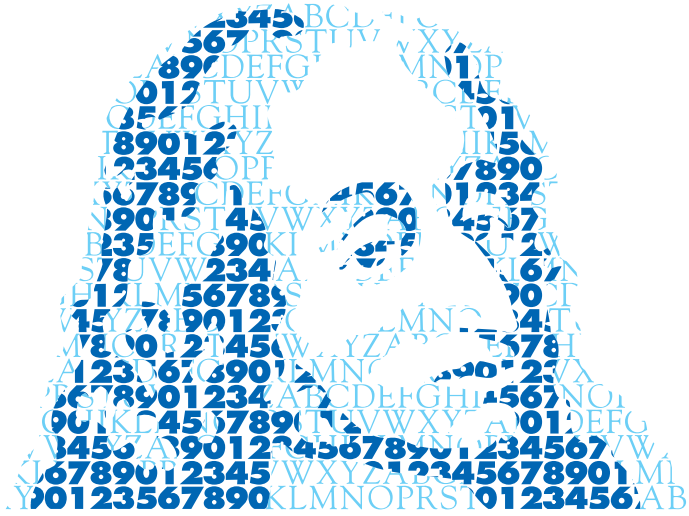
ANNALES MATHÉMATIQUES



BLAISE PASCAL

Katsuya Miyake

Twists of Hessian Elliptic Curves and Cubic Fields

Volume 16, n° 1 (2009), p. 27-45.

<http://ambp.cedram.org/item?id=AMBP_2009__16_1_27_0>

Publication éditée par le laboratoire de mathématiques de l'université Blaise-Pascal, UMR 6620 du CNRS Clermont-Ferrand — France

cedram

Article mis en ligne dans le cadre du Centre de diffusion des revues académiques de mathématiques
http://www.cedram.org/

Annales mathématiques Blaise Pascal **16**, 27-45 (2009)

Twists of Hessian Elliptic Curves and Cubic Fields

Katsuya Miyake

Abstract

In this paper we investigate Hesse's elliptic curves $H_\mu : U^3 + V^3 + W^3 = 3\mu UVW, \mu \in \mathbf{Q} - \{1\}$, and construct their twists, $H_{\mu,t}$ over quadratic fields, and $\tilde{H}(\mu, t), \mu, t \in \mathbf{Q}$ over the Galois closures of cubic fields. We also show that H_μ is a twist of $\tilde{H}(\mu, t)$ over the related cubic field when the quadratic field is contained in the Galois closure of the cubic field. We utilize a cubic polynomial, $R(t; X) := X^3 + tX + t, t \in \mathbf{Q} - \{0, -27/4\}$, to parametrize all of quadratic fields and cubic ones. It should be noted that $\tilde{H}(\mu, t)$ is a twist of H_μ as algebraic curves because it may not always have any rational points over $\mathbf{Q}$. We also describe the set of $\mathbf{Q}$-rational points of $\tilde{H}(\mu, t)$ by a certain subset of the cubic field. In the case of $\mu = 0$, we give a criterion for $\tilde{H}(0, t)$ to have a rational point over $\mathbf{Q}$.

1. Introduction

In 1840's L. O. Hesse (1811–74) investigated plane curves in a series of papers, and found an interesting family of elliptic curves of form

$$H_\mu : U^3 + V^3 + W^3 = 3\mu\, UVW$$

on the projective plane $\mathbf{P}^2(U : V : W)$. If $\mu \neq 1$, it is non-singular, and is an elliptic curve with points of order 3 defined over $\mathbf{Q}(\mu)$ where $\mathbf{Q}$ is the field of rational numbers.

Our concerns in this paper are to introduce systematically twists of the curves with μ in $\mathbf{Q} - \{1\}$ over quadratic fields and the Galois closures of cubic fields, and, in the latter case, to describe the set of the rational points of the curve over $\mathbf{Q}$ by a certain subset of the related cubic field. Here we mean by twists of the elliptic curves those as algebraic curves. This is because the twists we construct may not have any rational points over $\mathbf{Q}$ even though the curves themselves are defined over the field.

Keywords: Hessian elliptic curves, twists of elliptic curves, cubic fields.
Math. classification: 11G05, 12F05.

We utilize a cubic polynomial with a parameter t,

$$R(t;X) := X^3 + tX + t, \qquad t \in \mathbf{Q} - \{0, -27/4\}.$$

It parametrizes not only all cubic fields but also all quadratic ones; we exclude the values 0 and $-27/4$ of the parameter t to save $R(t;X)$ from multiple roots; indeed, the discriminant of the polynomial in X is $-t^2(4t+27)$. Let ξ be a root of $R(t;X) = 0$ in the complex number field $\mathbf{C}$ and put $K_t := \mathbf{Q}(\xi)$; if $R(t;X) = 0$ has a root r in $\mathbf{Q}$, then we pick it up as $\xi = r$ and have $K_t = \mathbf{Q}$; in this case, obviously, we have $t = -r^3/(r+1)$. Let $\tilde{K}_t$ be the splitting field of the cubic polynomial $R(t;X)$ over $\mathbf{Q}$. If t runs over all such rational values as $K_t = \mathbf{Q}$, then $\tilde{K}_t$ covers all quadratic fields as $\mathbf{Q}(\sqrt{-(4t+27)})$ besides $\mathbf{Q}$.

First in Section 2 we list some known facts on the Hessian curves. Then in Section 3 we define a family of curves $\tilde{H}(\mu,t), \mu, t \in \mathbf{Q}, \mu \neq 1, t \neq 0, -27/4$. Each of the curves is of genus 1 and a twist of H_μ over the splitting field $\tilde{K}_t$ as algebraic curves. In Section 4 we describe the set of $\mathbf{Q}$-rational points of $\tilde{H}(\mu,t)$ for such t as $R(t:X)$ is irreducible over $\mathbf{Q}$ by introducing a certain subset of the cubic field K_t.

In general, the curve $\tilde{H}(\mu,t)$, though defined over $\mathbf{Q}$, may not have any rational points over $\mathbf{Q}$. If $K_t = \mathbf{Q}$, however, it has at least one rational point over $\mathbf{Q}$, and hence is an elliptic curve defined over $\mathbf{Q}$; it is a quadratic twist of H_μ if $\tilde{K}_t$ is not $\mathbf{Q}$ but a quadratic field.

In Section 5, we show that the curve

$$H_{\mu,t} : 2u^3 + 6d_t uv^2 + w^3 = 3\mu\left(u^2 - d_t v^2\right), \qquad d_t = -(4t+27)$$

on the projective plane $\mathbf{P}^2(u:v:w)$ is a twist of $\tilde{H}(\mu,t)$ over K_t, and also a quadratic twist of H_μ (Theorem 5.1).

In Section 6, we give simple affine forms $A_{\mu,t}$ and A_μ of 3-isogenies of both $H_{\mu,t}$ and H_μ, respectively, and show that the former is the quadratic twist of the latter over $\mathbf{Q}(\sqrt{d_t})$ (Proposition 6.1).

