Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Akinari HOSHI

Complete solutions to a family of Thue equations of degree 12

Tome 29, n° 2 (2017), p. 549-568.

<http://jtnb.cedram.org/item?id=JTNB_2017__29_2_549_0>

Journal de Théorie des Nombres
de Bordeaux **29** (2017), 549–568

Complete solutions to a family of Thue equations of degree 12

par Akinari HOSHI

Résumé. We considérons une famille paramétrique non galoisienne d'équations de Thue $F_m(x, y) = \lambda$ de degré 12 où m est un paramètre entier et où λ est un diviseur de $729(m^2 + 3m + 9)$. En utilisant la méthode d'isomorphismes de corps développée dans [15], nous montrons que ces équations ont seulement des solutions triviales avec $xy(x + y)(x - y)(x + 2y)(2x + y) = 0$.

Abstract. We consider a parametric non-Galois family of Thue equations $F_m(x, y) = \lambda$ of degree 12 where m is an integral parameter and λ is a divisor of $729(m^2 + 3m + 9)$. Using the field isomorphism method which is developed in [15], we show that the equations have only the trivial solutions with $xy(x + y)(x - y) \cdot (x + 2y)(2x + y) = 0$.

1. Introduction

In 1909 Thue [36] showed that an equation $F(x, y) = \lambda$, where $F(X, Y) \in \mathbb{Z}[X, Y]$ is an irreducible binary form of degree $d \geq 3$ and $\lambda \in \mathbb{Z}$ is a non-zero integer, has only finitely many integral solutions $(x, y) \in \mathbb{Z}^2$. In 1968 Baker [3] proved that the equation $F(x, y) = \lambda$ can be solved effectively. Numerical methods for solving a Thue equation are developed by Tzanakis and de Weger [37] and Bilu and Hanrot [5].

In 1990 Thomas [35] investigated a family of Thue equations $F_m^{(3)}(X, Y) = \pm 1$ where

$$F_m^{(3)}(X, Y) = X^3 - mX^2Y - (m + 3)XY^2 - Y^3.$$

The equations $F_m^{(3)}(X, Y) = \pm 1$ are completely solved by Thomas [35] and Mignotte [28]. Several families of Thue equations of degree $d \leq 6$ have been

Manuscrit reçu le 30 décembre 2015, révisé le 5 juillet 2016, accepté le 12 septembre 2016.
Mathematics Subject Classification. 11D25, 11D41, 11R16, 11R20, 12F10.
Mots-clefs. Thue equations, simplest cubic fields, simplest sextic fields.
This work was partially supported by JSPS KAKENHI Grant Numbers 22740028, 25400027.

studied by many authors (see e.g. [13], [12]). Let

$$F_m^{(4)}(X,Y) = X^4 - mX^3Y - 6X^2Y^2 + mXY^3 + Y^4,$$
$$F_m^{(6)}(X,Y) = X^6 - 2mX^5Y - 5(m+3)X^4Y^2 - 20X^3Y^3 + 5mX^2Y^4 + 2(m+3)XY^5 + Y^6.$$

For $d = 3, 4, 6$, the splitting fields $L_m^{(d)}$ of $F_m^{(d)}(X,1)$ over $\mathbb{Q}$ are totally real cyclic Galois extensions of $\mathbb{Q}$ of degree d if $m \in \mathbb{Z}$ ($d = 3$), $m \in \mathbb{Z} \setminus \{0, \pm 3\}$ ($d = 4$), $m \in \mathbb{Z} \setminus \{-8, -3, 0, 5\}$ ($d = 6$), and called the simplest cubic, quartic and sextic fields (see e.g. [9]). Lettl and Pethö [26] and Chen and Voutier [6] solved the family of quartic Thue equations $F_m^{(4)}(X,Y) = \lambda$ where $\lambda \in \{\pm 1, \pm 4\}$, and Lettl, Pethö and Voutier [27] determined all primitive solutions to the Thue inequalities $|F_m^{(4)}(X,Y)| \leq 6m + 7$ and $|F_m^{(6)}(X,Y)| \leq 120m + 323$. A family of Thue equations of degree 8 is solved by Heuberger, Togbé and Ziegler [14]. In [15] and [16], the author determined solutions to the families of Thue equations $F_m^{(d)}(X,Y) = \lambda_d$ of degree $d = 3$ and 6 where $m \in \mathbb{Z}$, λ_3 is a divisor of $m^3 + 3m + 9$ and λ_6 is a divisor of $27(m^2 + 3m + 9)$. See also the quartic case [17].

The aim of this paper is to generalize the results in [15, 16] to the case of degree 12. Let

$$\begin{aligned} F_m(X,Y) = X^{12} &- 4mX^{11}Y - 22(m+3)X^{10}Y^2 - 220X^9Y^3 \\ &+ 165mX^8Y^4 + 264(m+3)X^7Y^5 + 924X^6Y^6 \\ &- 264mX^5Y^7 - 165(m+3)X^4Y^8 - 220X^3Y^9 \\ &+ 22mX^2Y^{10} + 4(m+3)XY^{11} + Y^{12}. \end{aligned}$$

The polynomial $f_m(X) = F_m(X,1)$ is irreducible over $\mathbb{Q}$ if $m \in \mathbb{Z} \setminus \{-8, -3, 0, 5\}$. In general, however, the root field $\mathbb{Q}(\theta)$ with $f_m(\theta) = 0$ is not a Galois extension of $\mathbb{Q}$. For $m \in \mathbb{Z} \setminus \{-8, -3, 0, 5\}$, the splitting field L_m of $f_m(X)$ over $\mathbb{Q}$ is a totally real Galois extension of $\mathbb{Q}$ of degree 24 or 12 whose Galois group is isomorphic to $D_4 \times C_3$ or $C_6 \times C_2$ where D_4 is the dihedral group of order 8 and C_n is the cyclic group of order n. There exist infinitely many integers $m \in \mathbb{Z}$ for which L_m are of degree 24 and of degree 12 respectively. Moreover, we have the field inclusions $L_m^{(3)} \subset L_m^{(6)} \subset L_m$ for arbitrary $m \in \mathbb{Z}$ where $L_m^{(3)}$ are the simplest cubic fields and $L_m^{(6)}$ are the simplest sextic fields. We use Okazaki's theorem (see [15, Theorem 1.4]) which claims that for $m \geq -1$, the simplest cubic fields are non-isomorphic to each other except for $m = -1, 0, 1, 2, 3, 5, 12, 54, 66, 1259, 2389$. Okazaki's theorem was reproved in [15, Section 1].

The method of this paper, *the field isomorphism method*, is developed in [18], [15] (see also [22]) and applied in [16] and [4]. It uses the splitting field L_m and is purely algebraic although it depends on Okazaki's theorem which was established by usual methods of analytic number theory: geometric gap principles in the theory of geometry of numbers and a result of Laurent, Mignotte and Nesterenko [25] in Baker's theory on linear forms in logarithms of algebraic numbers (see also [29], [38]). We remark that the method may work well only for the case where the genus of the curve $F_s(X,1)=0$ is zero.

We may assume that $m \geq -1$ because if $(x,y) \in \mathbb{Z}^2$ is a solution to $F_m(x,y)=\lambda$, then we have $F_{-m-3}(y,x)=\lambda$. The binary form $F_m(X,Y) \in \mathbb{Z}[X,Y]$ is invariant under the action of the cyclic group C_6 of order 6 with $C_6 : X \mapsto -Y, Y \mapsto X+Y$. Hence if we get a solution $(x,y) \in \mathbb{Z}^2$ to $F_m(x,y)=\lambda$, then we have another 5 solutions:

$$(-y, x+y),\ (-x-y, x),\ (-x,-y),\ (y,-x-y),\ (x+y,-x).$$

We also obtain $F_m(x-y, x+2y) = 729 F_m(x,y)$. The equation $F_m(x,y)=\lambda$ has the following solutions for $\lambda = c^{12}$ and $\lambda = 729c^{12}$:

$$F_m(0,\pm c) = F_m(\pm c, 0) = F_m(\pm c, \mp c) = c^{12},$$
$$F_m(\pm c, \pm c) = F_m(\pm 2c, \mp c) = F_m(\pm c, \mp 2c) = 729c^{12}.$$

We call such solutions $(x,y) \in \mathbb{Z}^2$ to $F_m(x,y)=\lambda$ with $xy(x+y)(x-y)\cdot(x+2y)(2x+y)=0$ the *trivial* solutions in the present paper. The main result of this paper is the following:

Theorem 1.1. *Let $m \in \mathbb{Z}$ and λ be a divisor of $729(m^2+3m+9)$. The equation $F_m(x,y)=\lambda$ has only the trivial solutions $(x,y) \in \mathbb{Z}^2$ with $xy(x+y)(x-y)(x+2y)(2x+y)=0$.*

