MATHEMATICS OF COMPUTATION
Volume 77, Number 262, April 2008, Pages 1153–1183
S 0025-5718(07)02094-7
Article electronically published on December 3, 2007

NOETHER'S PROBLEM AND $\mathbb{Q}$-GENERIC POLYNOMIALS FOR THE NORMALIZER OF THE 8-CYCLE IN S_8 AND ITS SUBGROUPS

KI-ICHIRO HASHIMOTO, AKINARI HOSHI, AND YŪICHI RIKUNA

ABSTRACT. We study Noether's problem for various subgroups H of the normalizer of a group $\mathbf{C}_8$ generated by an 8-cycle in S_8, the symmetric group of degree 8, in three aspects according to the way they act on rational function fields, i.e., $\mathbb{Q}(X_0,\dots,X_7)$, $\mathbb{Q}(x_1,\dots,x_4)$, and $\mathbb{Q}(x,y)$. We prove that it has affirmative answers for those H containing $\mathbf{C}_8$ properly and derive a $\mathbb{Q}$-generic polynomial with four parameters for each H. On the other hand, it is known in connection to the negative answer to the same problem for $\mathbf{C}_8/\mathbb{Q}$ that there does not exist a $\mathbb{Q}$-generic polynomial for $\mathbf{C}_8$. This leads us to the question whether and how one can describe, for a given field K of characteristic zero, the set of $\mathbf{C}_8$-extensions L/K. One of the main results of this paper gives an answer to this question.

1. INTRODUCTION

Let G be a transitive permutation group on the set $\underline{t}$ of n variables $t_1,\dots,t_n$ regarded as a group of k-automorphisms of $k(\underline{t}) = k(t_1,\dots,t_n)$, the field of rational functions over a given field k. Noether's problem, which will be abbreviated as NP in this paper, asks whether the subfield consisting of G-invariant elements of $k(\underline{t})$ is again a rational function field or not. As is well known, the motivation for this problem was that it is a main step toward the solution of the inverse Galois problem for G and k. Indeed if NP has an affirmative answer, then one can prove the existence of infinitely many Galois extensions L/k such that $\mathrm{Gal}(L/k) \cong G$ by applying Hilbert's irreducibility theorem, for a large class of fields k called *Hilbertian*. Unfortunately, it has been shown that NP does not always have an affirmative answer even for abelian groups, a well-known counterexample over $\mathbb{Q}$ being the case $G = \mathbf{C}_8$, the cyclic group of order 8. Nevertheless the importance of NP with its generalization to groups G acting linearly on $k(\underline{t})$ has recently increased because of its connection to *generic polynomials* (cf. [JLY]). Let $F(\underline{t}; X) \in k(\underline{t})[X]$ be a polynomial in X whose coefficients are rational functions of $t_1,\dots,t_n$. $F(\underline{t}; X)$ is called *a G-polynomial over k with n parameters*, if its Galois group over $k(\underline{t})$ is isomorphic to G.

Definition 1.1 (DeMeyer [DeM])**.** A G-polynomial $F(\underline{t}; X)$ over a field k is called *k-generic* if it has the following property: for every G-Galois extension L/K of infinite fields with $K \supset k$, there exists $\underline{a} \in K^n$ such that L is the splitting field of $F(\underline{a}; X) \in K[X]$ over K.

Received by the editor October 12, 2006 and, in revised form, January 25, 2007.
2000 *Mathematics Subject Classification.* Primary 12F12, 14E08, 11R32.

Let $\rho : G \to \mathbf{GL}_n(k)$ be a faithful linear representation of a finite group acting on $k(\underline{t})$ by k-linear transformations on $t_1, \ldots, t_n$ via ρ. Then $k(\underline{t})$ is a regular G-Galois extension over the fixed field $k(\underline{t})^G$. The same question as NP in this situation is called the Linear Noether's Problem, LNP for short. The following result of G. Kemper and E. Mattig is basic to the study of generic polynomials.

Fact 1.2 (Kemper-Mattig [KM])**.** *If the fixed field $k(\underline{x})^G$ is k-rational, i.e., purely transcendental over k, then there exists a k-generic G-polynomial with n parameters.*

Assuming the existence of k-generic G-polynomials for given k and G, a problem that arises naturally is to minimize the number of parameters.

Definition 1.3 (Jensen–Ledet–Yui [JLY])**.** For a finite group G and a field k, *the generic dimension of G/k*, denoted by $\mathrm{gd}_k(G)$, is defined to be the minimum number of parameters of k-generic G-polynomials. If no such polynomial exists, we set $\mathrm{gd}_k(G) = \infty$.

It is known in connection with the negative answer to NP for the cyclic group $\mathbf{C}_8$ of order 8 over $\mathbb{Q}$ that $\mathrm{gd}_{\mathbb{Q}}(\mathbf{C}_8) = \infty$. This leads us to the question whether and how one can describe, for any given field K of characteristic zero, the set of $\mathbf{C}_8$-extensions L/K. One of the main results of this paper gives a fairly satisfactory answer to this question. We shall construct the following family of polynomials:

$$\begin{aligned} F(a,b,c,d;X) := {} & X^8 - dX^6 \\ & + \left(\frac{(a^2+b^2-c^2)}{4(a^2+b^2)} + \frac{(a^2+b^2-1)^2((a-c)^2+b^2)}{2^4(a^2+b^2)(a^2+b^2+1)(a^2+(b-1)^2)} \right) d^2 X^4 \\ & - \frac{(a^2+b^2-1)^2(a^2+b^2-ac)(a^2+b^2-c^2)d^3}{2^5(a^2+b^2)^2(a^2+b^2+1)(a^2+(b-1)^2)} X^2 \\ & + \frac{b^2(a^2+b^2-1)^4(a^2+b^2-c^2)^2 d^4}{2^{10}(a^2+b^2)^3(a^2+b^2+1)^2(a^2+(b-1)^2)^2} \end{aligned}$$

of degree 8, and show that it is a *generic* polynomial over $\mathbb{Q}$ for the modular type 2-group $\mathbf{M}_{16}$ of order 16, when a, b, c, d are regarded as independent parameters (see below for the definition of $\mathbf{M}_{16}$). On the other hand, we define a polynomial equation in a, b, c and a new indeterminate e by

$$V(a,b,c,e) \;:=\; (a^2+b^2-c^2) - 2e^2(a^2+b^2+1) \;=\; 0.$$

Then we shall prove that $F(a,b,c,d;X)$ with the condition $V(a,b,c,e) = 0$ is a *versal* polynomial for $\mathbf{C}_8$ over $\mathbb{Q}$, in the sense of Buhler–Reichstein [BR]:

Theorem 1.4. *Let K be a field of characteristic zero and suppose that $a, b, c, d, e \in K$ satisfy $V(a,b,c,e) = 0$ while $a^2 + b^2$ is a nonsquare element in $K^\times$. Then the splitting field of $F(a,b,c,d;X)$ over K is a $\mathbf{C}_8$-extension of K which contains $K(\sqrt{a^2+b^2})$ as its unique quadratic subextension. Furthermore, any $\mathbf{C}_8$-extension of K is obtained in this way.*

Now we put

$$R(a,b,c) := \frac{2(a^2+b^2-c^2)}{a^2+b^2+1} \quad (=\, 4\,e^2\,).$$

As a corollary of the above theorem, we obtain

Corollary 1.5. *Let $K = k(\sqrt{a^2+b^2})$ be a quadratic extension of a field k of characteristic zero. For the existence of a $\mathbf{C}_8$-extension of k containing K, it is necessary and sufficient that there exists $c \in k^\times$ for which $R(a,b,c)$ is a nonzero square in k.*

As for the groups with $\mathrm{gd}_{\mathbb{Q}}(G) = \infty$, the next result is known (cf. [JLY]).

Fact 1.6. *Let G be an abelian group. Then $\mathrm{gd}_{\mathbb{Q}}(G) = \infty$ if and only if G has an element of order eight.*

Therefore, $\mathbf{C}_8$ is the smallest abelian group whose generic dimension over $\mathbb{Q}$ is infinite. This leads us also to the study of NP or LNP for the smallest nonabelian groups which contain $\mathbf{C}_8$ as a subgroup. There exist four such groups, all of which have order sixteen:

- $\mathbf{D}_8 \cong \langle \alpha, \beta \mid \alpha^8 = \beta^2 = 1,\ \beta\alpha\beta^{-1} = \alpha^{-1} \rangle$, the dihedral group,
- $\mathbf{QD}_8 \cong \langle \alpha, \beta \mid \alpha^8 = \beta^2 = 1,\ \beta\alpha\beta^{-1} = \alpha^{3} \rangle$, the quasi-dihedral group,
- $\mathbf{M}_{16} \cong \langle \alpha, \beta \mid \alpha^8 = \beta^2 = 1,\ \beta\alpha\beta^{-1} = \alpha^{5} \rangle$, the modular type 2-group,
- $\mathbf{Q}_{16} \cong \langle \alpha, \beta \mid \alpha^8 = 1,\ \alpha^4 = \beta^2,\ \beta\alpha\beta^{-1} = \alpha^{-1} \rangle$, the (generalized) quaternion group.