We have infinitely many one parameter subfamilies of $\tilde{H}(\mu,t)$ which have rational points over $\mathbf{Q}$. In the final Section 7 we show a few simple ones; namely,

Proposition 1.1. *Suppose that the cubic polynomial $R(t;X)$ is irreducible over $\mathbf{Q}$ for $t \in \mathbf{Q} - \{0, -27/4\}$. Then $\tilde{H}(\mu,t)$ has a rational point over $\mathbf{Q}$ in each of the following three cases: (1) in case of $\mu = t/3+1 \neq 1$, the point $(t:0:1)$ belongs to $\in \tilde{H}(\mu,t)[\mathbf{Q}]$, (2) in case of $\mu = 1-3t \neq 1$, the point*

$(1:1:0)$ *belongs to* $\in \tilde{H}(\mu,t)[\mathbf{Q}]$, *and (3) in case of* $\mu = 1-2t/3 \neq 1$, *the point* $(0:0:1)$ *belongs to* $\in \tilde{H}(\mu,t)[\mathbf{Q}]$.

Here we denote the set of $\mathbf{Q}$-rational points of $\tilde{H}(\mu,t)$ by $\tilde{H}(\mu,t)[\mathbf{Q}]$.

In the special case of $\mu = 0$, we give a necessary and sufficient condition on t for $\tilde{H}(0,t)$ to have a rational point over $\mathbf{Q}$;

Proposition 1.2. *In case of* $\mu = 0$, *the curve* $\tilde{H}(0,t)$ *has a rational point over* $\mathbf{Q}$ *for* $t \in \mathbf{Q} - \{0, -27/4\}$ *if and only if either* $t = -r^3/(r+1), r \in \mathbf{Q} - \{0,-1\}$, *or* $\tilde{H}(0,t)$ *is isomorphic over* $\mathbf{Q}$ *to* $\tilde{H}(0,t'), t' = h^3/(2h-1)^2, h \in \mathbf{Q} - \{0, 1/2\}$.

It should be noted that we have infinitely many those rational functions $\mu = f(t)$ of t for each of which the one-parameter family $\tilde{H}(f(t),t)$ has a rational point over $\mathbf{Q}(t)$. In deed, for example, take those rational functions of t, $x = x(t), y = y(t), z = z(t)$, with coefficients in $\mathbf{Q}$ which satisfy $\mathrm{Det}(M(x,y,z)) \neq 0$. (The 3×3 matrix $M(x,y,z)$ will be given in Section 3 to define $\tilde{H}(\mu,t)$.) Then we are able to determine $\mu = \mu(t)$ as a rational function of t in $\mathbf{Q}(t)$ so as to have the point $(x(t):y(t):z(t))$ over $\mathbf{Q}(t)$ on $\tilde{H}(\mu,t)$.

It may be of some help for interested readers to see the recent works [3], [4] and [5] of the author to understand the background of the present article.

2. Some facts on the Hessian curves H_μ

In this section we pick up some facts on the Hessian curves H_μ defined in the introduction from the textbooks of D. Husemöller [2, Chapter 4], and L. J. Mordell [6, Chapter 3].

Proposition 2.1. *(1) If* $\mu \neq 1$, H_μ *is an elliptic curve defined over* $\mathbf{Q}(\mu)$. *If we take, in this case, the point* $P_\infty = (1:-1:0)$ *as the origin of the addition on the elliptic curve, then all of its points of order* 3 *are given by the list (excluding* P_∞*),*

$$\begin{array}{lll} (0:-1:1), & (1:0:-1), & (1:-1:0) = P_\infty, \\ (0:-\omega:1), & (\omega:0:-\omega^2), & (-1:\omega^2:0), \\ (0:-\omega^2:1), & (\omega^2:0:-\omega), & (-1:\omega:0), \end{array}$$

where ω *is a primitive third root of unity.*
(2) If $\mu = 1$, *then* H_μ *is singular and consists of a line and a quadratic*

curve:

$$U^3+V^3+W^3-3UVW = \frac{-1}{2}(U+V+W)\{(U+V+W)^2-3(U^2+V^2+W^2)\}.$$

Proposition 2.2. *The affine elliptic curve*

$$A_\mu : y^2 + 3\mu xy + y = x^3$$

is a 3*-isogeny of an affine model*

$$u^3 + v^3 = 1 - 3\mu uv$$

of $H_\mu, (u = -U/W, v = -V/W)$*. The isogeny is given by* $x = -uv, y = -v^3$*.*

Theorem 2.3. *Suppose that* 3μ *belongs to the ring of rational integers* $\mathbf{Z}$*.*

(1) *Case of* $3\mu \neq -1, 3, 5$ *:*

(1-1) H_μ *has only three* $\mathbf{Q}$*-rational points, or*
(1-2) H_μ *has infinitely many* $\mathbf{Q}$*-rational points.*

(2) *Case of* $3\mu = -1$ *:* H_μ *has six* $\mathbf{Q}$*-rational points*

$$(0:-1:1), (1:0:-1), (1:-1:0), (1:1:-1), (1:-1:1), (-1:1:1).$$

(3) *Case of* $3\mu = 5$ *:* H_μ *has six* $\mathbf{Q}$*-rational points*

$$(0:-1:1), (1:0:-1), (1:-1:0), (1:1:2), (1:2:1), (2:1:1).$$

(4) *Case of* $3\mu = 3$ *:*

H_μ *is singular, and has infinitely many* $\mathbf{Q}$*-rational points.*

Remark 2.4. Mordell uses the tangential method to show the contents of this theorem. The supposition that 3μ is an integer is essential for the proof of the theorem.

3. The Twist $\tilde{H}(\mu, t)$

As we introduced them in Section 1, let $R(t; X)$ be the cubic polynomial

$$R(t; X) := X^3 + tX + t, \qquad t \in \mathbf{Q} - \{0, -27/4\},$$

and, define the fields K_t and $\tilde{K}_t$ as follows: let ξ be a root of $R(t; X) = 0$ in the complex number field $\mathbf{C}$ and put $K_t = \mathbf{Q}(\xi)$; if the equation $R(t; X) =$

0 has a root r in $\mathbf{Q}$, then we pick it up as $\xi = r$ and have $K_t = \mathbf{Q}$. Let $\tilde{K}_t$ be the splitting field of the cubic polynomial $R(t; X)$ over $\mathbf{Q}$. Then the degree $[\tilde{K}_t : \mathbf{Q}]$ varies over all the divisors of 6, and the degree $[K_t : \mathbf{Q}]$ is either 3 or 1.

