On $\sqrt{2}$-divison points of hyperelliptic curves of genus 2

橋本 喜一朗 (早稲田大学)　酒井 祐貴子 (早稲田大学)

1　はじめに

本稿では, $\sqrt{2}$ 乗法を持つ種数 2 の曲線に対して, その Jacobi 多様体の 2 等分点および $\sqrt{2}$ 等分点について考察する.

その内容は 2007 年 12 月の数理研における研究集会「代数的整数論とその周辺」でお話した「$\sqrt{2}$ 乗法を持つ種数 2 の generic な曲線族について」の結果の考察から, その後得られた結果の一つである. 数理研での講演の中では, 判別式 $\Delta = 5, 8$ の実乗法を持つ種数 2 の曲線とその曲線上の代数対応を, 射影平面上の 2 次曲線に関する幾何学を応用する初等的な方法で構成し, さらに代数対応が引き起こす写像が, $\mathrm{End}_{\mathbb{C}}(\mathrm{Jac}(X))$ において判別式 $\Delta = 5, 8$ の実二次体の整数環の生成元となることを示した.

我々の大きな目標は, これらの結果をさらに一般化し, 判別式が $\Delta > 8$ をみたす実乗法を持つ種数 2 の曲線を構成することである. さしあたり $\Delta = 12$, すなわち $\sqrt{3}$ 乗法を持つ種数 2 の曲線族を見つけることが当面の課題であるが, $\sqrt{3}$ の場合, 数理研における講演で述べたような Poncelet の定理による構成方法をそのまま用いてもうまくいかない. 従って, $\sqrt{3}$ 乗法を特徴付ける構造の詳しい研究, すなわち曲線の Jacobi 多様体の $\sqrt{3}$ 等分点の全体からなる群を調べることが必要である. そこで本稿では, すでに構成されている $\sqrt{2}$ 乗法を持つ曲線 X について, その $\sqrt{2}$ 等分点の全体からなる群を調べ, 次のような結果が得られた. 今後はこれを手掛かりとして研究を進めていきたい.

Theorem 1.1. $\sqrt{2}$ 乗法 $\phi : \mathrm{Pic}^0(X) \to \mathrm{Pic}^0(X), \phi^2 = \mathrm{id}$ を持つ曲線 X について, $\sqrt{2}$ 等分点の全体からなる群 $\mathrm{Ker}\phi$ は Weil pairing に関して $\mathrm{Pic}^0(X)[2]$ の maximal isotropic subgroup をなす.

2　Humbert の結果

数理研での講演と多少重複するが, 後半で使う結果を述べておく.

射影平面 $\mathbb{P}^2$ の双対空間を $(\mathbb{P}^2)^* = \{\mathbb{P}^2$ 内の直線 $\}$, また, $D \subset \mathbb{P}^2$ を 2 次曲線 (conic) としたとき D^* で D の接線全体の集合を表すことにする. 本稿を通じて, D_0, D_1 は 4 点で交わる射影平面 $\mathbb{P}^2$ 上の相異なる 2 次曲線を表すものとする. D_0 上の点列 $K = (P_1, \ldots, P_{n+1})$ が D_1 に関する Poncelet の折れ線である, とは $P_{i+1} \neq P_{i-1}$ かつ P_i と P_{i+1} を結ぶ直線 P_iP_{i+1} が全て D_1 に接することをいう. 更に $P_1 = P_{n+1}$ のとき K を Poncelet の n 角形という.

Theorem 2.1 (Poncelet, 1822). D_0, D_1 を 4 点で交わる射影平面 $\mathbb{P}^2$ 上の相異なる 2 次曲線, n を 3 以上の整数とする. このとき $P_iP_{i+1} \in {D_1}^*, P_{n+1} = P_1$ $(1 \leq i \leq n)$ をみたす D_0 上の n 個の点列が存在するなら, 任意の $Q_1 \in D_0$ に対し $Q_iQ_{i+1} \in {D_1}^*, Q_{n+1} = Q_1$ をみたす点列 $Q_2, \ldots, Q_{n+1}$ が存在する.

Humbert はテータ関数や Kummer 曲面の理論を用いて Poncelet の多角形と判別式 $\Delta = 5, 8$ の実乗法を持つ種数 2 の曲線との関係を導いた. $\Delta = 8$ の場合, その結果は次のように述べられる.

Theorem 2.2 (Humbert [5]). $K = (P_1, \ldots, P_4)$ を D_0, D_1 に対する Poncelet の 4 角形とし, P_5, P_6 を D_0 と D_1 の交点とする. このとき, D_0 の 2 重被覆 X でその分岐点がちょうど $\{P_1, \ldots, P_6\}$ となるものは種数 2 の曲線で, その Jacobi 多様体は二つの楕円曲線の積に分解する ($\Delta = 4$ の場合) か, $\Delta = 8$ の実乗法を持つ. 後者の場合は $\mathbb{Z}[\sqrt{2}] \subseteq \mathrm{End}(\mathrm{Jac}X)$ となる.

