TOKYO J. MATH.
VOL. 28, NO. 1, 2005

Geometric Generalization of Gaussian Period Relations with Application to Noether's Problem for Meta-Cyclic Groups

Ki-ichiro HASHIMOTO and Akinari HOSHI

Waseda University

Abstract. We study Noether's problem over $\mathbf{Q}$ for meta-cyclic groups. This paper is an extension of the previous work [2], which was concerned with the cyclic group C_n of order n. We shall give a simple description of the action of the normalizer of C_n in S_n to the function field $\mathbf{Q}(x_1, \cdots, x_n)$, in terms of the generators of the fixed field of C_n given in [2]. Using this, we settle Noether's problem for the dihedral group of order $2n$ ($n \leq 6$) and the Frobenius group of order 20 with explicit construction of independent generators of the fixed fields. We shall also reconstruct some simple one-parameter families of cyclic and dihedral polynomials.

1. Introduction

Let $K = \mathbf{Q}(x_1, \cdots, x_n)$ be the field of rational functions in n variables on which the symmetric group S_n of degree n acts through the permutation of the variables. The problem with which we are concerned is to determine whether, for a transitive subgroup G of S_n, the subfield K^G consisting of the G-invariant elements of K is again a rational function field over $\mathbf{Q}$ or not. This is called Noether's problem for G (over $\mathbf{Q}$) and has been one of the central problems in Galois theory (cf. [14],[25], [3]). In the case K^G is known to be rational, it is important to construct a set of independent generators of $K^G = \mathbf{Q}(t_1, \cdots, t_n)$ over $\mathbf{Q}$ explicitly, because one obtain from this a $\mathbf{Q}$-generic G-polynomial (cf. [3]) with parameters $t_1, \cdots, t_n$, which can be applied to various problems in number theory when the generators are chosen to be simple enough. In this context, we emphasize that our assumption on the constant field to be $\mathbf{Q}$ is fundamental.

For abelian groups, Noether's problem has been studied by various authors and a criterion under which it has an affirmative answer is known (cf. [8], [9]). In particular, for the cyclic group C_n of order n, Noether's problem over $\mathbf{Q}$ is known to have a negative answer for infinitely many n (e.g. $n = 8m$ ($m \in \mathbf{N}$), 47, 79, 113, 137, etc.), see [17],[1],[24],[8],[9],[25], [3]. On the other hand, very few is known for Noether's problem in the case of non abelian groups, except for the trivial case $G = S_n$ where the fixed field is generated by the elementary symmetric polynomials.

Received June 9, 2003; revised September 17, 2004
The first author is partly supported by the Grant-in-Aid for Scientific Research (B), No.15340015, Japan Society for the Promotion of Science.
The second author is supported by Grant-in-Aid for Scientific Research for JSPS Fellows.

We note that, regardless of the answer to Noether's problem, it is important to find a reasonable set of generators of K^G over $\mathbf{Q}$ and their (possible) relations, by several reasons. Obviously, it is often the first step to the solution of Noether's problem. Moreover, as it occurs in the present work, it is possible that if we do this for a normal subgroup H of G, then the description of the induced action of G/H on K^H becomes much simpler. The third reason is directly related to the possible description of the set of all G-extensions over an arbitrary field of characteristic 0, without assuming the existence of generic G-polynomials.

In this paper we study Noether's problem over $\mathbf{Q}$ for meta-cyclic groups. We shall settle, among others, Noether's problem for the dihedral group of order $2n$ ($n \leq 6$) and the Frobenius group of order 20 with *explicit* construction of independent generators of the fixed fields.

MAIN THEOREM. *Let G be the dihedral group of order $2n$ ($n \leq 6$) (resp. the Frobenius group F_{20} of order 20), which is regarded as a permutation group of order n (resp. 5). Then Noether's problem over $\boldsymbol{Q}$ for G has an affirmative answer. Namely we have*

$$\boldsymbol{Q}(x_1, \cdots, x_n)^G = \boldsymbol{Q}(f_1, \cdots, f_n), \quad f_1, \cdots, f_n \in \boldsymbol{Q}(x_1, \cdots, x_n)$$

where $n = 5$ for $G = F_{20}$.

The explicit form of the generators $f_1, \cdots, f_n$ will be given in the text.

The above result is obtained as follows. In the previous paper [2], we discussed a new approach, which is called *a geometric generalization of Gaussian period relations*, to study Noether's problem for the cyclic group C_n of order n. We obtained, among others, a system of generators $u_{i,j}$ ($0 \leq i, j \leq n-1$) for the fixed field K^{C_n}.

In the present paper, the group G is chosen to contain C_n as a normal subgroup such that G/C_n is a cyclic group. More generally, we consider the group of one-dimensional affine transformations over $\mathbf{Z}/n\mathbf{Z}$ which acts on $\mathbf{Q}(y_0, \cdots, y_{n-1})$ through the natural action on the indices of y_i's. Then we shall show in the key lemma of section 3 that the induced action of the quotient group by C_n on $K^{C_n} = \mathbf{Q}(u_{i,j} \mid 0 \leq i, j \leq n-1)$ has a remarkably simple description. Using this, we settle Noether's problem for each group G in the theorem by a case study with direct computaion. As application we shall reconstruct some "simple" one-parameter families of cyclic and dihedral polynomials.

The calculations in this paper were done by using computer manipulations with MAPLE and Mathematica [26] in Section 6.

2. Review of previous result

Here we describe briefly the idea of our approach by reviewing our previous work.

In [2], we discussed a new approach, which is called *a geometric generalization of Gaussian period relations*, to study Noether's problem in the case which G is the cyclic group C_n of order n. We gave, among others, explicit independent generators of the fixed field K^{C_n} ($n = 3, 4, 5$), from which we constructed a simple one-parameter family of polynomials with Galois group C_n ($3 \leq n \leq 7$) by specializing the parameters. This approach is

briefly described as follows (see [2] for details). Let $n \geq 2$ be a positive integer, $y_0, \cdots, y_{n-1}$ be independent variables, where the subscript of y is taken modulo n. Let σ be the cyclic permutation of $y_0, \cdots, y_{n-1}$, i.e. $\sigma : y_0 \mapsto y_1 \mapsto \cdots \mapsto y_{n-1} \mapsto y_0$. We define the $n \times n$ matrix R by the anti-circulant matrix

$$R := \begin{bmatrix} y_0 & y_1 & \cdots & y_{n-1} \\ y_1 & y_2 & \cdots & y_n \\ \vdots & \vdots & \ddots & \vdots \\ y_{n-1} & y_n & \cdots & y_{n-2} \end{bmatrix},$$

and denote by D the diagonal matrix $\mathrm{Diag}(y_0, \cdots, y_{n-1})$. We shall number the rows and columns of the matrices from 0 to $n-1$ to allow the use of residue classes modulo n. We see that the matrix R is invertible which enables us to make the following:

DEFINITION. We define the $n \times n$ matrix $U = [u_{i,j}]_{0 \leq i,j \leq n-1}$ by the equation

$$U := R\, D\, R^{-1}. \tag{1}$$

We call the entries $u_{i,j}$, $(0 \leq i, j \leq n-1)$ of the matrix U *the elementary cyclic elements of order* n.

The equation (1) is equivalent to the following system of relations, which is satisfied by Gaussian periods and cyclotomic numbers in cyclotomic fields (see [2]).

$$y_m\, y_{m+i} = \sum_{j=0}^{n-1} u_{i,j}\, y_{m+j}, \quad \text{for } 0 \leq m, i \leq n-1.$$

Hence the y_i's and the $u_{i,j}$'s are regarded as geometric analogues of Gaussian periods and cyclotomic numbers, respectively. This is the reason that we call our method using the elementary cyclic elements a geometric generalization of Gaussian period relations. We see that $u_{i,j} \in \mathbf{Q}(y_0, \cdots, y_{n-1})$ and $\sigma(u_{i,j}) = u_{i,j}$ for $0 \leq i, j \leq n-1$. Note that the $u_{i,j}$'s are homogeneous σ-invariants of degree one, i.e., they can be written as $u_{i,j} = f/g$ with $f, g \in \mathbf{Q}[y_0, \cdots, y_{n-1}]$ which are homogeneous and $\deg f - \deg g = 1$. The crucial fact in [2] is that the elementary cyclic elements $u_{i,j}$ generate the fixed field $\mathbf{Q}(y_0, \cdots, y_{n-1})^{C_n}$ over $\mathbf{Q}$ (see [2, Key lemma]). Namely we have

$$\mathbf{Q}(y_0, \cdots, y_{n-1})^{C_n} = \mathbf{Q}(u_{i,j} \mid 0 \leq i, j \leq n-1).$$

As a matter of fact, $\mathbf{Q}(y_0, \cdots, y_{n-1})$ is a root field of the characteristic polynomial of the matrix $U = [u_{i,j}]_{0 \leq i,j \leq n-1}$. Moreover, the elementary cyclic elements $u_{i,j}$ of order n satisfy the following properties (see [2, Proposition 3.2]).

$$u_{i,j} = u_{-i,j-i}, \quad (0 \leq i, j \leq n-1), \tag{2}$$

$$\sum_{i=0}^{n-1} u_{i,j} = \begin{cases} y_0 + y_1 + \cdots + y_{n-1} & \text{if } j \equiv 0 \mod n, \\ 0 & \text{if } j \not\equiv 0 \mod n, \end{cases} \tag{3}$$

$$\sum_{k=0}^{n-1} u_{i,k}\, u_{j-k,l-k} = \sum_{k=0}^{n-1} u_{j,k}\, u_{i-k,l-k}\,, \quad (0 \le i, j, l \le n-1)\,. \tag{4}$$

By using (2)–(4), for $n \ge 3$, we have

$$\mathbf{Q}(y_0, \cdots, y_{n-1})^{C_n} = \mathbf{Q}(u_{i,j} \mid 1 \le i \le j \le n-1)\,. \tag{5}$$

This means that we can always choose $n(n-1)/2$ generators of $\mathbf{Q}(y_0, \cdots, y_{n-1})^{C_n}$ over $\mathbf{Q}$. However since $n(n-1)/2 > n$ for $n > 3$, the equation (5) is not enough to give a solution of Noether's problem for C_n.

Therefore, in order to give an affirmative answer of this problem, one should show that $\mathbf{Q}(u_{i,j} \mid 1 \le i \le j \le n-1)$ is generated by exactly n independent rational functions over $\mathbf{Q}$.

In the previous paper [2], we gave a set of n generators of the fixed field $\mathbf{Q}(y_0, \cdots, y_{n-1})^{C_n}$ for $n = 3, 4, 5$ by using the elementary cyclic elements of order n as follows:

$$\mathbf{Q}(y_0, y_1, y_2)^{C_3} = \mathbf{Q}(u_{1,0}, u_{1,1}, u_{1,2})\,,$$

$$\mathbf{Q}(y_0, y_1, y_2, y_3)^{C_4} = \mathbf{Q}(u_{1,0}, u_{1,1}, u_{1,2}, u_{1,3})\,,$$

$$\mathbf{Q}(y_0, y_1, y_2, y_3, y_4)^{C_5} = \mathbf{Q}(u_{1,3} - u_{1,2}, u_{1,4} - u_{1,2}, u_{2,1} - u_{1,2}, u_{2,3} - u_{1,2}, u_{2,4} - u_{1,2})\,.$$

Note that the rationality and a set of generators for these fields has been known (c.f. [14], [12]). However, our method using the elementary cyclic elements $u_{i,j}$ has some advantages. Firstly we do not need a primitive n-th root of unity (cf. [12]), and a generating polynomial for the C_n-extension $\mathbf{Q}(y_0, \cdots, y_{n-1})/\mathbf{Q}(y_0, \cdots, y_{n-1})^{C_n}$ is obtained directly as the characteristic polynomial of the matrix U. This enables us to reconstruct simple one-parameter C_n-polynomials (e.g. whose constant term is equal to one) which have been discovered as Gaussian period polynomials by several authors (e.g. [7],[15], [21],[22]), see also [2]. Secondly, while in the original case of C_n-extensions of $\mathbf{Q}$ generated by Gaussian periods the C_n-fixed field $\mathbf{Q}$ admits no nontrivial group action, the field $\mathbf{Q}(y_0, \cdots, y_{n-1})$ generated by geometric generalization of Gaussian periods admits the action of meta-abelian groups which induces a nontrivial group action on the C_n-fixed field $\mathbf{Q}(y_0, \cdots, y_{n-1})^{C_n}$.

3. Induced action of G/C_n on K^{C_n} : Key Lemma

Let $\mathrm{Aff}(\mathbf{Z}/n\mathbf{Z})$ be the group of one-dimensional affine transformations $x \mapsto ax + b$ over $\mathbf{Z}/n\mathbf{Z}$. Namely we have

$$\mathrm{Aff}(\mathbf{Z}/n\mathbf{Z}) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \;\middle|\; a \in (\mathbf{Z}/n\mathbf{Z})^*, b \in \mathbf{Z}/n\mathbf{Z} \right\}.$$

The subgroup of $\mathrm{Aff}(\mathbf{Z}/n\mathbf{Z})$ consisting of the elements satisfying $a = 1$ (resp. $b = 0$) is identified with $\mathbf{Z}/n\mathbf{Z}$ (resp. $(\mathbf{Z}/n\mathbf{Z})^*$), so that we have

$$\mathrm{Aff}(\mathbf{Z}/n\mathbf{Z}) \;\cong\; (\mathbf{Z}/n\mathbf{Z}) \rtimes (\mathbf{Z}/n\mathbf{Z})^*\,.$$

By the above identification, each $\lambda \in (\mathbf{Z}/n\mathbf{Z})^*$ is associated to the permutation τ_λ of variables $y_0, \cdots, y_{n-1}$ satisfying

$$\tau_\lambda : y_i \mapsto y_{\lambda i}\,, \quad (0 \le i \le n-1)\,.$$

Note that $\tau_\lambda(y_0) = y_0$. Let F be a subgroup of $\mathrm{Aff}(\mathbf{Z}/n\mathbf{Z})$ which contains $\mathbf{Z}/n\mathbf{Z}$. Then we can write $F = (\mathbf{Z}/n\mathbf{Z}) \rtimes S$ with a subgroup $S \subseteq (\mathbf{Z}/n\mathbf{Z})^*$. Choosing a system of generators of S suitably, we can express F as $\langle\sigma\rangle \rtimes (\langle\tau_{\lambda_1}\rangle \times \cdots \times \langle\tau_{\lambda_r}\rangle)$. For example, the dihedral group D_n of order $2n$ is represented as $D_n = \langle\sigma\rangle \rtimes \langle\tau_{-1}\rangle$.

Now the important natural problem which arise here is to study the action of F on $\mathbf{Q}(y_0, \cdots, y_{n-1})$ defined through the permutation of the variables $y_0, \cdots, y_{n-1}$, and ask the Noether's problem in this setting. Since we have already a general description (5) for a system of generators of the fixed field $\mathbf{Q}(y_0, \cdots, y_{n-1})^{\langle\sigma\rangle}$ by the subgroup $C_n = \langle\sigma\rangle$, the problem is reduced to the study of the action of $S \cong F/C_n$ to $\mathbf{Q}(u_{i,j} \mid 0 \le i, j \le n-1)$. In particular we have $\mathbf{Q}(y_0, \cdots, y_{n-1})^F = \mathbf{Q}(u_{i,j} \mid 0 \le i, j \le n-1)^S$.