2. Construction of $f_s(X)$ of degree 12

Let K be a field with char $K \neq 2,3$ and $K(z)$ be the rational function field over K with variable z. We take the matrix

$$M_{12} = \begin{pmatrix} \sqrt{3}+1 & -1 \\ 1 & \sqrt{3}+2 \end{pmatrix}$$

of order 12 in $\mathrm{PGL}_2(K(\sqrt{3}))$. We will construct the polynomial $f_s(X) = F_s(X,1)$ of degree 12 via the matrix M_{12}. Let the matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PGL}_2(K(\sqrt{3}))$ act on $K(\sqrt{3})(z)$ by

$$M : \sqrt{3} \ \mapsto\ \sqrt{3},\ z\ \mapsto\ \frac{az+b}{cz+d}.$$

Then we have

$$M_{12}^2 \sim \begin{pmatrix} 1 & -1 \\ 1 & 2 \end{pmatrix},\ M_{12}^3 \sim \begin{pmatrix} \sqrt{3}-1 & -2 \\ 2 & \sqrt{3}+1 \end{pmatrix},$$
$$M_{12}^4 \sim \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix},\ M_{12}^6 \sim \begin{pmatrix} -1 & -2 \\ 2 & 1 \end{pmatrix}$$

where $\sim$ means the equality in $\mathrm{PGL}_2(K(\sqrt{3}))$, and the matrix M_{12} induces a $K(\sqrt{3})$-automorphism σ of $K(\sqrt{3})(z)$ of order 12:

$$\begin{aligned}(2.1)\qquad \sigma : z \ &\mapsto\ Z \ \mapsto\ \frac{z-1}{z+2} \ \mapsto \frac{Z-1}{Z+2} \ \mapsto\ -\frac{1}{z+1} \\ &\mapsto\ -\frac{1}{Z+1} \ \mapsto\ -\frac{z+2}{2z+1} \ \mapsto\ -\frac{Z+2}{2Z+1} \ \mapsto\ -\frac{z+1}{z} \\ &\mapsto\ -\frac{Z+1}{Z} \ \mapsto\ -\frac{2z+1}{z-1} \ \mapsto\ -\frac{2Z+1}{Z-1} \ \mapsto\ z\end{aligned}$$

where

$$Z = \frac{(\sqrt{3}+1)z-1}{z+\sqrt{3}+2}.$$

Hence we have the cyclic Galois extension $K(\sqrt{3},z)/K(\sqrt{3},z)^{\langle\sigma\rangle}$ of degree 12. We get the generating polynomial

$$\begin{aligned}f_s(X) &= \prod_{i=1}^{12}\Big(X-\sigma^i(z)\Big) \\ &= X^{12}-4sX^{11}-22(s+3)X^{10}-220X^9 \\ &\qquad\qquad +165sX^8+264(s+3)X^7+924X^6-264sX^5 \\ &\qquad\qquad -165(s+3)X^4-220X^3+22sX^2+4(s+3)X+1\end{aligned}$$

of the cyclic Galois field $K(\sqrt{3},z)$ over $K(\sqrt{3},z)^{\langle\sigma\rangle}=K(\sqrt{3})(s)$ where

$$\begin{aligned}s &= \frac{z^{12}-66z^{10}-220z^9+792z^7+924z^6-495z^4-220z^3+12z+1}{z(4z^{10}+22z^9-165z^7-264z^6+264z^4+165z^3-22z-4)} \\ &= \frac{(z^3-3z-1)(z^3+6z^2+3z-1)(z^6-6z^5-30z^4-20z^3+15z^2+12z+1)}{z(z+1)(z-1)(z+2)(2z+1)(z^2-2z-2)(z^2+4z+1)(2z^2+2z-1)}.\end{aligned}$$

The discriminant of $f_s(X)$ with respect to X is $2^{24}3^{45}(s^2+3s+9)^{11}$. In [31, 32, 33], for $q=2^n$, p^n and $2n$, Shen and Washington constructed cyclic polynomials $g_s^{(q)}(X)\in K(s)[X]$ over K of degree q where K is the real q-th cyclotomic field. When $q=12$, they take the matrix $M'=\begin{pmatrix} 1 & -1 \\ 1 & \sqrt{3}+1 \end{pmatrix}$ $\in \mathrm{PGL}_2(K(\sqrt{3}))$ of order 12. However, the generating polynomial $g_s^{(12)}(X)$ is in $K(\sqrt{3})(s)[X]$ but not in $K(s)[X]$. On the other hand, the polynomial

$f_s(X)$ is defined over not only $K(\sqrt{3})(s)$ but also $K(s)$. This is the reason why we take M_{12} instead of M'. In the case where $\sqrt{3} \in K$, the splitting field $\mathrm{Spl}_{K(s)} f_s(X)$ of $f_s(X)$ over $K(s) = K(\sqrt{3})(s)$ is a Galois extension of the rational function field $K(s)$ with cyclic Galois group of order 12. However, if $\sqrt{3} \notin K$, then the splitting field $\mathrm{Spl}_{K(s)} f_s(X)$ is not a regular extension of K.

From now on, we assume that $\sqrt{3} \notin K$. Let τ be an involution of $K(\sqrt{3}, z)$ defined by

$$\tau : \sqrt{3} \mapsto -\sqrt{3},\ z \mapsto z. \tag{2.2}$$

The splitting field $\mathrm{Spl}_{K(s)} f_s(X) = K(\sqrt{3}, z)$ is a Galois extension of $K(s) = K(\sqrt{3}, z)^{\langle \sigma, \tau \rangle}$ with the Galois group $H_{24} = \langle \sigma, \tau \rangle$ of order 24. The group H_{24} is given as

$$\begin{aligned} H_{24} &= \langle \sigma, \tau \mid \sigma^{12} = \tau^2 = 1, \tau\sigma\tau^{-1} = \sigma^7 \rangle \simeq C_{12} \rtimes C_2 \\ &= \langle \sigma^3, \tau \mid (\sigma^3)^4 = \tau^2 = 1, \tau\sigma^3\tau^{-1} = (\sigma^3)^{-1} \rangle \times \langle \sigma^4 \rangle \simeq D_4 \times C_3 \end{aligned}$$

where C_n is the cyclic group of order n and D_4 is the dihedral group of order 8.

There exist three subgroups $\langle \sigma^2, \tau \rangle$, $\langle \sigma \rangle$ and $\langle \sigma^2, \sigma\tau \rangle$ of order 12 of H_{24}. We have

$$\begin{aligned} K(\sqrt{3}, z)^{\langle \sigma^2, \tau \rangle} &= K(s)(\sqrt{s^2 + 3s + 9}), \\ K(\sqrt{3}, z)^{\langle \sigma \rangle} &= K(s)(\sqrt{3}), \\ K(\sqrt{3}, z)^{\langle \sigma^2, \sigma\tau \rangle} &= K(s)(\sqrt{3(s^2 + 3s + 9)}) \end{aligned} \tag{2.3}$$

because

$$\sum_{\sigma' \in \langle \sigma^2, \tau \rangle} \sigma'(z)/4 = \frac{(z^3 + 3z^2 - 1)(z^3 - 3z^2 - 6z + 1)}{z(z+1)(z-1)(z+2)(2z+1)} = \sqrt{s^2 + 3s + 9} + s.$$

The other equalities of (2.3) are established by a similar computation.

The group H_{24} may be regarded as the subgroup $\langle \sigma, \tau \rangle$ of the symmetric group S_{12} of degree 12 as permutation group on the roots of $f_s(X)$ where $\sigma = (1, \ldots, 12)$ and $\tau = (2, 8)(4, 10)(6, 12)$. Then the only two proper subgroups $\langle \sigma \rangle$ and $\langle \sigma^2, \sigma\tau \rangle$ are transitive in S_{12}. Hence $f_s(X)$ is irreducible over $K(s)(\sqrt{3})$ and over $K(s)(\sqrt{3(s^2 + 3s + 9)})$ but is reducible over $K(s)(\sqrt{s^2 + 3s + 9})$. We will explain this later, see (2.6).

The group H_{24} has the unique subgroup $\langle \sigma^3, \tau \rangle \simeq D_4$ of order 8. The group $\langle \sigma^3, \tau \rangle$ is normal in H_{24} and the corresponding cyclic cubic field over $K(s)$ is given by $K(\sqrt{3}, z)^{\langle \sigma^3, \tau \rangle} = K(s)(z_3)$ where

$$z_3 = \sum_{\sigma' \in \langle \sigma^3, \tau \rangle} \sigma'(z)/8 = \frac{z(z+2)(z^2 - 2z - 2)}{(2z+1)(2z^2 + 2z - 1)}.$$

The action of H_{24} of order 3 on the field $K(s)(z_3)$ is given by

$$\sigma : s \;\mapsto\; s,\; z_3 \;\mapsto\; -\frac{1}{z_3+1} \;\mapsto\; -\frac{z_3+1}{z_3} \;\mapsto\; z_3.$$

Hence the cubic field $K(s)(z_3)$ is the simplest cubic field of Shanks' type (cf. Shanks [30]) over $K(s)$, and the minimal polynomial of z_3 over $K(s)$ is given by

$$f_s^{(3)}(X) = \prod_{z' \in \mathrm{Orb}_{H_{24}}(z_3)} \Big(X - z'\Big) = X^3 - sX^2 - (s+3)X - 1. \tag{2.4}$$

The discriminant of the cubic polynomial $f_s^{(3)}(X)$ is $(s^2+3s+9)^2$.

