On a Galois group arising from an iterated map

By Masamitsu SHIMAKURA

Takushoku University Daiichi High School, 4-64-5 Ominami, Musashimurayama, Tokyo 208-0013, Japan

(Communicated by Kenji FUKAYA, M.J.A., April 12, 2018)

Abstract: We study the irreducibility and the Galois group of the polynomial $f(a,x) = x^8 + 3ax^6 + 3a^2x^4 + (a^2+1)ax^2 + a^2 + 1$ over $\mathbf{Q}(a)$ and $\mathbf{Q}$. This polynomial is a factor of the 4-th dynatomic polynomial for the map $\sigma(x) = x^3 + ax$.

Key words: Dynatomic polynomial; Galois group.

1. Introduction. The aim of this paper is to study the Galois group of a certain factor of a 4-th dynatomic polynomial. In general, the 4-th dynatomic polynomial for the polynomial map σ is defined by

$$\Phi_{4,\sigma}(x) = \frac{\sigma^4(x) - x}{\sigma^2(x) - x},$$

where σ^i is the i-fold iteration of σ with itself (see [9] for details).

Dynatomic polynomials have been intensively studied by Morton. For example, he computed the Galois group of $\Phi_{3,\sigma}(x)$ with $\sigma(x) = x^2 + a$ [5], and in particular, he was led to an analogue of Kummer theory for cyclic cubic extensions by using the map $\sigma(x) = x^2 - \frac{1}{4}(s^2+7)$ over the base field without cube roots of unity [6]. He also proved that the dynatomic curve $\Phi_{4,\sigma}(x) = 0$ with $\sigma(x) = x^2 + a$ has no rational points, i.e., $\Phi_{4,\sigma}(x)$ has no rational roots for rational values of a [7].

In this paper, we consider the 4-th dynatomic polynomial $\Phi_{4,\sigma}$ with $\sigma(x) = x^3 + ax$. The polynomial $\Phi_{4,\sigma}(x)$ has degree 72 and it has a factor:

$$f(a,x) = x^8 + 3ax^6 + 3a^2x^4 + (a^2+1)ax^2 + a^2 + 1. \tag{1.1}$$

We shall investigate the Galois groups of the polynomial $f(a,x)$ over $\mathbf{Q}(a)$ and its specializations over $\mathbf{Q}$.

In general, the Galois group of a dynatomic polynomial is isomorphic to a subgroup of a wreath product [8]. We show that the polynomial $f(a,x)$ has a Galois group which is isomorphic to the whole wreath product $C_4 \wr C_2$ over the function field $\mathbf{Q}(a)$ (see Theorem 2.1).

The group $C_4 \wr C_2$ has order 32 and has the following presentation:

$$\langle \sigma_1, \sigma_2, \tau \mid \sigma_1^4 = \sigma_2^4 = \tau^2 = 1, \sigma_1\sigma_2 = \sigma_2\sigma_1, \tau\sigma_1\tau = \sigma_2 \rangle.$$

Every Galois extension $L/\mathbf{Q}$ with this Galois group can be obtained as a class field of a certain quadratic field. By choosing the signature of L carefully, we can find such an extension that is a class field of a *real* quadratic field and that has an *odd* Artin representations of degree 2 induced from a character corresponding to the real quadratic field. This group $C_4 \wr C_2$ is known to be a minimal group with this property (see [4]). This is a strong motivation to construct Galois extensions with this Galois group systematically.

The outline of this paper is as follows: In Section 2, we show that the splitting field of the polynomial $f(a,x)$ is a $C_4 \wr C_2$-extension over the function field $\mathbf{Q}(a)$. In the rest of this paper, we are concerned with the Galois groups of the specializations $f(a,x)$ with various $a \in \mathbf{Q}$. In Section 3, we determine a condition for the irreducibility of $f(a,x)$ for specific values of a in $\mathbf{Q}$. For $a \in \mathbf{Q}$, let Σ_f^a be the splitting field of $f(a,x)$ over $\mathbf{Q}$. In Section 4, we give a condition for the Galois group $\mathrm{Gal}(\Sigma_f^a/\mathbf{Q})$ to be isomorphic to $C_4 \wr C_2$, and compute the signature of Σ_f^a. In Section 5, we classify the Galois group $\mathrm{Gal}(\Sigma_f^a/\mathbf{Q})$ when it is smaller than $C_4 \wr C_2$.

