A construction of an infinite family of dihedral quintic fields with unramified biquadratic extensions (Algebraic Number Theory and Related Topics 2018)

AUTHOR(S):

TSUNOGAI, Hiroshi

CITATION:

TSUNOGAI, Hiroshi. A construction of an infinite family of dihedral quintic fields with unramified biquadratic extensions (Algebraic Number Theory and Related Topics 2018). 数理解析研究所講究録別冊 2021, B86: 331-349

ISSUE DATE:

2021-07

URL:

http://hdl.handle.net/2433/265162

RIMS Kôkyûroku Bessatsu
B86 (2021), 331–349

A construction of an infinite family of dihedral quintic fields with unramified biquadratic extensions

By

Hiroshi TSUNOGAI*

Abstract

In this article, we give an infinite family of dihedral quintic fields with unramified biquadratic extensions by specializing a generic dihedral quintic polynomial to an explicit family of values of rational numbers.

§ 0. Introduction

In this article, we shall construct an infinite family of dihedral quintic fields having unramified biquadratic extensions by using a generic D_5-polynomial

$$f^{D_5}(a,b;X) := X^5 + (a-3)X^4 + (b-a+3)X^3 + (a^2-a-1-2b)X^2 + bX + a$$

over $\boldsymbol{Q}$ given by Brumer[2], Hashimoto[5], which was also reconstructed by Hashimoto and the author [6] with connection to cross-ratios.

The main result of this article is

Theorem A. *Let n, m be integers satisfying $n \geq 1$, $m \equiv 1 \pmod 8$ and $\dfrac{m}{2^{4n+2}} > \beta$ where $\beta = -1.3463\cdots$ is the unique real root of the cubic polynomial $-4b^3 + 32b^2 - 44b - 127$. Denote a root of $f(X) = f_{n,m}(X) := f^{D_5}(-1, \dfrac{m}{2^{4n+2}}; X)$, which is irreducible over $\boldsymbol{Q}$, by $\theta = \theta_{n,m}$ and the root field generated by θ by $K = K_{n,m} = \boldsymbol{Q}(\theta)$. We also put $L = L_{n,m} := K(\sqrt{\theta}, \sqrt{1-\theta})$.*

1. *The field K is a dihedral quintic field and the extension L/K is unramified.*

Received March 29, 2019. Revised July 3, 2019.
2020 Mathematics Subject Classification(s): 11R21,11R29,12E10
Key Words: *dihedral quintic fields, unramified extensions*
Supported by JSPS KAKENHI Grant Numbers JP22540032, JP26287006, JP18K03253.
*Department of Information and Communication Sciences, Faculty of Science and Technology, Sophia University, Kioi-cho, Chiyoda-ku, Tokyo, 102-8554 Japan.
e-mail: tsuno-h@sophia.ac.jp

2. *Moreover, when* $m \equiv 9 \pmod{16}$, L/K *is biquadratic.*

3. *For each fixed* n, *the family*

$$\{K_{n,m} \mid m \equiv 9 \,(\mathrm{mod}16), m > 0\}$$

is an infinite family of dihedral quintic fields having unramified biquadratic extensions.

For the dihedral quintic field $K = K_{n,m}$ in the theorem above, we also consider unramified extensions over the Galois closure $\widetilde{K} = \widetilde{K_{n,m}}$ of K over $\boldsymbol{Q}$. Since L/K is unramified, $\widetilde{L}/\widetilde{K}$ is also unramified, where $\widetilde{L} = \widetilde{L_{n,m}}$ denotes the Galois closure of L over $\boldsymbol{Q}$. Moreover we put $\widetilde{L}^{\sharp} := \widetilde{L}(\sqrt{-1})$.

Theorem B. *Let* n, m *be integers satisfying* $n \geq 1$, $m \equiv 9 \pmod{16}$ *and* $\dfrac{m}{2^{4n+2}} > \beta$. *Then* $\widetilde{L}^{\sharp}$ *is an unramified extension of* $\widetilde{K}$ *with Galois group isomorphic to* $(\boldsymbol{Z}/2\boldsymbol{Z})^5$. *In other words, the* 2*-rank of the ideal class group of* $\widetilde{K}$ *is at least five and the class number of* $\widetilde{K}$ *is divisible by* 32.

Moreover, for each fixed n, *the family*

$$\left\{ \widetilde{K}_{n,m} \,\middle|\, m \equiv 9 \,(\mathrm{mod}16), m > 0 \right\}$$

is an infinite family of number fields satisfying $\mathrm{Gal}(\widetilde{K}_{n,m}/\boldsymbol{Q}) \simeq D_5$ *and the* 2*-rank of the ideal class group of* $\widetilde{K}$ *is at least five.*

This study was inspired from Nakano's result [13] which gave an infinite family of cyclic quintic fields with even class number by specializing Lehmer's cyclic quintic polynomial [12]

$$f(T,X) = X^5 + T^2X^4 - 2(T^3 + 3T^2 + 5T + 5)X^3 + (T^4 + 5T^3 + 11T^2 + 15T + 5)X^2 + (T^3 + 4T^2 + 10T + 10)X + 1.$$

In fact, when for $t \in \boldsymbol{Q}$ we denote a root of $f(t,X) \in \boldsymbol{Q}[X]$ by θ_t and the root field of $f(t,X)$ by $K_t = \boldsymbol{Q}(\theta_t)$, he showed that $K_t(\sqrt{\theta_t(\theta_t - t - 1)})$ is an unramified quadratic extension over K_t for infinitely many values of $t \in \boldsymbol{Q}$ and that this family $K_t(\sqrt{\theta_t(\theta_t - t - 1)})/K_t$ includes infinitely many distinct cyclic quintic fields K_t.

On the other hand, various arithmetic properties of dihedral quintic fields obtained by specializing Brumer's polynomial $f^{D_5}(a,b;X)$ has been studied by many researchers (e.g. [1, 8, 9, 10, 11]). This study gives another application of Brumer's polynomial f^{D_5}.

The key property of f^{D_5} for our purpose is that, for each $a, b \in \boldsymbol{Q}$, if we denote a root of f^{D_5} by θ, both θ and $1 - \theta$ are simultaneously p-adic units for any prime

p with $v_p(a) = 0$ and $v_p(b) \geq 0$. Hashimoto and the author [6] reconstructed f^{D_5} with connection to cross-ratios, which explains this phenomenon well (see Section 1). Cross-ratios are rational functions on the moduli space $\mathcal{M}_{0,n}$ of projective lines with n marked points, which have their supports only on the boundary of $\mathcal{M}_{0,n}$. In this sense, cross-ratios may be regarded as "modular units in genus zero". From this point of view, it looks natural that cross-ratios are closely related with units of number fields, so is Brumer's polynomial f^{D_5}.

Acknowledgment. The author would like to appreciate the organizers of the workshop "Algebraic Number Theory and Related Topics 2018" for giving him this opportunity. This study started as a joint work with Yuichi Kato for his master's thesis [7] at Sophia University. The author thanks his eager cooperation including the observation of these phenomena using computers. This work was also supported by the Research Institute for Mathematical Sciences, a Joint Usage/Research Center located in Kyoto University.

§ 1. Review of construction of D_5-polnomials

We shall review a construction and some basic properties of a generic D_5-polynomial given by Brumer[2], Hashimoto[5] based on the manner of [6].

Let $x_1, \ldots, x_5$ be five indeterminates and $L := \boldsymbol{Q}(x_1, \ldots., x_5)$ be the rational function field over $\boldsymbol{Q}$ generated by them. The symmetric group $\mathfrak{S}_5$ of degree 5 acts on L via permutation of indices: $\sigma(x_i) := x_{\sigma(i)}$.

The projective general linear group $\mathrm{PGL}(2, \boldsymbol{Q})$ over $\boldsymbol{Q}$ acts on L via fractional linear transformation diagonally, commuting with the action of $\mathfrak{S}_5$. Define CR_5 to be the set of the cross-ratios of the indeterminates:

$$\mathrm{CR}_5 = \left\{ \frac{x_i - x_k}{x_i - x_l} \Big/ \frac{x_j - x_k}{x_j - x_l} \;\middle|\; i, j, k, l \text{ are all distinct} \right\}.$$

Then the fixed field $L^{\mathrm{PGL}(2,\boldsymbol{Q})}$ is generated by CR_5. In particular, $L^{\mathrm{PGL}(2,\boldsymbol{Q})} = \boldsymbol{Q}(x, y)$, which is purely transcendental over $\boldsymbol{Q}$ of degree two, where we put

$$\begin{cases} x = \dfrac{x_3 - x_1}{x_3 - x_5} \Big/ \dfrac{x_4 - x_1}{x_4 - x_5}, \\ y = \dfrac{x_2 - x_1}{x_2 - x_5} \Big/ \dfrac{x_3 - x_1}{x_3 - x_5}. \end{cases}$$

In fact, $L^{\mathrm{PGL}(2,\boldsymbol{Q})}$ is the function field of the moduli space $\mathcal{M}_{0,5}$ of projective lines with ordered five marked points, and the class of $(x_1, \ldots, x_5)$ modulo $\mathrm{PGL}(2, \boldsymbol{Q})$ is uniquely represented by $(0, xy, x, 1, \infty)$.

