Math. J. Okayama Univ. **66** (2024), 63–69

CONSTRUCTION OF FAMILIES OF DIHEDRAL QUINTIC POLYNOMIALS

Yasuhiro Kishi and Mei Yamada

Abstract. In this article, we give two families of dihedral quintic polynomials by using the Weber sextic resolvent and a certain elliptic curve.

1. Introduction

Let $\mathbb{Q}$ be the field of rational numbers. For $f(X) \in \mathbb{Q}[X]$, denote $\mathrm{Gal}(f/\mathbb{Q})$ the galois group of the minimal splitting field of f over $\mathbb{Q}$. If f is quintic and irreducible over $\mathbb{Q}$, then $\mathrm{Gal}(f/\mathbb{Q})$ is isomorphic to C_5 (the cyclic group of order 5), D_5 (the dihedral group of order 10), F_5 (the Frobenius group of order 20), A_5 (the alternating group of degree 5) or S_5 (the symmetric group of degree 5). The aim of this paper is to construct families of quintic polynomials with rational coefficients whose galois groups are isomorphic to D_5.

On the one hand, as is well known, any galois extensions of $\mathbb{Q}$ whose galois groups are isomorphic to D_5 are given as the minimal splitting fields of the quintic polynomial

$$f(X) = X^5 + (t-3)X^4 + (s-t+3)X^3 + (t^2-t-2s-1)X^2 + sX + t \in \mathbb{Q}[X]$$

([2, Theorem 2.3.5]), which is called Brumer's polynomial. This is a generic polynomial for D_5. On the other hand, the following results are known when restricting the form of the polynomial. As for a quintic binomial $f(X) = X^5 + a \in \mathbb{Q}[X]$, $\mathrm{Gal}(f/\mathbb{Q})$ is isomorphic to not D_5 but always F_5 if f is irreducible over $\mathbb{Q}$ (see, for example, [2, Theorem 2.3.4]). As for a quintic trinomial $f(X) = X^5 + aX^i + b \in \mathbb{Q}[X]$, in case of $i = 1$ (essentially the same in case of $i = 4$), $\mathrm{Gal}(f/\mathbb{Q})$ is isomorphic to D_5 if and only if the following three conditions holds: (i) f is irreducible over $\mathbb{Q}$; (ii) the discriminant of f is a perfect square in $\mathbb{Q}$; (iii) a and b are of the following form:

$$a = \frac{5^5\lambda\mu^4}{(\lambda-1)^4(\lambda^2-6\lambda+25)}, \quad b = a\mu \ (\lambda, \mu \in \mathbb{Q},\ \lambda \neq 1,\ \mu \neq 0)$$

([5, §189], [3, Theorem II.3.4], [2, Theorem 2.3.4]). In case of $i = 2$ (essentially the same in case of $i = 3$), $\mathrm{Gal}(f/\mathbb{Q})$ is isomorphic to D_5 essentially only when

$$(a, b) = (5, 3), (5, -15), (25, 300)$$

Mathematics Subject Classification. Primary 11R09; Secondary 11R32.

Key words and phrases. Quintic polynomials, Galois group.

([4, Theorem 3]). This is shown by using the elliptic curve

$$Y^2 = X^3 + 14X^2 + 625X.$$

In this paper, we treat the following quintic tetranomials:

$$f_{a,b,\mu}(X) := X^5 + abX^3 + a^2X + a^3\mu \in \mathbb{Q}[X] \ (a, b, \mu \in \mathbb{Q}^\times).$$

We note that the discriminant $disc(f_{a,b,\mu})$ of $f_{a,b,\mu}$ is

$$disc(f_{a,b,\mu}) = a^{10}\{5^5\mu^4a^2 + 4(27b^4 - 225b^2 + 500)b\mu^2a + 16(b+2)^2(b-2)^2\}.$$

Theorem 1. *For $b, \mu \in \mathbb{Q}^\times$, we define $a_i(b, \mu) \in \mathbb{Q}$ $(i \in \{1, 2\})$ by*

$$a_i(b,\mu) := \begin{cases} \dfrac{144(b+2)^2(2b+5)(6b^2+15b+10)}{5^4\mu^2} & \text{if } i = 1, \\ \dfrac{b^2(b-2)^2(3b+5)^2(3b-10)}{5^5(b^2+b-1)\mu^2} & \text{if } i = 2, \end{cases} \tag{1}$$

and put $a_i := a_i(b, \mu)$, for brevity. Assume that $f_{a_i,b,\mu}$ is irreducible over $\mathbb{Q}$. Then the galois group $\mathrm{Gal}(f_{a_i,b,\mu}/\mathbb{Q})$ is isomorphic to C_5 or D_5, especially for $b > 0$ (resp. $b > 10/3$), $\mathrm{Gal}(f_{a_1,b,\mu}/\mathbb{Q})$ (resp. $\mathrm{Gal}(f_{a_2,b,\mu}/\mathbb{Q})$) is isomorphic to D_5.

