された非特異曲線 C/K と以下の 3 つを満たす K 上定義された射 $\mu : C \times E \to C$ との対 (C, μ) を E/K の主等質空間という.

(a) 各 $p \in C$ に対して $\mu(p, O) = p$ である.

(b) 各 $p \in C$ と $P, Q \in E$ に対して,

$$\mu(\mu(p, P), Q) = \mu(p, P + Q)$$

が成り立つ.

(c) $p, q \in C$ に対して, $\mu(p, P) = q$ となる $P \in E$ が唯一つ存在している.

注 2.4.2. 以下の 2 つを注意として与える.

(1) 主等質空間の定義を代数群の言葉で言い換えると, 代数群としての E が K 上推移的に作用している非特異曲線 C/K のことである.

(2) $\theta : C' \to C$ が K 上同型射となる K 上定義された曲線 C'/K もまた主等質空間である. なぜなら, 射 $\mu' : C' \times E \to C'$ を

$$\mu'(p, P) := \theta^{-1}(\mu(\theta(p), P))$$

で与えれば直ちにこの μ' が上の定義を満たすことがいえるからである.

例 2.4.3 (主等質空間の例). K 上定義された楕円曲線 E/K を

$$\begin{aligned} E/K : y^2 = f(x) : &= x^3 + a_2x^2 + a_4x + a_6 \quad (a_i \in K) \\ &= (x - e_1)(x - e_2)(x - e_3) \quad (e_i \in \overline{K}) \end{aligned} \tag{2.4.4}$$

(但し, $i \neq j$ ならば $e_i \neq e_j$ である) とする. また,

$$\Delta = (e_2 - e_3)(e_3 - e_1)(e_1 - e_2)$$

とし, $\Lambda := (b_1, b_2, b_3) \in \prod_{i=1}^{3} K(e_i)^*$ を, $b_1b_2b_3 \in K^{*2}$ を満たし, 相異なる任意の $i, j \in \{1, 2, 3\}$ に対し, e_i と e_j が K 上共役ならば b_i と b_j もまた K 上共役となるものとして与える. これより, $H_0, G_0 \in \overline{K}[U_1, U_2, U_3]$ をそれぞれ,

$$Z_i = Z_i(U_1, U_2, U_3) := U_1 + U_2e_i + U_3e_i^2 \quad (i = 1, 2, 3)$$

として

$$\begin{aligned} H_0(U_1, U_2, U_3) &= \frac{1}{\Delta}\left\{(e_2 - e_3)b_1Z_1^2 + (e_3 - e_1)b_2Z_2^2 + (e_1 - e_2)b_3Z_3^2\right\}, \\ G_0(U_1, U_2, U_3) &= \frac{1}{\Delta}\left\{e_1(e_2 - e_3)b_1Z_1^2 + e_2(e_3 - e_1)b_2Z_2^2 + e_3(e_1 - e_2)b_3Z_3^2\right\} \end{aligned}$$

とする. このとき $\mathbb{P}^3$ における曲線 C_Λ を

$$C_\Lambda : \left\{H_0(U_1, U_2, U_3) = G_0(U_1, U_2, U_3) - T^2 = 0\right\} \tag{2.4.5}$$

とすれば, C_Λ は E/K の主等質空間となる. このことについては命題 2.4.17 で示すことにする. なお, この主等質空間は主定理における [2]-Selmer 群上の paring $\langle\cdot,\cdot\rangle$ の構成で用いられる. ここで, その構成のことも考え,

$$C_\Lambda = \left\{ H_i(U_1,U_2,U_3,T) := \frac{b_{i+1}Z_{i+1}^2 - b_{i+2}Z_{i+2}^2}{e_{i+1}-e_{i+2}} + T^2 = 0 \ ; \ i = 1,2,3 \right\} \tag{2.4.6}$$

であることを付け加えておく ($H_i = 0 (i = 1,2,3)$ のうち 2 つの式で十分ではあるが対称性のため 3 つの式で与えることにする). これが成り立つのは, 各 $i (i = 1,2,3)$ に対し添字を mod 3 で考えると

$$\begin{aligned}
&e_iH_0 - (G_0 - T^2) \\
&= \frac{e_i}{\Delta}\left\{(e_{i+1}-e_{i+2})b_iZ_i^2 + (e_{i+2}-e_i)b_{i+1}Z_{i+1}^2 + (e_i - e_{i+1})b_{i+2}Z_{i+2}^2\right\} \\
&\quad - \Big[\frac{1}{\Delta}\left\{e_i(e_{i+1}-e_{i+2})b_iZ_i^2 + e_{i+1}(e_{i+2}-e_i)b_{i+1}Z_{i+1}^2 + e_{i+2}(e_i-e_{i+1})b_{i+2}Z_{i+2}^2\right\} \\
&\qquad - T^2\Big] \\
&= \frac{1}{\Delta}\left\{(e_i-e_{i+1})(e_{i+2}-e_i)b_{i+1}Z_{i+1}^2 + (e_i-e_{i+2})(e_i-e_{i+1})b_{i+2}Z_{i+2}^2\right\} + T^2 \\
&= \frac{(e_i-e_{i+1})(e_{i+2}-e_i)(b_{i+1}Z_{i+1}^2 - b_{i+2}Z_{i+2}^2)}{(e_2-e_3)(e_3-e_1)(e_1-e_2)} + T^2 \\
&= \frac{b_{i+1}Z_{i+1}^2 - b_{i+2}Z_{i+2}^2}{e_{i+1}-e_{i+2}} + T^2 \\
&= H_i
\end{aligned}$$

となるため, e_i の取り方から $p = [U_1 : U_2 : U_3 : T] \in \mathbb{P}^3$ に対して

$$H_0(U_1,U_2,U_3) = G_0(U_1,U_2,U_3) - T^2 = 0$$

を満たすことと,

$$H_1(U_1,U_2,U_3,T) = H_2(U_1,U_2,U_3,T) = H_3(U_1,U_2,U_3,T) = 0$$

を満たすことは必要十分だからである.

ここで, 慣例として定義中の $\mu(p,P)$ を $p+P$ と書くことにすると, 定義中の (a) は P がこの和の単位元を意味し, (b) は結合律を意味する. また定義中の (c) から写像

$$\nu : C \times C \to E \qquad (p,q) \mapsto P$$

を得ることから, 慣例として $\mu(q,p)$ を $q-p$ と書くことにする. これらを用いて, これより主等質空間の性質を幾つか述べる.

命題 2.4.7 (主等質空間の性質). (詳細は [16, X §3] を参照.) E/K を K 上定義された楕円曲線とし, C/K を E/K の主等質空間とする. このとき以下の 3 つが成り立つ.

(a) 上で定めた $+, -$ と E 上の演算の $+, -$ を同時に用いることにすれば, 定義より各 $p, q \in C$, $P, Q \in E$ に対し以下の 5 つが成り立つ.

(i) $p + O = p$, (ii) $p - p = O$, (iii) $p + (q - p) = q$,
(iv) $(p + P) - p = P$, (v) $(q + Q) + (p + P) = (q - p) + (Q - P)$.

(b) 任意に取ってきた点 $p_0 \in C$ に対し, 射

$$\theta : E \ni P \mapsto p_0 + P (= \mu(p_0, P)) \in C$$

は $K(p_0)$ 上の同型射であり, 各 $p, q \in C$, $P \in E$ に対し

$$p + P = \theta(\theta^{-1}(p) + P), \quad q - p = \theta^{-1}(q) - \theta^{-1}(p)$$

が成り立つ.

(c) 写像 $\nu : C \times C \to E$ は K 上定義された射である.

次に Weil-Chatelet 群を定義し, Galois cohomology との関係を述べた後, E/K が C/K の Jacobi 多様体であることを述べてこの節を終わりにする.

定義 2.4.8 (Weil-Chatelet 群). E/K の任意の 2 つの主等質空間 C/K, C'/K に対し, $C/K \sim C'/K$ を E の C, C' への作用と可換となる K 同型射 $\theta : C \to C'$ が存在すると定めれば関係 $\sim$ は同値関係である. このとき, T を E/K の主等質空間からなる集合としたとき, $T/\sim$ を E/K の Weil-Chatelet 群といい, $WC(E/K)$ と書く. さらに E を含む同値類を trivial class という.

注 2.4.9 (Weil-Chatelet 群について). 以下を注意として与える.

(1) 次で与える命題 2.4.10 により $WC(E/K)$ は trivial class を単位元として群をなす.

(2) $\theta : C' \to C$ が K 上同型射となる K 上定義された曲線 C'/K もまた主等質空間であることは注 2.4.2 の (2) で述べたが, 必ずしも $C/K \sim C'/K$ とは限らない. これは後で述べる可換図式 (2.4.15) において $H^1(K, E) \to H^1(K, \mathrm{Isom}(E))$ が単射でないことに起因する.

(3) C/K を E/K の主等質空間とする. このとき, C/K が trivial class に含まれることと $C(K) \neq \emptyset$ であることは必要十分である ([16, X Prop. 3.3] を参照). 従って C/K が trivial class に含まれるかどうかを調べるためには C/K における K-有理点の存在性を調べればよい. これより Selmer 群の実質的な計算が可能となる. なお, Selmer 群の計算については節 2.6 で述べる.

命題 2.4.10 (Weil-Chatelet 群の群構造). ([16, X Thm. 3.6] を参照.) E/K を楕円曲線とする. このとき, 写像

$$WC(E/K) \to H^1(K, E) \qquad \{C/K\} \mapsto \{G_{\overline{K}/K} \ni \sigma \mapsto p_0^\sigma - p_0 \in E\} \tag{2.4.11}$$

(但し, p_0 は C 上の点として取る) は $p_0 \in C$ の取り方に寄らず定まり全単射である. 従ってこれにより $WC(E/K)$ に群の演算を自然に定義できる.

命題 2.4.7 の (b) より E/K の主等質空間 C/K は常に $\overline{K}$ 上同型であったが, 逆に E/K に $\overline{K}$ 上同型となる K 上定義された曲線 C/K がいつ E/K の主等質空間となるかを次に述べる. その後, 例 2.4.3 で与えた楕円曲線 E/K と C_Λ に対し, C_Λ が E/K の主等質空間であることを示す.

定義 2.4.12 (Twist). K 上定義された楕円曲線 E/K に対し, $\overline{K}$ 上同型な K 上定義された (非特異) 曲線 C/K を E/K の twist という. このとき, E/K の twist からなる集合に対し K 上同型なものを同一視した商集合を $\mathrm{Twist}(E/K)$ をとする.

$\mathrm{Isom}(E)$ を楕円曲線 E の自己同型射からなる集合とすれば, 写像の合成を演算として群をなす ($\mathrm{Isom}(E)$ は $\mathrm{Aut}\,(E)$ と違い, 自己同型射 ϕ は $\phi(O) = O$ を満たさなくてもよい). このとき次の命題が成り立つ.

命題 2.4.13 ($\mathrm{Twist}(E/K)$ と $H^1(K, \mathrm{Isom}(E))$). ([16, X Thm. 2.2] を参照.) K 上定義された楕円曲線 E/K に対し, 写像

$$\begin{aligned} \mathrm{Twist}(E/K) &\to H^1(K, \mathrm{Isom}(E)) \\ \{C/K\} &\mapsto \{G_{\overline{K}/K} \ni \sigma \mapsto \theta^\sigma \circ \theta^{-1} \in \mathrm{Isom}(E)\} \end{aligned} \tag{2.4.14}$$

は全単射である.

上の命題から次の可換図式を得る.

$$\begin{array}{ccc} WC(E/K) & \xrightarrow{\kappa_1} & H^1(K, E) \\ \downarrow{\scriptstyle \iota_1} & \circlearrowright & \downarrow{\scriptstyle \iota_2} \\ \mathrm{Twist}(E/K) & \xrightarrow{\kappa_2} & H^1(K, \mathrm{Isom}(E)) \end{array} \tag{2.4.15}$$

(但し, ι_1 は命題 2.4.7 の (b) より E/K の主等質空間が E/K の twist であることから得られる自然な写像であり, ι_2 は $\{\xi\} \in H^1(K, E)$ に対し

$$\{\tau_{\xi_\sigma} : E \ni P \mapsto P + \xi_\sigma \in E\} \in H^1(K, \mathrm{Isom}(E))$$

を対応させる写像である). これと注 2.4.2 の (2) から, E/K の twist C/K が E/K の主等質空間となるための必要十分条件として次を得る.

命題 2.4.16 (C/K が E/K の主等質空間となるための必要十分条件). E/K を K 上定義された楕円曲線, C/K を E/K の twist とする. このとき, C/K が E/K の主等質空間となるための必要十分条件はある 1-cocycle $\xi : G_{\overline{K}/K} \to E$ が存在して, ξ に対する 1-cocycle τ_{ξ_σ} を

$$\tau_{\xi_\sigma} : E \ni P \mapsto P + \xi_\sigma \in E$$

としたとき, 同型射 $\theta : C \to E$ による 1-cocycle

$$G_{\overline{K}/K} \ni \sigma \mapsto \theta^\sigma \circ \theta^{-1} \in \mathrm{Isom}(E)$$

と τ_{ξ_σ} が cohomologous となることである.

上の命題で与えた条件を用いて次の命題を示す.

命題 2.4.17. $E/K, C_\Lambda$ ともに例 2.4.3 で与えたものとする. このとき, C_Λ は E/K の主等質空間である.

証明. 方針としてはまず, C_Λ が E/K の twist であることを示した後, ある cohomology class $\{\xi\} \in H^1(K, E)$ が存在して $G_{\overline{K}/K}$ 上 $\theta^\sigma \circ \theta^{-1} = \tau_{\xi_\sigma}$ であることをいう. これがいえれば命題 2.4.16 から C/K は E/K の主等質空間である.

Step1 : C_Λ が K 上定義されていることを示す. これは, Galois 理論から C_Λ を定義する 2 つの方程式が, $f(x)$ の最小分解体を K' としたときの拡大 K'/K の Galois 群の作用で不変であることがいえればよい. 今, $\sigma \in \mathrm{Gal}(K'/K)$ はある $\sigma' \in \mathfrak{S}_3$ により

$$\sigma : \begin{cases} e_1 \mapsto e_{\sigma'(1)} \\ e_2 \mapsto e_{\sigma'(2)} \\ e_3 \mapsto e_{\sigma'(3)} \end{cases}$$

をひき起こすことから, 各 $i (i = 1, 2, 3)$ に対し

$$Z_i^\sigma = U_1 + U_2\sigma(e_i) + U_3\sigma(e_i^2) = U_1 + U_2 e_{\sigma'(i)} + U_3 e_{\sigma'(i)} = Z_{\sigma'(i)}$$

であるため, 添字を mod 3 で考えると

$$\begin{aligned} H_0^\sigma &= \frac{1}{\sigma(\Delta)}\Big\{\sigma((e_2 - e_3)b_1)Z_{\sigma'(1)}^2 + \sigma((e_3 - e_1)b_2)Z_{\sigma'(2)}^2 + \sigma((e_1 - e_2)b_3)Z_{\sigma'(3)}^2\Big\} \\ &= \frac{\mathrm{sig}(\sigma')}{\Delta}\Big\{(e_{\sigma'(2)} - e_{\sigma'(3)})b_{\sigma'(1)}Z_{\sigma'(1)}^2 + (e_{\sigma'(3)} - e_{\sigma'(1)})b_{\sigma'(2)}Z_{\sigma'(2)}^2 \\ &\qquad + (e_{\sigma'(1)} - e_{\sigma'(2)})b_{\sigma'(3)}Z_{\sigma'(3)}^2\Big\} \end{aligned}$$

となる. ここで, σ' は集合 $\{1, 2, 3\}$ から $\{1, 2, 3\}$ への全単射であることから各 $i (i = 1, 2, 3)$ に対して $\sigma'(i+1) = \sigma'(i) + 1$ であるか (このとき当然, $\sigma'(3) = \sigma'(1) + 2$), または各 $i (i = 1, 2, 3)$ に対して $\sigma'(i+1) = \sigma'(i) + 2$ であり, 前者であれば σ' は巡回置換

となる. また, $\mathfrak{S}_3$ において巡回置換は 3 個あり, それはすべて隅置換であることと隅置換と奇置換の個数が等しく $\#\mathfrak{S}_3 = 6$ であることから前者のときかつそのときのみ $\mathrm{sig}(\sigma') = 1$ となる. よって, 各 $i(i = 1, 2, 3)$ に対し

$$e_{\sigma'(i+1)} - e_{\sigma'(i+2)} = \mathrm{sig}(\sigma')(e_{\sigma'(i)+1} - e_{\sigma'(i)+2})$$

であるため

$$\begin{aligned} H_0^\sigma &= \frac{\mathrm{sig}(\sigma')^2}{\Delta}\Big\{(e_{\sigma'(1)+1} - e_{\sigma'(1)+2})b_{\sigma'(1)}Z_{\sigma'(1)}^2 + (e_{\sigma'(2)+1} - e_{\sigma'(2)+2})b_{\sigma'(2)}Z_{\sigma'(2)}^2 \\ &\qquad + (e_{\sigma'(3)+1} - e_{\sigma'(3)+2})b_{\sigma'(3)}Z_{\sigma'(3)}^2\Big\} \\ &= H_0 \end{aligned}$$

となり, G_0 も同様にすればよい. 従って, H_0, G_0 ともに K 上定義されているため C_Λ も K 上定義されている.

Step2 : C_Λ が E/K の twist であることを示す. Step1 で C_Λ が K 上定義されていることを示したので C_Λ と E/K が $\overline{K}$ 上同型を示す. E/K は

$$\begin{aligned} E/K : y^2 = f(x) :&= x^3 + a_2x^2 + a_4x + a_6 \quad (a_i \in K) \\ &= (x - e_1)(x - e_2)(x - e_3) \quad (e_i \in \overline{K}) \end{aligned} \tag{2.4.18}$$

で与えられおり, 変数変換

$$y = \frac{T}{U}, \quad x = \frac{V}{U}, \quad x^2 = \frac{W}{U} \tag{2.4.19}$$

により

$$\begin{aligned} H^{(1)}(U, V, W) &:= UW - V^2, \\ G^{(1)}(U, V, W) &:= VW + a_2V^2 + a_4UV + a_6U^2 \end{aligned}$$

としたときの $\mathbb{P}^3$ における曲線 C_1

$$C_1 : \left\{H^{(1)}(U, V, W) = G^{(1)}(U, V, W) - T^2 = 0\right\}$$

に K 上同型である (この変数変換による E から C_1 への同型射を α_1 とする). さらに, C_1 は変数変換

$$\begin{pmatrix} Z_1' \\ Z_2' \\ Z_3' \end{pmatrix} = \begin{pmatrix} -(2e_1^2 - 2e_1a_2 + a_4) & -2e_1 & 1 \\ -(2e_2^2 - 2e_2a_2 + a_4) & -2e_2 & 1 \\ -(2e_3^2 - 2e_3a_2 + a_4) & -2e_3 & 1 \end{pmatrix} \begin{pmatrix} U \\ V \\ W \end{pmatrix}, \ T = T \tag{2.4.20}$$

により

$$\begin{aligned} H^{(2)}(Z_1', Z_2', Z_3') &:= \frac{1}{4\Delta}\left\{(e_2 - e_3){Z_1'}^2 + (e_3 - e_1){Z_2'}^2 + (e_1 - e_2){Z_3'}^2\right\}, \\ G^{(2)}(Z_1', Z_2', Z_3') &:= \frac{1}{4\Delta}\left\{e_1(e_2 - e_3){Z_1'}^2 + e_2(e_3 - e_1){Z_2'}^2 + e_3(e_1 - e_2){Z_3'}^2\right\} \end{aligned}$$

としたときの $\mathbb{P}^3$ における曲線 C_2

$$C_2 : \big\{H^{(2)}(Z_1', Z_2', Z_3') = G^{(2)}(Z_1', Z_2', Z_3') - T^2 = 0\big\}$$

に $K(e_1, e_2, e_3)$ 上同型である (この変数変換による C_1 から C_2 への同型射を α_2 とする). なぜなら, 変数変換 (2.4.20) における変換行列の行列式は $-4\Delta \neq 0$ であり,

$$\begin{aligned}
-\Delta &= -(e_2 - e_3)(e_3 - e_1)(e_1 - e_2) \\
&= -(e_1e_2 - e_2^2 - e_1e_3 + e_2e_3)(e_3 - e_1) \\
&= -e_1e_2e_3 + e_2^2e_3 + e_1e_3^2 - e_2e_3^2 + e_1^2e_2 - e_1e_2^2 - e_1^2e_3 + e_1e_2e_3 \\
&= -e_2e_3^2 - e_3e_1^2 - e_1e_2^+e_2^2e_3 + e_3^2e_1 + e_1^2e_2 \\
&= e_1^2(e_2 - e_3) + e_2^2(e_3 - e_1) + e_3^2(e_1 - e_2)
\end{aligned}$$

となることと, $f(x) = x^3 + a_2x^2 + a_4x + a_6$ の解と係数の関係から

$$\begin{aligned}
-(2e_i^2 - 2e_ia_2 + a_4) &= -2e_i^2 + 2(e_i + e_{i+1} + e_{i+2})e_i - (e_{i+1}e_{i+2} + e_{i+2}e_i + e_ie_{i+1}) \\
&= e_i(e_{i+1} + e_{i+2}) - e_{i+1}e_{i+2}
\end{aligned}$$

ゆえ,

$$\begin{aligned}
H^{(2)}(Z_1', Z_2', Z_3') &= \frac{1}{4\Delta}\Big\{(e_2 - e_3){Z_1'}^2 + (e_3 - e_1){Z_2'}^2 + (e_1 - e_2){Z_3'}^2\Big\} \\
&= \frac{1}{4\Delta}\Big[(e_2 - e_3)\{-(2e_1^2 - 2e_1a_2 + a_4)U - 2e_1V + W\}^2 \\
&\qquad + (e_3 - e_1)\{-(2e_2^2 - 2e_2a_2 + a_4)U - 2e_2V + W\}^2 \\
&\qquad + (e_1 - e_2)\{-(2e_3^2 - 2e_3a_2 + a_4)U - 2e_3V + W\}^2\Big]
\end{aligned}$$

となる. ここで, 一番下の式を

$$\frac{1}{4\Delta}\big\{AU^2 + BV^2 + CW^2 + 2DUV + 2EUW + 2FVW\big\}$$

とおくと B, C, E, F はそれぞれ,

$$\begin{aligned}
B &= 4\big\{e_1^2(e_2 - e_3) + e_2^2(e_3 - e_1) + e_3^2(e_1 - e_2)\big\} = -4\Delta, \\
C &= (e_2 - e_3) + (e_3 - e_1) + (e_1 - e_2) = 0, \\
E &= -(2e_1^2 - 2e_1a_2 + a_4)(e_2 - e_3) - (2e_2^2 - 2e_2a_2 + a_4)(e_3 - e_1) \\
&\qquad - (2e_3^2 - 2e_3a_2 + a_4)(e_1 - e_2) \\
&= -2\{e_1^2(e_2 - e_3) + e_2^2(e_3 - e_1) + e_3^2(e_1 - e_2)\} \\
&= 2\Delta, \\
F &= -2\big\{e_1(e_2 - e_3) + e_2(e_3 - e_1) + e_3(e_1 - e_3)\big\} = 0
\end{aligned}$$

である. さらに A は

$$\begin{aligned}A &= (2e_1^2 - 2e_1a_2 + a_4)^2(e_2 - e_3) + (2e_2^2 - 2e_2a_2 + a_4)^2(e_3 - e_1) \\ &\quad + (2e_3^2 - 2e_3a_2 + a_4)^2(e_1 - e_2) \\ &= \big\{e_1(e_2 + e_3) - e_2e_3\big\}^2(e_2 - e_3) + \big\{e_2(e_3 + e_1) - e_3e_1\big\}^2(e_3 - e_1) \\ &\quad + \big\{e_3(e_1 + e_2) - e_1e_2\big\}^2(e_1 - e_2) \\ &= 0\end{aligned}$$

であり, D は

$$\begin{aligned}D &= 2e_1(2e_1^2 - 2e_1a_2 + a_4)(e_2 - e_3) + 2e_2(2e_2^2 - 2e_2a_2 + a_4)(e_3 - e_1) \\ &\quad + 2e_3(2e_3^2 - 2e_3a_2 + a_4)(e_1 - e_2) \\ &= -2e_1\big\{e_1(e_2 + e_3) - e_2e_3\big\}(e_2 - e_3) - 2e_2\big\{e_2(e_3 + e_1) - e_3e_1\big\}(e_3 - e_1) \\ &\quad - 2e_3\big\{e_3(e_1 + e_2) - e_1e_2\big\}(e_1 - e_2) \\ &= -4\Big\{(e_1e_2 - e_2e_3 + e_3e_1)(e_1e_2 - e_1e_3) \\ &\quad + (e_2e_3 - e_3e_1 + e_1e_2)(e_2e_3 - e_1e_2) \\ &\quad + (e_3e_1 - e_1e_2 + e_2e_3)(e_3e_1 - e_2e_3)\Big\} \\ &= 0\end{aligned}$$

となる. 以上より変数変換により

$$H^{(2)}(Z_1', Z_2', Z_3') = UW - V^2 = H^{(1)}(U, V, W)$$

である. また, 同様にして

$$G^{(2)}(Z_1', Z_2', Z_3') = VW + a_2V^2 + a_4UV + a_6U^2 = G^{(1)}(U, V, W)$$

となることから変数変換 (2.4.20) による射 α_2 は同型である. さらに, C_2 は変数変換 $Z_i = Z_i'/(2\sqrt{b_i})(i = 1, 2, 3), T = T$ により

$$\begin{aligned}H^{(3)}(Z_1, Z_2, Z_3) &:= \frac{1}{\Delta}\left\{(e_2 - e_3)b_1{Z_1}^2 + (e_3 - e_1)b_2{Z_2}^2 + (e_1 - e_2)b_3{Z_3}^2\right\}, \\ G^{(3)}(Z_1, Z_2, Z_3) &:= \frac{1}{\Delta}\left\{e_1(e_2 - e_3)b_1{Z_1}^2 + e_2(e_3 - e_1)b_2{Z_2}^2 + e_3(e_1 - e_2)b_3{Z_3}^2\right\}\end{aligned}$$

としたときの $\mathbb{P}^3$ における曲線

$$C_3 : \left\{H^{(3)}(Z_1, Z_2, Z_3) = G^{(3)}(Z_1, Z_2, Z_3) - T^2 = 0\right\}$$

に $K(\sqrt{b_1}, \sqrt{b_2}, \sqrt{b_3})$ 上同型であり (この変数変換よる C_2 から C_3 への同型射を α_3 とする), C_3 は C_Λ の与え方から変数変換

$$\begin{pmatrix}U_1 \\ U_2 \\ U_3\end{pmatrix} = \begin{pmatrix}1 & e_1 & e_1^2 \\ 1 & e_2 & e_2^2 \\ 1 & e_3 & e_3^2\end{pmatrix}^{-1}\begin{pmatrix}Z_1 \\ Z_2 \\ Z_3\end{pmatrix} \tag{2.4.21}$$

により C_Λ に $K(e_1,e_2,e_3)$ 上同型である (この変数変換よる C_3 から C_Λ への同型射を α_4 とする). 以上より $N_\Lambda := K(e_i, \sqrt{b_i}\ ;\ i=1,2,3)$ とすれば, $\theta := (\alpha_4\circ\alpha_3\circ\alpha_2\circ\alpha_1)^{-1}$ は C_Λ から E への N_Λ 上, 特に $\overline{K}$ 上の同型射ゆえ, C_Λ は E の twist である. ちなみに $\alpha_{13} := \alpha_3\circ\alpha_2\circ\alpha_1$ による $E[2]$ の元の行き先は

$$\begin{aligned}
\alpha_{13}(O) &= \left[\frac{1}{2\sqrt{b_1}} : \frac{1}{2\sqrt{b_2}} : \frac{1}{2\sqrt{b_3}} : 0\right] \\
\alpha_{13}(e_1,0) &= \left[\frac{-1}{2\sqrt{b_1}} : \frac{1}{2\sqrt{b_2}} : \frac{1}{2\sqrt{b_3}} : 0\right] \\
\alpha_{13}(e_2,0) &= \left[\frac{1}{2\sqrt{b_1}} : \frac{-1}{2\sqrt{b_2}} : \frac{1}{2\sqrt{b_3}} : 0\right] \\
\alpha_{13}(e_3,0) &= \left[\frac{1}{2\sqrt{b_1}} : \frac{1}{2\sqrt{b_2}} : \frac{-1}{2\sqrt{b_3}} : 0\right]
\end{aligned}$$

となる.