Let X be the set of the injective mappings from $\{1, 2, 3, 4\}$ to $\{1, 2, 3, 4, 5\}$. Then on X act $\mathfrak{S}_4$ from the right and $\mathfrak{S}_5$ from the left naturally. The mapping $\mathrm{cr} : X \longrightarrow \mathrm{CR}_5$

defined by $\mathrm{cr}(\tau) := \dfrac{x_{\tau(1)}-x_{\tau(3)}}{x_{\tau(1)}-x_{\tau(4)}}\Big/\dfrac{x_{\tau(2)}-x_{\tau(3)}}{x_{\tau(2)}-x_{\tau(4)}}$ induced the bijection $\overline{\mathrm{cr}} : X/V_4 \xrightarrow{\sim} \mathrm{CR}_5$ which commutes with the left action of $\mathfrak{S}_5$, where $V_4 = \langle (1\ 2)(3\ 4), (1\ 3)(2\ 4)\rangle$ is Klein's four group in $\mathfrak{S}_4$. Since $\mathfrak{S}_4$ decomposes into the semi-direct product of V_4 by $\mathfrak{S}_3$, $\mathfrak{S}_3$ acts on CR_5 from the right via $\overline{\mathrm{cr}}$, where the orbit of an element $\theta \in \mathrm{CR}_5$ by $\mathfrak{S}_3$ is $\{\theta_i | i = 0, \ldots, 5\}$ with

$$\theta_0 := \theta, \quad \theta_1 := 1-\theta, \quad \theta_2 := \frac{1}{\theta}, \tag{1.1}$$
$$\theta_3 := 1-\frac{1}{\theta} = \frac{\theta-1}{\theta}, \quad \theta_4 := \frac{1}{1-\theta}, \quad \theta_5 := 1-\frac{1}{1-\theta} = \frac{\theta}{\theta-1}.$$

Let D_5 be the subgroup of $\mathfrak{S}_5$ generated by $\alpha = (1\ 2\ 3\ 4\ 5)$ and $\beta = (1\ 3)(4\ 5)$, which is a dihedral group of degree 5 and is the stabilizer of a necklace permutation $(1, 2, 3, 4, 5)$. We consider the D_5-orbits in CR_5.

The action of D_5 on $\boldsymbol{Q}(x, y)$ is described as

$$\alpha : \begin{cases} x \longmapsto 1-xy \\ y \longmapsto \dfrac{1-y}{1-xy}, \end{cases} \qquad \beta : \begin{cases} x \longmapsto x \\ y \longmapsto \dfrac{1-y}{1-xy}. \end{cases}$$

Let $S = \mathrm{Orb}_{D_5}(x)$ be the D_5-orbit of x. Then we have

$$S = \left\{ x, 1-xy, y, \frac{1-y}{1-xy}, \frac{1-x}{1-xy} \right\}.$$

We also notice that for any $\theta \in S$, it holds that

$$1-\theta = \alpha(\theta)\alpha^{-1}(\theta). \tag{1.2}$$

Let

$$f(X) := \prod_{u \in S}(X-u) =: X^5 + c_4X^4 + c_3X^3 + c_2X^2 + c_1X + c_0 \in K^{D_5}[X],$$

and put $a := c_0, b := c_1$. Then we have the following[1]:

Theorem 1.1 ([6] Theorem 1)**.**

1. *The fixed field K^{D_5} of D_5 is rational and coincides with $\boldsymbol{Q}(a, b)$.*
2. *(reconstruction of Brumer[2], Hashimoto[5]) The polynomial*

$$f^{D_5}(a, b; X) := X^5 + (a-3)X^4 + (b-a+3)X^3 + (a^2-a-1-2b)X^2 + bX + a \tag{1.3}$$

is a generic polynomial for D_5 over $\boldsymbol{Q}$.

[1]Errata of [6]. Theorem 1(1): As seen in (1.3), $c_3 = b - a + 3$ is correct. Theorem 5(1): $v = ((2a^5 + 18a^4 - 140a^3 + 13a^2 - 2a) - (4a^3 + 20a^2 + 6a)b - \boldsymbol{(a^2 + 1)}b^2)/a^3$ is correct.

The discriminant $D(a,b)$ of f^{D_5} is a square since D_5 is an even subgroup of $\mathfrak{S}_5$. In fact, we have $D(a,b) = a^2 D_0(a,b)^2$, where

$$D_0(a,b) = -4b^3 + (a^2 - 30a + 1)b^2 + 2a(12a^2 - 17a - 7)b - a(4a^4 - 4a^3 - 40a^2 + 91a - 4). \tag{1.4}$$

Remark 1. The relation (1.2) characterizes the dihedral quintic polynomial (1.3). In fact, if a sequence $\boldsymbol{w} = (w^{(i)})_{i\in\boldsymbol{Z}}$ satisfies the relation $1 - w^{(i)} = w^{(i-1)}w^{(i+1)}$ for all $i \in \boldsymbol{Z}$, then $\boldsymbol{w}$ is periodic with period five (See e.g. Kihel[9][2]). Moreover, the group of the permutations of the set $\left\{w^{(i)}\middle| i = 0,1,2,3,4\right\}$ preserving the relations $1 - w^{(i)} = w^{(i-1)}w^{(i+1)}$ coincides with D_5.

Remark 2. Similarly to the minimal polynomial $f^{D_5}(a,b;X)$ of $\theta = \theta_0$, the minimal polynomials $f_i^{D_5}(a,b;X)$ of θ_i $(i = 1,\dots,5)$ presented in (1.1) are written in a concise form in terms of a, b:

$$\begin{aligned}
f_1^{D_5}(a,b;X) &= -f^{D_5}(a,b;1-X)\\
&= X^5 - (a+2)X^4 + (3a+b+1)X^3\\
&\qquad - (a^2+2a+b)X^2 + a(2a-1)X - a^2,\\
f_2^{D_5}(a,b;X) &= -X^5 f^{D_5}(a,b;1/X)\\
&= -aX^5 - bX^4 - (a^2 - a - 2b - 1)X^3\\
&\qquad + (a - b - 3)X^2 - (a-3)X - 1,\\
f_3^{D_5}(a,b;X) &= (1-X)^5 f^{D_5}(a,b;1/(1-X))\\
&= -aX^5 + (5a+b)X^4 - (a^2 + 9a + 2b - 1)X^3\\
&\qquad + (3a^2 + 6a + b)X^2 - a(3a+1)X + a^2,\\
f_4^{D_5}(a,b;X) &= X^5 f^{D_5}(a,b;(X-1)/X)\\
&= a^2X^5 - a(2a-1)X^4 + (a^2 + 2a + b)X^3\\
&\qquad - (3a + b + 1)X^2 + (a+2)X - 1,\\
f_5^{D_5}(a,b;X) &= (X-1)^5 f^{D_5}(a,b;X/(X-1))\\
&= a^2X^5 - a(3a+1)X^4 + (3a^2 + 6a + b)X^3\\
&\qquad - (a^2 + 9a + 2b - 1)X^2 + (5a+b)X - a.
\end{aligned}$$

This may give an explanation why both θ and $1-\theta$ behave well for our purpose.

For later use, we consider the unique quadratic subfield $\boldsymbol{Q}(x,y)^{C_5}$ of $\boldsymbol{Q}(x,y)/\boldsymbol{Q}(a,b)$, where $C_5 = \langle\alpha = (1\ 2\ 3\ 4\ 5)\rangle$ is the unique cyclic subgroup of order 5 of D_5 (see [6,

[2]In [9], it is written that this result is due to an unpublished note by H. Darmon. The polynomial $p(x)$ presented in p.471 *loc. cit.* coincides with $-f^{D_5}(S+3, T+2S+5; -x)$.

§4]). Let

$$c := \prod_{i \in \boldsymbol{Z}/5\boldsymbol{Z}} (\alpha^i(x) - \alpha^{i+1}(x)) = \prod_{u \in S} (u - \alpha(u)).$$

Then, we have $\alpha(c) = c, \beta(c) = -c$, from which follows $K^{C_5} = K^{D_5}(c) = \boldsymbol{Q}(a, b, c)$ and $c^2 \in \boldsymbol{Q}(a, b)$. By writing c^2, a, b in terms of x, y explicitly, we have $c^2 = D_0(a, b)$. (This shows that the choice of the signature of $D_0(a, b)$ in (1.4) is meaningful.) We can also consider

$$c' := \prod_{i \in \boldsymbol{Z}/5\boldsymbol{Z}} (\alpha^i(x) - \alpha^{i+2}(x)) = \prod_{u \in S} (u - \alpha^2(u))$$

instead of c. In fact, we have $c' = -ac$ and $D(a, b) = (cc')^2$.