2. The Galois group over a function field. In this section, we prove the following main theorem.

Theorem 2.1. *The Galois group of $f(a,x)$ over $\mathbf{Q}(a)$ is isomorphic to $C_4 \wr C_2$.*

Proof. By a straightforward computation, we can check $f(a,x) | f(a,\sigma(x))$. Hence if α is a root of $f(a,x)$, then so is $\sigma(\alpha)$.

2010 Mathematics Subject Classification. Primary 11R32; Secondary 12F10, 12F20.

doi: 10.3792/pjaa.94.43

The roots of $f(a,x)$ fall into two distinct orbits under σ. To be more specific, if we define

$$\alpha_1 = \frac{1}{2}\sqrt{-3a - \sqrt{a^2-8} + \sqrt{8+2a^2-2a\sqrt{a^2-8}}},$$

$$\alpha_2 = \frac{1}{2}\sqrt{-3a + \sqrt{a^2-8} + \sqrt{8+2a^2+2a\sqrt{a^2-8}}},$$

then the two orbits are $\{\sigma^j(\alpha_1)\}$ and $\{\sigma^j(\alpha_2)\}$ for $0 \le j \le 3$. If we set $\lambda_i(x) = \prod_{j=0}^{3}(x - \sigma^j(\alpha_i))$ for $i = 1, 2$, then $\lambda_i(x)$ are polynomials in $\mathbf{Q}(\sqrt{a^2-8})[x]$ of degree 4. Let L_i be the splitting field of $\lambda_i(x)$ over $\mathbf{Q}(\sqrt{a^2-8})$. Since σ has order 4, the extensions $L_i/\mathbf{Q}(\sqrt{a^2-8})$ are cyclic of degree 4. Let K_i be the intermediate field of $L_i/\mathbf{Q}(\sqrt{a^2-8})$ such that $[K_i : \mathbf{Q}(\sqrt{a^2-8})] = 2$. The fields K_1 and K_2 are explicitly given by

$$K_1 = \mathbf{Q}(\alpha_1^2) = \mathbf{Q}\left(\sqrt{8+2a^2-2a\sqrt{a^2-8}}\right), \tag{2.1}$$

$$K_2 = \mathbf{Q}(\alpha_2^2) = \mathbf{Q}\left(\sqrt{8+2a^2+2a\sqrt{a^2-8}}\right). \tag{2.2}$$

Since

$$\sqrt{8+2a^2-2a\sqrt{a^2-8}}\sqrt{8+2a^2+2a\sqrt{a^2-8}} = 8\sqrt{a^2+1} \notin \mathbf{Q}(\sqrt{a^2-8}),$$

we have $K_1 \neq K_2$. Let Σ_f be the splitting field of $f(a,x)$ over $\mathbf{Q}(\sqrt{a^2-8})$. Since the field Σ_f is the compositum of L_1 and L_2, the Galois group G' of $\Sigma_f/\mathbf{Q}(\sqrt{a^2-8})$ is isomorphic to $C_4 \times C_4$.

The group G' is generated by the following automorphisms:

$$\sigma_1 : \begin{cases} \sigma^j(\alpha_1) \longmapsto \sigma^{j+1}(\alpha_1) \\ \sigma^j(\alpha_2) \longmapsto \sigma^j(\alpha_2) \end{cases} (j = 0, \ldots, 3), \tag{2.3}$$

$$\sigma_2 : \begin{cases} \sigma^j(\alpha_1) \longmapsto \sigma^j(\alpha_1) \\ \sigma^j(\alpha_2) \longmapsto \sigma^{j+1}(\alpha_2) \end{cases} (j = 0, \ldots, 3). \tag{2.4}$$

If we set

$$\tau : \begin{cases} \sigma^j(\alpha_1) \longmapsto \sigma^j(\alpha_2) \\ \sigma^j(\alpha_2) \longmapsto \sigma^j(\alpha_1) \end{cases} (j = 0, \ldots, 3), \tag{2.5}$$

then this map τ is an extension of the generator of $\mathrm{Gal}(\mathbf{Q}(\sqrt{a^2-8})/\mathbf{Q}(a))$ to $\mathrm{Gal}(\Sigma_f/\mathbf{Q}(a))$.

