QUINTIC POLYNOMIALS OF HASHIMOTO–TSUNOGAI, BRUMER AND KUMMER

Masanari Kida, Guénaël Renault, Kazuhiro Yokoyama

QUINTIC POLYNOMIALS OF HASHIMOTO-TSUNOGAI, BRUMER, AND KUMMER

MASANARI KIDA, GUÉNAËL RENAULT, AND KAZUHIRO YOKOYAMA

Abstract. We establish an isomorphism between the quintic cyclic polynomials discovered by Hashimoto-Tsunogai and those arising from Kummer theory for certain algebraic tori. This enables us to solve the isomorphism problem for Hashimoto-Tsunogai polynomials and also Brumer's quintic polynomials.

1. Introduction

In their paper [6], Hashimoto and Tsunogai construct a quintic polynomial with two parameters having cyclic Galois group by using an action of S_5 on the moduli space of the projective lines with ordered five marked points. Their polynomial is

$$\begin{aligned}
\mathrm{HT}(A,B;X) &= Q^{-2}\left(Q^2X^5 - Q\left(A^3+A^2+10B^2A-3A+20B^2+3\right)X^4\right.\\
&+\left(-24B^2A+28B^2+210B^4A+3-28B^2A^2-40B^4-625B^6\right.\\
&\quad\left.-8A-135B^4A^2-3A^4+2A^5-7B^2A^4+7A^2+44A^3B^2\right)X^3\\
&+\left(4A^4-1+A^6+6A+305B^4+1250B^6+44B^2A^2-220B^4A\right.\\
&\quad\left.-52A^3B^2+345B^4A^2-2A^5+12B^2A+31B^2A^4+11B^2-6A^2\right)X^2\\
&+\left(2A^5-2A^4-8B^2A^4+36A^3B^2-145B^4A^2+3A^2\right.\\
&\quad\left.-22B^2A^2+4B^2A+120B^4A-2A-13B^2-180B^4-625B^6\right)X\\
&\left.-Q\left(A^3+A^2+7B^2A-B^2\right)\right) \in \mathbb{Q}(A,B)[X]
\end{aligned}$$

where $Q = -A+1+B^2A+7B^2$. The polynomial $\mathrm{HT}(A,B;X)$ is a generic polynomial for the cyclic group C_5 of order 5. By definition, all cyclic quintic extensions over any fields K containing $\mathbb{Q}$ can be obtained from $\mathrm{HT}(A,B;X)$ by choosing appropriate parameters A and $B \in K$. The polynomial $\mathrm{HT}(A,B;X)$ is also closely related to the quintic polynomial given by Brumer (see Section 3). In contrast, from this kind of geometric construction, it is usually difficult to extract algebraic or arithmetic information. Typical examples are the decomposition law and the isomorphism problem. We shall mainly discuss the latter problem in this paper. Namely we give a condition for $\mathrm{HT}(A,B;X)$'s with different parameters to define a same field.

On the other hand, a quintic Kummer polynomial is first computed by one of the authors in [10]. It arises from the Kummer theory for certain algebraic torus. To

Date: Version April 24, 2007.

2000 *Mathematics Subject Classification.* 12F10,11R32,12F12,11R20.

This research was partially supported by the Ministry of Education, Science, Sports and Culture, Grant-in-Aid for Scientific Research (C) No.19540015 (2007-2009) and by CREST of Japan Science and Technology Agency.

be more precise, let ζ be a primitive fifth root of unity and k a field of characteristic 0 not containing $\mathbb{Q}(\sqrt{5})$. Denote the automorphism of $k(\zeta)$ sending ζ to ζ^2 by τ, which generates the Galois group $\mathrm{Gal}(k(\zeta)/k)$. From our assumption, $k(\zeta)/k$ is a quartic extension. Let $T = R^{(1)}_{k(\zeta)/k}(\mathbb{G}_m)$ be the norm torus attached to the extension $k(\zeta)/k$. By definition, we have

$$T = \ker\left(N_{k(\zeta)/k} \ : \ R_{k(\zeta)/k}(\mathbb{G}_m) \longrightarrow \mathbb{G}_m\right).$$

In the paper [9], it is proved that T satisfies the Kummer duality

$$T(k)/\lambda T(k) \cong \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\bar{k}/k), \ker\lambda), \tag{1}$$

where λ is a self-isogeny of T of degree 5 induced by the self-isogeny on the split torus $\mathbb{G}_m^3$ given by

$$(X_1, X_2, X_3) \mapsto (X_1X_2^{-1}X_3^{-1}, X_1X_2^2, X_2X_3^2)$$

(see also [10, Section 5]). Our quintic Kummer polynomial is a defining polynomial of this descent Kummer extension. The explicit form of the quintic Kummer polynomial [1] corresponding to the projective parameters

$$(u_1 : u_2 : u_3 : u_4) \in \mathbb{P}^3(k) \twoheadrightarrow T(k)$$

is given by

$$\begin{aligned}\mathrm{Kum}(u_1, u_2, u_3, u_4; X) =& X^5 + \frac{1}{2}\mathrm{Tr}(\xi_3\alpha_1\alpha_3)X^3 + \mathrm{Tr}(\xi_2\alpha_1)X^2 \\ &+ \left(-\frac{1}{25} + \mathrm{Tr}(\xi_{11}\alpha_1^2\alpha_2\alpha_3) + \frac{1}{2}\mathrm{Tr}(\xi_{12}\alpha_1^2\alpha_3^2)\right)X \\ &+ \left(\mathrm{Tr}(\xi_{01}\alpha_1^4\alpha_2\alpha_3^2) + \mathrm{Tr}(\xi_{02}\alpha_1\alpha_2\alpha_3) + \mathrm{Tr}(\xi_{03}\alpha_2^2\alpha_4)\right) \in \mathbb{Q}(u_1, u_2, u_3, u_4)[X],\end{aligned}$$

where the constants ξ's are defined by

$$\begin{aligned}\xi_3 &= \frac{1}{5}(3\zeta + 2\zeta^2 + 3\zeta^4 + 2\zeta^3), & \xi_2 &= \frac{1}{25}(2\zeta - \zeta^2 - 2\zeta^4 + \zeta^3), \\ \xi_{11} &= \frac{1}{25}(\zeta + \zeta^4), & \xi_{12} &= \frac{1}{25}(-2\zeta - \zeta^2 - 2\zeta^4 - \zeta^3), \\ \xi_{01} &= \frac{1}{625}(\zeta - 2\zeta^2 - \zeta^4 + 2\zeta^3), & \xi_{02} &= \frac{1}{125}(\zeta^2 - \zeta^3), \\ \xi_{03} &= \frac{1}{125}(-\zeta - \zeta^2 + \zeta^4 + \zeta^3).\end{aligned}$$

and the parameters are encoded by

$$\begin{aligned}\alpha_1 &= \frac{u_1\zeta + u_2\zeta^2 + u_3\zeta^4 + u_4\zeta^3}{(u_1\zeta + u_2\zeta^2 + u_3\zeta^4 + u_4\zeta^3)^\tau}, \\ \alpha_i &= \alpha^{\tau^{i-1}} \quad (i = 1, 2, 3, 4)\end{aligned}$$

and Tr denotes the trace map from $k(\zeta)$ to k. Here and hereafter, we assume that τ acts trivially on the parameters u_i's. More precisely, we have to assume

$$\mathrm{Gal}\left(k(u_1, u_2, u_3, u_4, \zeta)/k(u_1, u_2, u_3, u_4)\right) \cong \mathrm{Gal}\left(k(\zeta)/k\right) = \langle\tau\rangle$$