Now let us introduce an algebraic curve $\tilde{H}(\mu, t)$ for $\mu, t \in \mathbf{Q}, t \neq 0, -27/4$ which is a twist of H_μ as algebraic curves over the splitting field $\tilde{K}_t$. We define it by making use of 3×3 matrices. Put

$$\Xi = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -t & -t & 0 \end{pmatrix}.$$

The following proposition is easily verified; the proof is omitted:

Proposition 3.1. *The characteristic polynomial of the matrix Ξ is equal to the cubic polynomial $R(t; X)$.*

To define our curve, take independent variables x, y, z and put

$$M(x, y, z) := x1_3 + y\Xi + z\Xi^2$$

where 1_3 is the unit matrix of size 3. The curve $\tilde{H}(\mu, t)$ is defined on the projective plane $\mathbf{P}^2(x : y : z)$ by

$$\tilde{H}(\mu, t) : \mathrm{Tr}\left(M(x, y, z)^3\right) = 3\mu\,\mathrm{Det}(M(x, y, z))$$

where Tr and Det denote the trace and the determinant of matrices, respectively.

It should be noted again that, in general, the curve $\tilde{H}(\mu, t)$ may not have any rational points over $\mathbf{Q}$, even though it is defined over $\mathbf{Q}$.

Theorem 3.2. *For $\mu, t \in \mathbf{Q}, \mu \neq 1, t \neq 0, -27/4$, the curve $\tilde{H}(\mu, t)$ is isomorphic to H_μ over $\tilde{K}_t$.*

Proof. Let α, β and γ be the distinct three roots of $R(t : X) = 0$ in $\mathbf{C}$. Since $R(t : X)$ is the characteristic polynomial of Ξ, these roots are the eigen values of Ξ; let $\boldsymbol{x}_\alpha, \boldsymbol{x}_\beta$ and $\boldsymbol{x}_\gamma$ be eigen vectors in the 3-dimensional column vector space over $\tilde{K}_t$ for the corresponding eigen values, respectively, and put

$$A = (\boldsymbol{x}_\alpha, \boldsymbol{x}_\beta, \boldsymbol{x}_\gamma).$$

Then this is a 3×3 matrix with entries in $\tilde{K}_t$. Since the eigen values are different from each other, A is invertible. By definition, furthermore, we

have

$$\Xi A = A \begin{pmatrix} \alpha & & \\ & \beta & \\ & & \gamma \end{pmatrix}.$$

Therefore, we see

$$A^{-1}\,\Xi\,A = \begin{pmatrix} \alpha & & \\ & \beta & \\ & & \gamma \end{pmatrix}, \qquad A^{-1}\,\Xi^2 A = \begin{pmatrix} \alpha^2 & & \\ & \beta^2 & \\ & & \gamma^2 \end{pmatrix}.$$

Since α, β and γ are different from each other, the matrix

$$\begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \beta & \beta^2 \\ 1 & \gamma & \gamma^2 \end{pmatrix}$$

is invertible. Put

$$(\,a_{ij}\,) := \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \beta & \beta^2 \\ 1 & \gamma & \gamma^2 \end{pmatrix}^{-1},$$

and

$$\boldsymbol{a}_j = \begin{pmatrix} a_{1j} \\ a_{2j} \\ a_{3j} \end{pmatrix}, \qquad j = 1, 2, 3;$$

then we see $a_{ij} \in \tilde{K}_t, 1 \le i, j \le 3$, and

$$\begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \beta & \beta^2 \\ 1 & \gamma & \gamma^2 \end{pmatrix} \boldsymbol{a}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \beta & \beta^2 \\ 1 & \gamma & \gamma^2 \end{pmatrix} \boldsymbol{a}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix},$$
$$\begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \beta & \beta^2 \\ 1 & \gamma & \gamma^2 \end{pmatrix} \boldsymbol{a}_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

Now we take

$$E_j = a_{1j}\,1_3 + a_{2j}\,\Xi + a_{3j}\,\Xi^2, \quad j = 1, 2, 3,$$

to have

$$A^{-1}\,E_1\,A = \begin{pmatrix} 1 & & \\ & 0 & \\ & & 0 \end{pmatrix}, \quad A^{-1}\,E_2\,A = \begin{pmatrix} 0 & & \\ & 1 & \\ & & 0 \end{pmatrix},$$

$$A^{-1}\,E_3\,A = \begin{pmatrix} 0 & & \\ & 0 & \\ & & 1 \end{pmatrix},$$

and, hence,

$$E_i\,E_j = E_j\,E_i = \delta_{ij}\,E_i, \qquad 1 \le i, j \le 3.$$

These $E_j, j = 1, 2, 3$, belong to $\tilde{K}_t$-subspace of dimension 3 spanned by $1_3, \Xi, \Xi^2$ in the space of 3×3 full matrix algebra over $\tilde{K}_t$. It is clear that $E_j, j = 1, 2, 3$, are linearly independent over $\tilde{K}_t$. Therefore, we can find such $b_{ij} \in \tilde{K}_t, 1 \le i, j \le 3$, as we have

$$\begin{aligned} 1_3 &= b_{11}\,E_1 + b_{21}\,E_2 + b_{31}\,E_3, \\ \Xi &= b_{12}\,E_1 + b_{22}\,E_2 + b_{32}\,E_3, \\ \Xi^2 &= b_{13}\,E_1 + b_{23}\,E_2 + b_{33}\,E_3. \end{aligned}$$

Then we see the equality

$$\begin{aligned} M(x, y, z) &= x\,1_3 + y\,\Xi + z\,\Xi^2 \\ &= u\,E_1 + v\,E_2 + w\,E_3 \end{aligned}$$

determine a linear transformation over $\tilde{K}_t$ which send (x, y, z) to (u, v, w). Since we have

$$A^{-1}\,M(x, y, z)\,A = \begin{pmatrix} u & & \\ & v & \\ & & w \end{pmatrix},$$

it is clear that we have the equations

$$\begin{aligned} \mathrm{Tr}\left(M(x, y, z)^3\right) &= u^3 + v^3 + z^3, \\ \mathrm{Det}(M(x, y, z)) &= uvw. \end{aligned}$$

This shows that the curve $\tilde{H}(\mu, t)$ is isomorphic to H_μ over $\tilde{K}_t$. □

Remark 3.3. Actually, $(\,b_{ij}\,)$ is the inverse matrix of $(\,a_{ij}\,)$; hence, we have

$$(\,b_{ij}\,) = (\,a_{ij}\,)^{-1} = \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \beta & \beta^2 \\ 1 & \gamma & \gamma^2 \end{pmatrix},$$

and

$$\begin{cases} u &= x + \alpha\, y + \alpha^2\, z, \\ v &= x + \beta\, y + \beta^2\, z, \\ w &= x + \gamma\, y + \gamma^2\, z, \end{cases} \qquad \begin{cases} x &= a_{11}u + a_{12}v + a_{13}w, \\ y &= a_{21}u + a_{22}v + a_{23}w, \\ z &= a_{31}u + a_{32}v + a_{33}w. \end{cases}$$

4. The Set of Q-rational Points of $\tilde{H}(\mu, t)$

In this section, we assume that the cubic polynomial $R(t; X)$ with $t \in \mathbf{Q}$ is irreducible over $\mathbf{Q}$. As in the preceding section, let α, β and γ be the distinct three roots of $R(t : X) = 0$ in $\mathbf{C}$. They are conjugates to each other by our present assumption. Pick up $\xi := \gamma$ without loss of generality. Then $K_t = \mathbf{Q}(\xi)$ is a cubic field.