There exist five subgroups $\langle\sigma^4\tau\rangle$, $\langle\sigma^2\tau\rangle$, $\langle\sigma^2\rangle$, $\langle\sigma\tau\rangle$ and $\langle\tau\sigma\rangle$ of order 6 of H_{24}, and only the group $\langle\sigma^2\rangle$ is normal in H_{24}. We have $K(\sqrt{3},z)^{\langle\sigma^2\rangle} = K(s)(\sqrt{3},\sqrt{s^2+3s+9})$.

There exist three subgroups $\langle\sigma^6,\tau\rangle$, $\langle\sigma^3\rangle$ and $\langle\sigma^6,\sigma^3\tau\rangle$ of order 4 of H_{24} which are normal in H_{24}. The three quotient groups $H_{24}/\langle\sigma^6,\tau\rangle$, $H_{24}/\langle\sigma^3\rangle$ and $H_{24}/\langle\sigma^6,\sigma^3\tau\rangle$ are cyclic group of order 6 and we have the corresponding cyclic sextic fields over $K(s)$:

$$\begin{aligned} K(\sqrt{3},z)^{\langle\sigma^6,\tau\rangle} &= K(s)(z_3,\sqrt{s^2+3s+9}),\\ K(\sqrt{3},z)^{\langle\sigma^3\rangle} &= K(s)(z_3,\sqrt{3}),\\ K(\sqrt{3},z)^{\langle\sigma^6,\sigma^3\tau\rangle} &= K(s)(z_3,\sqrt{3(s^2+3s+9)}). \end{aligned}$$

In particular, the first one is "the simplest sextic field" over $K(s)$ which means that the field $K(\sqrt{3},z)^{\langle\sigma^6,\tau\rangle}$ is given by $K(s)(z_6)$ where

$$z_6 = \sum_{\sigma' \in \langle\sigma^6,\tau\rangle} \sigma'(z)/4 = \frac{(z+1)(z-1)}{2z+1}$$

and the minimal polynomial of z_6 over $K(s)$ is given by

$$\begin{aligned} f_s^{(6)}(X) &= \prod_{z' \in \mathrm{Orb}_{H_{24}}(z_6)} \Big(X - z'\Big) \\ &= X^6 - 2sX^5 - 5(s+3)X^4 - 20X^3 + 5sX^2 + 2(s+3)X + 1 \end{aligned} \tag{2.5}$$

with discriminant $2^6 3^6 (s^2+3s+9)^5$.

The unique subgroup of order 3 of H_{24} is $\langle\sigma^4\rangle$. The field $K(\sqrt{3},z)^{\langle\sigma^4\rangle}$ is a Galois extension of $K(s)$ with Galois group D_4.

There exist five subgroups $\langle\tau\rangle$, $\langle\sigma^6\tau\rangle$, $\langle\sigma^6\rangle$, $\langle\sigma^3\tau\rangle$ and $\langle\sigma^9\tau\rangle$ of order 2 of H_{24}. The group $\langle\sigma^6\rangle$ is the commutator subgroup of H_{24} and the abelianization $H_{24}^{ab} = H_{24}/\langle\sigma^6\rangle$ of H_{24} is isomorphic to $C_6 \times C_2$. The other four groups of order 2 are not normal in H_{24}.

The three polynomials

$$\begin{aligned}
f_s^{(3)}(X) &= X^3 - 3X - 1 - sX(X+1),\\
f_s^{(6)}(X) &= f_{-3}^{(3)}(X) f_3^{(3)}(X) - sX(X+1)(X-1)(X+2)(2X+1),\\
f_s(X) &= f_{-6}^{(3)}(X) f_0^{(3)}(X) f_3^{(6)}(X) - sX(X+1)(X-1)(X+2)(2X+1)\\
&\qquad \cdot (X^2-2X-2)(X^2+4X+1)(2X^2+2X-1)
\end{aligned}$$

satisfy the following remarkable equations:

$$\begin{aligned}
f_s^{(6)}(X) &= (f_s^{(3)}(X))^2 - (s^2+3s+9)X^2(X+1)^2\\
&= f^{(3)}_{s+\sqrt{s^2+3s+9}}(X) f^{(3)}_{s-\sqrt{s^2+3s+9}}(X),\\
f_s(X) &= (f_s^{(6)}(X))^2\\
&\quad - (s^2+3s+9)X^2(X+1)^2(X-1)^2(X+2)^2(2X+1)^2\\
&= f^{(6)}_{s+\sqrt{s^2+3s+9}}(X) f^{(6)}_{s-\sqrt{s^2+3s+9}}(X).
\end{aligned} \tag{2.6}$$

3. Field intersection problem

We recall some basic results in the computational aspects of Galois theory (cf. e.g. [1], [7], [8]). Let K be a field with char $K \neq 2, 3$ and $\overline{K}$ be a fixed algebraic closure of K. Let $f(X) = \prod_{i=1}^m (X - \alpha_i) \in K[X]$ be a separable polynomial of degree m with some fixed order of the roots $\alpha_1, \ldots, \alpha_m \in \overline{K}$. Let $R = K[x_1, \ldots, x_m]$ be the polynomial ring over K with m variables $x_1, \ldots, x_m$. For an element Θ in R, we take the specialization map $\omega_f : R \to K(\alpha_1, \ldots, \alpha_m)$, $\Theta(x_1, \ldots, x_m) \mapsto \Theta(\alpha_1, \ldots, \alpha_m)$. The kernel of ω_f is the ideal $I_f = \{\Theta \in R \mid \Theta(\alpha_1, \ldots, \alpha_m) = 0\}$ in R. Let S_m be the symmetric group of degree m. We extend the action of S_m on m letters $\{1, \ldots, m\}$ to that on R by $\pi(\Theta(x_1, \ldots, x_m)) = \Theta(x_{\pi(1)}, \ldots, x_{\pi(m)})$. The Galois group of $f(X)$ over K is defined by $\mathrm{Gal}_K f(X) = \{\pi \in S_m \mid \pi(I_f) \subseteq I_f\}$, and $\mathrm{Gal}_K f(X)$ is isomorphic to the Galois group of the splitting field $\mathrm{Spl}_K f(X)$ of $f(X)$ over K. If we take another ordering of roots $\alpha_{\pi(1)}, \ldots, \alpha_{\pi(m)}$ of $f(X)$ for some $\pi \in S_m$, then the corresponding realization of $\mathrm{Gal}_K f(X)$ is conjugate in S_m. Hence, for arbitrary ordering of the roots of $f(X)$, $\mathrm{Gal}_K f(X)$ is determined up to conjugacy in S_m.

For $H \leq U \leq S_m$, $\Theta \in R$ is called a U-primitive H-invariant if $H = \mathrm{Stab}_U(\Theta) = \{\pi \in U \mid \pi(\Theta) = \Theta\}$. For a U-primitive H-invariant Θ, the polynomial

$$\mathcal{RP}_{\Theta,U}(X) = \prod_{\overline{\pi} \in U/H} (X - \pi(\Theta)) \in R^U[X]$$

where $\overline{\pi}$ runs through a system of left coset representatives of H in U, is called the *formal* U-relative H-invariant resolvent by Θ. The polynomial

$$\mathcal{RP}_{\Theta,U,f}(X) = \omega_f(\mathcal{RP}_{\Theta,U}(X))$$

is called the U-relative H-invariant resolvent of f by Θ. The following theorem is fundamental in the theory of resolvent polynomials (see e.g. [1, p. 95]).

Theorem 3.1. *Let $G = \mathrm{Gal}_K f(X)$, $H \leq U \leq S_m$ be finite groups with $G \leq U$ and Θ be a U-primitive H-invariant. Suppose that $\mathcal{RP}_{\Theta,U,f}(X) = \prod_{i=1}^{l} h_i^{e_i}(X)$ gives the decomposition of $\mathcal{RP}_{\Theta,U,f}(X)$ into a product of powers of distinct irreducible polynomials $h_i(X)$, $(i = 1, \ldots, l)$, in $K[X]$. Then we have a bijection*

$$\begin{aligned} G\backslash U/H &\longrightarrow \{h_1^{e_1}(X), \ldots, h_l^{e_l}(X)\} \\ G\pi H &\longmapsto h_\pi(X) = \prod_{\tau H \subseteq G\pi H} (X - \omega_f(\tau(\Theta))) \end{aligned}$$

where the product runs through the left cosets τH of H in U contained in $G\pi H$, that is, through $\tau = \pi_\sigma \pi$ where π_σ runs through a system of representatives of the left cosets of $G \cap \pi H \pi^{-1}$ in G; each $h_\pi(X)$ is irreducible or a power of an irreducible polynomial with $\deg(h_\pi(X)) = |G\pi H|/|H| = |G|/|G \cap \pi H \pi^{-1}|$.