Remark 1. It is known that the polynomial

$$f(X) = X^5 + sX^3 + tX^2 + t \in \mathbb{Q}[X]$$

is a generic polynomial for S_5 over $\mathbb{Q}$. Our polynomial $f_{a,b,1/a}$ is obtained from such f as $s = ab$ and $t = a^2$.

2. Weber sextic resolvent and two criteria

In this section, we introduce two criteria to determine the galois group. Now we define the Weber sextic resolvent which is a key ingredient of the proof of Theorem 1.

Definition ([2, Definition 2.3.2])**.** For a quintic polynomial $f(X) = X^5 + a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$ $(a_i \in \mathbb{Q})$, define the *Weber sextic resolvent* $G(Z)$ of f by

$$G(Z) := (Z^3 + b_4Z^2 + b_2Z + b_0)^2 - 2^{10}dZ \in \mathbb{Q}[Z],$$

where

$$\begin{aligned} b_0 = &-64a_2^4 - 176a_3^2a_1^2 + 28a_3^4a_1 - 16a_4^2a_3^2a_2^2 - 1600a_4^2a_0^2 - 64a_4a_2a_1^2 \\ &- 80a_3^2a_2a_0 + 384a_4^3a_1a_0 + 640a_4a_2^2a_0 - 192a_4^2a_3a_2a_0 \\ &- 1600a_2a_1a_0 - 128a_4^2a_2^2a_1 + 48a_4a_3^3a_0 - 640a_4a_3a_1a_0 \\ &+ 64a_4^3a_3a_2a_1 + 64a_4a_3a_2^3 + 224a_4^2a_3a_1^2 + 224a_3a_2^2a_1 \\ &+ 8a_4a_3^4a_2 - 112a_4a_3^2a_2a_1 - 16a_4^2a_3^3a_1 - 16a_3^3a_2^2 - 64a_4^4a_1^2 \end{aligned}$$

$$
\begin{aligned}
&+ 4000a_3a_0^2 - a_3^6 + 320a_1^3,\\
b_2 &= 3a_3^4 - 16a_4a_3^2a_2 + 16a_4^2a_2^2 + 16a_4^2a_3a_1 - 64a_4^3a_0 + 16a_3a_2^2\\
&\quad - 8a_3^2a_1 - 112a_4a_2a_1 + 240a_4a_3a_0 + 240a_1^2 - 400a_2a_0,\\
b_4 &= -3a_3^2 + 8a_4a_2 - 20a_1,\\
d &= disc(f).
\end{aligned}
$$

Then the following holds:

Proposition 1 ([2, Theorem 2.3.3])**.** *For an irreducible quintic polynomial $f(X) \in \mathbb{Q}[X]$, the Weber sextic resolvent $G(Z)$ of f has a rational root if and only if* $\mathrm{Gal}(f/\mathbb{Q})$ *is a solvable group, that is,* $\mathrm{Gal}(f/\mathbb{Q})$ *is isomorphic to C_5, D_5 or F_5.*

Moreover, the following holds in general:

Proposition 2. *For an irreducible polynomial $f(X) \in \mathbb{Q}[X]$ of degree n, the discriminant of f is a perfect square in $\mathbb{Q}$ if and only if* $\mathrm{Gal}(f/\mathbb{Q})$ *is isomorphic to a subgroup of A_n, especially for* $n = 5$, $\mathrm{Gal}(f/\mathbb{Q})$ *is isomorphic to C_5, D_5 or A_5.*