§ 2. Unramifiedness at Archimedean places

From now on, we consider a specialization

$$f(b; X) := f^{D_5}(-1, b; X) = X^5 - 4X^4 + (b + 4)X^3 - (2b - 1)X^2 + bX - 1$$

of our D_5-polynomial $f^{D_5}(a, b; X)$ at $a = -1$ so that the norm of a root of f is 1. The polynomials appearing in Remark 2 are also specialized as

(2.1)

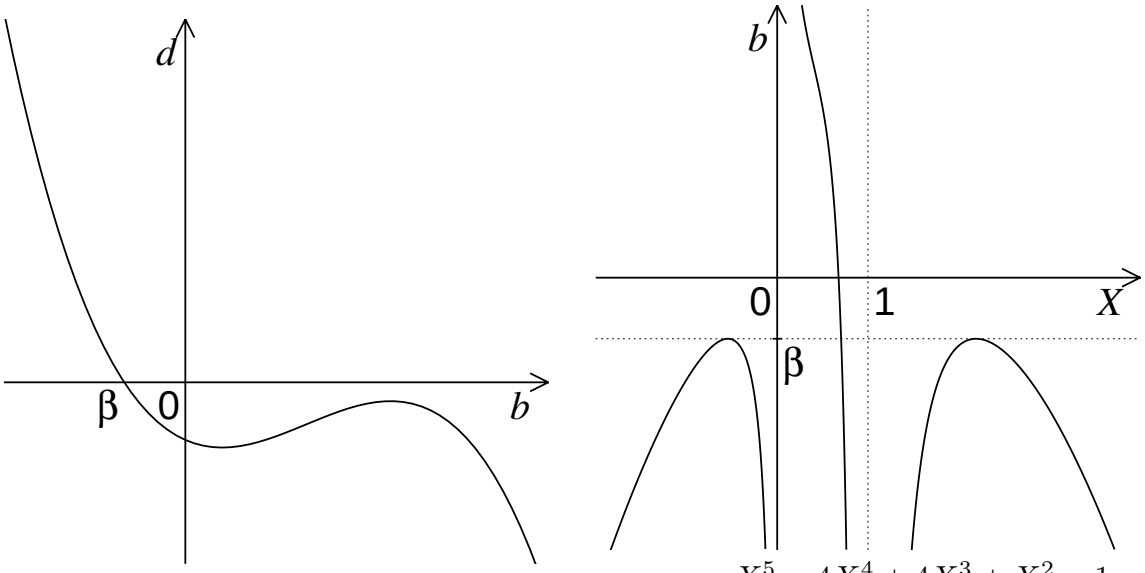
$$\begin{aligned}
f_1(b; X) &:= f_1^{D_5}(-1, b; X) = X^5 - X^4 + (b - 2)X^3 - (b - 1)X^2 + 3X - 1,\\
f_2(b; X) &:= f_2^{D_5}(-1, b; X) = X^5 - bX^4 + (2b - 1)X^3 - (b + 4)X^2 + 4X - 1,\\
f_3(b; X) &:= f_3^{D_5}(-1, b; X) = X^5 + (b - 5)X^4 - (2b - 9)X^3 + (b - 3)X^2 - 2X + 1,\\
f_4(b; X) &:= f_4^{D_5}(-1, b; X) = X^5 - 3X^4 + (b - 1)X^3 - (b - 2)X^2 + X - 1,\\
f_5(b; X) &:= f_5^{D_5}(-1, b; X) = X^5 - 2X^4 + (b - 3)X^3 - (2b - 9)X^2 + (b - 5)X + 1.
\end{aligned}$$

The discriminant of $f(b; X)$ is $D_0(b)^2$, where

$$D_0(b) := D_0(-1, b) = -4b^3 + 32b^2 - 44b - 127. \tag{2.2}$$

The polynomial $D_0(b)$ has the unique real root $\beta = -1.3463\cdots$ and $D_0(b) < 0$ if and only if $b > \beta$ (see Figure 1(i)). For $b \in \boldsymbol{Q}$ we denote a root field of $f(b; X)$ over $\boldsymbol{Q}$ by $K = K_b$, and the splitting field by $\widetilde{K} = \widetilde{K}_b$. If $\widetilde{K}$ is a D_5-extension of $\boldsymbol{Q}$, $\widetilde{K}$ includes the unique quadratic subfield $F = F_b = \boldsymbol{Q}(\sqrt{D_0(b)})$.

Proposition 2.1. *When $b > \beta$, the polynomial $f(b; X)$ has only one real root θ with $0 < \theta < 1$ and two pair of conjugate complex roots. When $b < \beta$, $f(b; X)$ has five real roots, one of which is between 0 and 1, two are greater than 1, and the other two are negative.*



(i) $d = -4b^3 + 32b^2 - 44b - 127$ (ii) $b = -\dfrac{X^5 - 4X^4 + 4X^3 + X^2 - 1}{X(X-1)^2}$

Figure 1. The graphs of (i) $d = D_0(b)$ and (ii) $f(b; X) = 0$

Proof. By solving the equation $f(b; X) = X^5 - 4X^4 + (b+4)X^3 - (2b-1)X^2 + bX - 1 = 0$ in b, we have

$$b = -\frac{X^5 - 4X^4 + 4X^3 + X^2 - 1}{X(X-1)^2}.$$

We obtain the result by figuring the graph on (x, b)-plain (see Figure 1(ii)). While direct calculation shows the threshold value is β, we also obtain the result in the following argument. Since $f(b; X)$ is a D_5-polynomial, the complex conjugate in $\mathrm{Gal}(\widetilde{K}/\boldsymbol{Q})$ is a product of an even number of disjoint transpositions, hence it is trivial (K is totally real) or a product of two disjoint transpositions. Since K is totally real if and only if $F = \boldsymbol{Q}(\sqrt{D_0(b)})$ is real, we conclude the result. □

Corollary 2.2. *Assume $b \in \boldsymbol{Q}$, $b > \beta$ and $f(b; X)$ is irreducible over $\boldsymbol{Q}$. Let $\theta = \theta_b$ be a root of $f(b; X)$, and denote $K = K_b = \boldsymbol{Q}(\theta_b)$. Then the extention $L = K(\sqrt{\theta}, \sqrt{1-\theta})$ over K is unramified at all Archimedean places of K.*

Remark 3. If $b < \beta$, in any quadratic subextension in L/K, some Archimedean place of K ramifies.

§ 3. Unramifiedness at Non-Archimedean places

Let n, m be integers satisfying the following assumption

$$n \geq 1, \quad m \equiv 1 \pmod 8 \quad \text{and} \quad \frac{m}{2^{4n+2}} > \beta. \tag{3.1}$$

For convinience, we also put $N = 2^{2n+1}$. We consider the polynomial

$$f(X) = f_{n,m}(X) := f(\frac{m}{2^{4n+2}}; X) = f(N^{-2}m; X) \tag{3.2}$$
$$= X^5 - 4X^4 + N^{-2}(m + 4N^2)X^3 - N^{-2}(2m - N^2)X^2 + N^{-2}mX - 1 \in \boldsymbol{Q}[X].$$

§ 3.1. The valuations of the roots of f

First we observe the valuations of the roots of f. For any odd prime p, all roots of f are p-adic units since f lies in $\boldsymbol{Z}_p[X]$ and is monic with constant term -1. On 2-adic valuations, by considering the 2-adic Newton polygon of f (Figure 2), we have

Proposition 3.1. *The 2-adic valuations of five roots of f are $4n+2, 0, 0, -2n-1, -2n-1$, where the valuation is normalized as $v(2) = 1$.*

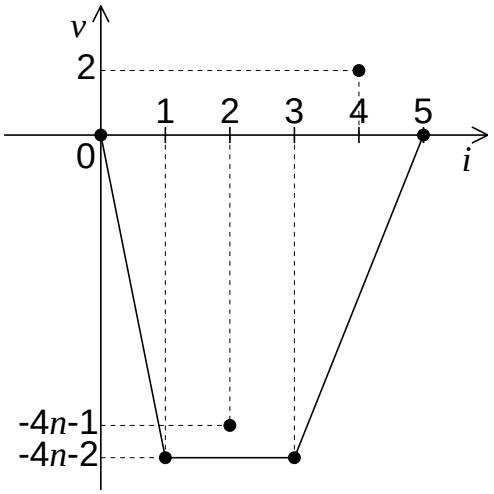


Figure 2. The 2-adic Newton polygon of $f_{n,m}(X)$

To make the coefficients to be integral, we use also

$$F(Z) := N^5 f(N^{-2}m; N^{-1}Z) \tag{3.3}$$
$$= Z^5 - 4NZ^4 + (m + 4N^2)Z^3 - N(2m - N^2)Z^2 + N^2mZ - N^5 \in \boldsymbol{Z}[Z].$$

Proposition 3.2. *Under the assumption* (3.1) *on n and m,*

1. *$f(X) = f_{n,m}(X)$ is irreducible over $\boldsymbol{Q}$. Hence K is a quintic field.*
2. *Moreover K is a dihedral quintic field, that is,* $\mathrm{Gal}(\widetilde{K}/\boldsymbol{Q}) \simeq D_5$.

