Math. J. Okayama Univ. **68** (2026), 1–12

GENERATOR OF THE QUADRATIC SUBEXTENSION OF AN ODD DIHEDRAL EXTENSION

Toru Komatsu

Abstract. In this paper we present an algorithm to make a generator of the quadratic subextension of an odd dihedral extension. As an application we solve the Galois group problem for the quintic polynomials given by Kishi and Yamada.

1. Introduction

For an integer n greater than one let $\mathfrak{C}_n$ and $\mathfrak{D}_n$ denote the cyclic and the dihedral group of degree n with order n and $2n$, respectively. Let K be a field of characteristic 0. For a polynomial $f(X)$ over K with positive degree let $\mathrm{Spl}(f/K)$ denote the minimal splitting field of $f(X)$ over K, and $\mathrm{Gal}(f/K)$ its Galois group $\mathrm{Gal}(\mathrm{Spl}(f/K)/K)$. If $f(X)$ is an irreducible polynomial over K of degree n with $\mathrm{Gal}(f/K) \simeq \mathfrak{D}_n$, then the field $M = \mathrm{Spl}(f/K)$ contains a unique subfield N such that $\mathrm{Gal}(M/N) \simeq \mathfrak{C}_n$ and $\mathrm{Gal}(N/K) \simeq \mathfrak{C}_2$. When n is not congruent to 1 modulo 4, the extension N/K is generated by the square root $\sqrt{\mathrm{disc}_X f(X)}$ of the discriminant $\mathrm{disc}_X f(X)$ of $f(X)$ with respect to X. For the case of $n \equiv 1 \pmod 4$, the discriminant $\mathrm{disc}_X f(X)$ is square in K since $\mathfrak{D}_n$ is included in the alternating group $\mathfrak{A}_n$ of degree n. In this paper we present an algorithm to make a generator of the extension N/K when n is odd. As an application we determine whether the Galois groups of the quintic polynomials given by Kishi and Yamada [7] are isomorphic to $\mathfrak{D}_5$ or $\mathfrak{C}_5$.

Theorem 1.1. *Let $f(X)$ be an irreducible polynomial over K of odd degree n equal to or greater than 3 with $\mathrm{Gal}(f/K) \simeq \mathfrak{D}_n$. For a root λ of $f(X)$ in $M = \mathrm{Spl}(f/K)$ we put $L = K(\lambda)$ and decompose $f(X)$ into irreducible factors $f_i(X)$ over L such that $f(X) = (X - \lambda)f_1(X) \cdots f_r(X)$. For each integer i with $1 \le i \le r$ let δ_i denote the discriminant $\mathrm{disc}_X f_i(X)$ of $f_i(X)$ and d_i its norm $\nu_{L/K}(\delta_i)$ where $\nu_{L/K}$ is the norm map from L to K. Then r is equal to $(n-1)/2$ and the square root $\sqrt{d_i}$ generates N over K for every integer i with $1 \le i \le r$ where N is a unique subextension of M/K with $[N : K] = 2$.*

Mathematics Subject Classification. Primary 11R32; Secondary 11R09,11R11.
Key words and phrases. Dihedral extension, quadratic subextension, Galois theory.

Remark. For the calculation of irreducible factorization over a number field the software packages Maple [9], PARI/GP [10] and Wolfram Mathematica [12] are equipped with functions `factor`, `factornf` and `Factor`, respectively.

For nonzero rational numbers a, b and μ, Kishi and Yamada [7] treat quintic polynomials of the form $f^{\mathrm{KY}}_{a,b,\mu}(X) = X^5 + abX^3 + a^2X + a^3\mu \in \mathbb{Q}[X]$ under relation $a = a_i(b, \mu)$ where $a_1(b, \mu) = 144(b + 2)^2(2b + 5)(6b^2 + 15b + 10)/(5^4\mu^2)$ and $a_2(b, \mu) = b^2(b - 2)^2(3b + 5)^2(3b - 10)/(5^5(b^2 + b - 1)\mu^2)$.

Theorem 1.2 (Kishi and Yamada [7]). *(1) Assume $f(X) = f^{\mathrm{KY}}_{a_1(b,\mu),b,\mu}(X)$ is irreducible over $\mathbb{Q}$. Then $\mathrm{Gal}(f/\mathbb{Q})$ is isomorphic to $\mathfrak{C}_5$ or $\mathfrak{D}_5$, especially for $b > 0$, $\mathrm{Gal}(f/\mathbb{Q})$ is isomorphic to $\mathfrak{D}_5$.*
(2) Assume $f(X) = f^{\mathrm{KY}}_{a_2(b,\mu),b,\mu}(X)$ is irreducible over $\mathbb{Q}$. Then $\mathrm{Gal}(f/\mathbb{Q})$ is isomorphic to $\mathfrak{C}_5$ or $\mathfrak{D}_5$, especially for $b > 10/3$, $\mathrm{Gal}(f/\mathbb{Q})$ is isomorphic to $\mathfrak{D}_5$.

In this paper we show that every irreducible polynomial of the first family $f^{\mathrm{KY}}_{a_1(b,\mu),b,\mu}(X)$ gives a $\mathfrak{D}_5$-extension of $\mathbb{Q}$ not only for $b > 0$ but also for $b \leq 0$ (Corollary 3.2) and that the second family $f^{\mathrm{KY}}_{a_2(b,\mu),b,\mu}(X)$ with $b < 2$ or $b > 10/3$ yields $\mathfrak{D}_5$-extensions of $\mathbb{Q}$ containing imaginary quadratic fields (Corollary 3.4). For the case of $2 \leq b \leq 10/3$, we give a simple criterion for an irreducible polynomial $f^{\mathrm{KY}}_{a_2(b,\mu),b,\mu}(X)$ to give a $\mathfrak{D}_5$-extension or a $\mathfrak{C}_5$-extension of $\mathbb{Q}$ (Lemma 3.5). The main purpose in this paper is to present an algorithm to make the generator of the quadratic subextension contained in $\mathfrak{D}_n$-extension with an odd number n at the second section (Theorem 2.3). We apply the algorithm to two quintic families of Kishi and Yamada [7] described above at the third section, to the quintic family of Brumer [1] and Hashimoto [5] at the fourth section and to the odd dihedral families of Hashimoto and Miyake [4] at the final section. We also exhibit the discriminants of the odd dihedral polynomials constructed by Hashimoto and Miyake [4].