For the study of this field, the following lemma plays a fundamental role.

KEY LEMMA. *Let $F = (\mathbf{Z}/n\mathbf{Z}) \rtimes S$ be as above. Then the action of F on $\boldsymbol{Q}(y_0, \cdots, y_{n-1})$ defined by the permutation of $y_0, \cdots, y_{n-1}$ induces the action of S on $\boldsymbol{Q}(y_0, \cdots, y_{n-1})^{\langle\sigma\rangle} = \boldsymbol{Q}(u_{i,j} \mid 0 \le i, j \le n-1)$, and is given by*

$$\tau_\lambda : u_{i,j} \mapsto u_{\lambda^{-1}i,\lambda^{-1}j}\,, \quad (0 \le i, j \le n-1) \tag{6}$$

for each $\tau_\lambda \in S$.

PROOF. We take the $n \times n$ matrix $B_\lambda := [\delta_{\lambda i,j}]_{0 \le i,j \le n-1}$, where $\delta_{i,j}$ is the Kronecker's delta. For any $n \times n$ matrix $A = [a_{i,j}]_{0 \le i,j \le n-1}$, we have

$$B_\lambda A B_\lambda^{-1} = [a_{\lambda^{-1}i,\lambda^{-1}j}]_{0 \le i,j \le n-1}\,.$$

By the definition (1), we obtain that $U = RDR^{-1}$ and

$$\begin{aligned}
\tau_\lambda(R) &= \tau_\lambda(\left[y_{i+j}\right]_{0 \le i,j \le n-1}) = \left[y_{\lambda(i+j)}\right]_{0 \le i,j \le n-1} = B_\lambda R B_\lambda^{-1}\,,\\
\tau_\lambda(D) &= \tau_\lambda(\left[\delta_{i,j}\, y_i\right]_{0 \le i,j \le n-1}) = \left[\delta_{i,j}\, y_{\lambda i}\right]_{0 \le i,j \le n-1} = B_\lambda D B_\lambda^{-1}\,,\\
\tau_\lambda(R^{-1}) &= (\tau_\lambda(R))^{-1} = B_\lambda R^{-1} B_\lambda^{-1}\,.
\end{aligned}$$

Hence the assertion follows from

$$\tau_\lambda(U) = \tau_\lambda(R)\tau_\lambda(D)\tau_\lambda(R^{-1}) = B_\lambda U B_\lambda^{-1} = [u_{\lambda^{-1}i,\lambda^{-1}j}]_{0 \le i,j \le n-1}\,. \qquad \square$$

By using this result we shall give a set of independent generators of the fixed fields $\mathbf{Q}(x_1, \cdots, x_n)^{D_n}$ $(n = 3, 4, 5, 6)$ and $\mathbf{Q}(x_1, \cdots, x_5)^{F_{20}}$ explicitly, where $D_n = (\mathbf{Z}/n\mathbf{Z}) \rtimes \{\pm 1\}$ is the dihedral group of order $2n$ and $F_{20} = (\mathbf{Z}/5\mathbf{Z}) \rtimes (\mathbf{Z}/5\mathbf{Z})^*$ is the Frobenius group of order 20.

We need some more lemmas to study Noether's problem for the dihedral groups D_n.

LEMMA 1. *Let $K = \boldsymbol{Q}(x_1, \cdots, x_n)$ be the field of rational functions in n variables, and α be the linear $\boldsymbol{Q}$-automorphism of K of order two such that*

$$\alpha \ : \ x_i \mapsto -x_i \, , \quad (i = 1, \cdots, n) \, .$$

Then we have $K^{\langle \alpha \rangle} = \boldsymbol{Q}(x_1^2, x_1x_2, \cdots, x_1x_n)$.

PROOF. We have $K = \mathbf{Q}(x_1, x_1x_2, \cdots, x_1x_n)$ and $\alpha(x_1x_i) = x_1x_i$ for $i = 2, \cdots, n$. The assertion follows from this, since K is a quadratic extension of $\mathbf{Q}(x_1^2, x_1x_2, \cdots, x_1x_n)$ and $\mathbf{Q}(x_1^2, x_1x_2, \cdots, x_1x_n) \subseteq K^{\langle \alpha \rangle}$. □

LEMMA 2. *Let $K = \boldsymbol{Q}(a_1, \cdots, a_n, b_1, \cdots, b_n)$ be the field of rational functions in $2n$ independent variables, and β be the linear $\boldsymbol{Q}$-automorphism of K of order two such that*

$$\beta \ : \ a_i \ \mapsto \ b_i \ \mapsto \ a_i \, , \quad (i = 1, \cdots, n) \, .$$

Then we have $K^{\langle \beta \rangle} = \boldsymbol{Q}(a_1 + b_1, \cdots, a_n + b_n, (a_1 - b_1)^2, (a_1 - b_1)(a_2 - b_2), \cdots, (a_1 - b_1)(a_n - b_n))$.

PROOF. We make the following transformation of the variables.

$$\begin{cases} a_i' := a_i + b_i \, , & (i = 1, \cdots, n) \, , \\ b_i' := a_i - b_i \, , & (i = 1, \cdots, n) \, . \end{cases}$$

Then we clearly have $K = \mathbf{Q}(a_1', \cdots, a_n', b_1', \cdots, b_n')$, and β acts on K as

$$\beta \ : \ a_i' \mapsto a_i', \quad b_i' \mapsto -b_i' \, , \quad (i = 1, \cdots, n) \, .$$

It follows from Lemma 1 that $K^{\langle \beta \rangle} = \mathbf{Q}(a_1', \cdots, a_n', {b_1'}^2, b_1'b_2', \cdots, b_1'b_n')$. □

REMARK. We apply this for $\beta = \tau_{-1}$ and $D_n = \langle \sigma \rangle \rtimes \langle \tau_{-1} \rangle$. From (5) and Key lemma (6) it follows that for any n, $\mathbf{Q}(y_0, \cdots, y_{n-1})^{D_n}$ is generated by $n(n-1)/2$ elements.

We shall make the case study on the fixed field $\mathbf{Q}(y_0, \cdots, y_{n-1})^F$, $F \subseteq \mathrm{Aff}(\mathbf{Z}/n\mathbf{Z})$ in detail for each degree ≤ 6.

4. The cubic case, C_3 and S_3

In this section, we treat the case $n = 3$. From (2) We see that the matrix $U = [u_{i,j}]$ is of the following form

$$U = \begin{bmatrix} \mathsf{A}' & \mathsf{B}' & \mathsf{C}' \\ \mathsf{B} & \mathsf{C} & \mathsf{D} \\ \mathsf{C} & \mathsf{D} & \mathsf{B} \end{bmatrix} ,$$

where by the definition (1) we have

$$\mathsf{A}' = \sum_{i=0}^{2} \sigma^i(-y_0^4 + y_0^2 \, y_1 \, y_2)/\det R \, , \qquad \mathsf{B}' = \sum_{i=0}^{2} \sigma^i(-y_0^2 \, y_1^2 + y_0 \, y_1^3)/\det R \, ,$$

$$\mathsf{C}' = \sum_{i=0}^{2} \sigma^i (y_0^3\, y_1 - y_0^2\, y_1^2)/\det R\,, \qquad \mathsf{B} = \sum_{i=0}^{2} \sigma^i (-y_0^3\, y_1 + y_0^2\, y_1\, y_2)/\det R\,,$$

$$\mathsf{C} = \sum_{i=0}^{2} \sigma^i (y_0^2\, y_1\, y_2 - y_0\, y_1^3)/\det R\,, \qquad \mathsf{D} = \sum_{i=0}^{2} \sigma^i (y_0^2\, y_1^2 - y_0^2\, y_1\, y_2)/\det R\,,$$

and $\det R = -(y_0 + y_1 + y_2)(y_0^2 - y_0\, y_1 + y_1^2 - y_0\, y_2 - y_1\, y_2 + y_2^2)$.

Let $\sigma = (012)$ be the cyclic permutation of order three and $\tau := \tau_{-1} = (12)$, so that

$$C_3 = \langle \sigma \rangle, \quad D_3 = S_3 = \langle \sigma, \tau \rangle.$$

By Key lemma, we see that τ acts on $\mathbf{Q}(y_0, y_1, y_2)^{\langle \sigma \rangle} = \mathbf{Q}(u_{i,j} \mid 0 \le i, j \le 2)$ as follows:

$$\tau \,:\, \mathsf{A}' \mapsto \mathsf{A}', \quad \mathsf{B}' \mapsto \mathsf{C}' \mapsto \mathsf{B}', \quad \mathsf{B} \mapsto \mathsf{C} \mapsto \mathsf{B}\,, \quad \mathsf{D} \mapsto \mathsf{D}\,. \tag{7}$$

It follows from (5) that

$$\mathbf{Q}(y_0, y_1, y_2)^{C_3} = \mathbf{Q}(\mathsf{B}, \mathsf{C}, \mathsf{D})\,. \tag{8}$$

and hence from (7) and (8), we have

$$\mathbf{Q}(y_0, y_1, y_2)^{S_3} = \mathbf{Q}(\mathsf{B} + \mathsf{C}, \mathsf{BC}, \mathsf{D})\,.$$

5. The quartic case, C_4 and D_4

We study the case $n = 4$ in this section. From (2), we see that the matrix $U = [u_{i,j}]$ is of the following form

$$U = \begin{bmatrix} \mathsf{A}' & \mathsf{B}' & \mathsf{C}' & \mathsf{D}' \\ \mathsf{B} & \mathsf{D} & \mathsf{E}_1 & \mathsf{E}_2 \\ \mathsf{C} & \mathsf{E}_3 & \mathsf{C} & \mathsf{E}_3 \\ \mathsf{D} & \mathsf{E}_1 & \mathsf{E}_2 & \mathsf{B} \end{bmatrix}.$$

For example, from the definition (1), we have

$$\mathsf{B} = \sum_{i=0}^{3} (-1)^i\, \sigma^i (-y_0^4\, y_1 - y_0\, y_1^3\, y_2 + y_0^2\, y_1\, y_2^2 - 2\, y_0\, y_1^2\, y_2^2 + y_0^2\, y_1\, y_2\, y_3)/\det R\,,$$

$$\mathsf{E}_1 = \sum_{i=0}^{3} (-1)^i\, \sigma^i (-y_0^2\, y_1^3 + y_0^3\, y_1\, y_2 + y_0^2\, y_1^2\, y_2 - y_0\, y_1\, y_2^3 - 2\, y_0^2\, y_1\, y_2\, y_3)/\det R\,,$$

$$\mathsf{D} = \tau(\mathsf{B})\,, \quad \mathsf{E}_2 = \tau(\mathsf{E}_1)\,,$$

and $\det R = -(y_0 + y_1 + y_2 + y_3)(y_0 - y_1 + y_2 - y_3)(y_0^2 + y_1^2 - 2\, y_0\, y_2 + y_2^2 - 2\, y_1\, y_3 + y_3^2)$.

Let $\sigma = (0123)$ be the cyclic permutation of order four and $\tau := \tau_{-1} = (13)$. We see that

$$C_4 = \langle \sigma \rangle\,, \quad D_4 = \langle \sigma, \tau \rangle\,.$$

By Key lemma, τ acts on $\mathbf{Q}(y_0, y_1, y_2, y_3)^{\langle\sigma\rangle} = \mathbf{Q}(u_{i,j} \mid 0 \le i, j \le 3)$ as follows:

$$\tau : \mathsf{A}' \mapsto \mathsf{A}', \quad \mathsf{B}' \mapsto \mathsf{D}' \mapsto \mathsf{B}', \quad \mathsf{C}' \mapsto \mathsf{C}', \quad \mathsf{B} \mapsto \mathsf{D} \mapsto \mathsf{B}, \quad \mathsf{C} \mapsto \mathsf{C}, \quad \mathsf{E}_1 \mapsto \mathsf{E}_2 \mapsto \mathsf{E}_1, \quad \mathsf{E}_3 \mapsto \mathsf{E}_3. \tag{9}$$

Using (4) and (5) for $n = 4$, we first have

$$\mathbf{Q}(y_0, y_1, y_2, y_3)^{C_4} = \mathbf{Q}(\mathsf{B}, \mathsf{D}, \mathsf{E}_1, \mathsf{E}_2) \qquad \text{(c.f. [2])}, \tag{10}$$

and then using (9) and (10), we obtain a set of independent generators of $\mathbf{Q}(y_0, y_1, y_2, y_3)^{D_4}$.

THEOREM 3. *We have*

$$\boldsymbol{Q}(y_0, y_1, y_2, y_3)^{D_4} = \boldsymbol{Q}(\mathsf{B}+\mathsf{D}, \mathsf{E}_1+\mathsf{E}_2, (\mathsf{B}-\mathsf{D})^2, (\mathsf{B}-\mathsf{D})(\mathsf{E}_1-\mathsf{E}_2)).$$

PROOF. We see that $(D_4/C_4) \cong \langle\tau\rangle$ acts on $\mathbf{Q}(y_0, y_1, y_2, y_3)^{C_4} = \mathbf{Q}(\mathsf{B}, \mathsf{D}, \mathsf{E}_1, \mathsf{E}_2)$ as $\tau : \mathsf{B} \mapsto \mathsf{D} \mapsto \mathsf{B}, \mathsf{E}_1 \mapsto \mathsf{E}_2 \mapsto \mathsf{E}_1$. Thus the assertion follows from Lemma 2. □

APPLICATION 1. From the above results on $\mathbf{Q}(y_0, y_1, y_2, y_3)^{C_4}$, $\mathbf{Q}(y_0, y_1, y_2, y_3)^{D_4}$, one can construct families of cyclic and dihedral polynomials of degree 4. In order to simplify the argument, we use the following non-singular linear transformation of the variables $\mathsf{B}, \mathsf{D}, \mathsf{E}_1, \mathsf{E}_2$ (cf. [2]).

$$\begin{cases} \mathsf{s} := \mathsf{B}+\mathsf{D}+\mathsf{E}_1+\mathsf{E}_2, \\ \mathsf{t} := \mathsf{B}-\mathsf{D}+\mathsf{E}_1-\mathsf{E}_2, \\ \mathsf{u} := \mathsf{B}-\mathsf{D}-\mathsf{E}_1+\mathsf{E}_2, \\ \mathsf{v} := \mathsf{B}+\mathsf{D}-\mathsf{E}_1-\mathsf{E}_2, \end{cases} \qquad \begin{cases} \mathsf{B} = (\mathsf{s}+\mathsf{t}+\mathsf{u}+\mathsf{v})/4, \\ \mathsf{D} = (\mathsf{s}-\mathsf{t}-\mathsf{u}+\mathsf{v})/4, \\ \mathsf{E}_1 = (\mathsf{s}+\mathsf{t}-\mathsf{u}-\mathsf{v})/4, \\ \mathsf{E}_2 = (\mathsf{s}-\mathsf{t}+\mathsf{u}-\mathsf{v})/4. \end{cases}$$