If we set $G_0 = \langle \sigma_1, \sigma_2, \tau \rangle$, then the generators of G_0 satisfy $\sigma_1^4 = \sigma_2^4 = \tau^2 = 1$, $\sigma_1\sigma_2 = \sigma_2\sigma_1$ and $\tau\sigma_1\tau = \sigma_2$. Thus G_0 is isomorphic to $C_4 \wr C_2$. Since the field Σ_f is an extension over $\mathbf{Q}(a)$ of degree 32, the group $\mathrm{Gal}(\Sigma_f/\mathbf{Q}(a))$ is isomorphic to $C_4 \wr C_2$. □

Next, we describe some intermediate fields of $\Sigma_f/\mathbf{Q}(a)$ for our later use. The subgroups of index 2 in $C_4 \wr C_2 = \langle \sigma_1, \sigma_2, \tau \rangle$ are

$$\langle \sigma_1^2, \sigma_1\tau \rangle, \quad \langle \sigma_1, \sigma_2 \rangle, \quad \langle \sigma_1^2, \sigma_1\sigma_2, \tau \rangle.$$

The quadratic fields over $\mathbf{Q}(a)$ corresponding to these subgroups are

$$k_0 = \Sigma_f^{\langle \sigma_1^2, \sigma_1\tau \rangle}, \tag{2.6}$$

$$k_1 = \Sigma_f^{\langle \sigma_1, \sigma_2 \rangle} = \mathbf{Q}(\sqrt{a^2-8}), \tag{2.7}$$

$$k_2 = \Sigma_f^{\langle \sigma_1^2, \sigma_1\sigma_2, \tau \rangle} = \mathbf{Q}(v) \tag{2.8}$$

with $v = \sqrt{a^2+1}$.

Proposition 2.2. *The quadratic extensions of k_2 inside Σ_f are given by the following*

$$M_1 = \mathbf{Q}(\sqrt{(v-1)(v-3)}),$$
$$M_2 = \mathbf{Q}(\sqrt{(v+1)(v+3)}),$$
$$M_3 = \mathbf{Q}(\sqrt{v(v-1)}),$$
$$M_4 = \mathbf{Q}(\sqrt{v(v-3)}),$$
$$M_5 = \mathbf{Q}(\sqrt{v(v+3)}),$$
$$M_6 = \mathbf{Q}(\sqrt{v(v-1)(v-3)(v+3)}).$$

The Galois groups of the extensions Σ_f/M_i ($i = 3, 4, 5, 6$) are

$$\mathrm{Gal}(\Sigma_f/M_3) = \langle \sigma_1^3\sigma_2, \sigma_1^3\sigma_2, \tau \rangle \cong D_4,$$
$$\mathrm{Gal}(\Sigma_f/M_4) = \langle \sigma_1\sigma_2, \tau \rangle \cong C_4 \times C_2,$$
$$\mathrm{Gal}(\Sigma_f/M_5) = \langle \sigma_1^2, \sigma_1\sigma_2 \rangle \cong C_4 \times C_2,$$
$$\mathrm{Gal}(\Sigma_f/M_6) = \langle \sigma_1^3\sigma_2, \sigma_2\tau \rangle \cong Q_8.$$

Proof. We can show our assertions by calculating the fixed subgroups in $\langle \sigma_1, \sigma_2, \tau \rangle$ corresponding to these fields. We omit the detail. □

3. Irreducibility under specializations. The Hilbert irreducibility theorem guarantees that there are infinitely many $a \in \mathbf{Q}$ such that $f(a,x)$ is irreducible and that the Galois group of $f(a,x)$ over $\mathbf{Q}$ is isomorphic to $C_4 \wr C_2$. In the next section, we shall give an explicit description of such rational a's. In this section, we give a criterion for the irreducibility of the specialization $f(a,x)$ with a in $\mathbf{Q}$. Recall that Σ_f^a is the splitting field of the specialization $f(a,x)$ with a in $\mathbf{Q}$.