Step3 : Step2 の θ に対し, K 上定義された射 $\kappa : C_\Lambda \to E$ が存在して, 可換図式

$$\begin{array}{ccc} E & \xrightarrow{[2]} & E \\ {\scriptstyle\theta^{-1}}\downarrow & \circlearrowleft & \nearrow{\scriptstyle\kappa} \\ C_\Lambda & & \end{array} \tag{2.4.22}$$

を得ることを示す. これについては θ の全単射性から C_Λ 上 $[2]\circ\theta = \kappa$ となる K 上定義された射 κ の存在性をいえば十分である. 今, $p := [u_1 : u_2 : u_3 : t] \in C_\Lambda$ に対し, $z_i = u_1 + u_2 e_i + u_3 e_i^2$, $z_i' = 2\sqrt{b_i} z_i (i=1,2,3)$ とし,

$$\begin{pmatrix} u \\ v \\ w \end{pmatrix} = \begin{pmatrix} -(2e_1^2 - 2e_1a_2 + a_4) & -2e_1 & 1 \\ -(2e_2^2 - 2e_2a_2 + a_4) & -2e_2 & 1 \\ -(2e_3^2 - 2e_3a_2 + a_4) & -2e_3 & 1 \end{pmatrix}^{-1} \begin{pmatrix} z_1' \\ z_2' \\ z_3' \end{pmatrix}$$

とし, さらに $x' = v/u,\ y' = t/u$ とすれば $x'^2 = w/u$ であり, 以上より $(x',y') = \theta(p)$ である. また, $P=(x,y) \in E$ に対し

$$x\circ[2](P) - e_i = \left\{\frac{x^2 - 2e_ix - (2e_i^2 - 2e_ia_2 + a_4)}{2y}\right\}^2 \tag{2.4.23}$$

である. よって, 各 $i(i=1,2,3)$ に対し

$$\begin{aligned}
x\circ([2]\circ\theta)(p) - e_i &= \left\{\frac{x'^2 - 2e_ix' - (2e_i^2 - 2e_ia_2 + a_4)}{2y'}\right\}^2 \\
&= \left\{\frac{(w/u) - 2e_i(v/u) - (2e_i^2 - 2e_ia_2 + a_4)}{2(t/u)}\right\}^2 \\
&= \left\{\frac{w - 2e_iv - (2e_i^2 - 2e_ia_2 + a_4)u}{2t}\right\}^2 \\
&= \left(\frac{z_i'}{2t}\right)^2 = \frac{(2\sqrt{b_i}z_i)^2}{4t^2} = \frac{b_iz_i^2}{t^2}
\end{aligned} \tag{2.4.24}$$

となり, 元々Eは(2.4.18)で与えられていることから, b_iの取り方から$b_1b_2b_3 = b^2$となる$b \in K$を取ると

$$\{y \circ ([2] \circ \theta)(p)\}^2 = \frac{b_1 {Z_1}^2}{t^2} \cdot \frac{b_2 {z_2}^2}{t^2} \cdot \frac{b_3 {z_3}^2}{t^2} = \left(\frac{bz_1z_2z_3}{t^3}\right)^2$$

ゆえ, $y \circ ([2] \circ \theta)(p)$は$bz_1z_2z_3/t^3$または$-bz_1z_2z_3/t^3$である. よって, 場合によっては$-b$を$b$とおき直して, 射$\kappa : C_\Lambda \to E$を

$$\kappa : C_\Lambda \ni p = [u_1 : u_2 : u_3 : t] \mapsto \left(e_1 + \frac{b_1 z_1^2}{t^2}, \frac{bz_1z_2z_3}{t^3}\right) \in E \tag{2.4.25}$$

で与える. このとき, 明らかにC_Λ上$[2] \circ \theta = \kappa$であり, この$\kappa$が$K$上定義されていることは$b_i, z_i$の与え方と, (2.4.24)より

$$x \circ ([2] \circ \theta)(p) = e_1 + \frac{b_1 z_1^2}{t^2} = e_2 + \frac{b_2 z_2^2}{t^2} = e_3 + \frac{b_3 z_3^2}{t^2}$$

であることからいえる. 従ってこのκから可換図式(2.4.22)を得る.

Step4 : C_ΛがE/Kの主等質空間であることを示す. $\sigma \in G_{\overline{K}/K}$と$P \in E$に対し$\xi_\sigma := \theta^\sigma \circ \theta^{-1}(P) - P$とする. このとき, ξ_σがPの取り方に依らずに定まることがいえれば

$$G_{\overline{K}/K} \ni \sigma \mapsto \theta^\sigma \circ \theta^{-1} \in \mathrm{Isom}(E)$$

が1-cocycleゆえ

$$\xi : G_{\overline{K}/K} \ni \sigma \mapsto \xi_\sigma \in E$$

もまた1-cocycleとなり, 当然$\theta^\sigma \circ \theta^{-1} = \tau_{\xi_\sigma}$であることから命題2.4.16より$C_\Lambda$は$E/K$の主等質空間である. よって$\xi_\sigma$が$P \in E$の取り方に依らない, すなわち$\sigma$を固定したときに得られる射

$$\phi : E \ni P \mapsto \theta^\sigma \circ \theta^{-1}(P) - P \in E$$

が定値写像であることを示す. ここで, [9, Ⅱ Prop. 6.8]からϕが全射であるかまたは定値であることからϕが全射でないこといえば十分である. 今, Step3におけるκと$[2]$がK上定義されていることと可換図式(2.4.22)から,

$$[2] = \kappa \circ \theta^{-1} = \kappa \circ \left(\theta^{-1}\right)^\sigma = \kappa \circ (\theta^\sigma)^{-1}$$

より$\kappa = [2] \circ \theta = [2] \circ \theta^\sigma$であるため, θの全単射性から$[2] = [2] \circ (\theta^\sigma \circ \theta^{-1})$となる. よって, 各$P \in E$に対し

$$[2]\left(\theta^\sigma \circ \theta^{-1}(P) - P\right) = O$$

となることから, 各 $P \in E$ に対し

$$\phi(P) = \theta^{\sigma} \circ \theta^{-1}(P) - P \in E[2] \subsetneq E \tag{2.4.26}$$

ゆえ ϕ は全射ではない. 従って, ξ_σ が P の取り方に寄らずに定まるため C_Λ は E/K の主等質空間である. □

ここで, K 上定義された楕円曲線 E/K の主等質空間 C/K の Jacobi 多様体について述べる. 次で述べる命題からそれが E/K であることがいえ, これを用いて主定理の pairing $\langle \cdot, \cdot \rangle$ を構成することとなる.

命題 2.4.27 (C/K の Jacobi 多様体). (詳細は [16, X Thm. 3.8] を参照.) C/K を E/K の主等質空間とする. このとき, $p_0 \in C$ に対して $\mathrm{Div}^0(C)$ から E への写像 sum を

$$\mathrm{sum} : \mathrm{Div}^0(C) \to E \qquad \sum_{p \in C} n_p(p) \mapsto \sum_{p \in C} [n_p](p - p_0)$$

としたとき (左の Σ は有限項からなる形式和で, 右の Σ は E 上の群の演算による和である), sum は $p_0 \in C$ の取り方に寄らず定まる. これより列

$$0 \longrightarrow \overline{K}^* \longrightarrow \overline{K}(C)^* \xrightarrow{\mathrm{div}} \mathrm{Div}^0(C) \xrightarrow{\mathrm{sum}} E \longrightarrow 0 \tag{2.4.28}$$

は群の完全列であり (div は 0 でない $f \in \overline{K}(C)^*$ に対し, f の divisor $\mathrm{div}(f)$ を対応させる写像), $\mathrm{Pic}^0(C) \cong E$ を得る. 特に $\mathrm{Pic}^0_K(C) \cong E(K)$ が成り立つ.

注 2.4.29 (Abel の定理との関連と Jacobi 多様体). 以下を注意として与える.

(1) $C = E$ であれば, $\mathrm{Im}(\mathrm{div}) = \mathrm{Ker}(\mathrm{sum})$ は本質的には Abel の定理 (定理 2.1.22) である.

(2) 一般に, 種数 1 の曲線 C/K に対して C/K が主等質空間となる K 上定義された楕円曲線 E/K が存在することが知られており, このとき上の命題から $\mathrm{Pic}^0(C) \cong E$ である. このことから代数幾何の言葉を用いればこの E/K は C/K の Jacobi 多様体であるといわれる.

例 2.4.30 (C_Λ と E/K). 例 2.4.3 で与えた楕円曲線 E/K と C_Λ において, 命題 2.4.17 から C_Λ は E/K の主等質空間であるため, 命題 2.4.27 より E/K は C_Λ の Jacobi 多様体である.

次に主定理の pairing $\langle \cdot, \cdot \rangle$ を構成のため, いくつかの記号の定義とそれらに関することを述べておくが, 命題 2.4.17 の証明で与えた記号を用いることにし, K は $\mathrm{ch}\,(K) = 0$ の完全体とする. まず, 命題 2.4.17 の Step2 から次を得る.

命題 2.4.31. $Y_0 : \{H_0 = 0\} \subset \mathbb{P}^2$ とし, $Y^{(1)} : \{H^{(1)} = 0\} \subset \mathbb{P}^2$ とすれば, $\alpha_2, \alpha_3, \alpha_4$ の与え方から $Y^{(1)}$ と Y_0 は同型であり, 下の可換図式が存在する.

$$\begin{array}{ccc} E & & \\ {\scriptstyle \alpha_1}\downarrow & & \\ C_1 & \xrightarrow{\phi^{(1)}} & Y^{(1)} \\ {\scriptstyle \alpha_4\circ\alpha_3\circ\alpha_2}\downarrow & \circlearrowright & \downarrow \\ C_\Lambda & \xrightarrow{\phi_0} & Y_0 \end{array} \tag{2.4.32}$$

(但し, $\phi^{(1)}, \phi_0$ は自明な degree 2 の K 上の射である).

例 2.4.3 で C_Λ が別の形で表すこともできることを述べたが, 次にそれからも上の命題と同様の可換図式を得ることを述べる. その前に幾つか記号を与える. 今, 各 $i(i = 1, 2, 3)$ に対し

$$H_{e_i} = H_{e_i}(U, V, W) := -\{e_i H^{(1)} - (G^{(1)} - T^2)\} \subset \mathbb{P}^2 \tag{2.4.33}$$

とおけば, e_i の取り方から

$$C_1 = \{H_{e_1} = H_{e_2} = H_{e_3} = 0\}$$

である. また変数変換 (2.4.20) により $H^{(1)} = H^{(2)}, G^{(1)} = G^{(2)}$ であることから例 2.4.3 の後半と同様にして, 各 $i(i = 1, 2, 3)$ に対し添え字を mod 3 で与えると

$$\begin{aligned} H_{e_i} &= -\{e_i H^{(2)} - (G^{(2)} - T^2)\} \\ &= -\left\{ \frac{(Z'_{i+1}/2)^2 - (Z'_{i+2}/2)^2}{e_{i+1} - e_{i+2}} + T^2 \right\} =: H'_{e_i}(Z_{i+1}, Z_{i+2}, T) \end{aligned}$$

を得る. よって, 変数変換 (2.4.20) により C_1 から $Y_{e_i} : \{H'_{e_i} = 0\} \subset \mathbb{P}^2$ への $K(e_{i+1}, e_{i+2})$ 上の射 $\phi_2^{(i)}$ を得る. また

$$H'_i(Z_{i+1}, Z_{i+2}, T) := \frac{b_{i+1} Z_{i+1}^2 - b_{i+2} Z_{i+2}^2}{e_{i+1} - e_{i+2}} + T^2 \quad (i = 1, 2, 3)$$

とし, $Y_i : \{H'_i = 0\} \subset \mathbb{P}^2$ とすれば, C_Λ から C_3 への $K(e_1, e_2, e_3)$ 上の同型射 α_4^{-1} を与える変数変換 (変数変換 (2.4.21) の逆変換) によって C_1 から Y_i への射 $\phi_2^{(i)}$ を得る. 以上より, H'_{e_i}, H'_i の与え方から変数変換

$$Z_{i+1} = \frac{Z'_{i+1}}{2\sqrt{b_{i+1}}}, \quad Z_{i+2} = \frac{Z'_{i+2}}{2\sqrt{b_{i+2}}}$$

で与えられる射 $\phi_3^{(i)}$ は Y_{e_i} から Y_i への $\overline{K}$ 上の同型射である. さらに, 後に証明する主定理の (d) の証明の Step1 から $Y_i (i = 1, 2, 3)$ に対し, ある $Q^{(i)}(R, S, T) \in K(e_i)[R, S, T]$ が存在して, $X_i : \{Q^{(i)} = 0\} \subset \mathbb{P}^2$ としたとき, 射

$$\psi_i : Y_i \ni [Z_{i+1} : Z_{i+2} : T] \mapsto \left[\frac{Z_{i+1} + Z_{i+2}}{2} : \frac{Z_{i+1} - Z_{i+2}}{2(e_{i+1} - e_{i+2})} : T \right] \in X_i \tag{2.4.34}$$

は同型射となる (主定理の (d) の証明の Step1 を参照). よって, $\phi_4^{(i)}, \psi_i$ の与え方から射の合成 $\psi_i \circ \phi_4^{(i)}$ は $\deg\left(\psi_i \circ \phi_4^{(i)}\right) = 2$ の $K(e_i)$ 上の射となる. また, $\mathbb{P}^2$ の曲線 X を

$$X : \{Q(R,S,T) := RS - T = 0\} \subset \mathbb{P}^2$$

としたとき, Y_{e_i} の与え方から Y_{e_i} から X への射

$$\psi_{e_i} : Y_{e_i} \ni [Z'_{i+1} : Z'_{i+2} : T] \mapsto \left[-\frac{Z'_{i+1} - Z'_{i+2}}{2(e_{i+1} - e_{i+2})} : \frac{Z'_{i+1} - Z'_{i+2}}{2} : T \right] \in X$$

は同型であり, E を定義する f が

$$\begin{aligned} f(x) &= (x - e_i)(x - e_{i+1})(x - e_{i+2}) \\ &= (x - e_i)(x^2 - (e_{i+1} + e_{i+2})x + e_{i+1}e_{i+2}) \\ &=: (x - e_i)(x^2 - f_i x + f'_i) \end{aligned}$$

であることと, $\phi_2^{(i)}, \psi_{e_i}$ の与え方から射の合成 $\psi_{e_i} \circ \phi_2^{(i)}$ は

$$\psi_{e_i} \circ \phi_2^{(i)} : C_1 \in [U : V : W : T] \mapsto [V - e_i U : W - f_i V + f'_i W : T] \in X$$

であり, $\deg\left(\psi_{e_i} \circ \phi_2^{(i)}\right) = 2$ の $K(e_i)$ 上の射である. 以上より次の命題を得る.

命題 2.4.35. 次の可換図式が存在する.

$$\begin{array}{ccccc} E & & & & \\ {\scriptstyle \alpha_1}\downarrow & & & & \\ C_1 & \xrightarrow{\phi_2^{(i)}} & Y_{e_i} & \xrightarrow{\psi_{e_i}} & X_{e_i} \\ {\scriptstyle \alpha_4\circ\alpha_3\circ\alpha_2}\downarrow & \circlearrowright & \downarrow{\scriptstyle \phi_3^{(i)}} & & \\ C_\Lambda & \xrightarrow[\phi_4^{(i)}]{} & Y_i & \xrightarrow[\psi_i]{} & X_i. \end{array} \tag{2.4.36}$$

上で述べた 2 つの可換図式から次の命題を述べる.

命題 2.4.37. $Y_0(K), X_i(K(e_i)) \neq \emptyset (i = 1,2,3)$ であるとし, $Q_0, Q_i (i = 1,2,3)$ をそれぞれ, Y_0 の K-有理点, X_i の $K(e_i)$-有理点とする. さらに, $D_0,\ D_i \in \mathrm{Div}(C_\Lambda) (i = 1,2,3)$ をそれぞれ, $\phi_0 : C_\Lambda \to Y_0$ による divisor (Q_0) の引き戻し, $\psi_i \circ \phi_4^{(i)} : C_\Lambda \to X_i$ による divisor (Q_i) の引き戻しとする. このとき divisor

$$2(D_i - D_0), \qquad 2(D_1 + D_2 + D_3 - 3D_0)$$

はそれぞれ, $K(e_i), K$ 上定義された principal divisor である.

証明. まず, $2(D_i - D_0)$ が $K(e_i)$ 上定義された proncipal divisor であることを示す. 始めに D_i についてみると, 射 $\psi_i \circ \phi_4^{(i)}$ が degree 2 で $K(e_i)$ 上定義されていることから D_i の与え方より, D_i は $\deg\ D_i = 2$ の $K(e_i)$ 上定義された effective divisor であり, さらに $\mathrm{sum}(D_i) = (e_i, 0)$ がいえる. なお $\mathrm{sum}(D_i) = (e_i, 0)$ については, 可換図式 (2.4.36) において, $(e_i, 0), O \in E$ に対し

$$\left(\psi_{e_i} \circ \phi_2^{(i)} \circ \alpha_1\right)(e_i, 0) = [0:1:0]$$
$$\left(\psi_{e_i} \circ \phi_2^{(i)} \circ \alpha_1\right)(O) = [0:1:0]$$

であるため, divisor $([0:1:0])$ は $\psi_{e_i} \circ \phi_2^{(i)} \circ \alpha_1$ により

$$((e_i, 0)) + (O) \in \mathrm{Div}_{K(e_i)}(E)$$

に持ち上がり, Y_i, Y_{e_i} ともに種数 0 であることから可換図式 (2.4.36) と命題 2.1.19 の (b) と命題 2.4.27 から

$$\mathrm{sum}(D_i) = (e_i, 0)$$

となるためいえる. 次に D_0 についてみると, 射 ϕ_0 が degree 2 で K 上定義されていることから D_0 の与え方より D_0 は $\deg\ D_0 = 2$ の $K(e_i)$ 上定義された effective divisor であり, さらに $\mathrm{sum}(D_0) = O$ がいえる. なお $\mathrm{sum}(D_0) = O$ については, 可換図式 (2.4.36) において $(x, y), (x, -y) \in E (y \neq 0)$ に対し

$$\phi^{(1)} \circ \alpha_1(x, y) = \phi^{(1)} \circ \alpha_1(x, -y) \tag{2.4.38}$$

であることと, $Y_0, Y^{(1)}$ ともに種数 0 であることから可換図式 (2.4.32) と命題 2.1.19 の (b) と命題 2.4.27 より

$$\mathrm{sum}(D_0) = O$$

となるためいえる. 以上より各 $i (i = 1, 2, 3)$ に対し, $2(D_i - D_0) \in \mathrm{Div}_{K(e_i)}(C_\Lambda)$ であり,

$$\mathrm{sum}(2(D_i - D_0)) = 2\mathrm{sum}(D_i) - 2\mathrm{sum}(D_0) = [2](e_i, 0) - [2]O = O$$

となる. 従って, 命題 2.4.27 と命題 2.1.19 の (c) から $2(D_i - D_0)$ は $K(e_i)$ 上定義された proncipal divisor である.

次に後者を示す. D_i, D_0 の与え方から

$$D_1 + D_2 + D_3 - 3D_0 \in \mathrm{Div}_K(C_\Lambda)$$

であり,

$$\mathrm{sum}(D_1 + D_2 + D_3 - 3D_0) = (e_1, 0) + (e_2, 0) + (e_3, 0) = 0$$

ゆえ, 再び命題 2.4.27 と命題 2.1.19 の (c) から $D_1 + D_2 + D_3 - 3D_0$ は K 上定義された proncipal divisor である. □

2.5 Selmer 群と Shafarevich-Tate 群

節 2.3 で, $E(K)$ の生成元 (または free part の rank やねじれ部分群) を求めるためには, ある $m \geq 2$ で $E(K)/mE(K)$ の生成元 (または群構造) を求めることに帰着できることを述べた. しかしながら, 一般の E/K に対して $E(K)/mE(K)$ を直接求めることも難しく (しかし, $E(K)_{\mathrm{tors}}$ だけを求めるのはそれに比べて易しい), そのため, $E(K)/mE(K)$ をこれより計算できそうな Selmer 群と呼ばれる群に埋め込んで考える. その際, Galois cohomology を用いて定義されるが, 主等質空間の言葉を用いて解釈することができる. これより Selmer 群, Shafarevich-Tate 群を定義するが, m 倍写像は K 上定義された isogeny であるため, 一般の E/K 上の K 上定義された isogeny ϕ に対して定義する. 以下, K は代数体とし, 群の準同型 $\phi : A \to B$ に対し $E[\phi] = \mathrm{Ker}(\phi)$ とする.

今, E/K, E'/K をそれぞれ K 上定義された楕円曲線, $\phi : E \to E'$ を定値ではない K 上定義された isogeny とする. このとき, 自明な $G_{\overline{K}/K}$-加群としての短完全列

$$0 \longrightarrow E[\phi] \longrightarrow E \xrightarrow{\phi} E' \longrightarrow 0 \tag{2.5.1}$$

から得られる Galois cohomology の長完全列

$$\begin{array}{c} 0 \longrightarrow E(K)[\phi] \longrightarrow E(K) \xrightarrow{\phi} E'(K) \xrightarrow{\delta} \\ H^1(K, E[\phi]) \longrightarrow H^1(K, E) \xrightarrow{\phi} H^1(K, E') \longrightarrow \cdots \end{array} \tag{2.5.2}$$

(但し, 下の ϕ は上の ϕ によって引き起こされたもので, 記号を混同して用いることにし, δ は connecting homomorphism である) を得る. また $v \in M_K$ (M_K は K の自明でない付値 v の同値類からなる集合) に対し, $K \subset K_v$ により E を K_v 上定義された楕円曲線とみれば, 短完全列 (2.5.1) と同様の $G_{\overline{K_v}/K_v}$-加群としての完全列から同様にして Galois cohomology の長完全列を得るため, 次の可換図式を得る.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E'(K)/\phi(E(K)) & \xrightarrow{\delta} & H^1(K, E[\phi]) & \xrightarrow{\iota} & H^1(K, E)[\phi] & \longrightarrow & 0 \\ & & \downarrow & \circlearrowright & \downarrow & \circlearrowright & \downarrow & & \\ 0 & \longrightarrow & \prod_{v \in M_K} E'(K_v)/\phi(E(K_v)) & \longrightarrow & \prod_{v \in M_K} H^1(K_v, E[\phi]) & \longrightarrow & \prod_{v \in M_K} H^1(K_v, E)[\phi] & \longrightarrow & 0 \end{array} \tag{2.5.3}$$

(但し, 上から下への写像のうち一番左は埋め込み $K \subset K_v$ によるものであり, その他は v の $\overline{K}$ への延長を一つ固定したときに得られる埋め込み $\lambda : \overline{K} \to \overline{K_v}$ による埋め込み $\lambda^* : G_{\overline{K_v}/K_v} \to G_{\overline{K}/K}$ によって引き起こされる制限写像である). これより以下を定義する.