Corollary 3.2. *If $G \leq \pi H \pi^{-1}$ for some $\pi \in U$, then $\mathcal{RP}_{\Theta,U,f}(X)$ has a linear factor over K. Conversely, if $\mathcal{RP}_{\Theta,U,f}(X)$ has a non-repeated linear factor over K, then there exists $\pi \in U$ such that $G \leq \pi H \pi^{-1}$.*

In the case where $\mathcal{RP}_{\Theta,U,f}(X)$ is not squarefree, we may take a suitable Tschirnhausen transformation $\hat{f}$ of f over K such that $\mathcal{RP}_{\Theta,U,\hat{f}}(X)$ is squarefree (cf. [7, Alg. 6.3.4]).

We now apply Theorem 3.1 to the case $m = 24$ and $f(X) = f_a(X) f_b(X)$ where

$$\begin{aligned} f_a(X) = X^{12} - 4aX^{11} - 22(a+3)X^{10} - 220X^9 \\ + 165aX^8 + 264(a+3)X^7 + 924X^6 - 264aX^5 \\ - 165(a+3)X^4 - 220X^3 + 22aX^2 + 4(a+3)X + 1 \end{aligned}$$

of degree 12 for $a \in K$. The reader may find the similar argument of the resolvent polynomials in the non-abelian group cases in [18, 19, 20, 21]. Let $K(\sqrt{3})(z)$ be the rational function field over $K(\sqrt{3})$ with variable z. Let σ and τ be K-automorphisms of $K(\sqrt{3}, z)$ as in (2.1) and (2.2). Then the field $K(\sqrt{3}, z)$ is the splitting field of $f_s(X)$ over $K(\sqrt{3}, z)^{\langle \sigma, \tau \rangle} = K(s)$ with Galois group $H_{24} = \langle \sigma, \tau \rangle$ (resp. $C_{12} = \langle \sigma \rangle$) if $\sqrt{3} \notin K$ (resp. $\sqrt{3} \in K$). We also take another rational function field $K(\sqrt{3})(w)$ over $K(\sqrt{3})$ with variable w, K-automorphisms

$$\sigma' : \sqrt{3} \mapsto \sqrt{3},\ w \mapsto \frac{(\sqrt{3}+1)w - 1}{w + \sqrt{3} + 2}, \quad \tau' : \sqrt{3} \mapsto -\sqrt{3},\ w \mapsto w$$

and the element

$$t = \frac{w^{12} - 66w^{10} - 220w^9 + 792w^7 + 924w^6 - 495w^4 - 220w^3 + 12w + 1}{w(4w^{10} + 22w^9 - 165w^7 - 264w^6 + 264w^4 + 165w^3 - 22w - 4)}$$

of $K(w)$ by the same manner of $K(\sqrt{3})(z)$, σ, τ and s as in Section 2. Then the field $K(\sqrt{3}, w)$ is the splitting field of $f_t(X)$ over $K(\sqrt{3}, w)^{H'_{24}} = K(t)$ with $H'_{24} = \langle \sigma', \tau' \rangle$. We extend the actions of σ and τ on $K(\sqrt{3}, z)$ and σ' and τ' on $K(\sqrt{3}, w)$ to these on $K(\sqrt{3}, z, w)$ by

$$\sigma : \sqrt{3} \mapsto \sqrt{3}, z \mapsto \frac{(\sqrt{3}+1)z - 1}{z + \sqrt{3} + 2}, w \mapsto w, \ \tau : \sqrt{3} \mapsto -\sqrt{3}, z \mapsto z, w \mapsto w,$$

$$\sigma' : \sqrt{3} \mapsto \sqrt{3}, z \mapsto z, w \mapsto \frac{(\sqrt{3}+1)w - 1}{w + \sqrt{3} + 2}, \ \tau' : \sqrt{3} \mapsto -\sqrt{3}, z \mapsto z, w \mapsto w.$$

Then $\tau = \tau'$ and the field $K(\sqrt{3}, z, w)$ is a Galois extension of $K(s, t) = K(\sqrt{3}, z, w)^{\langle \sigma, \sigma', \tau \rangle}$ whose Galois group is $\langle \sigma, \sigma', \tau \rangle \simeq (H_{24} \times H'_{24})/\langle (\tau, \tau') \rangle$ of order 288 (resp. $\langle \sigma, \sigma' \rangle \simeq C_{12} \times C_{12}$ of order 144) if $\sqrt{3} \notin K$ (resp. $\sqrt{3} \in K$).

For $a, b \in K$, we define

$$L_a = \mathrm{Spl}_K f_a(X), \qquad G_a = \mathrm{Gal}_K f_a(X),$$
$$f_{a,b}(X) = f_a(X) f_b(X), \qquad G_{a,b} = \mathrm{Gal}_K f_{a,b}(X).$$

After the specialization $s \mapsto a \in K$, we assume that the polynomial $f_a(X)$ is separable, that is $a^2 + 3a + 9 \neq 0$, and also irreducible over K. Then the Galois group G_a is isomorphic to H_{24} or $C_6 \times C_2$ (resp. C_{12}) if $\sqrt{3} \notin K$ (resp. $\sqrt{3} \in K$).

For a squarefree polynomial $\mathcal{R}(X) \in K[X]$ of degree l, we define the *decomposition type* $\mathrm{DT}(\mathcal{R})$ of $\mathcal{R}(X)$ by the partition of l induced by the degrees of the irreducible factors of $\mathcal{R}(X)$ over K. Via the decomposition type $\mathrm{DT}(\mathcal{R}_i)$ of the resolvent polynomial $\mathcal{R}_i(X)$, we get an answer of the field intersection problem, i.e. for $a, b \in K$ determine the intersection $L_a \cap L_b$ of the splitting fields L_a and L_b.

Theorem 3.3. *Assume* $(a^2 + 3a + 9)(b^2 + 3b + 9) \neq 0$*,* $f_a(X)$ *and* $f_b(X)$ *are irreducible over* K *and* $\#G_a \geq \#G_b$ *for* $a, b \in K$*. Let* $U = \langle \sigma, \sigma', \tau \rangle$ (*resp.* $\langle \sigma, \sigma' \rangle$), $H_i = \langle \sigma(\sigma')^i, \tau \rangle$, (*resp.* $\langle \sigma(\sigma')^i \rangle$), Θ_i *be a* U*-primitive* H_i*-invariant and* $\mathcal{R}_i(X) = \mathcal{RP}_{\Theta_i, U, f_{a,b}}(X)$ *for* $i = 1, 5, 7, 11$*. Assume that each* $\mathcal{R}_i(X)$ *is squarefree. If* $\sqrt{3} \notin K$ (*resp.* $\sqrt{3} \in K$)*, then the Galois group* $G_{a,b} = \mathrm{Gal}_K f_{a,b}(X)$ *and the intersection field* $L_a \cap L_b$ *are given by the decomposition types* $\mathrm{DT}(\mathcal{R}_i)$ *as in Table 3.1* (*resp. Table 3.2*).

G_a	G_b	$G_{a,b}$		DT($\mathcal{R}_1$)	DT($\mathcal{R}_5$)	DT($\mathcal{R}_7$)	DT($\mathcal{R}_{11}$)
H_{24}	H_{24}	$(C_{12}\times C_{12})\rtimes C_2$	$L_a\cap L_b=K(\sqrt{3})$	12	12	12	12
		$D_4\times C_6\times C_3$	$[L_a\cap L_b:K]=4$	12	12	12	12
				6^2	6^2	6^2	6^2
		$(C_4^2\rtimes C_2)\times C_3$	$[L_a\cap L_b:K]=6$	12	4^3	12	4^3
				4^3	12	4^3	12
		$D_4\times C_3^2$	$[L_a\cap L_b:K]=8$	12	12	6^2	6^2
				6^2	6^2	12	12
				6^2	6^2	3^2, 6	3^2, 6
				3^2, 6	3^2, 6	6^2	6^2
		$D_4\times C_6$	$[L_a\cap L_b:K]=12$	12	4^3	12	4^3
				4^3	12	4^3	12
				6^2	2^6	6^2	2^6
				2^6	6^2	2^6	6^2
		$D_4\times C_3$	$L_a=L_b$	12	4^3	6^2	2^6
				4^3	12	2^6	6^2
				6^2	2^6	12	4^3
				2^6	6^2	4^3	12
				6^2	2^6	3^2, 6	1^6, 2^3
				2^6	6^2	1^6, 2^3	3^2, 6
				3^2, 6	1^6, 2^3	6^2	2^6
				1^6, 2^3	3^2, 6	2^6	6^2
H_{24}	$C_6\times C_2$	$D_4\times C_6\times C_3$	$L_a\cap L_b=K(\sqrt{3})$	12	12	12	12
		$D_4\times C_3^2$	$[L_a\cap L_b:K]=4$	12	12	12	12
		$D_4\times C_6$	$[L_a\cap L_b:K]=6$	12	4^3	12	4^3
				4^3	12	4^3	12
		$D_4\times C_3$	$L_a\supset L_b$	12	4^3	12	4^3
				4^3	12	4^3	12
$C_6\times C_2$	$C_6\times C_2$	$C_6^2\times C_2$	$L_a\cap L_b=K(\sqrt{3})$	6^2	6^2	6^2	6^2
		$C_6\times C_6$	$[L_a\cap L_b:K]=4$	3^2, 6	3^2, 6	3^2, 6	3^2, 6
		$C_6\times C_2^2$	$[L_a\cap L_b:K]=6$	6^2	2^6	6^2	2^6
				2^6	6^2	2^6	6^2
		$C_6\times C_2$	$L_a=L_b$	3^2, 6	1^6, 2^3	3^2, 6	1^6, 2^3
				1^6, 2^3	3^2, 6	1^6, 2^3	3^2, 6

Table 3.1.