[1] Note that in [10, Theorem 2] there is a typo in the third term of the degree-one term in $\mathrm{Kum}(u_1, u_2, u_3, u_4; X)$.

and the trace map is, in fact, defined on $k(u_1, u_2, u_3, u_4, \zeta)$. Though this polynomial looks complicated and has more parameters than the Hashimoto-Tsunogai polynomial, it has many nice properties since it comes from Kummer theory. In addition to being a generic C_5-polynomial over $\mathbb{Q}$ (except for fields containing $\mathbb{Q}(\sqrt{5})$), it naturally preserves algebraic and arithmetic information. Actually we can solve the isomorphism problem and deduce the prime decomposition law for this Kummer family (see [10, Section 5]).

The first aim of this paper is to embed the Hashimoto-Tsunogai polynomial in this Kummer's quintic family. By doing so, we can settle the isomorphism problem for $\mathrm{HT}(A, B; T)$. One of our main theorems is the following.

Theorem 1.1. *The polynomial* $\mathrm{Kum}(-A - 5B, -5B - 1, A - 5B, 1 - 5B; X)$ *defines the same cyclic quintic field as* $\mathrm{HT}(A, B; X)$ *over* $\mathbb{Q}(A, B)$.

We prove this theorem in the next section.

The rest of the paper is organized as follows.

Choosing particular parameters in the Hashimoto-Tsunogai polynomial, we get Brumer's quintic polynomial, which is generic for the dihedral group of order 10. Using the result on the Hashimoto-Tsunogai polynomial, we can also settle the isomorphism problem for Brumer's family. This is the main subject in Section 3.

In Section 4, we prove a supplementary result concerning Brumer's quintic polynomials in the case where its splitting field contains $\mathbb{Q}(\sqrt{5})$.

In Section 5, we deduce a condition for a quadratic field to have an unramified quintic extension. Such an unramified extension is a D_5 extension over the rational number field $\mathbb{Q}$. Therefore it can be obtained by choosing appropriate parameters in Brumer's family.

In Section 6, we employ our method to study the isomorphism problems for cubic polynomials.

In Section 7, we construct an infinite family of Brumer polynomials defining an isomorphic splitting field. The technique of the proof used in this section is different from other sections. But this topic is of independent interest and the authors believe that it is worth including this section in this paper.

Throughout this paper, we denote a fixed primitive 5-th root of unity by ζ.

2. Proof of Theorem 1.1

In this section, we prove Theorem 1.1. We write the proof in detail, since we use a similar technique in the rest of this paper.

Let $Q = -A + 1 + B^2A + 7B^2$ be the quantity appeared in the denominator of $\mathrm{HT}(A, B; X)$. We cancel the denominator of $\mathrm{HT}(A, B; X)$ by setting

$$\mathrm{ht}(A, B; X) = Q^5\mathrm{HT}(A, B; X/Q).$$

We have $\mathrm{ht}(A, B; X) \in \mathbb{Q}[A, B][X]$.

To cancel the denominators of $\mathrm{Kum}(u_1, u_2, u_3, u_4; X)$, let

$$N = \mathrm{Norm}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(u_1\zeta + u_2\zeta^2 + u_3\zeta^4 + u_4\zeta^3)$$

be the norm form of $\mathbb{Q}(\zeta)/\mathbb{Q}$. By the defining formula of the α_i's, only divisors of N can appear in the denominators of $\mathrm{Kum}(u_1, u_2, u_3, u_4; X)$. By setting

$$u_1 = -A - 5B,\ u_2 = -5B - 1,\ u_3 = A - 5B,\ u_4 = 1 - 5B,$$

we define

$$\mathrm{kum}(A,B;X) = N^5\mathrm{Kum}(-A-5B,-5B-1,A-5B,1-5B;X/N) \in \mathbb{Q}[A,B][X].$$

Now we use Trager's scheme [15] (see also [4, 3.6.2]. In [1] this scheme is presented with some tricks in order to compute the splitting field of a polynomial). Let $\beta = \beta(A,B)$ be a root of $\mathrm{ht}(A,B;X)$ and $\gamma = \gamma(A,B)$ a root of $\mathrm{kum}(A,B;X)$. We compute a polynomial satisfied by $\beta + 2\gamma$ using the resultant

$$\mathrm{Res}_X(\mathrm{ht}(A,B;Y-2X), \mathrm{kum}(A,B;X)) \in \mathbb{Q}[A,B][Y]$$

with respect to X. This is a polynomial of degree 25 in Y. We factor this polynomial over $\mathbb{Q}[A,B]$ and obtain five distinct factors of degree 5. This computation is done by using Magma [2] and the result is checked again by Risa/Asir [12]. Since the both polynomials have C_5 as the Galois group, this result means that $\beta + 2\gamma$ is a primitive element of the composite field $\mathbb{Q}(A,B)(\beta,\gamma)$, which is equal to the splitting field of $\mathrm{ht}(A,B;X)$ and $\mathrm{kum}(A,B;X)$. Therefore we have $\mathbb{Q}(A,B)(\beta,\gamma) = \mathbb{Q}(A,B)(\beta) = \mathbb{Q}(A,B)(\gamma)$. This shows that $\mathrm{ht}(A,B;X)$ and $\mathrm{kum}(A,B;X)$ defines the same field. This completes the proof of the theorem.

Remark 2.1. In [10, Theorem 4], we embed Lehmer's quintic family to Kummer's family. In doing this, we compute a Lagrange resolvent ([5, Theorem 5.3.5(4)]). But in our present case, since the Galois action of $\mathrm{HT}(A,B;X)$ is not simply described, computing this Lagrange resolvent is not easy.

Remark 2.2. Evaluating each factor obtained in the proof by $\beta + 2\gamma$ in the quotient ring $\mathbb{Q}[A,B][X]/(\mathrm{ht}(A,B;X))$, we can get an explicit expression of β in terms of a polynomial in γ.

If the reader is interested in the explicit form of the factorization of the resultant and the explicit expression of β, please refer to one of the authors' webpage at `http://www-spiral.lip6.fr/~renault/softwares_en.html`.