定義 2.5.4 (Selmer 群と Shafarevich-Tate 群). ϕ を E/K から E'/K への isogeny

とする. このとき, E/K の ϕ-Selmer 群 $S^{(\phi)}(E/K)$ を

$$S^{(\phi)}(E/K) := \ker\left\{H^1(K, E[\phi]) \to \prod_{v\in M_K} H^1(K_v, E)[\phi]\right\} \tag{2.5.5}$$

で定義し, E/K の Shafarevich-Tate 群 $Ш(E/K)$ を

$$Ш(E/K) := \ker\left\{H^1(K, E) \to \prod_{v\in M_k} H^1(K_v, E)[\phi]\right\} \tag{2.5.6}$$

で定義する.

注 2.5.7. 以下を注意として与える.

(1) 可換図式 (2.5.3) から, $E'(K)/\phi(E(K))$ は $S^{(\phi)}(E/K)$ に埋め込まれる.

(2) 曲線 C/K が各 $v \in M_K$ で K_v-有理点をもつときいたる所局所的な有理点をもつという. このとき, Selmer 群と Shafarevich-Tate 群を主等質空間を使って解釈すると, 命題 2.4.10 から

$$H^1(K, E) \cong WC(E/K) \qquad H^1(K_v, E) \cong WC(E/K_v)$$

であることと注意 2.4.9 の (3) と可換図式 (2.5.3) から, Shafarevich-Tate 群はいたる所局所的な有理点をもつ E/K の主等質空間 C/K からなる群であり, Selmer 群は対応する E/K の主等質空間 C/K がいたる所局所的な有理点をもつような $\{\xi\} \in H^1(K, E[\phi])$ からなる群と解釈できる.

(3) 上の 2 つの定義はどちらも付値 v の $\overline{K}$ への延長のさせ方によらない. なぜなら, (2) で行った解釈において C/K のいたる所局所的な有理点の存在性は v の $\overline{K}$ への延長のさせ方によらないからである.

(4) $Ш(E/K)$ と Hasse の原理との関係を述べると, $Ш(E/K)[\phi] \neq \{0\}$ は至るところ局所的な有理点を持っているが, K-有理点を持たない主等質空間 (曲線) が存在していることを意味し (Hasse の原理が成立せず), 例えば, Selmer 曲線と呼ばれる楕円曲線

$$E/\mathbb{Q} : 3X^3 + 4X^3 + 5Z^3 = 0$$

に対して $Ш(E/\mathbb{Q})[\phi] \neq \{0\}$ である. 一方, $Ш(E/K)[\phi] = \{0\}$ はそういうものがないことを意味する (Hasse の原理が成立).

以下, $S^{(\phi)}(E/K)$ と $Ш(E/K)$ との関係とそれぞれの諸性質について述べる. ここで, $H^1(K, A)$ を Galois cohomology とし, $v \in M_K$ に対し I_v を惰性群とするとき, $\{\xi\} \in H^1(K, A)$ が制限写像

$$H^1(K, A) \to H^1(I_v, A)$$

により trivial class に対応しているならば $\{\xi\}$ は v で不分岐であるとする. また, $\{\xi\} \in H^1(K_v, A)$ に対しても同様に定義する.

命題 2.5.8. (詳細は [16, X Thm. 4.2] を参照.) $\phi : E/K \to E'/K$ を K 上定義された isogeny とする. このとき, 以下の 2 つが成り立つ.

(a) 可換図式 (2.5.3) から得られる下の列は群の完全列である.

$$0 \longrightarrow E'(K)/\phi(E(K)) \xrightarrow{\delta} S^{(\phi)}(E/K) \longrightarrow Ш(E/K)[\phi] \longrightarrow 0 \qquad (2.5.9)$$

(b) $S^{(\phi)}(E/K)$ は有限群である.

証明の方針. (a) について. 上の可換図式 (2.5.3) と $S^{(\phi)}(E/K)$ と $Ш(E/K)[\phi]$ の定義から列 (2.5.9) が完全列であることは明らかである.

(b) について. 今, M_K^∞ を無限素点からなる M_K の部分集合とし, M_K の部分集合 S を

$$\begin{aligned} S := M_k^\infty \cup \{v \in M_K \ ; \ P_v \mid \deg \phi\} \\ \cup \{v \in M_K \ ; \ E \text{ は } v \text{ で bad reduction を持つ}\} \end{aligned}$$

とすれば,

$$S^{(\phi)}(E/K) \subset H^1(K, E[\phi];\ S)$$

が成り立ち (但し,

$$H^1(K, E[\phi];\ S) := \{\{\xi\} \in H^1(K, E[\phi]) \ ; \ \{\xi\} \text{ は } S \text{ を除いたところで不分岐}\}$$

とする), 次で与える補題から $H^1(K, E[\phi];\ S)$ は有限集合であるため $S^{(\phi)}(E/K)$ もまた有限集合である. □

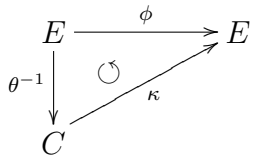
補題 2.5.10. A を有限 $G_{\overline{K}/K}$-加群とし, $S \subset M_k$ を無限素点を含む有限集合とする. このとき, $H^1(K, A;\ S)$ もまた有限集合である (但し,

$$H^1(K, A;\ S) := \{\{\xi\} \in H^1(K, A) \ ; \ \{\xi\} \text{ は } S \text{ を除いたところで不分岐}\}$$

とする).

前の節で $H^1(K, E)$ と主等質空間との対応を命題 2.4.10 で述べたが, 次に $H^1(K, E[\phi])$ と ϕ-covering との対応について述べておく.

定義 2.5.11 (ϕ-covering). 定値ではない K 上定義された isogeny $\phi : E/K \to E'/K$ に対し, 下の可換図式となる K 上定義された非特異曲線 C/K と $\overline{K}$ 上の同型射 $\theta : C \to E$ と K 上定義された射 $\kappa : C \to E$ の 3 つの pair (C, θ, κ) を E/K の ϕ-covering という.



(2.5.12)

さらに, 2 つの ϕ-covering (C, θ, κ), (C', θ', κ') に対し, $(C, \theta, \kappa) \sim (C', \theta', \kappa')$ を $P' \in E[\phi]$ と K 上の同型射 $\pi : C' \to C$ が存在して可換図式

$$\begin{array}{ccc} E & \xrightarrow{\tau_{P'}} & E \\ {\scriptstyle \theta'^{-1}}\downarrow & \circlearrowright & \downarrow{\scriptstyle \theta^{-1}} \\ C' & \xrightarrow[\pi]{} & C \end{array} \tag{2.5.13}$$

となるものとして定めれば関係 $\sim$ は同値関係であり, CV_ϕ を ϕ-covering からなる集合に対しこの同値関係で同一視した商集合をとする.

注 2.5.14. 以下を注意として与える.

(1) 例 2.4.3 および命題 2.4.17 における曲線 C_Λ, 射 $\theta : C_\Lambda \to E$, 射 $\kappa : C_\Lambda \to E$ による 3 つの pair $(C_\Lambda, \theta, \kappa)$ は, 命題 2.4.17 の証明の Step1, 2, 3 から E/K の [2]-covering である.

(2) 定義中の曲線 C/K は E/K の主等質空間である. なぜなら, 命題 2.4.17 の証明の Step4 において $(C_\Lambda, \theta, \kappa)$ が [2]-covering であることを用いて C_Λ が E/K の主等質空間であることを示していたが, これと全く同様にして示すことができるからである. 実際, $\sigma \in G_{\overline{K}/K}$ を固定したときの射

$$\psi : E \ni P \mapsto \theta^\sigma \circ \theta^{-1}(P) - P \in E[\phi]$$

が全射でない (すなわち定値写像である) ことをいえば十分であり, (C, θ, κ) が ϕ-covering であることから各 $P \in E$ に対し

$$\theta^\sigma \circ \theta^{-1}(P) - P \in E[\phi] \subsetneq E$$

がいえるため全射ではない. 従って C/K は E/K の主等質空間である.

(3) (2) と, 命題 2.4.17 の Step4 と同様の理由から写像

$$\xi_C : G_{\overline{K}/K} \ni \sigma \mapsto \theta^\sigma \circ \theta^{-1}(P) - P \in E[\phi]$$

は 1-cocycle である.

上の注の (3) は E/K の ϕ-covering (C, θ, κ) から 1-cocycle ξ_C への対応を意味するが, これにより CV_ϕ から $H^1(K, E[\phi])$ への対応を得ることができ, 次で与える命題によりその対応は全単射である.

命題 2.5.15. ([4, Lem. 13.1] を参照.) 定値ではない K 上定義された isogeny $\phi : E/K \to E'/K$ に対し, 写像

$$\mathrm{CV}_\phi \to H^1(K, E[\phi]) \qquad \{(C, \theta, \kappa)\} \mapsto \{\xi_C\}$$

は全単射である.

2.6 $S^{(\phi)}(E/K)$ の計算

前の節から $E'(K)/\phi(E(K))$ が $S^{(\phi)}(E/K)$ に埋め込まれるため, $S^{(\phi)}(E/K)$ を計算することを考える. その際, ϕ-Selmer 群の有限性の証明の方針で述べた

$$S^{(\phi)}(E/K) \subset H^1(K, E[\phi];\ S) \tag{2.6.1}$$

であることを利用する.

Step1 : まず, $H^1(K, E[\phi];\ S)$ を計算する. これについては $\phi = [m]$ かつ $E[m] \subset E(K)$ であれば, 容易に計算が可能である. なぜなら, このとき命題 2.1.26 の (b) から K は原始 m 乗根を含むため, $G_{\overline{K}/K}$-加群としての同型

$$E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}) \cong \mu_m \times \mu_m$$

を得ることと, Hilbert の定理 90 より

$$K^*/K^{*m} \ni \alpha \mapsto \beta^\sigma - \beta \in H^1(K, \mu_m) \tag{2.6.2}$$

が群の同型となることから (但し, $\beta \in \overline{K}$ は $\alpha = \beta^m$ を満たすものとして与える),

$$\begin{aligned} H^1(K, E[m];\ S) &\cong H^1(K, \mu_m \times \mu_m;\ S) \\ &\cong H^1(K, \mu_m;\ S) \times H^1(K, \mu_m;\ S) \\ &\cong K_S^*/(K_S^*)^m \times K_S^*/(K_S^*)^m \end{aligned}$$

が成り立ち (但し, K_S を K の元であって S を除いたところで可逆となる集合とする), $K_S^*/(K_S^*)^m$ を計算することに帰着するからである. なお $K = \mathbb{Q}$ とし, $m = 2$ かつ $S = \{\infty, 2, 3, 7, 11, 23\}$ とすれば

$$\mathbb{Q}_S^*/(\mathbb{Q}_S^*)^2 = \left\{ (-1)^a \cdot 2^b \cdot 3^c \cdot 7^d \cdot 11^e \cdot 23^f\ ;\ (a, b, c, d, e, f) \in \prod_{j=0}^{5} \{0, 1\} \right\} \tag{2.6.3}$$

となる.

Step2 : 今 $H^1(K, E[\phi];\ S)$ が求まったとして, 次にこの集合から $S^{(\phi)}(E/K)$ の元を見つけることを考える. よって, Selmer 群の定義から $\{\xi\} \in H^1(K, E[\phi];\ S)$ が $S^{(\phi)}(E/K)$ の元となるためには $\{\xi\}$ に対応する E/K の主等質空間 C_ξ/K が至るところ局所的な有理点をもっていなければならないが, 各 $v \in S$ で K_v-有理点をもつことがいえれば十分である (S が有限集合であることに注意する). この理由は次である. 今, $m = \deg(\phi)$ とし, $\hat{\phi}$ を ϕ の dual isogeny とする. このとき (2.6.1) より $v \notin S$ に対し $\{\xi\} \in H^1(K, E[\phi];\ S)$ は v で不分岐であり, 制限写像 $H^1(K, E) \to H^1(K_v, E)$ と $E[\phi] \subset E[m]$ によって引き起こされる写像 $H^1(K_v, E[\phi]) \to H^1(K_v, E[m])$ の合成によって対応する $\{\xi'\} \in H^1(K_v, E[m])$ もまた K_v の付値 $\tilde{v}$ で不分岐である. よって,

[4, Lem. 19.3] より $v \notin S$ に対し下の可換図式における $\mathrm{Im}(\delta'_v)$ と不分岐な元からなる $H^1(K_v, E[m])$ の部分集合が一致することと, 可換図式

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E'(K)/\phi(E(K)) & \xrightarrow{\delta} & H^1(K, E[\phi];\ S) & \longrightarrow & H^1(K,E)[\phi] & \longrightarrow & 0 \\
 & & \downarrow & \circlearrowright & \downarrow & \circlearrowright & \downarrow & & \\
0 & \longrightarrow & E'(K_v)/\phi(E(K_v)) & \xrightarrow{\delta_v} & H^1(K_v, E[\phi]) & \longrightarrow & H^1(K_v,E)[\phi] & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \hat{\phi}} & \circlearrowright & \downarrow & \circlearrowright & \downarrow & & \\
0 & \longrightarrow & E(K_v)/mE(K_v) & \xrightarrow{\delta'_v} & H^1(K_v, E[m]) & \longrightarrow & H^1(K_v,E)[m] & \longrightarrow & 0
\end{array}$$

から $\{\xi\} \in H^1(K, E[\phi];\ S)$ に対応する主等質空間 C_ξ/K が K_v-有理点をもつからである.

以上で $S^{(\phi)}(E/K)$ の判定を考えた. たとえそれが求まったとしても注 2.5.7 で述べたように必ずしも $Ш(E/\mathbb{Q})[\phi] = \{0\}$ とは限らないことから, 必ずしも

$$(E'(K)/\phi(E(K)) \cong)\ \delta(E'(K)/\phi(E(K))) = S^{(\phi)}(E/K)$$

とはならない. 従って次は $E'(K)/\phi(E(K))$ をどうやって見つけるかが問題になる. dual isogeny とそれに付随する完全列を用いた方法もあるが, 次の節では n^{th} $[m]$-descent について述べる.

2.7 n^{th} $[m]$-descent

前の項で ϕ-Selmer 群の求め方について述べた. しかし, それが求まったとしても上で述べたように一般に $E(K)/\phi(E(K))$ と一致するとは限らない. 従って ϕ-Selmer 群から始めて $E(K)/\phi(E(K))$ を含むよりより小さな群を考えていくことになる. この項では n^{th} $[m]$-descent を定義した後, これに関する話題について述べる.

今, 命題 2.5.8 の (a) から m を 2 以上の整数としたとき, 2 以上の各整数 n に対し $\phi = [m^i](i = 1, 2, \dots, n)$ とすれば直ちに下の可換図式を得る.

$$\begin{array}{ccccccccc}
E(K) & \longrightarrow & E(K)/m^nE(K) & \longrightarrow & E(K)/m^{n-1}E(K) & \longrightarrow & \cdots & \longrightarrow & E(K)/mE(K) \\
 & & \downarrow & \circlearrowright & \downarrow & \circlearrowright & & \circlearrowright & \downarrow \\
 & & S^{(m^n)}(E/K) & \xrightarrow{f_n} & S^{(m^{n-1})}(E/K) & \xrightarrow{f_{n-1}} & \cdots & \xrightarrow{f_2} & S^{(m)}(E/K)
\end{array} \tag{2.7.1}$$

(但し, 上の列における各写像は自然な全射準同型であり, $f_i(i = 2, 3, \dots, n)$ は E の 2 倍写像によって引き起こされた準同型である). これより以下を定義する.

定義 2.7.2. 上の可換図式において

$$S^{(m,n)}(E/K) := \mathrm{Im}\,(f_n \circ f_{n-1} \cdots \circ f_2) \subset S^{(m)}(E/K)$$

を求めることを n^{th} $[m]$-descent という. さらに, これより群の包含列

$$E(K)/mE(K) \subset S^{(m,n)}(E/K) \subset \cdots \subset S^{(m,2)}(E/K) \subset S^{(m,1)}(E/K) := S^{(m)}(E/K)$$

が考えられるが, この包含列から $E(K)/mE(K)$ を求めることを $[m]$-descent という.

注 2.7.3. 以下を注意として与える.

(1) ある $n \geq 1$ で $E(K)/mE(K) = S^{(m,n)}(E/K)$ となることと $m^{n-1}Ш(E/K)[m] = \{0\}$ であることは必要十分である.

(2) (1) から $Ш(E/K)$ が有限群であることがいえれば十分大きな整数 n を取ることにより $m^{n-1}Ш(E/K)[m] = \{0\}$ がいえ $S^{(m,n)}(E/K)$ が求めれば $E(K)/mE(K)$ が求めまることになる. しかしながら $Ш(E/K)$ の有限性は予想はされているが未解決問題である. よって, 十分大きな n を取ればよいことは確証されないが, $E(K)/mE(K) = S^{(m,n)}(E/K)$ となる $m, n, E/K$ は存在する (これについては章 5 を参照).

3　主定理とその証明

K を代数体 (場合によっては $\mathrm{ch}\,(K) = 0$ の完全体または局所体とする), E/K を K 上定義された楕円曲線とし, 記号簡略化のため以下 $S^{(2)} := S^{(2)}(E/K)$ とする.

3.1　主定理

前の節で n^{th} $[m]$-descent について述べたが, それをいかにして計算するかが問題になってくる. Cassels は [3] で 一般に n^{th} $[m]$-descent 上の $(n+1)^{\mathrm{th}}$ $[m]$-descent を判定する双線形な pairirng の存在性は示しているが, その際に構成された pairing は Galois cohomology を用いており, 実際の計算は困難であった. そこで, Cassels は [6] で [2]-Selmer 群上の $\mathrm{Im}(f_2)$ を判定する pairing を主等質空間を用いて構成した.

定理 3.1.1 (Cassels, [6]). 節 3.2 で構成する pairing $\langle \cdot, \cdot \rangle : S^{(2)} \times S^{(2)} \to \{\pm 1\}$ は以下の 4 つを満たす.

(a) $\langle \cdot, \cdot \rangle$ は well-defined である.

(b) $\langle \cdot, \cdot \rangle$ は双線形である.

(c) $\alpha \in S^{(2)}$ に対し, $\alpha \in \mathrm{Im}(f_2)$ となるための必要十分条件は任意の $\beta \in S^{(2)}$ に対して $\langle \alpha, \beta \rangle = 1$ となることである.

(d) $\alpha \in S^{(2)}$ に対し, $\langle \alpha, \alpha \rangle = 1$ である.

上の定理において, $S^{(2)}$, $\mathrm{Im}(f_2)$ ともに $\mathbb{F}_2$-線型空間であるが, pairing の値は ± 1 と乗法的に書くことにしていることに注意する. また, (c) の必要十分性から, $\alpha, \beta \in S^{(2)}$ に対し $\langle \alpha, \beta \rangle = -1$ となれば $\alpha, \beta \notin \mathrm{Im}(f_2)$ であり, (b), (d) より $S^{(2)}$ の相異なる 2 つの $\mathbb{F}_2$-基底の pairing の値が分かればすべての pairing の値が分かる. さらに主定理 (b), (c) より直ちに,

$$2 \mid \dim_{\mathbb{F}_2} S^{(2)} - \dim_{\mathbb{F}_2} \mathrm{Im}(f_2)$$

がいえる. これは弱 Selmer 予想といわれており別で証明されているが ([3, p. 264] を参照), その予想の別証明を与える. なお, この pairing は有名な Cassels pairing

$$Ш \times Ш \to \mathbb{Q}/\mathbb{Z}$$

の [2]-Selmer 群への引き戻しとなっている. $\langle \cdot, \cdot \rangle$ の構成の際, $S^{(2)}$, $\mathrm{Im}(f_2)$ を Galois cohomology を用いずに与え, 主等質空間と Hilbert 記号を用いて構成していることもあり計算が可能な pairing である (主定理の適用については章 5 を参照). 次の節でこの pairing $\langle \cdot, \cdot \rangle$ の構成を行う.

3.2 $S^{(2)}$ 上の pairing $\langle\cdot,\cdot\rangle$ の構成 (一般の場合)

$\mathrm{ch}\,(K) = 0$ であるため, 下の形で与えられた楕円曲線 E/K の Mordell-Weil 群 $E(K)/2E(K)$, Selmer 群 $S^{(2)}$, Shafarvich-Tate 群 $Ш(E/K)$ で議論すれば十分であり, この形の楕円曲線に対し $S^{(2)}$ 上の pairing $\langle\cdot,\cdot\rangle$ を構成する.

$$\begin{aligned} E/K : y^2 = f(x) :&= x^3 + a_2x^2 + a_4x + a_6 \quad (a_i \in K) \\ &= (x-e_1)(x-e_2)(x-e_3) \quad (e_i \in \overline{K}) \end{aligned} \tag{3.2.1}$$

(但し, $i \neq j$ ならば $e_i \neq e_j$ である). 以下, 場合によって K は $\mathrm{ch}\,(K) = 0$ の完全体または局所体とするが, どの Step においても E/K はこれで与えられた楕円曲線であるとする.

Step1 : $H^1(K, E[2])$ と同型な群を Galois cohomology を使わずに与える. なお, この Step において K は $\mathrm{ch}\,(K) = 0$ の完全体とする.

定義 3.2.2. 以下の (a), (b) を満たす $\Lambda := (b_1, b_2, b_3) \in \prod_{i=1}^3 K(e_i)^*$ からなる集合を kernel set といい, $\mathrm{KS}(E/K)$ と書く (以下, 単に KS と書くことにする).

(a) $b_1b_2b_3 \in K^{*2}$.

(b) 相異なる任意の $i, j \in \{1,2,3\}$ に対し, e_i と e_j が K 上共役ならば b_i と b_j もまた K 上共役である.

このとき次が成り立つ.

命題 3.2.3. (詳細は [4, p. 240], [2, §2], [10, Ⅳ 3, 4] を参照.) 以下の 2 つが成り立つ.

(a) KS は $\prod_{i=1}^3 K(e_i)^*$ の部分群であり, $\mathrm{KS}/\mathrm{KS}^2 \cong H^1(K, E[2])$ となる.

(b) 次で与えられる $E(K)/2E(K)$ から $\mathrm{KS}/\mathrm{KS}^2$ への写像 δ は well-defined で単射準同型となる.

$$\delta : E(K)/2E(K) \to \mathrm{KS}/\mathrm{KS}^2$$

$$\delta(P=(x_0,y_0)) := \begin{cases} (1,1,1) & (P = O \text{ のとき}) \\ ((e_1-e_3)(e_1-e_2),\ e_1-e_2,\ e_1-e_3) & (P = (e_1,0) \text{ のとき}) \\ (e_2-e_1,\ (e_2-e_3)(e_2-e_1),\ e_2-e_3) & (P = (e_2,0) \text{ のとき}) \\ (e_3-e_1,\ e_3-e_2,\ (e_3-e_2)(e_3-e_1)) & (P = (e_3,0) \text{ のとき}) \\ (x_0-e_1,\ x_0-e_2,\ x_0-e_3) & (\text{それ以外のとき}). \end{cases} \tag{3.2.4}$$

Step2 : $S^{(2)}$ と同型な群を Galois cohomology を使わずに与える. なお, この Step において K は代数体とする.

定義 3.2.5 ($S^{(2)}$ の再構成). $\Lambda = (b_1, b_2, b_3) \in \mathrm{KS}$ に対して, C_Λ を

$$Z_i = Z_i(U_1, U_2, U_3) := U_1 + U_2 e_i + U_3 e_i^2 \quad (i = 1, 2, 3)$$

としたときの,

$$C_\Lambda : \left\{ H_i(U_1, U_2, U_3, T) := \frac{b_{i+1} Z_{i+1}^2 - b_{i+2} Z_{i+2}^2}{e_{i+1} - e_{i+2}} + T^2 = 0 \ ; \ i = 1, 2, 3 \right\} \tag{3.2.6}$$

で与えられる $\mathbb{P}^3$ の 3 つ 2 次曲面の intersection とする (但し, 添え字は mod 3 で与える). このとき, 例 2.4.3 と命題 2.4.17 から C_Λ は E/K の主等質空間であり, 集合 $\mathrm{FD}(E/K)$(以下, 単に FD と書くことにする) を

$$\mathrm{FD}(E/K) := \{\Lambda \in \mathrm{KS} \ ; \ \text{各 } v \in M_K \text{ に対し, } C_\Lambda(K_v) \neq \emptyset\}$$

とする.