Theorem 3.1. *The specialization of the polynomial $f(a,x)$ with $a \in \mathbf{Q}$ is irreducible if and only if a is* not *one of the following forms with a rational solution (A,B) of the Diophantine equation $A^2 - 2B^2 = 1$:*

(3.1) $$\frac{2A}{B};$$

(3.2) $$\pm\frac{2(A+B)(A+2B)}{B(2A+3B)}.$$

Proof. We recall that $f(a,x)|f(a,\sigma(x))$. Let α_1 and α_2 be the roots of $f(a,x)$ given in the proof of Theorem 2.1. By $\sigma^4(\alpha_i)=\alpha_i$ $(i=1,2)$, we have $\sigma^2(\alpha_i)=-\alpha_i$.

Now we consider the following six polynomials:

$$\begin{aligned}\lambda_i(x) &= (x-\alpha_i)(x-\sigma(\alpha_i))(x+\alpha_i)(x+\sigma(\alpha_i))\\ &\in k_1[x];\\ \mu_i(x) &= (x-\alpha_i)(x+\alpha_i)(x-\sigma(\alpha_j))(x+\sigma(\alpha_j))\\ &\in M_1[x];\\ \nu_i(x) &= (x-\alpha_i)(x+\alpha_i)(x-\alpha_j)(x+\alpha_j)\in M_2[x]\end{aligned}$$

with $1\le i,j\le 2$ and $i\ne j$.

We shall show that $f(a,x)$ is reducible if and only if one of the fields k_1, M_1 and M_2 coincides with $\mathbf{Q}$.

At first, if $k_1=\mathbf{Q}$, $M_1=\mathbf{Q}$ or $M_2=\mathbf{Q}$, then $f(a,x)$ is obviously reducible over $\mathbf{Q}$.

Conversely, we assume that $f(a,x)$ is reducible over $\mathbf{Q}$. Let β be a root of an irreducible factor of $f(a,x)$. Since $f(a,x)|f(a,\sigma(x))$, we see that $-\beta$ and $\pm\sigma(\beta)$ are also roots of $f(a,x)$. Similarly, if γ is a root of $f(a,x)$ which is different from $\pm\beta$ and $\pm\sigma(\beta)$, then so are $-\gamma,\pm\sigma(\gamma)$. Now we set $g(x)=(x-\beta)(x-\sigma(\beta))(x+\beta)(x+\sigma(\beta))$ and $h(x)=(x-\gamma)(x-\sigma(\gamma))(x+\gamma)(x+\sigma(\gamma))$, and we obviously have $f(a,x)=g(x)h(x)$. Hence the pair $(g(x),h(x))$ coincides with one of $(\lambda_1(x),\lambda_2(x))$, $(\mu_1(x),\mu_2(x))$ or $(\nu_1(x),\nu_2(x))$. Thus we get $k_1=\mathbf{Q}$, $M_1=\mathbf{Q}$ or $M_2=\mathbf{Q}$.

Next we consider the conditions for k_1, M_1 or M_2 to coincide with $\mathbf{Q}$.

We first consider the case $k_1=\mathbf{Q}$, equivalently $\sqrt{a^2-8}\in\mathbf{Q}$. We can show that this condition is equivalent to $a=2A/B$ with a rational solution (A,B) of the Diophantine equation $A^2-2B^2=1$.

Next, if $M_1=\mathbf{Q}$, then we get $v\in\mathbf{Q}$ because $M_1\supset k_2$. Noting that $v^2=a^2+1$, we can write a in the form $a=(n^2-1)/(2n)$ with $n\in\mathbf{Q}$. This equation yields $v=(n^2+1)/(2n)$. Therefore $M_1=\mathbf{Q}$ is equivalent to the condition that

$$(v-1)(v-3)=((n-1)/(2n))^2((n-3)^2-8)$$

is a square. If there exists q in $\mathbf{Q}^\times$ such that $(n-3)^2-8=q^2$, then we have

$$\left(\frac{n-3}{q}\right)^2-2\left(\frac{2}{q}\right)^2=1.$$

If we set $n-3=2A/B$ with (A,B) satisfying $A^2-2B^2=1$, then the element $(v-1)(v-3)$ is a square. Hence we can get the following equality:

$$a=\frac{2(A+B)(A+2B)}{B(2A+3B)}.$$

The converse is clear.