2. Generator of the quadratic subextension

Let $f(X)$ be an irreducible polynomial over K of odd degree $n \geq 3$ with $\mathrm{Gal}(f/K) \simeq \mathfrak{D}_n$. Denote $M = \mathrm{Spl}(f/K)$ and $G = \mathrm{Gal}(f/K)$. Fix a root λ of $f(X)$ in M and put $L = K(\lambda)$. Let M^H stand for the subfield of M fixed by a subgroup H of G. There exists a unique element τ in G such that $L = M^{\langle\tau\rangle}$ where $\langle\tau\rangle$ is the subgroup of G generated by τ. Fix an element σ in G with order n and put $\tau_i = \sigma^i\tau\sigma^{-i}$ for each integer i. Then G decomposes into two disjoint subsets $S = \{\sigma^i \mid 0 \leq i \leq n-1\}$ and $T = \{\tau_i \mid 0 \leq i \leq n-1\}$. Note that σ^i are of odd order and τ_i are of order 2. By $\tau\sigma^i \notin S$, the order of $\tau\sigma^i$ is equal to 2. Thus $\tau\sigma^i$ is equal to its inverse $(\tau\sigma^i)^{-1} = \sigma^{-i}\tau^{-1} = \sigma^{-i}\tau$.

For each integer i put $L_i = M^{\langle \tau_i \rangle}$ and $\lambda_i = \sigma^i(\lambda)$. Note that $L_i = L_j$ if and only if $i \equiv j \pmod{n}$. Thus $L_0, \ldots, L_{n-1}$ are distinct from one another.

Lemma 2.1. *For every integer i we have $L_i = K(\lambda_i)$ and $\tau(\lambda_i) = \lambda_{-i}$.*

Proof. It follows from $\tau_i(\lambda_i) = \tau_i(\sigma^i(\lambda)) = \sigma^i(\tau(\lambda)) = \sigma^i(\lambda) = \lambda_i$ that $K(\lambda_i) \subset L_i$. Since λ_i is a root of $f(X)$, the degree $[K(\lambda_i) : K]$ is equal to n. Thus the equality $K(\lambda_i) = L_i$ holds. By $\tau\sigma^i = \sigma^{-i}\tau$ we have $\tau(\lambda_i) = \tau\sigma^i(\lambda) = \sigma^{-i}\tau(\lambda) = \lambda_{-i}$. □

Put $f_i(X) = (X - \lambda_i)(X - \lambda_{n-i})$ for each integer i with $1 \leq i \leq (n-1)/2$.

Lemma 2.2. *For every integer i with $1 \leq i \leq (n-1)/2$ the polynomial $f_i(X)$ is defined over L and irreducible over L.*

Proof. Lemma 2.1 implies that $f_i(X)$ is defined over $M^{\langle \tau \rangle} = L$. Since $L = L_0$ does not contain L_i (resp. L_{n-i}), the factor $X - \lambda_i$ (resp. $X - \lambda_{n-i}$) is not defined over L. Thus $f_i(X)$ is irreducible over L. □

For an integer i with $1 \leq i \leq (n-1)/2$ let δ_i denote the discriminant $\mathrm{disc}_X f_i(X)$ of $f_i(X)$, and d_i its norm $\nu_{L/K}(\delta_i)$ where $\nu_{L/K}$ is the norm map from L to K. Now put $N = M^{\langle \sigma \rangle}$.

Theorem 2.3. *The irreducible factorization of $f(X)$ over L has form $(X - \lambda_0)f_1(X) \cdots f_{(n-1)/2}(X)$. For every $i = 1, \ldots, (n-1)/2$ the square root $\sqrt{d_i}$ of d_i generates N over K, that is, $N = K(\sqrt{d_i})$. The product $d_1 \cdots d_{(n-1)/2}$ of $d_1, \ldots, d_{(n-1)/2}$ is equal to the discriminant $\mathrm{disc}_X f(X)$ of $f(X)$.*

Let us investigate the actions of G on δ_i and $\sqrt{d_i}$. For an integer c we define a finite set P_c consisting of the pairs of integers such that $P_c = \{(c+k, k) \in \mathbb{Z} \times \mathbb{Z} \mid k = 0, 1, \ldots, n-1\}$.

Lemma 2.4. *For every $i = 1, \ldots, (n-1)/2$ we have $d_i = \prod_{(a,b) \in P_{2i}} (\lambda_a - \lambda_b)^2$.*

Proof. The definition of $f_i(X)$ implies that $\delta_i = (\lambda_i - \lambda_{-i})^2$. By Lemma 2.1 the norm $d_i = \nu_{L/K}(\delta_i) = \prod_{k=0}^{n-1} \sigma^k(\delta_i)$ is equal to $\prod_{k=0}^{n-1}(\lambda_{i+k} - \lambda_{-i+k})^2 = \prod_{(a,b) \in P_{2i}} (\lambda_a - \lambda_b)^2$. □

For an integer $i = 1, \ldots, (n-1)/2$ we denote by γ_i the product $\prod_{(a,b) \in P_{2i}} (\lambda_a - \lambda_b)$ of which square is equal to the norm d_i.