注 3.2.7. C_Λ で 2 次曲面を考える主な理由は Hasse-Minkovski の定理 (定理 1.0.8) が使えることと種数が 0 となることが挙げられる .

定義と命題 3.2.3 から次を得る.

命題 3.2.8. FD は KS の部分群かつ $\mathrm{KS}^2 \subset \mathrm{FD}$ であり, $\mathrm{FD}/\mathrm{KS}^2 \cong S^{(2)}$ となる. さらに, 命題 3.2.3 の (b) における単射準同型 δ に対し $\mathrm{Im}(\delta) \subset \mathrm{FD}/\mathrm{KS}^2$ である.

Step3 : pairing $\langle \cdot, \cdot \rangle$ の構成に用いる local pairing $[\cdot, \cdot]$ を定義するが, この pairing には Hilbert 記号を用いる. なお, この Step では K を局所体 ($\mathbb{R}, \mathbb{C}$ も含める) とし, Step1 で与えた群 KS は $\mathrm{ch}\,(K) = 0$ の完全体 K に対して定義されているため, 当然 $\mathrm{ch}\,(K) = 0$ の局所体 K 上でも与えられ, $\mathrm{KS}/\mathrm{KS}^2 \times \mathrm{KS}/\mathrm{KS}^2$ 上の pairing $[\cdot, \cdot]$ を以下ようにして定める.

定義 3.2.9 (local pairing). K を局所体とし, E/K を (3.2.1) の形で与えられた楕円曲線とする. また, $(\cdot, \cdot)_{K(e_i)}$ を Hilbert 記号とし, 添え字集合 $I = \{1, 2, 3\}$ において $i, j \in I$ に対し, $i \sim j$ を e_i と e_j が K 上共役として定めれば関係 $\sim$ は同値関係であり, これによる I の商集合を $\mathfrak{I}$ とする. このとき, $\Lambda = (b_1, b_2, b_3), M = (c_1, c_2, c_3) \in \mathrm{KS}$ に対して pairing $[\Lambda, M]$ を

$$[\Lambda, M] = \prod_{\{i\} \in \mathfrak{I}_K} (b_i, c_i)_{K(e_i)} \tag{3.2.10}$$

で与えれば, これは KS の定め方と Hilbert 記号の定義から $\mathfrak{I}_K$ の代表元の取り方に依らず定まる. また, Hilbert 記号の性質から明らかにこの pairing $[\cdot, \cdot]$ は $\mathrm{KS}/\mathrm{KS}^2 \times \mathrm{KS}/\mathrm{KS}^2$ から $\{\pm 1\}$ への双線形な pairing を引き起こす. この pairing を local pairing といい, 断りがなければ $[\cdot, \cdot]$ で書くことにする.

これより $[\Lambda, M]$ は, 例えば各 $i \in I$ に対し $e_i \in K$ であれば

$$[\Lambda, M] = (b_1, c_1)_K (b_2, c_2)_K (b_3, c_3)_K$$

であり, $e_1 \in K$ かつ $e_2, e_3 \notin K$ であれば

$$[\Lambda, M] = (b_1, c_1)_K (b_2, c_2)_{K(e_2)} = (b_1, c_1)_K (b_3, c_3)_{K(e_3)}$$

であり, 各 $i \in I$ に対し $e_i \notin K$ であれば

$$[\Lambda, M] = (b_1, c_1)_{K(e_1)} = (b_2, c_2)_{K(e_2)} = (b_3, c_3)_{K(e_3)}$$

である. なお, local pairing $[\cdot, \cdot]$ は後で与える命題 3.3.14 から非退化である.

Step4 : Step3 で与えた local pairing $[\cdot, \cdot]$ を用いて FD/KS^2 上の pairing $\langle \cdot, \cdot \rangle$ を構成する. なお, この Step においては K を代数体とし, C_Λ は (3.2.6) または (2.4.5) で与えられているとし, 記号は命題 2.4.17 または命題 2.4.37 の周辺で与えられたものを使う. まず始めに, pairing を構成する際に必要な $\Lambda \in \mathrm{FD}$ に対する $L_0, L_i (i = 1, 2, 3)$ の取り方を与える. 今, $\Lambda \in \mathrm{FD}$ に対し FD の与え方から各 $v \in M_K$ に対し $C_\Lambda(K_v) \neq \emptyset$ であり, 命題 2.4.31 および命題 2.4.35 における 2 つの射

$$\phi_0 : C_\Lambda \to Y_0, \qquad \psi_i \circ \phi_4^{(i)} : C_\Lambda \to X_i$$

がそれぞれ $K, K(e_i)$ 上定義されていることから, 各 $v \in M_K$ に対し $Y_0(K_v) \neq \emptyset$, $X_i(K_v(e_i)) \neq \emptyset$ である. よって, $Y_0 \subset \mathbb{P}^2, X_i \subset \mathbb{P}^2$ が $K, K(e_i)$ 上定義された 2 次曲線であることから Hasse-Minkovski の定理 (定理 1.0.8) より Y_0, X_i はそれぞれ $K, K(e_i)$-有理点を持ち, しかもともに種数 0 ゆえ, それぞれ無限個の $K, K(e_i)$-有理点をもつ. これより, $Q_0, Q_i (i = 1, 2, 3)$ をそれぞれ Y_0 の K-有理点, X_i の $K(e_i)$-有理点として取る. このとき, 1 次形式 $L_0 \in K[U_1, U_2, U_3, T], L_i \in K(e_i)[U_1, U_2, U_3, T] (i = 1, 2, 3)$ をそれぞれ, Q_0 における Y_0 の接線を与える 1 次形式を射 $\phi_0 : C_\Lambda \to Y_0$ によって引き戻したもの, Q_i における X_i の接線を与える 1 次形式を射 $\psi_i \circ \phi_4^{(i)} : C_\Lambda \to X_i$ によって引き戻したものとして取る. 以上で L_0, L_i の取り方を述べたが, 場合によっては L_0 を以下のようにして取り直す. 今, $D_0,\ D_i \in \mathrm{Div}(C_\Lambda)$ をそれぞれ, $\phi_0 : C_\Lambda \to Y_0$ による divisor (Q_0) の引き戻し, $\psi_i \circ \phi_4^{(i)} : C_\Lambda \to X_i$ による divisor (Q_i) の引き戻しとすれば, それぞれ K, $K(e_i)$ 上定義された effective divisor であり, L_0, L_i, D_0, D_i の取り方から

$$\mathrm{div}\left(\frac{L_i}{L_0}\right) = 2(D_i - D_0)$$

となる. よって

$$\mathrm{div}\left(\prod_{i=1}^{3} \frac{L_i}{L_0}\right) = 2(D_1 + D_2 + D_3 - 3D_0)$$

であり, $D_1+D_2+D_3-3D_0$ は K 上定義されているが, 命題 2.4.37 より

$$\mathrm{div}(W)=D_1+D_2+D_3-3D_0$$

となる $W\in K(C_\Lambda)$ が存在するため,

$$\mathrm{div}\left(\prod_{i=1}^{3}\frac{L_i}{L_0}\right)=2\ \mathrm{div}(W)$$

となる. よって, C_Λ 上の関数として

$$\prod_{i=1}^{3}\frac{L_i}{L_0}=aW^2$$

となる $a\in K^*$ が存在するが, $a=1$ でなければ aL_0 を L_0 として取り直す. 従って $a^{-1}W$ を W として取り直せば上の左辺は W^2 に等しい. 以上より, 各 $v\in M_K$ に対し, KS_v を K_v に対して与えられる kernel set とし, $\phi_0(Q_v)\neq Q_0$ かつ $\psi_i\circ\phi_4^{(i)}(Q_v)\neq Q_i(i=1,2,3)$ となる C_Λ 上の K_v-有理点 Q_v を取れば

$$\mathfrak{J}_v(\Lambda):=\left\{\frac{L_1}{L_0}(Q_v),\frac{L_2}{L_0}(Q_v),\frac{L_3}{L_0}(Q_v)\right\}\in\mathrm{KS}_v \tag{3.2.11}$$

となる. よって, $\Lambda\in\mathrm{FD}$ に対するこの $\mathfrak{J}_v(\Lambda)$ を用いての pairing $\langle\cdot,\cdot\rangle$ を構成する. 実際, 次で与える pairing $\langle\cdot,\cdot\rangle$ が主定理を満たす.

定義 3.2.12 ($\langle\cdot,\cdot\rangle$ の構成). K を代数体とし, E/K を (3.2.1) の形で与えられた楕円曲線とする. このとき $\mathrm{FD}/\mathrm{KS}^2$ 上の pairing $\langle\cdot,\cdot\rangle$ を次で与える. $\alpha=\{\Lambda\},\beta\in\mathrm{FD}/\mathrm{KS}^2$ に対し, $\mathfrak{J}_v(\Lambda)$ を (3.2.11) で与えたものとしたとき

$$\langle\alpha,\beta\rangle=\prod_{v\in M_K}[\{\mathfrak{J}_v(\Lambda)\},\beta]_v$$

とする.

以上で pairing $\langle\cdot,\cdot\rangle$ を定義したが, それを定義する際に用いた $Q_i,L_i(i=0,1,2,3)$ の取り方に依らないことは節 3.4 で示す. また, paring $\langle\cdot,\cdot\rangle$ の構成の際に L_0,L_1 を使うのはこれで $\mathrm{Im}(f_2)$ と同型な $\mathrm{FD}/\mathrm{KS}^2$ の部分群 (後でこれを $\mathrm{SD}/\mathrm{KS}^2$ として与える) を定式化することができるからであり (補題 3.3.3 を参照), この pairing $\langle\cdot,\cdot\rangle$ が $\mathrm{Im}(f_2)$ を判定することとなる.

3.3 主定理の証明に使う補題の証明

主定理を証明する前に幾つか補題を示す. まず始めに $\mathrm{Im}(f_2)$ と同型な $\mathrm{FD}/\mathrm{KS}^2$ の部分群な群を考える.

定義 3.3.1 (SD). $\Lambda \in \mathrm{FD}$ に対して, L_i, L_0 を節 3.2 の Step4 の方法で取ってきたものとする. このとき, ある $\Lambda' := (\alpha_1, \alpha_2, \alpha_3) \in \mathrm{KS}$ が存在して, 各 v に対し

$$\alpha_i \cdot \frac{L_i}{L_0}(Q_v) \in \{K_v(e_i)\}^2 \quad (i = 1, 2, 3) \tag{3.3.2}$$

満たす C_Λ の K_v-有理点 Q_v が存在する $\Lambda \in \mathrm{FD}$ 全体からなる集合を SD とする.

補題 3.3.3 ($\mathrm{Im}(f_2)$ の定式化). 上で定めた集合 SD は KS^2 を含む FD の部分群であり, $\mathrm{SD}/\mathrm{KS}^2 \cong \mathrm{Im}(f_2)$ が成り立つ.

証明. [3, p. 274] から $\Lambda \in \mathrm{FD}$ に対して $\Lambda \in \mathrm{SD}$ となることと, $\Lambda \in \mathrm{FD}$ に対する [2]-covering $(C_\Lambda, \theta, \kappa)$ に対し, 可換図式

$$\begin{array}{ccccc} E & \xrightarrow{[2]} & E & \xrightarrow{[2]} & E \\ {\scriptstyle \theta'^{-1}}\downarrow & \circlearrowright & {\scriptstyle \theta^{-1}}\downarrow & \circlearrowright & \nearrow {\scriptstyle \kappa} \\ C' & \xrightarrow[\kappa']{} & C_\Lambda & & \end{array} \tag{3.3.4}$$

となる, 各 $v \in M_K$ で K_v-有理点をもつ K 上定義された曲線 C' と $\overline{K}$ 上の同型射 θ' と K 上定義された射 κ が存在する (つまり $(C', \theta, \kappa \circ \kappa')$ は [4]-covering である) ことが必要十分であることをいえばよい. 必要性は SD の与え方と [3, Lem. 4.1] からいえる. 次に十分性を示す. $\Lambda \in \mathrm{FD}$ に対し, 可換図式 (3.3.4) となる各 $v \in M_K$ で K_v-有理点をもつ K 上定義された曲線 C' と $\overline{K}$ 上の同型射 θ' と K 上定義された射 κ が存在するとする. このとき, 上の可換図式 (3.3.4) によって引き起こされる divisor の引き戻しの可換図式

$$\begin{array}{ccc} \mathrm{Div}(E) & \xleftarrow{[2]^*} & \mathrm{Div}(E) \\ {\scriptstyle (\theta'^{-1})^*}\uparrow & \circlearrowleft & {\scriptstyle (\theta^{-1})^*}\uparrow \\ \mathrm{Div}(C') & \xleftarrow[(\kappa')^*]{} & \mathrm{Div}(C_\Lambda) \end{array} \tag{3.3.5}$$

を得る. これより, 各 $i (i = 1, 2, 3)$ に対し

$$(\kappa')^* \left(\mathrm{div}(L_i/L_0)\right) = 2\ \mathrm{div}(W_i) \tag{3.3.6}$$

となる $W_i \in K(e_i)(C')$ が存在すれば, 命題 2.1.19 の (c) から $\alpha_i \cdot (\kappa')^*(L_i/L_0) = W_i^2$ となる $\alpha_i \in K(e_i)^*$ が存在し, 各 $v \in M_K$ に対し, うまく C' 上の K_v-有理点 Q'_v を取ることによって

$$\alpha_i \cdot \frac{L_i}{L_0}(\kappa(Q'_v)) = \{W_i(Q'_v)\}^2 \in (K(e_i)^*)^2 \quad (i = 1, 2, 3)$$

が成り立つ. よって, κ' が K 上定義されているため各 $v \in M_K$ に対し $\kappa'(Q'_v) \in C_\Lambda(K_v)$ であることから, $\Lambda \in \mathrm{SD}$ となり十分性が成り立つ. 従って, 各 $i(i=1,2,3)$ に対し (3.3.6) となる $W_i \in K(e_i)(C')$ が存在することを示す. ここで, 節 3.2 の Step4 より

$$\mathrm{div}\left(\frac{L_i}{L_0}\right) = 2(D_i - D_0) \in \mathrm{Div}_{K(e_i)}(C_\Lambda)$$

であることと, κ' が K 上定義されていることから $(\kappa')^*(D_i - D_0)$ は $K(e_i)$ 上定義されており, これが principal divisor であることを示せばよい. 今, L_i, L_0 の取り方から $(\theta^{-1})^*\big(\mathrm{div}(L_i/L_0)\big)$ と $\mathrm{div}(x - e_i)$ が線形同値であるため, $(\theta^{-1})^*\big((D_i - D_0)\big)$ と $(((e_i,0)) - (O))$ は線形同値である. さらに $[2]^*\,(((e_i,0)) - (O))$ が principal divisor であるため $(\theta^{-1} \circ [2])^*(D_i - D_0)$ は principal divisor となり, 可換図式 (3.3.5) と θ' が同型射であることから $(\kappa')^*(D_i - D_0)$ は principal divisor となる. 従って (3.3.2) が成り立ち, 十分性がいえる. 以上より $\mathrm{SD}/\mathrm{KS}^2 \cong \mathrm{Im}(f_2)$ である. □

次に pairing $\langle \cdot, \cdot \rangle$ が well-defined であることと双線形性を示すために幾つか補題を示す. その前に $\Lambda MN \in \mathrm{KS}^2$ を満たす $\Lambda = (b_1, b_2, b_3), M = (c_1, c_2, c_3), N = (d_1, d_2, d_3) \in \mathrm{KS}$ に対し, 以下のようにして K 上定義された射

$$\mu : C_\Lambda \times C_M \to C_N \tag{3.3.7}$$

を与える. 以下 K は完全体とする. 今, 生成点 $p_1 \in C_\Lambda, p_2 \in C_M$ に対し可換図式 (2.4.22) から

$$[z_1 : z_2 : z_3 : 1] := \alpha_{4,\Lambda}^{-1}(p_1), \quad [w_1 : w_2 : w_3 : 1] := \alpha_{4,M}^{-1}(p_2)$$

とし, それぞれ $b_1b_2b_3 = b^2$, $c_1c_2c_3 = c^2$ となる $b, c \in K$ に対し

$$\begin{aligned}(X_\Lambda, Y_\Lambda) &:= [2] \circ \theta_\Lambda(p_1) = \big(e_1 + b_1 z_1^2, b z_1 z_2 z_3\big)\\ (X_M, Y_M) &:= [2] \circ \theta_M(p_2) = \big(e_1 + c_1 w_1^2, c w_1 w_2 w_3\big)\end{aligned}$$

とする. このとき, (X_Λ, Y_Λ) と (X_M, Y_M) を通る直線を $y = A(x - X_\Lambda) + Y_\Lambda$ とし, $P = (X', Y')$ をその直線と E との第 3 交点とすれば

$$(x-e_1)(x-e_2)(x-e_3) - \{A(x - X_\Lambda) + Y_\Lambda\}^2 = (x - X_\Lambda)(x - X_M)(x - X') \tag{3.3.8}$$

が成り立つ. よって, 両辺に $x = e_i (i = 1, 2, 3)$ を代入すれば

$$-\{A(e_i - X_\Lambda) + Y_\Lambda\}^2 = (e_i - X_\Lambda)(e_i - X_M)(e_i - X') = (-b_i z_i^2)(-c_i w_i^2)(e_i - X')$$

ゆえ,

$$X' - e_i = (b_i c_i)^{-1} \left[z_i^{-1} w_i^{-1} \{ A(e_i - X_\Lambda) + Y_\Lambda \} \right]^2$$

となる. ここで, X_Λ, X_M の与え方から添え字を mod 3 で考えると

$$\begin{aligned}
A(e_i - X_\Lambda) + Y_\Lambda &= \frac{Y_\Lambda - Y_M}{X_\Lambda - X_M}(e_i - X_\Lambda) + Y_\Lambda \\
&= \frac{bz_i z_{i+1} z_{i+3} - cw_i w_{i+1} w_{i+2}}{X_\Lambda - X_M}(e_i - X_\Lambda) + bz_i z_{i+1} z_{i+3} \\
&= \frac{(bz_i z_{i+1} z_{i+3} - cw_i w_{i+1} w_{i+2})(e_i - X_\Lambda)}{X_\Lambda - X_M} \\
&\quad + \frac{(bz_i z_{i+1} z_{i+3})\big\{(X_\Lambda - e_i) - (X_M - e_i)\big\}}{X_\Lambda - X_M} \\
&= \frac{-cw_i w_{i+1} w_{i+2}(e_i - X_\Lambda) - bz_i z_{i+1} z_{i+2}(X_M - e_i)}{X_\Lambda - X_M} \\
&= \frac{cb_i z_i^2 w_{i+1} w_{i+2} - bc_i w_i^2 z_{i+1} z_{i+2}}{X_\Lambda - X_M}
\end{aligned}$$

であり, Λ, M, N の取り方から $b_i c_i d_i = A_i^2$ となる $A_i \in K(e_i)^*$ が存在するため (取り方から, $\{A_1^2, A_2^2, A_3^2\} \in \mathrm{KS}$ である),

$$\begin{aligned}
X' - e_i &= (b_i c_i)^{-1} \left[z_i^{-1} w_i^{-1} \{ A(e_i - X_\Lambda) + Y_\Lambda \} \right]^2 \\
&= d_i (A_i)^{-2} \left(\frac{cb_i z_i w_{i+1} w_{i+2} - bc_i w_i z_{i+1} z_{i+3}}{X_\Lambda - X_M} \right)^2
\end{aligned}$$

となる. 従って, $b_i, c_i, z_i, w_i, X_\Lambda, X_M, A_i$ の記号の与え方と $K(e_i, p_1, p_2)/K(p_1, p_2)$ が高々3 次の拡大であることから

$$Z_i := \frac{cb_i z_i w_{i+1} w_{i+2} - bc_i w_i z_{i+1} z_{i+3}}{A_i^2 (X_\Lambda - X_M)}$$

としたとき, $Z_i = u_1 + u_2 e_i + u_3 e_i^2$ となりかつ u_j(j=1,2,3) が i に依らないように $u_j \in K(p_1, p_2)$ を取ることができる. よって, u_j の与え方から $[u_1 : u_2 : u_3 : 1] \in C_N$ より K 上定義された射 μ

$$\mu : C_\Lambda \times C_M \ni (p_1, p_2) \mapsto [u_1 : u_2 : u_3 : 1] \in C_N \tag{3.3.9}$$

を得る. 以上により K 上定義された射を与えたが, 実はこれにより C_Λ が E/K の主等質空間であることの別証明を与えることもできる. 実際, $\Lambda = \Lambda, M = (1,1,1), N = \Lambda$ のときの射 μ が主等質空間の定義 2.4.1 の (a), (b), (c) を満たす. ここでは証明しないがこれを用いて次を示す.

補題 3.3.10. 以下の 2 つが成り立つ.

(a) $\Lambda^{(1)}\Lambda^{(2)}\Lambda^{(3)} \in \mathrm{KS}^2$ を満たす $\Lambda^{(r)} \in \mathrm{FD}(r=1,2,3)$ に対し, 生成点 $p^{(1)} \in C_{\Lambda^{(1)}}$, $p^{(2)} \in C_{\Lambda^{(2)}}$ が射 (3.3.9) によって $p^{(3)} \in C_{\Lambda^{(3)}}$ に対応しているとする. このとき, 各 i(i=1,2,3) に対し

$$\prod_{r=1}^{3} \frac{L_i^{(r)}}{L_0^{(r)}}(p^{(r)}) \in K(e_i)^* \left\{K\big(e_i, p^{(1)}, p^{(2)}, p^{(3)}\big)^*\right\}^2$$

を満たす.

(b) $\Lambda \in \mathrm{FD}$ とし, 生成点 $p \in C_\Lambda$,$P=(x,y) \in E$ とする. このとき, 各 i(i=1,2,3) に対し

$$\frac{(L_i/L_0)(p+P)}{(x-e_i)\cdot(L_i/L_0)(p)} \in \{K(e_i,p,P)^*\}^2$$

となる.

証明. (a) を示す. $\overline{K}$ 上の同型射 $\theta^{(r)} : C_{\Lambda^{(r)}} \to E$ に対し, $Q^{(r)} := \theta^{(r)}(p^{(r)})(r=1,2,3) \in E$ とする. 射 (3.3.9) を与える際の Z_i の置き方として場合によっては $-Z_i$ を Z_i と置き換えることによって

$$Q^{(1)} + Q^{(2)} + Q^{(3)} = O$$

とすることができる. これは 3 点 $Q^{(r)}(r=1,2,3)$ がある直線

$$y = Ax + B \left(A, B \in \overline{K}\big(p^{(1)}, p^{(2)}, p^{(3)}\big)\right)$$

上にあることを意味し, (3.3.8) の周辺と同様の議論から $(X^{(r)}, Y^{(r)}) := Q^{(r)}$ とすれば各 $i(i=1,2,3)$ に対し

$$-\prod_{r=1}^{3}(X^{(r)} - e_i) = (Ae_i - B)^2 \in \left\{\overline{K}(p^{(1)}, p^{(2)}, p^{(3)})^*\right\}^2 \tag{3.3.11}$$

となる. ここで, $x - e_i \in K(e_i)(E)$ に対して $\mathrm{div}(x-e_i) = 2(((e_i,0)) - (O))$ であることと, $X^{(r)}$ の与え方から

$$\begin{aligned}
\mathrm{div}(X^{(r)} - e_i) &= \mathrm{div}\Big(\big(\theta^{(r)}\big)^*(x-e_i)\Big) \\
&= \big(\theta^{(r)}\big)^*(\mathrm{div}(x-e_i)) \\
&= \big(\theta^{(r)}\big)^*\Big(2\big(((e_i,0)) - (O)\big)\Big) \\
&= 2\big(\theta^{(r)}\big)^*\big(((e_i,0)) - (O)\big) \in \mathrm{Div}\big(C_{\Lambda^{(r)}}\big)
\end{aligned}$$

であり, 節 3.2 の Step4 から

$$\mathrm{div}\left(\frac{L_i^{(r)}}{L_0^{(r)}}\right) = 2\big(D_i^{(r)} - D_0^{(r)}\big) \in \mathrm{Div}\big(C_{\Lambda^{(r)}}\big)$$

であるため, 各 r(r=1,2,3) に対し

$$\mathrm{div}\left(\frac{(L_i^{(r)}/L_0^{(r)})\big(p^{(r)}\big)}{X^{(r)}-e_i}\right)=2\left(\big(\theta^{(r)}\big)^*\big(((e_i,0))-(O)\big)-D_i^{(r)}+D_0^{(r)}\right)$$

となる. よって, 上の右辺を $2\mathfrak{D}_i^{(r)}\in \mathrm{Div}\big(C_{\Lambda^{(r)}}\big)$ とすれば, $\theta^{(r)}$ が同型射であることと $\mathfrak{D}_i^{(r)}$ の与え方から, $\deg\,\mathfrak{D}_i^{(r)}=0$ でありかつ $\mathrm{sum}(\mathfrak{D}_i^{(r)})=O$ である. 従って, 補題 2.4.27 と命題 2.1.19 の (c) から $\mathrm{div}(g_i^{(r)})=\mathfrak{D}_i^{(r)}$ となる $g_i^{(r)}\in\overline{K}\big(C_{\Lambda^{(r)}}\big)$ が存在する. よって, 各 r(r=1,2,3) に対し

$$\frac{(L_i^{(r)}/L_0^{(r)})\big(p^{(r)}\big)}{X^{(r)}-e_i}\in\overline{K}^*\left\{\overline{K}(e_i,p^{(1)},p^{(2)},p^{(3)})^*\right\}^2$$

となるため, (3.3.11) より

$$\prod_{r=1}^{3}\frac{L_i^{(r)}}{L_0^{(r)}}\big(p^{(r)}\big)\in\overline{K}^*\left\{\overline{K}\big(e_i,p^{(1)},p^{(2)},p^{(3)}\big)^*\right\}^2$$

が成り立つ. 従って, $L_i^{(r)}/L_0^{(r)}\big(p^{(r)}\big)\in K(e_i)(p^{(r)})$ であり, $K(e_i)\cap\overline{K}=K(e_i)$ ゆえ,

$$\prod_{r=1}^{3}\frac{L_i^{(r)}}{L_0^{(r)}}\big(p^{(r)}\big)\in K(e_i)^*\left\{K\big(e_i,p^{(1)},p^{(2)},p^{(3)}\big)^*\right\}^2$$

となり, (a) が成り立つ.