Theorem 2.3 (Humbert [5]). X を次式で定義される種数 2 の曲線とする.

$$X : y^2 = x(x - x_1)(x - x_2)(x - x_3)(x - x_4).$$

このとき, $\mathrm{Jac}(X)$ が $\Delta = 8$ の実乗法を持つ必要十分条件は $x_1, \ldots, x_4$ の適当な並べ替えに対して等式 $H_8(x_1, \ldots, x_4) = 0$ が成立することである. ここに H_8 は

$$\begin{aligned} H_8(x_1, x_2, x_3, x_4) = 4x_1x_2x_3x_4\Big((x_1 + x_3)(x_2 + x_4) - 2(x_1x_3 + x_2x_4)\Big)^2 \\ - (x_1 - x_3)^2(x_2 - x_4)^2(x_1x_3 + x_2x_4)^2. \end{aligned}$$

3 平面 2 次曲線上の代数対応

実乗法を持つ代数曲線の構成において重要になるのが平面 2 次曲線 (conic) に対する Poncelet 型の代数対応 T である. D_0, $D_1 \subset \mathbb{P}^2$ を 4 点で交わる 2 次曲線, P を D_0 上の一般の点とすると P から D_1 には 2 本の接線 ℓ, ℓ' が引け, それぞれの D_0 との (P とは異なる) 交点 Q_1, Q_1' が得られる. このようにして $P \mapsto \{Q_1, Q_1'\}$ なる 2 次の代数対応

$$T = \{(P, Q) \in D_0 \times D_0 \mid \ell := PQ \in {D_1}^*\}$$

が得られる. 最初の問題は, T の定義方程式を具体的に求めることであるが, ここでは簡単のため, D_0 を

$$D_0 : y = x^2 \tag{1}$$

と取り, $D_0 \ni (x, x^2) \mapsto x \in \mathbb{P}^1$ によって D_0 と $\mathbb{P}^1$ を同一視する. もう一方の 2 次曲線 D_1 は一般形

$$D_1 : c_6 + c_4x + c_1x^2 + c_5y + c_3xy + c_2y^2 = 0, \quad c_i \in \mathbb{C} \tag{2}$$

で与えておく. このとき, 上記の代数対応を考えると, D_0 上の一般の位置にある 2 点 $P = (x, x^2)$, $Q = (z, z^2)$ を通る直線が D_1 に接する条件を書き下すことにより次の結果を得る. $\mathbb{P}^2$ における 2 つの 2 次曲線 D_0, D_1 が上式 (1), (2) で与えられるとき, D_0 上の Poncelet 型の代数対応 T の定義方程式は次式で与えられる:

$$A_1(x, z) := a_6 + a_4xz + a_1x^2z^2 + a_5(x + z) + a_2xz(x + z) + a_3(x + z)^2 = 0, \tag{3}$$

$$\begin{aligned} (a_1, a_2, a_3, a_4, a_5, a_6) = (-4c_1c_2 + c_3^2, -2(2c_2c_4 - c_3c_5), c_5^2 - 4c_2c_6 \\ - 2(c_3c_4 - 2c_1c_5), 2(c_4c_5 - 2c_3c_6), c_4^2 - 4c_1c_6). \end{aligned} \tag{4}$$

ここで, $A_1(x,z)$ は x,z の対称式で各変数について 2 次式であることに注意する. また, (4) を逆に解いて $\{a_i\}$ から $\{c_i\}$ を求めるには根号が必要だが, 次の結果は 2 次曲線 D_1 が $A_1(x,z)$ から有理的に決定されることを示している. $c_1,\dots,c_6$ を独立変数とし,

$$\lambda := 8({c_2}{c_4}^2 - c_3c_4c_5 + c_1{c_5}^2 - 4c_1c_2c_6 + {c_3}^2c_6)$$

とおく. $\lambda \neq 0$ のとき, $(a_1,\dots,a_6)$ を (4) で定めると次の恒等式が成立する:

$$\begin{cases} \lambda c_1 = ({a_4}^2 - 4a_1a_6)/2, \\ \lambda c_2 = ({a_2}^2 - 4a_1a_3)/2, \\ \lambda c_3 = a_2a_4 - 2a_1a_5, \\ \lambda c_4 = a_4a_5 - 2a_2a_6, \\ \lambda c_5 = 2a_3a_4 - a_2a_5, \\ \lambda c_6 = ({a_5}^2 - 4a_3a_6)/2. \end{cases}$$