Proposition 4.1. *The splitting field $\tilde{K}_t$ of the cubic polynomial $R(t; X)$ over $\mathbf{Q}$ contains $\sqrt{d_t}$, $d_t = -(4t + 27)$, and $\tilde{K}_t = K_t(\sqrt{d_t})$.*
(1) We have $[\tilde{K}_t : \mathbf{Q}] = 3$ if and only if d_t is a square in $\mathbf{Q}$; in the case, we have $\tilde{K}_t = K_t$.
(2) We have $[\tilde{K}_t : \mathbf{Q}] = 6$ if and only if d_t is not a square in $\mathbf{Q}$; in the case, $\tilde{K}_t$ contains the quadratic field $\mathbf{Q}(\sqrt{d_t})$, and $\tilde{K}_t = K_t(\sqrt{d_t})$.

Proof. The proposition immediately follows from the following lemma. □

Lemma 4.2. *The notation and the assumptions being as above, we have $\tilde{K}_t = \mathbf{Q}(\xi, \alpha, \beta)$, and*

$$R(t; X) = (X - \xi)\,(X^2 + \xi\, X + \xi^2 + t), \qquad t = \frac{-\xi^3}{\xi + 1}.$$

The discriminant D of the quadratic factor is given by

$$D = -(3\xi^2 + 4t) = d_t \left(\frac{\xi}{2\xi + 3}\right)^2, \qquad d_t = -(4t + 27).$$

The proof of the lemma is easily obtained and hence omitted.

Let $\tilde{H}(\mu, t)[\mathbf{Q}]$ be the set of all $\mathbf{Q}$-rational points on the curve $\tilde{H}(\mu, t)$. To describe this set we define a subset $S_{\mu,t}$ of the cubic field K_t by

$$S_{\mu,t} = \{\eta \in K_t^\times \mid \mathrm{Tr}_{K_t/\mathbf{Q}}(\eta^3) = 3\mu\, \mathrm{N}_{K_t/\mathbf{Q}}(\eta)\}.$$

Here $\mathrm{Tr}_{K_t/\mathbf{Q}}$ and $\mathrm{N}_{K_t/\mathbf{Q}}$ are the trace map and the norm map of K_t over $\mathbf{Q}$, respectively. It is clear that the multiplicative group $\mathbf{Q}^\times$ naturally acts

on the set $S_{\mu,t}$. We denote the set of orbits by $S_{\mu,t}/\sim_{\mathbf{Q}^\times}$.

Theorem 4.3. *Let the notation and the assumptions be as above. Then there exists a canonical one-to-one and onto correspondence between the two sets, $S_{\mu,t}/\sim_{\mathbf{Q}^\times}$ and $\tilde{H}(\mu,t)[\mathbf{Q}]$.*

Proof. An element η of K_t is uniquely expressed as

$$\eta = a + b\,\xi + c\,\xi^2, \qquad a, b, c \in \mathbf{Q}.$$

Then the conjugates of η over $\mathbf{Q}$ are given by

$$\eta' = a + b\,\alpha + c\,\alpha^2,$$
$$\eta'' = a + b\,\beta + c\,\beta^2.$$

Therefore, if we use the notation in the proof of Theorem 3.2 in the preceding Section 3, we have

$$A^{-1}\,M(a,b,c)\,A = \begin{pmatrix} \eta' & & \\ & \eta'' & \\ & & \eta \end{pmatrix}.$$

It is, hence, clear that $\eta = a + b\,\xi + c\,\xi^2 \in K_t$ belongs to $S_{\mu,t}$ if and only if the point $(a : b : c)$ on the projective plane $\mathbf{P}^2(x : y : z)$ belongs to $\tilde{H}(\mu,t)[\mathbf{Q}]$. The theorem is now clear. □

We transfer the well-known tangential method on elliptic curves into our $S_{\mu,t}$.

Proposition 4.4. *If $\eta \in K_t$ belongs to $S_{\mu,t}$, then $\sqrt{d_t}\,\eta\left(\eta'^3 - \eta''^3\right)$ also belongs to $S_{\mu,t}$.*

Proof. The proposition easily follows from the following Lemma 4.5 and Corollary 4.7. □

Lemma 4.5. *If η belongs to K_t, then $\sqrt{d_t}\,\eta\left(\eta'^3 - \eta''^3\right)$ in $\tilde{K}_t$ also belongs to K_t. The conjugates of $\rho := \sqrt{d_t}\,\eta\left(\eta'^3 - \eta''^3\right)$ over $\mathbf{Q}$ are $\rho' = \sqrt{d_t}\,\eta'\left(\eta''^3 - \eta^3\right)$ and $\rho'' = \sqrt{d_t}\,\eta''\left(\eta^3 - \eta'^3\right)$.*

Proof. If $\tilde{K}_t = K_t$, then the lemma is obvious. Suppose $\tilde{K}_t \supsetneqq K_t$. Let σ and τ be the generators of the Galois groups $\mathrm{Gal}(\tilde{K}_t/K_t)$ and $\mathrm{Gal}(\tilde{K}_t/\mathbf{Q}(\sqrt{d_t})$, respectively. Then we have $\sigma^2 = \tau^3 = \mathrm{id}$. Since $\tilde{K}_t = K_t(\sqrt{d_t})$, we have

$\sqrt{d_t}^{\sigma} = -\sqrt{d_t}$. Since $K_t = \mathbf{Q}(\xi)$, and $\xi' = \alpha$ and $\xi'' = \beta$ by our notation, we have $\tilde{K}_t = K_t(\xi') = K_t(\xi'')$, and hence $\xi'^{\sigma} = \xi''$ and $\xi''^{\sigma} = \xi'$. Therefore, $\eta'^{\sigma} = \eta''$ and $\eta''^{\sigma} = \eta'$. We also have $\eta^{\sigma} = \eta$. We now see

$$\{\sqrt{d_t}\,\eta\,(\eta'^3 - \eta''^3)\}^{\sigma} = -\sqrt{d_t}\,\eta\,(\eta''^3 - \eta'^3) = \sqrt{d_t}\,\eta\,(\eta'^3 - \eta''^3),$$

and $\sqrt{d_t}\,\eta\,(\eta'^3 - \eta''^3) \in K_t$. Since we have

$$\sqrt{d_t}^{\tau} = \sqrt{d_t}, \qquad \eta^{\tau} = \eta', \qquad \eta^{\tau^2} = \eta'',$$

the lemma is now clear. □

Lemma 4.6. *We have:*

$$x(y-z)^3 + y(z-x)^3 + z(x-y)^3 = (x+y+z)\,(y-z)\,(z-x)\,(x-y).$$

Proof. The proof is omitted because it is obtained by strait-forward calculation. □

Corollary 4.7.

$$\begin{aligned}\{x(y^3-z^3)\}^3 + \{y(z^3-x^3)\}^3 + \{z(x^3-y^3)\}^3 \\ = (x^3+y^3+z^3)\,(y^3-z^3)\,(z^3-x^3)\,(x^3-y^3).\end{aligned}$$

Proof. Just replace the x, y, z in the identity of the lemma by x^3, y^3, z^3, respectively. □

5. The Twist $H_{\mu,t}$ of $\tilde{H}(\mu,t)$ over K_t

In this section we give a twist $H_{\mu,t}$ of $\tilde{H}(\mu,t)$ over K_t, and also show that $H_{\mu,t}$ is a quadratic twist of the Hessian curve H_{μ}.