Lemma 2.5. *For every $i = 1, \ldots, (n-1)/2$ we have $\sigma(\gamma_i) = \gamma_i$ and $\tau(\gamma_i) = -\gamma_i$.*

Proof. Since $\sigma(\lambda_i) = \lambda_{i+1}$ and $\tau(\lambda_i) = \lambda_{-i}$ by Lemma 2.1 one has

$$\begin{aligned}\sigma(\gamma_i) &= \prod_{(a,b)\in P_{2i}} \sigma(\lambda_a - \lambda_b) = \prod_{(a,b)\in P_{2i}} (\lambda_{a+1} - \lambda_{b+1}) = \prod_{(a',b')\in P_{2i}} (\lambda_{a'} - \lambda_{b'}) = \gamma_i,\\ \tau(\gamma_i) &= \prod_{(a,b)\in P_{2i}} \tau(\lambda_a - \lambda_b) = \prod_{(a,b)\in P_{2i}} (\lambda_{-a} - \lambda_{-b})\\ &= (-1)^n \prod_{(a,b)\in P_{2i}} (\lambda_{-b} - \lambda_{-a}) = (-1)^n \prod_{(a',b')\in P_{2i}} (\lambda_{a'} - \lambda_{b'}) = -\gamma_i\end{aligned}$$

for odd n. □

Proof of Theorem 2.3. Since $L_0, \dots, L_{n-1}$ are distinct from one another, so are $\lambda_0, \dots, \lambda_{n-1}$. This means that $f(X) = \prod_{i=0}^{n-1}(X - \lambda_i)$. Lemma 2.2 implies the first assertion. Lemma 2.5 means that $N = M^{\langle\sigma\rangle} = K(\gamma_i) = K(\sqrt{d_i})$, which is the second assertion. By the relation $\lambda_a = \lambda_{a+n}$, the difference $\lambda_{a+k} - \lambda_a$ for an odd k with $0 < k < n$ is equal to $-(\lambda_{a'+k'} - \lambda_{a'})$ for even k' with $0 < k' < n$ where $a' = a + k$ and $k' = n - k$. Thus the discriminant $\mathrm{disc}_X f(X)$ of $f(X)$ has a decomposition into the product of d_i such that

$$\mathrm{disc}_X f(X) = \prod_{0\le a<b\le n-1} (\lambda_a - \lambda_b)^2 = \prod_{i=1}^{(n-1)/2} \prod_{(a,b)\in P_{2i}} (\lambda_a - \lambda_b)^2 = \prod_{i=1}^{(n-1)/2} d_i,$$

which is the third assertion. □

Theorem 2.3 shows Theorem 1.1.

Remark. In the case of $K = \mathbb{Q}$ Williamson [11, Proposition 3] gives the same generator as Theorems 1.1 and 2.3 by using the resolvent. Williamson's method requires not only the computation of the resolvent with degree $n(n-1)$ but also its factorization over $\mathbb{Q}$.

When we treat numerical examples, the resultant of two polynomials is useful to calculate the norm d_i. For two polynomials $g(X) = g_l X^l + g_{l-1}X^{l-1} + \cdots + g_1 X + g_0$ and $h(X) = h_m X^m + h_{m-1}X^{m-1} + \cdots + h_1 X + h_0$ with $g_l \neq 0$ and $h_m \neq 0$ we define the resultant $\mathrm{Res}_X(g(X), h(X))$ of $g(X)$ and $h(X)$ by the determinant of $(l+m) \times (l+m)$ matrix

$$\begin{bmatrix} g_l & g_{l-1} & \cdots & g_1 & g_0 & & & O\\ & g_l & g_{l-1} & \cdots & g_1 & g_0 & & \\ & & \ddots & & & & \ddots & \\ O & & & g_l & g_{l-1} & \cdots & g_1 & g_0\\ h_m & h_{m-1} & \cdots & h_1 & h_0 & & & O\\ & h_m & h_{m-1} & \cdots & h_1 & h_0 & & \\ & & \ddots & & & & \ddots & \\ O & & & h_m & h_{m-1} & \cdots & h_1 & h_0 \end{bmatrix}$$

called the Sylvester matrix. It is known that $\mathrm{Res}_X(g(X), h(X))$ is equal to $g_l^m h_m^l \prod_{i,j}(\alpha_i - \beta_j) = g_l^m \prod_i h(\alpha_i)$ where $g(X) = g_l \prod_{i=1}^{l}(X - \alpha_i)$ and $h(X) = h_m \prod_{j=1}^{m}(X - \beta_j)$.

Lemma 2.6. *For every $i = 1, \ldots, (n-1)/2$ the norm d_i is equal to the resultant $\mathrm{Res}_X(f(X), \tilde{\delta}_i(X))$ where $\tilde{\delta}_i(X)$ is a polynomial over K such that $\tilde{\delta}_i(\lambda) = \delta_i$.*

Proof. Since $\tilde{\delta}_i(X)$ is defined over K, the norm $d_i = \prod_{k=0}^{n-1} \sigma^k(\delta_i)$ is equal to $\prod_{k=0}^{n-1} \tilde{\delta}_i(\lambda_k) = \mathrm{Res}_X(f(X), \tilde{\delta}_i(X))$. □

3. Two quintic families by Kishi and Yamada

Recall the quintic polynomials of Kishi and Yamada [7] with the form $f_{a,b,\mu}^{\mathrm{KY}}(X) = X^5 + abX^3 + a^2X + a^3\mu \in \mathbb{Q}[X]$ and two specializations $a_1(b,\mu) = 144(b+2)^2(2b+5)(6b^2+15b+10)/(5^4\mu^2)$ and $a_2(b,\mu) = b^2(b-2)^2(3b+5)^2(3b-10)/(5^5(b^2+b-1)\mu^2)$. With one indeterminate b let $\mathbb{Q}(b)$ denote the field of rational functions in b over $\mathbb{Q}$ and $\mathbb{Z}[b]$ the ring of polynomials in b over $\mathbb{Z}$. We consider $f_{a_i(b,\mu),b,\mu}^{\mathrm{KY}}(X)$ as polynomials over $\mathbb{Q}(b)$. As described in the paper [7, Remark 2], due to the relation $f_{a_i(b,\mu),b,\mu}^{\mathrm{KY}}(X) = f_{a_i(b,1),b,1}^{\mathrm{KY}}(\mu X)/\mu^5$ one has that $\mathrm{Spl}(f_{a_i(b,\mu),b,\mu}^{\mathrm{KY}}/\mathbb{Q}(b)) = \mathrm{Spl}(f_{a_i(b,\mu'),b,\mu'}^{\mathrm{KY}}/\mathbb{Q}(b))$ for nonzero μ and μ'. We define $f_b^{\mathrm{KY1}}(X) = f_{a_1(b,\mu),b,\mu}^{\mathrm{KY}}(X)$ with $\mu = 2^2 3(b+2)/5^3$ and $f_b^{\mathrm{KY2}}(X) = f_{a_2(b,\mu),b,\mu}^{\mathrm{KY}}(X)$ with $\mu = b(b-2)(3b+5)/(5^3(b^2+b-1))$. Then $f_b^{\mathrm{KY1}}(X)$ and $f_b^{\mathrm{KY2}}(X)$ are monic polynomials over $\mathbb{Z}[b]$. As a model over the function field $\mathbb{Q}(b)$ we have