For these groups, it is known (cf. [JLY]) that

$$2 \le \mathrm{gd}_{\mathbb{Q}}(\mathbf{D}_8),\ \mathrm{gd}_{\mathbb{Q}}(\mathbf{QD}_8) \le 5, \quad 3 \le \mathrm{gd}_{\mathbb{Q}}(\mathbf{M}_{16}) \le 5, \quad 2 \le \mathrm{gd}_{\mathbb{Q}}(\mathbf{Q}_{16}).$$

The upper bounds are determined by constructing generic Galois extensions.[1] One of the motivations of this paper is to improve these upper bounds by giving generic polynomials with four parameters except for $\mathbf{Q}_{16}$.[2]

Our construction is based on the positive answers to four-dimensional LNP over $\mathbb{Q}$ for these three groups with an explicitly given set of generators. Actually, we study NP for these groups at the same time by observing that they are maximal subgroups of index two of the single group $\mathbf{G}_0$, which is the normalizer of a group generated by an 8-cycle in the symmetric group S_8 of degree 8. The group $\mathbf{G}_0$ is a meta-abelian group of order 32 and is isomorphic to the affine transformation group over $\mathbb{Z}/8\mathbb{Z}$, which is expressed as $(\mathbb{Z}/8\mathbb{Z}) \rtimes (\mathbb{Z}/8\mathbb{Z})^\times$. We denote by A the element of $\mathbf{G}_0$ corresponding to $1 \in \mathbb{Z}/8\mathbb{Z}$ and by $B_{_D}, B_{_Q}, B_{_M} \in \mathbf{G}_0$ the elements of order 2 corresponding to those in $(\mathbb{Z}/8\mathbb{Z})^\times$ so that

$$\langle A, B_{_D} \rangle \cong \mathbf{D}_8, \quad \langle A, B_{_Q} \rangle \cong \mathbf{QD}_8, \quad \langle A, B_{_M} \rangle \cong \mathbf{M}_{16}$$

respectively. As is well known, $\mathbf{G}_0$ has a faithful representation $\rho : \mathbf{G}_0 \to \mathbf{GL}_4(\mathbb{Q})$, which is unique up to the conjugation in $\mathbf{GL}_4(\mathbb{Q})$. Our results in the first two sections are computational answers to NP and LNP for subgroups of $\mathbf{G}_0$.

Theorem 1.7. *Noether's Problems and Linear Noether's Problems for $\mathbf{G}_0/\mathbb{Q}$ with respect to the representation ρ, as well as its subgroups $\mathbf{D}_8$, $\mathbf{QD}_8$, and $\mathbf{M}_{16}$, have affirmative answers.*

We then apply the result of Kemper-Mattig [KM] to obtain the following.

Corollary 1.8. *We have*

$$\mathrm{gd}_{\mathbb{Q}}(\mathbf{G}_0),\ \mathrm{gd}_{\mathbb{Q}}(\mathbf{D}_8),\ \mathrm{gd}_{\mathbb{Q}}(\mathbf{QD}_8),\ \mathrm{gd}_{\mathbb{Q}}(\mathbf{M}_{16}) \ \le\ 4.$$

[1] The left sides of the above equalities are trivial except for $\mathbf{M}_{16}$. In general, $\mathrm{ed}_k(G) \le \mathrm{gd}_k(G)$, where $\mathrm{ed}_k(G)$ is the essential dimension of G/k. Also, $\mathrm{ed}_{\mathbb{Q}}(G) = 1$ if and only if G is isomorphic to $\mathbf{C}_2, \mathbf{C}_3$, or $\mathbf{D}_3$ (see [BR], [Led2]).

[2] It has been settled that NP has a negative solution for $\mathbf{Q}_{16}$ (cf. [GMS], Theorem 34.7).

We should remark that the results of Theorem 1.7 have recently been obtained for $\mathbf{D}_8$, $\mathbf{QD}_8$, and $\mathbf{M}_{16}$ by [CHK] in a considerably different way. What we do here is *not only* to prove the rationality of the fixed fields, *but also* to find a set of explicit generators which enables us to construct a $\mathbb{Q}$-generic polynomial for each of these groups with four parameters, which is as simple as possible so that one can apply it to various problems in number theory. The construction of the latter is the main part of this paper, and is discussed in section 4. Instead of printing the results here, we remark that our generic polynomials are given in a consistent way with respect to the lattice of subgroups of $\mathbf{G}_0$, in such a way that the polynomial for a subgroup is obtained by a specialization of the parameters of the one for another group containing it. The $\mathbb{Q}$-versal polynomial for $\mathbf{C}_8$ mentioned above in Theorem 1.4 will be discussed in section 5 as an application. We shall also describe a nontrivial example which illustrates the validity of Theorem 1.4.

In section 6, we study the similar problems for another realization of $\mathbf{G}_0$ as a subgroup of the Cremona group $\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(x, y)$ of dimension two, which cannot be lifted to a linear action of a higher-dimensional function field. We shall prove that a generalized version of Noether's problem for the *nonlinear* action of the subgroups of $\mathbf{G}_0$ mentioned above has again affirmative answers. It is worth remarking that, in contrast to the original NP and LNP, we have in this case an *affirmative* answer for a subgroup isomorphic to $\mathbf{C}_8$.

Finally, we remark that almost all results of this paper are valid for base fields of arbitrary characteristic different from 2.

2. Reduction of NP to LNP for $\mathbf{G}_0$

In this section we study the original version of NP for $\mathbf{G}_0$ and its subgroups containing $\mathbf{C}_8$. Let $\mathbf{G}_0$ be the normalizer of the 8-cycle in the symmetric group S_8 of degree 8. The group $\mathbf{G}_0$ has order 32 and is isomorphic to the group of the affine transformations $x \mapsto bx + a$ over $\mathbb{Z}/8\mathbb{Z}$:

$$\mathbf{G}_0 \cong \left\{ \begin{pmatrix} 1 & 0 \\ a & b \end{pmatrix} \in \mathbf{GL}_2(\mathbb{Z}/8\mathbb{Z}) \;\middle|\; a \in \mathbb{Z}/8\mathbb{Z},\ b \in (\mathbb{Z}/8\mathbb{Z})^\times \right\}.$$

Hence the group $\mathbf{G}_0$ is expressed as a semi-direct product $(\mathbb{Z}/8\mathbb{Z}) \rtimes (\mathbb{Z}/8\mathbb{Z})^\times$ where the action of $(\mathbb{Z}/8\mathbb{Z})^\times$ on $\mathbb{Z}/8\mathbb{Z}$ is by multiplication. We denote by A the element of $\mathbf{G}_0$ corresponding to $1 \in \mathbb{Z}/8\mathbb{Z}$ and by $B_{D}, B_{Q}, B_{M} \in \mathbf{G}_0$ the elements of order 2 corresponding to those in $(\mathbb{Z}/8\mathbb{Z})^\times$ so that they transform $j \in \mathbb{Z}/8\mathbb{Z}$ to

$$A : j \longmapsto j + 1, \quad B_{D} : j \longmapsto -j, \quad B_{Q} : j \longmapsto 3j, \quad B_{M} : j \longmapsto 5j.$$

Then we have

$$B_{D} A B_{D}^{-1} = A^{-1}, \quad B_{Q} A B_{Q}^{-1} = A^3, \quad B_{M} A B_{M}^{-1} = A^5$$

so that

$$\langle A \rangle \cong \mathbf{C}_8, \quad \langle A, B_{D} \rangle \cong \mathbf{D}_8, \quad \langle A, B_{Q} \rangle \cong \mathbf{QD}_8, \quad \langle A, B_{M} \rangle \cong \mathbf{M}_{16},$$

where $\mathbf{D}_8, \mathbf{QD}_8, \mathbf{M}_{16}$ are the dihedral group, the quasi-dihedral group, and the modular type 2-group, respectively, of order 16.