To state the isomorphism condition, the following definition is useful.

Definition 2.3. For the parameters A and B, we set

$$\beta_i = \beta_i(A,B) = ((-A-5B)(\zeta) + (-5B-1)(\zeta^2) + (A-5B)(\zeta^4) + (1-5B)(\zeta^3))^{\tau^{i-1}}$$

which is the numerator of α_i with parameters A and B. Here we assume that τ acts trivially on A and B. Using these β_i, we define

$$\Gamma(A,B) = \beta_1^4\beta_2^2\beta_3\beta_4^3 \in \mathbb{Q}(A,B,\zeta). \tag{2}$$

Corollary 2.4. *Assume that* $\mathbb{Q}(A,B) = \mathbb{Q}(A',B')$ *and that* $\mathbb{Q}(A,B)$ *does not contain* $\mathbb{Q}(\sqrt{5})$. *Then two polynomials* $\mathrm{HT}(A,B;X)$ *and* $\mathrm{HT}(A',B';X)$ *define the same quintic field over* $\mathbb{Q}(A,B)$ *if and only if there exists an integer* j *prime to* 5 *such that*

$$\Gamma(A,B) \equiv \Gamma(A',B')^j \pmod{(\mathbb{Q}(A,B,\zeta)^\times)^5}.$$

Proof. Let $L_{A,B}$ be the cyclic quintic field defined by $\mathrm{Kum}(-A-5B,-5B-1,A-5B,1-5B;X)$. By Theorem 1.1, the field $L_{A,B}$ coincides with the splitting field of $\mathrm{HT}(A,B;X)$. Now the extension $L_{A,B}(\zeta)/\mathbb{Q}(A,B,\zeta)$ is a classical Kummer extension. In [10, Equation (7)] it is shown that our Kummer duality (1) implies

$$L_{A,B}(\zeta) = \mathbb{Q}(A,B,\zeta)\left(\sqrt[5]{\alpha_1^4\alpha_2\alpha_3^2}\right) = \mathbb{Q}(A,B,\zeta)\left(\sqrt[5]{\Gamma(A,B)}\right).$$

Since $L_{A,B}$ is a unique cyclic quintic extension over $\mathbb{Q}(A,B)$ inside $L_{A,B}(\zeta)$, two fields $L_{A,B}$ and $L_{A',B'}$ are isomorphic if and only if $L_{A,B}(\zeta)$ and $L_{A',B'}(\zeta)$ are isomorphic. Thus the result now follows from [5, Corollary 10.2.7(2)]. □

3. Brumer's quintic family

Let a, b be rational parameters. Brumer's quintic polynomial is given by

$$\mathrm{Bru}(a,b;X) = X^5 + (-3+a)X^4 + (3+b-a)X^3 + (-1-a-2b+a^2)X^2 + bX + a.$$

There are several known proofs showing that $\mathrm{Bru}(a,b;X)$ is a generic polynomial for the dihedral group D_5 of order 10 (see, for example, [8, Theorem 2.3.5] and [6, Theorem 1]. See also [13], where a *relation ideal* for this polynomial is computed and give another proof of this result). In this section, we solve the isomorphism problem for $\mathrm{Bru}(a,b;X)$. This can be achieved by using the results in the previous section, since Hashimoto and Tsunogai establish a relationship between $\mathrm{HT}(A,B;X)$ and $\mathrm{Bru}(a,b;X)$. We now state this relation. We set

$$d(a,b) = -4b^3 - (-a^2+30a-1)b^2 - (-24a^3+34a^2+14a)b - (4a^5-4a^4-40a^3+91a^2-4a).$$

Let $c = c(a,b)$ be a zero of

$$c^2 - d(a,b) = 0. \tag{3}$$

It is known that the D_5-extension over $\mathbb{Q}(a,b)$ defined by $\mathrm{Bru}(a,b;X)$ contains the quadratic extension $\mathbb{Q}(a,b,c)$. With parameters given by

$$A = -\frac{2a^3-2a^2+13a-7ab+b}{8a^2-33a-ab-7b+2}, \quad B = -\frac{c}{8a^2-33a-ab-7b+2}, \tag{4}$$

Hashimoto and Tsunogai ([6, Theorem 2]) proved that $\mathrm{HT}(A,B;X)$ and $\mathrm{Bru}(a,b;X)$ define the same field over $\mathbb{Q}(a,b)$.

Therefore, assuming $\mathbb{Q}(a,b) = \mathbb{Q}(a',b')$, two polynomials $\mathrm{Bru}(a,b;X)$ and $\mathrm{Bru}(a',b';X)$ define the same field if and only if the following two properties are satisfied:

(i) the quadratic fields $\mathbb{Q}(a,b,c)$ and $\mathbb{Q}(a',b',c')$ coincide, where $c' = c(a',b')$.
(ii) $\mathrm{HT}(A,B;X)$ and $\mathrm{HT}(A',B';X)$ define the same cyclic quintic field over $\mathbb{Q}(a,b,c)$, where A' and B' are given by (4) with a' and b'.

For parameters a and b, we set

$$\Delta(a,b) = \Gamma(A,B) \in \mathbb{Q}(\zeta,a,b,c,\zeta)$$

where A and B are substituted by (4).

The following theorem immediately follows from Corollary 2.4.

Theorem 3.1. *Assume that* $\mathbb{Q}(a,b) = \mathbb{Q}(a',b')$ *and that* $\mathbb{Q}(a,b,c)$ *does not contain* $\mathbb{Q}(\sqrt{5})$. *Then two Brumer polynomials* $\mathrm{Bru}(a,b;X)$ *and* $\mathrm{Bru}(a',b';X)$ *define the same* D_5*-extension over* $\mathbb{Q}(a,b)$ *if and only if the following two conditions holds:*

(i) $d(a,b) \equiv d(a',b') \pmod{(\mathbb{Q}(a,b)^\times)^2}$;
(ii) $\Delta(a,b) \equiv \Delta(a',b')^j \pmod{(\mathbb{Q}(a,b,c,\zeta)^\times)^5}$ *for some integer* j *coprime to* 5.