Proof. See, for example, [1, Proposition 6.3.1]. □

3. Proof and Remarks

First, we treat the following quintic tetranomial:

$$f(X) = X^5 + abX^3 + a^2cX + a^3\mu \ (a, b, c, \mu \in \mathbb{Q}^\times).$$

Then the Weber sextic resolvent $G(Z)$ of f is

$$
\begin{aligned}
G(Z) = Z^6 &+ 2(-3b^2 - 20c)a^2Z^5 + (15b^4 + 104b^2c + 880c^2)a^4Z^4\\
&+ 4\{2000b\mu^2a + (-5b^6 - 4b^4c - 368b^2c^2 - 2240c^3)\}a^6Z^3\\
&+ \{8000(-3b^2 - 20c)b\mu^2a\\
&\qquad + (15b^8 - 176b^6c + 1440b^4c^2 + 1280b^2c^3 + 44800c^4)\}a^8Z^2\\
&+ 2\{-1600000\mu^4a^2 + 32(-1353b^4 + 13400b^2c - 2000c^2)b\mu^2a\\
&\qquad + (-3b^{10} + 92b^8c - 992b^6c^2\\
&\qquad\qquad + 896b^4c^3 + 20736b^2c^4 - 54272c^5)\}a^{10}Z\\
&+ \{16000000b^2\mu^4a^2 + 8000(-b^6 + 28b^4c - 176b^2c^2 + 320c^3)b\mu^2a\\
&\qquad + (b^{12} - 56b^{10}c + 1136b^8c^2 - 10496b^6c^3\\
&\qquad\qquad + 48896b^4c^4 - 112640b^2c^5 + 102400c^6)\}a^{12}.
\end{aligned}
$$

Moreover, for $b, c \in \mathbb{Q}^\times$, we define the elliptic curve $C_{b,c}$ by

$$C_{b,c} : Y^2 = X^3 + 2(7b^2 - 60c)X^2 + 625(b^4 - 8b^2c + 16c^2)X.$$

Furthermore, for $b, c, s \in \mathbb{Q}$, we define three rational numbers $A(b, c, s)$, $B(b, c, s)$, $C(b, c, s)$ by

$$\begin{aligned} A(b, c, s) &= -2^{10}5^{10}(s - 25b^2), \\ B(b, c, s) &= 2^6 5^5 b\{5s^3 - 25(3b^2 + 20c)s^2 - (1353b^4 - 13400b^2c + 2000c^2)s \\ &\qquad - 625(b^6 - 28b^4c + 176b^2c^2 - 320c^3)\}, \\ C(b, c, s) &= \{s^2 - 10(b^2 + 4c)s + 25(b^4 - 8b^2c + 16c^2)\}^2 \\ &\qquad \times \{s^2 - 10(b^2 + 12c)s + 25(b^4 - 40b^2c + 400c^2)\}. \end{aligned}$$

By straightforward calculations, we get two equalities

$$5^6 G(a^2s/5) = a^{12}\{A(b, c, s)\mu^4a^2 + B(b, c, s)\mu^2a + C(b, c, s)\} \tag{2}$$

and

$$\begin{aligned} &B(b, c, s)^2 - 4A(b, c, s)C(b, c, s) \\ &\quad = 2^{12}5^{10}\{s^2 - 2(11b^2 + 20c)s - (59b^4 - 840b^2c - 400c^2)\}^2 \\ &\qquad \times \{s^3 + 2(7b^2 - 60c)s^2 + 625(b^4 - 8b^2c + 16c^2)s\}. \end{aligned} \tag{3}$$

Proposition 3. *Let $a, b, c, \mu \in \mathbb{Q}^\times$. If the Weber sextic resolvent $G(Z)$ of $f(X) = X^5 + abX^3 + a^2cX + a^3\mu$ has a rational root $Z = r$, then r can be expressed as $r = a^2s/5$ such that s is the X-coordinate of a certain rational point of $C_{b,c}$, and $a \in \mathbb{Q}^\times$ satisfies the equation*

$$A(b, c, s)\mu^4a^2 + B(b, c, s)\mu^2a + C(b, c, s) = 0. \tag{4}$$

Conversely, let $b, c, \mu \in \mathbb{Q}^\times$ and s the X-coordinate of a rational point of $C_{b,c}$. Then numbers a satisfying (4) are rational, and the Weber sextic resolvent $G(Z)$ of $f(X) = X^5 + abX^3 + a^2cX + a^3\mu$ has a rational root $Z = a^2s/5$.