Then it follows from (10) that $\mathbf{Q}(y_0, y_1, y_2, y_3)^{C_4} = \mathbf{Q}(\mathsf{s}, \mathsf{t}, \mathsf{u}, \mathsf{v})$. Indeed one can check this assertion directly as follows:

$$\mathsf{A}' = -\frac{2\,\mathsf{s}^2\mathsf{t}+\mathsf{s}^2\mathsf{u}+\mathsf{t}\mathsf{u}^2+3\,\mathsf{u}^3-\mathsf{s}\mathsf{t}\mathsf{v}+\mathsf{s}\mathsf{u}\mathsf{v}+\mathsf{u}\mathsf{v}^2}{4\,\mathsf{u}(\mathsf{s}-\mathsf{v})}, \quad \mathsf{B}' = -\frac{2\,\mathsf{s}\mathsf{t}+\mathsf{s}\mathsf{u}-2\,\mathsf{u}^2-\mathsf{t}\mathsf{v}}{4\,\mathsf{u}},$$

$$\mathsf{C}' = -\frac{2\,\mathsf{s}^2\mathsf{t}+\mathsf{s}^2\mathsf{u}+\mathsf{t}\mathsf{u}^2-\mathsf{u}^3-\mathsf{s}\mathsf{t}\mathsf{v}-3\,\mathsf{s}\mathsf{u}\mathsf{v}+\mathsf{u}\mathsf{v}^2}{4\,\mathsf{u}(\mathsf{s}-\mathsf{v})}, \quad \mathsf{D}' = -\frac{2\,\mathsf{s}\mathsf{t}+\mathsf{s}\mathsf{u}+2\,\mathsf{u}^2-\mathsf{t}\mathsf{v}}{4\,\mathsf{u}},$$

$$\mathsf{C} = \frac{2\,\mathsf{s}^2\mathsf{t}-\mathsf{s}^2\mathsf{u}+\mathsf{t}\mathsf{u}^2-\mathsf{u}^3-\mathsf{s}\mathsf{t}\mathsf{v}+\mathsf{s}\mathsf{u}\mathsf{v}-\mathsf{u}\mathsf{v}^2}{4\,\mathsf{u}(\mathsf{s}-\mathsf{v})}, \qquad \mathsf{E}_3 = \frac{2\,\mathsf{s}\mathsf{t}-\mathsf{s}\mathsf{u}-\mathsf{t}\mathsf{v}}{4\,\mathsf{u}}, \tag{11}$$

where

$$\mathsf{s} = \frac{(y_0+y_2)(y_1+y_3)}{y_0+y_1+y_2+y_3}, \quad \mathsf{t} = \frac{(y_0-y_2)(y_1-y_3)}{y_0-y_1+y_2-y_3},$$

$$\mathsf{u} = \frac{(y_0-y_2)(y_1-y_3)(y_0-y_1+y_2-y_3)}{(y_0-y_2)^2+(y_1-y_3)^2},$$

$$\mathsf{v} = \frac{(y_0+y_2)(y_1-y_3)^2+(y_0-y_2)^2(y_1+y_3)}{(y_0-y_2)^2+(y_1-y_3)^2}.$$

Hence by using (11), we obtain a $\mathbf{Q}$-generic C_4-polynomial $g^{C_4}(\mathsf{s},\mathsf{t},\mathsf{u},\mathsf{v};X)$ with four parameters $\mathsf{s},\mathsf{t},\mathsf{u},\mathsf{v}$ as the characteristic polynomial of the matrix U (i.e. as the generating polynomial for the cyclic extension $\mathbf{Q}(y_0,y_1,y_2,y_3)/\mathbf{Q}(\mathsf{s},\mathsf{t},\mathsf{u},\mathsf{v})$ of degree four).

$$\begin{aligned} g^{C_4}(\mathsf{s},\mathsf{t},\mathsf{u},\mathsf{v};X) &:= X^4 + \frac{\mathsf{u}^2+\mathsf{v}^2}{\mathsf{s}-\mathsf{v}}X^3 \\ &- \frac{(\mathsf{u}^2+\mathsf{v}^2)(4\,\mathsf{s}^2\mathsf{t}+2\,\mathsf{s}^2\mathsf{u}+\mathsf{t}\mathsf{u}^2-\mathsf{u}^3-4\,\mathsf{s}\mathsf{t}\mathsf{v}-2\,\mathsf{s}\mathsf{u}\mathsf{v}+\mathsf{t}\mathsf{v}^2-\mathsf{u}\mathsf{v}^2)}{4\,\mathsf{u}(\mathsf{s}-\mathsf{v})^2}X^2 \\ &+ \frac{(\mathsf{u}^2+\mathsf{v}^2)(-\mathsf{s}\mathsf{u}^3+4\,\mathsf{s}^2\mathsf{t}\mathsf{v}+\mathsf{t}\mathsf{u}^2\mathsf{v}-4\,\mathsf{s}\mathsf{t}\mathsf{v}^2-\mathsf{s}\mathsf{u}\mathsf{v}^2+\mathsf{t}\mathsf{v}^3)}{4\,\mathsf{u}(\mathsf{s}-\mathsf{v})^2}X \\ &+ \frac{\mathsf{u}^2+\mathsf{v}^2}{16\,\mathsf{u}(\mathsf{s}-\mathsf{v})^2}(4\,\mathsf{s}^2\mathsf{t}^2\mathsf{u}-4\,\mathsf{s}^2\mathsf{t}\mathsf{u}^2+\mathsf{s}^2\mathsf{u}^3+\mathsf{t}^2\mathsf{u}^3-\mathsf{t}\mathsf{u}^4-4\,\mathsf{s}\mathsf{t}^2\mathsf{u}\mathsf{v} \\ &+ 4\,\mathsf{s}\mathsf{t}\mathsf{u}^2\mathsf{v}-4\,\mathsf{s}^2\mathsf{t}\mathsf{v}^2+\mathsf{s}^2\mathsf{u}\mathsf{v}^2+\mathsf{t}^2\mathsf{u}\mathsf{v}^2-2\,\mathsf{t}\mathsf{u}^2\mathsf{v}^2+4\,\mathsf{s}\mathsf{t}\mathsf{v}^3-\mathsf{t}\mathsf{v}^4)\,. \end{aligned}$$

Since the action of τ on $\mathbf{Q}(\mathsf{s},\mathsf{t},\mathsf{u},\mathsf{v})$ is given simply by $\mathsf{s}\mapsto\mathsf{s}$, $\mathsf{t}\mapsto-\mathsf{t}$, $\mathsf{u}\mapsto-\mathsf{u}$, $\mathsf{v}\mapsto\mathsf{v}$, we also have $\mathbf{Q}(y_0,y_1,y_2,y_3)^{D_4}=\mathbf{Q}(\mathsf{s},\mathsf{t}^2,\mathsf{t}\mathsf{u},\mathsf{v})$ from Lemma 1. Putting $\mathsf{T}:=\mathsf{t}^2$, $\mathsf{U}:=\mathsf{t}\mathsf{u}$ we obtain a $\mathbf{Q}$-generic D_4-polynomial $g^{D_4}(\mathsf{s},\mathsf{T},\mathsf{U},\mathsf{v};X)$ as the generating polynomial for the dihedral extension $\mathbf{Q}(y_0,y_1,y_2,y_3)/\mathbf{Q}(\mathsf{s},\mathsf{T},\mathsf{U},\mathsf{v})$ of degree 8.

$$\begin{aligned} g^{D_4}(\mathsf{s},\mathsf{T},\mathsf{U},\mathsf{v};X) &:= X^4 + \frac{\mathsf{U}^2+\mathsf{T}\mathsf{v}^2}{\mathsf{T}(\mathsf{s}-\mathsf{v})}X^3 \\ &- \frac{(\mathsf{u}^2+\mathsf{T}\mathsf{v}^2)(4\,\mathsf{s}^2\mathsf{T}^2+2\,\mathsf{s}^2\mathsf{T}\mathsf{U}+\mathsf{T}\mathsf{U}^2-\mathsf{U}^3-4\,\mathsf{s}\mathsf{T}^2\mathsf{v}-2\,\mathsf{s}\mathsf{T}\mathsf{U}\mathsf{v}+\mathsf{T}^2\mathsf{v}^2-\mathsf{T}\mathsf{U}\mathsf{v}^2)}{4\,\mathsf{T}^2\mathsf{U}(\mathsf{s}-\mathsf{v})^2}X^2 \\ &+ \frac{(\mathsf{U}^2+\mathsf{T}\mathsf{v}^2)(-\mathsf{s}\mathsf{U}^3+4\,\mathsf{s}^2\mathsf{T}^2\mathsf{v}+\mathsf{T}\mathsf{U}^2\mathsf{v}-4\,\mathsf{s}\mathsf{T}^2\mathsf{v}^2-\mathsf{s}\mathsf{T}\mathsf{U}\mathsf{v}^2+\mathsf{T}^2\mathsf{v}^3)}{4\,\mathsf{T}^2\mathsf{U}(\mathsf{s}-\mathsf{v})^2}X \\ &+ \frac{\mathsf{u}^2+\mathsf{T}\mathsf{v}^2}{16\,\mathsf{T}^2\mathsf{U}(\mathsf{s}-\mathsf{v})^2}(4\,\mathsf{s}^2\mathsf{T}^2\mathsf{U}-4\,\mathsf{s}^2\mathsf{T}\mathsf{U}^2+\mathsf{s}^2\mathsf{U}^3+\mathsf{T}\mathsf{U}^3-\mathsf{U}^4-4\,\mathsf{s}\mathsf{T}^2\mathsf{U}\mathsf{v}+4\,\mathsf{s}\mathsf{T}\mathsf{U}^2\mathsf{v} \\ &- 4\,\mathsf{s}^2\mathsf{T}^2\mathsf{v}^2+\mathsf{s}^2\mathsf{T}\mathsf{U}\mathsf{v}^2+\mathsf{T}^2\mathsf{U}\mathsf{v}^2-2\,\mathsf{T}\mathsf{U}^2\mathsf{v}^2+4\,\mathsf{s}\mathsf{T}^2\mathsf{v}^3-\mathsf{T}^2\mathsf{v}^4)\,. \end{aligned}$$

We seek a suitable specialization of the parameters of the above polynomials to obtain simple families which can be used to study various problems in algebraic number theory, such as construction of units, unramified extensions, etc. We shall describe three examples for such specialization.

(i) We specialize the parameters of above $g^{C_4}(\mathsf{s},\mathsf{t},\mathsf{u},\mathsf{v};X)$ (resp. $g^{D_4}(\mathsf{s},\mathsf{T},\mathsf{U},\mathsf{v};X)$) as $\mathsf{s}:=(\mathsf{u}^2+12)/4$, $\mathsf{t}:=\mathsf{u}/2$, $\mathsf{v}:=2$ (resp. $\mathsf{s}:=(\mathsf{U}'+12)/4$, $\mathsf{T}:=\mathsf{U}'/4$, $\mathsf{U}:=\mathsf{U}'/2$, $\mathsf{v}:=2$) then we have the following simple one-parameter C_4-polynomial over $\mathbf{Q}(\mathsf{u})$ (resp. D_4-polynomial over $\mathbf{Q}(\mathsf{U}')$).

$$g^{C_4}((\mathsf{u}^2+12)/4,\mathsf{u}/2,\mathsf{u},2;X)=X^4+4X^3-(10+\mathsf{u}^2)X^2+4X+1\,,$$

$$g^{D_4}((\mathsf{U}'+12)/4,\mathsf{U}'/4,\mathsf{U}'/2,2;X)=X^4+4X^3-(10+\mathsf{U}')X^2+4X+1\,.$$

Note that the D_4-polynomial over $\mathbf{Q}(\mathsf{u})$ is obtained by the specialization $\mathsf{u}^2 \mapsto \mathsf{u}$ from the C_4-polynomial $g^{C_4}((\mathsf{u}^2+12)/4, \mathsf{u}/2, \mathsf{u}, 2; X)$. This corresponds to the quadratic extension $\mathbf{Q}(\mathsf{u})/\mathbf{Q}(\mathsf{u}^2)$.

(ii) We specialize the parameters s, v of $g^{C_4}(\mathsf{s}, \mathsf{t}, \mathsf{u}, \mathsf{v}; X)$ (resp. $g^{D_4}(\mathsf{s}, \mathsf{T}, \mathsf{U}, \mathsf{v}; X)$) as $\mathsf{s} := 1, \mathsf{v} := 0$ then we obtain a C_4-polynomial h^{C_4} (resp. D_4-polynomial h^{D_4}) with two parameters t, u (resp. T, U) as follows:

$$h^{C_4}(\mathsf{t}, \mathsf{u}; X) := g^{C_4}(1, \mathsf{t}, \mathsf{u}, 0; X) = X^4 + \mathsf{u}^2 X^3 - \frac{\mathsf{u}(4\,\mathsf{t} + 2\,\mathsf{u} + \mathsf{t}\mathsf{u}^2 - \mathsf{u}^3)}{4} X^2 - \frac{\mathsf{u}^4}{4} X + \frac{\mathsf{u}^2(4\,\mathsf{t}^2 - 4\,\mathsf{t}\mathsf{u} + \mathsf{u}^2 + \mathsf{t}^2\mathsf{u}^2 - \mathsf{t}\mathsf{u}^3)}{16},$$

$$h^{D_4}(\mathsf{T}, \mathsf{U}; X) := g^{D_4}(1, \mathsf{T}, \mathsf{U}, 0; X) = X^4 + \frac{\mathsf{U}^2}{\mathsf{T}} X^3 - \frac{\mathsf{U}(4\,\mathsf{T}^2 + 2\,\mathsf{T}\mathsf{U} + \mathsf{T}\mathsf{U}^2 - \mathsf{U}^3)}{4} X^2 - \frac{\mathsf{U}^4}{4\,\mathsf{T}^2} X + \frac{\mathsf{U}^2(4\,\mathsf{T}^2 - 4\,\mathsf{T}\mathsf{U} + \mathsf{U}^2 + \mathsf{T}\mathsf{U}^2 - \mathsf{U}^3)}{16\,\mathsf{T}^2}.$$

By specializing the parameters of $h^{C_4}(\mathsf{t}, \mathsf{u}; X)$ (resp. $h^{D_4}(\mathsf{T}, \mathsf{U}; X)$) as $\mathsf{u} := 2\,\mathsf{t}$ (resp. $\mathsf{U} := 2\,\mathsf{T}$) and shifting X slightly, we obtain the following one-parameter C_4-polynomial over $\mathbf{Q}(\mathsf{t})$ (resp. D_4-polynomial over $\mathbf{Q}(\mathsf{T})$).

$$h^{C_4}(\mathsf{t}, 2\,\mathsf{t}; \mathsf{t}\,X)/\mathsf{t}^4 = X^4 + 4\,\mathsf{t}X^3 + 2\,(\mathsf{t}^2 - 2)X^2 - 4\,\mathsf{t}X - \mathsf{t}^2,$$

$$h^{D_4}\left(\frac{1}{\mathsf{T}}, \frac{1}{2\,\mathsf{T}}; \frac{X}{\mathsf{T}}\right)\mathsf{T}^4 = X^4 + 4\,X^3 + 2\,(1 - 2\,\mathsf{T})X^2 - 4\,\mathsf{T}X - \mathsf{T}.$$