次に上で述べた代数対応 T の合成を考える. $T^2 = T\circ T$ は 4 価の代数対応になるが, 定義よりそのうちの 2 価は恒等写像であり, 残りの 2 価の部分が長さ 2 の Poncelet の折れ線によって得られる点を対応させる代数対応 T_2 を定める. 作図からわかることだが, T_2 の定義方程式 $A_2(x,z)=0$ は終結式を用いて

$$A_2(x,z) = \frac{1}{(x-z)^2}\mathrm{Res}_u\Big(A_1(x,u),\, A_1(z,u)\Big)$$

によって与えられる. 右辺の $(x-z)^2$ は恒等写像にあたる部分である. 係数を整理すれば $A_2(x,z)$ は (3) と同様に

$$A_2(x,z) = a'_6 + a'_4xz + a'_1x^2z^2 + a'_5(x+z) + a'_2xz(x+z) + a'_3(x+z)^2 \tag{5}$$

と書ける. ここで $a'_1,\dots,a'_6$ は $a_1,\dots,a_6$ の 4 次同次式である.

以上の結果を用いると, Poncelet の 4 角形に関して次の補題が得られる.

Lemma 3.1. D_0, D_1 に対して Poncelet の 4 角形が得られるための必要十分条件は, (5) が完全平方式になることである.

$$A_2(x,z) = c\cdot B(x,z)^2, \qquad (c \text{ は定数}).$$

Remark 3.2. $B(x,z)=0$ は D_0 の対合写像 (involution)

$$(x,x^2)\in D_0 \mapsto (z,z^2)\in D_0$$

を与えている. このとき $z=\overline{x}$ とも記す.

Remark 3.3. 参考までに 5 角形の場合も述べておくと, D_0, D_1 に対して Poncelet の 5 角形が得られるための必要十分条件は, 上記の $A_1(x,z), A_2(x,z)$ に対し次式が成り立つことである.

$$\frac{1}{(x-z)^2}\mathrm{Res}_u(A_2(u,z),A_2(u,x)) = c'\cdot A_1(x,z), \qquad (c' \text{ は定数}).$$

4　種数 2 の曲線と Poncelet 型代数対応の持ち上げ

一般に種数 2 の曲線は超楕円曲線となる．これを射影直線 $\mathbb{P}^1$ の二重被覆とみなすと, ちょうど 6 個の点で分岐する．本研究の基本的アイデアの一つは, $\mathbb{P}^1$ を射影平面上の 2 次曲線 D_0 で置き換え, 前節の結果を種数 2 の曲線と関連付けることである．

比較のため, まず $\Delta = 5$ の場合の結果について述べる (詳細は [7] 参照)．この場合, 分岐点として D_0 に内接する Poncelet の 5 角形の 5 頂点 $P_1, \ldots, P_5$ を選ぶ．すると分岐点が 1 個不足するが, 残りの 1 個は 2 つの 2 次曲線の交点から選ぶことにする．簡単な議論から曲線の同型類は 4 点のうちどの 1 点を選んでも変わらないことがわかる．この点を P_6 とし, 今後のために

$$P_i = (x_i, x_i^2) \qquad (1 \leq i \leq 6)$$

と定める．このとき $A_1(x, x_6) = c\ (x-\alpha)^2, A_2(x, x_6) = c'(x-\beta)^2$ をみたす α, β がそれぞれ唯一存在する (c, c' は定数)．

以上の設定の下で, 超楕円曲線

$$X : y^2 = f(x) := (x-x_1)(x-x_2)(x-x_3)(x-x_4)(x-x_5)(x-x_6) \tag{6}$$

が得られる．更に, X 上の有理関数

$$j(x) := (x-x_6)(x-\alpha)(x-\beta)$$

を考える．このとき次の定理が成り立つ (詳細は [7] 参照)．

Theorem 4.1 ([7], $\Delta = 5$). $\pi : X \to D_0$ を上記の 2 重被覆写像とするとき, D_0 上の Poncelet 型代数対応 $T = T_1, T_2$ を X 上の 2 次の代数対応 $\hat{T}_1, \hat{T}_2$ に持ち上げることができる．$\hat{T}_i \subset X \times X$ は次のように定まる:

$$\big((x,y),(u,w)\big) \in \hat{T}_i \quad (i=1,2) \quad \overset{\text{def}}{\Longleftrightarrow} \quad j(u)y = j(x)w,\ A_1(x,u) = 0.$$