Proof. Let $a, b, c, \mu \in \mathbb{Q}^\times$, and assume that the Weber sextic resolvent $G(Z)$ of $f(X) = X^5 + abX^3 + a^2cX + a^3\mu$ has a rational root $Z = r$. Noting that $a \neq 0$, we put

$$s := 5r/a^2.$$

Then by (2), we have

$$0 = 5^6G(r) = 5^6G(a^2s/5) = a^{12}\{A(b, c, s)\mu^4a^2 + B(b, c, s)\mu^2a + C(b, c, s)\}, \tag{5}$$

and hence $a \in \mathbb{Q}^\times$ satisfies (4). Thus it is sufficient to show that s is the X-coordinate of a certain rational point of $C_{b,c}$. If $s \neq 25b^2$, then we have

$A(b,c,s) \neq 0$. Solving (4) for a, we have

$$a = \frac{-B(b,c,s) \pm \sqrt{B(b,c,s)^2 - 4A(b,c,s)C(b,c,s)}}{2A(b,c,s)\mu^2}.$$

Since a is rational, it must hold that $B(b,c,s)^2 - 4A(b,c,s)C(b,c,s) \in \mathbb{Q}^2$. Hence by (3), there exists $t \in \mathbb{Q}$ such that

$$t^2 = s^3 + 2(7b^2 - 60c)s^2 + 625(b^4 - 8b^2c + 16c^2)s.$$

Then $(X,Y) = (s,t)$ is a rational point of $C_{b,c}$. If $s = 25b^2$, then we can verify that $(X,Y) = (s, 100b(2b^2 - 5c))$ is a rational point of $C_{b,c}$.

Conversely, let $b, c, \mu \in \mathbb{Q}^\times$, s the X-coordinate of a rational point of $C_{b,c}$, and $a \in \mathbb{C}$ satisfying (4). If $A(b,c,s) = 0$, it is clear that $a \in \mathbb{Q}$. If $A(b,c,s) \neq 0$, we obtain $a \in \mathbb{Q}$ by (3). Moreover, it follows from (2) and (4) that $G(a^2s/5) = 0$. □

Proof of Theorem 1. For $b, \mu \in \mathbb{Q}^\times$, we define $a_i := a_i(b,\mu) \in \mathbb{Q}$ $(i \in \{1,2\})$ by (1). First, we can verify that the discriminants $disc(f_{a_i,b,\mu})$ of $f_{a_i,b,\mu}$ for $i \in \{1,2\}$ are both perfect squares:

$$disc(f_{a_1,b,\mu}) = \frac{2^4a^{10}(b+2)^2(18b^2+50b+35)^2(54b^2+225b+230)^2}{5^4},$$
$$disc(f_{a_2,b,\mu}) = \frac{a^{10}(b-2)^2(3b^3-20b-20)^2(9b^3-15b+10)^2}{5^4(b^2+b-1)^2}.$$

Next, we consider two rational points

$$(X,Y) = (5^3(b+2)^2, 2^25^3(b+2)^2(3b+5)), (5(b-2)^2, 2^25(b-2)^2(3b+5))$$

of $C_{b,1}$. By putting $s_1 := 5^3(b+2)^2$, $s_2 := 5(b-2)^2$ and by straightforward calculations, we have the following equality:

$$A(b,1,s_i)\mu^4a_i^2 + B(b,1,s_i)\mu^2a_i + C(b,1,s_i) = 0.$$

Then $a = a_i$ satisfies (4). Hence by Proposition 3, the Weber sextic resolvent $G(Z)$ of $f_{a_i,b,\mu}$ has a rational root. By Propositions 1 and 2, therefore, $\mathrm{Gal}(f_{a_i,b,\mu}/\mathbb{Q})$ is isomorphic to C_5 or D_5 if $f_{a_i,b,\mu}$ is irreducible over $\mathbb{Q}$.

Now assume $b > 0$ (resp. $b > 10/3$). Then we easily see $a_1 > 0$ (resp. $a_2 > 0$), and hence

$$f'_{a_i,b,\mu}(x) = 5x^4 + 3a_ibx^2 + a_i^2 > 0$$

for any real number x. Thus $f_{a_i,b,\mu}$ has non-real roots which implies that $\mathrm{Gal}(f_{a_i,b,\mu}/\mathbb{Q})$ contains the complex conjugate involution. Therefore, $\mathrm{Gal}(f_{a_i,b,\mu}/\mathbb{Q})$ is not isomorphic to C_5. The proof of Theorem 1 is now completed. □

Remark 2. Since

$$f_{a_i(b,\mu),b,\mu}(X) = \frac{1}{\mu^5} f_{a_i(b,1),b,1}(\mu X),$$

the minimal splitting fields of $f_{a_i(b,\mu),b,\mu}$ over $\mathbb{Q}$ for $\mu \in \mathbb{Q}^\times$ are all the same.