(iii) By specializing the parameters of $h^{C_4}(\mathsf{t}, \mathsf{u}; X)$ (resp. $h^{D_4}(\mathsf{T}, \mathsf{U}; X)$) as $\mathsf{u} := \mathsf{t}/2$ (resp. $\mathsf{U} := \mathsf{T}$), we get the following one-parameter C_4-polynomial over $\mathbf{Q}(\mathsf{t})$ (resp. D_4-polynomial over $\mathbf{Q}(\mathsf{T})$).

$$16^2\, h^{C_4}(\mathsf{t}/2, \mathsf{t}/2; \mathsf{t}\,X/4)/\mathsf{t}^4 = X^4 + \mathsf{t}X^3 - 6\,X^2 - \mathsf{t}X - 1,$$

$$16\, h^{D_4}(\mathsf{T}, \mathsf{T}; X/2) = X^4 + 2\,\mathsf{T}X^3 + -6\,\mathsf{T}X^2 - 2\,\mathsf{T}^2X - \mathsf{T}^2.$$

6. The quintic case, C_5, D_5 and F_{20}

We treat the case $n = 5$ in this section. From (2), we see that the matrix $U = [u_{i,j}]$ is of the following form.

$$U = \begin{bmatrix} \mathsf{A}' & \mathsf{B}' & \mathsf{C}' & \mathsf{D}' & \mathsf{E}' \\ \mathsf{B} & \mathsf{E} & \mathsf{F}_1 & \mathsf{G}_1 & \mathsf{F}_2 \\ \mathsf{C} & \mathsf{F}_3 & \mathsf{D} & \mathsf{G}_2 & \mathsf{G}_3 \\ \mathsf{D} & \mathsf{G}_2 & \mathsf{G}_3 & \mathsf{C} & \mathsf{F}_3 \\ \mathsf{E} & \mathsf{F}_1 & \mathsf{G}_1 & \mathsf{F}_2 & \mathsf{B} \end{bmatrix}.$$

Let $\sigma = (01234)$ be the cyclic permutation of order five, $\omega := \tau_2 = (1243)$ and $\tau := \tau_{-1} = \omega^2 = (14)(23)$. We see that the subgroups of $\mathrm{Aff}(\mathbf{Z}/5\mathbf{Z})$ containing $\mathbf{Z}/5\mathbf{Z}$ are

$$C_5 = \langle \sigma \rangle\,, \quad D_5 = \langle \sigma, \tau \rangle\,, \quad F_{20} = \langle \sigma, \omega \rangle\,.$$

By Key lemma, τ and ω act on $\mathbf{Q}(y_0, \cdots, y_4)^{\langle \sigma \rangle} = \mathbf{Q}(u_{i,j} \mid 0 \le i, j \le 4)$ as follows:

$$\begin{aligned}\tau \;:\; & \mathsf{A}' \mapsto \mathsf{A}', \quad \mathsf{B}' \mapsto \mathsf{E}' \mapsto \mathsf{B}', \quad \mathsf{C}' \mapsto \mathsf{D}' \mapsto \mathsf{C}', \quad \mathsf{B} \mapsto \mathsf{E} \mapsto \mathsf{B}\,, \quad \mathsf{C} \mapsto \mathsf{D} \mapsto \mathsf{C}\,, \\ & \mathsf{F}_1 \mapsto \mathsf{F}_2 \mapsto \mathsf{F}_1\,, \quad \mathsf{F}_3 \mapsto \mathsf{F}_3\,, \quad \mathsf{G}_1 \mapsto \mathsf{G}_1\,, \quad \mathsf{G}_2 \mapsto \mathsf{G}_3 \mapsto \mathsf{G}_2\,, \qquad (12)\end{aligned}$$

$$\begin{aligned}\omega \;:\; & \mathsf{A}' \mapsto \mathsf{A}', \quad \mathsf{B}' \mapsto \mathsf{C}' \mapsto \mathsf{E}' \mapsto \mathsf{D}' \mapsto \mathsf{B}', \quad \mathsf{B} \mapsto \mathsf{C} \mapsto \mathsf{E} \mapsto \mathsf{D} \mapsto \mathsf{B}\,, \\ & \mathsf{F}_1 \mapsto \mathsf{G}_3 \mapsto \mathsf{F}_2 \mapsto \mathsf{G}_2 \mapsto \mathsf{F}_1\,, \quad \mathsf{F}_3 \mapsto \mathsf{G}_1 \mapsto \mathsf{F}_3\,. \qquad (13)\end{aligned}$$

Indeed we see from (1) that $\mathsf{F}_1, \mathsf{F}_2, \mathsf{F}_3, \mathsf{G}_1, \mathsf{G}_2, \mathsf{G}_3$ are given explicitly as follows:

$$\begin{aligned}\mathsf{F}_1 = \sum_{i=0}^{4} \sigma^i (& - y_0^2 y_1^4 + 2 y_0^3 y_1^2 y_2 + y_0^2 y_1^3 y_2 - y_0^3 y_1 y_2^2 + y_0 y_1 y_2^4 - y_0^4 y_1 y_3 \\ & - y_0^3 y_1 y_2 y_3 - 3 y_0 y_1^2 y_2^2 y_3 + 2 y_0 y_1 y_2^3 y_3 + y_0 y_1^3 y_3^2 \\ & + 2 y_0^2 y_1 y_2 y_3^2 - 3 y_0 y_1^2 y_2 y_3^2 - y_0 y_1 y_2^2 y_3^2 + 2 y_0^2 y_1 y_2 y_3 y_4) / \det R\,,\end{aligned}$$

$$\begin{aligned}\mathsf{G}_1 = \sum_{i=0}^{4} \sigma^i (& y_0^3 y_1^3 - y_0^4 y_1 y_2 - y_0^3 y_1^2 y_2 - y_0 y_1^2 y_2^3 - y_0 y_1 y_2^4 + y_0^4 y_2 y_3 \\ & + 2 y_0 y_1^3 y_2 y_3 + 2 y_0^2 y_1 y_2^2 y_3 - y_0 y_1^2 y_2^2 y_3 + 2 y_0 y_1 y_2^3 y_3 \\ & - 3 y_0^2 y_1^2 y_3^2 + y_0^2 y_1 y_2 y_3^2 + 2 y_0 y_1^2 y_2 y_3^2 - 3 y_0^2 y_1 y_2 y_3 y_4) / \det R\,,\end{aligned}$$

$$\mathsf{F}_2 = \omega^2(\mathsf{F}_1)\,, \quad \mathsf{F}_3 = \omega(\mathsf{G}_1)\,, \quad \mathsf{G}_2 = \omega^3(\mathsf{F}_1)\,, \quad \mathsf{G}_3 = \omega(\mathsf{F}_1)\,,$$

where

$$\begin{aligned}\det R &= \sum_{i=0}^{4} \sigma^i (y_0^5 - 5 y_0 y_1^3 y_2 + 5 y_0^2 y_1 y_2^2 + 5 y_0^2 y_1^2 y_3 - 5 y_0^3 y_2 y_3 - y_0 y_1 y_2 y_3 y_4) \\ &= (y_0 + \cdots + y_4) \sum_{i=0}^{4} \sigma^i (y_0^4 - y_0^3 y_1 + y_0^2 y_1^2 - y_0 y_1^3 - y_0^3 y_2 + 2 y_0^2 y_1 y_2 - 3 y_0 y_1^2 y_2 \\ &\quad + y_0^2 y_2^2 + 2 y_0 y_1 y_2^2 - y_0 y_2^3 + 2 y_0^2 y_1 y_3 + 2 y_0 y_1^2 y_3 - 3 y_0^2 y_2 y_3 - y_0 y_1 y_2 y_3)\,.\end{aligned}$$

By using (4) and (5), we obtain that

$$\mathbf{Q}(y_0, \cdots, y_4)^{C_5} = \mathbf{Q}(\mathsf{F}_1, \mathsf{F}_2, \mathsf{F}_3, \mathsf{G}_1, \mathsf{G}_2, \mathsf{G}_3)\,, \qquad (14)$$

where $\mathsf{F}_1, \mathsf{F}_2, \mathsf{F}_3, \mathsf{G}_1, \mathsf{G}_2, \mathsf{G}_3$ satisfy the following quartic relation (see also [2]).

$$\begin{aligned}&\mathsf{F}_1^2\mathsf{F}_2^2 - 2\,\mathsf{F}_1\mathsf{F}_2\mathsf{F}_3^2 + \mathsf{F}_3^4 + \mathsf{F}_1\mathsf{F}_2\mathsf{F}_3\mathsf{G}_1 - \mathsf{F}_3^3\mathsf{G}_1 - 2\,\mathsf{F}_1\mathsf{F}_2\mathsf{G}_1^2 + \mathsf{F}_3^2\mathsf{G}_1^2 - \mathsf{F}_3\mathsf{G}_1^3 + \mathsf{G}_1^4 \\ &-\mathsf{F}_2^3\mathsf{G}_2 + \mathsf{F}_1^2\mathsf{F}_3\mathsf{G}_2 + \mathsf{F}_1^2\mathsf{G}_1\mathsf{G}_2 + \mathsf{F}_2\mathsf{F}_3\mathsf{G}_2^2 + \mathsf{F}_2\mathsf{G}_1\mathsf{G}_2^2 - \mathsf{F}_1\mathsf{G}_2^3 - \mathsf{F}_1^3\mathsf{G}_3 + \mathsf{F}_2^2\mathsf{F}_3\mathsf{G}_3\end{aligned}$$

$$-\mathsf{F}_1\mathsf{F}_2\mathsf{G}_2\mathsf{G}_3 + \mathsf{F}_2^2\mathsf{G}_1\mathsf{G}_3 - 2\,\mathsf{F}_3^2\mathsf{G}_2\mathsf{G}_3 + \mathsf{F}_3\mathsf{G}_1\mathsf{G}_2\mathsf{G}_3 - 2\,\mathsf{G}_1^2\mathsf{G}_2\mathsf{G}_3 + \mathsf{F}_1\mathsf{F}_3\mathsf{G}_3^2$$
$$+\mathsf{F}_1\mathsf{G}_1\mathsf{G}_3^2 + \mathsf{G}_2^2\mathsf{G}_3^2 - \mathsf{F}_2\mathsf{G}_3^3 = 0\,. \tag{15}$$

This equation (15) is cubic in each variable. However we observe that, if we pick up one of the variables F_1, F_2, F_3, G_1, G_2, G_3 and translate the others by this, then (15) is transformed to a linear equation with respect to the chosen variable. For example, we translate the variables by G_1, that is,

$$\mathsf{s}_1 := \mathsf{F}_1 - \mathsf{G}_1\,,\quad \mathsf{s}_2 := \mathsf{F}_2 - \mathsf{G}_1\,,\quad \mathsf{s}_3 := \mathsf{F}_3 - \mathsf{G}_1\,,\quad \mathsf{s}_4 := \mathsf{G}_2 - \mathsf{G}_1\,,\quad \mathsf{s}_5 := \mathsf{G}_3 - \mathsf{G}_1\,,$$

and see that equation (15) is transformed to

$$\begin{aligned}\mathsf{G}_1\,(&-\mathsf{s}_1^3 + 2\,\mathsf{s}_1^2\mathsf{s}_2 + 2\,\mathsf{s}_1\mathsf{s}_2^2 - \mathsf{s}_2^3 + \mathsf{s}_1^2\mathsf{s}_3 - 3\,\mathsf{s}_1\mathsf{s}_2\mathsf{s}_3 + \mathsf{s}_2^2\mathsf{s}_3 - 2\,\mathsf{s}_1\mathsf{s}_3^2 - 2\,\mathsf{s}_2\mathsf{s}_3^2 + 3\,\mathsf{s}_3^3\\
&+2\,\mathsf{s}_1^2\mathsf{s}_4 - \mathsf{s}_1\mathsf{s}_2\mathsf{s}_4 - 3\,\mathsf{s}_2^2\mathsf{s}_4 + 2\,\mathsf{s}_1\mathsf{s}_3\mathsf{s}_4 + 2\,\mathsf{s}_2\mathsf{s}_3\mathsf{s}_4 - 2\,\mathsf{s}_3^2\mathsf{s}_4 - 3\,\mathsf{s}_1\mathsf{s}_4^2 + 2\,\mathsf{s}_2\mathsf{s}_4^2 + \mathsf{s}_3\mathsf{s}_4^2\\
&-\mathsf{s}_4^3 - 3\,\mathsf{s}_1^2\mathsf{s}_5 - \mathsf{s}_1\mathsf{s}_2\mathsf{s}_5 + 2\,\mathsf{s}_2^2\mathsf{s}_5 + 2\,\mathsf{s}_1\mathsf{s}_3\mathsf{s}_5 + 2\,\mathsf{s}_2\mathsf{s}_3\mathsf{s}_5 - 2\,\mathsf{s}_3^2\mathsf{s}_5 - \mathsf{s}_1\mathsf{s}_4\mathsf{s}_5 - \mathsf{s}_2\mathsf{s}_4\mathsf{s}_5\\
&-3\,\mathsf{s}_3\mathsf{s}_4\mathsf{s}_5 + 2\,\mathsf{s}_4^2\mathsf{s}_5 + 2\,\mathsf{s}_1\mathsf{s}_5^2 - 3\,\mathsf{s}_2\mathsf{s}_5^2 + \mathsf{s}_3\mathsf{s}_5^2 + 2\,\mathsf{s}_4\mathsf{s}_5^2 - \mathsf{s}_5^3)\\
&+\mathsf{s}_1^2\mathsf{s}_2^2 - 2\,\mathsf{s}_1\mathsf{s}_2\mathsf{s}_3^2 + \mathsf{s}_3^4 - \mathsf{s}_2^3\mathsf{s}_4 + \mathsf{s}_1^2\mathsf{s}_3\mathsf{s}_4 + \mathsf{s}_2\mathsf{s}_3\mathsf{s}_4^2 - \mathsf{s}_1\mathsf{s}_4^3 - \mathsf{s}_1^3\mathsf{s}_5 + \mathsf{s}_2^2\mathsf{s}_3\mathsf{s}_5\\
&-\mathsf{s}_1\mathsf{s}_2\mathsf{s}_4\mathsf{s}_5 - 2\,\mathsf{s}_3^2\mathsf{s}_4\mathsf{s}_5 + \mathsf{s}_1\mathsf{s}_3\mathsf{s}_5^2 + \mathsf{s}_4^2\mathsf{s}_5^2 - \mathsf{s}_2\mathsf{s}_5^3 = 0\,.\end{aligned}$$

Hence we have $\mathsf{G}_1 \in \mathbf{Q}(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, \mathsf{s}_4, \mathsf{s}_5)$ which implies that $\mathbf{Q}(y_0, \cdots, y_4)^{C_5} = \mathbf{Q}(\mathsf{s}_1, \mathsf{s}_2, \mathsf{s}_3, \mathsf{s}_4, \mathsf{s}_5)$. Namely we obtain the following.