Proof. First we assume that $\sqrt{3}\notin K$. We apply Theorem 3.1 to $U=\langle\sigma,\sigma',\tau\rangle$, $H=H_i=\langle\sigma(\sigma')^i,\tau\rangle$ $(i=1,5,7,11)$ and any subgroup $G=G_{a,b}\le U$ with transitive G_a, $G_b\le S_{12}$. Indeed, we may regard U, $H_i\le S_{24}$ as permutation group in 24 letters where

$$\sigma=(1,\ldots,12)\in S_{12},$$
$$\sigma'=(13,\ldots,24)\in S'_{12},$$
$$\tau=(2,8)(4,10)(6,12)(14,20)(16,22)(18,24)\in S_{24}.$$

G_a	G_b	$G_{a,b}$		$\mathrm{DT}(\mathcal{R}_1)$	$\mathrm{DT}(\mathcal{R}_5)$	$\mathrm{DT}(\mathcal{R}_7)$	$\mathrm{DT}(\mathcal{R}_{11})$
C_{12}	C_{12}	$C_{12} \times C_{12}$	$L_a \cap L_b = K$	12	12	12	12
		$C_{12} \times C_6$	$[L_a \cap L_b : K] = 2$	6^2	6^2	6^2	6^2
		$C_{12} \times C_4$	$[L_a \cap L_b : K] = 3$	12	4^3	12	4^3
				4^3	12	4^3	12
		$C_{12} \times C_3$	$[L_a \cap L_b : K] = 4$	6^2	6^2	3^4	3^4
				3^4	3^4	6^2	6^2
		$C_{12} \times C_2$	$[L_a \cap L_b : K] = 6$	6^2	2^6	6^2	2^6
				2^6	6^2	2^6	6^2
		C_{12}	$L_a = L_b$	6^2	2^6	3^4	1^{12}
				2^6	6^2	1^{12}	3^4
				3^4	1^{12}	6^2	2^6
				1^{12}	3^4	2^6	6^2

TABLE 3.2.

Then the decomposition types $\mathrm{DT}(\mathcal{R}_i)$ in Table 3.1 can be obtained by the formula $\deg(h_\pi(X)) = |G\pi H_i|/|H_i| = |G|/|G \cap \pi H_i \pi^{-1}|$. We may check it by GAP [34] via the the command `DoubleCosetRepsAndSizes`(U, G, H_i) for any subgroup $G \leq U$ with transitive $G|_{S_{12}} \leq S_{12}$ and $G|_{S'_{12}} \leq S'_{12}$. For the case where $\sqrt{3} \in K$, we may get Table 3.2 by the similar manner. $\square$

Corollary 3.4. *Assume that $\sqrt{3} \in K$, $G_a = G_b = C_{12}$ and each $\mathcal{R}_i(X)$ is squarefree for $a, b \in K$. Then the splitting fields L_a and L_b coincide if and only if* (*only*) *one of the polynomials $\mathcal{R}_i(X)$* $(i = 1, 5, 7, 11)$ *splits completely into twelve linear factors over K.*

4. Field isomorphism problem

In order to obtain an explicit answer to the field isomorphism problem of $f_s(X)$, i.e. whether the splitting fields $\mathrm{Spl}_K f_a(X)$ and $\mathrm{Spl}_K f_b(X)$ coincide for $a, b \in K$, we should seek suitable U-primitive H_i-invariants Θ_i for $i = 1, 5, 7, 11$ where U and H_i are given as in Theorem 3.3. It follows from [2, Theorem 1.4] that there exists $\langle \sigma\sigma' \rangle$-invariant Θ_1 such that $K(z, w) = K(z, \Theta_1)$. Moreover we may obtain the following U-primitive H_i-invariants Θ_i which satisfy $K(z, w) = K(z, \Theta_i)$.

Lemma 4.1. *Let*

$$\begin{aligned}
\Theta_1 &= \frac{z+1+zw}{-z+w},\\
\Theta_5 &= \frac{z(z^4+5z^3-10z-5)+(z+1)(z^4-z^3-9z^2-z+1)w}{-(z+1)(z^4-z^3-9z^2-z+1)+(5z^4+10z^3-5z-1)w},\\
\Theta_7 &= \frac{-(5z^4+10z^3-5z-1)+(z+1)(z^4-z^3-9z^2-z+1)w}{z(z^4+5z^3-10z-5)+(5z^4+10z^3-5z-1)w},\\
\Theta_{11} &= \frac{-1+zw}{z+1+w}.
\end{aligned}$$

Then the elements Θ_i $(i=1,5,7,11)$ are U-primitive H_i-invariants and the actions of σ on $K(\Theta_i)$ are given by

$$\sigma : \Theta_j \mapsto \frac{(\sqrt{3}+1)\Theta_j - 1}{\Theta_j+\sqrt{3}+2}, \quad \Theta_k \mapsto \frac{(\sqrt{3}-2)\Theta_k - 1}{\Theta_k+\sqrt{3}-1}$$

for $j=1,11$ and $k=5,7$, which are the same as the actions of σ and σ^5 on $K(z)$ respectively.

Remark 4.2. $\Theta_{11}(z,w)=\Theta_1(z,-w-1)$ *and* $\Theta_7(z,w)=\Theta_5(z,-w-1)$.

By Lemma 4.1, the resolvent $\mathcal{R}_i(X) = \mathcal{RP}_{\Theta_i,U,f_{a,b}}(X)$ is given by $\mathcal{R}_i(X)=f_{A_i}(X)$ for some $A_i \in K$. Indeed, we have the following:

Theorem 4.3. *Let Θ_i $(i=1,5,7,11)$ be as in Lemma 4.1. Then*

$$\mathcal{R}_i(X) = f_{A_i}(X)$$

where

$$\begin{aligned}
A_1 &= \frac{3a+9+ab}{-a+b},\\
A_5 &= \frac{-3a(a^4+15a^3-270a-405)-(a+3)(a^4-3a^3-81a^2-27a+81)b}{(a+3)(a^4-3a^3-81a^2-27a+81)-(5a^4+30a^3-135a-81)b},\\
A_7 &= \frac{-9(5a^4+30a^3-135a-81)+(a+3)(a^4-3a^3-81a^2-27a+81)b}{a(a^4+15a^3-270a-405)+(5a^4+30a^3-135a-81)b},\\
A_{11} &= \frac{-9+ab}{a+3+b}.
\end{aligned}$$

Proof. This can be done by a straightforward computation. □

Remark 4.4. $A_{11}(a,b)=A_1(a,-b-3)$ *and* $A_5(a,b)=A_7(a,-b-3)$.

Note that the discriminant $\mathrm{disc}(\mathcal{R}_i)$ of the polynomials $\mathcal{R}_i(X)$ are given by

$$\mathrm{disc}(\mathcal{R}_i) = \begin{cases} \dfrac{2^{24}3^{45}(a^2+3a+9)^{11}(b^2+3b+9)^{11}}{d_i^{22}} & \text{if } \ i=1,11, \\ \dfrac{2^{24}3^{45}(a^2+3a+9)^{55}(b^2+3b+9)^{11}}{d_i^{22}} & \text{if } \ i=5,7, \end{cases}$$

where

$$\begin{aligned} d_1 &= a-b, \\ d_5 &= (a+3)(a^4-3a^3-81a^2-27a+81)-(5a^4+30a^3-135a-81)b, \\ d_7 &= a(a^4+15a^3-270a-405)+(5a^4+30a^3-135a-81)b, \\ d_{11} &= a+b+3. \end{aligned} \tag{4.1}$$

The following theorem can be easily seen by inspecting Tables 3.1 and 3.2.