さらに, $\hat{T}_i$ は $\mathrm{Pic}^0(X)$ の自己準同型 ϕ_i を引き起こし, 次式が成立する．

$$\phi_i{}^2 + \phi_i - 1 = 0 \quad (i = 1, 2).$$

一方 $\Delta = 8$ の場合は Poncelet の 4 角形の 4 頂点 $P_1, \ldots, P_4$ の他にもう 2 点を選ぶ必要があるが $\Delta = 5$ の場合と違い, $D_0 \cap D_1$ から 2 点を選ぶ際は少々注意が必要である．実際, D_0, D_1 の 4 つの交点 $D_0 \cap D_1 = \{P_5, P_5', P_6, P_6'\}$ は対合 (involution) $B(x,z) = 0$ によって 2 点ずつ対になって, $B(x_5, x_5') = 0, B(x_6, x_6') = 0$ をみたすことがわかる．更に $A_1(x, x_5) = c(x-\eta_1)^2, A_1(x, x_6) = c'(x-\eta_2)^2$ をみたす $\eta_1, \eta_2 \in \mathbb{C}$ がそれぞれ唯一決まる．よって $\Delta = 8$ の場合は 6 個の分岐点として, Poncelet の 4 角形の頂点 $P_i (1 \leq i \leq 4)$ と $P_5, P_6 \in D_0 \cap D_1$ を選ぶことにする．すなわち $B(x_5, x_6) \neq 0$ となるように D_0, D_1 の 2 つの交点を選んで, 種数 2 の曲線を方程式 (6) によって定める．この曲線上への前節の D_0 上の代数対応 T の「持ち上げ」を考える．その際, 鍵になるのが次の補題である．まず P_∞ を $x = \infty$ に対応する D_0 の点とし, P_∞ から D_1 への 2 本の接線が再び D_0 と交わる点を $Q_\infty, Q_\infty' \in D_0$ とする．

Lemma 4.2 ($\Delta = 8$). 上記の Q_∞, Q_∞' の座標を $Q_\infty = (u_\infty, {u_\infty}^2)$, $Q_\infty' = (u_\infty', {u_\infty'}^2)$ とし, X 上の有理関数を

$$j(x) := \frac{(x-x_1)(x-x_2)(x-x_3)(x-x_4)(x-\eta_1)(x-\eta_2)}{(x-u_\infty)^3(x-u_\infty')^3}$$

とおくと, 次が成り立つ. ただし, $B(x,\overline{x})=0$.

$$\begin{aligned}&(1)\quad j(\overline{x})=-j(x),\\&(2)\quad A_1(u,x_i)=0\ (i=1,2)\Rightarrow f(x_1)f(x_2)\ =\ j(u)^2.\end{aligned}$$

ここで定義した有理関数 $j(x)$ により, $\Delta=8$ の場合の代数対応 T の「持ち上げ」の存在とその表示式を与えることが可能になる.

Theorem 4.3 ($\Delta=8$). 超楕円曲線 X を上のように定めるとき, D_0 上の Poncelet 型代数対応 T を X 上の 2 次の代数対応 $\hat{T}$ に持ち上げることができる. $\hat{T}\subset X\times X$ は次のように定まる: $A_1(x,u_i)=0\ (i=1,2)$, $B(u_1,u_2)=0$ とするとき

$$\Big((x,y),(u_i,w_i)\Big)\in\hat{T}\quad(i=1,2)\quad\overset{\text{def}}{\Longleftrightarrow}\quad w_1w_2\ =\ j(x).\tag{7}$$

このとき, $\hat{T}$ は $\mathrm{Pic}^0(X)$ の自己準同型 ϕ_i を引き起こし, 次式が成立する:

$$\phi^2-2=0.$$

最後の関係式は, 以下の様に因子の計算から証明できる.

$$\begin{aligned}\phi:(u,w)&\mapsto(x_1,y_1)+(x_2,y_2),\\\phi^2:(u,w)&\mapsto(u,w)+(\overline{u},\overline{w_1})+(u,w)+(\overline{u},\overline{w_2})\\&=(u,w)+(\overline{u},\overline{w_1})+(u,w)+(\overline{u},-\overline{w_1})\end{aligned}$$

より

$$\begin{aligned}\phi^2-2\mathrm{id}:(u,w)&\mapsto(\overline{u},\overline{w_1})+(\overline{u},-\overline{w_1})\\&=\mathrm{div}(x-\overline{u})_0\sim\mathrm{div}(x-\overline{u})_\infty=\mathrm{div}(x)_\infty\end{aligned}$$

となり, これは $\mathrm{Pic}^0(\mathrm{X})$ で ϕ^2-2 がゼロ写像であることを示している.

Remark 4.4. 上記の定理における代数対応 $\hat{T}$ の定義式 (7) は正確には $X\times X$ の座標関数 x,y,u,w の有理式ではない. u_1,u_2 は u の 2 次方程式 $A_1(x,u)=0$ の根であるから 2 次の代数関数であることに注意すると, 実際には, (7) が u_1,u_2, および w_1,w_2 に関して対称形であることから $\hat{T}$ が有理的に表示されることがわかる.

Remark 4.5. $B(x_5,x_6)=0$ なる組を選んで X を定めると, その Jacobi 多様体は $\Delta=4$ の "singular relation" をみたし, 楕円曲線の積と同種 (isogenous) になることが示される.