PROPOSITION 4. *We have*

$$\boldsymbol{Q}(y_0, \cdots, y_4)^{C_5} = \boldsymbol{Q}(\mathsf{F}_1 - \mathsf{G}_1, \mathsf{F}_2 - \mathsf{G}_1, \mathsf{F}_3 - \mathsf{G}_1, \mathsf{G}_2 - \mathsf{G}_1, \mathsf{G}_3 - \mathsf{G}_1)\,.$$

From Proposition 4 and the description (12) of the action of τ, a set of independent generators of the fixed field $\mathbf{Q}(y_0, \cdots, y_4)^{D_5}$ is obtained as follows, which gives an affirmative answer to Noether's problem for D_5:

THEOREM 5. *We have*

$$\begin{aligned}&\boldsymbol{Q}(y_0, \cdots, y_4)^{D_5}\\
&= \boldsymbol{Q}(\mathsf{F}_3 - \mathsf{G}_1, \mathsf{F}_1 + \mathsf{F}_2 - 2\,\mathsf{G}_1, \mathsf{G}_2 + \mathsf{G}_3 - 2\,\mathsf{G}_1, (\mathsf{F}_1 - \mathsf{F}_2)^2, (\mathsf{F}_1 - \mathsf{F}_2)(\mathsf{G}_2 - \mathsf{G}_3))\,.\end{aligned}$$

PROOF. We note by (12) that $(D_5/C_5) \cong \langle\tau\rangle$ acts on $\mathbf{Q}(y_0, \cdots, y_4)^{C_5} = \mathbf{Q}(\mathsf{s}_1, \cdots, \mathsf{s}_5)$ by

$$\tau : \mathsf{s}_1 \mapsto \mathsf{s}_2 \mapsto \mathsf{s}_1\,,\quad \mathsf{s}_3 \mapsto \mathsf{s}_3,\quad \mathsf{s}_4 \mapsto \mathsf{s}_5 \mapsto \mathsf{s}_4\,.$$

Hence we obtain that $\mathbf{Q}(\mathsf{s}_1, \cdots, \mathsf{s}_5)^{\langle\tau\rangle} = \mathbf{Q}(\mathsf{s}_3,\ \mathsf{s}_1 + \mathsf{s}_2,\ \mathsf{s}_4 + \mathsf{s}_5, (\mathsf{s}_1 - \mathsf{s}_2)^2, (\mathsf{s}_1 - \mathsf{s}_2)(\mathsf{s}_4 - \mathsf{s}_5))$ from Lemma 2. Thus the assertion follows. □

We next consider the case $G = F_{20}$. We first make the following bi-rational transformation of the generators of $\mathbf{Q}(y_0, \cdots, y_4)^{C_5} = \mathbf{Q}(\mathsf{s}_1, \cdots, \mathsf{s}_5)$, where $\mathsf{s}_1 = \mathsf{F}_1 - \mathsf{G}_1$,

$\mathsf{s}_2 = \mathsf{F}_2 - \mathsf{G}_1, \mathsf{s}_3 = \mathsf{F}_3 - \mathsf{G}_1, \mathsf{s}_4 = \mathsf{G}_2 - \mathsf{G}_1, \mathsf{s}_5 = \mathsf{G}_3 - \mathsf{G}_1.$

$$\begin{cases} \mathsf{a}_1 := \mathsf{s}_1 - \mathsf{s}_2\,, \\ \mathsf{a}_2 := \mathsf{s}_4 - \mathsf{s}_5\,, \\ \mathsf{a}_3 := \mathsf{s}_3\,, \\ \mathsf{a}_4 := \mathsf{s}_1 + \mathsf{s}_2 - \mathsf{s}_4 - \mathsf{s}_5\,, \\ \mathsf{a}_5 := \mathsf{s}_1 + \mathsf{s}_2 - 2\,\mathsf{s}_3 + \mathsf{s}_4 + \mathsf{s}_5\,, \end{cases} \qquad \begin{cases} \mathsf{s}_1 = (2\,\mathsf{a}_1 + 2\,\mathsf{a}_3 + \mathsf{a}_4 + \mathsf{a}_5)/4\,, \\ \mathsf{s}_2 = (-2\,\mathsf{a}_1 + 2\,\mathsf{a}_3 + \mathsf{a}_4 + \mathsf{a}_5)/4\,, \\ \mathsf{s}_3 = \mathsf{a}_3\,, \\ \mathsf{s}_4 = (2\,\mathsf{a}_2 + 2\,\mathsf{a}_3 - \mathsf{a}_4 + \mathsf{a}_5)/4\,, \\ \mathsf{s}_5 = (-2\,\mathsf{a}_2 + 2\,\mathsf{a}_3 - \mathsf{a}_4 + \mathsf{a}_5)/4\,. \end{cases}$$

Then we have

$$\mathbf{Q}(y_0, \cdots, y_4)^{C_5} = \mathbf{Q}(\mathsf{a}_1, \mathsf{a}_2, \mathsf{a}_3, \mathsf{a}_4, \mathsf{a}_5)\,,$$

where

$$\mathsf{a}_1 = \mathsf{F}_1 - \mathsf{F}_2, \quad \mathsf{a}_2 = \mathsf{G}_2 - \mathsf{G}_3, \quad \mathsf{a}_3 = \mathsf{F}_3 - \mathsf{G}_1\,,$$
$$\mathsf{a}_4 = \mathsf{F}_1 + \mathsf{F}_2 - \mathsf{G}_2 - \mathsf{G}_3, \quad \mathsf{a}_5 = \mathsf{F}_1 + \mathsf{F}_2 - 2\mathsf{F}_3 - 2\mathsf{G}_1 + \mathsf{G}_2 + \mathsf{G}_3\,.$$

Using this, we obtain a set of independent generators of the fixed field $\mathbf{Q}(y_0, \cdots, y_4)^{F_{20}}$, which gives an affirmative answer to Noether's problem for F_{20}:

THEOREM 6. *We have*

$$\boldsymbol{Q}(y_0, \cdots, y_4)^{F_{20}} = \boldsymbol{Q}(\mathsf{a}_1^2 + \mathsf{a}_2^2, (\mathsf{a}_1^2 - \mathsf{a}_2^2)\mathsf{a}_3, \mathsf{a}_1\mathsf{a}_2\mathsf{a}_3, \mathsf{a}_3\mathsf{a}_4, \mathsf{a}_5)\,.$$

PROOF. From (13), $(F_{20}/C_5) \cong \langle\omega\rangle$ acts on $\mathbf{Q}(y_0, \cdots, y_4)^{C_5} = \mathbf{Q}(\mathsf{a}_1, \mathsf{a}_2, \mathsf{a}_3, \mathsf{a}_4, \mathsf{a}_5)$ as

$$\omega : \mathsf{a}_1 \mapsto \mathsf{a}_2 \mapsto -\mathsf{a}_1 \mapsto -\mathsf{a}_2 \mapsto \mathsf{a}_1\,, \quad \mathsf{a}_3 \mapsto -\mathsf{a}_3\,,\ \mathsf{a}_4 \mapsto -\mathsf{a}_4\,, \quad \mathsf{a}_5 \mapsto \mathsf{a}_5\,.$$

We put $\mathsf{b}_3 := \mathsf{a}_1\mathsf{a}_2\mathsf{a}_3,\ \mathsf{b}_4 := \mathsf{a}_3\mathsf{a}_4$, then we have $\mathbf{Q}(y_0, \cdots, y_4)^{C_5} = \mathbf{Q}(\mathsf{a}_1, \mathsf{a}_2, \mathsf{b}_3, \mathsf{b}_4, \mathsf{a}_5)$ and see that the action of ω on these generators is given as

$$\mathsf{a}_1 \mapsto \mathsf{a}_2 \mapsto -\mathsf{a}_1 \mapsto -\mathsf{a}_2 \mapsto \mathsf{a}_1\,, \quad \mathsf{b}_3 \mapsto \mathsf{b}_3, \quad \mathsf{b}_4 \mapsto \mathsf{b}_4, \quad \mathsf{a}_5 \mapsto \mathsf{a}_5\,.$$

It is well known and easy to show that

$$\mathbf{Q}(\mathsf{a}_1, \mathsf{a}_2)^{\langle\omega\rangle} = \mathbf{Q}\left(\mathsf{a}_1^2 + \mathsf{a}_2^2\,, \frac{\mathsf{a}_1^2 - \mathsf{a}_2^2}{\mathsf{a}_1\mathsf{a}_2}\right),$$

(see, for example, [4], [3]). The assertion is now an easy consequence of these results. □

7. The sextic case, C_6 and D_6

In this section, we study the case $n = 6$. From (2), the matrix $U = [u_{i,j}]$ has the following form.

$$U = \begin{bmatrix} \mathsf{A}' & \mathsf{B}' & \mathsf{C}' & \mathsf{D}' & \mathsf{E}' & \mathsf{F}' \\ \mathsf{B} & \mathsf{F} & \mathsf{G}_1 & \mathsf{H}_1 & \mathsf{I}_2 & \mathsf{G}_2 \\ \mathsf{C} & \mathsf{G}_3 & \mathsf{E} & \mathsf{I}_2 & \mathsf{J} & \mathsf{H}_2 \\ \mathsf{D} & \mathsf{H}_3 & \mathsf{I}_3 & \mathsf{D} & \mathsf{H}_3 & \mathsf{I}_3 \\ \mathsf{E} & \mathsf{I}_2 & \mathsf{J} & \mathsf{H}_2 & \mathsf{C} & \mathsf{G}_3 \\ \mathsf{F} & \mathsf{G}_1 & \mathsf{H}_1 & \mathsf{I}_1 & \mathsf{G}_1 & \mathsf{B} \end{bmatrix}.$$

Let $\sigma = (012345)$ be the cyclic permutation of order six and $\tau := \tau_{-1} = (15)(24)$. We see that the subgroups of $\mathrm{Aff}(\mathbf{Z}/6\mathbf{Z})$ containing $\mathbf{Z}/6\mathbf{Z}$ are

$$C_6 = \langle \sigma \rangle, \qquad D_6 = \langle \sigma, \tau \rangle.$$

By Key lemma, τ acts on $\mathbf{Q}(y_0, \cdots, y_5)^{\langle\sigma\rangle} = \mathbf{Q}(u_{i,j} \mid 0 \le i, j \le 5)$ as follows:

$$\begin{aligned} \tau \,:\, & \mathsf{A}' \mapsto \mathsf{A}', \quad \mathsf{B}' \mapsto \mathsf{F}' \mapsto \mathsf{B}', \quad \mathsf{C}' \mapsto \mathsf{E}' \mapsto \mathsf{C}', \quad \mathsf{D}' \mapsto \mathsf{D}', \\ & \mathsf{B} \mapsto \mathsf{F} \mapsto \mathsf{B}, \quad \mathsf{C} \mapsto \mathsf{E} \mapsto \mathsf{C}, \quad \mathsf{D} \mapsto \mathsf{D}, \quad \mathsf{G}_1 \mapsto \mathsf{G}_2 \mapsto \mathsf{G}_1, \quad \mathsf{G}_3 \mapsto \mathsf{G}_3, \\ & \mathsf{H}_1 \mapsto \mathsf{I}_1 \mapsto \mathsf{H}_1, \quad \mathsf{H}_2 \mapsto \mathsf{I}_2 \mapsto \mathsf{H}_2, \quad \mathsf{H}_3 \mapsto \mathsf{I}_3 \mapsto \mathsf{H}_3, \quad \mathsf{J} \mapsto \mathsf{J}. \end{aligned} \tag{16}$$

We first prove the following lemma which is analogous to the equation (14) in the quintic case.

LEMMA 7. *We have*

$$\boldsymbol{Q}(y_0, \cdots, y_5)^{C_6} = \boldsymbol{Q}(\mathsf{G}_1, \mathsf{G}_2, \mathsf{G}_3, \mathsf{H}_1, \mathsf{H}_2, \mathsf{H}_3, \mathsf{I}_1, \mathsf{I}_2, \mathsf{I}_3).$$

PROOF. From (5), we have that $\mathbf{Q}(y_0, \cdots, y_5)^{C_6} = \mathbf{Q}(u_{i,j} \mid 1 \le i \le j \le 5)$, where $u_{i,j}$ is the elementary cyclic elements of order 6. Hence we should show that $\mathsf{B}, \mathsf{C}, \mathsf{D}, \mathsf{E}, \mathsf{F}, \mathsf{J} \in \mathbf{Q}(\mathsf{G}_1, \mathsf{G}_2, \mathsf{G}_3, \mathsf{H}_1, \mathsf{H}_2, \mathsf{H}_3, \mathsf{I}_1, \mathsf{I}_2, \mathsf{I}_3)$. By using (2)–(4), we obtain the following four quadratic relations.

$$\begin{aligned} & \mathsf{D}\mathsf{H}_1 + \mathsf{H}_1^2 + \mathsf{D}\mathsf{H}_2 - \mathsf{F}\mathsf{H}_2 + \mathsf{H}_1\mathsf{H}_2 - \mathsf{B}\mathsf{H}_3 - \mathsf{G}_2\mathsf{H}_3 \\ & \quad - \mathsf{G}_3\mathsf{H}_3 - \mathsf{H}_2\mathsf{H}_3 - \mathsf{G}_1\mathsf{I}_1 - \mathsf{G}_2\mathsf{I}_2 + \mathsf{H}_1\mathsf{I}_2 + \mathsf{G}_2\mathsf{I}_3 + \mathsf{G}_3\mathsf{I}_3 = 0, \\ & \mathsf{G}_2\mathsf{H}_1 + \mathsf{G}_1\mathsf{H}_2 - \mathsf{G}_1\mathsf{H}_3 - \mathsf{G}_3\mathsf{H}_3 - \mathsf{D}\mathsf{I}_1 - \mathsf{H}_2\mathsf{I}_1 \\ & \quad - \mathsf{I}_1^2 + \mathsf{B}\mathsf{I}_2 - \mathsf{D}\mathsf{I}_2 - \mathsf{I}_1\mathsf{I}_2 + \mathsf{F}\mathsf{I}_3 + \mathsf{G}_1\mathsf{I}_3 + \mathsf{G}_3\mathsf{I}_3 + \mathsf{I}_2\mathsf{I}_3 = 0, \\ & \mathsf{G}_3\mathsf{H}_2 - \mathsf{G}_2\mathsf{H}_3 - \mathsf{D}\mathsf{I}_1 + \mathsf{E}\mathsf{I}_1 - \mathsf{D}\mathsf{I}_2 - \mathsf{H}_1\mathsf{I}_2 \\ & \quad - \mathsf{I}_1\mathsf{I}_2 - \mathsf{I}_2^2 + \mathsf{C}\mathsf{I}_3 + \mathsf{G}_2\mathsf{I}_3 + \mathsf{I}_1\mathsf{I}_3 + \mathsf{H}_1\mathsf{J} - \mathsf{H}_3\mathsf{J} + \mathsf{I}_3\mathsf{J} = 0, \\ & \mathsf{C}\mathsf{H}_1 - \mathsf{D}\mathsf{H}_1 - \mathsf{D}\mathsf{H}_2 - \mathsf{H}_1\mathsf{H}_2 - \mathsf{H}_2^2 + \mathsf{E}\mathsf{H}_3 \\ & \quad + \mathsf{G}_1\mathsf{H}_3 + \mathsf{H}_1\mathsf{H}_3 - \mathsf{H}_2\mathsf{I}_1 + \mathsf{G}_3\mathsf{I}_2 - \mathsf{G}_1\mathsf{I}_3 + \mathsf{H}_3\mathsf{J} + \mathsf{I}_1\mathsf{J} - \mathsf{I}_3\mathsf{J} = 0. \end{aligned}$$