Let $H_{\mu,t}$ be the curve on the projective plane $\mathbf{P}^2(u:v:w)$ defined by

$$H_{\mu,t} : 2u^3 + 6d_t uv^2 + w^3 = 3\mu\left(u^2 - d_t v^2\right) w$$

where $d_t = -(4t+27)$ as above.

Theorem 5.1. *Suppose that $\mu, t \in \mathbf{Q}, \mu \neq 1, t \neq 0, -27/4$.*
(1) The curve $\tilde{H}(\mu,t)$ is isomorphic to $H_{\mu,t}$ over K_t.
(2) The curve $H_{\mu,t}$ is a twist of the Hessian curve H_{μ} over $\mathbf{Q}(\sqrt{d_t}) =$

$\mathbf{Q}(\sqrt{-(4t+27)})$, *and an elliptic curve defined over* $\mathbf{Q}$ *with a* $\mathbf{Q}$*-rational point* $(u:v:w)=(0:1:0)$. *The isomorphism is given by*

$$\begin{cases} U = u + \sqrt{d_t}\, v, \\ V = u - \sqrt{d_t}\, v, \\ W = w, \end{cases} \qquad \begin{cases} u = (U+V)/2, \\ v = (U-V)/(2\sqrt{d_t}), \\ w = W. \end{cases}$$

Proof. This time we only use the root ξ of $R(t;X)=0$. By Lemma 4.2 we have

$$R(t;X) = (X-\xi)\,(X^2+\xi\,X+\xi^2+t), \quad t = \frac{-\xi^3}{\xi+1}, \quad \xi^2+t = \frac{\xi^2}{\xi+1}.$$

The discriminant D of the quadratic factor was also given by

$$D = -(3\xi^2+4t) = d_t\left(\frac{\xi}{2\xi+3}\right)^2, \qquad d_t = -(4t+27).$$

Put $\rho := \dfrac{\xi}{2(2\xi+3)}$ and

$$P(t;X) := X^2+\xi\,X+\xi^2+t.$$

Then we easily see

$$P(t;X) = (X+\xi/2)^2 - \rho^2 d_t = (X-\xi)\,(X+2\xi)+3\xi^2+t.$$

Since $R(t;X)$ does not have any multiple roots, we have $3\xi^2+t \neq 0$. Therefore,

$$1 = (3\xi^2+t)^{-1}P(t;X) - (3\xi^2+t)^{-1}Q(t;X), \qquad Q(t;X) = (X-\xi)\,(X+2\xi).$$

Define 3×3 matrices E_1 and E_2 this time by 'inserting' $X := \Xi$ as

$$E_1 := -\left(3\xi^2+t\right)^{-1} Q(t;\Xi),$$

$$E_2 := \left(3\xi^2+t\right)^{-1} P(t;\Xi).$$

(The constant terms of Q and P should be replaced by scalar matrices.) These belong to the linear span by $1_3, \Xi, \Xi^2$ over K_t in the space of full matrix algebra of size 3 over K_t. By definition and from $R(t;\Xi)=0$, we easily see

$$E_1+E_2 = 1_3, \qquad E_iE_j = E_jE_i = \delta_{ij}E_i, \quad E_i\Xi = \Xi\,E_i, \quad 1\le i,j\le 2.$$

Since $E_i^2 = E_i$, the eigen values of $E_i, i=1,2$, should be either 0 or 1. Let us show $\mathrm{rank}(E_2)=1$; then we also have $\mathrm{rank}(E_1)=2$ because

$E_1 + E_2 = 1_3$ and $E_1E_2 = E_2E_1$. As in the proof of Theorem 3.2, we diagonalize Ξ over $\tilde{K}_t$; namely,

$$A^{-1}\,\Xi\,A = \begin{pmatrix} \alpha & & \\ & \beta & \\ & & \xi \end{pmatrix}.$$

Then we see

$$A^{-1}\,P(t;\Xi)\,A = A^{-1}(\Xi - \alpha 1_3)\,(\Xi - \beta 1_3)\,A$$
$$= \begin{pmatrix} 0 & & \\ & \beta-\alpha & \\ & & \xi-\alpha \end{pmatrix} \begin{pmatrix} \alpha-\beta & & \\ & 0 & \\ & & \xi-\beta \end{pmatrix} = \begin{pmatrix} 0 & & \\ & 0 & \\ & & P(t;\xi) \end{pmatrix}.$$

Since $R(t;X)$ does not have any multiple roots, we see $P(t;\xi) \neq 0$. This shows

$$\mathrm{rank}(E_2) = \mathrm{rank}((3\xi^2 + t)^{-1}P(t;\Xi)) = 1.$$

Let $V = K_t^3$ be the 3-dimensional column vector space over K_t, and put $V_1 := E_1V$ and $V_2 := E_2V$. Then $V = V_1 \oplus V_2$, $\dim_{K_t}(V_1) = 2, \dim_{K_t}(V_2) = 1$, and $E_1V_2 = E_2V_1 = \{\mathbf{0}\}$. Since $E_i\,\Xi = \Xi\,E_i, i = 1,2$, we have $\Xi\,V_i = V_i, i = 1,2$. Take a non-zero vector $\boldsymbol{x}$ from V_2. Then $V_2 = K_t\boldsymbol{x}, E_2\boldsymbol{x} = \boldsymbol{x}$, and $\Xi\,\boldsymbol{x} = \xi\boldsymbol{x}$.

As for V_1, there is such a vector $\boldsymbol{a} \in V_1$ as $\boldsymbol{a}$ and $(\Xi + (\xi/2)1_3)\boldsymbol{a}$ are linearly independent over K_t. Indeed, suppose that we have $(\Xi+(\xi/2)1_3)\boldsymbol{a} = a\,\boldsymbol{a}$ with $a \in K_t$. Then we have $\Xi\,\boldsymbol{a} = (a - \xi/2)\boldsymbol{a}$; hence, the number $(a - \xi/2)$ belongs to K_t and is an eigen value of Ξ. This cannot be ξ because the latter has an eigen vector $\boldsymbol{x}$ in V_2. Therefore it is one of the roots α and β of $P(t;X)$. This shows that both α and β belong to K_t. We may assume $a - \xi/2 = \alpha$ without losing generality. Take an eigen vector $\boldsymbol{b} \in K_t^3$ for β; that is, $\Xi\,\boldsymbol{b} = \beta\,\boldsymbol{b}$, and so $(\Xi - \beta 1_3)\boldsymbol{b} = 0$. Then we have $E_2\boldsymbol{b} = 0$ and hence $\boldsymbol{b} \in V_1$. Put $\boldsymbol{a}' := \boldsymbol{a} + \boldsymbol{b}$. Then $\boldsymbol{a}'$ is in V_1, and

$$\left(\Xi + \frac{\xi}{2}1_3\right)\boldsymbol{a}' = \left(\alpha + \frac{\xi}{2}\right)\boldsymbol{a} + \left(\beta + \frac{\xi}{2}\right)\boldsymbol{b}.$$

Since $\boldsymbol{a}$ and $\boldsymbol{b}$ are eigen vectors belonging to different eigen values, they are linearly independent over K_t. This shows that the vector $(\alpha+\xi/2)\boldsymbol{a} + (\beta + \xi/2)\boldsymbol{b}$ is not equal to any scalar multiple of $\boldsymbol{a}' = \boldsymbol{a} + \boldsymbol{b}$. Hence we obtained the desired vector $\boldsymbol{a}'$ in place of $\boldsymbol{a}$ which we picked up at the beginning.