(b) を示す. (a) より $\Lambda^{(1)}=\Lambda^{(3)}=\Lambda$, $\Lambda^{(2)}=C_{(1,1,1,)}$ とすれば $C_{(1,1,1)}$ と E が K 上同型であることとこの補題のすぐ上で述べたことから

$$\frac{(L_i/L_0)(p+P)}{(x-e_i)\cdot(L_i/L_0)(p)}\in K(e_i)^*\left\{K(e_i,p,P)^*\right\}^2$$

を得る. ここで特殊化 $P\to O$ により $(x-e_i)(x/y)^2\to 1$ となることから特殊化 $P\to O$ により

$$\frac{(L_i/L_0)(p+P)}{(x-e_i)(x/y)^2\cdot(L_i/L_0)(p)}\to 1$$

であるため

$$\frac{(L_i/L_0)(p+P)}{(x-e_i)\cdot(x/y)^2\cdot(L_i/L_0)(p)}\in\left\{K(e_i,p,P)^*\right\}^2$$

がいえる. 従って

$$\frac{(L_i/L_0)(p+P)}{(x-e_i)\cdot(L_i/L_0)(p)}\in\left\{K(e_i,p,P)^*\right\}^2$$

となり, (b) が成り立つ. □

次に KS の構造について見る.

命題 3.3.12 (KS/KS^2 の構造). K を $\mathrm{ch}\,(K) \neq 0$ の完全体とする. このとき, KS/KS^2 は (3.2.1) における f の K 上の分解の仕方によって以下のようになる.

(a) f が K で (3つの)1次因子の積に分解されるとき KS/KS^2 は $K^*/(K^*)^2 \times K^*/(K^*)^2$ に同型である.

(b) f が 1 根のみ K の元であるとき, K の元ではない f の根 e_i に対して $K_1 := K(e_i)$ としたとき KS/KS^2 は $K_1^*/(K_1^*)^2$ に同型である.

(c) f が K_v 上既約であるとき, f の根 e_i に対し $K_2 := K(e_i)$ としたとき KS/KS^2 は $K_2^*/\{K^*(K_2^*)^2\}$ に同型である.

証明. (a) を示す. このとき, KS が $\prod_{i=1}^3 K^*$ の部分群であることから写像

$$\mathrm{KS}/\mathrm{KS}^2 \ni \{(b_1, b_2, b_3)\} \mapsto (\{b_2\}, \{b_3\}) \in K^*/(K^*)^2 \times K^*/(K^*)^2$$

は well-defined でありかつ群の準同型である. さらに, この写像の全単射性は KS の定め方から明らかゆえ, (a) が成り立つ.

(b) を示す. このとき, 場合によっては添え字を入れ変えて $e_1 \in K$ かつ $e_2, e_3 \notin K$(e_2 と e_3 は K 上共役である) としてよく, $K_1 = K(e_2) = K(e_3)$ である. まず, (a) の前半と同様にして, 写像

$$\mathrm{KS}/\mathrm{KS}^2 \ni \{(b_1, b_2, b_3)\} \mapsto \{b_2\} \in K_1^*/(K_1^*)^2$$

は well-defined でありかつ群の準同型である. よってこの写像が全単射であることを示せばよい. まず, 単射性は上の写像において KS の与え方から b_2 と b_3 が K 上共役であることと $b_1b_2b_3 \in (K^*)^2$ より明らか. 次に全射性を示す. $\{\beta\} \in K_1^*/(K_1^*)^2$ に対し $\beta \in K_1$ の共役元を β' とすれば K_1/K が 2 次拡大より $\beta\beta' = \mathrm{N}_{K_1/K}(\beta) \in K^*$ ゆえ, $\alpha\beta\beta' = (K^*)^2$ となる $\alpha \in K$ を取ってくれば KS の与え方から $(\alpha, \beta, \beta') \in \mathrm{KS}$ となる. よって, 上の写像によりこれを代表元とする元が $\{\beta\}$ に対応し, 全射性がいえる. 以上より (b) が成り立つ.

(c) を示す. 今, e_1, e_2, e_3 は K 上共役であるため $K_2 = K(e_1)$ としてよく, 共役写像 $\sigma_2 : K(e_1) \to K(e_2)$, $\sigma_3 : K(e_1) \to K(e_2)$ と $\beta_1 \in K_2^*$ に対し $\beta_2 := \sigma_2(\beta_1)$, $\beta_3 := \sigma_3(\beta_1)$ とする. このとき, K_1/K は 3 次の分離拡大より

$$\beta_1\beta_2\beta_3 = \mathrm{N}_{K_2/K}(\beta_1) \in K^*$$

であるため, 次の群の準同型

$$\phi : (K_1)^* \ni \beta_1 \mapsto \{(\beta_2\beta_3, \beta_3\beta_1, \beta_1\beta_2)\} \in \mathrm{KS}/\mathrm{KS}^2$$

を得る. よって, これが全射かつ $\ker(\phi) = K^*(K_2^*)^2$ をいえばよい. まず全射性を示す. $(b_1, b_2, b_3) \in \mathrm{KS}$ に対し, KS の与え方から $b_1b_2b_3 \in (K^*)^2$ ゆえ, 各 $i (i = 1, 2, 3)$ に

対し $b_i(b_{i+1}b_{i+2})^{-1} \in (K(e_i)^*)^2$ となることと, 再び KS の与え方と σ_2, σ_3 の与え方から $\sigma_2(b_1) = b_2, \sigma_3(b_1) = b_3$ であるため

$$\phi(b_1) = \{(b_2b_3, b_3b_1, b_1b_2)\} = \{(b_1, b_2, b_3)\} \tag{3.3.13}$$

となり全射性がいえる. 次に $\ker(\phi) = K^*(K_2^*)^2$ を示すが, 写像 ϕ の与え方から明らかに $\ker(\phi) \supset K^*(K_2^*)^2$ がいえるため $\ker(\phi) \subset K^*(K_2^*)^2$ を示す. ここで, f の最小分解体を K' としたとき Galois 理論から K' は 3 次の巡回拡大体であるかまたは Galois 群が $\mathfrak{S}_3$ と同型になる 6 次の拡大体であることからこの 2 つで場合分けをして示す.

(i) 前者のとき,

$$K' = K(e_1) = K(e_2) = K(e_3) = K_2$$

であり, $\mathrm{Gal}(K'/K)$ の生成元 σ として

$$\sigma : \begin{cases} e_1 \mapsto e_2 \\ e_2 \mapsto e_3 \\ e_3 \mapsto e_1 \end{cases}$$

をひき起こすものを取る. このとき, $\beta_1 \in \ker(\phi)$ に対し, ϕ の与え方から $\beta_2\beta_3 = \beta^2$ となる $\beta \in (K(e_1)^*)^2 = (K'^*)^2$ が存在し, $\beta_3/\beta_2 = (\beta/\beta_2)^2$ である. よって, β_2, β_3 の与え方から

$$\mathrm{N}_{K(e_1)/K}\left(\beta/\beta_2\right)^2 = \mathrm{N}_{K(e_1)/K}\left(\left(\beta/\beta_2\right)^2\right) = \mathrm{N}_{k(e_1)/K}\left(\beta_3/\beta_2\right) = 1$$

となる. ここで, $[K(e_1) : K] = 3$ より $-\beta$ を β とおき直せば $\mathrm{N}_{K(e_1)/K}(\beta/\beta_2) = 1$ であるため, Hilbert の定理 90 から $\beta/\beta_2 = \sigma(\gamma)/\gamma$ となる $\gamma \in K(e_1)^*$ が存在する. これより, $\beta_1/\sigma^2(\gamma) \in K^*$ をいえば $\beta_1 \in K^*(K_2^*)^2$ となる. よって, $\beta_1/\sigma^2(\gamma) \in K^*$ を示す. 今, β, γ の取り方から

$$(\sigma(\gamma)/\gamma)^2 = (\beta/\beta_2)^2 = \beta_3/\beta_2 = \sigma^2(\beta_1)/\sigma(\beta_1)$$

より

$$\sigma^2(\beta_1)/(\sigma(\gamma))^2 = \sigma(\beta_1)/\gamma^2$$

となる. これより, 両辺に σ^2 を作用させれば σ の位数が 3 であることから

$$\begin{aligned} \sigma\left(\beta_1/(\sigma^2(\gamma))^2\right) &= \sigma^2\left(\sigma^2(\beta_1)/(\sigma(\gamma))^2\right) \\ &= \sigma^2\left(\sigma(\beta_1)/\gamma^2\right) \\ &= \beta_1/(\sigma^2(\gamma))^2 \end{aligned}$$

となる. よってこれは $\mathrm{Gal}(K(e_1)/K) = \langle\sigma\rangle$ より $\beta_1/(\sigma^2(\gamma))^2 \in K^*$ を意味し, $\beta_1 \in K^*(K_2^*)^2$ となる. 従って, このとき $\ker(\phi) \subset K^*(K_2^*)^2$ がいえる.

(ii) 後者のとき, Galois 理論から $\mathrm{Gal}(K'/K)$ の 2 つの生成元 σ, τ として

$$\sigma : \begin{cases} e_1 \mapsto e_2 \\ e_2 \mapsto e_3 \\ e_3 \mapsto e_1 \end{cases} \qquad \tau : \begin{cases} e_1 \mapsto e_1 \\ e_2 \mapsto e_3 \\ e_3 \mapsto e_2 \end{cases}$$

をひき起こすものを取れば, Galois の基本定理から $K^{\langle\sigma\rangle} = K(\sqrt{D})$(ある $D \in K^*$) であり $K^{\langle\tau\rangle} = K(e_1)$ である. このとき, $\beta_1 \in \ker(\phi)$ とすれば $K'/K(\sqrt{D})$ は 3 次の巡回拡大ゆえ, (i) から $\beta_1 = c\gamma^2$ となる $c \in K(\sqrt{D})^*$ と $\gamma \in K'$ が存在する. ここで, $\tau(\gamma)/\gamma \in K(\sqrt{D})$ がいえる. なぜなら, τ の取り方と $\beta_1 \in K(e_1)^*$ であることから

$$c\gamma^2 = \beta_1 = \tau(\beta_1) = \tau(c)\tau(\gamma)^2$$

より, τ と c の取り方から

$$(\tau(\gamma)/\gamma)^2 = c/\tau(c) \in K(\sqrt{D})$$

であるため, $[K' : K(\sqrt{D})] = 3$ より, $\tau(\gamma)/\gamma) \in K(\sqrt{D})$ となるからである. よって, $\mathrm{Gal}(K(\sqrt{D})/K) \cong \langle\tau\rangle$ から $\mathrm{N}_{K(\sqrt{D})/K}(\tau(\gamma)/\gamma) = 1$ となるため, Hilbert の定理 90 から $\tau(\gamma)/\gamma = \tau(\delta)/\delta$ となる $\delta \in K(\sqrt{D})^*$ が存在する. これより $c\delta^2 \in K^*$ かつ $\gamma/\delta \in K(e_1)^*$ がいえれば

$$\beta_1 = c\delta^2 = (c\delta^2)(\gamma/\delta)^2 \in K^*(k(e_1)^*)^2$$

となり, $\ker(\phi) \subset K^*(K_2^*)^2$ がいえる. よって $c\delta^2 \in K^*$ かつ $\gamma/\delta \in K(e_1)^*$ を示す. まず, $\gamma/\delta \in K(e_1)^*$ は τ の取り方から $\tau(\gamma/\delta) = \gamma/\delta$ をいえば十分であり, δ の取り方から

$$\tau\left(\frac{\gamma}{\delta}\right) = \frac{\tau(\gamma)}{\tau(\delta)} = \frac{\tau(\gamma)\gamma}{\tau(\gamma)\delta} = \frac{\gamma}{\delta}$$

となるためいえる. 次に $c\delta^2 \in K^*$ については c, δ の取り方から $c\delta^2 \in K(\sqrt{D}) = K^{\langle\sigma\rangle}$ ゆえ $\tau(c\delta^2) = c\delta^2$ をいえば十分であり, δ の取り方から

$$\tau(c\delta^2) = \tau(c)\tau(\delta)^2 = \left(\frac{c\gamma}{\tau(\gamma)}\right)^2 \cdot \left(\frac{\tau(\gamma)\delta}{\gamma}\right)^2 = c\delta^2$$

となるため, $c\delta^2 \in K^*$ がいえる. よって, このとき $\ker(\phi) \subset K^*(K_2^*)^2$ となる. 以上より (c) が成り立つ. □

次は local pairing に関する命題を示す. ここでは K を局所体 ($\mathbb{R}, \mathbb{C}$ も含める) とすることに注意しておく.

命題 3.3.14. 定義 3.2.9 で与えた双線形な local pairing $[\cdot,\cdot]$ は非退化であり, 節 3.2 の Step1 で与えた単射準同型 (3.2.3)δ に対し $\mathrm{Im}(\delta) \times \mathrm{Im}(\delta)$ 上 trivial である.

証明. step1 : $[\cdot,\cdot]$ が非退化であることを示す. $[\cdot,\cdot]$ が左非退化かつ右非退化であることを示すが, Hilbert 記号の対称性から左非退化をいえば十分であり, $\{(1,1,1)\}$ ではない $\{\Lambda=(a,b,c)\}\in \mathrm{KS}/\mathrm{KS}^2$ に対し, $[\Lambda,M]=-1$ となる $M\in\mathrm{KS}$ が存在することをいえばよい (但し, ここでの $[\cdot,\cdot]$ は local pairing をひき起こす pairing(3.2.10) である). ここで, E/K は (3.2.1) で与えられており次の 3 つの場合に分けて証明する.

(i) E を与える f が K で (3 つの)1 次因子の積に分解される場合. Λ の取り方から一般性を失うことなく $a\notin (K^*)^2$ としてよい. これより Hilbert 記号の非退化性 (命題 1.0.13 の (a)) から $(a,\mu)_K=-1$ となる $\mu\in K^*$ が存在するため, $M=(1,\mu,\mu)\in\mathrm{KS}$ とすれば,

$$\begin{aligned}[\Lambda,M]&=(a,1)_K(b,\mu)_K(c,\mu)_K\\&=(bc,\mu)_K\\&=(a^{-1},\mu)_K\\&=(a,\mu)_K=-1\end{aligned}$$

となり, このとき $[\Lambda,M]=-1$ となる M が存在する.

(ii) f が 1 根のみ K の元である場合. 場合によっては添え字を変えて $e_1\in K$ かつ $e_2,e_3\notin K$ とすれば f は

$$K(e_2,e_3)=K(e_2)=K(e_3)=K(\sqrt{D})\ (\text{ある } D\in K^*)$$

上 (3 つの)1 次因子の積に分解されている. このとき, まず, $aK^*\notin (K^*)^2$ であれば (i) と同様の議論から $(a,\mu)_K=-1$ となる $\mu\in K^*$ が存在するため ($e_1\in K$ であった), $M=(1,\mu,\mu)$ とすれば Hilbert 記号の性質 (命題 1.0.13) から

$$\begin{aligned}[\Lambda,M]&=(a,1)_K(b,\mu)_{K(e_2)}\\&=(b,\mu)_{K(\sqrt{D})}\\&=(\mathrm{N}_{K(\sqrt{D})/K}(b),\mu)_K\\&=(bc,\mu)_K\\&=(a^{-1},\mu)_K\\&=(a,\mu)_K=-1\end{aligned}$$

となる. 次に, $a\in(K^*)^2$ であれば代表元 Λ として $b\in K^*\setminus((K^*)^2\cup D(K^*)^2)$ となるように取ることができる (取り直しても $a\in(K^*)^2$ であることには変わらない). この理由は次である. KS の与え方と $a\in(K^*)^2$ より b と c は K 上共役でありかつ $bc\in(K^*)^2$ であるため $bc=d^2$ となる $d\in K^*$ が存在する. よって

$$\mathrm{N}_{K(\sqrt{D})/K}(b/d)=bc/d^2=d^2/d^2=1$$

であるため, Hilbert の定理 90 からある $d'=\alpha+\beta\sqrt{D}\in K(\sqrt{D})^*$ に対し

$$\frac{b}{d}=\frac{\alpha-\beta\sqrt{D}}{\alpha+\beta\sqrt{D}}=\frac{(\alpha-\beta\sqrt{D})^2}{\alpha^2-\beta^2D}$$

となり,

$$b = \frac{d}{\alpha^2 - \beta^2 D}(\alpha - \beta\sqrt{D})^2 \in K^*(K(\sqrt{D})^*)^2$$

がいえるため, $b \in K^* \setminus ((K^*)^2 \cup D(K^*)^2)$ としてよい. このとき, Hilbert 記号の非退化性から $(b, \epsilon)_K = -1$ となる $\epsilon \in K^*$ が存在する. よって, $\mathrm{N}_{K(\sqrt{D})/K}(\gamma) = \epsilon$ となる $\gamma \in K(\sqrt{D})$ を取り, $\gamma' \in K(\sqrt{D})$ を γ の K 上の共役元とし, $M = (\epsilon, \gamma, \gamma')$ とすれば ϵ, γ の取り方と Hilbert 記号の性質 (命題 1.0.13) から

$$\begin{aligned}
[\Lambda, M] &= (a, \epsilon)_K (b, \gamma)_{K(e_2)} \\
&= (b, \gamma)_{K(\sqrt{D})} \\
&= (b, \mathrm{N}_{K(\sqrt{D})/K}(\gamma))_K \\
&= (b, \epsilon)_K = -1
\end{aligned}$$

となる. 従ってこのとき $[\Lambda, M] = -1$ となる M が存在する.

(iii) f が K_v 上既約である場合. f の最小分解体を K' としたとき, Galois 理論から拡大 K'/K が 3 次の巡回拡大であるか, もしくは Galois 群が $\mathfrak{S}_3$ と同型になる 6 次の拡大であるため, この 2 つの場合に分けて示す. まず, K' が前者のとき

$$K' = K(e_1) = K(e_2) = K(e_3)$$

であり, 当然 K' 上で f は一次因子の積に分解されることから (i) より $v_1 v_2 v_3 \in (K^*)^2$ を満たすある $\{v_1, v_2, v_3\} \in \prod_{i=1}^3 K'^*$ が存在して

$$(a, v_1)_{K'} (b, v_2)_{K'} (c, v_3)_{K'} = -1$$

となる. よって, $\mathrm{Gal}(K'/K)$ の生成元 σ として

$$\sigma : \begin{cases} e_1 \mapsto e_2 \\ e_2 \mapsto e_3 \\ e_3 \mapsto e_1 \end{cases}$$

をひき起こすものを取り,

$$\mu_1 = v_1 \cdot \sigma^{-1}(v_2) \cdot \sigma^{-2}(v_3), \quad \mu_2 = \sigma(\mu_1), \quad \mu_3 = \sigma^2(\mu_1)$$

として $M = (\mu_1, \mu_2, \mu_3)$ とすれば σ と v_i の取り方から $M \in \mathrm{KS}$ ゆえ,

$$\begin{aligned}
[\Lambda, M] = (a, \mu_1)_{K(e_1)} &= (a, \mu_1)_{K'} \\
&= \left(a, v_1 \cdot \sigma^{-1}(v_2) \cdot \sigma^{-2}(v_3)\right)_{K'} \\
&= \left(a, v_1\right)_{K'} \left(a, \sigma^{-1}(v_2)\right)_{K'} \left(a, \sigma^{-2}(v_2)\right)_{K'} \\
&= (a, v_1)_{K'} (b, v_2)_{K'} (c, v_3)_{K'} \\
&= -1
\end{aligned}$$

となる. 最後に K' が後者のとき, Galois 理論から $\mathrm{Gal}(K'/K)$ の生成元 σ, τ として

$$\sigma : \begin{cases} e_1 \mapsto e_2 \\ e_2 \mapsto e_3 \\ e_3 \mapsto e_1 \end{cases} \qquad \tau : \begin{cases} e_1 \mapsto e_1 \\ e_2 \mapsto e_3 \\ e_3 \mapsto e_2 \end{cases}$$

をひき起こすものを取ることができる. 今, KS の与え方と Λ の取り方から $a \notin (K(e_1)^*)^2$ であるため, Hilbert 記号の非退化性から $(a, \gamma) = -1$ となる $\gamma \in K(e_1)^*$ が存在する. これより,

$$\mu_1 = \sigma(\gamma) \cdot \sigma^2(\gamma), \quad \mu_2 = \sigma(\mu_1), \quad \mu_3 = \sigma(\mu_2) = \sigma^2(\mu_1)$$

として $M = (\mu_1, \mu_2, \mu_3)$ とすれば σ と γ の取り方から $M \in \mathrm{KS}$ である. このとき, $\mathrm{Gal}(K'/K(e_1)) = \langle \tau \rangle$ であり, b, c は $K(e_1)$ 上共役であるため

$$\begin{aligned} (b, \gamma)_{K'} = (c, \gamma)_{K'} &= (\mathrm{N}_{K'/K(e_1)}(c), \gamma)_{K(e_1)} \\ &= (bc, \gamma)_{K(e_1)} \\ &= (a, \gamma)_{K(e_1)} = -1 \end{aligned}$$

となる. よって, σ, τ の与え方から $\tau(\sigma(\gamma)) = \sigma^2(\gamma)$ ゆえ

$$\begin{aligned} [\Lambda, M] = (a, \mu_1)_{K(e_1)} &= \big(a, \mathrm{N}_{K'/K(e_1)}(\sigma(\gamma))\big)_{K(e_1)} \\ &= (a, \sigma(\gamma))_{K'} \\ &= (\sigma(c), \sigma(\gamma))_{K'} \\ &= (c, \gamma)_{K'} = -1 \end{aligned}$$

となり, このとき $[\Lambda, M] = -1$ となる M が存在する. 以上より local pairing $[\cdot, \cdot]$ は非退化である.

Step2 : $\mathrm{Im}(\delta) \times \mathrm{Im}(\delta)$ 上 trivial であることを示す. K が局所体であることと δ が準同型であることから, $x, y \neq 0$ かつ $x \neq u$ となる $P = (x, y), Q = (u, v) \in E(K)$ に対して示せばよい. このとき, $z = (x - u)^{-1}$ としたときの自明な等式

$$z(x - e_i) - z(u - e_i) = 1 \quad (i = 1, 2, 3) \tag{3.3.15}$$

から,

$$z(x - e_i) \cdot 1^2 - z(u - e_i) \cdot 1^2 - 1^2 = 0$$

であるため, Hilbert 記号の定義と Hilbert 記号の双線形性より各 $i (i = 1, 2, 3)$ に対して

$$\begin{aligned} 1 &= (z(x - e_i), -z(u - e_i))_{K(e_i)} \\ &= (z, -z)_{K(e_i)}(x - e_i, -z)_{K(e_i)}(z, u - e_i)_{K(e_i)}(x - e_i, u - e_i)_{K(e_i)} \\ &= (x - e_i, -z)_{K(e_i)}(z, u - e_i)_{K(e_i)}(x - e_i, u - e_i)_{K(e_i)} \end{aligned}$$

が成り立つ. よって,

$$[\delta(P),\delta(Q)] = \prod_{\{i\}\in\mathfrak{I}_K}(x-e_i,u-e_i)_{K(e_i)}$$
$$= \left\{\prod_{\{i\}\in\mathfrak{I}_K}(x-e_i,-z)_{K(e_i)}\right\}\left\{\prod_{\{i\}\in\mathfrak{I}_K}(z,u-e_i)_{K(e_i)}\right\} \tag{3.3.16}$$

となり, ここで以下の 3 つの場合に分けて示す.

(i) f が K 上 (3 つの)1 次因子の積に分解されるとき. E 上が (3.2.1) で与えられていることから

$$\prod_{i=1}^{3}(x-e_i,-z)_K = (y^2,-z)_K = 1, \quad \prod_{i=1}^{3}(z,u-e_i)_K = (z,v^2)_K = 1$$

となり, (3.3.16) から $[\delta(P),\delta(Q)] = 1$ となる.