Observe that this is a system of linear equations in $\mathsf{B}, \mathsf{C}, \mathsf{E}, \mathsf{F}$. Hence we easily solve this as

$$\begin{aligned}
\mathsf{B} = (&-\mathsf{G}_2\mathsf{H}_1\mathsf{H}_2 - \mathsf{G}_1\mathsf{H}_2^2 + \mathsf{G}_1\mathsf{H}_2\mathsf{H}_3 + \mathsf{G}_3\mathsf{H}_2\mathsf{H}_3 + \mathsf{D}\mathsf{H}_2\mathsf{I}_1 + \mathsf{H}_2^2\mathsf{I}_1 + \mathsf{H}_2\mathsf{I}_1^2 + \mathsf{D}\mathsf{H}_2\mathsf{I}_2 \\
&+\mathsf{H}_2\mathsf{I}_1\mathsf{I}_2 - \mathsf{D}\mathsf{H}_1\mathsf{I}_3 - \mathsf{H}_1^2\mathsf{I}_3 - \mathsf{D}\mathsf{H}_2\mathsf{I}_3 - \mathsf{G}_1\mathsf{H}_2\mathsf{I}_3 - \mathsf{G}_3\mathsf{H}_2\mathsf{I}_3 - \mathsf{H}_1\mathsf{H}_2\mathsf{I}_3 + \mathsf{G}_2\mathsf{H}_3\mathsf{I}_3 \\
&+\mathsf{G}_3\mathsf{H}_3\mathsf{I}_3 + \mathsf{H}_2\mathsf{H}_3\mathsf{I}_3 + \mathsf{G}_1\mathsf{I}_1\mathsf{I}_3 + \mathsf{G}_2\mathsf{I}_2\mathsf{I}_3 - \mathsf{H}_1\mathsf{I}_2\mathsf{I}_3 - \mathsf{H}_2\mathsf{I}_2\mathsf{I}_3 - \mathsf{G}_2\mathsf{I}_3^2 - \mathsf{G}_3\mathsf{I}_3^2)/ \\
&(\mathsf{H}_2\mathsf{I}_2 - \mathsf{H}_3\mathsf{I}_3)\,, \\
\mathsf{C} = (&\mathsf{G}_3\mathsf{H}_2\mathsf{H}_3 - \mathsf{G}_2\mathsf{H}_3^2 + \mathsf{D}\mathsf{H}_1\mathsf{I}_1 + \mathsf{D}\mathsf{H}_2\mathsf{I}_1 + \mathsf{H}_1\mathsf{H}_2\mathsf{I}_1 + \mathsf{H}_2^2\mathsf{I}_1 - \mathsf{D}\mathsf{H}_3\mathsf{I}_1 - \mathsf{G}_1\mathsf{H}_3\mathsf{I}_1 \\
&-\mathsf{H}_1\mathsf{H}_3\mathsf{I}_1 + \mathsf{H}_2\mathsf{I}_1^2 - \mathsf{D}\mathsf{H}_3\mathsf{I}_2 - \mathsf{H}_1\mathsf{H}_3\mathsf{I}_2 - \mathsf{G}_3\mathsf{I}_1\mathsf{I}_2 - \mathsf{H}_3\mathsf{I}_1\mathsf{I}_2 - \mathsf{H}_3\mathsf{I}_2^2 + \mathsf{G}_2\mathsf{H}_3\mathsf{I}_3 \\
&+\mathsf{G}_1\mathsf{I}_1\mathsf{I}_3 + \mathsf{H}_3\mathsf{I}_1\mathsf{I}_3 + \mathsf{H}_1\mathsf{H}_3\mathsf{J} - \mathsf{H}_3^2\mathsf{J} - \mathsf{H}_3\mathsf{I}_1\mathsf{J} - \mathsf{I}_1^2\mathsf{J} + \mathsf{H}_3\mathsf{I}_3\mathsf{J} + \mathsf{I}_1\mathsf{I}_3\mathsf{J})/ \\
&(\mathsf{H}_1\mathsf{I}_1 - \mathsf{H}_3\mathsf{I}_3)\,, \\
\mathsf{E} = (&-\mathsf{G}_3\mathsf{H}_1\mathsf{H}_2 + \mathsf{G}_2\mathsf{H}_1\mathsf{H}_3 + \mathsf{D}\mathsf{H}_1\mathsf{I}_1 + \mathsf{D}\mathsf{H}_1\mathsf{I}_2 + \mathsf{H}_1^2\mathsf{I}_2 + \mathsf{H}_1\mathsf{I}_1\mathsf{I}_2 + \mathsf{H}_1\mathsf{I}_2^2 - \mathsf{D}\mathsf{H}_1\mathsf{I}_3 \\
&-\mathsf{G}_2\mathsf{H}_1\mathsf{I}_3 - \mathsf{D}\mathsf{H}_2\mathsf{I}_3 - \mathsf{H}_1\mathsf{H}_2\mathsf{I}_3 - \mathsf{H}_2^2\mathsf{I}_3 + \mathsf{G}_1\mathsf{H}_3\mathsf{I}_3 + \mathsf{H}_1\mathsf{H}_3\mathsf{I}_3 - \mathsf{H}_1\mathsf{I}_1\mathsf{I}_3 - \mathsf{H}_2\mathsf{I}_1\mathsf{I}_3 \\
&+\mathsf{G}_3\mathsf{I}_2\mathsf{I}_3 - \mathsf{G}_1\mathsf{I}_3^2 - \mathsf{H}_1^2\mathsf{J} + \mathsf{H}_1\mathsf{H}_3\mathsf{J} - \mathsf{H}_1\mathsf{I}_3\mathsf{J} + \mathsf{H}_3\mathsf{I}_3\mathsf{J} + \mathsf{I}_1\mathsf{I}_3\mathsf{J} - \mathsf{I}_3^2\mathsf{J})/(\mathsf{H}_1\mathsf{I}_1 - \mathsf{H}_3\mathsf{I}_3)\,, \\
\mathsf{F} = (&\mathsf{G}_2\mathsf{H}_1\mathsf{H}_3 + \mathsf{G}_1\mathsf{H}_2\mathsf{H}_3 - \mathsf{G}_1\mathsf{H}_3^2 - \mathsf{G}_3\mathsf{H}_3^2 - \mathsf{D}\mathsf{H}_3\mathsf{I}_1 - \mathsf{H}_2\mathsf{H}_3\mathsf{I}_1 - \mathsf{H}_3\mathsf{I}_1^2 + \mathsf{D}\mathsf{H}_1\mathsf{I}_2 + \mathsf{H}_1^2\mathsf{I}_2 \\
&+\mathsf{D}\mathsf{H}_2\mathsf{I}_2 + \mathsf{H}_1\mathsf{H}_2\mathsf{I}_2 - \mathsf{D}\mathsf{H}_3\mathsf{I}_2 - \mathsf{G}_2\mathsf{H}_3\mathsf{I}_2 - \mathsf{G}_3\mathsf{H}_3\mathsf{I}_2 - \mathsf{H}_2\mathsf{H}_3\mathsf{I}_2 - \mathsf{G}_1\mathsf{I}_1\mathsf{I}_2 - \mathsf{H}_3\mathsf{I}_1\mathsf{I}_2 \\
&-\mathsf{G}_2\mathsf{I}_2^2 + \mathsf{H}_1\mathsf{I}_2^2 + \mathsf{G}_1\mathsf{H}_3\mathsf{I}_3 + \mathsf{G}_3\mathsf{H}_3\mathsf{I}_3 + \mathsf{G}_2\mathsf{I}_2\mathsf{I}_3 + \mathsf{G}_3\mathsf{I}_2\mathsf{I}_3 + \mathsf{H}_3\mathsf{I}_2\mathsf{I}_3)/(\mathsf{H}_2\mathsf{I}_2 - \mathsf{H}_3\mathsf{I}_3)\,.
\end{aligned}$$

It follows that $\mathsf{B}, \mathsf{C}, \mathsf{E}, \mathsf{F} \in \mathbf{Q}(\mathsf{D}, \mathsf{G}_1, \mathsf{G}_2, \mathsf{G}_3, \mathsf{H}_1, \mathsf{H}_2, \mathsf{H}_3, \mathsf{I}_1, \mathsf{I}_2, \mathsf{I}_3, \mathsf{J})$. From above equations and (4) again, by using computer manipulations (e.g. Mathematica [26]), we can find the following relations of $\mathsf{D}, \mathsf{G}_1, \mathsf{G}_2, \mathsf{G}_3, \mathsf{H}_1, \mathsf{H}_2, \mathsf{H}_3, \mathsf{I}_1, \mathsf{I}_2, \mathsf{I}_3, \mathsf{J}$.

$$\begin{cases}
\mathsf{G}_1\mathsf{H}_2 - \mathsf{G}_3\mathsf{H}_3 - \mathsf{H}_2\mathsf{I}_1 - \mathsf{G}_2\mathsf{I}_2 + \mathsf{H}_1\mathsf{I}_2 + \mathsf{G}_3\mathsf{I}_3 + \mathsf{J}(-\mathsf{G}_1 + \mathsf{G}_2 - \mathsf{H}_1 + \mathsf{H}_3 + \mathsf{I}_1 - \mathsf{I}_3) = 0\,, \\
\varphi_1(\mathsf{D}, \mathsf{G}_1, \mathsf{G}_2, \mathsf{G}_3, \mathsf{H}_1, \mathsf{H}_2, \mathsf{H}_3, \mathsf{I}_1, \mathsf{I}_2, \mathsf{I}_3) = 0\,,
\end{cases}$$

where

$$\begin{aligned}
&\varphi_1(\mathsf{D}, \mathsf{G}_1, \mathsf{G}_2, \mathsf{G}_3, \mathsf{H}_1, \mathsf{H}_2, \mathsf{H}_3, \mathsf{I}_1, \mathsf{I}_2, \mathsf{I}_3) := \\
&\quad \mathsf{D}(\mathsf{H}_1 + \mathsf{H}_2 - \mathsf{I}_1 - \mathsf{I}_2)(\mathsf{H}_1\mathsf{I}_2 - \mathsf{H}_3\mathsf{I}_1 - \mathsf{H}_3\mathsf{I}_2 + \mathsf{H}_3\mathsf{I}_3) + \mathsf{G}_2\mathsf{H}_1^2\mathsf{H}_3 + \mathsf{G}_1\mathsf{H}_1\mathsf{H}_2\mathsf{H}_3 \\
&\quad +\mathsf{G}_2\mathsf{H}_1\mathsf{H}_2\mathsf{H}_3 + \mathsf{G}_1\mathsf{H}_2^2\mathsf{H}_3 - \mathsf{G}_1\mathsf{H}_1\mathsf{H}_3^2 - \mathsf{G}_3\mathsf{H}_1\mathsf{H}_3^2 - \mathsf{G}_1\mathsf{H}_2\mathsf{H}_3^2 - \mathsf{G}_3\mathsf{H}_2\mathsf{H}_3^2 - \mathsf{G}_2\mathsf{H}_1\mathsf{H}_3\mathsf{I}_1 \\
&\quad -\mathsf{G}_1\mathsf{H}_2\mathsf{H}_3\mathsf{I}_1 - \mathsf{H}_1\mathsf{H}_2\mathsf{H}_3\mathsf{I}_1 - \mathsf{H}_2^2\mathsf{H}_3\mathsf{I}_1 + \mathsf{G}_1\mathsf{H}_3^2\mathsf{I}_1 + \mathsf{G}_3\mathsf{H}_3^2\mathsf{I}_1 - \mathsf{H}_1\mathsf{H}_3\mathsf{I}_1^2 + \mathsf{H}_3\mathsf{I}_1^3 + \mathsf{H}_1^3\mathsf{I}_2 \\
&\quad -\mathsf{G}_1^2\mathsf{H}_2\mathsf{I}_2 - \mathsf{G}_2\mathsf{G}_3\mathsf{H}_2\mathsf{I}_2 + \mathsf{G}_1\mathsf{H}_1\mathsf{H}_2\mathsf{I}_2 + \mathsf{G}_3\mathsf{H}_1\mathsf{H}_2\mathsf{I}_2 + \mathsf{H}_1^2\mathsf{H}_2\mathsf{I}_2 - 2\mathsf{G}_2\mathsf{H}_1\mathsf{H}_3\mathsf{I}_2 \\
&\quad -\mathsf{G}_3\mathsf{H}_1\mathsf{H}_3\mathsf{I}_2 - \mathsf{G}_1\mathsf{H}_2\mathsf{H}_3\mathsf{I}_2 - \mathsf{H}_1\mathsf{H}_2\mathsf{H}_3\mathsf{I}_2 - \mathsf{H}_2^2\mathsf{H}_3\mathsf{I}_2 + \mathsf{G}_1\mathsf{H}_3^2\mathsf{I}_2 + \mathsf{G}_3\mathsf{H}_3^2\mathsf{I}_2 - \mathsf{G}_1\mathsf{H}_1\mathsf{I}_1\mathsf{I}_2 \\
&\quad -\mathsf{H}_1^2\mathsf{I}_1\mathsf{I}_2 - \mathsf{H}_1\mathsf{H}_2\mathsf{I}_1\mathsf{I}_2 + \mathsf{G}_2\mathsf{H}_3\mathsf{I}_1\mathsf{I}_2 + \mathsf{G}_3\mathsf{H}_3\mathsf{I}_1\mathsf{I}_2 - \mathsf{H}_1\mathsf{H}_3\mathsf{I}_1\mathsf{I}_2 + \mathsf{G}_1\mathsf{I}_1^2\mathsf{I}_2 + 2\mathsf{H}_3\mathsf{I}_1^2\mathsf{I}_2 \\
&\quad -\mathsf{G}_2\mathsf{H}_1\mathsf{I}_2^2 + \mathsf{G}_2\mathsf{H}_3\mathsf{I}_2^2 + \mathsf{G}_3\mathsf{H}_3\mathsf{I}_2^2 + \mathsf{G}_1\mathsf{I}_1\mathsf{I}_2^2 + \mathsf{G}_2\mathsf{I}_1\mathsf{I}_2^2 - \mathsf{H}_1\mathsf{I}_1\mathsf{I}_2^2 + \mathsf{H}_3\mathsf{I}_1\mathsf{I}_2^2 + \mathsf{G}_2\mathsf{I}_2^3
\end{aligned}$$

$$
\begin{aligned}
&-H_1I_2^3+G_1^2H_3I_3+G_2G_3H_3I_3+H_1^2H_3I_3+G_1H_2H_3I_3+G_3H_2H_3I_3+H_1H_2H_3I_3\\
&-G_2H_3^2I_3-G_3H_3^2I_3-2G_1H_3I_1I_3-G_3H_3I_1I_3+H_3^2I_1I_3+G_2H_1I_2I_3+G_3H_1I_2I_3\\
&+H_1H_2I_2I_3+H_2^2I_2I_3-G_1H_3I_2I_3-G_2H_3I_2I_3-G_3H_3I_2I_3+H_1H_3I_2I_3+H_2H_3I_2I_3\\
&+H_3^2I_2I_3-G_2I_1I_2I_3-G_3I_1I_2I_3-H_3I_1I_2I_3-G_2I_2^2I_3-G_3I_2^2I_3-H_3I_2^2I_3+G_2H_3I_3^2\\
&+G_3H_3I_3^2-H_1H_3I_3^2-H_2H_3I_3^2\,. \qquad (17)
\end{aligned}
$$