Proof. (1) Since $f(b;X)$ is a D_5-polynomial over $\boldsymbol{Q}(b)$, f cannot have a cubic irreducible factor. Hence it suffices to show that f has no rational roots for proving the irreducibility of f over $\boldsymbol{Q}$.

Suppose that θ is a rational root of $f(X) = f_{n,m}(X)$. Since θ is a p-adic unit for any odd prime p, and the 2-adic valuation $v_2(\theta)$ is one of $4n+2, 0$ or $-2n-1$, all possible values of θ are $\pm 2^{4n+2}, \pm 1$ and $\pm 2^{-2n-1}$. On the other hand, θ is the unique real root of f, which lies in the range $0 < \theta < 1$. Hence θ must be 2^{-2n-1}, which is impossible because

$$\begin{aligned} N^5 f(N^{-2}m; 2^{-2n-1}) &= F(1) \\ &= 1 - 4N + (m + 4N^2) - N(2m - N^2) + mN^2 - N^5 \\ &\equiv 1 + m \equiv 2 \not\equiv 0 \pmod 8. \end{aligned}$$

Here we use $8|N$.

(2) It suffices to show that $\widetilde{K}/\boldsymbol{Q}$ does not degenerate into a cyclic quintic extension. Since

$$\begin{aligned} (2^{-1}N^3)^2 \cdot D_0(N^{-2}m) &= (2^{-1}N^3)^2(-4N^{-6}m^3 + 32N^{-4}m^2 - 44N^{-2}m - 127) \\ &= -m^3 + 8m^2N^2 - 11mN^4 - 127 \cdot 2^{12n+4} \\ &\equiv -1 \pmod 8, \end{aligned}$$

$D_0(N^{-2}m)$ is not a square in $\boldsymbol{Q}$. From this the assertion holds. □

Remark 4. We can also deduce (2) by investigating the rational points of the elliptic curve $E : c^2 = -4b^3 + 32b^2 - 44b - 127$. Changing variables by $b = -x + 3, c = 2y + 1$, we can see that E is isomorphic to $E' : y^2 + y = x^3 - x^2 - 10x - 20$ over $\boldsymbol{Q}$, which is the elliptic curve labeled `11a1` in Cremona's table [3]. From this table we know $E'(\boldsymbol{Q}) = \langle(5,5)\rangle = \{(5,5), (16,-61), (16,60), (5,-6)), O\} \simeq \boldsymbol{Z}/5\boldsymbol{Z}$, hence $E(\boldsymbol{Q}) = \langle(-2,11)\rangle = \{(-2,\pm 11), (-13,\pm 121), O\}$. But neither $b = -2$ nor -13 is the case.

Denote a root of $f_{n,m}(X)$, which is irreducible over $\boldsymbol{Q}$, by $\theta = \theta_{n,m}$ and the root field generated by $\theta_{n,m}$ by $K = K_{n,m} = \boldsymbol{Q}(\theta_{n,m})$. In the previous section, we have already seen that the extention $L = K(\sqrt{\theta}, \sqrt{1-\theta})$ over K is unramified at all Archimedean places of K.

§ 3.2. Unramifiedness at odd primes

As already seen, for any odd prime p, θ is a p-adic unit. Moreover, considering $f_1(X) = -f(1-X)$, we can see also that $1-\theta$ is a p-adic unit. Therefore, the extention $L = K(\sqrt{\theta}, \sqrt{1-\theta})$ over K is unramified at all places above p.

§ 3.3. Unramifiedness at 2

For extensions of local fields, it is known that if two polynomials are p-adically near enough their root fields and their splitting fields coincide with each other. Here we need to know that in our case what precision is enough to determine the root field and the prime decomposition in it. For this purpose we prepare the following lemma:

Lemma 3.3. *Let $F(X) = X^2 - cX + d \in \boldsymbol{Z}_2[X]$ be a monic quadratic polynomial with $c, d \in \boldsymbol{Z}_2, c \equiv 0 \pmod 8, d \equiv 1 \pmod 8$. Denote a root of F by Θ.*

1. *Then F is irreducible over $\boldsymbol{Q}_2$ and the root field $k = \boldsymbol{Q}_2(\Theta)$ of F over $\boldsymbol{Q}_2$ is $\boldsymbol{Q}_2(\sqrt{-1})$.*
2. *Moreover put $G(Y) := 4F(2^{-1}Y^2) = Y^4 - 2cY^2 + 4d \in \boldsymbol{Z}_2[Y]$. Then the root field $k(\sqrt{2\Theta})$ of G over $\boldsymbol{Q}_2$ is $\boldsymbol{Q}_2(\sqrt{-1})$ (resp. $\boldsymbol{Q}_2(\sqrt{-1}, \sqrt{5})$) if $d \equiv 1$(resp. 9) $\pmod{16}$. In particular, $k(\sqrt{2\Theta})/k$ is unramified.*

Proof. (1) It follows since

$$F(X) = X^2 - cX + d = \left(X - \frac{c}{2}\right)^2 - \left(\frac{c^2}{4} - d\right)$$

and $\dfrac{c^2}{4} - d \equiv -1 \pmod 8$. (2) Since $d \equiv 1 \pmod 8$, d is a square in $\boldsymbol{Z}_2$, hence we can put $d = u^2$, where we choose the signature of u to be $u \equiv 1 \pmod 4$. Then a root $\sqrt{2\Theta}$ of $G(Y) = Y^4 - 2cY^2 + 4u^2 \in \boldsymbol{Z}_2[Y]$ is of the form $\pm\sqrt{c+u} \pm \sqrt{c-u}$, where we note that $\sqrt{c+u}\sqrt{c-u} = \sqrt{c^2-u^2} = \sqrt{c^2-d} \in \boldsymbol{Q}_2(\sqrt{-1})$. Hence

$$k(\sqrt{2\Theta}) = \boldsymbol{Q}_2(\sqrt{-1}, \sqrt{c+u}) = \begin{cases} \boldsymbol{Q}_2(\sqrt{-1}) & (d \equiv 1 \pmod{16}) \\ \boldsymbol{Q}_2(\sqrt{-1}, \sqrt{5}) & (d \equiv 9 \pmod{16}), \end{cases}$$

since $u \equiv 1$(resp. 5) $\pmod 8$ when $d \equiv 1$(resp. 9) $\pmod{16}$. The last assertion holds since $\boldsymbol{Q}_2(\sqrt{-1}, \sqrt{5})$ is the unique unramified quadratic extension of $\boldsymbol{Q}_2(\sqrt{-1})$. □

Now we are ready to prove the first two assertion of Theorem A, for which it is enough to show the following proposition:

Proposition 3.4. *Let n, m be integers satisfying $n \geq 1$, $n \equiv 2 \pmod 4$ and $m \equiv 1 \pmod 8$. Then the factorization of $f(X) = f_{n,m}(X)$ into irreducible factors over $\boldsymbol{Q}_2$ is*

$$f(X) = g_0(X)g_1(X)g_2(X), \tag{3.4}$$

where g_0 is of degree 1 and the 2-adic valuation of its root is $4n+2$, g_1 is of degree 2 and the 2-adic valuation of its roots are 0, and g_2 is of degree 2 and the 2-adic valuation

of its root is $-2n-1$. *Moreover, if we denote the prime ideal dividing* 2 *corresponding to* g_i *by* $\mathfrak{p}_i$, *the prime decomposition of* 2 *in* K *is*

$$2\mathcal{O}_K = \mathfrak{p}_0\mathfrak{p}_1^2\mathfrak{p}_2^2, \tag{3.5}$$

and

1. *the completion* $K_{\mathfrak{p}_0}$ *of* K *at* $\mathfrak{p}_0$ *is* $\boldsymbol{Q}_2$, *and* $\mathfrak{p}_0$ *splits in both* $K(\sqrt{\theta})/K$ *and* $K(\sqrt{1-\theta})/K$ *(hence splits completely in* L/K*).*
2. *the completion* $K_{\mathfrak{p}_1}$ *of* K *at* $\mathfrak{p}_1$ *is* $\boldsymbol{Q}_2(\sqrt{-1})$, *and* $\mathfrak{p}_1$ *is unramified in both* $K(\sqrt{1-\theta})/K$ *and* $K(\sqrt{\dfrac{\theta}{1-\theta}})/K$ *(hence also in* L/K*). In these two extension,* $\mathfrak{p}_1$ *splits if* $m \equiv 1 \pmod{16}$, *is inert if* $m \equiv 9 \pmod{16}$.
3. *the completion* $K_{\mathfrak{p}_2}$ *of* K *at* $\mathfrak{p}_2$ *is* $\boldsymbol{Q}_2(\sqrt{-1})$, *and* $\mathfrak{p}_2$ *is unramified in both* $K(\sqrt{\theta})/K$ *and* $K(\sqrt{1-\theta})/K$ *(hence also in* L/K*). In these two extension,* $\mathfrak{p}_1$ *splits if* $m \equiv 1 \pmod{16}$, *is inert if* $m \equiv 9 \pmod{16}$.