One can regard $\mathbf{G}_0$ as a permutation group of degree 8 through its natural action on $\mathbb{Z}/8\mathbb{Z}$. We denote the elements $A, B_{D}, B_{Q}, B_{M} \in \mathbf{G}_0$ by $\alpha, \beta_{D}, \beta_{Q}, \beta_{M}$, respectively, when they are regarded as permutations of degree 8. Thus we have

$$\alpha = (01234567), \quad \beta_{D} = (17)(26)(35), \quad \beta_{Q} = (13)(26)(57), \quad \beta_{M} = (15)(37).$$

We assign to each $j \in \mathbb{Z}/8\mathbb{Z}$ a variable X_j, and denote by V the $\mathbb{Q}$-vector space spanned by $X_0, \dots, X_7$. Then $\mathbf{G}_0$ acts linearly on V via the above identification $\mathbf{G}_0 = \langle \alpha, \beta_{_D}, \beta_{_Q} \rangle$ where the latter acts on the set $\{X_0, \dots, X_7\}$ through the permutation of their subscripts.

In order to obtain $\mathbb{Q}$-generic polynomials for subgroups of $\mathbf{G}_0$ which have minimal possible parameters, we study the reduction of NP to LNP in dimension 4. Thus our first task is to decompose the natural representation of $\mathbf{G}_0$ on V into irreducible subspaces. For this one makes an observation that $\mathrm{Z}(\mathbf{G}_0) = \langle A^4 \rangle$ is the center of $\mathbf{G}_0$ and $\mathbf{G}_0/\mathrm{Z}(\mathbf{G}_0) \cong \mathbf{D}_4 \times \mathbf{C}_2$, where $\mathbf{D}_4$ (resp. $\mathbf{C}_2$) is the dihedral group of order 8 (cyclic group of order 2). It follows that $\mathbf{G}_0$ has exactly eight (resp. two, one) irreducible representations of degree 1 (resp. 2, 4), corresponding to the equality $2^5 = 8 \cdot 1^2 + 2 \cdot 2^2 + 4^2$. With this fact in mind, we put

$$\begin{cases} x_1 := X_0 - X_4, \\ x_2 := X_1 - X_5, \\ x_3 := X_2 - X_6, \\ x_4 := X_3 - X_7, \end{cases} \quad \begin{cases} y_1 := X_0 + X_4, \\ y_2 := X_1 + X_5, \\ y_3 := X_2 + X_6, \\ y_4 := X_3 + X_7, \end{cases} \quad \begin{cases} z_1 := y_1 + y_2 + y_3 + y_4, \\ z_2 := y_1 - y_2 + y_3 - y_4, \\ z_3 := y_1 - y_3, \\ z_4 := y_2 - y_4. \end{cases}$$

Then we have the following decomposition of V into irreducible $\mathbb{Q}[\mathbf{G}_0]$-modules:

$$V = V_1 \oplus V_\varepsilon \oplus V_2 \oplus V_4,$$

where $V_1 = \mathbb{Q}z_1, V_\varepsilon = \mathbb{Q}z_2, V_2 = \mathbb{Q}z_3 + \mathbb{Q}z_4, V_4 = \mathbb{Q}x_1 + \mathbb{Q}x_2 + \mathbb{Q}x_3 + \mathbb{Q}x_4$. Using V_4 with its basis given above, we have the following realization of $\mathbf{G}_0$ as a subgroup of $\mathbf{GL}_{\mathbb{Q}}(V_4) \cong \mathbf{GL}_4(\mathbb{Q})$:

$$\rho(A) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \end{pmatrix}, \qquad \rho(B_{_D}) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix},$$

$$\rho(B_{_Q}) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \qquad \rho(B_{_M}) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

Let $\mathbb{Q}(V)$ (resp. $\mathbb{Q}(V_4)$) be the rational function field of $X_0, \dots, X_7$ (resp. $x_1, \dots, x_4$) over $\mathbb{Q}$. Since the representations of $\mathbf{G}_0$ on V, V_4 are faithful, one can apply the so-called No-Name Lemma, which shows that the extension $\mathbb{Q}(V)^H/\mathbb{Q}(V_4)^H$ is rational for any subgroup H of $\mathbf{G}_0$ (see [JLY], p.22). For this, we denote by $W \subseteq \mathbb{Q}(V)$ the vector space over $\mathbb{Q}(V_4)$ spanned by V, which is of dimension $5 = \dim_{\mathbb{Q}}(V) - \dim_{\mathbb{Q}}(V_4) + 1$. The group $\mathbf{G}_0$ acts semi-linearly on W. We shall construct a basis $\{1, g_1, g_2, g_3, g_4\}$ of W consisting of $\mathbf{G}_0$-invariant elements explicitly, whose existence is known in general from the No-Name Lemma. To find such a basis explicitly we note first that the set $\{1, z_1, z_2, z_3, z_4\}$ forms a basis of W. Note also that we have

$$\alpha : \begin{cases} z_2 \mapsto -z_2, \\ z_3 \mapsto z_4, \\ z_4 \mapsto -z_3, \end{cases} \qquad \beta_{_D},\, \beta_{_Q} : \begin{cases} z_2 \mapsto z_2, \\ z_3 \mapsto z_3, \\ z_4 \mapsto -z_4, \end{cases} \qquad \beta_{_M} : \begin{cases} z_2 \mapsto z_2, \\ z_3 \mapsto z_3, \\ z_4 \mapsto z_4. \end{cases}$$

Consider the $\mathbb{Q}$-vector space $\mathrm{Sym}^2(\mathbf{V}_4)$ consisting of quadratic forms in $x_1, \dots, x_4$, which is of dimension 10. From $\rho(A)^4 = -I_4$ we see that the action of $\mathbf{G}_0$ on

$\mathrm{Sym}^2(\mathbf{V}_4)$ factors through its quotient by $Z(\mathbf{G}_0) = \langle \alpha^4 \rangle$, so that the images of $\alpha^2, \beta_D, \beta_Q, \beta_M$ in $\mathbf{GL}_{\mathbb{Q}}(\mathrm{Sym}^2(\mathbf{V}_4))$ generate an abelian elementary 2-group. Hence $\mathrm{Sym}^2(\mathbf{V}_4)$ decomposes according to the characters of this group.

Lemma 2.1. *Let* $\mathrm{Sym}^2(\mathbf{V}_4)$ *be the vector space of quadratic forms in* $x_1, \ldots, x_4$ *over* $\mathbb{Q}$. *Then* $\mathrm{Sym}^2(\mathbf{V}_4)$ *is decomposed as a sum of simultaneous eigenspaces for* $\alpha^2, \beta_D, \beta_Q, \beta_M$ *as follows*:

TABLE 1.

α^2	β_D	β_Q	β_M	*dimension*	*basis*
1	1	1	1	2	$x_1^2 + x_3^2, \quad x_2^2 + x_4^2$
1	−1	1	−1	1	$x_1x_2 - x_2x_3 + x_1x_4 + x_3x_4$
1	1	−1	−1	1	$x_1x_2 + x_2x_3 - x_1x_4 + x_3x_4$
1	−1	−1	1	0	
−1	1	1	1	2	$x_2x_4, \quad x_1^2 - x_3^2$
−1	−1	1	−1	1	$x_1x_2 + x_2x_3 + x_1x_4 - x_3x_4$
−1	1	−1	−1	1	$x_1x_2 - x_2x_3 - x_1x_4 - x_3x_4$
−1	−1	−1	1	2	$x_1x_3, \quad x_2^2 - x_4^2$

From this it follows that, up to a constant factor, $h_\varepsilon := x_1^2 - x_2^2 + x_3^2 - x_4^2$ is the unique quadratic form in $x_1, \ldots, x_4$ such that $h_\varepsilon z_2$ is $\mathbf{G}_0$-invariant. Using these results one can obtain the following $\mathbf{G}_0$-invariant elements $\{g_1, g_2, g_3, g_4\}$ which, together with 1, form a basis of W:

$$\begin{cases} g_1 := z_1, \\ g_2 := (x_1^2 - x_2^2 + x_3^2 - x_4^2)z_2, \\ g_3 := (x_2x_4)z_3 - (x_1x_3)z_4, \\ g_4 := (x_1^2 - x_3^2)z_3 + (x_2^2 - x_4^2)z_4. \end{cases}$$

We now obtain the explicit version of the 'No-Name Lemma' for $\mathbb{Q}(V)^H/\mathbb{Q}(V_4)^H$.