Proposition 3.1. *For $f(X) = f_b^{\mathrm{KY1}}(X)$ let N be a unique subextension of the extension $M/\mathbb{Q}(b)$ with $[N : \mathbb{Q}(b)] = 2$ where $M = \mathrm{Spl}(f/\mathbb{Q}(b))$. Then the square root $\sqrt{-(b+2)(2b+5)(6b^2+15b+10)}$ is a generator of N over $\mathbb{Q}(b)$.*

Proof. Put $d = \mathrm{disc}_X f(X)$ the discriminant of $f(X)$. With a calculator one sees that $d = 2^4 5^{16} \theta_1^2 \theta_2^{10} \theta_3^{10} \theta_4^2 \theta_5^2$ where $\theta_1 = \theta_1(b) = b+2$, $\theta_2 = \theta_2(b) = 2b+5$, $\theta_3 = \theta_3(b) = 6b^2+15b+10$, $\theta_4 = \theta_4(b) = 18b^2+50b+35$ and $\theta_5 = \theta_5(b) = 54b^2+225b+230$. Theorem 2.3 implies $d = d_1d_2$ under the notation as in Theorem 2.3. Since $f(X)$ is a monic polynomial over $\mathbb{Z}[b]$, its roots λ are integral over $\mathbb{Z}[b]$ and so are d_i by Lemma 2.4. Thus d_1 and d_2 are divisors of d in $\mathbb{Z}[b]$, that is, there exist integers c_i and $r_{i,j} \geq 0$ such that $d_i = c_i \theta_1^{r_{i,1}} \cdots \theta_5^{r_{i,5}}$. Now put $\mathcal{D} = \{d_1, d_2\}$. For example, using a calculator, at $b = 0$ one can calculate the irreducible factorization $f(X) = (x-\lambda)f_1(X)f_2(X)$ over $\mathbb{Q}(\lambda)$, the discriminants δ_i of $f_i(X)$ and their norms d_i such that $\mathcal{D} = \{-2^8 5^{20} 23^2, -2^{10} 5^{20} 7^2\}$. To distinguish between d_1 and d_2

when b moves, we focus on the prime 7. For each integer k with $0 \le k \le 5$ put $b_k = 7k$, and define a value $d_{1,k}$ to be the element in $\mathcal{D}$ having a factor 7 where $\mathcal{D} = \{d_1, d_2\}$ is calculated at $b = b_k$. Also, $d_{2,k}$ is defined so that $\{d_{1,k}, d_{2,k}\} = \mathcal{D}$. Define a 6×6 matrix $A = [a_{ij}]$ and two 6×1 matrices $V_1 = [v_{1,i}]$ and $V_2 = [v_{2,i}]$ such that $a_{ij} = \log|\theta_j(b_{i-1})|$ for $1 \le j \le 5$ and $a_{i6} = 1$, and $v_{1,i} = \log|d_{1,i-1}|$ and $v_{2,i} = \log|d_{2,i-1}|$. With a calculator one sees that $A^{-1}V_1 \fallingdotseq {}^t[1\ 5\ 5\ 2\ 0\ 15.65]$ and $A^{-1}V_2 \fallingdotseq {}^t[1\ 5\ 5\ 0\ 2\ 12.88]$ where $\fallingdotseq$ stands for approximate equality and the symbol ^{t} means the transpose of a matrix. This implies that $(r_{1,1}, r_{1,2}, r_{1,3}, r_{1,4}, r_{1,5}) = (1, 5, 5, 2, 0)$ and $(r_{2,1}, r_{2,2}, r_{2,3}, r_{2,4}, r_{2,5}) = (1, 5, 5, 0, 2)$. The values $d_{i,0}$ at $b = 0$ yield that $c_1 = d_{1,0}/(\theta_1(0)^1 \cdots \theta_5(0)^0) = -2^4 5^8$ and $c_2 = d_{2,0}/(\theta_1(0)^1 \cdots \theta_5(0)^2) = -5^8$. Indeed, in such a case one has $\log|c_1| = 15.648\ldots$ and $\log|c_2| = 12.875\ldots$. Hence we have $d_1 = -2^4 5^8 \theta_1 \theta_2^5 \theta_3^5 \theta_4^2$ and $d_2 = -5^8 \theta_1 \theta_2^5 \theta_3^5 \theta_5^2$. Theorem 2.3 verifies $N = \mathbb{Q}(b, \sqrt{d_1}) = \mathbb{Q}(b, \sqrt{d_2}) = \mathbb{Q}(b, \sqrt{-\theta_1\theta_2\theta_3})$. $\square$

As a specialization to $\mathbb{Q}$ we have

Corollary 3.2. *Let b be a rational number such that $f(X) = f_b^{\mathrm{KY1}}(X)$ is irreducible over $\mathbb{Q}$. Then* $\mathrm{Spl}(f/\mathbb{Q})$ *is a $\mathfrak{D}_5$-extension of $\mathbb{Q}$ containing a quadratic field $\mathbb{Q}(\sqrt{q_1(b)})$ where $q_1(b) = -(b+2)(2b+5)(6b^2+15b+10)$.*

Proof. Let us define two curves $C : c^2 = q_1(b)$ and $E : y^2 + xy = x^3 - 3x - 3$. Then there exist birational maps

$$\beta_1 : C \to E, (b, c) \mapsto \Big(-\frac{1}{b+2}, \frac{b+c+2}{2(b+2)^2}\Big),$$
$$\beta_2 : E \to C, (x, y) \mapsto \Big(-\frac{2x+1}{x}, \frac{x+2y}{x^2}\Big)$$

such that $\beta_2 \circ \beta_1$ and $\beta_1 \circ \beta_2$ are identity maps. The curve E is an elliptic curve of conductor 150 with LMFDB label 150.c4 in [8] and with Cremona label 150a1 in [2]. Due to [2] and [8], the Mordell-Weil group $E(\mathbb{Q})$ of E over $\mathbb{Q}$ is $E(\mathbb{Q}) = \{O, (2, -1)\} \simeq \mathbb{Z}/2\mathbb{Z}$ where O is the point at infinity on E. Thus the $\mathbb{Q}$-rational points on C are two points $g(O) = (-2, 0)$ and $g(2, -1) = (-5/2, 0)$. The polynomials $f_{-2}^{\mathrm{KY1}}(X) = (X+10)^2 X (X-10)^2$ and $f_{-5/2}^{\mathrm{KY1}}(X) = X^5$ are reducible over $\mathbb{Q}$. Hence the value $q_1(b)$ is not square in $\mathbb{Q}$ for any $b \in \mathbb{Q}$ such that $f(X)$ is irreducible over $\mathbb{Q}$. $\square$