Compiling these, we deduce that any prime ideal of K *dividing* 2 *is unramified in* L/K. *In particular, when* $m \equiv 9 \pmod{16}$, L/K *is a biquadratic extension.*

Proof. The factorization (3.4) of f comes from the argument on the Newton polygon of f except the irreducibility of g_1 and g_2.

For the root θ with 2-adic valuation $v_2(\theta) = 4n+2$ (i.e. for the factor g_0), we can apply Hensel's Lemma directly for the integralized polynomial F for f, presented in (3.3), to show that $\theta \equiv 2^{4n+2} \pmod{2^{4n+5}}$. This implies that both θ and $1-\theta$ are square in $\boldsymbol{Q}_2$. Here, for parallel treatise as other factors g_1 and g_2, we prefer to give an explanation using the polynomials f_2 and f_3, presented in (2.1), which have $\theta_2 = \dfrac{1}{\theta}$ and $\theta_3 = \dfrac{\theta-1}{\theta}$ as one of their roots respectively. Consider the integralized polynomial

$$\begin{aligned} F_2(Z) &:= N^{10} f_2(N^{-2}m; N^{-2}Z) \\ &= Z^5 - mZ^4 + N^2(2m - N^2)Z^3 - N^4(m + 4N^2)Z^2 + 4N^8 Z - N^{10} \end{aligned}$$

for f_2, which has $N^2\theta_2 = N^2\dfrac{1}{\theta}$ as the unique unit root. Applying Hensel's Lemma to the congruence

$$F_2(Z) \equiv Z^5 - mZ^4 \equiv Z^4(Z-m) \pmod{N},$$

we obtain $N^2\theta_2 \equiv m \pmod{N}$. Since $8|N$, we have $N^2\theta_2 \equiv 1 \pmod{8}$, which shows that $N^2\theta_2$ (and hence θ) is a square in $\boldsymbol{Q}_2$. Similarly, considering the integralized polynomial

$$\begin{aligned} F_3(Z) &:= N^{10} f_3(N^{-2}m; N^{-2}Z) \\ &= Z^5 + (m - 5N^2)Z^4 - N^2(2m - 9N^2)Z^3 + N^4(m - 3N^2)Z^2 - 2N^8 Z + N^{10} \end{aligned}$$

for f_3, and applying Hensel's Lemma to the congruence

$$F_3(Z) \equiv Z^5 + mZ^4 \equiv Z^4(Z+m) \pmod{N},$$

we also obtain $N^2\theta_3 \equiv -m \pmod{N}$. Since $N^2\dfrac{1-\theta}{\theta} = -N^2\theta_3 \equiv 1 \pmod{8}$, $\dfrac{1-\theta}{\theta}$ is a square in $\boldsymbol{Q}_2$. Thus the local extension $\boldsymbol{Q}_2(\sqrt{\theta}, \sqrt{1-\theta})/\boldsymbol{Q}_2$ is trivial, i.e., the corresponding prime ideal $\mathfrak{p}_0$ in K lying above 2 decomposes completely in the extension $L = K(\sqrt{\theta}, \sqrt{1-\theta})/K$. In particular, $\mathfrak{p}_0$ is unramified in L/K.

Next we consider the quadratic factor g_1 of f whose roots are 2-adic units. Here we use the polynomials f_4 and f_5, presented in (2.1), which have $\theta_4 = \dfrac{1}{1-\theta}$ and $\theta_5 = \dfrac{\theta}{\theta-1}$ as one of their roots respectively. Consider the integralized polynomial

$$\begin{aligned} F_4(Z) &:= N^5 f_4(N^{-2}m; N^{-1}Z) \\ &= Z^5 - 3NZ^4 + (m-N^2)Z^3 - N(m-2N^2)Z^2 + N^4Z - N^5 \end{aligned}$$

for f_4, which has $N\theta_4 = N\dfrac{1}{1-\theta}$ as a unit root. Applying Hensel's Lemma to the congruence

$$F_4(Z) \equiv Z^5 - NZ^4 + mZ^3 - NmZ^2 \equiv Z^2(Z-N)(Z^2+m) \pmod{2N},$$

we know that $N\theta_4 = 2^{2n}\dfrac{2}{1-\theta}$ is a root of a monic quadratic factor of F_4 congruent to $Z^2 + m \pmod{2N}$. Since $16|2N$, we can apply Lemma 3.3 for this factor. Then first we have $\boldsymbol{Q}_2(1-\theta) = \boldsymbol{Q}_2(N\theta_4) = \boldsymbol{Q}_2(\sqrt{-1})$, which shows that the factor g_1 is irreducible over $\boldsymbol{Q}_2$. Denote the corresponding prime factor of $2\mathcal{O}_K$ by $\mathfrak{p}_1$. Then, since the localization $K_{\mathfrak{p}_1}$ of K at $\mathfrak{p}_1$ is $\boldsymbol{Q}_2(\sqrt{-1})$, $\mathfrak{p}_1$ is a prime ideal of degree one and ramifies in $K/\boldsymbol{Q}$. Moreover, in $K(\sqrt{1-\theta}) = K(\sqrt{2N\theta_4})/K$, $\mathfrak{p}_1$ splits when $m \equiv 1 \pmod{16}$, and is inert when $m \equiv 9 \pmod{16}$. This also shows that $K(\sqrt{1-\theta})/K$ is a quadratic extension when $m \equiv 9 \pmod{16}$. Similarly, next consider the integralized polynomial

$$\begin{aligned} F_5(Z) &:= N^5 f_5(N^{-2}m; N^{-1}Z) \\ &= Z^5 - 2NZ^4 + (m-3N^2)Z^3 - N(2m-9N^2)Z^2 + N^2(m-5N^2)Z + N^5 \end{aligned}$$

for f_5, which has $N\theta_5 = N\dfrac{\theta}{\theta-1}$ as a unit root. The congruence

$$F_5(Z) \equiv Z^5 + mZ^3 \equiv Z^3(Z^2+m) \pmod{2N}$$

shows that $N\theta_5 = N\dfrac{\theta}{\theta-1}$ is a root of a monic quadratic factor of F_5 congruent to $Z^2 + m \pmod{2N}$. Again, from Lemma 3.3, we have $\boldsymbol{Q}_2(\sqrt{\dfrac{\theta}{1-\theta}}) = \boldsymbol{Q}_2(\theta, \sqrt{\dfrac{\theta}{\theta-1}}) =$

$\boldsymbol{Q}_2(\sqrt{-1}, \sqrt{2N\theta_5})$ coincides with $\boldsymbol{Q}_2(\sqrt{-1})$ (resp. $\boldsymbol{Q}_2(\sqrt{-1}, \sqrt{5})$) when $m \equiv 1$ (resp. 9) (mod 16). Hence in $K(\sqrt{\dfrac{\theta}{1-\theta}})/K$, $\mathfrak{p}_1$ splits when $m \equiv 1 \pmod{16}$, and is inert when $m \equiv 9 \pmod{16}$. This also shows that $K(\sqrt{\dfrac{\theta}{1-\theta}})/K$ is a quadratic extension when $m \equiv 9 \pmod{16}$.