It follows that $D, J \in \mathbf{Q}(G_1, G_2, G_3, H_1, H_2, H_3, I_1, I_2, I_3)$, which completes the proof. □

By the same way as in the proof of Lemma 7 above, we obtain the following three relations of $D, G_1, G_2, G_3, H_1, H_2, H_3, I_1, I_2, I_3$.

$$
\begin{cases}
r_1'(D, G_1, G_2, G_3, H_1, H_2, H_3, I_1, I_2, I_3) = 0\,,\\
r_2'(D, G_1, G_2, G_3, H_1, H_2, H_3, I_1, I_2, I_3) = 0\,,\\
r_3(G_1, G_2, G_3, H_1, H_2, H_3, I_1, I_2, I_3) = 0\,,
\end{cases}
$$

where

$$
r_1'(D, G_1, G_2, G_3, H_1, H_2, H_3, I_1, I_2, I_3) := \tau(\varphi_1(D, G_1, G_2, G_3, H_1, H_2, H_3, I_1, I_2, I_3))\,,
$$

$$
\begin{aligned}
&r_2'(D, G_1, G_2, G_3, H_1, H_2, H_3, I_1, I_2, I_3) :=\\
&\quad D(-H_1H_2I_1-H_1H_3I_1+H_1^2I_2-G_1H_2I_2+G_2H_2I_2-H_1H_3I_2+H_2I_1I_2+H_3I_1I_2\\
&\quad -H_1I_2^2+H_3I_2^2+H_1^2I_3+H_1H_2I_3+G_1H_3I_3-G_2H_3I_3-H_1I_2I_3-H_2I_2I_3)+G_2H_1^2H_2\\
&\quad +G_1H_1H_2^2+G_2H_1^2H_3-G_3H_1H_2H_3-G_1H_1H_3^2-G_3H_1H_3^2-H_1H_2^2I_1-H_1H_2H_3I_1\\
&\quad -H_1H_2I_1^2-H_1H_3I_1^2+H_1^3I_2-G_1^2H_2I_2-G_1G_3H_2I_2+H_1^2H_2I_2-G_1H_2^2I_2+G_2H_2^2I_2\\
&\quad -H_1H_2^2I_2-2G_2H_1H_3I_2-G_3H_1H_3I_2-G_1H_2H_3I_2+G_2H_2H_3I_2+G_3H_2H_3I_2\\
&\quad -H_1H_2H_3I_2+G_1H_3^2I_2+G_3H_3^2I_2-G_1H_1I_1I_2+G_2H_2I_1I_2+G_3H_2I_1I_2-H_1H_2I_1I_2\\
&\quad +H_2^2I_1I_2-H_1H_3I_1I_2+H_2H_3I_1I_2+H_3I_1^2I_2-G_2H_1I_2^2-G_1H_2I_2^2+G_2H_2I_2^2-H_1H_2I_2^2\\
&\quad +G_2H_3I_2^2+G_3H_3I_2^2+H_2H_3I_2^2+G_1I_1I_2^2+H_2I_1I_2^2+H_3I_1I_2^2+G_2I_2^3-H_1I_2^3+H_1^3I_3\\
&\quad +G_1H_1H_2I_3+G_3H_1H_2I_3+H_1^2H_2I_3+G_1^2H_3I_3+G_1G_3H_3I_3+G_1H_1H_3I_3\\
&\quad -2G_2H_1H_3I_3-G_2H_2H_3I_3+G_1H_3^2I_3-G_2H_3^2I_3-G_1H_1I_1I_3-G_2H_3I_1I_3-G_3H_3I_1I_3\\
&\quad +H_3I_1^2I_3+G_3H_1I_2I_3-G_1H_2I_2I_3-G_3H_2I_2I_3+H_1H_3I_2I_3+H_2H_3I_2I_3+G_1I_1I_2I_3\\
&\quad -G_3I_2^2I_3-H_1I_2^2I_3-H_2I_2^2I_3-H_3I_2^2I_3+G_2H_1I_3^2+G_3H_1I_3^2-G_2I_2I_3^2-G_3I_2I_3^2\,,
\end{aligned}
$$

$$
\begin{aligned}
&r_3(G_1, G_2, G_3, H_1, H_2, H_3, I_1, I_2, I_3) := G_1G_2-G_3^2-G_2H_1+H_1^2+G_3H_2\\
&\quad -H_2^2+G_1H_3-G_2H_3-G_1I_1-H_1I_1+I_1^2+G_3I_2+H_2I_2-I_2^2-G_1I_3+G_2I_3\,.
\end{aligned}
$$

We eliminate D from the relation $r_1' = 0$ (resp. $r_2' = 0$) by using $\varphi_1 = 0$ in (17), and obtain a relation $r_1 = 0$ (resp. $r_2 = 0$) of $\mathsf{G}_1, \mathsf{G}_2, \mathsf{G}_3, \mathsf{H}_1, \mathsf{H}_2, \mathsf{H}_3, \mathsf{I}_1, \mathsf{I}_2, \mathsf{I}_3$. Thus we have three relations $r_1 = 0$, $r_2 = 0$, $r_3 = 0$ of $\mathsf{G}_1, \mathsf{G}_2, \mathsf{G}_3, \mathsf{H}_1, \mathsf{H}_2, \mathsf{H}_3, \mathsf{I}_1, \mathsf{I}_2, \mathsf{I}_3$. Next, as in the quintic case, we transform the variables as follows:

$$\begin{array}{llll} \mathsf{v}_1 := \mathsf{G}_1 - \mathsf{G}_3\,, & \mathsf{v}_2 := \mathsf{G}_2 - \mathsf{G}_3\,, & \mathsf{v}_3 := \mathsf{H}_1 - \mathsf{G}_3\,, & \mathsf{v}_4 := \mathsf{H}_2 - \mathsf{G}_3\,, \\ \mathsf{v}_5 := \mathsf{H}_3 - \mathsf{G}_3\,, & \mathsf{v}_6 := \mathsf{I}_1 - \mathsf{G}_3\,, & \mathsf{v}_7 := \mathsf{I}_2 - \mathsf{G}_3\,, & \mathsf{v}_8 := \mathsf{I}_3 - \mathsf{G}_3\,. \end{array} \tag{18}$$

Then it follows from Lemma 7 that $\mathbf{Q}(y_0, \cdots, y_5)^{C_6} = \mathbf{Q}(\mathsf{v}_1, \cdots, \mathsf{v}_8, \mathsf{G}_3)$ and we see that the quartic relation $r_1(\mathsf{G}_1, \mathsf{G}_2, \mathsf{G}_3, \mathsf{H}_1, \mathsf{H}_2, \mathsf{H}_3, \mathsf{I}_1, \mathsf{I}_2, \mathsf{I}_3)$ is transformed to a linear relation in G_3.

$$\begin{aligned} &r_1(\mathsf{v}_1 + \mathsf{G}_3, \mathsf{v}_2 + \mathsf{G}_3, \mathsf{G}_3, \mathsf{v}_3 + \mathsf{G}_3, \mathsf{v}_4 + \mathsf{G}_3, \mathsf{v}_5 + \mathsf{G}_3, \mathsf{v}_6 + \mathsf{G}_3\,, \mathsf{v}_7 + \mathsf{G}_3, \mathsf{v}_8 + \mathsf{G}_3) = \\ &\quad \mathsf{G}_3(\mathsf{v}_3 - \mathsf{v}_5 - \mathsf{v}_6 + \mathsf{v}_8)(\mathsf{v}_1^2 - \mathsf{v}_2^2 + 2\,\mathsf{v}_2\mathsf{v}_3 + 2\,\mathsf{v}_3^2 + 2\,\mathsf{v}_1\mathsf{v}_4 + \mathsf{v}_2\mathsf{v}_4 + 2\,\mathsf{v}_3\mathsf{v}_4 - \mathsf{v}_1\mathsf{v}_5 \\ &\quad -\mathsf{v}_2\mathsf{v}_5 - 2\,\mathsf{v}_3\mathsf{v}_5 - 2\,\mathsf{v}_4\mathsf{v}_5 - 2\,\mathsf{v}_1\mathsf{v}_6 + \mathsf{v}_4\mathsf{v}_6 + 4\,\mathsf{v}_5\mathsf{v}_6 - 2\,\mathsf{v}_6^2 - \mathsf{v}_1\mathsf{v}_7 - 2\,\mathsf{v}_2\mathsf{v}_7 - \mathsf{v}_3\mathsf{v}_7 \\ &\quad +4\,\mathsf{v}_5\mathsf{v}_7 - 2\,\mathsf{v}_6\mathsf{v}_7 + \mathsf{v}_1\mathsf{v}_8 + \mathsf{v}_2\mathsf{v}_8 - 4\,\mathsf{v}_3\mathsf{v}_8 - 4\,\mathsf{v}_4\mathsf{v}_8 + 2\,\mathsf{v}_6\mathsf{v}_8 + 2\,\mathsf{v}_7\mathsf{v}_8) + \mathsf{v}_2\mathsf{v}_3^3 \\ &\quad +\mathsf{v}_1\mathsf{v}_3^2\mathsf{v}_4 + \mathsf{v}_2\mathsf{v}_3^2\mathsf{v}_4 + \mathsf{v}_1\mathsf{v}_3\mathsf{v}_4^2 - \mathsf{v}_1\mathsf{v}_3^2\mathsf{v}_5 - \mathsf{v}_2\mathsf{v}_3^2\mathsf{v}_5 - 2\,\mathsf{v}_1\mathsf{v}_3\mathsf{v}_4\mathsf{v}_5 - \mathsf{v}_2\mathsf{v}_3\mathsf{v}_4\mathsf{v}_5 - \mathsf{v}_1\mathsf{v}_4^2\mathsf{v}_5 \\ &\quad +\mathsf{v}_1\mathsf{v}_3\mathsf{v}_5^2 + \mathsf{v}_1\mathsf{v}_4\mathsf{v}_5^2 - \mathsf{v}_2\mathsf{v}_3^2\mathsf{v}_6 + \mathsf{v}_3^3\mathsf{v}_6 - \mathsf{v}_1^2\mathsf{v}_4\mathsf{v}_6 - \mathsf{v}_3\mathsf{v}_4^2\mathsf{v}_6 + \mathsf{v}_2^2\mathsf{v}_5\mathsf{v}_6 + \mathsf{v}_1\mathsf{v}_3\mathsf{v}_5\mathsf{v}_6 \\ &\quad -\mathsf{v}_2\mathsf{v}_3\mathsf{v}_5\mathsf{v}_6 - \mathsf{v}_1\mathsf{v}_3\mathsf{v}_6^2 - 2\,\mathsf{v}_3^2\mathsf{v}_6^2 - \mathsf{v}_3\mathsf{v}_4\mathsf{v}_6^2 + \mathsf{v}_3\mathsf{v}_5\mathsf{v}_6^2 - \mathsf{v}_5^2\mathsf{v}_6^2 + \mathsf{v}_1\mathsf{v}_6^3 + \mathsf{v}_3\mathsf{v}_6^3 - \mathsf{v}_2^2\mathsf{v}_3\mathsf{v}_7 \\ &\quad +\mathsf{v}_2^2\mathsf{v}_5\mathsf{v}_7 - \mathsf{v}_3^2\mathsf{v}_6\mathsf{v}_7 + 2\,\mathsf{v}_3\mathsf{v}_5\mathsf{v}_6\mathsf{v}_7 - 2\,\mathsf{v}_5^2\mathsf{v}_6\mathsf{v}_7 + \mathsf{v}_1\mathsf{v}_6^2\mathsf{v}_7 + \mathsf{v}_2\mathsf{v}_6^2\mathsf{v}_7 + \mathsf{v}_3\mathsf{v}_5\mathsf{v}_7^2 - \mathsf{v}_5^2\mathsf{v}_7^2 \\ &\quad +\mathsf{v}_2\mathsf{v}_6\mathsf{v}_7^2 - \mathsf{v}_3\mathsf{v}_6\mathsf{v}_7^2 + \mathsf{v}_1^2\mathsf{v}_3\mathsf{v}_8 + \mathsf{v}_1^2\mathsf{v}_4\mathsf{v}_8 - \mathsf{v}_1^2\mathsf{v}_5\mathsf{v}_8 - \mathsf{v}_2^2\mathsf{v}_5\mathsf{v}_8 + \mathsf{v}_2\mathsf{v}_3\mathsf{v}_5\mathsf{v}_8 - \mathsf{v}_3^2\mathsf{v}_5\mathsf{v}_8 \\ &\quad +\mathsf{v}_4^2\mathsf{v}_5\mathsf{v}_8 - \mathsf{v}_1\mathsf{v}_5^2\mathsf{v}_8 + \mathsf{v}_2\mathsf{v}_5^2\mathsf{v}_8 - \mathsf{v}_1\mathsf{v}_3\mathsf{v}_6\mathsf{v}_8 + \mathsf{v}_2\mathsf{v}_3\mathsf{v}_6\mathsf{v}_8 + \mathsf{v}_3^2\mathsf{v}_6\mathsf{v}_8 + 2\,\mathsf{v}_3\mathsf{v}_4\mathsf{v}_6\mathsf{v}_8 \\ &\quad +\mathsf{v}_4^2\mathsf{v}_6\mathsf{v}_8 + \mathsf{v}_1\mathsf{v}_5\mathsf{v}_6\mathsf{v}_8 + 2\,\mathsf{v}_3\mathsf{v}_5\mathsf{v}_6\mathsf{v}_8 + \mathsf{v}_4\mathsf{v}_5\mathsf{v}_6\mathsf{v}_8 - \mathsf{v}_1\mathsf{v}_6^2\mathsf{v}_8 - \mathsf{v}_2\mathsf{v}_6^2\mathsf{v}_8 - \mathsf{v}_5\mathsf{v}_6^2\mathsf{v}_8 \\ &\quad +\mathsf{v}_3\mathsf{v}_5\mathsf{v}_7\mathsf{v}_8 - \mathsf{v}_1\mathsf{v}_6\mathsf{v}_7\mathsf{v}_8 - 2\,\mathsf{v}_2\mathsf{v}_6\mathsf{v}_7\mathsf{v}_8 - \mathsf{v}_2\mathsf{v}_7^2\mathsf{v}_8 + \mathsf{v}_5\mathsf{v}_7^2\mathsf{v}_8 - \mathsf{v}_3^2\mathsf{v}_8^2 - 2\,\mathsf{v}_3\mathsf{v}_4\mathsf{v}_8^2 - \mathsf{v}_4^2\mathsf{v}_8^2 \\ &\quad +\mathsf{v}_1\mathsf{v}_5\mathsf{v}_8^2 - \mathsf{v}_2\mathsf{v}_5\mathsf{v}_8^2 + \mathsf{v}_2\mathsf{v}_6\mathsf{v}_8^2 + \mathsf{v}_2\mathsf{v}_7\mathsf{v}_8^2 = 0\,. \end{aligned}$$