Remark. In the paper [7] they say that they have not yet found any examples of rational numbers b such that $\mathrm{Gal}(f_{a_1(b,\mu),b,\mu}^{\mathrm{KY}}/\mathbb{Q}) \simeq \mathfrak{C}_5$. Corollary 3.2 above guarantees that no such examples exist.

By the same way as for the first family, one can see the following assertion for the second one. As a model over the function field $\mathbb{Q}(b)$ we have

Proposition 3.3. *For $f(X) = f_b^{\mathrm{KY2}}(X)$ let N be a unique subextension of the extension $M/\mathbb{Q}(b)$ with $[N : \mathbb{Q}(b)] = 2$ where $M = \mathrm{Spl}(f/\mathbb{Q}(b))$. Then the square root $\sqrt{-5(b-2)(3b-10)}$ is a generator of N over $\mathbb{Q}(b)$.*

Proof. Put $d = \mathrm{disc}_X f(X)$. With a calculator one sees $d = 5^6\theta_1^2\theta_2^{10}\theta_3^8\theta_4^2\theta_5^2$ where $\theta_1 = \theta_1(b) = b-2$, $\theta_2 = \theta_2(b) = 3b-10$, $\theta_3 = \theta_3(b) = b^2+b-1$, $\theta_4 = \theta_4(b) = 3b^3-20b-20$ and $\theta_5 = \theta_5(b) = 9b^3-15b+10$. As for the first family, by Theorem 2.3 and Lemma 2.4, the norms d_1 and d_2 are divisors of d in $\mathbb{Z}[b]$, that is, there exist integers c_i and $r_{i,j} \geq 0$ such that $d_i = c_i\theta_1^{r_{i,1}} \cdots \theta_5^{r_{i,5}}$. Now put $\mathcal{D} = \{d_1, d_2\}$. For example, using a calculator, at $b = 3$ one can calculate $\mathcal{D} = \{5^3 11^4, 2^8 5^3 11^4 13^2\}$. To distinguish between d_1 and d_2 when b moves, we focus on the prime 13. For each integer k with $0 \leq k \leq 5$ put $b_k = 13k+3$, and define a value $d_{1,k}$ to be the element in $\mathcal{D}$ having a factor 13 where $\mathcal{D} = \{d_1, d_2\}$ is calculated at $b = b_k$. Also, $d_{2,k}$ is defined so that $\{d_{1,k}, d_{2,k}\} = \mathcal{D}$. Define a 6×6 matrix $A = [a_{ij}]$ and two 6×1 matrices $V_1 = [v_{1,i}]$ and $V_2 = [v_{2,i}]$ such that $a_{ij} = \log|\theta_j(b_{i-1})|$ for $1 \leq j \leq 5$ and $a_{i6} = 1$, and $v_{1,i} = \log|d_{1,i-1}|$ and $v_{2,i} = \log|d_{2,i-1}|$. With a calculator one sees that $A^{-1}V_1 \fallingdotseq {}^t[1\ 5\ 4\ 0\ 2\ 4.828]$ and $A^{-1}V_2 \fallingdotseq {}^t[1\ 5\ 4\ 2\ 0\ 4.828]$. This implies that $(r_{1,1}, r_{1,2}, r_{1,3}, r_{1,4}, r_{1,5}) = (1,5,4,0,2)$ and $(r_{2,1}, r_{2,2}, r_{2,3}, r_{2,4}, r_{2,5}) = (1,5,4,2,0)$. The values $d_{i,0}$ at $b = 3$ yield that $c_1 = d_{1,0}/(\theta_1(3)^1 \cdots \theta_5(3)^2) = -5^3$ and $c_2 = d_{2,0}/(\theta_1(3)^1 \cdots \theta_5(3)^0) = -5^3$. Indeed, in such a case one has $\log|c_1| = \log|c_2| = 4.8283\ldots$. Hence we have $d_1 = -5^3\theta_1\theta_2^5\theta_3^4\theta_5^2$ and $d_2 = -5^3\theta_1\theta_2^5\theta_3^4\theta_4^2$. Theorem 2.3 verifies $N = \mathbb{Q}(b, \sqrt{d_1}) = \mathbb{Q}(b, \sqrt{d_2}) = \mathbb{Q}(b, \sqrt{-5\theta_1\theta_2})$. □

As a specialization to $\mathbb{Q}$ we have

Corollary 3.4. *Let b be a rational number such that $f(X) = f_b^{\mathrm{KY2}}(X)$ is irreducible over $\mathbb{Q}$. Put $M = \mathrm{Spl}(f/\mathbb{Q})$ and $q_2(b) = -5(b-2)(3b-10)$. Then $q_2(b)$ is the square of a rational number if and only if M is a $\mathfrak{C}_5$-extension of $\mathbb{Q}$, that is, a cyclic quintic field. If $q_2(b)$ is not square, then M is a $\mathfrak{D}_5$-extension of $\mathbb{Q}$ containing a quadratic field $\mathbb{Q}(\sqrt{q_2(b)})$. In particular, when $b < 2$ or $b > 10/3$, the quadratic field $\mathbb{Q}(\sqrt{q_2(b)})$ is imaginary.*

Lemma 3.5. *For a rational number b, the value $q_2(b) = -5(b-2)(3b-10)$ is the square of a rational number if and only if $b = 2$ or $b = 2 + 4/(5t^2+3)$ for some rational number t.*