(ii) f の 1 根のみ K の元であるとき. 添え字を入れ換えて $e_1 \in K$ かつ $e_2, e_3 \notin K$ としてもよい. よって, 再び E 上が (3.2.1) で与えられていることから

$$\begin{aligned}(x-e_1,-z)_K(x-e_2,-z)_{K(e_2)} &= (x-e_1,-z)_K\left(\mathrm{N}_{K(e_2)/K}(x-e_2),-z\right)_K\\ &= (x-e_1,-z)_K\left((x-e_2)(x-e_3),-z\right)_K\\ &= \left((x-e_1)(x-e_2)(x-e_3),-z\right)_K\\ &= (y^2,-z)_K = 1\end{aligned}$$

であり, また同様にして

$$(z,u-e_1)_K(z,u-e_2)_{K(e_2)} = 1$$

となる. よって (3.3.16) から $[\delta(P),\delta(Q)] = 1$ である.

(iii) f が K 上既約であるとき. 再び E 上が (3.2.1) で与えられていることから

$$\begin{aligned}(x-e_1,-z)_K(e_1) &= \left(\mathrm{N}_{K(e_2)/K}(x-e_2),-z\right)_K\\ &= \left((x-e_1)(x-e_2)(x-e_3),-z\right)_K\\ &= (y^2,-z)_K = 1\end{aligned}$$

であり, また同様にして $(z,u-e_1)_{K(e_1)} = 1$ となる. よって (3.3.16) から $[\delta(P),\delta(Q)] = 1$ である. 以上より $\mathrm{Im}(\delta)\times\mathrm{Im}(\delta)$ 上 trivial である □

次に, 主定理の (c) を示すのに必要な approximation theorem と呼ばれる定理を示す. まず, 幾つか補題を示すが K は始めの 2 つの補題において $\mathbb{Q}_v$(ある $v \in M_{\mathbb{Q}}$) の有限次拡大体とし, それ以後, 代数体とすることに注意しておく.

補題 3.3.17. K は $\mathbb{Q}_v$(ある $v \in M_{\mathbb{Q}}$) の有限次拡大体とする. このとき

$$e = \begin{cases} 0 & (f \text{ が } K \text{ 上既約であるとき}) \\ 1 & (f \text{ の } 1 \text{ 根のみ } K \text{ の元であるとき}) \\ 2 & (f \text{ が } K \text{ 上 } 1 \text{ 次因子の積に分解されるとき}) \end{cases}$$

とし, $d = [K : \mathbb{Q}_v]$,$W = \mathrm{KS}/\mathrm{KS}^2$ とすれば

$$\#\mathrm{Im}(\delta) = \#(E(K)/2E(K)) = \begin{cases} 2^{e-d} & (v = \infty) \\ 2^{e+d} & (v = 2) \\ 2^e & (\text{それ以外のとき}) \end{cases} \tag{3.3.18}$$

が成り立ち, さらに $\#W = (\#\mathrm{Im}(\delta))^2$ が成り立つ.

証明. Step1 : 次の 2 つを引用する. (a) は Herbrand の補題と呼ばれ, [13, Ⅵ 65:9] より引用する. また (b) は [16, Ⅶ Prop. 6.3] より引用する.

(a) G を Abel 群, H を有限指数の G の部分群とし, G の 2 つの自己準同型 Φ, Ψ が

$$\Phi \circ \Psi(G) = \Psi \circ \Phi(G) = \{1_G\}, \quad \Phi(H) \subset H, \quad \Psi(H) \subset H$$

を満たすとする. このとき, $G_\Phi = \mathrm{Ker}(\Phi)$, $H_\Phi = H \cap \mathrm{Ker}(\Phi)$ とし, Ψ に対しても同様に与えれば,

$$\frac{(G_\Phi : \Psi(G))}{(G_\Psi : \Phi(G))} = \frac{(H_\Phi : \Psi(H))}{(H_\Psi : \Phi(H))}$$

が成り立つ.

(b) K は補題の仮定を満たす体とし, R をその付値環とする. このとき, K 上定義された楕円曲線 E/K に対して $E(K)$ は R^+ と同型な有限指数の部分群をもつ (R^+ は環 R の和による加法群とする).

Step2 : まず前半を示す. $v = \infty$ のとき, K は $\mathbb{C}$ または $\mathbb{R}$ である. 今, $K = \mathbb{C}$ であれば $\mathbb{C}$ は代数的閉体ゆえ, f は常に $\mathbb{C}$ 上 1 次因子の積に分解される. よって $e = 2$ であり, $d = 2$ であることから $2^{2-2} = 1$ となる. 一方, 命題 (2.1.8) の上で述べたように $E(\mathbb{C})$ はある複素 1 次元トーラス $\mathbb{C}/\Lambda$ と, 特に群として同型であることから明らかに $E(\mathbb{C})/2E(\mathbb{C})$ は自明な群となり, このとき (3.3.18) が成り立つ.

また $K = \mathbb{R}$ であれば, $[\mathbb{C} : \mathbb{R}] = 2$ より f は $\mathbb{R}$ 上既約ではなく, f の判別式を Δ_f とすれば f が $\mathbb{R}$ で 1 根のみ (3 根) もつときかつそのときのみ $\Delta_f < 0 (\Delta_f > 0)$ である. よって, $\Delta(E) = 16\Delta_f$ であることと, $d = 1$ より

$$2^{e-d} = \begin{cases} 1 & (\Delta(E) < 0) \\ 2 & (\Delta(E) > 0) \end{cases}$$

となる. 一方, [17, p. 188] より

$$\#E(\mathbb{R})/2E(\mathbb{R}) = \begin{cases} 1 & (\Delta(E) < 0) \\ 2 & (\Delta(E) > 0) \end{cases}$$

であることからこのとき (3.3.18) が成り立つ.

$v \neq \infty$ のとき, Step1 の (b) から R^+ を $E(K)$ の部分群とみなし, Step1 の (a) において $G = E(K), H = R^+, \Psi = [2]$ とし, Φ を常に O に移る定値写像とすれば (a) の仮定を満たし, このとき

$$\begin{array}{llll} G_\Phi = E(K), & \Psi(G) = 2E(K), & G_\Psi = E(K)[2], & \Phi(G) = \{O\}, \\ H_\Phi = R^+, & \Psi(H) = 2R^+, & H_\Psi = \{O\}, & \Phi(H) = \{O\} \end{array}$$

であるため,

$$\begin{aligned} \#E(K)/2E(K) = (E(K) : 2E(K)) &= (E(K)[2] : \{O\})(R^+ : 2R^+) \\ &= \#E(K)[2](R^+ : 2R^+) \end{aligned}$$

となる. ここで, e の与え方から $\#E(K)[2] = 2^e$ であり,

$$(R^+ : 2R^+) = \begin{cases} 2^d & (v = 2 \text{ のとき}) \\ 1 & (v \neq 2 \text{ のとき}) \end{cases}$$

ゆえ, このとき (3.3.18) が成り立つ.

後半は $v \neq \infty$ のとき, $K = \mathbb{C}$ であれば前半の証明より $\#\mathrm{Im}(\delta) = 1$ である. 一方, E を与える f が $\mathbb{C}$ 上 1 次因子の積に分解されることと, $\mathbb{C}^*/(\mathbb{C}^*)^2$ が自明な群であることから, 命題 3.3.12 の (a) より $\#W = 1 \cdot 1 = 1$ となるため $\#W = (\#\mathrm{Im}(\delta))^2$ が成り立つ. 次に $K = \mathbb{R}$ かつ $\Delta(E) > 0$ であれば, 前半の証明から $\#\mathrm{Im}(\delta) = 2$ である. 一方, 前半より E を与える f が $\mathbb{R}$ 上 1 次因子の積に分解されることと, $\mathbb{R}^*/(\mathbb{R}^*)^2 \cong \mathbb{Z}/2\mathbb{Z}$ から, 命題 3.3.12 の (a) より $\#W = 2 \cdot 2 = 4$ となるため $\#W = (\#\mathrm{Im}(\delta))^2$ が成り立つ. また, $K = \mathbb{R}$ かつ $\Delta(E) < 0$ であれば, 前半の証明から $\#\mathrm{Im}(\delta) = 1$ である. 一方, 前半より E を与える f が $\mathbb{R}$ で 1 根もち, 命題 3.3.12 の (b) で与えた $K_1 = \mathbb{R}(e_i)$ は $\mathbb{R}$ の 2 次拡大体, 即ち $K_1 = \mathbb{C}$ である. よって $\mathbb{C}^*/(\mathbb{C}^*)^2$ は自明な群であるため, 命題 3.3.12 の (b) より $\#W = 1$ となり $\#W = (\#\mathrm{Im}(\delta))^2$ が成り立つ.

$v \neq 2, \infty$ のとき, $e = 1, 2$ のときは命題 3.3.12 と [7, §11 Thm. 11.3] または [11, II §3 Prop. 6] から明らか. $e = 0$ のときは

$$\#W = \#(K_2^*/(K_2^*)^2)/\#(K^*/(K^*)^2) \tag{3.3.19}$$

がいえれば, 再び [7, §11 Thm. 11.3] または [11, II §3 Prop. 6] から $\#W = \#\mathrm{Im}(\delta) = 1$ となる. よって (3.3.19) を示せばよい. ここで, $K_2^{*2} \subset K^*(K_2^*)^2 \subset K_2^*$ より群の第 2 同型定理と命題 3.3.12 の (c) から

$$W \cong K_2^*/\left(K^*(K_2^*)^2\right) \cong \left(K_2^*/(K_2^*)^2\right) / \left(K^*(K_2^*)^2/(K_2^*)^2\right)$$

が成り立つ. さらに群の第 1 同型定理と $K^* \cap (K_2^*)^2 = (K^*)^2$ であることから

$$\left(K^*(K_2^*)^2/(K_2^*)^2\right)/(K_2^*)^2 \cong K^*/\left(K^* \cap (K_2^*)^2\right) = K^*/(K^*)^2$$

となる. 従って

$$W \cong (K_2^*/(K_2^*)^2)/(K^*/(K^*)^2) \tag{3.3.20}$$

ゆえ (3.3.19) が成り立つことからこのときも $\#W = \#\mathrm{Im}(\delta)$ が成り立つ.

$v = 2$ のとき, [11, II §3 Prop. 6] より L を $\mathbb{Q}_2$ の有限次拡大とするとき $\#(L^*/(L^*)^2) = 2^{2+[L:\mathbb{Q}_2]}$ となることを用いて示す. $e = 2$ のときは命題 3.3.12 と前半から明らか. $e = 1$ のときは $[K_1 : \mathbb{Q}_2] = [K_1 : K][K : \mathbb{Q}_2] = 2d$ であるため, 命題 3.3.12 と前半から

$$\#W = \#(K_1^*/(K_1^*)^2) = 2^{2+[K_1:\mathbb{Q}_2]} = 2^{2+2d} = (2^{1+d})^2 = \#(\mathrm{Im}(\delta))^2$$

となる. また, $e = 2$ のときは $[K_2 : \mathbb{Q}_2] = [K_2 : K][K : \mathbb{Q}_2] = 3d$ であることから $e = 1$ のときと同様にすればよい. 以上より後半が成り立ち, 補題が成り立つ. □

補題 3.3.21. K を $\mathbb{Q}_v$(v は K の有限素点) の有限次拡大体とし, $\Lambda = (b_1, b_2, b_3) \in \mathrm{KS}$ する. このとき, 各 $i(i = 1, 2, 3)$ に対し $K(\sqrt{b_i})/K(e_i)$ が不分岐拡大ならば Λ は不分岐であるとする ($\mathrm{KS}/\mathrm{KS}^2$ に対しても同様に定義する). これより, $v \neq 2, \infty$ でありかつ K の付値で E/K が good reduction をもてば, (3.2.3) で与えた単射準同型 δ に対し, $\mathrm{Im}(\delta)$ は不分岐なものからなる $\mathrm{KS}/\mathrm{KS}^2$ の部分集合に一致する.

証明. Step1 : K を局所体, R をその付値環, k をその剰余体とし, E/K を K 上定義された楕円曲線 E/K とする. このとき, 次の 3 つを引用する. (a) は [16, VII Prop. 3.1] より引用する. また, (b) は Neron-Ogg-Shafarevich の criteiron と呼ばれるものの一部であり, [16, VII Thm. 7.1] より引用し, (c) は semi-stable reduction theorem と呼ばれるもの一部であり, [16, VII Prop. 5.4] より引用する.

(a) $\tilde{E}$ を reduction 写像 $R \to k$ によって引き起こされる k 上定義された曲線とする. このとき, E が K で good reduction をもつならば $(\mathrm{ch}\,(k), m) = 1$ となる各整数 $m \geq 1$ に対し, reduction 写像 $E(K)[m] \to \tilde{E}(k)$ は単射となる.

(b) E が K で good reduction をもてば $(\mathrm{ch}\,(k), m) = 1$ となる各整数 $m \geq 1$ に対し, $K(E[m])/K$ は不分岐拡大となる.

(c) K'/K が不分岐拡大であれば K における E の reduction と K' における E の reduction の種類は同じである.

Step2 : 補題を証明する. まず, $P \in E(K)$ に対し $\delta(P) \in \mathrm{KS}/\mathrm{KS}^2$ が不分岐であることを示す. 今, $\delta(P) = \{(\delta_1(P), \delta_2(P), \delta_3(P))\}$ とし, 各 $i(i = 1, 2, 3)$ に対し ord_{v_i} を $K(e_i)$ の付値 v_i を正規化したものとする. このとき, 各 $i(i = 1, 2, 3)$ に対し,

$$\mathrm{ord}_{v_i}(\delta_i(P)) \equiv 0 \pmod 2 \tag{3.3.22}$$

がいえれば $K(\sqrt{\delta_i(P)})/K$ は不分岐拡大ゆえ, $\delta(P) \in \mathrm{KS}/\mathrm{KS}^2$ は不分岐となる. よって (3.3.22) を示す. まず, $P = (a, b) \notin E(K)[2]$ のとき δ の与え方から各 $i(i = 1, 2, 3,)$ に対し

$$\mathrm{ord}_{v_i}(\delta_i(P)) \equiv \mathrm{ord}_{v_i}(a - e_i) \pmod 2$$

であり, 各 $i(i = 1, 2, 3)$ に対し $\mathrm{ord}_{v_i}(a-e_i) \equiv 0 \pmod 2$ をいえばよい. 各 $i(i = 1, 2, 3)$ に対し $\mathrm{ord}_{v_i}(a - e_i) = 0$ のときは自明である. また, ある i で $\mathrm{ord}_{v_i}(a - e_i) \geq 1$ ならば, E は (3.2.1) で与えられているため $\mathrm{ord}_{v_i}(b) \geq 1$ である. ここで K' を f の最小分解体とし, ord_v を K' の正規付値とすれば当然 $K(e_i) \subset K'$ より

$$\mathrm{ord}_v(a - e_i) \geq 1, \qquad \mathrm{ord}_v(b) \geq 1$$

である. これは, k' を k の剰余体とするときの reduction 写像 $E(K) \to \tilde{E}(k)$ により P と $(e_i, 0)$ が同じ点に対応することを意味する. 一方, $\mathrm{ch}\,(k) \neq 2$ であるため, Step1 の (a) と (c) から $E[2] = E(K')[2] \to \tilde{E}(k')$ は単射ゆえ, reduction 写像により $(e_i, 0)$ と $(e_{i+1}, 0)$ と $(e_{i+2}, 0)$ は互いに異なる点に対応する. よって, これは

$$\mathrm{ord}_v(a - e_{i+1}) = \mathrm{ord}_v(a - e_{i+2}) = 0$$

を意味し, Step2 の (b) から

$$\mathrm{ord}_{v_i}(a - e_{i+1})(a - e_{i+2}) = 0$$

となる. 従って

$$\begin{aligned} \mathrm{ord}_{v_i}(a - e_i) &= \mathrm{ord}_{v_i}(a - e_i)(a - e_{i+1})(a - e_{i+2}) \\ &= \mathrm{ord}_{v_i}(b^2) \\ &= 2\mathrm{ord}_{v_i}(b) \equiv 0 \pmod 2 \end{aligned}$$

となり, これは各 i(i=1,2,3) に対していえるため, このとき $\delta(P)$ は不分岐である. また, $P \in E(K)[2]$ のときも同様にすればよい. 以上から $P \in E(K)$ に対し $\delta(P) \in \mathrm{KS}/\mathrm{KS}^2$ は不分岐である. これより, $\#\mathrm{Im}(\delta)$ と $\mathrm{KS}/\mathrm{KS}^2$ で不分岐なものの集合の元の個数 d' が同じであれば補題が成り立つ. ここで, [11, II §3 Prop. 6] から L を $\mathbb{Q}_v(v$ は $\mathbb{Q}$ の有限素点) の有限次拡大とすれば $\#(U_L/U_L^2) = 2$ であること, 命題 3.3.12 と前半から $d' = 2^e = \#\mathrm{Im}(\delta)$ となり, 補題が成り立つ. □

以後, K は代数体とする.

補題 3.3.23. $\alpha, \beta \in \mathrm{KS}/\mathrm{KS}^2$ とする. このとき, 有限個を除いたすべての $v \in M_K$ に対し $[\alpha, \beta]_v = 1$ であり (但し, $[\cdot, \cdot]_v$ は K_v に対する $\mathrm{KS}_v/\mathrm{KS}_v^2 \times \mathrm{KS}_v/\mathrm{KS}_v^2$ 上の local pairing である),

$$\prod_{v \in M_K} [\alpha, \beta]_v = 1$$

となる.

証明. $[\cdot,\cdot]_v$ の定め方と注 (命題 1.0.13 の (b)) から明らか. □

定理 3.3.24 (approximation). $(\alpha_v)_{v\in M_K} \in \prod_{v\in M_K} \mathrm{KS}_v/\mathrm{KS}^2$ は有限個を除いたすべての $v \in M_K$ で, $\alpha_v \in \mathrm{Im}(\delta_v)$ であるとする (但し, δ_v は K_v に対して定まる単射準同型 (3.2.3) である). このとき, 各 $v \in M_K$ に対し $\alpha\alpha_v^{-1} \in \mathrm{Im}(\delta_v)$ となる $\alpha \in \mathrm{KS}/\mathrm{KS}^2$ が存在するための必要十分条件は各 $\beta \in \mathrm{FD}/\mathrm{KS}^2$ に対し

$$\prod_{v\in M_K} [\alpha_v, \beta]_v = 1$$

となることである.

証明. Step1 : $S \subset M_K$ を無限素点を含む有限集合としたとき K_S を S を除いたところで可逆となる K^* の元からなる集合とする. このとき次を [7, pp. 70-72] から引用し, 幾つか記号を定義する. ある無限素点を含む M_K の有限集合 S_0 が存在し, S_0 を含む任意の有限集合 S に対し以下の 2 つを満たす.

(a) $\#(K_S/K_S^2) = 2^{\#S}$ である.

(b) 自然な写像 $K \to K_v (v \in M_K)$ によって引き起こされる写像

$$K_S/K_S^2 \to \prod_{v\in S} K_v/K_v^2$$

は単射である.

これより, 同様のことが $K(e_i)(i = 1, 2, 3), K'(K'$ は f の最小分解体) にもいえる. よって S として S の各素点 v の上にある $K(e_i), K'$ の素点がともにすべて上の (a),(b) を満たすように取り直せる. さらに S を除いたところで good reduction を持つように S を取り直す. また, KS_S を KS の元であって S を除いたところで不分岐な集合とし, $W_S = \mathrm{KS}_S/\mathrm{KS}_S^2$ とし, $W_v = \mathrm{KS}_v/\mathrm{KS}_v^2$ とすれば, S の取り方から (b) によって引き起こされる局所化写像 $W_S \to \prod_{v\in S} W_v$ は単射となる.

Step2 : Step1 で与えた記号に対し $H = \prod_{v\in S} \#\mathrm{Im}(\delta_v)$ とすれば $\prod_{v\in S} \#W_S = H^2$ であり, $\#W_S = H$ である.

前者は補題 3.3.17 から明らか. 後者を示す.

(i) f が K 上 (3 つの)1 次因子の積に分解されるとき. まず, Step1 における S の取り方と補題 3.3.17 から

$$H = \prod_{v\in S} \#(\mathrm{Im}(\delta_v)) = (2^2)^{\#S}$$

である. 一方, 命題 3.3.12 の (a) と Step1 における S の取り方から

$$\#W_S = \#\left(\mathrm{KS}_S/\mathrm{KS}_S^2\right) = \#(K_S^*/(K_S^*)^2)^2 = (2^{\#S})^2 = (2^2)^{\#S}$$

となり, $\#W_S = H$ が成り立つ.

(ii) f が 1 根のみ K の元である場合. L を S の上にある K_1 の素点からなる集合とし, 各 $v \in M_k$ に対する f の K_v 上の既約因子の数を g_v とすれば [11, Ⅱ §1 Cor. 1] より

$$\#L - \#S = \sum_{v \in S}(g_v - 2)$$

である. よって S の取り方と命題 3.3.12 から

$$\#W_S = \#(K_{1L}^*/K_{1L}^*) = 2^{\#L} = 2^{\sum_{v\in S}(g_v-1)} = \prod_{v\in S}\#(\mathrm{Im}(\delta_v)) = H$$

となる.

(iii) f が K 上既約であるとき. L' を S の上にある K_2 の上にある素点からなる集合とすれば再び [11, Ⅱ §1 Cor. 1] より

$$\#L - \#S = \sum_{v \in S}(g_v - 1)$$

となることから (ii) と同様にすれば $\#W_S = H$ を得る. 以上より $\#W_S = H$ が成り立つ.

Step3 : 命題を示す. まず, 必要性は補題 3.3.23 と命題 3.3.14 の後半より明らか. 次に十分性を示す前に幾つか述べる. まず, Step1 で与えた S を含む有限集合であってその集合を除いたすべての素点 v に対して $\Lambda_v \in \mathrm{Im}(\delta_v)$ となるように S を取り直せば当然, Step1,2 で述べたこととがこの S に対しても成り立つ. また, 各 $v \in M_k$ に対する $\mathrm{KS}_v/\mathrm{KS}_v^2$ 上の local pairing $[\cdot,\cdot]_v$ は, $\prod_{v\in S}[\cdot,\cdot]$ によって命題 3.3.14 から非退化な双線形形式

$$\Gamma : \prod_{v\in S} W_v \times \prod_{v\in S} W_v \to \{\pm 1\}$$

を引き起こし, $M := \prod_{v\in S}\mathrm{Im}(\delta_v)$ とすれば $M \times M$ 上 trivial である. ここで, R を Step1 で与えた局所化写像による W_S の image とすれば, S の取り方から局所化写像は単射であるため, Step2 より $\#R = \#W_S = H$ である. また, 局所化写像と Γ の与え方から, 補題 3.3.23 より Γ は $R \times R$ 上 trivial である. よって, M, R, Γ の与え方と Γ の双線形性から $(MR) \times (M \cap R)$ 上 trivial であり, $\#R = H = \#M$ であることと群の同型定理から $\#MR \cdot \#M \cap R = H^2$ となる. 従って MR と $M \cap R$ は Γ における $\prod_{v\in S} W_v$ の直交補空間となる. これより, 十分性を示す. 各 $\beta \in \mathrm{FD}/\mathrm{KS}^2$ に対し

$$\prod_{v\in M_K}[\alpha_v, \beta]_v = 1$$

であるとすれば, FD の与え方から $\mathrm{FD}/\mathrm{KS}^2 \cong M \cap R$ となることと, Γ の与え方から $(\alpha_v)_{v\in S} \in MR$ である. よって M, R の与え方から, ある $(d_v)_{v\in S} \in M$ と $\alpha \in W_S$ が存在して

$$(\alpha_v)_{v\in S} = (d_v\alpha)_{v\in S}$$

となり, これは各 $v \in S$ に対し $\alpha\alpha_v^{-1} \in \mathrm{Im}(\delta_v)$ となることを意味する. 一方, S, W_S の与え方と補題 3.3.21 から $v \in M \setminus S$ に対して $\alpha, \alpha_v \in \mathrm{Im}(\delta_v)$ である. よって, 各 $v \in M_K$ に対し $\alpha\alpha_v^{-1} \in \mathrm{Im}(\delta_v)$ となることから十分性がいえ, 命題が成り立つ. □

次で与える補題は $\langle \cdot, \cdot \rangle$ が L_0 を使わなくても定まることを意味し, Application と主定理の (d) の証明で用いられる. なお, paring $\langle \cdot, \cdot \rangle$ が well-defined であることはまだ示してはいないが, これが示されたと仮定して証明する.

補題 3.3.25. $\alpha = \{\Lambda\}, \beta = \{(c_1, c_2, c_3)\} \in \mathrm{FD}/\mathrm{KS}^2$ に対し

$$\langle \alpha, \beta \rangle = \prod_{v \in M_K} \prod_{\{i\} \in \mathfrak{I}_{K_v}} (L_i(Q_v), c_i)_{K_v(e_i)} \tag{3.3.26}$$

となる (但し, Λ に対して L_i, L_0, Q_v は節 3.2 の Step4 の方法で取ってきたものであり,$\mathfrak{I}_{K_v}$ は節 3.2 の Step3 で与えたものである).