Proposition 2.2. *For any subgroup* H *of* $\mathbf{G}_0$, *the extension* $\mathbb{Q}(V)^H/\mathbb{Q}(V_4)^H$ *is rational and is generated by* $\{g_1, g_2, g_3, g_4\}$.

Thus NP is reduced, *simultaneously* for all subgroups H of $\mathbf{G}_0$, to LNP in degree 4, which asks the rationality of the extension $\mathbb{Q}(V_4)^H/\mathbb{Q}$.

3. LNP FOR SUBGROUPS H OF $\mathbf{G}_0$

Throughout this section, we put $\underline{x} = \{x_1, x_2, x_3, x_4\}$ and denote the field $\mathbb{Q}(V_4)$ by $\mathbb{Q}(\underline{x}) = \mathbb{Q}(x_1, x_2, x_3, x_4)$. Our aim here is to find for each subgroup H of $\mathbf{G}_0$ containing $\mathbf{C}_8$ properly a simple system of generators of the fixed field $\mathbb{Q}(\underline{x})^H$, which, as a consequence, gives the affirmative answer to LNP in these cases.

3.1. **New forms of low degree.** We see that $\mathbf{G}_0 = \langle \alpha, \beta_{_D}, \beta_{_Q} \rangle$ acts on $\underline{x}$ through the linear representation ρ as permutations up to the factors ± 1:

$$\begin{cases} \rho(A) = \alpha : (x_1, x_2, x_3, x_4) \longmapsto (x_2, x_3, x_4, -x_1), \\ \rho(A)^4 : (x_1, x_2, x_3, x_4) \longmapsto (-x_1, -x_2, -x_3, -x_4), \\ \rho(B_{_D}) = \beta_{_D} : (x_1, x_2, x_3, x_4) \longmapsto (x_1, -x_4, -x_3, -x_2), \\ \rho(B_{_Q}) = \beta_{_Q} : (x_1, x_2, x_3, x_4) \longmapsto (x_1, x_4, -x_3, x_2), \\ \rho(B_{_M}) = \beta_{_M} : (x_1, x_2, x_3, x_4) \longmapsto (x_1, -x_2, x_3, -x_4). \end{cases}$$

Here we extend subgroups $H \subset \mathbf{G}_0$ to $\mathbf{G}_{128}$ (resp. $\mathbf{G}_{64}$) of order 128 (resp. 64) by introducing

$$\begin{cases} \delta : (x_1, x_2, x_3, x_4) \longmapsto (x_2, -x_1, x_4, x_3), \\ \gamma := \delta^2 : (x_1, x_2, x_3, x_4) \longmapsto (-x_1, -x_2, x_3, x_4). \end{cases}$$

We define $\mathbf{G}_{128} := \langle \alpha, \beta_{_D}, \beta_{_Q}, \beta_{_M}, \delta \rangle$ and $\mathbf{G}_{64} := \langle \alpha, \beta_{_D}, \beta_{_Q}, \beta_{_M}, \gamma \rangle$. Then $\mathbf{G}_{128}$ and $\mathbf{G}_{64}$ contain $\mathbf{G}_0$. We give some basic homogeneous polynomials in $x_1, \ldots, x_4$ of low degrees which are semi-invariants of a subgroup $H \subseteq \mathbf{G}_{128}$:

TABLE 2.

α	$\beta_{_D}$	$\beta_{_Q}$	$\beta_{_M}$	γ	δ	new forms to H	H
1	1	1	1	1	1	$f_2,\ f_{4,a},\ f_{4,b},\ f_6, f_8$	$\mathbf{G}_{128}$
1	1	1	1	1	-1	g_8	$\mathbf{G}_{64}$
1	1	1	1	-1	$*$	h_4	$\mathbf{G}_0$
1	1	-1	-1	$*$	$*$	p_2	$\mathbf{D}_8$
1	-1	1	-1	$*$	$*$	q_6	$\mathbf{QD}_8$
1	-1	-1	1	$*$	$*$	r_6	$\mathbf{M}_{16}$

where f is called a *new form* if it is not invariant by a larger subgroup, and

$$\begin{aligned} f_2(\underline{x}) &:= x_1^2 + x_2^2 + x_3^2 + x_4^2, \\ f_{4,a}(\underline{x}) &:= x_1^2 x_3^2 + x_2^2 x_4^2, \\ f_{4,b}(\underline{x}) &:= (x_1^2 + x_3^2)(x_2^2 + x_4^2), \\ f_6(\underline{x}) &:= x_1^2 x_2^2 x_3^2 + x_1^2 x_2^2 x_4^2 + x_1^2 x_3^2 x_4^2 + x_2^2 x_3^2 x_4^2, \\ f_8(\underline{x}) &:= x_1^2 x_2^2 x_3^2 x_4^2, \\ g_8(\underline{x}) &:= x_1 x_2 x_3 x_4 (x_1^2 - x_3^2)(x_2^2 - x_4^2), \\ h_4(\underline{x}) &:= (x_1 x_4 - x_2 x_3)(x_1 x_2 + x_3 x_4), \\ p_2(\underline{x}) &:= x_1 x_2 + x_2 x_3 - x_1 x_4 + x_3 x_4, \\ q_6(\underline{x}) &:= (x_1^2 x_3^2 - x_2^2 x_4^2)(x_1 x_2 - x_2 x_3 + x_1 x_4 + x_3 x_4), \\ r_6(\underline{x}) &:= x_1 x_2 x_3 x_4 (x_1^2 - x_2^2 + x_3^2 - x_4^2). \end{aligned}$$

3.2. **Fixed fields $\mathbb{Q}(\underline{x})^H$.** Now we can determine the fixed fields for those subgroups H of $\mathbf{G}_{128}$ appearing in Table 2. Our first result is

Lemma 3.1. *The field consisting of* $\mathbf{G}_{128}$*-invariant functions in* $\mathbb{Q}(\underline{x})$ *is generated over* $\mathbb{Q}$ *by five elements as*

$$\mathbb{Q}(\underline{x})^{\mathbf{G}_{128}} \quad = \quad \mathbb{Q}(f_2, f_{4,a}, f_{4,b}, f_6, f_8).$$

Proof. Note first that $f_2, f_{4,a}, f_{4,b}, f_6, f_8$ are invariant under the action of $\mathbf{G}_{128}$. The elementary symmetric polynomials in $x_1^2, \ldots, x_4^2$ are f_2, $f_{4,a} + f_{4,b}$, f_6, and f_8, respectively. It follows that the fixed field $\mathbb{Q}(x_1^2, \ldots, x_4^2)^{S_4}$ of the symmetric group S_4 is contained in $\mathbb{Q}(f_2, f_{4,a}, f_{4,b}, f_6, f_8)$. On the other hand, the S_4-orbit of $f_{4,a}$ consists of three functions $f_{4,a} = x_1^2x_3^2 + x_2^2x_4^2$, $f'_{4,a} = x_1^2x_2^2 + x_3^2x_4^2$, $f''_{4,a} = x_1^2x_4^2 + x_2^2x_3^2$, so that we have

$$[\mathbb{Q}(f_2, f_{4,a}, f_{4,b}, f_6, f_8) : \mathbb{Q}(x_1^2, \ldots, x_4^2)^{S_4}] = 3.$$

We next observe that the group of $\mathbb{Q}$-automorphisms of $\mathbb{Q}(\underline{x})$ that preserve the set $\{x_1^2, \ldots, x_4^2\}$ is the wreath product

$$C_2 \wr S_4 \quad = \quad \left\{ \varphi \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\underline{x})) \;\middle|\; \varphi\big(\{x_1^2, \ldots, x_4^2\}\big) = \{x_1^2, \ldots, x_4^2\} \right\},$$

and it contains $\mathbf{G}_{128}$ as a Sylow 2-subgroup. Since the fixed field of this group in $\mathbb{Q}(\underline{x})$ is $\mathbb{Q}(x_1^2, \ldots, x_4^2)^{S_4}$, we conclude $\mathbb{Q}(\underline{x})^{\mathbf{G}_{128}} = \mathbb{Q}(f_2, f_{4,a}, f_{4,b}, f_6, f_8)$. □

It can be checked by direct computation that the five functions in Lemma 3.1 are subject to a single equation

$$f_6^2 - f_2 f_{4,a} f_6 + f_{4,a}^2 f_{4,b} + f_2^2 f_8 - 4 f_{4,b} f_8 \quad = \quad 0. \tag{1}$$

It follows that $f_{4,b}$ is expressed by $f_2, f_{4,a}, f_6, f_8$. Then we obtain from Lemma 3.1 the following:

Theorem 3.2 (LNP for $\mathbf{G}_{128}$)**.** *The fixed field of* $\mathbf{G}_{128}$ *in* $\mathbb{Q}(\underline{x})$ *is*

$$\mathbb{Q}(\underline{x})^{\mathbf{G}_{128}} \quad = \quad \mathbb{Q}(f_2, f_{4,a}, f_6, f_8).$$

□

Theorem 3.3 (LNP for $\mathbf{G}_{64}$)**.** *We have*

$$\mathbb{Q}(\underline{x})^{\mathbf{G}_{64}} \quad = \quad \mathbb{Q}(a_k,\, b_k,\, c_k,\, d_k),$$

where

$$\begin{cases} a_k \;:=\; \dfrac{(x_1^2 + x_3^2)^2 (x_2^2 + x_4^2)^2}{x_1^2 x_2^2 x_3^2 x_4^2}, \\ b_k \;:=\; \dfrac{(x_1^2 - x_3^2)(x_2^2 - x_4^2)}{x_1 x_2 x_3 x_4}, \\ c_k \;:=\; \dfrac{x_1^2x_2^2x_3^2 + x_1^2x_2^2x_4^2 + x_1^2x_3^2x_4^2 + x_2^2x_3^2x_4^2}{(x_1^2 + x_3^2)(x_2^2 + x_4^2)}, \\ d_k \;:=\; x_1^2 + x_2^2 + x_3^2 + x_4^2. \end{cases}$$

Proof. We see from Table 2 that g_8 is a new form to $\mathbf{G}_{64}$ such that $\delta(g_8) = -g_8$, which implies that

$$\mathbb{Q}(\underline{x})^{\mathbf{G}_{64}} = \mathbb{Q}(\underline{x})^{\mathbf{G}_{128}}(g_8) = \mathbb{Q}(f_2, f_{4,a}, f_{4,b}, f_6, f_8, g_8).$$

One can show by a direct computation that these six functions satisfy the equality

$$g_8^2 - 4 f_{4,a} f_{4,b} f_8 - f_{4,b}^2 f_8 + 4 f_2 f_6 f_8 - 16 f_8^2 \quad = \quad 0. \tag{2}$$

Thus $\mathbb{Q}(\underline{x})^{\mathbf{G}_{64}}$ is the function field of an algebraic variety defined over $\mathbb{Q}$ by two equations (1), (2). We shall show that it is birational to the affine space $\mathbb{A}^4$ over $\mathbb{Q}$. For this we first solve (2) in $f_{4,a}$ as

$$f_{4,a} \;=\; \frac{1}{4f_8f_{4,b}}\Big(4f_2f_6f_8 - 16f_8^2 + g_8^2 - f_8f_{4,b}^2\Big)$$

and substitute it in (1) to obtain

$$\begin{aligned}(3)\qquad & f_{4,b}^4f_8^2 - 4f_2f_{4,b}^2f_6f_8^2 + 16f_{4,b}f_6^2f_8^2 + 16f_2^2f_{4,b}f_8^3 - 32f_{4,b}^2f_8^3\\ & - 64f_2f_6f_8^3 + 256f_8^4 - 2f_{4,b}^2f_8g_8^2 + 4f_2f_6f_8g_8^2 - 32f_8^2g_8^2 + g_8^4 \;=\; 0.\end{aligned}$$

Now transform the coordinate $(f_2, f_{4,b}, f_6, f_8, g_8)$ to $(a_k, b_k, c_k, d_k, e_k)$ birationally by

$$\begin{cases} f_2 = d_k, & f_{4,b} = \dfrac{a_kc_ke_k}{4}, \quad f_6 = \dfrac{a_kc_k^2e_k}{4}, \quad f_8 = \dfrac{a_kc_k^2e_k^2}{16}, \quad g_8 = \dfrac{a_kb_kc_k^2e_k^2}{16},\\ a_k = f_{4,b}^2/f_8, & b_k = g_8/f_8, \quad c_k = f_6/f_{4,b}, \quad d_k = f_2, \quad e_k = 4f_8/f_6.\end{cases}$$

Then we have $\mathbb{Q}(\underline{x})^{\mathbf{G}_{64}} = \mathbb{Q}(f_2, f_{4,b}, f_6, f_8, g_8) = \mathbb{Q}(a_k, b_k, c_k, d_k, e_k)$. On the other hand, we see that (3) is transformed to

$$\begin{aligned}&(a_k - 8b_k - b_k^2 - 16)(a_k + 8b_k - b_k^2 - 16)c_ke_k\\ &\quad + 16(4a_kc_k^2 - 16c_kd_k - a_kc_kd_k + b_k^2c_kd_k + 4d_k^2) \;=\; 0,\end{aligned}$$

which is linear in e_k. It follows that $\mathbb{Q}(\underline{x})^{\mathbf{G}_{64}} = \mathbb{Q}(a_k, b_k, c_k, d_k)$, which proves the theorem. □

By similar arguments we obtain the following set of generators of the fixed field $\mathbb{Q}(\underline{x})^H$ for each subgroup H containing $\mathbf{C}_8$ properly, which seems to be the simplest among such generators. Here we confine ourselves to stating only the result, since another, though less simple, set of generators will be produced during our construction of a $\mathbb{Q}$-generic polynomial for H in the next section. We note that, in particular, these results imply the affirmative answer to LNP, hence to NP as well, for H.

Theorem 3.4 (LNP for $\mathbf{G}_0$)**.** *We have*

$$\mathbb{Q}(\underline{x})^{\mathbf{G}_0} \;=\; \mathbb{Q}(a_f,\, b_f,\, c_f,\, d_f),$$

$$\begin{cases} a_f \;:=\; \dfrac{(x_1x_4 - x_2x_3)(x_1x_2 + x_3x_4)}{(x_1^2 + x_3^2)(x_2^2 + x_4^2)},\\ b_f \;:=\; \dfrac{(x_1^2 - x_3^2)(x_2^2 - x_4^2)}{x_1x_2x_3x_4},\\ c_f \;:=\; \dfrac{x_1^2x_2^2x_3^2 + x_1^2x_2^2x_4^2 + x_1^2x_3^2x_4^2 + x_2^2x_3^2x_4^2}{(x_1^2 + x_3^2)(x_2^2 + x_4^2)},\\ d_f \;:=\; x_1^2 + x_2^2 + x_3^2 + x_4^2.\end{cases}$$

Theorem 3.5 (LNP for $\mathbf{D}_8$)**.** *We have*

$$\mathbb{Q}(\underline{x})^{\mathbf{D}_8} \;=\; \mathbb{Q}(a_d,\, b_d,\, c_d,\, d_d),$$

$$\begin{cases} a_d &:= \dfrac{x_1^2x_3^2 - x_2^2x_4^2}{(x_1^2x_3^2 + x_2^2x_4^2)(x_1^2 - x_2^2 + x_3^2 - x_4^2)}, \\ b_d &:= \dfrac{(x_1^2x_3^2 + x_2^2x_4^2)(x_1x_2 - x_2x_3 + x_1x_4 + x_3x_4)}{x_1x_2x_3x_4}, \\ c_d &:= x_1x_2 + x_2x_3 - x_1x_4 + x_3x_4, \\ d_d &:= x_1^2 + x_2^2 + x_3^2 + x_4^2. \end{cases}$$

Theorem 3.6 (LNP for $\mathbf{QD}_8$)**.** *We have*

$$\mathbb{Q}(\underline{x})^{\mathbf{QD}_8} = \mathbb{Q}(a_q, b_q, c_q, d_q),$$

$$\begin{cases} a_q &:= \dfrac{(x_1^2x_3^2 - x_2^2x_4^2)(x_1x_2 + x_2x_3 - x_1x_4 + x_3x_4)}{x_1x_2x_3x_4}, \\ b_q &:= \dfrac{(x_1^2x_3^2 + x_2^2x_4^2)(x_1x_2 + x_2x_3 - x_1x_4 + x_3x_4)}{x_1x_2x_3x_4(x_1x_2 - x_2x_3 + x_1x_4 + x_3x_4)}, \\ c_q &:= \dfrac{x_1^2 - x_2^2 + x_3^2 - x_4^2}{x_1x_2 - x_2x_3 + x_1x_4 + x_3x_4}, \\ d_q &:= x_1^2 + x_2^2 + x_3^2 + x_4^2. \end{cases}$$