Hence we have $\mathsf{G}_3 \in \mathbf{Q}(\mathsf{v}_1, \cdots, \mathsf{v}_8)$. This shows that

$$\mathbf{Q}(y_0, \cdots, y_5)^{C_6} = \mathbf{Q}(\mathsf{v}_1, \mathsf{v}_2, \mathsf{v}_3, \mathsf{v}_4, \mathsf{v}_5, \mathsf{v}_6, \mathsf{v}_7, \mathsf{v}_8)\,.$$

By eliminating the variable G_3 from the relation

$$r_2(\mathsf{v}_1 + \mathsf{G}_3, \mathsf{v}_2 + \mathsf{G}_3, \mathsf{G}_3, \mathsf{v}_3 + \mathsf{G}_3, \mathsf{v}_4 + \mathsf{G}_3, \mathsf{v}_5 + \mathsf{G}_3\,, \mathsf{v}_6 + \mathsf{G}_3, \mathsf{v}_7 + \mathsf{G}_3, \mathsf{v}_8 + \mathsf{G}_3) = 0\,,$$

we obtain the following relation of $\mathsf{v}_1, \cdots, \mathsf{v}_8$.

$$\begin{aligned} &\mathsf{v}_1\mathsf{v}_2\mathsf{v}_3^2 - \mathsf{v}_2\mathsf{v}_3^3 + \mathsf{v}_3^4 - \mathsf{v}_1^3\mathsf{v}_4 + \mathsf{v}_1^2\mathsf{v}_2\mathsf{v}_4 + \mathsf{v}_1^2\mathsf{v}_3\mathsf{v}_4 - \mathsf{v}_1\mathsf{v}_2\mathsf{v}_3\mathsf{v}_4 - \mathsf{v}_2^2\mathsf{v}_3\mathsf{v}_4 + \mathsf{v}_2\mathsf{v}_3^2\mathsf{v}_4 + \mathsf{v}_1^2\mathsf{v}_4^2 \\ &\quad -\mathsf{v}_1\mathsf{v}_2\mathsf{v}_4^2 + \mathsf{v}_2\mathsf{v}_3\mathsf{v}_4^2 - \mathsf{v}_3^2\mathsf{v}_4^2 + \mathsf{v}_1\mathsf{v}_2^2\mathsf{v}_5 - \mathsf{v}_2^3\mathsf{v}_5 - \mathsf{v}_1^2\mathsf{v}_3\mathsf{v}_5 - \mathsf{v}_1\mathsf{v}_2\mathsf{v}_3\mathsf{v}_5 + \mathsf{v}_2^2\mathsf{v}_3\mathsf{v}_5 \\ &\quad +\mathsf{v}_1\mathsf{v}_3^2\mathsf{v}_5 - \mathsf{v}_3^3\mathsf{v}_5 - \mathsf{v}_1^2\mathsf{v}_4\mathsf{v}_5 + 2\,\mathsf{v}_1\mathsf{v}_2\mathsf{v}_4\mathsf{v}_5 - \mathsf{v}_1\mathsf{v}_3\mathsf{v}_4\mathsf{v}_5 - \mathsf{v}_1\mathsf{v}_4^2\mathsf{v}_5 + \mathsf{v}_3\mathsf{v}_4^2\mathsf{v}_5 + \mathsf{v}_1^2\mathsf{v}_5^2 \end{aligned}$$

$$
\begin{aligned}
&-v_1v_2v_5^2+v_1v_4v_5^2-v_2v_4v_5^2-v_1v_3^2v_6-v_3^3v_6+v_1v_2v_4v_6-v_1v_3v_4v_6+v_3^2v_4v_6\\
&-v_1v_4^2v_6+v_3v_4^2v_6-v_1v_2v_5v_6+2\,v_1v_3v_5v_6+v_1v_4v_5v_6-v_2v_4v_5v_6-v_3v_4v_5v_6\\
&-2\,v_1v_5^2v_6+2\,v_2v_5^2v_6-v_1v_2v_6^2+v_2v_3v_6^2-2\,v_3v_4v_6^2+v_2v_5v_6^2+v_4v_5v_6^2+v_1v_6^3\\
&+v_3v_6^3+v_4v_6^3-v_5v_6^3-v_6^4-v_1v_2^2v_7+v_2^3v_7-v_1v_2v_3v_7-v_3^3v_7+v_1v_2v_5v_7\\
&+v_3^2v_5v_7-v_1v_5^2v_7+v_2v_5^2v_7+v_1^2v_6v_7+v_1v_2v_6v_7-v_2^2v_6v_7+v_2v_3v_6v_7+2\,v_3^2v_6v_7\\
&-v_2v_5v_6v_7-v_3v_5v_6v_7-v_1v_6^2v_7-v_3v_6^2v_7+v_1v_2v_7^2-v_2^2v_7^2+v_2v_3v_7^2-v_2v_5v_7^2\\
&-v_1v_6v_7^2-v_3v_6v_7^2+v_5v_6v_7^2+v_6^2v_7^2+v_1^3v_8-v_1^2v_2v_8+v_1v_2v_3v_8-v_1v_3^2v_8+v_3^3v_8\\
&-v_1v_2v_4v_8+v_1v_3v_4v_8+v_1v_4^2v_8-v_3v_4^2v_8-v_1^2v_5v_8+v_2^2v_5v_8+2\,v_1v_3v_5v_8\\
&-2\,v_2v_3v_5v_8-v_1^2v_6v_8+v_1v_2v_6v_8+v_2^2v_6v_8-2\,v_2v_3v_6v_8+v_3v_4v_6v_8+2\,v_1v_5v_6v_8\\
&-2\,v_2v_5v_6v_8-v_2v_6^2v_8-v_4v_6^2v_8+v_6^3v_8-2\,v_1v_2v_7v_8+v_2^2v_7v_8+v_1v_3v_7v_8\\
&-v_2v_3v_7v_8-v_3^2v_7v_8+v_2v_6v_7v_8+v_3v_6v_7v_8+v_2v_7^2v_8-v_6v_7^2v_8+v_1v_2v_8^2\\
&-v_2^2v_8^2-2\,v_1v_3v_8^2+2\,v_2v_3v_8^2-v_1v_4v_8^2+v_2v_4v_8^2+v_1v_7v_8^2-v_2v_7v_8^2=0\,.
\end{aligned}
\tag{19}
$$

On the other hand, the relation $r_3 = 0$ is transformed by (18) to the following

$$
\begin{aligned}
&v_1v_2-v_2v_3+v_3^2-v_4^2+v_1v_5-v_2v_5-v_1v_6-v_3v_6+v_6^2+v_4v_7\\
&-v_7^2-v_1v_8+v_2v_8=0\,.
\end{aligned}
\tag{20}
$$

Therefore we have that $\mathbf{Q}(y_0,\cdots,y_5)^{C_6} = \mathbf{Q}(v_1,\cdots,v_8)$, where $v_1,\cdots,v_8$ satisfy the equations (19) and (20). Using this, we obtain the following set of generators of the fixed field $\mathbf{Q}(y_0,\cdots,y_5)^{C_6}$, which gives an affirmative answer to Noether's problem for C_6.

PROPOSITION 8. *We have*

$$
\boldsymbol{Q}(y_0,\cdots,y_5)^{C_6} = \boldsymbol{Q}(G_1-G_3, G_2-G_3, H_1-G_3, H_2-G_3, I_1-G_3, I_2-G_3)\,.
$$

PROOF. We should show that $v_5, v_8 \in \mathbf{Q}(v_1,v_2,v_3,v_4,v_6,v_7)$. We have from (20) that

$$
v_5 = \frac{v_1v_2-v_2v_3+v_3^2-v_4^2-v_1v_6-v_3v_6+v_6^2+v_4v_7-v_7^2-v_1v_8+v_2v_8}{v_2-v_1}\,.
$$

By using this, we can eliminate v_5 from the equation (19). A direct computation shows that the result is a linear equation in v_8. Hence we have $\mathbf{Q}(y_0,\cdots,y_5)^{C_6} = \mathbf{Q}(v_1,v_2,v_3,v_4,v_6,v_7)$, which completes the proof. □

From Proposition 8 and (16), we obtain the following set of independent generators of the fixed field $\mathbf{Q}(y_0,\cdots,y_5)^{D_6}$. It shows, in particular, that Noether's problem for D_6 also has an affirmative answer.

THEOREM 9. *We have*

$$\boldsymbol{Q}(y_0,\cdots,y_5)^{D_6} = \boldsymbol{Q}(\mathsf{G}_1+\mathsf{G}_2-2\,\mathsf{G}_3, \mathsf{H}_1+\mathsf{I}_1-2\,\mathsf{G}_3, \mathsf{H}_2+\mathsf{I}_2-2\,\mathsf{G}_3\,, \\ (\mathsf{G}_1-\mathsf{G}_2)^2, (\mathsf{G}_1-\mathsf{G}_2)(\mathsf{H}_1-\mathsf{I}_1)\,, (\mathsf{G}_1-\mathsf{G}_2)(\mathsf{H}_2-\mathsf{I}_2))\,.$$

PROOF. We see that $(D_6/C_6) \cong \langle\tau\rangle$ acts on $\mathbf{Q}(y_0,\cdots,y_5)^{C_6} = \mathbf{Q}(\mathsf{v}_1,\mathsf{v}_2,\mathsf{v}_3,\mathsf{v}_4,\mathsf{v}_6,\mathsf{v}_7)$ as

$$\tau : \mathsf{v}_1 \mapsto \mathsf{v}_2 \mapsto \mathsf{v}_1\,, \quad \mathsf{v}_3 \mapsto \mathsf{v}_6 \mapsto \mathsf{v}_3\,, \quad \mathsf{v}_4 \mapsto \mathsf{v}_7 \mapsto \mathsf{v}_4\,.$$

It follows from Lemma 2 that

$$\mathbf{Q}(y_0,\cdots,y_5)^{D_6} = \mathbf{Q}(\mathsf{v}_1+\mathsf{v}_2, \mathsf{v}_3+\mathsf{v}_6, \mathsf{v}_4+\mathsf{v}_7\,, (\mathsf{v}_1-\mathsf{v}_2)^2, (\mathsf{v}_1-\mathsf{v}_2)(\mathsf{v}_3-\mathsf{v}_6)\,, \\ (\mathsf{v}_1-\mathsf{v}_2)(\mathsf{v}_4-\mathsf{v}_7))\,.$$

The assertion follows from this. □

References

[1] S. ENDO and T. MIYATA, Invariants of finite abelian groups, J. Math. Soc. Japan **25** (1973), 7–26.

[2] K. HASHIMOTO and A. HOSHI, Families of cyclic polynomials obtained from geometric generalization of Gaussian period relations, to appear in Math. Comp.

[3] C. JENSEN, A. LEDET and N. YUI, *Generic polynomials*, *constructive aspects of the inverse Galois problem*, Mathematical Sciences Research Institute Publications, **45** (2002), Cambridge.

[4] G. KEMPER, A constructive approach to Noether's Problem, Manuscripta Math. **90** (1996), 343–363.

[5] G. KEMPER and E. MATTIG, Generic polynomials with few parameters, J. Symbolic Comp. **30** (2000), 843–857.

[6] D. H. LEHMER and E. LEHMER, The Lehmer project, Math. Comp. **61** (1993), 313–317.

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

[8] H. W. LENSTRA, Rational functions invariant under a finite abelian group, Invent. Math. **25** (1974), 299–325.

[9] H. W. LENSTRA, Rational functions invariant under a cyclic group, Queen's Papers in Pure and Appl. Math. **54** (1980), 91–99.

[10] T. MAEDA, Noether's problem for A_5, J. Algebra **125** (1989), 418–430.

[11] G. MALLE and B. H. MATZAT, *Inverse Galois Theory*, Springer Monographs in Mathematics, Springer, (1999).

[12] K. MASUDA, On a problem of Chevalley, Nagoya Math. J. **8** (1955), 59–63.

[13] K. MASUDA, Application of theory of the group of classes of projective modules to existence problem of independent parameters of invariant, J. Math. Soc. Japan **20** (1968), 223–232.

[14] E. NOETHER, Gleichungen mit vorgeschriebener Gruppe, Math. Ann. **78** (1918), 221–229.

[15] R. SCHOOF and L. C. WASHINGTON, Quintic polynomials and real cyclotomic fields with large class numbers, Math. Comp. **50** (1988), 543–556.

[16] J-P. SERRE, *Topics in Galois Theory*, Research Notes in Mathematics, **1** (1992), Jones and Bartlett Publishers.

[17] R. G. SWAN, Invariant rational functions and a problem of Steenrod, Invent. Math. **7** (1969), 148–158.

[18] R. G. SWAN, Noether's Problem in Galois Theory, *Emmy Noether in Bryn Mawr* (1983), Springer, 21–40.

[19] F. THAINE, Properties that characterize Gaussian periods and cyclotomic numbers, Proc. Amer. Math. Soc. **124** (1996), 35–45.

[20] F. THAINE, On the coefficients of Jacobi sums in prime cyclotomic fields, Trans. Amer. Math. Soc. **351** (1999), 4769–4790.

[21] F. THAINE, Families of irreducible polynomials of Gaussian periods and matrices of cyclotomic numbers, Math. Comp. **69** (2000), 1653–1666.

[22] F. THAINE, Jacobi sums and new families of irreducible polynomials of Gaussian periods, Math. Comp. **70** (2001), 1617–1640.

[23] V. E. VOSKRESENSKIĬ, On the question of the structure of the subfield of invariants of a cyclic group of automorphisms of the field $\mathbf{Q}(x_1, \cdots, x_n)$ (Russian). Izv. Akad. Nauk SSSR Ser. Mat. **34** (1970), 366–375. English translation : Math. USSR-Izv. **4** (1970), 371–380.

[24] V. E. VOSKRESENSKIĬ, Fields of invariants of abelian groups (Russian). Uspekhi Mat. Nauk **28** (1973), 77–102. English translation: Russian Math. Surveys **28** (1973), 79–105.

[25] V. E. VOSKRESENSKIĬ, *Algebraic groups and their birational invariants*, Translations of Mathematical Monographs **179** (1998), Amer. Math. Soc.

[26] S. WOLFRAM, *The Mathematica book. Fourth edition*, Wolfram Media, Inc., Cambridge University Press, (1999).

Present Address:
DEPARTMENT OF MATHEMATICAL SCIENCES, SCHOOL OF SCIENCE AND ENGINEERING,
WASEDA UNIVERSITY,
OHKUBO, SHINJUKU-KU, TOKYO 169–8555, JAPAN.
e-mail: khasimot@waseda.jp
hoshi@ruri.waseda.jp