Theorem 4.5. *Let d_1, d_5, d_7 and d_{11} be as in (4.1). For $a, b \in K$ with $d_1d_5d_7d_{11} \neq 0$ and $(a^2+3a+9)(b^2+3b+9) \neq 0$, assume that $f_a(X)$ and $f_b(X)$ are irreducible over K. Then the splitting fields of $f_a(X)$ and of $f_b(X)$ over K coincide if and only if the decomposition types* $\mathrm{DT}(\mathcal{R}_i)$ *where $\mathcal{R}_i(X) = f_{A_i}(X)$ $(i=1,5,7,11)$ are given as in Table 4.1.*

K	$G_a = G_b$	$\mathrm{DT}(\mathcal{R}_1)$	$\mathrm{DT}(\mathcal{R}_5)$	$\mathrm{DT}(\mathcal{R}_7)$	$\mathrm{DT}(\mathcal{R}_{11})$
$\sqrt{3} \in K$	C_{12}	6^2	2^6	3^4	1^{12}
		2^6	6^2	1^{12}	3^4
		3^4	1^{12}	6^2	2^6
		1^{12}	3^4	2^6	6^2
$\sqrt{3} \notin K$	H_{24}	12	4^3	6^2	2^6
		4^3	12	2^6	6^2
		6^2	2^6	12	4^3
		2^6	6^2	4^3	12
		6^2	2^6	$3^2,\ 6$	$1^6,\ 2^3$
		2^6	6^2	$1^6,\ 2^3$	$3^2,\ 6$
		$3^2,\ 6$	$1^6,\ 2^3$	6^2	2^6
		$1^6,\ 2^3$	$3^2,\ 6$	2^6	6^2
	$C_6 \times C_2$	$3^2,\ 6$	$1^6,\ 2^3$	$3^2,\ 6$	$1^6,\ 2^3$
		$1^6,\ 2^3$	$3^2,\ 6$	$1^6,\ 2^3$	$3^2,\ 6$

TABLE 4.1.

Lemma 4.6. *Let d_1, d_5, d_7 and d_{11} be as in* (4.1) *and* $\xi(u) = u(u+1)\cdot(u-1)(u+2)(2u+1)(u^2-2u-2)(u^2+4u+1)(2u^2+2u-1)$ *for* $u \in K$. *Assume that* $d_1d_5d_7d_{11} \neq 0$ *and* $(a^2+3a+9)(b^2+3b+9) \neq 0$ *for* $a, b \in K$.

(1) *The polynomial* $f_{A_1}(X)$ (*resp.* $f_{A_{11}}(X)$) *has a linear factor over* K *if and only if there exists* $u \in K$ *such that*

$$B = A(u) \tag{4.2}$$

where $B = b$ (*resp.* $B = -b-3$) *and*

$$A(X) = \frac{9\,\xi(X) + f_{-3}(X)}{-a\,\xi(X) + f_0(X)} = a + \frac{(a^2+3a+9)\,\xi(X)}{f_a(X)}.$$

(2) *The polynomial* $f_{A_7}(X)$ (*resp.* $f_{A_5}(X)$) *has a linear factor over* K *if and only if there exists* $u' \in K$ *such that*

$$B = A(u') \tag{4.3}$$

where $B = b$ (*resp.* $B = -b-3$) *and*

$$\begin{aligned} A(X) &= \frac{(270a^3-729)\xi(X) + (a^5-270a^2)f_0(X) + (15a^4-405a)f_{-3}(X)}{g_a(X)} \\ &= -\frac{a(a^4+15a^3-270a-405)}{5a^4+30a^3-135a-81} + \frac{(a^2+3a+9)^5\,\xi(X)}{(5a^4+30a^3-135a-81)g_a(X)} \end{aligned}$$

with

$$g_a(X) = a^2(a^3-270)\,\xi(X) - a(5a^3-135)f_0(X) - (30a^3-81)f_{-3}(X).$$

(3) *Assume that* $f_a(X)$ *is irreducible and* $\mathrm{Gal}_{\mathbb{Q}} f_a(X) = C_6 \times C_2$. *For* $B = b$, *there exists* $u \in K$ *which satisfies* (4.2) *if and only if there exists* $u' \in K$ *which satisfies* (4.3).

Proof. Note that A_i is a linear fractional function in b over $K(a)$ for $i = 1, 5, 7, 11$. The assertions (1) and (2) are just obtained by solving the equation $f_{A_i}(X) = 0$ in b. The assertion (3) follows from Theorem 4.5 (see also Table 4.1). □

Lemma 4.7. *Let d_1, d_5, d_7 and d_{11} be as in* (4.1). *For* $a, b \in K$, *if* $d_1d_5d_7d_{11} = 0$, *that is* $b = a$, $b = -a-3$,

$$\begin{aligned} b &= -\frac{a(a^4+15a^3-270a-405)}{5a^4+30a^3-135a-81} \\ \text{or} \qquad b &= \frac{(a+3)(a^4-3a^3-81a^2-27a+81)}{5a^4+30a^3-135a-81}, \end{aligned}$$

then $\mathrm{Spl}_K f_a(X) = \mathrm{Spl}_K f_b(X)$.

Proof. For $i = 1, 5, 7, 11$, we consider the resolvent $d_i\mathcal{R}_i(X)$ instead of $\mathcal{R}_i(X)$. If $d_i = 0$, then the decomposition type $\mathrm{DT}(d_i\mathcal{R}_i)$ is given as $1^5, 2^3$ (resp. 1^{11}) if $\sqrt{3} \notin K$ (resp. $\sqrt{3} \in K$). By Theorem 3.1 (Corollary 3.2), we have $\mathrm{Spl}_K f_a(X) = \mathrm{Spl}_K f_b(X)$ (see also Table 4.1). Note that the vanishing simple root corresponds to the point at infinity, i.e. $X = x/y$ with $y = 0$ (see also [20, p. 47]). □

By Theorem 4.5 and Lemma 4.6, for a fixed $a \in K$ with $a^2 + 3a + 9 \neq 0$, we have $\mathrm{Spl}_K f_b(X) = \mathrm{Spl}_K f_a(X)$ where b is given as in Lemma 4.6(1) for arbitrary $u \in K$ with $f_a(u) \neq 0$ and $b^2 + 3b + 9 \neq 0$.

Corollary 4.8. *Let K be an infinite field with* $\mathrm{char}\, K \neq 2, 3$. *For a fixed $a \in K$ with $a^2 + 3a + 9 \neq 0$, there exist infinitely many $b \in K$ such that $\mathrm{Spl}_K f_b(X) = \mathrm{Spl}_K f_a(X)$.*

On the other hand, by Siegel's theorem for curves of genus 0 (cf. [23, Theorem 6.1], [24, Chapter 8, Section 5]), we have the following:

Corollary 4.9. *Let K be a number field and $\mathcal{O}_K$ be the ring of integers in K. Assume that $a \in \mathcal{O}_K$ with $a^2 + 3a + 9 \neq 0$. Then there exist only finitely many integers $b \in \mathcal{O}_K$ such that* $\mathrm{Spl}_K f_b(X) = \mathrm{Spl}_K f_a(X)$. *In particular, there exist only finitely many integers $b \in \mathcal{O}_K$ such that $f_{A_i}(X)$ $(i = 1, 5, 7, 11)$ has a linear factor over K.*

5. The case $K = \mathbb{Q}$

For $m \in \mathbb{Z}$, we consider the polynomial $f_m(X) = F_m(X, 1)$ of degree 12 over $\mathbb{Q}$. Define

$$\begin{aligned} L_m &= \mathrm{Spl}_{\mathbb{Q}} f_m(X), & L_m^{(6)} &= \mathrm{Spl}_{\mathbb{Q}} f_m^{(6)}(X), & L_m^{(3)} &= \mathrm{Spl}_{\mathbb{Q}} f_m^{(3)}(X), \\ G_m &= \mathrm{Gal}_{\mathbb{Q}} f_m(X), & G_m^{(6)} &= \mathrm{Gal}_{\mathbb{Q}} f_m^{(6)}(X), & G_m^{(3)} &= \mathrm{Gal}_{\mathbb{Q}} f_m^{(3)}(X). \end{aligned}$$

We intend to generalize the following two theorems for the simplest cubic fields $L_m^{(3)}$ and the simplest sextic fields $L_m^{(6)}$ to the case of L_m.

Theorem 5.1 (Gras [10], [11]).

(1) *For $m \in \mathbb{Z}$, $f_m^{(3)}(X)$ is irreducible over $\mathbb{Q}$ and $G_m^{(3)} = C_3$.*

(2) *For $m \in \mathbb{Z} \setminus \{-8, -3, 0, 5\}$, $f_m^{(6)}(X)$ is irreducible over $\mathbb{Q}$. In particular, we have*

$$G_m^{(6)} = \begin{cases} C_6 & \text{if} \quad m \in \mathbb{Z} \setminus \{-8, -3, 0, 5\}, \\ C_3 & \text{if} \quad m \in \{-8, -3, 0, 5\}. \end{cases}$$

Moreover, for $m \in \mathbb{Z}$ the unique cubic subfield of $L_m^{(6)}$ is the simplest cubic field $L_m^{(3)}$ and the field $\mathbb{Q}(\sqrt{m^2 + 3m + 9})$ is a subfield of $L_m^{(6)}$.

Theorem 5.2 (Okazaki, Hoshi [15], [16]).