さて, 定理 4.2 の主張は Poncelet の 4 角形の上には一箇所で交差した形のいわば 8 角形型の 2 重被覆があるというものだった. よって Poncelet の 4 角形の各頂点の持ち上げが ϕ によってどのような写像に移るかはわかった. さらに定理 4.2 の考察により 2 つの conic の交点に関して次の命題を得る. まず, 4 つの交点の x 座標を $\alpha=P_5,\beta=P_6,\gamma,\delta$ とする.

Proposition 4.6. 先に求めた ϕ によって P_5,P_6 はそれぞれ以下のように移る.

$$\begin{aligned}\phi:P_5=(\alpha,0)&\mapsto(\eta_1,\xi_1)+(\eta_1,-\xi_1),\\P_6=(\beta,0)&\mapsto(\eta_2,\xi_2)+(\eta_2,-\xi_2).\end{aligned}$$

Proposition 4.7.

$$\begin{aligned}\phi : (\eta_1, \xi_1) &\mapsto P_5 + (\delta, \zeta_1),\\ (\eta_2, \xi_2) &\mapsto P_6 + (\gamma, \zeta_2)\end{aligned}$$

とすると

$$\begin{aligned}\phi : (\eta_1, -\xi_1) &\mapsto P_5 + (\delta, -\zeta_1),\\ (\eta_2, -\xi_2) &\mapsto P_6 + (\gamma, -\zeta_2).\end{aligned}$$

5　2等分点の決定と構造

以後, 簡単のため分岐点のうちの 1 つを 1 次分数変換で ∞ とし, 5 次型の曲線 $X : y^2 = \prod_{i=1}^{5}(x - x_i)$ について考える. つまり分岐点は $P_i = (x_i, 0)$ $(1 \leq i \leq 5), P_\infty = (\infty, \infty)$. このとき, 任意の i について

$$\begin{aligned}\mathrm{div}(x - x_i) &= 2P_i - 2P_\infty\\ &= 2(P_i - P_\infty)\\ &\sim 0.\end{aligned}$$

よって, $P_i - P_\infty \in \mathrm{Pic}^0(X)[2]$ であり, 等分点の集合が群構造を持つことにより

$$\{P_{i_1} + \cdots + P_{i_k} - kP_\infty | \{i_1, \ldots, i_k\} \subseteq \{1, \ldots, 5\}\} \subseteq \mathrm{Pic}^0(X)[2] \simeq \left(\mathbb{Z}/2\mathbb{Z}\right)^{\oplus 4}. \tag{8}$$

ここで, 左辺の集合では, 見かけ上 $2^5 = 32$ 個の元が表示されているが, $\mathrm{Pic}^0(X)[2]$ の位数は 16 であるので, 同一の元が 2 回ずつ重複しているのではないかと考えられる. 実際,

$$\begin{aligned}\mathrm{div}(y) &= P_1 + P_2 + P_3 + P_4 + P_5 - 5P_\infty\\ &\sim 0\end{aligned}$$

より

$$\begin{aligned}P_2 + P_3 + P_4 + P_5 - 4P_\infty &\sim P_\infty - P_1 \sim P_1' - P_\infty,\\ P_3 + P_4 + P_5 - 3P_\infty &\sim -P_1 - P_2 + 2P_\infty \sim P_1' + P_2' - 2P_\infty\end{aligned}$$

であるので, 以後, 原点と $P - P_\infty, P + Q - 2P_\infty$ の形の因子のみ考えればよく, $P - P_\infty, P + Q - 2P_\infty$ が互いに非線形同値であることが確かめられれば (8) において等号が成り立つことがわかる. これは以下に述べる命題 5.5 にから直ちに導かれる.

簡単のため, X は上記のように 5 次型の曲線 $y^2 = \prod_{i=1}^{5}(x - x_i)$ であるとする. このとき, 任意の $D \in \mathrm{Div}^0(X)$ は次に定義される semi-reduced divisor, reduced divisor と線形同値になることが示される. これはよく知られた事実であるが ([1] 参照), 本稿において果たす役割の重要性を考慮して, 証明を与えておく.

Definition 5.1. 次数 0 の因子 $D \in \mathrm{Div}^0(X)$ は, ある $n \in \mathbb{N}$ が存在して

$$D = P_1 + \cdots + P_n - nP_\infty, \qquad P_i \neq P_\infty$$

と書けるとき, semi-reduced divisor であるという. 特に $n = 1$ のとき, または $n = 2$ で $P_2 \neq \overline{P_1}$ のとき reduced divisor という. ただし, $P = (x, y) \in X$ に対して $\overline{P} := (x, -y)$ とおく (hyperelliptic involution).

Lemma 5.2. 種数 2 の曲線上の 2 位の関数は x の 1 次分数式に限る.