Proof. One has that $q_2(2) = 0$ and $q_2(2 + 4/(5t^2+3)) = 2^4 5^2 t^2/(5t^2+3)^2$. Conversely, if $q_2(b) = s^2$ with $b \neq 2$ and $s \in \mathbb{Q}$, then $-(3b-10)/(5b-10) = (s/(5b-10))^2 = t^2$, which implies $b = (10t^2+10)/(5t^2+3) = 2 + 4/(5t^2+3)$ for $t = s/(5b-10) \in \mathbb{Q}$. □

4. Quintic family by Brumer and Hashimoto

Brumer [1] and Hashimoto [5] (see also [3, Section 2.3] and [6]) give a $\mathbb{Q}$-generic $\mathfrak{D}_5$-polynomial

$f_{s,t}^{\mathrm{Br}}(X) = X^5 + (t-3)X^4 + (-t+s+3)X^3 + (t^2 - t - 2s - 1)X^2 + sX + t$

over $\mathbb{Q}(s,t)$ the field of rational functions over $\mathbb{Q}$ with two indeterminates s and t.

Proposition 4.1. *For $f(X) = f_{s,t}^{\mathrm{Br}}(X)$ let N be a unique subextension of the extension $M/\mathbb{Q}(s,t)$ with $[N : \mathbb{Q}(s,t)] = 2$ where $M = \mathrm{Spl}(f/\mathbb{Q}(s,t))$. Then the square root $\sqrt{-\theta_1}$ is a generator of N over $\mathbb{Q}(s,t)$ where*

$$\begin{aligned}\theta_1 = {}& 4t^5 - 4t^4 - (24s+40)t^3 - (s^2 - 34s - 91)t^2 \\ & +(30s^2 + 14s - 4)t + 4s^3 - s^2.\end{aligned}$$

Proof. Put $d = \mathrm{disc}_X f(X)$. With a calculator one sees that $d = \theta_1^2\theta_2^2$ where

$$\begin{aligned}\theta_1 = \theta_1(s,t) = {}& 4t^5 - 4t^4 - (24s+40)t^3 - (s^2 - 34s - 91)t^2 \\ & +(30s^2 + 14s - 4)t + 4s^3 - s^2\end{aligned}$$

and $\theta_2 = \theta_2(s,t) = t$. As for Propositions 3.1 and 3.3, by Theorem 2.3 and Lemma 2.4, the norms d_1 and d_2 are divisors of d in $\mathbb{Z}[s,t]$, that is, there exist integers c_i and $r_{i,j} \geq 0$ such that $d_i = c_i\theta_1^{r_{i,1}}\theta_2^{r_{i,2}}$. For example, with a calculator one can see that $\{d_1, d_2\} = \{-2^2 739, -739\}$, $\{-2^2 131, -131\}$ and $\{-2^4 1123, -1123\}$ at $(s,t) = (1,-2)$, $(1,2)$ and $(1,4)$, respectively. Note that $(\theta_1, \theta_2) = (739, -2)$, $(131, 2)$ and $(1123, 4)$ at $(s,t) = (1,-2)$, $(1,2)$ and $(1,4)$, respectively. Hence we conclude $d_1 = -\theta_1\theta_2^2$ and $d_2 = -\theta_1$. Theorem 2.3 verifies $N = \mathbb{Q}(s,t,\sqrt{d_1}) = \mathbb{Q}(s,t,\sqrt{d_2}) = \mathbb{Q}(s,t,\sqrt{-\theta_1})$. □

Remark. Proposition 4.1 described above is already known in [3, Section 2.3] and [6].

Remark. Since $f_{s,t}^{\mathrm{Br}}(X)$ is a $\mathbb{Q}$-generic $\mathfrak{D}_5$-polynomial, there exist rational functions $s_i(b)$ and $t_i(b)$ in $\mathbb{Q}(b)$ such that $\mathrm{Spl}(f_{s_i(b),t_i(b)}^{\mathrm{Br}}/\mathbb{Q}(b))$ is equal to $\mathrm{Spl}(f_b^{\mathrm{KY}i}/\mathbb{Q}(b))$ for each $i = 1, 2$. We find such functions as follows:

$$\begin{aligned}
s_1(b) &= -\frac{10(2322b^5 + 21204b^4 + 75545b^3 + 131460b^2 + 112100b + 37600)}{(b+2)(54b^2 + 225b + 230)^2}, \\
t_1(b) &= \frac{4(18b^2 + 50b + 35)}{54b^2 + 225b + 230}, \\
s_2(b) &= -\frac{5(9b^7 - 45b^6 - 78b^5 + 322b^4 + 334b^3 - 500b^2 - 200b + 400)}{(b-2)(3b^3 - 20b - 20)^2}, \\
t_2(b) &= \frac{9b^3 - 15b + 10}{3b^3 - 20b - 20}.
\end{aligned}$$

Then one has

$$-\theta_1(s_1(b),t_1(b)) = -\frac{2^2 5^6 (2b+5)(6b^2+15b+10)h_1(b)^2}{(b+2)^3(54b^2+225b+230)^6},$$
$$-\theta_1(s_2(b),t_2(b)) = -\frac{5^3(3b-10)(b^2+b-1)^2 h_2(b)^2}{(b-2)^3(3b^3-20b-20)^6}$$

where

$$h_1(b) = 2754b^6 + 24840b^5 + 88005b^4 + 153600b^3 + 133400b^2 + 48000b + 2000,$$
$$h_2(b) = 81b^8 - 333b^7 - 486b^6 + 2238b^5 + 1406b^4 - 3840b^3 - 400b^2 + 2400b - 800.$$

Hence we obtain the same assertions as Propositions 3.1 and 3.3. For the verification of the equalities $\mathrm{Spl}(f^{\mathrm{Br}}_{s_i(b),t_i(b)}/\mathbb{Q}(b)) = \mathrm{Spl}(f^{\mathrm{KY}i}_b/\mathbb{Q}(b))$, it is enough to check with a calculator that the resultant $\mathrm{Res}_X(f^{\mathrm{Br}}_{s_i(b),t_i(b)}(X), f^{\mathrm{KY}i}_b(X+Y)) \in \mathbb{Q}(b)[Y]$ decomposes into one irreducible polynomial of degree 5 and two irreducible polynomials of degree 10 over $\mathbb{Q}(b)$ for each $i = 1, 2$. Indeed, for two $\mathfrak{D}_5$-polynomials $g(X) = \prod_{i=1}^5 (X-\alpha_i)$ and $h(X) = \prod_{j=1}^5 (X-\beta_j)$ over K, the resultant $\mathrm{Res}_X(g(X), h(X+Y))$ is equal to $\prod_{i,j}(Y+\alpha_i-\beta_j)$, and the degree of $-\alpha_i+\beta_j$ over K is 1 or 5 if $K(\alpha_i) = K(\beta_j)$, 10 if $K(\alpha_i)$ and $K(\beta_j)$ are not equal but conjugate over K and 25 otherwise.