We can treat the case $M_2=\mathbf{Q}$ similarly. Indeed, if $n+3=2A/B$ where (A,B) satisfies $A^2-2B^2=1$, then the element $(v+1)(v+3)$ is a square. Thus, in this case, a has the form

$$a=\frac{2(A-B)(A-2B)}{B(2A-3B)}.$$

Replacing the sign of B implies (3.2). The converse is clear again. □

Remark 3.2. We can obtain infinitely many non-isomorphic fields if we specialize $a\in\mathbf{Q}$. To prove this, it is enough to show that there are infinitely many quadratic fields k_1 when a runs through the rational integers. This follows from the result of Estermann [3].

4. Non-degenerate case. In this section, we see exactly when the Galois group of a specialization $f(a,x)$ with $a\in\mathbf{Q}$ is isomorphic to $C_4\wr C_2$.

Theorem 4.1. *We assume that the specialization $f(a,x)$ with $a\in\mathbf{Q}$ is irreducible. The Galois group of $f(a,x)$ is isomorphic to $C_4\wr C_2$ if and only if $a\ne\dfrac{n^2-1}{2n}$ with a rational number n.*

Proof. Since $f(a,x)$ is irreducible, it follows from Theorem 2.1 that the extensions L_i/k_1 are cyclic extensions of degree 4 and we have $k_1\ne\mathbf{Q}$.

If $\mathrm{Gal}(\Sigma_f^a/\mathbf{Q})$ is isomorphic to $C_4\wr C_2$, then Σ_f^a/k_1 is an extension of degree 16, hence we get $K_1\ne K_2$. By (2.1) and (2.2), the fields are $K_1\ne K_2$ if and only if $\sqrt{a^2+1}\notin\mathbf{Q}$, equivalently a does not have the form $(n^2-1)/(2n)$ with $n\in\mathbf{Q}$.

Conversely, if $a\ne(n^2-1)/(2n)$ for any $n\in\mathbf{Q}$, then the extensions L_1/k_1 and L_2/k_1 are distinct cyclic extensions of degree 4 because $K_1\ne K_2$. Moreover $k_1/\mathbf{Q}$ is a quadratic extension because the polynomial $f(a,x)$ is irreducible; hence we get $[\Sigma_f^a:\mathbf{Q}]=32$. □

The complex conjugation lies in one of the conjugacy classes of order less than or equal to 2. The following conjugacy classes of G are of order less than or equal to 2:

$\mathrm{Cl}(1)$, $\mathrm{Cl}(\sigma_1^2\sigma_2^2)$ of length 1;

$\mathrm{Cl}(\sigma_1^2)$ of length 2;

$\mathrm{Cl}(\tau)$ of length 4.

The following theorem describes the signature of Σ_f^a whose Galois group is isomorphic to $C_4 \wr C_2$.

Proposition 4.2. *We assume that the specialization $f(a,x)$ with $a \in \mathbf{Q}$ has the Galois group isomorphic to $C_4 \wr C_2$.*

(i) *If $a < -2\sqrt{2}$, then Σ_f^a is a real field.*

(ii) *If $-2\sqrt{2} < a < 2\sqrt{2}$, then Σ_f^a is an imaginary field and the complex conjugation lies in $\mathrm{Cl}(\tau)$.*

(iii) *If $2\sqrt{2} < a$, then Σ_f^a is a CM-field (i.e., the complex conjugation lies in $\mathrm{Cl}(\sigma_1^2\sigma_2^2)$ contained in the center of the group).*

Proof. By the proof of Theorem 2.1, the group $C_4 \wr C_2$ is generated by σ_1, σ_2 and τ defined by (2.3), (2.4) and (2.5), respectively. Let α_1 and α_2 be the roots of $f(a,x)$ defined in the proof of Theorem 2.1. The quadratic fields contained in Σ_f^a are k_0, k_1 and k_2 (see (2.6), (2.7) and (2.8)). In particular, k_2 is a real quadratic field for any $a \in \mathbf{Q}$.