(1) *For* $m, n \in \mathbb{Z}$ *with* $-1 \le m < n$, *if* $L_m^{(3)} = L_n^{(3)}$, *then* $m, n \in \{-1, 0, 1, 2, 3, 5, 12, 54, 66, 1259, 2389\}$. *In particular, we have*

$$L_{-1}^{(3)} = L_5^{(3)} = L_{12}^{(3)} = L_{1259}^{(3)},\ L_0^{(3)} = L_3^{(3)} = L_{54}^{(3)},\ L_1^{(3)} = L_{66}^{(3)},\ L_2^{(3)} = L_{2389}^{(3)}.$$

(2) *For* $m, n \in \mathbb{Z}$, $L_m^{(6)} = L_n^{(6)}$ *if and only if* $m = n$ *or* $m = -n - 3$.

Theorem 5.3. *For* $m \in \mathbb{Z} \setminus \{-8, -3, 0, 5\}$, $f_m(X)$ *is irreducible over* $\mathbb{Q}$. *In particular,*

$$G_m = \begin{cases} H_{24} & \text{if} \quad m \in \mathbb{Z} \setminus \{-8,-3,0,5\} \text{ and } \sqrt{3(m^2+3m+9)} \notin \mathbb{Z}, \\ C_6 \times C_2 & \text{if} \quad m \in \mathbb{Z} \setminus \{-8,-3,0,5\} \text{ and } \sqrt{3(m^2+3m+9)} \in \mathbb{Z}, \\ C_6 \times C_2 & \text{if} \quad m \in \{-8, 5\}, \\ C_6 & \text{if} \quad m \in \{-3, 0\}. \end{cases}$$

Moreover, for $m \in \mathbb{Z}$ *the unique cubic subfield of* L_m *is the simplest cubic field* $L_m^{(3)}$ *and the fields* $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{m^2+3m+9})$, $\mathbb{Q}\left(\sqrt{3(m^2+3m+9)}\right)$ *and* $L_m^{(6)}$ *are subfields of* L_m.

Proof. From (2.4), (2.5) and Theorem 5.1(1), we have $\mathbb{Q} \subsetneq L_m^{(3)} \subset L_m^{(6)} \subset L_m$ and $G_m \not\le D_4$. By (2.3), if $\sqrt{m^2+3m+9} \notin \mathbb{Z}$ and $\sqrt{3(m^2+3m+9)} \notin \mathbb{Z}$, then $f_m(X)$ is irreducible over $\mathbb{Q}$ and $G_m = H_{24}$.

Now we assume that $\sqrt{m^2+3m+9} \in \mathbb{Z}$. An easy calculation shows that $\sqrt{m^2+3m+9} \in \mathbb{Z}$ if and only if $m \in \{-8,-3,0,5\}$ for $m \in \mathbb{Z}$. For $m \in \{-8,-3,0,5\}$, by (2.6), the polynomial $f_m(X)$ splits into irreducible factors over $\mathbb{Q}$ as

$$f_{-8}(X) = f_{-15}^{(6)}(X) f_{-1}^{(6)}(X), \qquad f_{-3}(X) = f_{-3}^{(3)}(X) f_3^{(3)}(X) f_{-6}^{(6)}(X),$$
$$f_0(X) = f_{-6}^{(3)}(X) f_{-3}^{(3)}(X) f_3^{(6)}(X), \qquad f_5(X) = f_{-2}^{(6)}(X) f_{12}^{(6)}(X).$$

Hence it follows from Theorem 5.1(2) and Theorem 5.2 that $G_m = C_6 \times C_2$ (resp. C_6) for $m \in \{-8, 5\}$ (resp. $m \in \{-3, 0\}$).

Assume that $\sqrt{3(m^2+3m+9)} \in \mathbb{Z}$. Then $m \notin \{-8,-3,0,5\}$. From (2.3) we have $G_m \le C_6 \times C_2$. We consider $f_m(X)$ over $\mathbb{Q}(\sqrt{m^2+3m+9}) = \mathbb{Q}(\sqrt{3})$. From Theorem 5.1(2), (2.5) and (2.6), we have that $f_m(X)$ splits into two factors as $f_{m+\sqrt{m^2+3m+9}}^{(6)}(X) f_{m-\sqrt{m^2+3m+9}}^{(6)}(X)$ over $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{3}) \subsetneq L_m^{(6)} \subset L_m$ and $C_3 \le \mathrm{Gal}_{\mathbb{Q}(\sqrt{3})} f_m(X) \le C_6$. Hence $\mathrm{DT}(f_m)$ over $\mathbb{Q}(\sqrt{3})$ is $6, 6$ or $3, 3, 3, 3$. It is enough to show that $f_{m \pm \sqrt{m^2+3m+9}}^{(6)}(X) \notin \mathbb{Q}[X]$ are irreducible over $\mathbb{Q}(\sqrt{3})$. From (2.6), $f_{m_1}^{(6)}(X)$ splits into two cubic factors over $\mathbb{Q}(\sqrt{3})$ if and only if $m_1^2 + 3m_1 + 9$ is square in $\mathbb{Q}(\sqrt{3})$. However, for $m_1 = m \pm \sqrt{m^2+3m+9}$, $m_1^2 + 3m_1 + 9 = 2m^2 + 6m + 18 \pm (2m+3) \cdot$

$\sqrt{m^2+3m+9}$ is not square in $\mathbb{Q}(\sqrt{3})$ because $m^2+3m+9=3c^2$ for some odd integer $c \in \mathbb{Z}$ and the coefficient $(2m+3)c$ of $\sqrt{3}$ in $m_1^2+3m_1+9 \in \mathbb{Z}[\sqrt{3}]$ is odd. Thus we see that $f^{(6)}_{m\pm\sqrt{m^2+3m+9}}(X)$ is irreducible over $\mathbb{Q}(\sqrt{3})$ and $f_m(X)$ is irreducible over $\mathbb{Q}$. $\square$

Lemma 5.4. *There exist infinitely many integers m such that*

$$\sqrt{3(m^2+3m+9)} \in \mathbb{Z}.$$

Indeed, such integers $m \geq -1$ are given by

$$m = \frac{3}{2}\left(\frac{\sqrt{3}}{2}(\varepsilon^{2r-1}-\varepsilon^{-(2r-1)})-1\right) = \frac{3(3b_{2r-1}-1)}{2} \quad (r \in \mathbb{Z}, r \geq 1)$$

where $\varepsilon = \sqrt{3}+2$ is a fundamental unit of $\mathbb{Z}[\sqrt{3}]$ and $\varepsilon^{2r-1} = a_{2r-1} + b_{2r-1}\sqrt{3}$ with $a_{2r-1}, b_{2r-1} \in \mathbb{Z}$.

Proof. Assume that for $m \geq -1$, there exists $c \in \mathbb{Z}_{>0}$ such that $m^2 + 3m+9 = 3c^2$. Define $m_0 := m/3 \in \mathbb{Z}$ and $c_0 := c/3 \in \mathbb{Z}$. Then it follows that $(2m_0+1)^2+3 = 12c_0^2$. Define $l = (2m_0+1)/3 \in \mathbb{Z}$. Then we have $(\sqrt{3}l+2c_0)(\sqrt{3}l-2c_0) = -1$. Hence there exists $j \geq 1$ such that $\sqrt{3}l+2c_0 = \varepsilon^j$. We also have $3l+2\sqrt{3}c_0 = \sqrt{3}\varepsilon^j$ and $3l-2\sqrt{3}c_0 = (-\sqrt{3})\varepsilon^{-j}$. By adding the both sides, we get $m = \frac{3}{2}(\frac{\sqrt{3}}{2}(\varepsilon^j-\varepsilon^{-j})-1) = \frac{3}{2}(3b_j-1)$. It is easy to see that $m \in \mathbb{Z}$ if and only if $j = 2r-1$. $\square$

Examples of the integers m and r with $\sqrt{3(m^2+3m+9)} \in \mathbb{Z}$, i.e. $G_m = C_6 \times C_2$, are given as follows:

r	1	2	3	4	5	6	7	8	9
m	3	66	939	13098	182451	2541234	35394843	492986586	6866417379

By Theorem 5.2 and Theorem 5.3, we get:

Theorem 5.5. *For $m, n \in \mathbb{Z}$, $L_m = L_n$ if and only if $m = n$ or $m = -n-3$.*

Proof. We may assume that $-1 \leq m < n$ without loss of generality. When $(m,n) = (0,5)$, i.e. $G_m = G_n = C_6$, we have $L_0 \neq L_5$. When $m \in \mathbb{Z}\setminus\{0,5\}$, i.e. $G_m = H_{24}$ or $C_6 \times C_2$, by Theorem 5.3 the unique cubic subfield of L_m is $L_m^{(3)}$. It follows from Theorem 5.2 that $L_m \neq L_n$ except for $m, n \in \{-1, 1, 2, 3, 12, 54, 66, 1259, 2389\}$. For the exceptional cases, we may confirm that $L_m \neq L_n$ by Theorem 4.5. $\square$

Theorem 5.6. *If there exists a non-trivial solution $(x,y) \in \mathbb{Z}^2$ to $F_m(x,y) = \lambda$, i.e. $xy(x+y)(x-y)(x+2y)(2x+y) \neq 0$, where λ is a divisor of $729(m^2+3m+9)$, then there exists $n \in \mathbb{Z} \setminus \{m, -m-3\}$ such that $L_n = L_m$.*