Example 3.2. Let us consider

$$\mathrm{Bru}(1,0;X) = X^5 - 2X^4 + 2X^3 - X^2 + 1.$$

The discriminant of this polynomial is 47^2. Its splitting field K_0 is an unramified cyclic quintic extension over $k_0 = \mathbb{Q}(\sqrt{-47})$, which coincides with the Hilbert class field of k_0, since the class number of k_0 is 5. We shall show that

$$\mathrm{Bru}(5,-43;X) = X^5 + 2X^4 - 45X^3 + 105X^2 - 43X + 5$$

has the same splitting field as $\mathrm{Bru}(1,0;X)$ does. In fact, we have

$$d(1,0) = -47, \quad d(5,-43) = -7943 = 13^2 \cdot d(1,0).$$

Thus they have the same quadratic subfield k_0. We compute

$$\begin{aligned}\Delta(1,0) = {} & \frac{1}{51764766400764507882149} \\ & \times (-1389598090379846016000\theta^7 + 327585345693709056000\theta^6 \\ & - 22788447658717288729600\theta^5 + 1264730529918331257600000\theta^4 \\ & - 121776231689302425765120000\theta^3 + 12303554581549491465344000\theta^2 \\ & - 2100713228774548590058240000\theta + 361512713131558684185344000)\end{aligned}$$

and

$$\begin{aligned}\Delta(5,-43) = {} & \frac{1}{3342005893184375612029355674097696549} \\ & \times (272139912396910259110087101202472323840000\theta^7 \\ & - 98412862776754104316953355552659511040000\theta^6 \\ & + 40607264386433828955054550157653337456640000\theta^5 \\ & - 35597437577755549941258123306443911808000000\theta^4 \\ & + 20107103247684822255556703257391117806732800\theta^3 \\ & - 28120459386200154473752354421698218101273600\theta^2 \\ & + 32817477561227882663584532140657371115612160000\theta \\ & - 61283012514355646372980029147433992951477760000),\end{aligned}$$

where $\theta = \sqrt{-47} + \zeta$ is a primitive element of $\mathbb{Q}(\sqrt{-47}, \zeta)$. Then we have

$$\Delta(1,0) = \Delta(5,-43)^2 w^5$$

with

$$\begin{aligned}w = {} & -\frac{1}{1730900504206195972290357039567 80} \\ & \times (-17923362519164587812721632\theta^7 - 61021321258567091804980913\theta^6 \\ & - 26864839642754412009724765220\theta^5 - 86162191698218877377627991080\theta^4 \\ & - 133820593407682936889507718982\theta^3 - 373410590307164678518505330012\theta^2 \\ & - 223395158918229413886125804509 2\theta - 48790135678224727230025362267 34).\end{aligned}$$

Among the rational integers in the range $-400 \le a, b \le 400$, there are 25 pairs defining the same field as $\mathrm{Br}(1,0)$:

$$\begin{aligned}(a,b) = {} & (-23,125),(-5,36),(-5,59),(-5,372),(-1,-1),(-1,4),(-1,5),(-1,46), \\ & (1,-6),(1,-1),(1,0),(1,41),(5,-43),(5,4),(11,34),(11,149),(13,47),\end{aligned}$$

$$(19,-24),(19,59),(19,101),(23,-188),(25,155),(31,264),(43,378),(55,-169).$$

One naturally makes a question whether there are infinitely many these pairs or not. We will discuss this issue in the final section.

4. Supplementary result

In the previous section, we have settled the isomorphism problem for Brumer's polynomials in almost all cases. The exception is the case where the quadratic subfield of the D_5-extension contains $\mathbb{Q}(\sqrt{5})$. Even if $\mathbb{Q}(u_1,u_2,u_3,u_4)$ contains $\mathbb{Q}(\sqrt{5})$, $\mathrm{Kum}(u_1,u_2,u_3,u_4;X)$ gives all cyclic quintic extensions over $\mathbb{Q}(a,b,c)$ by Theorem 1.1. But in this case the Galois action on the parameters is no more trivial and the Kummer duality (1) does not holds. This means that we cannot conclude the Kummer generator is given by (2). To resolve the isomorphism problem for this case, instead of quartic descent (1), we use a quadratic descent Kummer theory.

Let k be a field not containing the fifth root of unity ζ but contain $\sqrt{5}$. Then the 5-th power map [5] on the 1-dimensional norm torus $T = R^{(1)}_{k(\zeta)/k}\mathbb{G}_m$ induces the Kummer duality

$$T(k)/[5]T(k) \cong \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\bar{k}/k), \ker[5]). \tag{5}$$

Setting $\delta = (\zeta^2-\zeta^{-2})^2 = \dfrac{-5+\sqrt{5}}{2}$, we have $k = k(\delta)$ and $k(\zeta) = k(\sqrt{\delta})$. The quintic cyclic polynomial arising from this duality is computed in [9, Example 6.1]:

$$\mathrm{Kum}_2(u_1,u_2;X) = 16X^5 - 20X^3 + 5X - \frac{u_1^2+\delta u_2^2}{u_1^2-\delta u_2^2}.$$

with parameters $(u_1 : u_2) \in \mathbb{P}^1(k)$. The Galois group of $\mathrm{Kum}_2(u_1,u_2;X)$ over k is C_5.

We prove the following theorem.

Proposition 4.1. *Assume that* $\mathbb{Q}(A,B,\zeta) \cap \mathbb{Q}(\delta,A,B) = \mathbb{Q}(\delta)$ *holds. Let*

$$u_1 = \frac{1}{4}\{(A^3+2A-4A^2-75B^2+25B^2A+3) + \delta(-20B^2+15B^2A-A^2+A+1)\}, \tag{6}$$

$$u_2 = \frac{1}{4}\{(20B-5A^2B-75B^3) + \delta(-25B^3+5B)\}. \tag{7}$$

Then $\mathrm{HT}(A,B;X)$ *and* $\mathrm{Kum}_2(u_1,u_2;X)$ *define the same quintic cyclic field over* $\mathbb{Q}(\delta,A,B)$.

Proof. The proof is almost the same as that of Theorem 1.1. We cancel the denominators and compute the factorization of the resultant

$$\mathrm{Res}_X(\mathrm{ht}(A,B;Y-2X), \mathrm{kum}_2(A,B;X)) \in \mathbb{Q}[A,B][Y].$$

Since the base field is larger than before, the computation becomes harder. But again in this case, we obtain five distinct factors of degree 5. □

Using the quadratic descent Kummer theory (5), the solution of the isomorphism problem for this case can be given. Before stating it, we need the following definition.

Definition 4.2. For the parameters a and b, we have set

$$A = -\frac{2a^3-2a^2+13a-7ab+b}{8a^2-33a-ab-7b+2}, \quad B = -\frac{c}{8a^2-33a-ab-7b+2}$$

where $c = c(a,b)$ is a solution of $c^2 - d(a,b) = 0$ (see (3) and (4)). Using these A and B, we define

$$\Lambda(a,b) = \frac{u_1 + \sqrt{\delta}u_2}{u_1 - \sqrt{\delta}u_2}$$

and

$$\overline{\mathrm{Kum}_2}(a,b;X) = \mathrm{Kum}_2(u_1,u_2;X)$$

where u_1 and u_2 are given by (6) and (7).