(i) If $a < -2\sqrt{2}$, then it is easy to see that the four elements α_1^2, α_2^2, $\sigma_1(\alpha_1)^2$ and $\sigma_2(\alpha_2)^2$ are positive. This gives the result.

(ii) If $-2\sqrt{2} < a < 2\sqrt{2}$, then k_1 and k_0 are imaginary quadratic fields. The field k_2 is contained in the totally imaginary quartic field $\mathbf{Q}(\sqrt{a^2-8}, \sqrt{a^2+1})$ and the fixed group of this quartic field is $\langle\sigma_1^2, \sigma_1\sigma_2\rangle$. On the other hand, the fixed subgroup of k_2 is $\langle\sigma_1^2, \sigma_1\sigma_2, \tau\rangle$. This implies that the complex conjugation lies in the conjugacy class of τ.

(iii) If $2\sqrt{2} < a$, then both α_1^2 and α_2^2 are negative. The field Σ_f^a contains subfields $N = \mathbf{Q}(\alpha_1\alpha_2)$, $N_1 = \mathbf{Q}(\alpha_1, \alpha_2^2)$ and $N_2 = \mathbf{Q}(\alpha_1^2, \alpha_2)$ of degree 16. Since both α_1^2 and α_2^2 are negative, the fields N_1 and N_2 are totally imaginary. Thus the field $\Sigma_f^a = \mathbf{Q}(\alpha_1, \alpha_2)$ is also totally imaginary. On the other hand, the field N is the composite field of all M_i's in Proposition 2.2. We can show that N is totally real by examining the generators. Since the fixed subgroup of N is $\langle\sigma_1^2\sigma_2^2\rangle$, the complex conjugation acts as $\sigma_1^2\sigma_2^2$.

□

Remark 4.3. By Proposition 4.2, if $-2\sqrt{2} < a < 2\sqrt{2}$, then $\mathrm{Gal}(\Sigma_f^a/\mathbf{Q})$ has an odd faithful irreducible 2-dimensional complex representation induced from a character corresponding to the real quadratic field k_1.

In the paper [4], they constructed $C_4 \wr C_2$-extensions with the complex conjugation lying in $\mathrm{Cl}(\sigma_1^2)$.

5. Degenerate cases. In this section, we classify the Galois groups $\mathrm{Gal}(\Sigma_f^a/\mathbf{Q})$ when it is smaller than $C_4 \wr C_2$ and the polynomial $f(a,x)$ is irreducible over $\mathbf{Q}$.

By Theorem 4.1, $\mathrm{Gal}(\Sigma_f^a/\mathbf{Q}) \not\cong C_4 \wr C_2$ if and only if $a = (n^2-1)/(2n)$ with $n \in \mathbf{Q}$. Then we have $v = (n^2+1)/(2n) \in \mathbf{Q}$ and this implies $k_2 = \mathbf{Q}$.

Since the Galois group of $f((n^2-1)/(2n), x)$ over the function field $\mathbf{Q}(n)$ is $\mathrm{Gal}(\Sigma_f/\mathbf{Q}(n)) = \mathrm{Gal}(\Sigma_f/k_2) \cong Q_8 \rtimes C_2$, the Galois group of a specialization $f((n^2-1)/(2n), x)$ with $n \in \mathbf{Q}$ is isomorphic to a subgroup of $Q_8 \rtimes C_2$. If $f(a,x)$ is irreducible with a specific $a \in \mathbf{Q}$ and the Galois group of $f(a,x)$ is smaller than $Q_8 \rtimes C_2$, then we have $[\Sigma_f^a : \mathbf{Q}] = 8$. Hence, in this case, $f(a,x)$ is an irreducible Galois polynomial. The fields M_1 and M_2 in Proposition 2.2 cannot coincide with $\mathbf{Q}$ by the proof of Theorem 3.1. Hence from Proposition 2.2, it follows that one of M_3, M_4, M_5 or M_6 has to coincide with the base field $\mathbf{Q}$. Therefore, we conclude that the Galois group of $f(a,x)$ is isomorphic to one of the groups $D_4, C_2 \times C_4, Q_8$ by the same proposition.