証明. paring $\langle \cdot, \cdot \rangle$ が well-defined であることは仮定して証明する. Hilbert 記号の性質 (命題 1.0.13) と補題 3.3.23 と各 v に対して $L_0(Q_v) \in K_v$ であることから

$$\begin{aligned}
\left\{ \prod_{v \in M_K} \prod_{\{i\} \in \mathfrak{I}_{K_v}} (L_i(Q_v), c_i)_{K_v(e_i)} \right\} \langle \alpha, \beta \rangle^{-1} &= \prod_{v \in M_K} \prod_{\{i\} \in \mathfrak{I}_{K_v}} (L_0(Q_v), c_i)_{K_v(e_i)} \\
&= \prod_{v \in M_K} \prod_{\{i\} \in \mathfrak{I}_{K_v}} \left(L_0(Q_v), N_{K_v(e_i)/K_v}(c_i)\right)_{K_v} \\
&= \prod_{v \in M_K} (L_0(Q_v), c_1 c_2 c_3)_{K_v} \\
&= 1
\end{aligned}$$

となり, 一番上と一番下の右側に対し右から $\langle \alpha, \beta \rangle$ を掛ければ (3.3.26) が成り立つ. □

3.4 主定理の証明

これより前の節で示した幾つかの補題を用いて主定理を証明する.

(*a*) の証明. $\alpha = \{\Lambda\}, \beta = \{(c_1, c_2, c_3)\} \in \mathrm{FD}/\mathrm{KS}^2$ に対して, 以下の 2 つがいえればよい.

(i) 各 $v \in M_K$ に対し local pairing

$$[\{\mathfrak{J}_v(\Lambda)\}, \beta]_v = \prod_{\{i\} \in \mathfrak{I}_K} \left(\frac{L_i}{L_0}(Q_v'), c_i \right)_{K_v(e_i)} \tag{3.4.1}$$

が Q_v の取り方に寄らず定まりかつ有限個を除いたすべての $v \in M_K$ で 1 となるとなる.

(ii) $\langle \alpha, \beta \rangle$ の値は各 $i(i = 0, 1, 2, 3)$ に対して Q_i を固定したときの L_i の取り方と, Q_i の取り方に寄らない.

まず (i) が成り立つことを示す. 前者は各 $v \in M_K$ に対し, 命題 2.4.17 から C_Λ/K_v は E/K_v の主等質空間であるため, Q'_v を C_Λ の別の K_v-有理点として取ってくれば命題 2.4.7 から E 上の K_v-有理点 $Q = (x_v, y_v)$ が存在して, $Q'_v = Q_v + Q$ とできる. これより補題 3.3.10 の (b) から各 $i(i = 1, 2, 3)$ に対し, ある $h_{i,v} \in K_v(e_i)^*$ が存在して

$$\frac{(L_i/L_0)(Q'_v)}{(x_v - e_i) \cdot (L_i/L_0)(Q_v)} = h_{i,v}^2$$

となる. よって, $\delta_v(Q), \beta \in \mathrm{Im}(\delta_v)$ であるため ($\beta \in \mathrm{Im}(\delta_v)$ は FD の定義からいえる), 命題 3.3.14 より

$$\begin{aligned}
\prod_{\{i\} \in \mathfrak{I}_K} \left(\frac{L_i}{L_0}(Q'_v), c_i \right)_{K_v(e_i)} &= \left[\delta_v(Q), \beta \right]_v \times \prod_{\{i\} \in \mathfrak{I}_K} (h_{i,v}, c_i)^2_{K_v(e_i)} \\
&\quad \times \prod_{\{i\} \in \mathfrak{I}_K} \left(\frac{L_i}{L_0}(Q'_v), c_i \right)_{K_v(e_i)} \\
&= \prod_{\{i\} \in \mathfrak{I}_K} \left(\frac{L_i}{L_0}(Q'_v), c_i \right)_{K_v(e_i)} \\
&= \left[\{ \mathfrak{J}_v(\Lambda) \}, \beta \right]_v
\end{aligned}$$

となり (3.4.1) は $Q_v \in C_\Lambda(K_v)$ の取り方に寄らない. 次に, 後者の (3.4.1) が有限個を除いたすべての $v \in M_K$ で 1 となることを示す. 今, 有限個を除いたすべての $v \in M_K$ で $E, C_\Lambda, L_0, L_i (i = 1, 2, 3)$ が good reduction をもつため, この v に対し C_Λ は十分に多くの K_v-有理点をもつことから, その中で $L_i(Q_v)(i = 1, 2, 3), L_0(Q_v)$ がともに $U_{K_v(e_i)}$ の元となるような点 Q_v を取れば (3.4.1) が C_Λ 上の K_v-有理点の取り方に寄らないことと命題 (1.0.13) の (c) からこの値は 1 となり後者が成り立つ.

次に (ii) を示す. まず, $\langle \alpha, \beta \rangle$ の値が各 $i(i = 1, 2, 3)$ に対して Q_i を固定したときの L_i の取り方に寄らないことを示す. L_i の取り方から L_i は $\alpha \in K(e_i)^*$ ($i = 0$ のときは便宜上 $e_0 = 1$ としておく) 倍を除いて一意的に定まっており, 節 3.2 の Step4 での取り方を満たす別の 1 次形式 $L'_i \in K(e_i)[U_1, U_2, U_3, T]$ を取ってくれば $L'_i = \alpha_i L_i$ となる $\alpha_i \in K(e_i)^*$ が存在する. このとき, L_i, L_0 の取り方から

$$\frac{\alpha_1}{\alpha_0} \cdot \frac{\alpha_2}{\alpha_0} \cdot \frac{\alpha_3}{\alpha_0} \in (K^*)^2$$

より

$$A := \left\{ \frac{\alpha_1}{\alpha_0}, \frac{\alpha_2}{\alpha_0}, \frac{\alpha_3}{\alpha_0} \right\} \in \mathrm{KS}$$

ゆえ, 補題 3.3.23 から

$$\begin{aligned}\prod_{v\in M_K}\prod_{\{i\}\in\mathfrak{I}_K}\left(\frac{L_i'}{L_0'}(Q_v),c_i\right)_{K_v(e_i)} &= \prod_{v\in M_K}\prod_{\{i\}\in\mathfrak{I}_K}\left(\frac{\alpha_i L_i}{\alpha_0 L_0}(Q_v),c_i\right)_{K_v(e_i)}\\ &= \left\{\prod_{v\in M_K}[\{A\},\beta]\right\}\left\{\prod_{v\in M_K}\prod_{\{i\}\in\mathfrak{I}_K}\left(\frac{L_i}{L_0}(Q_v),c_i\right)_{K_v(e_i)}\right\}\\ &= \prod_{v\in M_K}\prod_{\{i\}\in\mathfrak{I}_K}\left(\frac{L_i}{L_0}(Q_v),c_i\right)_{K_v(e_i)}\\ &= \langle\alpha,\beta\rangle\end{aligned}$$

となるため, $\langle\alpha,\beta\rangle$ の値は $L_i(i=0,1,2,3)$ の取り方に寄らない. 最後に $\langle\alpha,\beta\rangle$ の値が $Q_i(i=0,1,2,3)$ の取り方に寄らないことを示す. ここで, $Q_i'(i=0,1,2,3)$ をそれぞれ, Y_i の $K(e_i)$-有理点として取り (便宜上 $e_0=1$ とする), $L_i'(i=0,1,2,3)$ として節 3.2 の Step4 のやり方で取ってきたそれぞれ対する 1 次形式として取る. また, 1 次形式 $\mathfrak{L}\in K(e_i)[U_1,U_2,U_3,T](i=1,2,3)$ を $Y_i\subset\mathbb{P}^2$ における Q_i と Q_i' と結んだ直線を与える 1 次形式を射 $C_\Lambda\to Y_i$ によって引き戻したものとすれば, この取り方から $L_iL_i'=\beta_i\mathfrak{L}^2$ となる $\beta_i\in K(e_i)^*$ が存在する. よって, L,L' の取り方から (ii) の前半と同様にして

$$B:=\left\{\frac{\beta_1}{\beta_0},\frac{\beta_2}{\beta_0},\frac{\beta_3}{\beta_0}\right\}\in \mathrm{KS}$$

がいえるため, Hilbert 記号の性質 (命題 1.0.13) と補題 (3.3.23) より

$$\begin{aligned}&\left\{\prod_{v\in M_K}\prod_{\{i\}\in\mathfrak{I}_K}\left(\frac{L_i'}{L_0'}(Q_v),c_i\right)_{K_v(e_i)}\right\}\left\{\prod_{v\in M_K}\prod_{\{i\}\in\mathfrak{I}_K}\left(\frac{L_i}{L_0}(Q_v),c_i\right)_{K_v(e_i)}\right\}\\ &=\left\{\prod_{v\in M_K}\prod_{\{i\}\in\mathfrak{I}_K}\left(\frac{\beta_i\mathfrak{L}_i^2}{\beta_0\mathfrak{L}_0^2}(Q_v),c_i\right)_{K_v(e_i)}\right\}\\ &=\left\{\prod_{v\in M_K}[\{B\},\beta]_v\right\}\left\{\prod_{v\in M_K}\prod_{\{i\}\in\mathfrak{I}_K}\left(\frac{\mathfrak{L}_i}{\mathfrak{L}_0}(Q_v),c_i\right)^2_{K_v(e_i)}\right\}\\ &=1\end{aligned}$$

となる. 従って, 両辺の右側に一番上の等式の左側の右側を掛ければ

$$\prod_{v\in M_K}\prod_{\{i\}\in\mathfrak{I}_K}\left(\frac{L_i'}{L_0'}(Q_v),c_i\right)_{K_v(e_i)}=\prod_{v\in M_K}\prod_{\{i\}\in\mathfrak{I}_K}\left(\frac{L_i}{L_0}(Q_v),c_i\right)_{K_v(e_i)}$$

ゆえ, $\langle\alpha,\beta\rangle$ の値は $Q_i(i=0,1,2,3)$ の取り方に寄らない. 以上より主定理の (a) が成り立つ.

(b) の証明. $\alpha=\{\Lambda\},\alpha'=\{\Lambda\},\beta=\{M\},\beta'=\{M'\}\in \mathrm{FD}/\mathrm{KS}^2$ に対し

(i) $\langle \alpha\alpha', \beta\rangle = \langle \alpha, \beta\rangle\langle \alpha', \beta\rangle$,

(ii) $\langle \alpha, \beta\beta'\rangle = \langle \alpha, \beta\rangle\langle \alpha, \beta'\rangle$

が成り立つことを示す. まず (ii) は Hilbert 記号の双線形性 (命題 1.0.13 の (a)) より明らか. 次に (i) を示す. 今, $\Lambda'' = \Lambda\Lambda'$ とすれば $\Lambda\Lambda'\Lambda'' \in \mathrm{KS}^2$ ゆえ, 補題 3.3.10 より $L_i, L_i', L_i''(i = 0, 1, 2, 3)$ をそれぞれ $\Lambda, \Lambda', \Lambda''$ に対して節 3.2 の Step4 の方法で取ってきたものとする. 各 $v \in M_K$ に対し, Q_v, Q_v', Q_v'' をそれぞれ $C_\Lambda, C_{\Lambda'}, C_{\Lambda''}$ 上の K_v-有理点としてうまく取ってくれば, 各 $i(i = 1, 2, 3)$ に対し, ある $a_i \in K(e_i)^*$ と $h_{i,v} \in K_v(e_i)^*$ が存在して

$$\frac{L_i}{L_0}(Q_v) \cdot \frac{L_i'}{L_0'}(Q_v') \cdot \frac{L_i''}{L_0''}(Q_v'') = a_i \cdot h_{i,v}^2$$

となる. よって L_i, L_i', L_i'' の取り方から $\{a_1, a_2, a_3\} \in \mathrm{KS}$ ゆえ, Hilbert 記号の性質 (命題 1.0.13) と補題 (3.3.23) から

$$\begin{aligned}
&\langle \alpha, \beta\rangle\langle \alpha', \beta\rangle\langle \alpha\alpha', \beta\rangle \\
&= \left\{ \prod_{v\in M_K} \prod_{\{i\}\in\mathfrak{I}_K} \left(\frac{L_i}{L_0}(Q_v), c_i\right)_{K_v(e_i)} \right\} \left\{ \prod_{v\in M_K} \prod_{\{i\}\in\mathfrak{I}_K} \left(\frac{L_i'}{L_0'}(Q_v'), c_i\right)_{K_v(e_i)} \right\} \\
&\quad \times \left\{ \prod_{v\in M_K} \prod_{\{i\}\in\mathfrak{I}_K} \left(\frac{L_i''}{L_0''}(Q_v''), c_i\right)_{K_v(e_i)} \right\} \\
&= \prod_{v\in M_K} \prod_{\{i\}\in\mathfrak{I}_K} \left(\frac{L_i}{L_0}(Q_v) \cdot \frac{L_i'}{L_0'}(Q_v') \cdot \frac{L_i''}{L_0''}(Q_v''), c_i\right)_{K_v(e_i)} \\
&= \prod_{v\in M_K} \prod_{\{i\}\in\mathfrak{I}_K} (a_i, c_i)_{K_v(e_i)} (h_{i,v}, c_i)_{K_v(e_i)}^2 \\
&= \prod_{v\in M_K} \prod_{\{i\}\in\mathfrak{I}_K} (a_i, c_i)_{K_v(e_i)} \\
&= 1
\end{aligned}$$

となり両辺の左から $\langle \alpha\alpha', \beta\rangle$ を掛ければ (ii) を得る. 以上より pairirng $\langle \cdot, \cdot\rangle$ は双線形である.

(c) の証明. (必要性.) 補題 3.3.3 と補題 (3.3.23) と Hilbert 記号の性質 (命題 1.0.13) から明らか.

(十分性.) 任意の $\beta \in \mathrm{FD}/\mathrm{KS}^2$ に対し

$$1 = \langle \alpha, \beta\rangle = \prod_{v\in M_K} [\{\mathfrak{J}_v(\Lambda)\}, \beta]_v$$

であるとする. このとき, ある $\Lambda' := (\alpha_1, \alpha_2, \alpha_3) \in \mathrm{KS}$ に対し, 各 $v \in M_K$ で,

$$\alpha_i \cdot \frac{L_i}{L_0}(Q_v) \in \{K_v(e_i)\}^2 \tag{3.4.2}$$

を満たす C_Λ 上の K_v-有理点 Q_v が存在することがいえれば, 補題 3.3.3 より $\Lambda \in \mathrm{SD}$ であるため十分性が成り立つ. 今, 定理 3.3.24 からある $\{\Lambda' = (\alpha_1, \alpha_2, \alpha_3)\} \in \mathrm{KS}/\mathrm{KS}^2$ が存在して, 各 $v \in M_K$ に対し

$$\{\Lambda'\} \cdot \{\mathfrak{J}_v(\Lambda)\}^{-1} \in \mathrm{Im}(\delta_v)$$

となる. よってこの Λ' に対し各 $v \in M_K$ で (3.4.2) が成り立つような C_Λ 上の K_v-有理点が存在性すればよい. 上より, 各 $v \in M_v$ に対し E のある K_v-有理点 $P_v = (x_v, y_v)$ と $\lambda_v = (g_{1,v}, g_{2,v}, g_{3,v}) \in \mathrm{KS}_v$ が存在して, 各 $i(i = 1, 2, 3)$ に対し

$$\alpha_i = (x_v - e_i) \cdot g_{i,v}^2 \cdot \frac{L_i}{L_0}(Q_v)$$

となる. また, 補題 3.3.10 の (b) より各 $i(i = 1, 2, 3)$ に対し, ある $d_i \in K_v(e_i)^*$ が存在して

$$\frac{L_i/L_0(Q_v + P_v)}{(x_v - e_i) \cdot (L_i/L_0)(Q_v)} = d_i^2$$

となる. 従って各 $i(i = 1, 2, 3)$ に対し

$$\begin{aligned} \alpha_i \cdot \frac{L_i}{L_0}(Q_v + P_v) &= \alpha_i \left(d_i^2 \cdot (x_v - e_i) \cdot \frac{L_i}{L_0}(Q_v) \right) \\ &= \alpha_i \cdot d_i^2 \cdot \alpha_i \cdot g_{i,v}^{-2} \\ &= (\alpha_i \cdot d_i \cdot g_{i,v}^{-1})^2 \in K_v(e_i)^2 \end{aligned}$$

となり, 上の $Q_v + P_v$ を Q_v として取りな直せば (3.4.2) が成り立ち, 十分性が成り立つ. 以上より主定理の (c) が成り立つ.

(d) の証明. Step1 : 次の 2 つを示す.

(i) $C_\Lambda(\Lambda = (b_1, b_2, b_3)$ とする) を定義する $H_i(i = 1, 2, 3)$ において, $b_{i+1} \neq b_{i+2}$ であればある 1 次形式 $R, S \in K(e_i)[U_1, U_2, U_3]$ と $A, B, C \in K(e_i)^*$ が存在して

$$H_i(U_1, U_2, U_3, T) = AR^2 + 2BRS + CS^2 + T^2 \tag{3.4.3}$$

となる (A,B,C,R,S は当然 i に依存するが簡略化のためあえてここでは添え字を付けないことにする). さらに A かつ C が 0 でなければ $B - AC \in b_i(K(e_i)^*)^2$ を満たす.

(ii) (3.4.3) の右辺を $Q^{(i)}(R, S, T)$ とし, A かつ C が 0 でないとし, $\omega_i(i = 1, 2)$ を $Ax^2 + Bx + C = 0$ の根とする. このとき, $\{Q^{(i)}(R, S, T) = 0\} \subset \mathbb{P}^2$ 上の 2 点 $[r_1 : s_1 : t_1], [r_2 : s_2 : t_2]$ に対して

$$\prod_{i=1}^{2} \{(t_1 r_2 - t_2 r_1) - \omega_i(t_1 s_2 - t_2 s_1)\} = -t_1 t_2 W \tag{3.4.4}$$

が成り立つ (但し,

$$W = \frac{2}{A}\big\{Ar_1r_2 + B(r_1s_2 + s_1r_2) + Cs_1s_2 + t_1t_2\big\}$$
$$= \frac{1}{A}\left\{Q(r_1 + r_2, s_1 + s_2, t_1 + t_2) - Q(r_1, s_1, t_1) - Q(r_2, s_2, t_2)\right\}$$

とする).

まず, (i) については以下, 各 $i(i = 1, 2, 3)$ に対し議論し, いくつか記号を定義するが, 記号簡略化のため添え字は付けないことにする. 前半は, 今, $\lambda = e_{i+1} - e_{i+2}$ とすると $\lambda^2 \in K(e_i)$ であるため, $b_{i+1} = a+b\lambda$ かつ $b_{i+2} = a-b\lambda$ となる $a, b \in K(e_i)$ が存在する. また同様にして, $Z_{i+1} = R + S\lambda$ かつ $Z_{i+2} = R - S\lambda$ となる $R, S \in K(e_i)[U_1, U_2, U_3]$ が存在する (Z_i は (3.2.6) で与えた記号である). よって

$$\begin{aligned} H_i(U_1, U_2, U_3, T) &= \frac{b_{i+1}Z_{i+1}^2 - b_{i+2}Z_{i+2}^2}{e_{i+1} - e_{i+2}} + T^2 \\ &= \frac{(a + b\lambda)(R + S\lambda)^2 - (a - b\lambda)(R - S\lambda)^2}{\lambda} + T^2 \\ &= \frac{1}{\lambda}\left[2b\lambda R^2 + 2\{(a + b\lambda) + (a - b\lambda)\}RS + 2b\lambda^3S^2\right] + T^2 \\ &= 2bR^2 + 4aRS + 2b\lambda^2S^2 + T^2 \end{aligned}$$

となり, $A = 2b, B = 2a, C = 2b\lambda^2 \in K(e_i)$ とおけば (3.4.3) を得る. 後半は記号の与え方から

$$\begin{aligned} B^2 - AC = 4(a^2 - b^2\lambda) &= 4(a + b\lambda)(a - b\lambda) \\ &= 4b_i^{-1}b_ib_{i+1}b_{i+2} \\ &= b_i\big(2b_i^{-1}\big)^2(b_ib_{i+1}b_{i+2}) \in b_i(K(e_i)^*)^2 \end{aligned}$$

となり後半も成り立つ. 従って (i) が成り立つ.

(ii) を示す. $\omega_i(i = 1, 2)$ は $Ax^2 + Bx + C = 0$ の根であったことから, 解と係数の関係より

$$-(\omega_1 + \omega_2) = -\frac{2B}{A}, \quad \omega_1\omega_2 = \frac{C}{A}$$

であることと, $Q^{(i)}(r_1,s_1,t_1)=0, Q^{(i)}(r_2,s_2,t_2)=0$ であることから

$$
\begin{aligned}
&\prod_{i=1}^{2}\{(t_1r_2-t_2r_1)-\omega_i(t_1s_2-t_2s_1)\}\\
&=\big\{(t_1r_2-t_2r_1)-\omega_1(t_1s_2-t_2s_1)\big\}\big\{(t_1r_2-t_2r_1)-\omega_2(t_1s_2-t_2s_1)\big\}\\
&=(t_1r_2-t_2r_1)^2-(\omega_1+\omega_2)(t_1r_2-t_2r_1)(t_1s_2-t_2s_1)+\omega_1\omega_2(t_1s_2-t_2s_1)^2\\
&=\frac{1}{A}\big\{A(t_1r_2-t_2r_1)^2+2B(t_1r_2-t_2r_1)(t_1s_2-t_2s_1)+C(t_1s_2-t_2s_1)^2\big\}\\
&=\frac{1}{A}\Big[A(t_1^2r_2^2+t_2^2r_1^2-2t_1t_2r_1r_2)+2B\{t_1^2r_2s_2-t_1t_2(r_1s_2+r_2s_1)+t_2^2r_1s_1\}\\
&\qquad+C(t_1^2s_2^2+t_2^2s_1^2-2t_1t_2s_1s_2)\\
&=\frac{1}{A}\Big[t_1^2(Ar_2^2+2Br_2s_2+Cs_2^2)+t_2^2(Ar_1^2+2Br_1s_1+Cs_1^2)\\
&\qquad-2t_1t_2\{Ar_1r_2+B(r_1s_2+r_2s_1)+Cs_1s_2\}\Big]\\
&=\frac{1}{A}\Big[t_1^2(-t_2^2)+t_2^2(-t_1^2)-2t_1t_2\{Ar_1r_2+B(r_1s_2+r_2s_1)+Cs_1s_2\}\Big]\\
&=-t_1t_2\Big[\frac{2}{A}\big\{Ar_1r_2+B(r_1s_2+s_1r_2)+Cs_1s_2+t_1t_2\big\}\Big]
\end{aligned}
$$

となり (3.4.4) が成り立つ.

Step2 : 主定理の (d) を示す. $\alpha=\beta$ のとき $\langle\alpha,\beta\rangle=1$ を示すが, ここで主定理の (a) から α,β の代表元として $\Lambda=\{b_1,b_2,b_3\}$ としてよく, 適当に e_i の添え字を入れかえることによって $b_2=b_3=b'$ となるときとそうでないときで場合分けする.

まず, 後者のときを示す. $Q_i:=[r_1:s_1:t_1]$ を X_i 上の $K(e_i)$-有理点とし ($X_i:\{Q^{(i)}(R,S,T)=0\}$ であった), 各 $v\in M_K$ に対する C_Λ 上の K_v-有理点 Q_v に対し $[r_2:s_2:t_2]:=\psi_i\circ\phi_4^{(i)}(Q_v)$ とし, このときの (3.4.4) における左辺を $l_i\in K(e_i)$ とし, W の値を W_i とする. このとき, X_i,L_i,W の与え方から, $L_i(Q_v)=W_i$ であり, A,B,C,ω_1,ω_2 の与え方と Step1 の (i) の後半から各 $i(i=1,2,3)$ に対し

$$K(\omega_1,\omega_2,e_i)=K(\omega_1,e_i)=K(\omega_2,e_i)=K(\sqrt{b_i},e_i)$$

ゆえ, $V_i=(t_1r_2-t_2r_1)-\omega_1(t_1s_2-t_2s_1)$ とすれば $l_i=\mathrm{N}_{K(\sqrt{b_i},e_i)/K}(V_i)$ であることから命題 (1.0.13) の (d) より

$$(l_i,b_i)_{K(e_i)}=(V_i,b_i)_{K(\sqrt{b_i},e_i)}=\Big(V_i,\big(\sqrt{b_i}\big)^2\Big)_{K(\sqrt{b_i},e_i)}=1$$

となる. よって, 各 $i(i=1,2,3)$ に対して $l_i=-t_1t_2L_i(Q_v)$ より

$$(L_i(Q_v),b_i)_{K(e_i)}=(-t_1,b_i)_{K_v(e_i)}(t_2,b_i)_{K_v(e_i)}$$

であることから, 補題 3.3.25 より

$$\begin{aligned}\langle \alpha, \alpha \rangle &= \prod_{v \in M_K} \prod_{\{i\} \in \mathfrak{I}_{K_v}} (L_i(Q_v), b_i)_{K_v(e_i)} \\ &= \left\{ \prod_{v \in M_K} \prod_{\{i\} \in \mathfrak{I}_{K_v}} (-t_1, b_i)_{K_v(e_i)} \right\} \left\{ \prod_{v \in M_K} \prod_{\{i\} \in \mathfrak{I}_{K_v}} (t_2, b_i)_{K_v(e_i)} \right\}\end{aligned}$$

となる. ここで, 右辺の左側の積の値については $-t_1, b_i \in K(e_i)^*$ より補題 3.3.23 の証明と同様の議論から 1 であることがいえる. 次に右辺の右側の積の値については KS の与え方から $b_1 b_2 b_3 = b^2$ となる $b \in K^*$ が存在し, 射 $\psi_i \circ \phi_4^{(i)}$ の与え方 (2.4.34) から $t_2 \in K_v$ であるため, 各 $v \in M_K$ に対し

$$\prod_{\{i\} \in \mathfrak{I}_{K_v}} (t_2, b_i)_{K_v(e_i)} = (t_2, b_1 b_2 b_3)_{K_v} = \left(t_2, b^2\right)_{K_v} = 1$$

となり, 以上から $\langle \alpha, \alpha \rangle = 1$ となる.