Thirdly, we consider the quadratic factor g_2 of f whose roots θ are of 2-adic valuation $v_2(\theta) = -2n-1$. Here we use the polynomials f itself and f_1 in (2.1), which have θ and $\theta_1 = 1-\theta$ as one of their roots respectively. Consider the integralized polynomial

$$\begin{aligned} F(Z) &= N^5 f(N^{-2}m; N^{-1}Z) \\ &= Z^5 - 4NZ^4 + (m+4N^2)Z^3 - N(2m-N^2)Z^2 + N^2mZ - N^5 \in \boldsymbol{Z}[Z] \end{aligned}$$

for f, presented already in (3.3), which has $N\theta$ as a unit root. Applying Hensel's Lemma to the congruence

$$F(Z) \equiv Z^5 + mZ^3 \equiv Z^3(Z^2+m) \pmod{2N},$$

we know that $N\theta$ is a root of a monic quadratic factor of F congruent to Z^2+m (mod $2N$). Hence again we can apply Lemma 3.3 for this factor. Then first we have $\boldsymbol{Q}_2(\theta) = \boldsymbol{Q}_2(N\theta) = \boldsymbol{Q}_2(\sqrt{-1})$, which shows that also the factor g_2 is irreducible over $\boldsymbol{Q}_2$. Denote the corresponding prime factor of $2\mathcal{O}_K$ by $\mathfrak{p}_2$. Then, since the localization $K_{\mathfrak{p}_2}$ of K at $\mathfrak{p}_2$ is $\boldsymbol{Q}_2(\sqrt{-1})$, $\mathfrak{p}_2$ is a prime ideal of degree one and ramifies in $K/\boldsymbol{Q}$. Moreover, in $K(\sqrt{\theta}) = K(\sqrt{2N\theta})/K$, $\mathfrak{p}_2$ splits when $m \equiv 1 \pmod{16}$, and is inert when $m \equiv 9 \pmod{16}$. This also shows that $K(\sqrt{\theta})/K$ is a quadratic extension when $m \equiv 9 \pmod{16}$. Now, when $m \equiv 9 \pmod{16}$, we know all of the extensions $K(\sqrt{\theta}), K(\sqrt{1-\theta}), K(\sqrt{\dfrac{\theta}{1-\theta}})$ are quadratic over K, hence $K(\sqrt{\theta}, \sqrt{1-\theta})$ is a biquadratic extension over K. Finally, consider the integralized polynomial

$$\begin{aligned} F_1(Z) &:= N^5 f_1(N^{-2}m; N^{-1}Z) \\ &= Z^5 - NZ^4 + (m-2N^2)Z^3 - N(m-N^2)Z^2 + 3N^4Z - N^5 \end{aligned}$$

for f_1, which has $N\theta_1 = N(1-\theta)$ as a unit root. The congruence

$$F_1(Z) \equiv Z^5 - NZ^4 + mZ^3 - NmZ^2 \equiv Z^2(Z-N)(Z^2+m) \pmod{2N}$$

shows that $N\theta_1$ is a root of a monic quadratic factor of F_1 congruent to Z^2+m (mod $2N$). Again, from Lemma 3.3, we have $\boldsymbol{Q}_2(\sqrt{1-\theta}) = \boldsymbol{Q}_2(\sqrt{2N\theta_1})$ coincides with $\boldsymbol{Q}_2(\sqrt{-1})$ (resp. $\boldsymbol{Q}_2(\sqrt{-1}, \sqrt{5})$) when $m \equiv 1$ (resp. 9) (mod 16). Hence, in $K(\sqrt{1-\theta})/K$, $\mathfrak{p}_2$ splits when $m \equiv 1 \pmod{16}$, and is inert when $m \equiv 9 \pmod{16}$.

That is all to be proved. □

Remark 5. If $m \equiv 1 \pmod{16}$, $L = K(\sqrt{\theta}, \sqrt{1-\theta})$ may coincide with K. In fact, $(n,m) = (1,-47), (1,257)$ are the cases (see also Section 6, Table 1(i)). When $(n,m) = (1,-47)$, for a root θ of $f_{n,m}(X) = X^5 - 4X^4 + \frac{209}{64}X^3 + \frac{79}{32}X^2 - \frac{47}{64}X - 1$, we have

$$\theta = \left(-\frac{96}{133}\theta^4 + \frac{352}{133}\theta^3 - \frac{467}{266}\theta^2 - \frac{13}{14}\theta - \frac{8}{133}\right)^2,$$
$$1-\theta = \left(\frac{16}{133}\theta^4 - \frac{16}{19}\theta^3 + \frac{337}{532}\theta^2 + \frac{117}{76}\theta - \frac{75}{133}\right)^2.$$

When $(n,m) = (1,257)$, for a root θ of $f_{n,m}(X) = X^5 - 4X^4 + \frac{513}{64}X^3 - \frac{225}{32}X^2 + \frac{257}{64}X - 1$, we have

$$\theta = \left(\frac{32}{121}\theta^4 - \frac{32}{121}\theta^3 - \frac{31}{242}\theta^2 + \frac{205}{242}\theta + \frac{40}{121}\right)^2,$$
$$1-\theta = \left(\frac{144}{121}\theta^4 - \frac{496}{121}\theta^3 + \frac{3593}{484}\theta^2 - \frac{2005}{484}\theta + \frac{169}{121}\right)^2.$$

§ 4. Infiniteness

In this section, we show the infiniteness of the family

$$\{K_{n,m} \mid m \equiv 9 \,(\mathrm{mod}16), m > 0\} \tag{4.1}$$

for each fixed positive integer n. It suffices to show the infiniteness of the family of the unique quadratic subfield $F_{n,m} = \boldsymbol{Q}(\sqrt{D_0(b)})$ of the Galois closure $\widetilde{K}_{n,m}$ of K. We will give the proof in two different way.

The first proof employs the following theorem in analytic number theory:

Theorem 4.1 (Erdös [4]). *Let $f(x) \in \boldsymbol{Z}[x]$ be a polynomial of degree $l \geq 3$ whose coefficients are integers with highest common factor 1. Assume that $l \geq 3$ and that $f(x)$ is not divisible by the $(l-1)$-th power of a linear polynomial with integral coefficients. (When l is a power of 2, we require an additional assumption that $f(n) \not\equiv 0 \pmod{2^{l-1}}$ for some integer n.) Then there are infinitely many positive integers n for which $f(n)$ is $(l-1)$-th power free.*

For each fixed positive integer n, put

$$d(m) := 2^{12n+4} D_0\left(\frac{m}{2^{4n+2}}\right) = -m^3 + 2^{4n+5}m^2 - 2^{8n+4} \cdot 11m - 2^{12n+4} \cdot 127 \in \boldsymbol{Z}[m]$$

and $\widetilde{d}(T) := d(16T+9) \in \boldsymbol{Z}[T]$. Then the coefficients of $\widetilde{d}(T)$ are coprime because the coefficient of T^3 is a power of 2 and the constant term is odd. Moreover, since

$\widetilde{d}(T) \equiv -T^3 - T^2 + T - 1 \pmod 3$, which is irreducible over $\boldsymbol{F}_3$, $\widetilde{d}(T)$ does not have multiple roots. Hence we can apply Theorem 4.1 for $\widetilde{d}(T)$ with $l = 3$, which implies that $\widetilde{d}(t)$ are square-free integers for infinitely many positive integers t. Since $\widetilde{d}(t)$ tends to $-\infty$ when $t \longrightarrow \infty$, $\widetilde{d}(t)$ attains infinitely many different square-free values, which give infinitely many different quadratic fields $\boldsymbol{Q}(\sqrt{\widetilde{d}(t)}) = F_{n,16t+9}$ belonging to our family (4.1). This completes the proof.

In another way of proof we use Dirichlet's prime number theorem in arithmetic progression. Let m_i $(i = 1, \ldots, r)$ be finite numbers of positive integers satisfying $m_i \equiv 9 \pmod{16}$, and put $F_i := F_{n,m_i} = \boldsymbol{Q}(\sqrt{d(m_i)})$. We shall show that there exists a prime number p with $p \equiv 9 \pmod{16}$ such that $F := F_{n,p} = \boldsymbol{Q}(\sqrt{d(p)})$ is different from all F_i. First we may remove F_i's where 127 ramifies beforehand, because in the following construction we shall obtain F where 127 does not ramify. Let $d(F_i)$ be the discriminant of F_i, and put $M := \operatorname{lcm}\{d(F_i) | 1 \leq i \leq r\}$. Then we have $(M, 127) = 1$ and $v_2(M) \leq 3$ since $d(F_i)$ are the discriminants of quadratic fields. Hence there exists a prime number p satisfying

$$p \equiv 1 \pmod M, \quad p \equiv 9 \pmod{16}, \quad \text{and} \quad p \equiv -1 \pmod{127}.$$

Then, at first,

$$\begin{aligned} d(p) &= -p^3 + 2^{4n+5}p^2 - 2^{8n+4} \cdot 11p - 2^{12n+4} \cdot 127 \\ &\equiv -(-1)^3 + 2^{4n+5}(-1)^2 - 2^{8n+4} \cdot 11 \cdot (-1) \pmod{127} \\ &\equiv 1 + 32 \cdot (2^n)^4 + 16 \cdot 11 \cdot (2^n)^8 \not\equiv 0 \pmod{127}, \end{aligned}$$

since no possible value of $2^n \equiv 1, 2, 4, 8, 16, 32, 64 \pmod{127}$ gives a zero of the polynomial $1 + 32T^4 + 16 \cdot 11T^8 \in \boldsymbol{F}_{127}[T]$. Hence 127 does not ramify in $F := \boldsymbol{Q}(\sqrt{d(p)})/\boldsymbol{Q}$. Moreover, since $d(p) \equiv -(2^{6n+2})^2 \cdot 127 \pmod p$, we have

$$\left(\frac{d(p)}{p}\right) = \left(\frac{-127}{p}\right) = \left(\frac{p}{127}\right) = \left(\frac{-1}{127}\right) = -1.$$

Hence p is inert in F. On the other hand, p splits in each $F_i/\boldsymbol{Q}$ since $p \equiv 1 \pmod{d(F_i)}$. Thus we have $F \neq F_i$, which is desired.