Theorem 3.7 (LNP for $\mathbf{M}_{16}$)**.** *We have*

$$\mathbb{Q}(\underline{x})^{\mathbf{M}_{16}} = \mathbb{Q}(a_m, b_m, c_m, d_m),$$

where

$$\begin{cases} a_m &:= \dfrac{(x_1^2 - x_2^2 + x_3^2 - x_4^2)(x_1x_2 + x_2x_3 - x_1x_4 + x_3x_4)}{x_1x_2 - x_2x_3 + x_1x_4 + x_3x_4}, \\ b_m &:= \dfrac{(x_1^2x_3^2 + x_2^2x_4^2)(x_1^2 - x_2^2 + x_3^2 - x_4^2)}{x_1x_2x_3x_4}, \\ c_m &:= \dfrac{x_1^2x_3^2 - x_2^2x_4^2}{x_1x_2x_3x_4}, \\ d_m &:= x_1^2 + x_2^2 + x_3^2 + x_4^2. \end{cases}$$

4. $\mathbb{Q}$-generic polynomial with four parameters for H

Once we have an explicitly given set a, b, c, d of generators of the fixed field $\mathbb{Q}(\underline{x})^H$ of $H \subseteq \mathbf{G}_{128}$ in $\mathbb{Q}(\underline{x})$, it is not difficult to find a $\mathbb{Q}$-generic polynomial for H. Indeed an irreducible polynomial of arbitrary primitive element θ of $\mathbb{Q}(\underline{x})$ (i.e., $\mathbb{Q}(\underline{x}) = \mathbb{Q}(a, b, c, d)(\theta)$) is a $\mathbb{Q}$-generic polynomial with parameters a, b, c, d by the result of Kemper-Mattig [KM]. However, it is quite often the case that the resulting polynomial is too big and complicated to be printed, even if we start from fairly simple generators of the fixed field. Our aim, on the other hand, is to find $\mathbb{Q}$-generic polynomials which are simple enough to the extent that one can make use of them in various aspects of number theory (cf. [Has], [HT]). In this section, therefore, we reset the set of generators of $\mathbb{Q}(\underline{x})^H$ obtained in §3 and try to find another set of generators which satisfies our request. Thus the same symbols such as a_k, b_k, c_k, d_k are used for distinct sets of generators in §3 and §4.

We remark also that a $\mathbb{Q}$-generic $\mathbf{D}_8$ (resp. $\mathbf{QD}_8$, $\mathbf{M}_{16}$) polynomial with *five* parameters is given explicitly in [Led1].

One of our devices to fulfill this requirement is to look at the natural biquartic polynomial

$$F(X) \quad = \quad (X^2 - x_1^2)(X^2 - x_2^2)(X^2 - x_3^2)(X^2 - x_4^2).$$

As in the proof of Lemma 3.1, the splitting field of the polynomial $F(X)$ over $\mathbb{Q}(\underline{x})^H$ is $\mathbb{Q}(\underline{x})$ for $H \subseteq C_2 \wr S_4$. Hence if we can express the coefficients of $F(X)$ by our generators of the fixed field $\mathbb{Q}(\underline{x})^H = \mathbb{Q}(a, b, c, d)$ of $H \subseteq C_2 \wr S_4$ in $\mathbb{Q}(\underline{x})$, then the resulting polynomial $F_H(a, b, c, d; X)$ is $\mathbb{Q}$-generic for H (e.g., $F_H(a, b, c, d; X) = X^8 - aX^6 + bX^4 - cX^2 + d$ is $\mathbb{Q}$-generic for $H = C_2 \wr S_4$). The starting point of our construction is the following:

Theorem 4.1. *The polynomial*

$$F_{\mathbf{G}_{128}}(a, b, c, d; X) \quad := \quad X^8 - aX^6 + (b + j)X^4 - cX^2 + d, \tag{4}$$

$$j \quad = \quad \frac{abc - c^2 - a^2 d}{b^2 - 4d},$$

is a generic $\mathbf{G}_{128}$*-polynomial over* $\mathbb{Q}$.

Proof. The observation in the proof of Lemma 3.1 leads us to an equality

$$F(X) \; = \; \prod_{i=1}^{4} \left(X^2 - x_i^2\right) \quad = \quad X^8 - f_2 X^6 + (f_{4,a} + f_{4,b})X^4 - f_6 X^2 + f_8.$$

Putting

$$a = f_2, \quad b = f_{4,a}, \quad c = f_6, \quad d = f_8, \quad j = f_{4,b}, \tag{5}$$

then we have $\mathbb{Q}(\underline{x})^{\mathbf{G}_{128}} = \mathbb{Q}(a, b, c, d, j)$, and (1) is rewritten as $j = (abc - c^2 - a^2 d)/(b^2 - 4d)$. □

Our strategy now is to find the best expression for f_2, $f_{4,a}$, $f_{4,b}$, f_6 and f_8 by a suitably chosen set of generators of L^H. We first study the fixed field of $\alpha^2 : (x_1, x_2, x_3, x_4) \longmapsto (x_3, x_4, -x_1, -x_2)$. Put

$$u_1 := \frac{x_2 x_4 (x_1^2 + x_3^2)}{x_1 x_3 (x_2^2 + x_4^2)}, \qquad u_2 := x_1^2 + x_3^2, \tag{6}$$

$$u_3 := x_1 x_2 + x_2 x_3 - x_1 x_4 + x_3 x_4, \qquad u_4 := x_1 x_2 - x_2 x_3 + x_1 x_4 + x_3 x_4.$$

Proposition 4.2. *We have* $\mathbb{Q}(\underline{x})^{\langle \alpha^2 \rangle} = \mathbb{Q}(u_1, \ldots, u_4)$.

Proof. One sees that u_1, u_2, u_3, u_4 are invariant by α^2, and that x_2, x_4 are solved from the last two equations as

$$x_2 = \frac{(x_1 + x_3)u_3 + (x_1 - x_3)u_4}{2(x_1^2 + x_3^2)}, \quad x_4 = \frac{(x_1 + x_3)u_4 - (x_1 - x_3)u_3}{2(x_1^2 + x_3^2)}.$$

Also we have an equality

$$x_3 = \frac{(u_3^2 - u_4^2)(u_2 - 2x_1^2)}{2\big(u_1(u_3^2 + u_4^2) - 2u_3 u_4\big)x_1}.$$

Hence one has $\mathbb{Q}(\underline{x}) = \mathbb{Q}(u_3, u_4, x_1, x_3) = \mathbb{Q}(u_1, u_2, u_3, u_4, x_1)$. Furthermore we obtain by eliminating x_2, x_3, x_4 that x_1 satisfies a quartic equation over $\mathbb{Q}(u_1, \ldots, u_4)$:

$$4(x_1^4 - u_2 x_1^2)(u_3^2 + u_4^2)(u_3^2 + u_1^2 u_3^2 - 4u_1 u_3 u_4 + u_4^2 + u_1^2 u_4^2) + u_2^2 (u_3^2 - u_4^2)^2 \; = \; 0.$$

It follows that

$$[\mathbb{Q}(\underline{x}) : \mathbb{Q}(u_1, \dots, u_4)] = 4 = [\mathbb{Q}(\underline{x}) : \mathbb{Q}(\underline{x})^{\langle \alpha^2 \rangle}],$$

which proves the assertion. □

Since $\langle \alpha^2 \rangle$ is a normal subgroup of the groups $\mathbf{C}_8$, $\mathbf{D}_8$, $\mathbf{QD}_8$, $\mathbf{M}_{16}$, and $\mathbf{G}_{64}$, the field $\mathbb{Q}(u_1, \dots, u_4)$ is stable under the action of these groups. Indeed we find the action of their generators as

$$\begin{cases} \alpha : (u_1, u_2, u_3, u_4) \mapsto \left(\dfrac{-1}{u_1}, \dfrac{u_3^2 + u_4^2}{2u_2}, u_3, -u_4 \right), \\ \beta_{_D} : (u_1, u_2, u_3, u_4) \mapsto (-u_1, u_2, u_3, -u_4), \\ \beta_{_Q} : (u_1, u_2, u_3, u_4) \mapsto (-u_1, u_2, -u_3, u_4), \\ \beta_{_M} : (u_1, u_2, u_3, u_4) \mapsto (u_1, u_2, -u_3, -u_4), \\ \gamma : (u_1, u_2, u_3, u_4) \mapsto (u_1, u_2, u_4, u_3). \end{cases}$$

Remark 4.3. Let $K_3 := \mathbb{Q}(X, Y, Z)$ be the rational function field over $\mathbb{Q}$ with three variables X, Y, Z and ι the involution defined by

$$\iota : (X, Y, Z) \mapsto \left(\frac{-1}{X}, \frac{Z^2 + 1}{2Y}, -Z \right).$$

Then $K_3^{\langle \iota \rangle}$ is *not* rational over $\mathbb{Q}$, because if we put $(w_2, w_4) := \left(\dfrac{u_2}{u_3}, \dfrac{u_4}{u_3} \right)$, then we have $\mathbb{Q}(u_1, u_2, u_3, u_4) = \mathbb{Q}(u_1, w_2, u_3, w_4)$, and α acts on it as an involution

$$\alpha : (u_1, w_2, u_3, w_4) \mapsto \left(\frac{-1}{u_1}, \frac{w_4^2 + 1}{2w_2}, u_3, -w_4 \right).$$

Hence the assertion follows from the fact that $L^{\langle \alpha \rangle} = \mathbb{Q}(u_1, w_2, u_3, w_4)^{\langle \alpha \rangle}$ is not rational over $\mathbb{Q}$.