Remark 3. (1) There are some examples in which the galois group $\mathrm{Gal}(f_{a_2,b,\mu}/\mathbb{Q})$ is isomorphic to C_5 in the case $b < 10/3$. For instance, let $b = 5/2$, $\mu = 5/(2^3 31)$ (resp. $b = 13/4$, $\mu = 13 \cdot 59/(2^6 5^2 41)$). Then we have

$$a_2 = a_2(b,\mu) = -62 \quad (\text{resp. } a_2 = a_2(b,\mu) = -164)$$

and

$$f_{a_2,b,\mu}(X) = X^5 - 155X^3 + 3844X - 4805$$
$$(\text{resp. } f_{a_2,b,\mu}(X) = X^5 - 533X^3 + 26896X - \frac{1289327}{25}).$$

By using GP/PARI, we see that $f_{a_2,b,\mu}$ are irreducible over $\mathbb{Q}$ and $\mathrm{Gal}(f_{a_2,b,\mu}/\mathbb{Q})$ are isomorphic to C_5 in these cases. The authors have not yet found any examples in which $\mathrm{Gal}(f_{a_1,b,\mu}/\mathbb{Q})$ is isomorphic to C_5.

(2) As we have seen in the end of proof of Theorem 1, the minimal splitting field of $f_{a_1,b,\mu}$ (resp. $f_{a_2,b,\mu}$) over $\mathbb{Q}$ is never contained in the field $\mathbb{R}$ of real numbers under the condition $b > 0$ (resp. $b > 10/3$). Here, we give some examples where it is with $b < 0$ (resp. $b < 10/3$). Let $b = -9/4$, $\mu = 3/(2^2 5^2)$ (resp. $b = 3$, $\mu = 2 \cdot 3 \cdot 7/(5^3 11)$). Then we have

$$a_1 = a_1(b,\mu) = 53 \quad (\text{resp. } a_2 = a_2(b,\mu) = -55)$$

and

$$f_{a_1,b,\mu}(X) = X^5 - \frac{477}{4}X^3 + 2809X + \frac{446631}{100}$$
$$(\text{resp. } f_{a_2,b,\mu}(X) = X^5 - 165X^3 + 3025X - 5082).$$

We can verify that $f_{a_1,b,\mu}$ (resp. $f_{a_2,b,\mu}$) has five real roots, which are in the range $(-10,-9)$, $(-5,-4)$, $(-2,-1)$, $(7,8)$ and $(8,9)$ (resp. $(-12,-11)$, $(-6,-5)$, $(2.4,2.5)$, $(2.6,2.7)$ and $(12,13)$). Moreover, we see by using GP/PARI that $\mathrm{Gal}(f_{a_i,b,\mu}/\mathbb{Q})$ are isomorphic to D_5 in these cases. Thus the minimal splitting fields of $f_{a_i,b,\mu}$ over $\mathbb{Q}$ are both contained in $\mathbb{R}$.

Acknowledgement

The authors would like to thank the referee for his/her careful reading and for giving many valuable comments.

References

[1] H. Cohen, "A course in computational algebraic number theory," Graduate Texts in Mathematics, 138, Springer-Verlag, Berlin, 1993.

[2] 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.

[3] C. U. Jensen and N. Yui, *Polynomials with D_p as Galois group*, J. Number Theory, **15**, no. 3 (1982), 347–375.

[4] B. K. Spearman and K. S. Williams, *On solvable quintics X^5+aX+b and X^5+aX^2+b*, Rocky Mountain J. Math., **26**, no. 2 (1996), 753–772.

[5] H. Weber, "Lehrbuch der Algebra, Zweite Auflage," Friedrrich Vieweg und Sohn, Braunschweig, 1898.

Yasuhiro Kishi
Department of Mathematics,
Faculty of Education
Aichi University of Education
Kariya, Aichi, 448-8542, Japan
e-mail address: ykishi@auecc.aichi-edu.ac.jp

Mei Yamada
Department of Mathematics,
Faculty of Education
Aichi University of Education
Kariya, Aichi, 448-8542, Japan
e-mail address: 3ta96s913@gmail.com

(*Received March 29, 2022*)
(*Accepted July 14, 2023*)