次に前者を示すが, 前者は適当に e_i の添え字を入れかえることによって $b_2 = b_3 = b'$ となるときであり, (a) から $b_1 = 1$ としてよい. ここで, $b' = 1$(すなわち $\Lambda = (1, 1, 1)$) であれば明らかに $\langle \alpha, \alpha \rangle = 1$ であるため $b' = 1$ でないとする. このとき, KS の与え方から $e_1 \in K$ であり, Λ の与え方から L_2, L_3 に対して, 後者のときと同様に Step1 の (i), (ii) を適用する. すると, 各 $i (i = 2, 3)$ に対し各 $v \in M_K$ で

$$(L_i(Q_v), b_i)_{K(e_i)} = (-t_1, b')_{K_v(e_i)} (t_2, b')_{K_v(e_i)}$$

となる (後者のときと同じ記号を用い, $t_1 \in K(e_i)^*$ であり, t_2 は i に寄らない). よって, 自明な等式

$$(L_1(Q_v), 1)_{K_v(e_1)} = (-1, 1)_{K_v(e_1)} (t_2, 1)_{K_v(e_1)}$$

から $i = 1$ のときの $-t_1$ を -1 とすることによって

$$\begin{aligned}\langle \alpha, \alpha \rangle &= \prod_{v \in M_K} \prod_{\{i\} \in \mathfrak{I}_{K_v}} (L_i(Q_v), b_i)_{K_v(e_i)} \\ &= \left\{ \prod_{v \in M_K} \prod_{\{i\} \in \mathfrak{I}_{K_v}} (-t_1, b_i)_{K_v(e_i)} \right\} \left\{ \prod_{v \in M_K} \prod_{\{i\} \in \mathfrak{I}_{K_v}} (t_2, b_i)_{K_v(e_i)} \right\}\end{aligned}$$

となり, 後者のときと同様にすれば $\langle \alpha, \alpha \rangle = 1$ を得る. 以上より (d) が成り立つ.

以上より, $S^{(2)}$ と同型な FD/KS^2 に対して構成した pairing $\langle \cdot, \cdot \rangle$ に対し主定理が成り立つ. □

4 pairing $\langle\cdot,\cdot\rangle$ の再構成 (特別な場合)

$\langle\cdot,\cdot\rangle$ の構成の際用いた楕円曲線 (3.2.1) は以下の 3 つに場合分けされる.

(a) $e_i \in K$ $(i=1,2,3)$ である.

(b) ある i のみ $e_i \in K$ である

(c) $e_i \notin K$ $(i=1,2,3)$ である.

ここでは計算しやすくするため, (a) の場合に対して簡単に pairing $\langle\cdot,\cdot\rangle$ を与える.

Step1 : $S^{(2)}$ を簡単に与える.

命題 4.0.5. (3.2.1) の形で与えられた楕円曲線 E/K が上の (a) を満たすとする. このとき KS, FD はそれぞれ以下で与えられる.

$$\mathrm{KS} = \left\{ \Lambda = (b_1,b_2,b_3) \in \prod_{i=1}^{3} K^* \ ; \ b_1b_2b_3 \in K^{*2} \right\}$$
$$\mathrm{FD} = \{\Lambda \in \mathrm{KS} \ ; \ \text{各 } v \in M_K \text{ に対し, } C_\Lambda(K_v) = \emptyset\}$$

(但し, $\Lambda = (b_1,b_2,b_3) \in \mathrm{KS}$ に対する C_Λ は

$$C_\Lambda : \left\{ H_i := b_{i+1}Z_{i+1}^2 - b_{i+2}Z_{i+2}^2 + (e_{i+1}-e_{i+2})T^2 = 0 \ ; \ i=1,2,3 \right\}$$

で与えられる $\mathbb{P}^3$ の 3 つ 2 次曲面の intersection とする). 従って $S^{(2)} \cong \mathrm{FD}/\mathrm{KS}^2$ を得る.

Step2 : $S^{(2)}$ 上の pairing $\langle\cdot,\cdot\rangle$ を簡単に与える.

命題 4.0.6. (3.2.1) の形で与えられた楕円曲線 E/K が上の (a) を満たすとする. このとき $S^{(2)}$ 上の pairing $\langle\cdot,\cdot\rangle$ は次で与えられる. まず, $\alpha = \{\Lambda\} \in \mathrm{FD}/\mathrm{KS}^2$ に対する C_Λ において, 各 $i(i=1,2,3)$ に対し Q_i を円錐曲線 $Y_i : \{H_i = 0\} \subset \mathbb{P}^2$ の $\mathbb{Q}$-有理点として取り, さらに添え字を mod 3 で与えたとき 1 次形式

$$L_i := a_{i+1}Z_{i+1} + a_{i+2}Z_{i+2} + aT \quad (a_{i+1}, a_{i+2}, a \in \mathbb{Q})$$

を $L_i = 0$ が Q_i における Y_i の接線となるように取る. また, FD の与え方から各 $v \in M_\mathbb{Q}$ に対して $L_i(Q_v) \neq 0$ となる C_Λ 上の $\mathbb{Q}_v$-有理点を取る. これより, $\alpha = \{\Lambda\}, \beta = \{(c_1,c_2,c_3)\} \in \mathrm{FD}/\mathrm{KS}^2$ に対して

$$\langle \alpha, \beta \rangle = \prod_{v \in M_\mathbb{Q}} \prod_{i=1}^{3} (L_i(Q_v), c_i)_v$$

(但し, $(\cdot,\cdot)_v$ を Hilbert 記号とする) となる.

5　主定理を用いた計算例

主定理を用いて $\mathbb{Q}$ 上定義された楕円曲線

$$E/\mathbb{Q} : y^2 = x(x-343)(x+59049)$$

の $\mathrm{SD}/\mathrm{KS}^2$ を計算する. この楕円曲線は [8, p. 120] より引用したもので Cassels の論文 [6] でも計算はなされている. $Ш(E/\mathbb{Q})[2] \neq \{0\}$ であることから $E(\mathbb{Q})/2E(\mathbb{Q}) \subsetneq \mathrm{FD}/\mathrm{KS}^2 (\cong S^{(2)})$ であり, $E(\mathbb{Q})_{\mathrm{tors}}$ と $\mathrm{SD}/\mathrm{KS}^2$ を計算することによって $\mathrm{rank}E(\mathbb{Q}) = 0$ を得る. 以下の Step でそれらを計算していくことにする.

Step1 : $E(\mathbb{Q})_{\mathrm{tors}}$ を求める. まず, 例 2.1.40 より

$$E[2] = E(\mathbb{Q})[2] = \{O, (0,0), (343,0), (-59049,0)\} \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$$

である. 一方,

$$\begin{aligned} \Delta(E) &= -16 \cdot 343^2 \cdot 59049^2 \cdot (343+59049)^2 \\ &= -16 \cdot 7^3 \cdot 3^{10} \cdot 2^{11} \cdot 29 \end{aligned}$$

より $5 \nmid \Delta(E)$ であることから $E[2] \subset E(\mathbb{Q})_{\mathrm{tors}} \hookrightarrow \tilde{E}(\mathbb{F}_5)$ となり,

$$\#\tilde{E}(\mathbb{F}_5) = 4$$

であることから $E(\mathbb{Q})_{\mathrm{tors}}$ は位数 4 の部分群をもち, 位数 4 の群の部分群である. 従って, $E(\mathbb{Q})_{\mathrm{tors}} = E[2] \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ であり, 自明でない 4-torsion point が存在しないことから $E(\mathbb{Q})_{\mathrm{tors}} \subset E(\mathbb{Q})/2E(\mathbb{Q})$ とみなせる.

Step2 : $\mathrm{FD}/\mathrm{KS}^2$ を求める. $\mathrm{FD}/\mathrm{KS}^2$ が

$$\mathrm{FD}/\mathrm{KS}^2 = \langle (-1,-1,1), (1,2,2), (7,7,1), (1,29,29) \rangle \tag{5.0.7}$$

となることを示す. 命題 2.5.8 から

$$S := \{\infty, 2, 3, 7, 29\} \subset M_{\mathbb{Q}}$$

とすれば, 節 2.6 の Step1 から

$$S^{(2)} \subset H^1(K, E[2];\ S) \cong \mathbb{Q}_S^*/{\mathbb{Q}_S^*}^2 \times \mathbb{Q}_S^*/{\mathbb{Q}_S^*}^2$$

である. よって, 命題 3.2.8 における $H^1(K, E[2])$ と $\mathrm{KS}/\mathrm{KS}^2$ との対応と節 2.6 の Step1 から

$$H^1(K, E[2];\ S) \cong \langle (k,k,1), (k,1,k,), (1,k,k)\ ;\ k \in \{-1,2,3,7,19\} \rangle \subset \mathrm{KS}/\mathrm{KS}^2 \tag{5.0.8}$$

である. ここで, 上における中央の集合を A とし, $\Lambda := (b_1, b_2, b_3) \in \mathrm{KS}/\mathrm{KS}^2$ に対応する C_Λ は命題 4.0.5 より

$$C_\Lambda : \begin{cases} H_1 = b_2 Z_2^2 - b_3 Z_3^2 + 2^{11} \cdot 29 T^2 = 0 \\ H_2 = -b_1 Z_1^2 + b_3 Z_3^2 - 3^{10} T^2 = 0 \\ H_3 = b_1 Z_1^2 - b_2 Z_2^2 - 7^3 T^2 = 0 \end{cases}$$

であり, 節 2.6 の Step2 より $\Lambda \in A$ が $\mathrm{FD}/\mathrm{KS}^2$ の元となるための必要十分条件は C_Λ が各 $v \in S$ で $\mathbb{Q}_v$-有理点をもつことである.

始めに A の生成元をみていく. まず, $\Lambda = (-1, 1, -1)$ に対して C_Λ は $\mathbb{R}$-有理点をもたない. なぜなら $\{H_1 = 0\} \subset \mathbb{P}^3$ 上の $\mathbb{R}$-有理点は $[1 : 0 : 0 : 0]$ のみであるが, この点は $\{H_3 = 0\} \subset \mathbb{P}^3$ 上にはないからである. よって, $(-1, 1, -1)$ は $\mathrm{FD}/\mathrm{KS}^2$ の元ではない. 全く同様にして $(1, -1, -1)$ もまた $\mathrm{FD}/\mathrm{KS}^2$ の元ではない. 次に $\Lambda = (2, 2, 1)$ に対して C_Λ は $\mathbb{Q}_2$-有理点をもたない. なぜなら C_Λ が $\mathbb{Q}_2$-有理点をもつと仮定すれば, 2 の何乗かを各成分に掛けることにより, その $\mathbb{Q}_2$-有理点の成分を各成分の order が 0 以上であって少なくとも 1 つの成分の order が 0 となるような $[z_1 : z_2 : z_3 : t]$ として取り直すことができ,

$$0 = \frac{1}{2} H_1(z_1, z_2, z_3, t) = 2^{11} \cdot 29 t^2 + 2 z_2^2 - z_3^2 \equiv -z_3^2 \pmod 2$$

より $z_3 \equiv 0 \pmod 2$ となり, 再びこの等式を mod 4 で考えれば $z_2 \equiv 0 \pmod 2$ であり, このことから $H_3 = 0$ を mod 2 で考えれば $t \equiv 0 \pmod 2$ となり, また同様にして $z_1 \equiv 0 \pmod 2$ ゆえ, 各成分の order が 1 以上となり, 各成分の取り方に矛盾するからである. これと同様にして,

$$\begin{array}{llll} (2,1,2), & (3,3,1), & (3,1,3), & (1,3,3), \\ (7,1,7), & (1,7,7), & (29,29,1), & (29,1,29), \end{array}$$

もまた $\mathrm{FD}/\mathrm{KS}^2$ の元ではない.

次に, 任意の $\Lambda \in A$ は $(k,k,1), (k,1,k), (1,k,k,)(k \in -1, 2, 3, 7, 29$ の幾つかの積で表されているが, $\mathrm{KS}/\mathrm{KS}^2$ で考えているため 2 乗のものを除いて考えてよい. このとき, Λ に $(-1,1,-1)$ が含まれておりかつ $(1,-1,-1)$ と $(-1,-1,1)$ が含まれていなければ, 上で述べた $(-1,1,-1)$ が $\mathrm{FD}/\mathrm{KS}^2$ の元でないことと同様にして Λ は $\mathrm{FD}/\mathrm{KS}^2$ の元ではない. また $(1,-1,-1)$ が含まれておりかつ $(-1,1,-1)$ と $(-1,-1,1)$ が含まれていなくても同様の理由により $\mathrm{FD}/\mathrm{KS}^2$ の元でない. さらに, これと同じように Λ に上で挙げた $\mathrm{FD}/\mathrm{KS}^2$ の元ではないものが含まれているならばその元が入らないのと同様の理由により Λ は $\mathrm{FD}/\mathrm{KS}^2$ に入らない. 従って,

$$\mathrm{FD}/\mathrm{KS}^2 \subset \langle (-1,-1,1), (1,2,2), (7,7,1), (1,29,29) \rangle \tag{5.0.9}$$

である. ここで命題 3.2.8 から $E(K)/2E(K) \to \mathrm{KS}/\mathrm{KS}^2$ により

$$\begin{aligned} O &\mapsto (1,1,1) \\ (0,0) &\mapsto (-7,-7,1) \\ (343,0) &\mapsto (7, 2\cdot 7\cdot 29, 2\cdot 29) \\ (-59049,0) &\mapsto (-1, -2\cdot 29, 2\cdot 29) \end{aligned}$$

であるため, $(1,2,2)$ と $(7,7,1)$ が $\mathrm{FD}/\mathrm{KS}^2$ の元となることをいえば

$$(-1,-1,1) = (7,7,1)(-7,-7,1) \in \mathrm{FD}/\mathrm{KS}^2$$

であり,

$$(1,29,29) = (-1,-1,1)(1,2,2)(-1,-2\cdot 29, 2\cdot 29) \in \mathrm{FD}/\mathrm{KS}^2$$

となるため (5.0.7) が成り立つ. よって, $C_{(7,7,1)}$ と $C_{(1,2,2)}$ が各 $v \in S$ で $\mathbb{Q}_v$-有理点をもつことをいう.

まず $C_{(7,7,1)}$ において, 点 $[z_1 : z_2 : z_3 : 0] \in C_{(7,7,1)}$ は

$$7z_2^2 - z_3^2 = z_3^2 - 7z_1^2 = 7z_1^2 - 7z_2^2 = 0$$

を満たすため, 各 $v \in S$ に対し $7x_v^2 - y_v^2 = 0$ を満たす $x_v, y_v \in \mathbb{Q}_v$ が存在することがいえれば, 各 $v \in S$ に対し $[x_v : x_v : y_v : 0]$ は $C_{(7,7,1)}$ 上の $\mathbb{Q}_v$-有理点となる. よってそれを示す. まず $v = \infty$ のときは明らか. $v = 2, 3, 7, 29$ のとき, それぞれ, $7x^2 - y^2$ は mod 16 で $(x,y) = (1,5)$ mod 3 で $(x,y) = (2,5)$, mod 7 で $(x,y) = (1,0)$, mod 29 で $(x,y) = (1,6)$ を根にもち, それぞれ, Hensel の補題 (補題 1.0.10) の適用条件を満たすことから, このとき $7x_v^2 - y_v^2 = 0$ を満たす $x_v, y_v \in \mathbb{Q}_v$ が存在する. よって, $C_{(7,7,1)}$ は各 $v \in S$ で $\mathbb{Q}_v$-有理点をもつ.

次に $C_{(1,2,2)}$ において $C_{(1,2,2)}$ は

$$C_\Lambda : \begin{cases} H_1 = Z_2^2 - Z_3^2 + 2^{10}\cdot 29T^2 = 0 \\ H_2 = -Z_1^2 + 2Z_3^2 - 3^{10}T^2 = 0 \\ H_3 = Z_1^2 - 2Z_2^2 - 7^3T^2 = 0 \end{cases}$$

である. $v = \infty$ のときは $C_{(7,7,1)}$ のときと同様にして $\mathbb{R}$-有理点をもつ. $v = 2$ のとき, $T = Z_3 = 1$ と仮定して Q_2-有理点をもつことをいう. このとき $H_1 = 0$ から

$$Z_2^2 = 1 - 29\cdot 2^{10} \equiv 1 \pmod{16}$$

より $Z \equiv 1 \pmod{16}$ から Hensel の補題を使えば $z_2^2 = 1 - 29\cdot 2^{10}$ を満たす $z_2 \in \mathbb{Q}_2$ が存在する. また $H_2 = 0$ から

$$Z_1^2 = 2 - 3^{10} \equiv 9 \pmod{16}$$

より $Z_1 \equiv 5 \pmod{16}$ から Hensel の補題を使えば $z_1^2 = 2 - 3^{10}$ を満たす $z_1 \in \mathbb{Q}_2$ が存在する. よって $[z_1 : z_2 : 1 : 1]$ が $C_{(1,2,2)}$ 上の $\mathbb{Q}_2$-有理点となる. $v = 3, 7, 29$ のときもこれと同様にして $C_{(1,2,2)}$ 上の $\mathbb{Q}_2$-有理点の存在性を示すことができる. よって, $C_{(1,2,2)}$ は各 $v \in S$ で $\mathbb{Q}_v$-有理点をもつ. 従って,

$$\begin{aligned} \mathrm{FD}/\mathrm{KS}^2 &= \langle (-1,-1,1), (1,2,2), (7,7,1), (1,29,29) \rangle \\ &= \langle (-7,-7,1), (7, 2\cdot 7\cdot 29, 2\cdot 29), (1,2,2), (1,7,7) \rangle \end{aligned} \tag{5.0.10}$$

である.

Step3 : $\mathrm{SD}/\mathrm{KS}^2$ を求める. $\mathrm{SD}/\mathrm{KS}^2$ が

$$\mathrm{SD}/\mathrm{KS}^2 = \langle (-7,-7,1), (7, 2\cdot 7\cdot 29, 2\cdot 29) \rangle \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \tag{5.0.11}$$

となることを示す. これがいえれば

$$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \cong E(\mathbb{Q})_{\mathrm{tors}} \subset E(\mathbb{Q})/2E(\mathbb{Q}) \subset \mathrm{SD}/\mathrm{KS}^2 \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$$

より $\mathrm{rank} E(\mathbb{Q}) = 0$ となる. ここで (5.0.11) は主定理 3.1.1 の (c), (d) から

$$\langle (1,2,2), (1,7,7) \rangle = -1$$

をいえば十分である. 今, $C_{(1,2,2)}$ は

$$C_{(1,2,2)} : \begin{cases} H_1 = 2Z_2^2 - 2Z_3^2 + 2^{11}\cdot 29 T^2 = 0 \\ H_2 = -Z_1^2 + 2Z_3^2 - 3^{10} T^2 = 0 \\ H_3 = Z_1^2 - 2Z_2^2 - 7^3 T^2 = 0 \end{cases}$$

である. これより各 $i (i = 1, 2, 3)$ に対し, $\{H_i = 0\} \subset \mathbb{P}^2$ の $\mathbb{Q}$-有理点 Q_i として

$$\begin{aligned} Q_1 &: [z_2 : z_3 : t] = [1 : -1 : 0], \\ Q_2 &: [z_1 : z_3 : t] = [3^5 : 3^5 : 1], \\ Q_3 &: [z_1 : z_2 : t] = [21 : 7 : 1] \end{aligned}$$

を取り, Q_i における $\{H_i = 0\} \subset \mathbb{P}^2$ の接線であって Z_i の係数が 0 となる 1 次形式 $L_i \in K[Z_1, Z_2, Z_3, T]$ としてそれぞれ,

$$\begin{aligned} L_1 &= Z_2 + Z_3, \\ L_2 &= Z_1 - 2Z_3 + 3^5 T, \\ L_3 &= 3Z_1 - 2Z_2 - 7^2 T \end{aligned}$$

を取れば $7 \in \mathbb{Q}_v^2 (v = \infty, 3, 29)$ であることから, Hilbert 記号の性質 (命題 1.0.13) より pairing における Hilbert 記号は $v = 2, 7$ 以外の素点で 1 となる. よって, Hensel

の補題 (補題 1.0.10) を使うことにより Q_2 は $[\alpha : \beta : 1 : 1] \in C_\Lambda(\mathbb{Q}_2)$ として取り (但し, $\alpha, \beta \in \mathbb{Q}_2$ はそれぞれ, $\alpha \equiv 5 \pmod{16}$, $\beta \equiv 1 \pmod{16}$ を満たす), Q_7 は $[\alpha' : 3 : \gamma' : 1] \in C_\Lambda(\mathbb{Q}_7)$ として取れば (但し, $\alpha', \gamma' \in \mathbb{Q}_7$ はそれぞれ, $\alpha' \equiv 2 \pmod 7$, $\gamma' \equiv 2 \pmod 7$ を満たす),

$$\begin{aligned}
L_1(Q_2) &\equiv 1 + 1 \equiv 2 \pmod{16} \\
L_2(Q_2) &\equiv 5 - 2 \cdot 1 + 3^5 \cdot 1 \equiv 6 \pmod{16} \\
L_1(Q_7) &\equiv 3 + 2 \equiv 5 \pmod 7 \\
L_2(Q_7) &\equiv 2 - 2 \cdot 2 + 3^5 \cdot 1 \equiv 3 \pmod 7
\end{aligned}$$

ゆえ,

$$\begin{aligned}
\langle (1,2,2), (1,7,7) \rangle &= (L_1(Q_2), 7)_2 (L_2(Q_2), 7)_2 (L_3(Q_3), 1)_2 \\
&\qquad \times (L_1(Q_7), 7)_7 (L_2(Q_7), 7)_7 (L_3(Q_7), 1)_7 \\
&= (L_1(Q_2), 7)_2 (L_2(Q_2), 7)_2 (L_1(Q_7), 7)_7 (L_2(Q_7), 7)_7 \\
&= (2, 7)_2 (6, 7)_2 (5, 7)_7 (3, 7)_7 \\
&= (2, 7)_2{}^2 (3, 7)_2 (5, 7)_7 (3, 7)_7 \\
&= (-1)^{\frac{3-1}{2} \cdot \frac{7-1}{2}} \times \left(\frac{5}{7}\right) \left(\frac{3}{7}\right) \\
&= 1 \cdot (-1)(-1)(-1) \\
&= -1
\end{aligned}$$

となる. 従って $\mathrm{SD}/\mathrm{KS}^2 \cong (\mathbb{Z}/2\mathbb{Z})^2$ となり, $\mathrm{rank} E(\mathbb{Q}) = 0$ である.

参考文献

[1] Z.I. Borevich and I.R. Shafarevich. *Number theory.* Academic Press, New York, San Francisco, London, 1966.

[2] Brumer, A. and Kramer, K. The rank of elliptic curves. *Duke Math. J.* no.4, 44:715–743, 1977.

[3] Cassels, L. W. S. Arithmetic on curves of genus 1. III. the Tate-Šafarevič and Selmer groups. *Proc. London Math. Soc.* (3), 12:259–296, 1962.

[4] Cassels, L. W. S. Diophantine equations with special reference to elliptic curves. *J. London Math. Soc.*, 41:193–291, 1966.

[5] Cassels, L. W. S. *Lectures on elliptic curves*, volume 24 of *London Mathematical Society Student Texts.* Cambridge University Press, Cambridge, 1991.

[6] Cassels, L. W. S. Second descents for elliptic curves. *J. Reine Angew. Math.*, 494:101–127, 1998.

[7] C. Chevalley. *Class Field Theory*. Nagoya University, Nagoya, 1954.

[8] B. M. M. de Weger. A+B=C and big Ш's. *Quart. J. Math. Oxford (2)*, 49:105–128, 1998.

[9] R. Hartshorne. *Algebraic geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, Heidelberg, New York, 1977.

[10] Anthony W. Knapp. *Elliptic curves*, volume 40 of *Mathematical Notes*. Princeton University Press, Princeton, 1992.

[11] S. Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[12] R. Martin and W. McMillen. An elliptic curve over q with rank at least 24. Number Theory Listserver, May 2000.

[13] O.T. O'Meara. *Introduction to quadratic forms*, volume Bd. 117 of *Die Grundlehren der mathematischen Wissenschaften* . Springer-Verlag, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1963.

[14] J.P. Serre. *A Course in Arithmetic*, volume 7 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, Heiderberg, New York, 1973.

[15] J.P. Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, New York, 1979.

[16] J.H. Silverman. *The Arthmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[17] J. Tate. The Arithmetic of Elliptic Curves. *Invent. Math.*, 23:179–206, 1974.

[18] 岩澤 健吉. **局所類体論**. 岩波書店, 1980.