Proposition 4.4. *We have $\mathbb{Q}(\underline{x})^{\langle \alpha \rangle} = \mathbb{Q}(c_1, \dots, c_5)$, where $c_1, \dots, c_5$ are given by*

$$(c_1, \dots, c_5) \quad = \quad \left(\frac{u_1^2 - 1}{2u_1}, \frac{2u_2^2 + u_3^2 + u_4^2}{2u_2u_3}, \frac{2u_2^2 - u_3^2 - u_4^2}{2u_2u_4}, \frac{(u_1^2 + 1)u_4}{2u_1u_3}, u_3 \right)$$

and satisfy a single equation

$$(c_1^2 + 1)(c_2^2 - 2) - (c_3^2 + 2)c_4^2 \quad = \quad 0. \tag{7}$$

Proof. We have $[\mathbb{Q}(u_1, \dots, u_4) : \mathbb{Q}(u_1, \dots, u_4)^{\langle \alpha \rangle}] = 2$, since α acts on $\mathbb{Q}(u_1, \dots, u_4)$ as an involution. Note also that $c_1, \dots, c_5$ are all invariant by α. From (7) we find the following expression of u_2, u_3, u_4:

$$u_2 = \frac{1}{2} \left(c_2c_5 + \frac{2c_3c_4c_5u_1}{u_1^2 + 1} \right), \quad u_3 = c_5, \quad u_4 = \frac{2c_4c_5u_1}{u_1^2 + 1}.$$

Hence we have $\mathbb{Q}(u_1, \dots, u_4) = \mathbb{Q}(c_1, \dots, c_5, u_1)$. Since u_1 is a root of the quadratic equation $u_1^2 - 2c_1u_1 - 1 = 0$, we have $[\mathbb{Q}(c_1, \dots, c_5, u_1) : \mathbb{Q}(c_1, \dots, c_5)] = 2$. It follows that $\mathbb{Q}(u_1, \dots, u_4)^{\langle \alpha \rangle} = \mathbb{Q}(c_1, \dots, c_5)$, which proves the first assertion. The relation (7) now is checked by a direct computation. □

Let $(a_g, b_g, j_g, c_g, d_g) := (f_2, f_{4,a}, f_{4,b}, f_6, f_8)$ be as in (5). We see from (6) that

$$\begin{cases} a_g = \dfrac{2u_2^2+u_3^2+u_4^2}{2u_2}, \\ b_g = \dfrac{(u_3^2-u_4^2)^2(4u_2^4+u_1^2u_3^4+2u_1^2u_3^2u_4^2+u_1^2u_4^4)}{16u_2^2(u_3^2+u_4^2)(u_3^2+u_1^2u_3^2-4u_1u_3u_4+u_4^2+u_1^2u_4^2)}, \\ c_g = \dfrac{(u_3^2-u_4^2)^2(2u_2^2+u_1^2u_3^2+u_1^2u_4^2)}{16u_2(u_3^2+u_1^2u_3^2-4u_1u_3u_4+u_4^2+u_1^2u_4^2)}, \\ d_g = \dfrac{u_1^2(u_3^2-u_4^2)^4}{64(u_3^2+u_1^2u_3^2-4u_1u_3u_4+u_4^2+u_1^2u_4^2)^2}. \end{cases}$$

Combining this with (7) we obtain, after some computations which are omitted here, the following expressions:

$$\begin{cases} a_g = c_2c_5, \\ b_g = \dfrac{(c_1^2-c_4^2+1)^2(c_2^2+c_1^2c_2^2-2c_1c_2c_3c_4+c_3^2c_4^2)c_5^2}{16(c_1^2+1)(c_1^2+c_4^2+1)(c_1^2-2c_4+c_4^2+1)}, \\ j_g = \dfrac{(c_2^2+c_3^2)c_5^2}{2(c_3^2+2)}, \\ c_g = \dfrac{(c_2+c_1^2c_2-c_1c_3c_4)(c_1^2-c_4^2+1)^2c_5^3}{16(c_1^2+1)^2(c_1^2-2c_4+c_4^2+1)}, \\ d_g = \dfrac{(c_1^2-c_4^2+1)^4c_5^4}{256(c_1^2+1)^3(c_1^2-2c_4+c_4^2+1)^2}. \end{cases} \tag{8}$$

Now we observe that the action of $\beta_{_M}$ on $c_1, \dots, c_5$ is described simply as

$$\beta_{_M} : (c_1, c_2, c_3, c_4, c_5) \mapsto (c_1, -c_2, -c_3, c_4, -c_5).$$

One can obtain a system of generators of the fixed field of $\mathbb{Q}(c_1, \dots, c_5)$ by $\beta_{_M}$. Put

$$\begin{aligned} (a_m, b_m, c_m, d_m) &= \left(\frac{c_1}{c_4}, \frac{1}{c_4}, \frac{c_3}{c_2}, c_2c_5\right) \\ &= \left(\frac{(u_1^2-1)u_3}{(u_1^2+1)u_4}, \frac{2u_1u_3}{(u_1^2+1)u_4}, \frac{(2u_2^2-u_3^2-u_4^2)u_3}{(2u_2^2+u_3^2+u_4^2)u_4}, \frac{2u_2^2+u_3^2+u_4^2}{2u_2}\right). \end{aligned} \tag{9}$$

From (6) one can express a_m, b_m, c_m, d_m as elements of $\mathbb{Q}(\underline{x})$. Namely we have the following result, which is slightly more complicated than (4):

$$\begin{cases} a_m = \dfrac{(x_1^2x_4^2-x_2^2x_3^2)}{(x_1x_2-x_2x_3+x_1x_4+x_3x_4)} \\ \qquad \cdot \dfrac{(x_1^2x_2^2-x_3^2x_4^2)(x_1x_2+x_2x_3-x_1x_4+x_3x_4)}{(x_1^2x_2^4x_3^2+x_1^4x_2^2x_4^2+4x_1^2x_2^2x_3^2x_4^2+x_2^2x_3^4x_4^2+x_1^2x_3^2x_4^4)}, \\ b_m = \dfrac{2x_1x_2x_3x_4(x_1^2+x_3^2)(x_2^2+x_4^2)}{(x_1x_2-x_2x_3+x_1x_4+x_3x_4)} \\ \qquad \cdot \dfrac{(x_1x_2+x_2x_3-x_1x_4+x_3x_4)}{(x_1^2x_2^4x_3^2+x_1^4x_2^2x_4^2+4x_1^2x_2^2x_3^2x_4^2+x_2^2x_3^4x_4^2+x_1^2x_3^2x_4^4)}, \\ c_m = \dfrac{(x_1x_2+x_2x_3-x_1x_4+x_3x_4)(x_1^2-x_2^2+x_3^2-x_4^2)}{(x_1x_2-x_2x_3+x_1x_4+x_3x_4)(x_1^2+x_2^2+x_3^2+x_4^2)}, \\ d_m = x_1^2+x_2^2+x_3^2+x_4^2. \end{cases} \tag{10}$$

Now we clearly have $\mathbb{Q}(a_m, b_m, c_m, d_m) \subseteq \mathbb{Q}(\underline{x})^{\mathbf{M}_{16}}$.

Proposition 4.5. *We have* $\mathbb{Q}(\underline{x})^{\mathbf{M}_{16}} = \mathbb{Q}(c_1, \ldots, c_5)^{\langle \beta_{M} \rangle} = \mathbb{Q}(a_m, b_m, c_m, d_m)$.