Proof. 仮定より

$$\mathrm{div}(g) = P + Q - (R + S).$$

このとき $x(R) = a, x(S) = b$ とすると

$$\begin{aligned}\mathrm{div}(x - a) &= R + R' - 2P_\infty,\\ \mathrm{div}(x - b) &= S + S' - 2P_\infty.\end{aligned}$$

さらに $g_0 = g(x - a)(x - b)$ とおくと

$$\mathrm{div}(g_0) = P + Q + R' + S' = 4P_\infty$$

となる. すなわち

$$g_0 \in L(4P_\infty) := \{g \in \mathbb{C}(X)^\times \mid \mathrm{div}(g) + 4P_\infty \succ 0\} \cup \{0\}$$

すると, Riemann-Roch の定理よりベクトル空間 $L(4P_\infty)$ は 3 次元で, 基底として $1, x, x^2$ が取れるので $g_0 = a_0 + b_0 x + c_0 x^2$ と書ける. すなわち

$$g = \frac{a_0 + b_0 x + c_0 x^2}{(x - a)(x - b)}.$$

もしこれが既約なら g は 4 位の関数となり仮定に反する. よって可約であり 2 位の関数は x の 1 次分数式に限ることがわかる. □

Proposition 5.3. 任意の次数 0 の因子 $D \in \mathrm{Div}^0(X)$ $(D \neq 0)$ は semi-reduced divisor と線形同値である.

Proof. $D \in \mathrm{Div}^0(X),\ D \neq 0$ に対し,

$$D = D_0 - D_\infty, \quad D_0 = Q_1 + \cdots + Q_n, \quad D_\infty = Q_1'' + \cdots + Q_n''$$

と書くことにする. $Q_j' := \overline{Q_j''} = (b_j, -c_j)$ によって

$$\begin{aligned}\mathrm{div}(x - b_j) &= Q_j' + Q_j'' - 2P_\infty\\ &\sim 0.\end{aligned}$$

ゆえに $-Q_j'' \sim Q_j' - 2P_\infty$ が各 j について成立するので

$$\begin{aligned}D &= Q_1 + \cdots + Q_n - (Q_1'' + \cdots + Q_n'')\\ &\sim Q_1 + \cdots + Q_n + Q_1' + \cdots + Q_n' - 2nP_\infty.\end{aligned}$$

□

Proposition 5.4. 任意の次数 0 の因子 $D \in \mathrm{Div}^0(X)$ $(D \neq 0)$ は reduced divisor と線形同値である.

Proof. 命題 5.3 と帰納法によって $n=3$ の場合を示せば十分である. よって $D=Q_1+Q_2+Q_3-3P_\infty$ を考える. $D'=5P_\infty-(Q_1+Q_2)$ をとると, Riemann-Roch の定理より $L(D')$ の次元は 2 となる. したがって D' の基底を g_1,g_2 とすると $^\exists a,b$ s.t. $g=ag_1+bg_2, g(Q_3)=0$. このとき, g が高々5 位の関数であることから $^\exists Q_4,Q_5$ s.t. $\mathrm{div}(g)=Q_1+Q_2+Q_3+Q_4+Q_5-5P_\infty$. ここで $x(Q_4)=x_4, x(Q_5)=x_5$ とすると $\mathrm{div}(x-x_i)=(Q_i+{Q_i}'-2P_\infty)\sim 0 \ \ (i=4,5)$ となることを用いて

$$\begin{aligned} D &\sim D-\mathrm{div}(g) \\ &=(-Q_4-Q_5+2P_\infty)+(Q_4+Q_4'-2P_\infty)+(Q_5+Q_5'-2P_\infty) \\ &=Q_4'+Q_5'-2P_\infty. \end{aligned}$$

□

Proposition 5.5. 2 つの異なる reduced divisor は互いに非線形同値である.

Proof. $P+Q-2P_\infty, R+S-2P_\infty$ の場合を示せば後は同様に議論できる. もしこの 2 つが線形同値なら $^\exists g$ s.t. $\mathrm{div}(g)=P+Q-(R+S)$. よって補題 5.2 より $g=(ax+b)(cx+d)^{-1}$ と書ける. 分子の零点が $x=-b/a$ であることから $x(P_0)=-b/a$ とすると $\mathrm{div}(ax+b)=P_0+P_0'-2P_\infty$. 分母についても $x(Q_0)=-d/c$ とすると $\mathrm{div}(cx+d)=Q_0+Q_0'-2P_\infty$. よって $\mathrm{div}(g)=P_0+P_0'-(Q_0+Q_0')\sim 0$. 元の g と見比べて P と Q が互いに共役であることがわかり仮定に反する. □

以上の議論をあわせると

$$\begin{aligned} \mathrm{Pic}^0(X)[2] &= \{P_{i_1}+\cdots+P_{i_k}-kP_\infty | \{i_1,\ldots,i_k\}\subseteq\{1,\ldots,5\}\} \\ &= \{P_{i_1}+\cdots+P_{i_k}-kP_\infty | \{i_1,\ldots,i_k\}\subseteq\{1,2\}\}. \end{aligned}$$