Proposition 5.1. *We assume that $a = \dfrac{n^2-1}{2n}$ for some $n \in \mathbf{Q}$.*

(i) *If there exists $Y \in \mathbf{Q}$ which satisfies $Y^2 = n^2 + 1$, then $\mathrm{Gal}(\Sigma_f^a/\mathbf{Q}) \cong D_4$.*

(ii) *If there exists $Y \in \mathbf{Q}$ which satisfies $Y^2 = n^4 - 6n^3 + 2n^2 - 6n + 1$ or $Y^2 = n^4 + 6n^3 + 2n^2 + 6n + 1$, then $\mathrm{Gal}(\Sigma_f^a/\mathbf{Q}) \cong C_4 \times C_2$.*

(iii) *If there exists $Y \in \mathbf{Q}$ which satisfies $Y^2 = (n^2+1)(n^2-6n+1)(n^2+6n+1)$, then $\mathrm{Gal}(\Sigma_f^a/\mathbf{Q}) \cong Q_8$.*

(iv) *If none of the conditions above holds, then $\mathrm{Gal}(\Sigma_f^a/\mathbf{Q}) \cong Q_8 \rtimes C_2$.*

Proof. (i) If there exists a rational number Y satisfying $Y^2 = n^2 + 1$, then we have $\sqrt{v(v \pm 1)} = (n \pm 1)/(2n)Y \in \mathbf{Q}$; and hence, $M_3 = \mathbf{Q}$. Thus we get $\mathrm{Gal}(\Sigma_f^a/\mathbf{Q}) \cong D_4$.

(ii) If there exists a rational number Y satisfying $Y^2 = n^4 - 6n^3 + 2n^2 - 6n + 1$, then we have $\sqrt{v(v-3)} = (n-1)/(2n)Y \in \mathbf{Q}$; and hence, $M_4 = \mathbf{Q}$. If there exists a rational number Y which satisfies $Y^2 = n^4 + 6n^3 + 2n^2 + 6n + 1$, then we get $M_5 = \mathbf{Q}$ similarly. Thus in the cases where $M_4 = \mathbf{Q}$ or $M_5 = \mathbf{Q}$, we have $\mathrm{Gal}(\Sigma_f^a/\mathbf{Q}) \cong C_4 \times C_2$.

(iii) If there exists $Y \in \mathbf{Q}$ such that $Y^2 = (n^2+1)(n^2-6n+1)(n^2+6n+1)$, then we have $\sqrt{v(v-1)(v-3)(v+3)} = (n-1)/(4n^2)Y \in \mathbf{Q}$. This implies $M_6 = \mathbf{Q}$. Therefore, we get $\mathrm{Gal}(\Sigma_f^a/\mathbf{Q}) \cong Q_8$.

(iv) If none of the conditions in (i) and (ii) and (iii) is satisfied, then none of the fields M_i ($i = 3,4,5,6$) coincides with $\mathbf{Q}$. Hence, we get $\mathrm{Gal}(\Sigma_f^a/\mathbf{Q}) = \langle \sigma_1^2, \sigma_1\sigma_2, \tau \rangle \cong Q_8 \rtimes C_2$.

□

Remark 5.2. (i) The curve $Y^2 = n^4 - 6n^3 + n^2 - 6n + 1$ in Proposition 5.1 (ii) is a non-singular plane curve of genus 1 and has a rational point $(0:1:0)$ in the projective coordinates. Therefore it has a Weierstrass model $E:\ Y^2Z - 6XYZ - 54YZ^2 = X^3 + 14X^2Z + 45XZ^2$ with $(y:n:z) \mapsto (2n^2z - 6nz^2 + 2yz^2 - 7z^3 : 4n^3 - 12n^2z + 4nyz - 14nz^2 : z^3)$. The Mordell-Weil group of E is

$$E(\mathbf{Q}) = \langle(-9:0:1),(9:126:1)\rangle \cong \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}.$$

Since the inverse map gives $n = 4X^3 - 12X^2Z + 4XYZ - 14XZ^2$, the point $(9:126:1)$ on E gives $a = 24/7$, for example. In general, these corresponding a's have huge heights. All these elliptic curve computation were done with Magma [1].