Corollary 4.3. *Suppose that* $\mathbb{Q}(a,b,c) = \mathbb{Q}(a',b',c') \supset \mathbb{Q}(\sqrt{5})$ *where* $c' = c(a',b')$. *Then* $\mathrm{Bru}(a,b;X)$ *and* $\mathrm{Bru}(a',b';X)$ *define the same* D_5 *extension if and only if there exists an integer* j *coprime to* 3 *satisfying*

$$\Lambda(a,b) \equiv \Lambda(a',b')^j \pmod{(\mathbb{Q}(a,b,\zeta)^\times)^5}. \tag{8}$$

Proof. By Proposition 4.1, we have only to show that $\overline{\mathrm{Kum}_2}(a,b;X)$ and $\overline{\mathrm{Kum}_2}(a',b';X)$ define the same field over $\mathbb{Q}(a,b,c)$. By the argument similar to those given in [10], we can prove that the field defined by $\overline{\mathrm{Kum}_2}(a,b;X)$ is contained in

$$\mathbb{Q}(a,b,\zeta)\left(\sqrt[5]{\Lambda(a,b)}\right).$$

Thus by the same argument as Corollary 2.4, this corollary follows again from [5, Corollary 10.2.7(2)]. □

We give the condition (8) in a computationally convenient form. We can rewrite it using the following general lemma.

Lemma 4.4. *Let* k *be a field of characteristic* 0. *We assume that* $K = k(\zeta_n)$ *is a cyclic extension over* k, *where* ζ_n *is a primitive* n*-th root of unity. Let* τ *be a generator of the Galois group of* K/k. *Let* a_1, a_2 *be elements of* $K^\times$. *Then* $K\left(\sqrt[n]{\frac{a_1}{a_1^\tau}}\right) \cong K\left(\sqrt[n]{\frac{a_2}{a_2^\tau}}\right)$ *if and only if there exist an integer* j *prime to* n *and* $t \in k$ *and* $\gamma \in K^\times$ *so that* $a_1 = t a_2^j \gamma^n$ *holds.*

Proof. By [5, Corollary 10.2.7(2)], these two fields are isomorphic if and only if there exist an integer prime to n and $\delta \in K^\times$ such that $\frac{a_1}{a_1^\tau} = \left(\frac{a_2}{a_2^\tau}\right)^j \delta^n$. Taking the norm to k, we see $N_{K/k}\delta = 1$. By Hilbert's theorem 90, we can find $\gamma \in K$ satisfying $\delta = \gamma/\gamma^\tau$. It yields that

$$\left(\frac{a_2^j\gamma^n}{a_1}\right)^\tau = \frac{a_2^j\gamma^n}{a_1}.$$

This shows that $t = a_2^j\eta^n/a_1$ is an element of k. Since the opposite direction is almost obvious, this completes the proof. □

By noting that the generator of $\mathrm{Gal}(\mathbb{Q}(a,b,\zeta)/\mathbb{Q}(a,b,c))$ acts by $\sqrt{d} \mapsto -\sqrt{d}$, it follows from Lemma 4.4 that the condition (8) is equivalent to

$$u_1 + \sqrt{d}u_2 \equiv t(u_1' + \sqrt{d}u_2')^j \pmod{(\mathbb{Q}(a,b,\zeta)^\times)^5}$$

for some $t \in \mathbb{Q}(a,b,d)$ and some integer j prime to 3.

5. Arithmetic application

Since we have embedded the Brumer family to the Kummer family, it becomes easier to deduce arithmetic information. The decomposition law in the quintic Kummer family is essentially given in [10, Theorem 2]. Here in this section, we use this decomposition law to construct quadratic fields whose class number is divisible by 5.

We have the following proposition.

Proposition 5.1. *Let a and b be rational numbers and $B_{a,b}$ the splitting field of* $\mathrm{Br}(a,b;X)$. *Assume that $\mathbb{Q}(c)$ is neither $\mathbb{Q}(\sqrt{5})$ nor $\mathbb{Q}$. Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Q}(\zeta,c)$ and $v_{\mathfrak{p}}$ the normalized exponential discrete valuation associated to $\mathfrak{p}$. We set $\mathfrak{p}_c = \mathfrak{p} \cap \mathscr{O}_{\mathbb{Q}(c)}$. For $i = 1,\dots,4$, we define*

$$s_i = v_{\mathfrak{p}^{\tau^{i-1}}}(\beta_1),$$
$$u(\mathfrak{p}) = 4s_1 + 2s_4 + s_3 + 3s_2.$$

When $\mathfrak{p}$ is prime to 5, then $\mathfrak{p}_c$ is unramified in $B_{a,b}/\mathbb{Q}(c)$ if and only if

$$u(\mathfrak{p}) \equiv 0 \pmod 5 \tag{9}$$

holds. When $\mathfrak{p}$ is lying above 5, $\mathfrak{p}_c$ is unramified in $B_{a,b}/\mathbb{Q}(c)$ if and only if, in addition to that (9) *holds, the congruence*

$$x^5 \equiv \Delta(a,b) \pmod{\mathfrak{p}^{5+v_{\mathfrak{p}}(\Delta(a,b))}} \tag{10}$$

has a solution x in $\mathscr{O}_{\mathbb{Q}(\zeta,c)}$.

Proof. Since the extension degree $[\mathbb{Q}(\zeta):\mathbb{Q}(c)]$ is prime to 5, the extension $B_{a,b}/\mathbb{Q}(c)$ is unramified at $\mathfrak{p}_c$ if and only if $\mathfrak{p}$ is unramified in $\mathbb{Q}(\zeta,\sqrt[5]{\Delta(a,b)})/\mathbb{Q}(\zeta,a,b)$. It is easy to deduce from Hecke's theory [5, 10.2.3] that the Kummer extension $\mathbb{Q}(\zeta,\sqrt[5]{\Delta(a,b)})/\mathbb{Q}(\zeta,a,b)$ is unramified at $\mathfrak{p}$ if and only if the following two conditions are satisfied:

$$v_{\mathfrak{p}}(\Delta(a,b)) \equiv 0 \pmod 5 \text{ for all } \mathfrak{p},$$
$$\text{and (10) has a solution } x \text{ in } \mathscr{O}_{\mathbb{Q}(\zeta,c)} \text{ if } \mathfrak{p}|5.$$

We can readily show that the first condition is equivalent to (9). □

Corollary 5.2. *Let S be a set of prime ideals of $\mathbb{Q}(\zeta,c)$ containing prime ideals lying above 5 and prime divisors of β_1 lying above rational primes p satisfying $\left(\frac{d_{\mathbb{Q}(c)}}{p}\right) \equiv p \pmod 5$. Then the class number h_c of $\mathbb{Q}(c)$ is divisible by 5 if and only if the following two conditions are satisfied:*

For all prime ideals in S, we have $u(\mathfrak{p}) \equiv 0 \pmod 5$.