6 $\sqrt{2}$ 等分点の決定と構造

4 章で構成した曲線 $X: y^2=\prod_{i=1}^6(x-x_i)$ に対して 2 等分点及び $\sqrt{2}$ 等分点を考える. ただし分岐点は $P_i=(x_i,0)\ (1\le i\le 6), x_5=\alpha, x_6=\beta$. このとき任意の i に対し $\mathrm{div}(x-x_i)=2P_i-(P_\infty+P_\infty')$ であることから

$$\begin{aligned} \mathrm{div}\left(\frac{x-x_i}{x-x_j}\right) &= 2P_i-(P_\infty+P_\infty')-(2P_j-(P_\infty+P_\infty')) \\ &= 2(P_i-P_j)\sim 0. \end{aligned}$$

よって種数 2 の曲線が 6 次型の場合, 前節と同じ議論をすれば

$$\mathrm{Pic}^0(X)[2]=\{P_i-P_j | i<j\}\cup\{0\}$$

であることがわかる.

ここで, 定理 4.3 より Poncelet の 4 角形から構成した ϕ が $\mathrm{Pic}^0(X)$ 上で $\phi^2-2\,\mathrm{id}=0$ をみたすことより

$$\mathrm{Ker}\phi\subset\mathrm{Pic}^0(X)[2].$$

よって, $\mathrm{Pic}^0(X)[2]$ の各元に ϕ を施し $\mathrm{Ker}\phi$ の元となるものを探すことにする. 第 4 章の結果から, ϕ による $\mathrm{Pic}^0(X)[2]$ の各元の像は次の表のようになることがわかる.

$D \in \mathrm{Pic}^0(X)[2]$	$\phi(D)$
$P_1 - P_2$	$\phi(P_1 - P_2) = P_2 + P_4 - (P_1 + P_3)$.
$P_2 - P_3$	$\phi(P_2 - P_3) = P_1 + P_3 - (P_2 + P_4)$.
$P_3 - P_4$	$\phi(P_3 - P_4) = P_2 + P_4 - (P_1 + P_3)$.
$P_4 - P_5$	$\phi(P_4 - P_5) = P_1 + P_3 - ((\eta_1, \xi_1) + (\eta_1, -\xi_1))$.
$P_5 - P_6$	$\phi(P_5 - P_6) = (\eta_1, \xi_1) + (\eta_1, -\xi_1) - ((\eta_2, \xi_2) + (\eta_2, -\xi_2))$ $\sim \mathrm{div}(x - \eta_1)_0 - \mathrm{div}(x - \eta_2)_0$ $\sim \mathrm{div}(x - \eta_1)_\infty - \mathrm{div}(x - \eta_2)_\infty$ $\sim \mathrm{div}(x)_\infty - \mathrm{div}(x)_\infty = 0$.
$P_1 - P_3$	$\phi(P_1 - P_3) = P_2 + P_4 - (P_2 + P_4) = 0$.
$P_2 - P_4$	$\phi(P_2 - P_4) = P_1 + P_3 - (P_1 + P_3) = 0$.
$P_3 - P_5$	$\phi(P_3 - P_5) = P_2 + P_4 - ((\eta_1, \xi_1) + (\eta_1, -\xi_1))$.
$P_4 - P_6$	$\phi(P_4 - P_6) = P_1 + P_3 - ((\eta_2, \xi_2) + (\eta_2, -\xi_2))$.
$P_1 - P_4$	$\phi(P_1 - P_4) = P_2 + P_4 - (P_1 + P_3)$.
$P_2 - P_5$	$\phi(P_2 - P_5) = P_1 + P_3 - ((\eta_1, \xi_1) + (\eta_1, -\xi_1))$.
$P_3 - P_6$	$\phi(P_3 - P_6) = P_2 + P_4 - ((\eta_2, \xi_2) + (\eta_2, -\xi_2))$.
$P_1 - P_5$	$\phi(P_1 - P_5) = P_2 + P_4 - ((\eta_1, \xi_1) + (\eta_1, -\xi_1))$.
$P_2 - P_6$	$\phi(P_2 - P_6) = P_1 + P_3 - ((\eta_2, \xi_2) + (\eta_2, -\xi_2))$.
$P_1 - P_6$	$\phi(P_1 - P_6) = P_2 + P_4 - ((\eta_2, \xi_2) + (\eta_2, -\xi_2))$.