Now for our choice of $\boldsymbol{x} \in V_2$ and $\boldsymbol{a} \in V_1$, put $\boldsymbol{x}_1 := \boldsymbol{a}, \boldsymbol{x}_2 := \rho^{-1}(\Xi + (\xi/2)1_3)\boldsymbol{a}$, where $\rho = \xi/(2(2\xi+3))$ as we picked it up at the beginning of the proof, and $\boldsymbol{x}_3 := \boldsymbol{x}$. Then the 3×3 matrix $B := (\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3)$ over K_t is regular. Moreover, we easily see

$$\begin{aligned}\Xi\, B &= (\Xi\, \boldsymbol{x}_1, \Xi\, \boldsymbol{x}_2, \Xi\, \boldsymbol{x}_3) \\ &= \left(-\frac{\xi}{2}\, \boldsymbol{x}_1 + \rho\, \boldsymbol{x}_2,\ \rho^{-1} \left(\Xi + \frac{\xi}{2} 1_3 \right)^2 \boldsymbol{x}_1 - \frac{\xi}{2}\, \boldsymbol{x}_2,\ \xi\, \boldsymbol{x}_3 \right).\end{aligned}$$

On the vector space V_1, we have

$$\begin{aligned}E_1 P(t;\Xi) = P(t;\Xi) E_1 &= \left(\Xi^2 + \xi\, \Xi + \frac{\xi^2}{\xi+1} \right) E_1 \\ &= \left(\left(\Xi + \frac{\xi}{2} 1_3 \right)^2 - \rho^2 d_t 1_3 \right) E_1 = 0.\end{aligned}$$

Therefore we have $\rho^{-1}(\Xi + (\xi/2)1_3)^2\, \boldsymbol{x}_1 = \rho d_t \boldsymbol{x}_1$. Thus we obtained

$$\Xi\, B = B \begin{pmatrix} -\frac{\xi}{2} & \rho d_t & \\ \rho & -\frac{\xi}{2} & \\ & & \xi \end{pmatrix}.$$

Hence we see

$$B^{-1} E_1\, B = \begin{pmatrix} 1 & & \\ & 1 & \\ & & 0 \end{pmatrix},$$

$$B^{-1} \left(\Xi + \frac{\xi}{2} 1_3 \right) E_1\, B = \begin{pmatrix} 0 & \rho d_t & \\ \rho & 0 & \\ & & 0 \end{pmatrix},$$

$$B^{-1} E_2\, B = \begin{pmatrix} 0 & & \\ & 0 & \\ & & 1 \end{pmatrix}.$$

Therefore, the linear subspace spanned by the three matrices $E_1, \rho^{-1}(\Xi + (\xi/2)1_3)E_1$, E_2 over K_t in the full matrix algebra of size 3 coincides with the one spanned by $1_3, \Xi, \Xi^2$ over K_t. Expressing now as

$$\begin{aligned}M(x,y,z) &= x 1_3 + y\, \Xi + z\, \Xi^2 \\ &= u\, E_1 + v\, \rho^{-1} \left(\Xi + \frac{\xi}{2} 1_3 \right) E_1 + w\, E_2,\end{aligned}$$

we have a linear transformation over K_t which relates (x, y, z) to (u, v, w), and also

$$B^{-1}M(x, y, z)B = \begin{pmatrix} u & d_t v & \\ v & u & \\ & & w \end{pmatrix}.$$

Thus we obtained

$$\begin{aligned} \mathrm{Tr}\left(M(x, y, z)^3\right) &= 2\left(u^3 + 3d_t uv^2\right) + w^3, \\ \mathrm{Det}(M(x, y, z)) &= \left(u^2 - d_t v^2\right) w. \end{aligned}$$

From this we immediately see the statement (1) of the theorem.

As for (2) of the theorem, it is easily confirmed by a straightforward way; the calculation is omitted. □

6. The 3-Isogeny of $H_{\mu,t}$

By Proposition 2.2 in Section 2, we gave a simple affine model A_μ of the 3-isogeny of the Hessian elliptic curve H_μ for $\mu \neq 1$; namely,

$$A_\mu : y^2 + 3\mu xy + y = x^3.$$

We now give an affine model $A_{\mu,t}$ of a 3-isogeny of the elliptic curve

$$H_{\mu,t} : 2u^3 + 6d_t uv^2 + w^3 = 3\mu\left(u^2 - d_t v^2\right) w$$

for $\mu \neq 0, 1$. This affine curve is a quadratic twist of A_μ over $\mathbf{Q}(\sqrt{d_t})$. Define $A_{\mu,t}$ by

$$A_{\mu,t} : d_t Y^2 = \left(\frac{2X - 1}{3\mu}\right)^3 + X^2, \qquad d_t = -(4t + 27).$$

It has a $\mathbf{Q}$-rational point $(X : Y : Z) = (0 : 1 : 0)$ at infinity.

Proposition 6.1. *Suppose that $\mu, t \in \mathbf{Q}, \mu \neq 0, 1, t \neq 0, -27/4$.*
(1) The elliptic curve $A_{\mu,t}$ is an affine model of a 3-isogeny of the elliptic curve $H_{\mu,t}$ defined by

$$\begin{cases} X &= \left(\dfrac{u}{-w}\right)^3 + 3d_t\left(\dfrac{u}{-w}\right)\left(\dfrac{v}{-w}\right)^2, \\ Y &= 3\left(\dfrac{u}{-w}\right)^2\left(\dfrac{v}{-w}\right) + d_t\left(\dfrac{v}{-w}\right)^3. \end{cases}$$

(2) If d_t is not a square in $\mathbf{Q}$, moreover, $A_{\mu,t}$ is the quadratic twist of A_μ over the quadratic field $\mathbf{Q}(\sqrt{d_t})$.