5. Odd dihedral families by Hashimoto and Miyake

Let n be an odd number greater than 1. Let ζ be a primitive n-th root of unity in $\mathbb{C}$, and put $\omega = \zeta + \zeta^{-1}$. For an integer i, we denote $\omega_i = \zeta^i + \zeta^{-i}$ and $\xi_i = (\zeta^i - \zeta^{-i})/(\zeta - \zeta^{-1}) \in \mathbb{Q}(\omega)$. Hashimoto and Miyake [4] (see also [3, Section 5.5]) give a $\mathbb{Q}(\omega)$-generic $\mathfrak{D}_n$-polynomial $f^{\mathrm{HM}}_t(X) = \Xi(X) + t$ with one indeterminate t where $\Xi(X) = \prod_{i=0}^{n-1}(X - \xi_i\xi_{i+1}) \in \mathbb{Q}(\omega)[X]$. Let $\overline{K}$ represent the algebraic closure of a field K. As a model over the function field $\mathbb{Q}(\omega, t)$ we have

Theorem 5.1 (Hashimoto-Miyake [4], cf. [3, Section 5.5])**.** *For a root λ of $f^{\mathrm{HM}}_t(X)$ in $\overline{\mathbb{Q}(\omega,t)}$, let us fix a root x of $X^2 - (\omega+\lambda^{-1})X + 1$ in $\overline{\mathbb{Q}(\omega,t)}$. Then we have $f^{\mathrm{HM}}_t(X) = \prod_{i=0}^{n-1}(X-\lambda_i)$ where $x_i = (-\xi_{i-1}x+\xi_i)/(-\xi_i x+\xi_{i+1})$ and $\lambda_i = x_i/(x_i^2 - \omega x_i + 1)$. In particular, we have $\mathrm{Spl}(f^{\mathrm{HM}}_t/\mathbb{Q}(\omega,t)) = \mathbb{Q}(\omega,t,x)$ and $\mathrm{Gal}(f^{\mathrm{HM}}_t/\mathbb{Q}(\omega,t)) \simeq \mathfrak{D}_n$. The group $\mathrm{Gal}(f^{\mathrm{HM}}_t/\mathbb{Q}(\omega,t))$ is generated by σ and τ of order n and 2 with $\sigma\tau = \tau\sigma^{-1}$ where $\sigma^i(x) = x_i$ and $\tau(x) = 1/x$.*

Proposition 5.2. *For $f(X) = f^{\mathrm{HM}}_t(X)$ let N be a unique subextension of the extension $M/\mathbb{Q}(\omega,t)$ with $[N : \mathbb{Q}(\omega,t)] = 2$ where $M = \mathrm{Spl}(f/\mathbb{Q}(\omega,t))$. Then the square root $\sqrt{-\theta_1\theta_2}$ is a generator of N over $\mathbb{Q}(\omega,t)$ where $\theta_1 = t$ and $\theta_2 = (4-\omega^2)^n t + 4$.*

Proof. Let notation be as in Theorem 5.1. Theorem 2.3 implies that the irreducible factorization of $f(X)$ over $\mathbb{Q}(\omega,t,\lambda)$ is of the form $f(X) = (X -$

$\lambda)\prod_{i=1}^{(n-1)/2} f_i(X)$. We calculate the explicit form of $f_i(X)$. Since $\xi_{-1}=-1$, $\xi_0=0$ and $\xi_1=1$, one has that $x_0=x$ and $\lambda_0=\lambda$. The relation $x_i=\sigma^i(x)$ implies that $\lambda_i=\sigma^i(\lambda)$. The relations $\tau(x)=1/x$ and $\xi_{n-i}=-\xi_i$ yield $\tau(x_i)=1/x_{n-i}$ and $\tau(\lambda_i)=\lambda_{n-i}$. Thus we may have $f_i(X)=(X-\lambda_i)(X-\lambda_{n-i})$ for each $i=1,\dots,(n-1)/2$. Note that $x_i-\zeta^{\pm 1}=\zeta^{\pm i}(x-\zeta^{\pm 1})/(-\xi_i x+\xi_{i+1})$, respectively. Thus λ_i and λ_{n-i} have representations

$$\begin{aligned}\lambda_i &= \frac{x_i}{(x_i-\zeta)(x_i-\zeta^{-1})} = \frac{(-\xi_{i-1}x+\xi_i)(-\xi_i x+\xi_{i+1})}{x^2-\omega x+1},\\ \lambda_{n-i} &= \tau(\lambda_i) = \frac{(-\xi_{i-1}x^{-1}+\xi_i)(-\xi_i x^{-1}+\xi_{i+1})}{x^{-2}-\omega x^{-1}+1}\\ &= \frac{(-\xi_{i+1}x+\xi_i)(-\xi_i x+\xi_{i-1})}{x^2-\omega x+1},\end{aligned}$$

respectively. Consider the discriminant δ_i of $f_i(X)$ and its norm d_i. By the relation $\xi_{i+1}-\xi_{i-1}=\omega_i$, the difference $\lambda_i-\lambda_{n-i}$ is $\lambda_i-\lambda_{n-i}=-\xi_i\omega_i(x^2-1)/(x^2-\omega x+1)$. The relation $x+x^{-1}=\omega+\lambda^{-1}$ implies that

$$\begin{aligned}\delta_i &= \operatorname{disc}_X f_i(X) = (\lambda_i-\lambda_{n-i})^2 = \xi_i^2\omega_i^2\frac{(x+x^{-1})^2-4}{(x+x^{-1}-\omega)^2}\\ &= \xi_i^2\omega_i^2((\omega+2)\lambda+1)((\omega-2)\lambda+1).\end{aligned}$$