For prime ideals $\mathfrak{p}$ lying above 5, the congruence (10) *has a solution.*

Proof. By class field theory, the class number h_c is divisible by 5 if and only if there exists an unramified extension of degree 5 over $\mathbb{Q}(c)$. It is easy to observe that the unramified extension is a D_5-extension over $\mathbb{Q}$. Thus we can apply Proposition 5.1 to our case. Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Q}(\zeta,c)$. If the decomposition group of $\mathfrak{p}$ in $\mathbb{Q}(\zeta,c)/\mathbb{Q}(c)$ is not trivial, then $u(\mathfrak{p}) = 10s_1$ or $5s_1 + 5s_4$ and the condition (9) is always satisfied. From the prime decomposition law in cyclotomic fields, we have

the decomposition group is trivial if and only if $\left(\frac{d_{\mathbb{Q}(c)}}{p}\right) \equiv p \pmod 5$. The prime ideals lying above these primes are possibly ramified primes in $\mathbb{Q}(\zeta, \sqrt[5]{\Delta(a,b)})$. The corollary now follows from Proposition 5.1. □

The general solution of (9) is

$$(s_1, s_2, s_3, s_4) = (5k + a + b, -5k - 2a - c, 10k + 4a + 3c, -5k - a - 2b)$$

and typical solutions are $(s_1, s_2, s_3, s_4) = (s, s, s, s), (0, 0, 1, 2), \dots$ etc. Note that $u(\mathfrak{p}) \bmod 5$ does not depend on the choice of $\mathfrak{p}$ lying above $\mathfrak{p}_c$.

There is an algorithm to solve the congruence (10). This algorithm is explained in [5, 10.2.4]. Since our case is one of the easiest case, we write it down here. Dividing $\Delta(a, b)$ by an appropriate powers of uniformizer at $\mathfrak{p}$, we may assume $v_{\mathfrak{p}}(\Delta(a, b)) = 0$. Now we find an element y satisfying $y^5 \equiv \Delta(a, b) \pmod{\mathfrak{p}}$. This requires only a cheap computation because $(\mathcal{O}_{\mathbb{Q}(\zeta,c)}/\mathfrak{p})^*$ is of order 4 or 24. Then the congruence (10) is solvable if and only if $v_{\mathfrak{p}}(y^5 - \Delta(a, b)) \geq 5$.

Example 5.3. We consider Bru(1, 0) in Example 3.2 again. We compute

$$\begin{aligned}\beta_1 = {} & \frac{1}{988907761786907} \\ & \times (267349738220\theta^7 + 1533902716170\theta^6 \\ & + 41291511455160\theta^5 + 302133947784150\theta^4 \\ & + 2257196872167400\theta^3 + 18117815686536210\theta^2 \\ & + 44539619360343190\theta + 33723166487238680).\end{aligned}$$

The prime ideal lying above 19 appear as a prime divisor of β_1. Since $\left(\frac{-47}{19}\right) = -1 \equiv 19 \pmod 5$, the prime ideal lying above 19 is possibly ramified. We compute $(s_1, s_2, s_3, s_4) = (2, 0, 0, 1)$ for a choice of $\mathfrak{p}$ and $u(\mathfrak{p}) = 5$. Thus the prime ideal in $\mathbb{Q}(\sqrt{-47})$ lying above 19 does not ramify in $B_{0,1}$.

6. Cubic polynomials

In this section, we apply our method to cubic generic polynomials to solve the isomorphism problems for cubic polynomials. Several authors considered the isomorphism problems for this cubic case. See, for example, [3], [11] and [7]. The authors are indebted to Akinari Hoshi for these references. Our approach is similar to that of Chapman [3]. He uses classical Kummer theory to characterize the isomorphisms among cyclic cubic polynomials. On the other hand, we use a descent Kummer theory.

If the base field k contains $\sqrt{-3}$, the classical Kummer theory takes care of it. Thus we may assume that the base field k does not contain $\sqrt{-3}$. Consider the 1-dimensional norm torus $T = R^{(1)}_{k(\sqrt{-3})/k}\mathbb{G}_m$. Then the third power map [3] on T induces the Kummer duality

$$T(k)/[3]T(k) \cong \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\bar{k}/k), \ker[3]).$$

The Kummer polynomial for this case is computed in [9, Example 6.1]:

$$\mathrm{Kum}_3(u_1, u_2; X) = 4X^3 - 3X - \frac{u_1^2 + du_2^2}{u_1^2 - du_2^2}.$$

with parameters $(u_1 : u_2) \in \mathbb{P}^1(k)$.

We start with Shanks' simplest cubic polynomial

$$\mathrm{Sha}(t; X) = X^3 - tX^2 + (t-3)X + 1,$$

which is a generic C_3-polynomial over $\mathbb{Q}$.

The relationship between these two cubic polynomials is given by the following proposition.

Proposition 6.1. *Let*

$$u_1 = 8t^3 - 36t^2 + 108t - 108, \quad u_2 = 12t^2 - 36t + 108.$$

The cubic polynomials $\mathrm{Sha}(t; X)$ *and* $\mathrm{Kum}_3(u_1, u_2; X)$ *define the same cyclic cubic field over* $\mathbb{Q}(t)$.

We can prove this proposition by the same method used in Theorem 1.1. Thus we omit the proof.

Corollary 6.2 (cf. [3, Proposition 4])**.** *We assume* $\mathbb{Q}(t) = \mathbb{Q}(t')$. *Then two Shanks' polynomials* $\mathrm{Sha}(t; X)$ *and* $\mathrm{Sha}(t'; X)$ *define the same field if and only if there exists an integer* j *prime to* 3 *and* $s \in \mathbb{Q}(t)$ *such that*

$$u_1 + \sqrt{-3}u_2 \equiv s(u_1' + \sqrt{-3}u_2')^j \pmod{(\mathbb{Q}(t, \sqrt{-3})^\times)^3}$$

holds.

Proof. As in Corollary 4.3, we know that the field defined by $\mathrm{Kum}_3(u_1, u_2; X)$ is contained in $\mathbb{Q}(a, b, \sqrt{-3})\left(\sqrt[3]{\frac{u_1+\sqrt{-3}u_2}{u_1-\sqrt{-3}u_2}}\right)$. Therefore the corollary is derived by a similar argument as Corollary 4.3 using Lemma 4.4. □

Of course we can rewrite the condition as in [3, Corollary 1 to Proposition 4].

Next we consider the following generic S_3-polynomial:

$$\mathrm{G}(t; X) = X^3 + tX + t.$$

Although Chapman's method is limited to the cyclic case, we can deal with this S_3-polynomial in a similar manner.

We can show:

Proposition 6.3. *The two cubic polynomials* $\mathrm{G}(t; X)$ *and* $\mathrm{Kum}_3(4\sqrt{-4t^3 - 27t^2}, 12t; X)$ *define the same* S_3*-extension over* $\mathbb{Q}(t)$.