§ 5. Unramified extensions over $\widetilde{K}$

In this section, we consider the splitting field $\widetilde{K}$ of

$$f(X) = f(b; X) = X^5 - 4X^4 + (b+4)X^3 - (2b-1)X^2 + bX - 1,$$

that is, the Galois closure of a root field $K = \boldsymbol{Q}(\theta)$, where θ is a root of f, and show Theorem B. We continue assuming that $b = \dfrac{m}{2^{4n+2}}$ satisfies $m \equiv 9 \pmod{16}$, n being a

positive integer, and $b > \beta$. As seen in the previous sections, under these assumptions, $L = K(\sqrt{\theta}, \sqrt{1-\theta})$ is a unramified biquadratic extension of K.

Since the prime decomposition of 2 in K is $2\mathcal{O}_K = \mathfrak{p}_0\mathfrak{p}_1^2\mathfrak{p}_2^2$ as in (3.5), it decomposes in $\widetilde{K}$ as

$$2\mathcal{O}_{\widetilde{K}} = \prod_{i \in \boldsymbol{Z}/5\boldsymbol{Z}} \mathfrak{P}_i^2,$$

where $\mathfrak{p}_0\mathcal{O}_{\widetilde{K}} = \mathfrak{P}_0^2, \mathfrak{p}_1\mathcal{O}_{\widetilde{K}} = \mathfrak{P}_1\mathfrak{P}_{-1}$ and $\mathfrak{p}_2\mathcal{O}_{\widetilde{K}} = \mathfrak{P}_2\mathfrak{P}_{-2}$. The action of $\mathrm{Gal}(\widetilde{K}/K) = D_5$ on the set $\{\mathfrak{P}_i | i \in \boldsymbol{Z}/5\boldsymbol{Z}\}$ is compatible with the natural action of D_5 on $\boldsymbol{Z}/5\boldsymbol{Z}$, that is, $\alpha(i) = i+1, \beta(i) = -i$. In particular, the prime $\mathfrak{p}_0$ ramifies in $\widetilde{K}/K$, hence $L\widetilde{K}/\widetilde{K}$ is an unramified biquadratic extension.

Let $\theta^{(i)}$ $(i = 0, 1, 2, 3, 4)$ be the conjugates of $\theta = \theta_0$ over $\boldsymbol{Q}$, i.e. the roots of f. Then we have also that $\widetilde{K}(\sqrt{\theta^{(i)}}, \sqrt{1-\theta^{(i)}})/\widetilde{K}$ is an unramified biquadratic extension for each i.

Moreover we consider the extension $\widetilde{K}(\sqrt{-1})/\widetilde{K}$.

Proposition 5.1. *The extension $\widetilde{K}(\sqrt{-1})/\widetilde{K}$ is a non-trivial, (that is, quadratic) unramified extension.*

Proof. To show the non-triviality, it suffices to show that $\sqrt{-1} \notin F = \boldsymbol{Q}(\sqrt{D_0(b)})$, since F is the unique quadratic field in $\widetilde{K}$. This is equivalent to that b is never the first coordinate of a rational point (b, c) of the elliptic curve $E : -c^2 = D_0(b) = -4b^3 + 32b^2 - 44b - 127$. Changing variables by $b = (x+11)/4, c = y/4$, we can see that E is isomorphic to $E' : y^2 = x^3 + x^2 - 165x + 1427$ over $\boldsymbol{Q}$, which is the elliptic curve labeled `176b2` in Cremona's table [3]. From this table we know $E'(\boldsymbol{Q}) = \{O\}$. Hence, for any $b \in \boldsymbol{Q}$, $\sqrt{-1}$ does not belong to F.

Since the localization $\widetilde{K}_{\mathfrak{P}_i}$ of $\widetilde{K}$ at $\mathfrak{P}_i$ is $\boldsymbol{Q}_2(\sqrt{-1})$, any prime $\mathfrak{P}_i$ lying over 2 splits in $\widetilde{K}(\sqrt{-1})/\widetilde{K}$. In particular, $\widetilde{K}(\sqrt{-1})/\widetilde{K}$ is unramified. □

Therefore we obtain an unramified extension

$$\widetilde{L} := \widetilde{K}\left(\sqrt{-1}, \sqrt{\theta^{(i)}}, \sqrt{1-\theta^{(i)}} \middle| i \in \boldsymbol{Z}/5\boldsymbol{Z}\right)$$

over $\widetilde{K}$ whose Galois group $\widetilde{G} := \mathrm{Gal}(\widetilde{L}/\widetilde{K})$ is an elementary 2-group. We want to know the 2-rank of $\widetilde{G}$.

First, we have

$$\widetilde{L} = \widetilde{K}(\sqrt{-1}, \sqrt{\theta^{(0)}}, \sqrt{\theta^{(1)}}, \sqrt{\theta^{(2)}}, \sqrt{\theta^{(3)}})$$

owing to the following multiplicative relations among $\theta^{(i)}$ and $1-\theta^{(i)}$ (see (1.2)):

$$1 - \theta^{(i)} = \theta^{(i-1)}\theta^{(i+1)} \quad (i \in \boldsymbol{Z}/5\boldsymbol{Z}),$$

$$\prod_{i \in \boldsymbol{Z}/5\boldsymbol{Z}} \theta^{(i)} = 1.$$

Hence the 2-rank of $\widetilde{G}$ is at most 5.

By Proposition 3.4, in $K(\sqrt{\theta})/K$, $\mathfrak{p}_0$ and $\mathfrak{p}_1$ decompose, and $\mathfrak{p}_2$ is inert. Hence, in $\widetilde{K}(\sqrt{\theta})/\widetilde{K}$, $\mathfrak{P}_0$ and $\mathfrak{P}_{\pm 1}$ decompose, and $\mathfrak{P}_{\pm 2}$ are inert. Considering the action of $\mathrm{Gal}(\widetilde{K}/\boldsymbol{Q}) = D_5$, we obtain the following table describing the behavior of prime ideals $\mathfrak{P}_i$ in each subextension $\widetilde{K}_i/\widetilde{K}_{i-1}$ (+ denotes "decompose", and − denotes "inert"):

$\widetilde{K}_0 := \widetilde{K}$	$\mathfrak{P}_0$	$\mathfrak{P}_1$	$\mathfrak{P}_2$	$\mathfrak{P}_{-2}$	$\mathfrak{P}_{-1}$
$\widetilde{K}_1 := \widetilde{K}(\sqrt{-1})$	+	+	+	+	+
$\widetilde{K}_2 := \widetilde{K}(\sqrt{-1}, \sqrt{\theta_0})$	+	+	−	−	+
$\widetilde{K}_3 := \widetilde{K}(\sqrt{-1}, \sqrt{\theta_0}, \sqrt{\theta_1})$	+	+			−
$\widetilde{K}_4 := \widetilde{K}(\sqrt{-1}, \sqrt{\theta_0}, \sqrt{\theta_1}, \sqrt{\theta_2})$	−	+			
$\widetilde{K}_5 := \widetilde{K}(\sqrt{-1}, \sqrt{\theta_0}, \sqrt{\theta_1}, \sqrt{\theta_2}, \sqrt{\theta_3}) = \widetilde{L}$		−			

For $2 \leq i \leq 5$, each subextension $\widetilde{K}_i/\widetilde{K}_{i-1}$ is non-trivial since some prime ideal is inert in it. Combining Proposition 5.1, we obtain that $\widetilde{L}$ is an unramified extension of $\widetilde{K}$ with Galois group isomorphic to $(\boldsymbol{Z}/2\boldsymbol{Z})^5$.

The infiniteness of $\widetilde{K}$ follows from the result in the previous section asserting that the infinitess of F. Thus the proof of Theorem B is completed.

§ 6. Examples

Here we give tables of examples of ideal class groups $\mathrm{Cl}(K)$ of K and $\mathrm{Cl}(\widetilde{K})$ of $\widetilde{K}$ for $n = 3, m \equiv 1 \pmod 8, -160 < m < 400$ using PARI/GP [14]. In the tables, $[a_1, \ldots, a_r]$ denotes a finite abelian group isomorphic to $\boldsymbol{Z}/a_1\boldsymbol{Z} \times \cdots \times \boldsymbol{Z}/a_r\boldsymbol{Z}$ and [ ] denotes a trivial group. Note that, when $n = 3$, the inequality $\dfrac{m}{2^{4n+2}} > \beta = -1.3463\cdots$ holds if and only if $m > -86.16\cdots$. We indicate this threshold by the horizontal lines among the items.

Remark 6. In the cases $m = -47, 257 \equiv 1 \pmod{16}$ (denoted with $*$ in the table), it occurs that $L = K$ (See Remark 5).