(ii) The genus 2 curve

$$C : Y^2 = (n^2+1)(n^2-6n+1)(n^2+6n+1)$$

appeared in Proposition 5.1 (iii) has rational points $(1:\pm 1:0)$ and $(0:\pm 1:1)$ in the projective coordinates. These points are irrelevant for our purpose. It is very probable that these are all the rational points on C. The anonymous referee suggested us to use the elliptic Chabauty method by Bruin and Stoll [2] to prove this assertion. We describe the method here.

We decompose the right-hand side of the defining equation of C as a product of

$$A(n) = (n+i)(n^2-6n+1)$$

and

$$B(n) = (n-i)(n^2+6n+1) \in \mathbf{Q}(i)[n].$$

The resultant computation shows $\delta = \gcd(A(n),B(n)) \mid i^2(1+i)^{14}3^4$. We consider an elliptic curve $E_\delta : \delta z^2 = A(n)$ defined over $\mathbf{Q}(i)$. We shall compute the rational points on E_δ over $\mathbf{Q}(i)$ whose n-coordinates are rational and substitute the value of n to C to find the corresponding Y. Since the point (n,z) on $\delta z^2 = A(n)$ corresponds to the point (n,dz) on $d^2\delta z^2 = A(n)$, it suffices to consider squarefree δ's. Thus we may assume $\delta \in \{1,i,3,3i,1+i,3(1+i)\}$. If $\delta \in \{1,3i,3(1+i)\}$, then we find $\operatorname{rank} E_\delta = 0$ and the n-coordinates of the torsion points are 1, which gives $(1:\pm 1:0)$ on C. For the other δ, we have $\operatorname{rank} E_\delta = 1$. Using Magma, we can compute the subgroup E' of $E_\delta(\mathbf{Q}(i))$ of an odd finite index. We apply the elliptic Chabauty method with the map $u : E' \longrightarrow \mathbf{P}^1$, $(X:Y:Z) \mapsto (X:Z)$ to find the subset of E' whose image under u is contained in $\mathbf{P}^1(\mathbf{Q})$. The program successfully finds some points on E_δ with rational n-coordinates but, at this moment, we cannot guarantee that they are all. For example, when $\delta = 3$, the program finds three possible points on E_3

$$\left\{(0:1:0), \left(-\frac{5}{4} : \pm\frac{46+69i}{8} : 1\right)\right\},$$

but the bound of the number of the possible points is greater than 3.

Acknowledgments. The author would like to thank the anonymous referee for his/her helpful and constructive comments on Proposition 5.1. The author also would like to express his gratitude to Prof. Masanari Kida and Dr. Genki Koda for their helpful discussion during the preparation of this paper.

References

[1] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. **24** (1997), no. 3–4, 235–265.

[2] N. Bruin and M. Stoll, The Mordell-Weil sieve: proving non-existence of rational points on curves, LMS J. Comput. Math. **13** (2010), 272–306.

[3] T. Estermann, Einige Sätze über quadratfreie Zahlen, Math. Ann. **105** (1931), no. 1, 653–662.

[4] M. Kida and G. Koda, Isoclinism classes of Galois groups of number fields. (Preprint).

[5] P. Morton, Arithmetic properties of periodic points of quadratic maps, Acta Arith. **62** (1992), no. 4, 343–372.

[6] P. Morton, Characterizing cyclic cubic extensions

by automorphism polynomials, J. Number Theory **49** (1994), no. 2, 183–208.
[7] P. Morton, Arithmetic properties of periodic points of quadratic maps. II, Acta Arith. **87** (1998), no. 2, 89–102.
[8] P. Morton and P. Patel, The Galois theory of periodic points of polynomial maps, Proc. London Math. Soc. (3) **68** (1994), no. 2, 225–263.
[9] J. H. Silverman, *The arithmetic of dynamical systems*, Graduate Texts in Mathematics, 241, Springer, New York, 2007.