Proof. It is easy to show that the splitting field Spl_G of $\mathrm{G}(t; X)$ contains the quadratic field $\mathbb{Q}(\sqrt{-4t^3 - 27t^2}) = \mathbb{Q}(\sqrt{-4t - 27})$. We factorize

$$\mathrm{Res}_X(\mathrm{G}(t; Y - 2X), \mathrm{Kum}_3(4\sqrt{-4t^3 - 27t^2}, 12t; X)) \in \mathbb{Q}(t)[Y].$$

It decomposes into a cubic and a sextic irreducible factors. This means that Spl_G contains the stem field of $\mathrm{Kum}_3(4\sqrt{-4t^3 - 27t^2}, 12t; X)$, which is a cubic extension. Thus Spl_G is a S_3-extension over $\mathbb{Q}(t)$ containing a root of $\mathrm{Kum}_3(4\sqrt{-4t^3 - 27t^2}, 12t; X)$, hence the splitting fields of these two polynomials coincide. □

As a corollary, we obtain:

Corollary 6.4. *Assume that* $\mathbb{Q}(t) = \mathbb{Q}(t')$. *Define*

$$u_1 = u_1(t) = 4\sqrt{-4t^3 - 27t^2} \text{ and } u_2 = u_2(t) = 12t.$$

Two polynomials $\mathrm{G}(t; X)$ *and* $\mathrm{G}(t'; X)$ *define the same field if and only if the following two conditions are satisfied:*

(i) $4t + 27 = (4t' + 27)v^2$ *for some* $v \in \mathbb{Q}(t)^\times$;

(ii) $u_1(t) + \sqrt{-3}u_2(t) \equiv s(u_1(t') + \sqrt{-3}u_2(t'))^j \pmod{(\mathbb{Q}(\sqrt{-4t^3 - 27t^2}, \sqrt{-3})^\times)^3}$ *for some integer* j *prime to* 3 *and* $s \in \mathbb{Q}(\sqrt{-4t^3 - 27t^2})$.

We also omit the proof of this corollary.

It is interesting to know a relationship between this corollary and Theorem 1 in [7].

7. Brumer's quintic polynomials defining the Hilbert class field of $\mathbb{Q}(\sqrt{-47})$

This section serves as an appendix of this paper. Here we shall construct an infinite family of Brumer polynomials defining an isomorphic splitting field. We prove the following theorem.

Theorem 7.1. *Let* E *be an elliptic curve defined by*

$$E: \ y^2 = x^3 + 1316x^2 + 212064x + 78074896.$$

For a rational point $(x, y) \in E(\mathbb{Q})$, *let* $b = x/188$. *If* $\mathrm{Bru}(1, b; X)$ *is irreducible, then* $\mathrm{Bru}(1, b; X)$ *has the same splitting field as* $\mathrm{Bru}(1, 0; X)$. *Moreover, there are infinitely many* b*'s for which* $\mathrm{Bru}(1, b; X)$ *is irreducible.*

Proof. Let K_0 be the splitting field of $\mathrm{Bru}(1, 0; X)$. As we see in Example 3.2, K_0 is the Hilbert class field of $k_0 = \mathbb{Q}(\sqrt{-47})$. We consider

$$\mathrm{Bru}(1, b; X) = X^5 - 2X^4 + (2 + b)X^3 + (-1 - 2b)X^2 + bX + 1.$$

The splitting field of $\mathrm{Bru}(1, b; X)$ contains k_0 if and only if the Diophantine equation $-47u^2 = d(1, b)$ has a solution $u \in \mathbb{Q}$. Namely we have

$$-47u^2 = -4b^3 - 28b^2 - 24b - 47.$$

Setting $x = 188b$, $y = 8836u$, we have the elliptic curve E in the statement of the theorem. The elliptic curve E is of conductor $11 \cdot 47^2$ and the discriminant of the model is $2^{12} \cdot 11^5 \cdot 47^6$. The Mordell-Weil group is a torsion-free group of rank 2 generated by $P_1 = (-188, 8836)$ and $P_2 = (0, -8836)$. We write the rational point $(x, y) \in E(\mathbb{Q})$ by the fractions

$$x = \frac{r}{t^2}, \ y = \frac{s}{t^3} \quad (r, s, t \in \mathbb{Z})$$

in the lowest terms. Then we have

$$b = \frac{r}{2^2 \cdot 47t^2}.$$

We substitute these equations to $\mathrm{Bru}(1, b; X)$ and clear the denominators and obtain the following equivalent polynomial:

(11)

$$B(b; X) = X^5 - 2^2 \cdot 47X^4 + (2^3 \cdot 47t^2 + 47r)X^3 + (-2^3 \cdot 47^3t^3 - 2^2 \cdot 47^2)X^2 + 2^2 \cdot 47^3rt^2X + 2^5 \cdot 47^5t^5$$

whose discriminant is $2^{12} \cdot 47^{14} t^8 s^4$. Let F be a quintic field generated by a zero of $B(b; X)$. We shall show that the splitting field of $B(b; X)$ coincides with the Hilbert class field of k_0. To prove this, by Sase's argument in [14], it is enough to show that there is no fully ramified prime in $F/\mathbb{Q}$. The extension $F/\mathbb{Q}$ is unramified out side $2, 47$, and the primes dividing t and s. As we see in Section 5, the only primes satisfying $\left(\frac{-47}{p}\right) \equiv p \pmod 5$ possibly ramify in the splitting field over k_0. Therefore, in particular, we can ignore those primes not congruent to ± 1 modulo 5. Hence, we may and do assume that the possible ramifying prime p is neither 2 nor 47. If p ramifies totally in $F/\mathbb{Q}$, then it follows from [4, Proposition 6.2.1] that

$$B(b; X) \equiv (X + a)^5 \pmod p \tag{12}$$

for some $a \in \mathbb{Z}$. If p is a prime divisor of t, then we have

$$B(b; X) \equiv X^5 + 47rX^3 \pmod p.$$

This yields $p|r$. This contradicts to $(t, r) = 1$. Thus we may assume that p does not divides t. The remaining possibility of p is a prime divisor of s. Comparing the constant terms of (11) and (12), we must have

$$a^5 \equiv 2^5 \cdot 47^5 t^5 \pmod p.$$

If $a \equiv 2 \cdot 47t \pmod p$, then, by looking at the fourth-degree term, we have $2 \cdot 5 \cdot 47t \equiv -2^2 \cdot 47t \pmod p$. It follows $7t \equiv 0 \pmod p$. This is impossible by our assumption. If $a \not\equiv 2 \cdot 47t \pmod p$, then $p \equiv 1 \pmod 5$ must hold. Then we have $a \equiv 2 \cdot 47tv \pmod p$ for some element $v \in \mathbb{F}_p^\times$ of order 5. Comparing the fourth-degree term, we obtain $5u \equiv -2 \pmod p$. In particular, p cannot be 5. Using this relation, we derive a condition on p from other terms. From the degree-one term and the degree-two term, we have