Proof. For simplicity, put $f := u/(-w)$ and $g := v/(-w)$. Then we have $X = f^3 + 3d_t f\, g^2, Y = 3\, f^2 g + d_t g^3$, and hence, on one hand, $X^2 - d_t Y^2 = (f^2 - d_t g^2)^3$ by a straightforward way. On the other hand, by dividing the both sides of the defining equation of $H_{\mu,t}$, we obtain $2X-1 = -3\mu(f^2 - d_t g^2)$. Therefore, we have $X^2 - d_t Y^2 = ((2X-1)/(-3\mu))^3$. This is equivalent to the defining equation of $A_{\mu,t}$. The first statement of the proposition is proved. To see the second one, set

$$X = \frac{3\mu\, x + 1}{2}, \quad Y = y + \frac{3\mu\, x + 1}{2}.$$

Since we have $x = (2X-1)/(3\mu)$, we easily see that the defining equation of A_μ is equivalent to the equation

$$Y^2 = \left(\frac{2X-1}{3\mu}\right)^3 + X^2.$$

Hence $A_{\mu,t}$ is nothing but the standard quadratic twist of A_μ over $\mathbf{Q}(\sqrt{d_t})$ combined with the above transformation $(x, y) \mapsto (X, Y)$. □

7. Some cases of non-empty $\tilde{H}(\mu, t)[\mathbf{Q}]$

As we stated in Introduction, we now show the two propositions to demonstrate some cases of non-empty $\tilde{H}(\mu, t)[\mathbf{Q}]$.

Proof of Proposition 1.1. Let us start with the 3×3 matrix Ξ. Since $t \neq 0$ in each case, we have $\mathrm{Det}(\Xi) = -t \neq 0$. Note that $R(t; \Xi) = \Xi^3 + t\,\Xi + t 1_3 = 0$. The matrix $\Xi^{-1} = -1_3 - t^{-1}\Xi^2$ corresponds to the point $(-1 : 0 : -1/t) = (t : 0 : 1)$ on the projective plane $\mathbf{P}^2(x : y : z)$. Since $\Xi^{-2} = -\Xi^{-1} - (1/t)\Xi$ and $\Xi^{-3} = -(1/t)1_3 - \Xi^{-2}$, we see $\mathrm{Tr}(\Xi^{-3}) = -3/t - 1$. Hence we have the case (1) of the proposition because $\mathrm{Det}(\Xi^{-1}) = -1/t$. In the same manner, we can easily show the cases (2) and (3) for $\Xi^3 = -t(1_3 + \Xi)$ and Ξ^2, respectively. □

In the special case of $\mu = 0$ we give a necessary and sufficient condition on t for $\tilde{H}(0, t)$ to have a rational point over $\mathbf{Q}$.

Proposition 7.1. *In case of $\mu = 0$, the curve $\tilde{H}(0,t)$ has a rational point over $\mathbf{Q}$ for $t \in \mathbf{Q} - \{0, -27/4\}$ if and only if either $t = -r^3/(r+1), r \in \mathbf{Q} - \{0, -1\}$, or $\tilde{H}(0,t)$ is isomorphic to $\tilde{H}(0,t'), t' = h^3/(2h-1)^2, h \in \mathbf{Q} - \{0, 1/2\}$ over $\mathbf{Q}$.*

Proof. We easily see that the 3×3 matrices $1_3, \Xi$, and Ξ^2 are linearly independent over $\mathbf{Q}$. Let us denote the subalgebra generated by Ξ in the full matrix algebra of 3×3 matrices over $\mathbf{Q}$ by $\mathcal{A}_t$; namely,

$$\mathcal{A}_t = \mathbf{Q}1_3 + \mathbf{Q}\,\Xi + \mathbf{Q}\,\Xi^2.$$

Since $R(t;X)$ is the characteristic polynomial of Ξ, $\mathcal{A}_t$ is isomorphic to the quotient algebra $\mathbf{Q}[X]/(R(t;X))$. Hence $R(t;X)$ is irreducible over $\mathbf{Q}$ if and only if $\mathcal{A}_t$ is isomorphic to a cubic field.

Suppose first that $R(t;X)$ is reducible over $\mathbf{Q}$. Then it has a root r in $\mathbf{Q}$; we have $t = -r^3/(r+1)$ with $r \in \mathbf{Q} - \{0, -1\}$ because $r^3 + tr + t = 0$. Then it follows from Theorem 5.1, (2), that $\tilde{H}(0,t)$ has a rational point over $\mathbf{Q}$. Conversely, if $t = -r^3/(r+1)$ with $r \in \mathbf{Q} - \{0, -1\}$, then r is a root of $R(t;X)$, and hence $R(t;X)$ is reducible over $\mathbf{Q}$. Therefore, Theorem 5.1, (2), assures that $\tilde{H}(0,t)$ has a rational point over $\mathbf{Q}$.

Suppose now that $R(t;X)$ is irreducible over $\mathbf{Q}$, and that $\Theta \neq 0$ in $\mathcal{A}_t$ satisfies

$$\mathrm{Tr}(\Theta^3) = 0.$$

Then Θ is invertible in $\mathcal{A}_t$ because this is isomorphic to a cubic field. Moreover, Θ generates $\mathcal{A}_t$ over $\mathbf{Q}$ because it cannot be a scalar matrix $a1_3, a \in \mathbf{Q} - \{0\}$, and because a cubic field does not contain any non-trivial subfields. Let $\varphi(X) = X^3 + a\,X^2 + b\,X + c, a, b, c \in \mathbf{Q}$, be the characteristic polynomial of Θ. Since Θ is invertible, we have $c = -\mathrm{Det}(\Theta) \neq 0$. Hence we also have $a = -\mathrm{Tr}(\Theta) \neq 0$; indeed, if we assume $a = 0$, then we should have

$$\mathrm{Tr}(\Theta^3) = \mathrm{Tr}(-a\,\Theta^2 - b\,\Theta - c1_3) = -3c \neq 0.$$

Put $\Omega := a^{-1}\Theta, f := a^{-2}b, g := a^{-3}c$. Then we have

$$\Omega^3 + \Omega^2 + f\,\Omega + g1_3 = 0$$

because $\varphi(\Theta) = \Theta^3 + a\,\Theta^2 + b\,\Theta + c1_3 = 0$. By taking squares of the both side of the equation, $\Omega^3 + f\,\Omega = -\Omega^2 - g1_3$, we easily obtain

$$(\Omega^2)^3 + (2f-1)(\Omega^2)^2 + (f^2 - 2g)(\Omega^2) - g^2 1_3 = 0,$$

and hence, $\mathrm{Tr}\,(\Omega^2) = -2f + 1$. (Note that the cubic polynomial $X^3 + (2f-1)X^2 + (f^2 - 2g)X - g^2$ has to be the characteristic polynomial of

$\Omega = a^{-1}\Theta$ because it generates $\mathcal{A}_t$ which is isomorphic to a cubic field.) Therefore, we have

$$\mathrm{Tr}(\Omega^3) = \mathrm{Tr}(-\Omega^2 - f\,\Omega - g1_3) = 2f - 1 + f - 3g = 3f - 3g - 1,$$

and hence, $f = g + 1/3$ from $a^{-3}\mathrm{Tr}(\Theta^3) = 0$. Thus we obtain

$$(\Omega + \frac{1}{3}1_3)^3 + g(\Omega + \frac{1}{3}1_3) + \left(\frac{2}{3}g - \frac{1}{27}\right)1_3 = 0. \qquad (*)$$