Proof. Assume that there exists a non-trivial solution (x,y) to $F_m(x,y)=\lambda$ where λ is a divisor of $729(m^2+3m+9)$. From Theorem 4.5 and Lemma 4.6 with $u=x/y$, we have that

$$n=m+\frac{(m^2+3m+9)\Xi(x,y)}{F_m(x,y)}\in\mathbb{Q}\setminus\{m\}$$

implies $L_n=L_m$ where

$$\begin{aligned}\Xi(x,y)&=xy(x+y)(x-y)(x+2y)(2x+y)\\&\qquad\cdot(x^2-2xy-2y^2)(x^2+4xy+y^2)(2x^2+2xy-y^2).\end{aligned}$$

When $m\in\mathbb{Z}\setminus\{-8,-3,0,5\}$ ($G_m=H_{24}$ or $C_6\times C_2$), it follows from Theorem 4.5 and Lemma 4.6 that $n\neq -m-3$ (see Table 4.1). When $m\in\{-8,-3,0,5\}$ ($G_m=C_6\times C_2$ or C_6), we may check that $\mathrm{DT}(\mathcal{R}_{11})$ is $3^2,6$ for $m=n$. Hence $n\in\mathbb{Q}\setminus\{m,-m-3\}$. If $x\not\equiv y \pmod 3$, then $F_m(x,y)\equiv 1 \pmod 3$. Hence $F_m(x,y)=\lambda$ is a divisor of m^2+3m+9 and $n\in\mathbb{Z}\setminus\{m,-m-3\}$. If $x\equiv y \pmod 3$, then 729 is a divisor of $\Xi(x,y)$, and hence $n\in\mathbb{Z}\setminus\{m,-m-3\}$. ☐

Proof of Theorem 1.1. By combining Theorem 5.5 and Theorem 5.6, we obtain Theorem 1.1. ☐

Acknowledgment. *The author is grateful to the referee for careful reading and suggesting many improvements.*

References

[1] C. Adelmann, *The decomposition of primes in torsion point fields*, Lecture Notes in Mathematics, vol. 1761, Springer, 2001, vi+142 pages.

[2] H. Ahmad, M. Hajja & M.-c. Kang, “Negligibility of projective linear automorphisms”, *J. Algebra* **199** (1998), no. 1, p. 344-366.

[3] A. Baker, “Contributions to the theory of Diophantine equations. I. On the representation of integers by binary forms”, *Philos. Trans. R. Soc. Lond.* **263** (1968), p. 173-191.

[4] M. A. Bennett & S. R. Dahmen, “Klein forms and the generalized superelliptic equation”, *Ann. Math.* **177** (2013), no. 1, p. 171-239.

[5] Y. Bilu & G. Hanrot, “Solving Thue equations of high degree”, *J. Number Theory* **60** (1996), no. 2, p. 373-392.

[6] J. Chen & P. Voutier, “Complete solution of the Diophantine equation $X^2+1=dY^4$ and a related family of quartic Thue equations”, *J. Number Theory* **62** (1997), no. 1, p. 71-99.

[7] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer, 1993, xxi+534 pages.

[8] ———, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, vol. 193, Springer, 2000, xv+578 pages.

[9] I. Gaál, *Diophantine equations and power integral bases. New computational methods*, Birkhäuser, 2002, xviii+184 pages.

[10] M.-N. Gras, “Familles d’unités dans les extensions cycliques réelles de degré 6 de Q”, *Publ. Math. Fac. Sci. Besançon, Théor. Nombres* **1984/85–1985/86** (1986), Exp. no. 2, 27 p.

[11] ———, “Special units in real cyclic sextic fields”, *Math. Comput.* **48** (1987), p. 179-182.

[12] C. Heuberger, “Parametrized Thue Equations : A Survey”, *RIMS Kokyuroku* **1511** (2006), p. 82-91.

[13] C. Heuberger, A. Pethő & R. F. Tichy, "Complete solution of parametrized Thue equations", *Acta Math. Inform. Univ. Ostrav.* **6** (1998), no. 1, p. 93-113.

[14] C. Heuberger, A. Togbé & V. Ziegler, "Automatic solution of families of Thue equations and an example of degree 8", *J. Symb. Comput.* **38** (2004), no. 3, p. 1145-1163.

[15] A. Hoshi, "On correspondence between solutions of a family of cubic Thue equations and isomorphism classes of the simplest cubic fields", *J. Number Theory* **131** (2011), no. 11, p. 2135-2150.

[16] ———, "On the simplest sextic fields and related Thue equations", *Funct. Approximatio, Comment. Math.* **47** (2012), no. 1, p. 35-49.

[17] ———, "On the simplest quartic fields and related Thue equations", in *Computer mathematics. 9th Asian symposium, ASCM 2009, Fukuoka, Japan, December 14–17, 2009, 10th Asian symposium, ASCM 2012, Beijing, China, October 26–28, 2012*, Springer, 2014, p. 67-85.

[18] A. Hoshi & K. Miyake, "A geometric framework for the subfield problem of generic polynomials via Tschirnhausen transformation", in *Number theory and applications. Proceedings of the international conferences on number theory and cryptography, Allahabad, India, December 2006 and February 2007*, Hindustan Book Agency, 2009, p. 65-104.

[19] ———, "On the field intersection problem of quartic generic polynomials via formal Tschirnhausen transformation", *Comment. Math. Univ. St. Pauli* **58** (2009), no. 1, p. 51-89.

[20] ———, "A note on the field isomorphism problem of $X^3 + sX + s$ and related cubic Thue equations", *Interdiscip. Inf. Sci.* **16** (2010), no. 1, p. 45-54.

[21] ———, "On the field intersection problem of solvable quintic generic polynomials", *Int. J. Number Theory* **6** (2010), no. 5, p. 1047-1081.

[22] ———, "Some Diophantine problems arising from the isomorphism problem of generic polynomials", in *Number theory. Dreaming in dreams. Proceedings of the 5th China-Japan seminar, Higashi-Osaka, Japan, August 27–31, 2008*, Series on Number Theory and Its Applications, vol. 6, World Scientific, 2010, p. 87-105.

[23] S. Lang, *Elliptic curves: Diophantine analysis*, Grundlehren der Mathematischen Wissenschaften, vol. 231, Springer, 1978, xi+261 pages.

[24] ———, *Fundamentals of Diophantine geometry*, Springer, 1983, xviii+370 pages.

[25] M. Laurent, M. Mignotte & Y. Nesterenko, "Formes linéaires en deux logarithmes et déterminants d'interpolation", *J. Number Theory* **55** (1995), no. 2, p. 285-321.

[26] G. Lettl & A. Pethő, "Complete solution of a family of quartic Thue equations", *Abh. Math. Semin. Univ. Hamb.* **65** (1995), p. 365-383.

[27] G. Lettl, A. Pethő & P. Voutier, "Simple families of Thue inequalities", *Trans. Amer. Math. Soc.* **351** (1999), no. 5, p. 1871-1894.

[28] M. Mignotte, "Verification of a conjecture of E. Thomas", *J. Number Theory* **44** (1993), no. 2, p. 172-177.

[29] R. Okazaki, "Geometry of a cubic Thue equation", *Publ. Math.* **61** (2002), no. 3-4, p. 267-314.

[30] D. Shanks, "The simplest cubic fields", *Math. Comput.* **28** (1974), p. 1137-1152.

[31] Y.-Y. Shen, "Unit groups and class numbers of real cyclic octic fields", *Trans. Amer. Math. Soc.* **326** (1991), no. 1, p. 179-209.

[32] Y.-Y. Shen & L. C. Washington, "A family of real 2^n-tic fields", *Trans. Amer. Math. Soc.* **345** (1994), no. 1, p. 413-434.

[33] ———, "A family of real p^n-tic fields", *Can. J. Math.* **47** (1995), no. 3, p. 655-672.

[34] The GAP Group, "GAP — Groups, Algorithms, and Programming, Version 4.4.12", 2008, `http://www.gap-system.org`.

[35] E. Thomas, "Complete solutions to a family of cubic Diophantine equations", *J. Number Theory* **34** (1990), no. 2, p. 235-250.

[36] A. Thue, "Über Annäherungswerte algebraischer Zahlen", *J. Reine Angew. Math.* **135** (1909), p. 284-305.

[37] N. Tzanakis & B. M. de Weger, "On the practical solution of the Thue equation", *J. Number Theory* **31** (1989), no. 2, p. 99-132.

[38] I. WAKABAYASHI, "Number of solutions for cubic Thue equations with automorphisms", *Ramanujan J.* **14** (2007), no. 1, p. 131-154.

Akinari HOSHI
Department of Mathematics
Niigata University
8050 Ikarashi 2-no-cho, Nishi-ku,
Niigata 950-2181, Japan
E-mail: hoshi@math.sc.niigata-u.ac.jp
URL: http://mathweb.sc.niigata-u.ac.jp/~hoshi/