$$5^3 t^2 r \equiv 2^6 \cdot 47t^4 \pmod p,$$
$$2 \cdot 3^2 \cdot 47t^3 \equiv -5^2 tr \pmod p,$$

respectively. Noticing that $(t, p) = 1$, we eliminate r in these congruences and get $2 \cdot 11 \cdot 47t^2 \equiv 0 \pmod p$. Therefore the only possible ramifying prime is 11. Using the degree three-term does not make any further restriction. Now let $p = 11$. Since $p|s$, we have $p|Y$ and also $b \equiv X \pmod p$. We consider the reduction $\tilde{E}$ of E modulo 11. The curve $\tilde{E}$ is singular and defined by

$$y^2 = (x + 4)(x + 7)^2$$

over $\mathbb{F}_p$. It follows from $y = 0$ that $b = x = 4$ or 7. But the points $P_1 \bmod p$ and $P_2 \bmod p$ do not fall on the singular point $(4, 0)$. Therefore no rational point $P \in E(\mathbb{Q})$ maps to $(4, 0)$ under the reduction map $E \longrightarrow \tilde{E}$ modulo 11. Thus we conclude $b \equiv 7 \pmod p$. In this case, $B(b; X)$ does not become a 5-th power of a linear factor modulo 11. Thus we conclude that there is no fully ramified prime in $F/\mathbb{Q}$. This completes the proof of the first half of the theorem.

Next we consider the reduction map modulo 2: $E \longrightarrow \tilde{E}$. Here $\tilde{E}$ is a singular curve over $\mathbb{F}_2$ defined by $y^2 = x^3$. There are two $\mathbb{F}_2$-rational points on the curve: $(0, 0)$ and $(1, 1)$. The former point is singular and the latter is non-singular. We can prove that if $(x, y) \in E(\mathbb{Q})$ maps to the singular point $(0, 0) \in \tilde{E}(\mathbb{F}_2)$, then $\mathrm{Bru}(1, b; X)$ is irreducible with $b = x/188$. In fact, if the assumption is satisfied, then $b = 0$ in $\mathbb{F}_2$. Then $\mathrm{Bru}(1, b; X)$ is congruent to $X^5 + X^2 + 1$, which is a irreducible polynomial

in $\mathbb{F}_2[X]$. This shows that $\mathrm{Bru}(1, b; X)$ is irreducible in $\mathbb{Q}[X]$. The rational points in $E(\mathbb{Q})$ reducing to the non-singular point $(1, 1)$ forms a subgroup E_0 in $E(\mathbb{Q})$. By a simple computation, the group E_0 is generated by $P_1 - 2P_2$ and $5P_2$. Thus it is of index 5 in $E(\mathbb{Q})$. Therefore there are infinitely many $P \in E(\mathbb{Q})$ which is not reduced to $(1, 1)$. This completes the proof of the theorem. □

We compute several b's satisfying the assumptions of the theorem. In the following, the triples (n_1, n_2, b) are listed where $P = n_1P_1 + n_2P_2$ $(0 \le n_1 \le 3, -3 \le n_2 \le 3)$ and $b = x(P)/188$:

$$(0, 2, -293/47), (0, 3, -61429/85849), (1, -3, 66390/121), (1, -1, -6), (1, 0, -1),$$
$$(1, 1, 41), (1, 2, 2220/1681), (2, -3, -67116/51529), (2, -2, 1135/47), (2, -1, 47/25),$$
$$(2, 0, -210/47), (2, 2, 2801442/323783), (2, 3, 18802504019/4449023401), (3, -3, -7947571/2007889),$$
$$(3, -2, -102024/38809), (3, 0, 153864/26569), (3, 1, -12424675/4566769),$$
$$(3, 2, -22382213557/5810250625), (3, 3, 304170202183950/109697574742921).$$

Note that $-P$ gives the same b as P, therefore we omit such triples.

References

[1] H. Anai, M. Noro, and K. Yokoyama, *Computation of the splitting fields and the Galois groups of polynomials*, Algorithms in algebraic geometry and applications (Santander, 1994), Birkhäuser, Basel, 1996, pp. 29–50.

[2] 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, Computational algebra and number theory (London, 1993).

[3] R. J. Chapman, *Automorphism polynomials in cyclic cubic extensions*, J. Number Theory **61** (1996), no. 2, 283–291.

[4] H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag, Berlin, 1993.

[5] ———, *Advanced topics in computational number theory*, Springer-Verlag, New York, 2000.

[6] K. Hashimoto and H. Tsunogai, *Generic polynomials over* **Q** *with two parameters for the transitive groups of degree five*, Proc. Japan Acad. Ser. A Math. Sci. **79** (2003), no. 9, 142–145.

[7] A. Hoshi and K. Miyake, *Tschirnhausen transformation of a cubic generic polynomial and a* 2*-dimensional involutive cremona transformation*, To appear in Proc. Japan Acad. Ser. A Math. Sci. (2007).

[8] C. U. Jensen, A. Ledet, and N. Yui, *Generic polynomials*, Mathematical Sciences Research Institute Publications, vol. 45, Cambridge University Press, Cambridge, 2002.

[9] M. Kida, *Kummer theory for norm algebraic tori*, J. Algebra **293** (2005), no. 2, 427–447.

[10] ———, *Cyclic polynomials arising from kummer theory of norm algebraic tori*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 102–113.

[11] T. Komatsu, *Generic sextic polynomial related to the subfield problem of a cubic polynomial*, Preprint (2006).

[12] M. Noro and T. Takeshima, *Risa/Asir – computer algebra system*, ISSAC '92: Papers from the international symposium on Symbolic and algebraic computation (New York, NY, USA), ACM Press, 1992, pp. 387–396.

[13] G. Renault, *Computation of the splitting field of a dihedral polynomial*, ISSAC '06: Proceedings of the 2006 international symposium on Symbolic and algebraic computation (New York, NY, USA), ACM Press, 2006, pp. 290–297.

[14] M. Sase, *On a family of quadratic fields whose class numbers are divisible by five*, Proc. Japan Acad. Ser. A Math. Sci. **74** (1998), no. 7, 120–123.

[15] B. M. Trager, *Algebraic factoring and rational function integration*, Proceedings of the 1976 ACM Symposium on Symbolic and Algebraic Computation, 1976, pp. 219–226.

Masanari Kida
Department of Mathematics
The University of Electro-Communications
Chofu, Tokyo 182-8585, Japan

E-mail: kida@sugaku.e-one.uec.ac.jp

Guénaël Renault
LIP6 – Équipe SPIRAL
Université Pierre et Marie Curie
4 place Jussieu
F-75252 Paris Cedex 05
France
E-mail: guenael.renault@lip6.fr

Kazuhiro Yokoyama
Department of Mathematics
Rikkyo University
Nishi-Ikebukuro, Tokyo 171-8501, Japan
E-mail: yokoyama@rkmath.rikkyo.ac.jp