Here we have $g = -\mathrm{Det}(\Omega) \neq 0$ and $\dfrac{2}{3}g - \dfrac{1}{27} = -\mathrm{Det}(\Omega + \dfrac{1}{3}1_3) \neq 0$. Put now

$$\Xi' := \left(\frac{2}{3}g - \frac{1}{27}\right)^{-1}\left(\frac{g}{a}\Theta + \frac{g}{3}1_3\right),$$
$$t' := g^3\left(\frac{2}{3}g - \frac{1}{27}\right)^{-2}.$$

Then by multiplying the both sides of the equation $(*)$ by $g^3(2g/3 - 1/27)^{-3}$, we have ${\Xi'}^3 + t'\,\Xi' + t'1_3 = 0$. Finally put $h := 9g$. Then we obtain

$$\begin{cases} {\Xi'}^3 + t'\,\Xi' + t'1_3 = R(t';\Xi') = 0, \\ t' = \dfrac{h^3}{(2h-1)^2}, \qquad h \neq 0, \dfrac{1}{2} \end{cases} \qquad (**)$$

and,

$$\frac{3}{a}\Theta = \frac{2h-1}{h}\Xi' - 1_3.$$

Since Ξ' also generates $\mathcal{A}_t$ over $\mathbf{Q}$, we have

$$\mathcal{A}_t = \mathcal{A}_{t'} = \mathbf{Q}1_3 + \mathbf{Q}\,\Xi' + \mathbf{Q}\,{\Xi'}^2.$$

It is now clear that the equation $M(x,y,z) = M'(x',y',z')$ with

$$M(x,y,z) = x1_3 + y\,\Xi + z\,\Xi^2,$$
$$M'(x',y',z') = x'1_3 + y'\,\Xi' + z'\,{\Xi'}^2$$

determines a linear transformation $(x,y,z) \mapsto (x',y',z')$ over $\mathbf{Q}$ which induces an isomorphism of $\tilde{H}(0,t)$ to $\tilde{H}(0,t')$ defined over $\mathbf{Q}$.

Conversely, suppose that the above $(**)$ is satisfied by Ξ and t in place of Ξ' and t', respectively, for simplicity. Put $\Theta := (2h-1)h^{-1}\Xi - 1$. Then we have

$$\Theta^3 = \left(\frac{2h-1}{h}\right)^3\Xi^3 - \frac{3(2h-1)^2}{h^2}\Xi^2 + \frac{3(2h-1)}{h}\Xi - 1_3.$$

We also have $\mathrm{Tr}(\Xi) = 0$. It follows from $(\Xi^3 + t\,\Xi)^2 = t^2 1_3$ that

$$(\Xi^2)^3 + 2t(\Xi^2)^2 + t^2\,\Xi^2 - t^2 1_3 = 0,$$

and hence, $\mathrm{Tr}(\Xi^2) = -2t$. Therefore, we see

$$\begin{aligned}\mathrm{Tr}(\Theta^3) &= \left(\frac{2h-1}{h}\right)^3 \mathrm{Tr}(\Xi^3) + \frac{6t(2h-1)^2}{h^2} - 3\\ &= \left(\frac{2h-1}{h}\right)^3 (-t\mathrm{Tr}(\Xi) - 3t) + 6h - 3\\ &= -3t\left(\frac{2h-1}{h}\right)^3 + 6h - 3\\ &= -3(2h-1) + 6h - 3 = 0.\end{aligned}$$

Thus we found such $\Theta \in \mathcal{A}_t$ as we have $\mathrm{Tr}\left(\Theta^3\right) = 0$. The proof of Proposition 7.1 is completed. □

Remark 7.2. In the proof of the final part of Proposition 7.1, we saw that the isomorphism of $\tilde{H}(0,t)$ to $\tilde{H}(0,t')$ was obtained from a linear transformation of $K_t = K_{t'}$ defined by the base change $\{1, \xi, \xi^2\}$ and $\{1, \xi', \xi'^2\}$ of K_t as a $\mathbf{Q}$-space. In the forthcoming paper [1] by Akinari Hoshi and the author, a necessary and sufficient condition for $K_t = K_{t'}$ is obtained. Namely,

Proposition 7.3. *Let the notation and the assumptions be as above; in particular, suppose that $R(t;X)$ with $t \in \mathbf{Q}$ is irreducible over $\mathbf{Q}$. Then $K_t = K_{t'}$ for $t' \in \mathbf{Q}$ if and only if there exists such an element $u \in \mathbf{Q}$ as*

$$t' = t(u^2 + 9u - 3t)^3/(u^3 - 2tu^2 - 9tu - 2t^2 - 27t)^2.$$

Since the condition $K_t = K_{t'}$ is reciprocal in t and t', so should the latter condition of the proposition be. Indeed, let T and U be two independent variables, and put

$$\begin{aligned}T' &:= T(U^2 + 9U - 3T)^3/(U^3 - 2TU^2 - 9TU - 2T^2 - 27T)^2,\\ U' &:= -(U^2 + 3T)(U^2 + 9U - 3T)/(U^3 - 2TU^2 - 9TU - 2T^2 - 27T).\end{aligned}$$

Then we have a rational endomorphism of the rational function field $k(T,U)$ of two variables, $\Phi : k(T,U) \to k(T,U)$, by assigning (T',U') to (T,U). The endomorphism Φ is involutive; that is, $\Phi \circ \Phi$ is equal to the identity map. Hence Φ is an automorphism of $k(T,U)$ and an involutive Cremona transformation of dimension 2.

References

[1] A. Hoshi et K. Miyake – Tschirnhausen transformation of a cubic generic polynomial and a 2-dimensional involutive Cremona transformation, *Proc. Japan Acad. Ser. A Math. Sci.* **83** (2007), no. 3, p. 21–26.

[2] D. Husemoller – *Elliptic curves*, Graduate Texts in Mathematics, vol. 111, Springer-Verlag, New York, 1987, With an appendix by Ruth Lawrence.

[3] K. Miyake – Some families of Mordell curves associated to cubic fields, *Proceedings of the International Conference on Special Functions and their Applications (Chennai, 2002)*, vol. 160, 2003, p. 217–231.

[4] ———, An introduction to elliptic curves and their Diophantine geometry—Mordell curves, *Ann. Sci. Math. Québec* **28** (2004), no. 1-2, p. 165–178 (2005).

[5] ———, Two expositions on arithmetic of cubics, Number theory, Ser. Number Theory Appl., vol. 2, World Sci. Publ., Hackensack, NJ, 2007, p. 136–154.

[6] L. J. Mordell – *Diophantine equations*, Pure and Applied Mathematics, Vol. 30, Academic Press, London, 1969.

Katsuya Miyake
Department of Mathematics
School of Fundamental Science and
Engineering
Waseda University
3–4–1 Ohkubo Shinjuku-ku
Tokyo, 169-8555
Japan
miyakek@aoni.waseda.jp