Remark 7. We can see that in some cases the 2-rank of $\mathrm{Cl}(K)$ is 2 and the 2-rank of $\mathrm{Cl}(\widetilde{K})$ is 5. Therefore our result is best possible in a sence.

Remark 8. We can find also that in some cases the 2-rank of $\mathrm{Cl}(K)$ and the 2-rank of $\mathrm{Cl}(\widetilde{K})$ are around the twice of the lower bounds obtained in the theorems. These fields are maybe given by two different parameters (n, m).

References

[1] Anai, H., Kondo, T., A family of sixth degree expressions with Galois group A_5 — the computation of splitting fields and Galois groups, (in Japanese) *Studies in the theory of computer algebra and its applications*, *Sūrikaisekikenkyūsho Kōkyūroku* No. **941** (1996), 57–72.

[2] Brumer, A., Curves with real multiplications, in preparation.

[3] Cremona, J. E., *Algorithms for modular elliptic curves, 2nd ed.*, Cambridge Univ. Press, Cambridge, 1997.

[4] Erdös, P., Arithmetical properties of polynomials, *J. London Math. Soc.* **28** (1953), 416–425.

[5] Hashimoto, K., On Brumer's family of RM-curves of genus two, *Tohoku Math. J.* (2) **52** (2000), no. 4, 475–488.

[6] Hashimoto, K., Tsunogai, H., Generic polynomials over $\boldsymbol{Q}$ with two parameters for the transitive groups of degree five, *Proc. Japan Acad.* **79A** (2003), 148–151.

[7] Kato, Y., A construction of an infinite family of dihedral quintic fields with unramified quadratic extensions, master's thesis (in Japanese), Sophia University, 2018.

[8] Kida, M., Rikuna, Y., Sato, A., Classifying Brumer's quintic polynomials by weak Mordell-Weil groups, *Int. J. Number Theory* **6** (2010), no. 3, 691–704.

[9] Kihel, O., Groupe des unités pour des extensions diédrales complexes de degré 10 sur $\boldsymbol{Q}$, *J. Théor. Nombres Bordeaux* **13** (2001), no. 2, 469–482.

[10] Kondo, T., Some examples of unramified extensions over quadratic fields, *Sci. Rep. Tokyo Woman's Christian Univ.*, No. **120**–**121** (1977), 1399–1410.

[11] Lavallee, M. J., Spearman, B. K., Williams, K. S., Yang, Q., Dihedral quintic fields with a power basis, *Math. J. Okayama Univ.* **47** (2005), 75–79.

[12] Lehmer, E., Connection between Gaussian periods and cyclic units, *Math. Comp.* **50** (1988), 535–541.

[13] Nakano, S., A family of quintic cyclic fields with even class number parameterized by rational points on an elliptic curve, *J. Number Theory* **129** (2009), 2943–2951.

[14] The PARI-Group, PARI/GP version 2.9.1, Bordeaux, 2016. available from `http://pari.math.u-bordeaux.fr/`

m	$\mathrm{Cl}(K)$	$\mathrm{Cl}(\widetilde{K})$
-159	$[5]$	$[50, 10]$
-143	$[\,]$	$[3]$
-127	$[\,]$	$[12, 4, 2]$
-111	$[\,]$	$[4]$
-95	$[10, 2]$	$[10, 2, 2, 2]$
-79	$[2, 2]$	$[26, 2, 2, 2, 2, 2, 2, 2]$
-63	$[4, 4]$	$[180, 4, 4, 4, 4]$
$^*-47$	$[\,]$	$[4]$
-31	$[2, 2]$	$[228, 2, 2, 2, 2, 2]$
-15	$[60, 12]$	$[3300, 60, 12, 12, 2, 2]$
1	$[2, 2]$	$[244, 2, 2, 2, 2, 2]$
17	$[6, 6, 2, 2]$	$[648, 6, 6, 6, 6, 2, 2, 2, 2]$
33	$[4, 4]$	$[244, 4, 4, 4, 4, 2]$
49	$[6, 6]$	$[210, 6, 6, 6, 6, 2]$
65	$[2, 2, 2, 2]$	$[308, 2, 2, 2, 2, 2, 2, 2, 2, 2]$
81	$[10, 10]$	$[600, 10, 10, 2, 2]$
97	$[2, 2]$	$[196, 2, 2, 2, 2, 2, 2]$
113	$[4, 4]$	$[300, 4, 4, 4, 2, 2, 2]$
129	$[10, 2, 2, 2]$	$[300, 10, 2, 2, 2, 2, 2, 2, 2, 2, 2]$
145	$[4, 4]$	$[112, 4, 4, 4, 4, 4]$
161	$[10, 2]$	$[700, 10, 2, 2, 2, 2]$
177	$[2, 2, 2, 2]$	$[124, 2, 2, 2, 2, 2, 2, 2, 2, 2]$
193	$[8, 8]$	$[1432, 8, 8, 8, 4]$
209	$[4, 4]$	$[48, 4, 4, 4, 4, 4, 2]$
225	$[10, 2]$	$[500, 10, 2, 2, 2, 2]$
241	$[124, 4]$	$[8308, 124, 4, 4, 4]$
^{*257}	$[\,]$	$[2, 2]$
273	$[2, 2]$	$[56, 2, 2, 2, 2, 2, 2]$
289	$[4, 4]$	$[60, 4, 4, 4, 4, 2, 2]$
305	$[10, 2]$	$[1500, 10, 2, 2, 2]$
321	$[4, 4, 2, 2]$	$[32, 4, 4, 4, 4, 2, 2, 2, 2, 2, 2]$
337	$[2, 2]$	$[228, 2, 2, 2, 2, 2]$
353	$[2, 2]$	$[452, 2, 2, 2, 2]$
369	$[2, 2]$	$[126, 2, 2, 2, 2, 2]$
385	$[10, 2]$	$[1700, 10, 2, 2, 2]$

(i) $m \equiv 1 \pmod{16}$

m	$\mathrm{Cl}(K)$	$\mathrm{Cl}(\widetilde{K})$
-151	$[\,]$	$[4]$
-135	$[\,]$	$[2]$
-119	$[\,]$	$[2]$
-103	$[\,]$	$[6, 2, 2]$
-87	$[\,]$	$[\,]$
-71	$[2, 2]$	$[372, 2, 2, 2, 2]$
-55	$[2, 2]$	$[392, 2, 2, 2, 2]$
-39	$[2, 2]$	$[40, 2, 2, 2, 2, 2, 2]$
-23	$[2, 2]$	$[548, 2, 2, 2, 2]$
-7	$[10, 2]$	$[360, 20, 2, 2, 2, 2]$
9	$[2, 2]$	$[26, 2, 2, 2, 2, 2, 2, 2]$
25	$[10, 2]$	$[100, 10, 2, 2, 2, 2]$
41	$[2, 2]$	$[308, 2, 2, 2, 2, 2]$
57	$[2, 2]$	$[208, 2, 2, 2, 2, 2]$
73	$[10, 10]$	$[240, 10, 10, 10, 10, 2]$
89	$[10, 2, 2, 2]$	$[2700, 10, 2, 2, 2, 2, 2, 2, 2]$
105	$[2, 2]$	$[98, 2, 2, 2, 2, 2]$
121	$[2, 2]$	$[264, 2, 2, 2, 2, 2]$
137	$[2, 2]$	$[540, 2, 2, 2, 2, 2]$
153	$[2, 2, 2, 2]$	$[336, 2, 2, 2, 2, 2, 2, 2, 2]$
169	$[10, 2]$	$[1440, 2, 2, 2, 2]$
185	$[2, 2]$	$[78, 2, 2, 2, 2, 2, 2]$
201	$[2, 2]$	$[160, 2, 2, 2, 2]$
217	$[2, 2]$	$[258, 2, 2, 2, 2, 2]$
233	$[2, 2]$	$[46, 2, 2, 2, 2, 2, 2, 2]$
249	$[2, 2, 2, 2]$	$[176, 2, 2, 2, 2, 2, 2, 2, 2]$
265	$[2, 2, 2, 2]$	$[144, 2, 2, 2, 2, 2, 2, 2, 2, 2]$
281	$[2, 2]$	$[72, 2, 2, 2, 2, 2, 2]$
297	$[10, 2]$	$[900, 10, 2, 2, 2]$
313	$[2, 2]$	$[200, 2, 2, 2, 2, 2]$
329	$[2, 2]$	$[112, 2, 2, 2, 2, 2]$
345	$[30, 6]$	$[60, 6, 6, 6, 6]$
361	$[2, 2]$	$[48, 2, 2, 2, 2]$
377	$[10, 2]$	$[390, 10, 10, 2, 2, 2]$
393	$[10, 2]$	$[500, 10, 2, 2, 2, 2, 2]$

(ii) $m \equiv 9 \pmod{16}$

Table 1. $b = \dfrac{m}{64}, m \equiv 1 \text{ or } 9 \pmod{16}$