Here one can see that $\xi_i\xi_{i+1}+1/(\omega\pm 2)=(\omega_{2i+1}\mp 2)/(\omega^2-4)$, $\prod_{i=0}^{n-1}(\omega_{2i+1}+2)=4$ and $\prod_{i=0}^{n-1}(\omega_{2i+1}-2)=0$. Thus the norms $\nu((\omega\pm 2)\lambda+1)$ of $(\omega\pm 2)\lambda+1$ from $\mathbb{Q}(\omega,t,\lambda)$ to $\mathbb{Q}(\omega,t)$ are

$$\begin{aligned}\nu((\omega+2)\lambda+1) &= \nu(-(\omega+2))\nu\Big(-\frac{1}{\omega+2}-\lambda\Big) = -(\omega+2)^n f\Big(-\frac{1}{\omega+2}\Big)\\ &= -(\omega+2)^n\Big(t+\prod_{i=0}^{n-1}\Big(-\frac{1}{\omega+2}-\xi_i\xi_{i+1}\Big)\Big)\\ &= -(\omega+2)^n\Big(t+(-1)^n\prod_{i=0}^{n-1}\frac{\omega_{2i+1}-2}{\omega^2-4}\Big) = -(\omega+2)^n t,\\ \nu((\omega-2)\lambda+1) &= -(\omega-2)^n\Big(t-\frac{4}{(\omega^2-4)^n}\Big),\end{aligned}$$

respectively. Hence the norm d_i of δ_i from $\mathbb{Q}(\omega,t,\lambda)$ to $\mathbb{Q}(\omega,t)$ is equal to

$$\begin{aligned}d_i &= \nu(\delta_i) = \xi_i^{2n}\omega_i^{2n}(\omega+2)^n(\omega-2)^n t\Big(t-\frac{4}{(\omega^2-4)^n}\Big)\\ &= -\xi_i^{2n}\omega_i^{2n}t((4-\omega^2)^n t+4) = -\xi_i^{2n}\omega_i^{2n}\theta_1\theta_2.\end{aligned}$$

Theorem 2.3 verifies $N=\mathbb{Q}(\omega,t,\sqrt{d_i})=\mathbb{Q}(\omega,t,\sqrt{-\theta_1\theta_2})$. □

Remark. By $|\omega|<2$, the coefficient $(4-\omega^2)^n$ of t in θ_2 is positive. Thus $\mathbb{Q}(\omega,\sqrt{-\theta_1\theta_2})$ is totally imaginary when $t\in\mathbb{Q}(\omega)$ is totally positive.

Corollary 5.3. *The discriminant* $\mathrm{disc}_X f^{\mathrm{HM}}(X)$ *of* $f^{\mathrm{HM}}(X)$ *is equal to* $n^n(\omega^2-4)^{-n(n-1)/2}t^{(n-1)/2}((4-\omega^2)^n t+4)^{(n-1)/2}$.

Proof. Theorem 2.3 implies $\mathrm{disc}_X f^{\mathrm{HM}}(X) = \prod_{i=1}^{(n-1)/2} d_i$ where d_i are the norms in the proof of Proposition 5.2. Due to the relations $\prod_{i=1}^{(n-1)/2}(-\xi_i^2) = n(\omega^2-4)^{-(n-1)/2}$ and $\prod_{i=1}^{(n-1)/2}\omega_i^2 = 1$, we conclude $\prod_{i=1}^{(n-1)/2} d_i = n^n(\omega^2-4)^{-n(n-1)/2}t^{(n-1)/2}((4-\omega^2)^n t+4)^{(n-1)/2}$. □

Acknowledgement

The author would like to thank Professor Miho Aoki for the information of Williamson's paper at the second section and Professor Akinari Hoshi for the suggestion to calculate the quadratic generator of Kishi and Yamada's families $f_b^{\mathrm{KY}i}(X)$ via Brumer and Hashimoto's polynomial $f_{s,t}^{\mathrm{Br}}(X)$ as described at the fourth section. The author would like to thank the referee for his/her careful reading and for giving many valuable comments.

References

[1] A. Brumer, Curves with real multiplication, in preparation.

[2] J. Cremona, *The elliptic curve database for conductors to 130000*, ANTS-VII Proceedings, Lecture Notes in Computer Science **4076** (2006) 11–29.

[3] C.U. Jensen, A. Ledet and N. Yui, Generic polynomials, Constructive aspects of the inverse Galois problem, Mathematical Sciences Research Institute Publications **45** Cambridge University Press, Cambridge (2002).

[4] K. Hashimoto and K. Miyake, *Inverse Galois problem for dihedral groups*, Number theory and its applications. Proceedings of the conference held at the RIMS, Kyoto, Japan, November 10-14, 1997. Kluwer Academic Publishers. Dev. Math. **2** (1999) 165–181.

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

[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 **79** No. 9 (2003) 142–145.

[7] Y. Kishi and M. Yamada, *Construction of families of dihedral quintic polynomials*, Math. J. Okayama Univ. **66** (2024) 63–69.

[8] The LMFDB Collaboration, *The L-functions and modular forms database*, `https://www.lmfdb.org`, 2025.

[9] Maple, Maplesoft, a division of Waterloo Maple Inc., Waterloo, Ontario.

[10] The PARI Group, *PARI/GP version 2.17.2*, Univ. Bordeaux, 2025, `http://pari.math.u-bordeaux.fr/`

[11] C.J. Williamson, *Odd degree polynomials with dihedral Galois groups*, J. Number Theory **34** No. 2 (1990) 153–173.

[12] Wolfram Research, Inc., *Mathematica, Version 14.2*, Champaign, IL, 2025, `https://www.wolfram.com/mathematica`

Toru Komatsu
Department of Mathematics
Faculty of Science and Technology
Tokyo University of Science
2641 Yamazaki, Noda-shi, Chiba-ken, 278-8510, Japan
e-mail address: komatsutoru.math@gmail.com

(*Received December 26, 2024*)
(*Accepted March 5, 2025*)