さらに

$$\begin{aligned}
&\mathrm{div}(y) = P_1 + P_2 + P_3 + P_4 + P_5 + P_6 - 3(P_\infty + P'_\infty),\\
&\mathrm{div}(x - x_3) = 2P_3 - (P_\infty + P'_\infty),\\
&\mathrm{div}(x - x_4) = 2P_4 - (P_\infty + P'_\infty)
\end{aligned}$$

より

$$\begin{aligned}
&P_1 - P_3 + P_2 - P_4 - (P_5 + P_6)\\
&\quad = P_1 + P_2 + P_3 + P_4 + P_5 + P_6 - 2(P_3 + P_4 + P_5)\\
&\quad \sim 3(P_\infty + P'_\infty) - 2(P_\infty + P'_\infty) - 2P_5\\
&\quad = P_\infty + P'_\infty - 2P_5 \sim 0.
\end{aligned}$$

すなわち $P_1 - P_3 + P_2 - P_4 \sim P_5 + P_6$ であることがわかり, 次の結果が得られた.

Theorem 6.1. $\sqrt{2}$ 乗法 $\phi : \mathrm{Pic}^0(X) \to \mathrm{Pic}^0(X)$ を持つ曲線 X について, $\sqrt{2}$ 等分点の全体からなる群 $\mathrm{Ker}\phi$ は $P_1 - P_3, P_2 - P_4$ で生成され Weil pairing に関して $\mathrm{Pic}^0(X)[2]$ の maximal isotropic subgroup をなす.

Proof. $\mathrm{Ker}\phi$ が位数 4 の $\mathrm{Pic}^0(X)[2]$ の部分群であることはすでに示した. Divisor に対する Weil pairing の定義として次のようなものが知られている ([2] 参照).

Definition 6.2. $D_1, D_2 \in \mathrm{Pic}^0(X)[n]$ に対し $nD_1 \sim 0, nD_2 \sim 0$ より $^\exists f_1, f_2 \in \mathbb{C}(X)^\times$ s.t. $\mathrm{div}(f_1) = nD_1, \mathrm{div}(f_2) = nD_2$. $\mathrm{Supp}D_1 \cap \mathrm{Supp}D_2 = \emptyset$ のとき Weil pairing $e(D_1, D_2)$ は次のように定義される.

$$e(D_1, D_2) := \frac{f_1(D_1)}{f_2(D_2)}, \qquad f(D) = \prod_i^l f(P_i)^{a_i}, \qquad D = \sum_{i=1}^l a_i P_i.$$

この定義にしたがって計算してみると $P_1 - P_3, P_2 - P_4$ に対して Weil pairing の値が 1 になることが確かめられる.

$$2(P_1 - P_3) = \mathrm{div}\left(\frac{x - x_1}{x - x_3}\right),\ 2(P_2 - P_4) = \mathrm{div}\left(\frac{x - x_2}{x - x_4}\right)$$

と書けることより,

$$f_{P_1 - P_3} = \frac{x - x_1}{x - x_3}, \qquad f_{P_2 - P_4} = \frac{x - x_2}{x - x_4}$$

として Weil pairing を計算すると

$$\begin{aligned} e(P_1 - P_3, P_2 - P_4) &= \frac{f_{P_1 - P_3}(P_2 - P_4)}{f_{P_2 - P_4}(P_1 - P_3)} \\ &= \frac{f_{P_1 - P_3}(P_2)/f_{P_1 - P_3}(P_4)}{f_{P_2 - P_4}(P_1)/f_{P_2 - P_4}(P_3)} \\ &= \frac{(x_2 - x_1)/(x_2 - x_3) \cdot (x_3 - x_2)/(x_3 - x_4)}{(x_4 - x_1)/(x_4 - x_3) \cdot (x_1 - x_2)/(x_1 - x_4)} = 1. \end{aligned}$$

これで $\mathrm{Ker}\phi$ が isotropic subgroup であることが示された. maximal であることは, Weil pairing の非退化性から直ちに従う. □

参考文献

[1] D. G. Cantor, *Computing in Jacobian of a Hyperelliptic Curve*, Math. Comp., **48** (1987), 95–101.

[2] J. Boxall, D. Grant and F. Leprevost, 5-*torsion points on curves of genus* 2, J. London Math. Soc. (2) **64** (2001), 29–43

[3] 橋本 喜一朗, 種数 2 の代数曲線の代数対応による実乗法の構成, 研究集会「群スキームの変形と整数論への応用」報告集 (1996 数理研講究録 No 942).

[4] K. Hashimoto and Y. Sakai, *On versal family of genus* 2 *curves with* $\sqrt{2}$*-multiplication*, RIMS Kokyuroku Bessatsu.

[5] G. Humbert, *Sur les fonctions abeliennes singulieres*, Œuvres de G. Humbert 2, pub. par les soins de Pierre Humbert et de Gaston Julia, Paris, Gauthier-Villars (1936), 297–401.

[6] F. Oort and H. J. M. Bos, ポンスレの閉形定理 (上野健爾 訳), 数学セミナー 1986.5–1986.8

[7] Y. Sakai, *Poncelet's Theorem and Curves of Genus Two with Real Multiplication of* $\Delta = 5$, preprint (2008).