Proof. It follows that $\mathbb{Q}(a_m, b_m, c_m, d_m, c_2) = \mathbb{Q}(c_1, \ldots, c_5) = \mathbb{Q}(u_1, \ldots, u_4)^{\langle \alpha \rangle}$ from (9). Also we see from $\beta_{M}(c_2) = -c_2$ that this field is a quadratic extension of $\mathbb{Q}(a_m, b_m, c_m, d_m)$; hence $\mathbb{Q}(a_m, b_m, c_m, d_m) = \mathbb{Q}(c_1, \ldots, c_5)^{\langle \beta_{M} \rangle}$ is the fixed field of $\mathbf{M}_{16}$. □

We next seek the expressions for a_g, b_g, j_g, c_g, d_g by a_m, b_m, c_m, d_m. These are obtained from (8) and (9) as follows:

$$\begin{cases} a_g = d_m, \\ b_g = \dfrac{(a_m^2 + b_m^2 - 1)^2 (a_m^2 + b_m^2 - 2a_m c_m + c_m^2) d_m^2}{2^4 (a_m^2 + b_m^2)(a_m^2 + b_m^2 + 1)(a_m^2 - 2b_m + b_m^2 + 1)}, \\ j_g = \dfrac{(a_m^2 + b_m^2 - c_m^2) d_m^2}{4(a_m^2 + b_m^2)}, \\ c_g = \dfrac{(a_m^2 + b_m^2 - 1)^2 (a_m^2 + b_m^2 - a_m c_m)(a_m^2 + b_m^2 - c_m^2) d_m^3}{2^5 (a_m^2 + b_m^2)^2 (a_m^2 + b_m^2 + 1)(a_m^2 - 2b_m + b_m^2 + 1)}, \\ d_g = \dfrac{b_m^2 (a_m^2 + b_m^2)^4 (a_m^2 + b_m^2 - c_m^2)^2 d_m^4}{2^{10} (a_m^2 + b_m^2)^3 (a_m^2 + b_m^2 + 1)^2 (a_m^2 - 2b_m + b_m^2 + 1)^2}. \end{cases}$$

Substituting these into (5) and then replacing a_m, b_m, c_m, d_m by a, b, c, d, we obtain the following polynomial:

$$\begin{aligned} (11) \quad F_{\mathbf{M}_{16}}(a, b, c, d; X) &= X^8 - dX^6 \\ &+ \left(\frac{(a^2 + b^2 - c^2)}{4(a^2 + b^2)} + \frac{(a^2 + b^2 - 1)^2 \big((a - c)^2 + b^2\big)}{2^4 (a^2 + b^2)(a^2 + b^2 + 1)\big(a^2 + (b - 1)^2\big)} \right) d^2 X^4 \\ &- \frac{(a^2 + b^2 - 1)^2 (a^2 + b^2 - ac)(a^2 + b^2 - c^2) d^3}{2^5 (a^2 + b^2)^2 (a^2 + b^2 + 1)\big(a^2 + (b - 1)^2\big)} X^2 \\ &+ \frac{b^2 (a^2 + b^2 - 1)^4 (a^2 + b^2 - c^2)^2 d^4}{2^{10} (a^2 + b^2)^3 (a^2 + b^2 + 1)^2 \big(a^2 + (b - 1)^2\big)^2}. \end{aligned}$$

Theorem 4.6. $F_{\mathbf{M}_{16}}(a, b, c, d; X) \in \mathbb{Q}(a, b, c, d)[X]$ *is a generic polynomial over* $\mathbb{Q}$ *for* $\mathbf{M}_{16}$*, when we regard* a, b, c, d *as independent parameters.*

We shall next study the case for $\mathbf{G}_0$. From (9) we observe that

$$\beta_{D} : (a_m, b_m, c_m, d_m) \mapsto (-a_m, b_m, -c_m, d_m).$$

It follows that the fixed field of $\mathbb{Q}(a_m, b_m, c_m, d_m)$ by this action of β_{D} is generated by

$$(12) \qquad a_f := a_m^2, \quad b_f := \frac{b_m}{2}, \quad c_f := \frac{c_m - a_m}{2a_m}, \quad d_f := d_m,$$

and we have

$$(13)\qquad \begin{cases} a_g = d_f, \\ b_g = \dfrac{(a_f+4b_f^2-1)^2(b_f^2+a_fc_f^2)d_f^2}{4\big(a_f+(2b_f-1)^2\big)(a_f+4b_f^2)(a_f+4b_f^2+1)}, \\ j_g = \dfrac{\big(b_f^2-a_fc_f(c_f+1)\big)d_f^2}{a_f+4b_f^2}, \\ c_g = \dfrac{(a_f+4b_f^2-1)^2(a_fc_f-2b_f^2)\big(a_fc_f(c_f+1)-b_f^2\big)d_f^3}{4\big(a_f+(2b_f-1)^2\big)(a_f+4b_f^2)^2(a_f+4b_f^2+1)}, \\ d_g = \dfrac{b_f^2(a_f+4b_f^2-1)^4\big(b_f^2-a_fc_f(c_f+1)\big)^2d_f^4}{16\big(a_f+(2b_f-1)^2\big)^2(a_f+4b_f^2)^3(a_f+4b_f^2+1)^2}. \end{cases}$$

Substitute the above expressions into (5) and replace a_f, b_f, c_f, d_f by a, b, c, d. We thus obtain the following polynomial:

$$\begin{aligned}(14)\quad F_{\mathbf{G}_0}(a,b,c,d;X) &= X^8 - dX^6 \\ &+ \left(\frac{b^2-ac(c+1)}{(a+4b^2)} + \frac{(a+4b^2-1)^2(b^2+ac^2)}{4\big(a+(2b-1)^2\big)(a+4b^2)(a+4b^2+1)}\right)d^2X^4 \\ &- \frac{(a+4b^2-1)^2(ac-2b^2)\big(ac(c+1)-b^2\big)d^3}{4\big(a+(2b-1)^2\big)(a+4b^2)^2(a+4b^2+1)}X^2 \\ &+ \frac{b^2(a+4b^2-1)^4\big(b^2-ac(c+1)\big)^2d^4}{16\big(a+(2b-1)^2\big)^2(a+4b^2)^3(a+4b^2+1)^2}.\end{aligned}$$

Theorem 4.7. *$F_{\mathbf{G}_0}(a,b,c,d;X) \in \mathbb{Q}(a,b,c,d)[X]$ is a generic polynomial over $\mathbb{Q}$ for $\mathbf{G}_0$, when we regard a,b,c,d as independent parameters.*

We next study the descent from $\mathbf{G}_0$ to $\mathbf{G}_{64}$. Put $a_k := a_f/(4b_f^2)$. Then we have $\mathbb{Q}(a_f,b_f,c_f,d_f) = \mathbb{Q}(a_k,b_f,c_f,d_f)$, and observe from (12) that a_k, c_f, d_f are invariant under γ. It is easy to see that b_f is transformed as

$$\gamma : b_f \mapsto \frac{1}{4(a_k+1)b_f},$$

so that putting $b_k := 1/(b_f+\gamma(b_f))$, we obtain a system of generators of the fixed field of $\mathbf{G}_{64}$:

$$\mathbb{Q}(x_1,\dots,x_4)^{\mathbf{G}_{64}} = \mathbb{Q}(a_k,b_k,c_k,d_k),$$

where

$$a_k = \frac{a_f}{4b_f^2}, \quad b_k = \frac{a_f+4b_f^2}{(a_f+4b_f^2+1)b_f}, \quad c_k = c_f, \quad d_k = d_f.$$

Combining this and (13) we have

$$\begin{cases} a_g = d_k, \\ b_g = \dfrac{(a_k - b_k^2 + 1)(4a_kc_k^2 + 1)d_k^2}{2^4(a_k + 1)(a_k - b_k + 1)}, \\ c_g = \dfrac{(a_k - b_k^2 + 1)(2a_kc_k - 1)\big(4a_kc_k(c_k + 1) - 1\big)d_k^3}{2^5(a_k + 1)^2(a_k - b_k + 1)}, \\ d_g = \dfrac{(a_k - b_k^2 + 1)^2\big(4a_kc_k(c_k + 1) - 1\big)^2d_k^4}{2^{10}(a_k + 1)^3(a_k - b_k + 1)^2}. \end{cases}$$

Substituting these into (5) and then replacing a_k, b_k, c_k, d_k by a, b, c, d, we obtain the following:

Theorem 4.8. *The polynomial*

$$F_{\mathbf{G}_{64}}(a, b, c, d; X) = X^8 - dX^6 + \left(\frac{(a - b^2 + 1)(4ac^2 + 1)}{2^4(a + 1)(a - b + 1)} - \frac{4ac(c + 1) - 1}{4(a + 1)}\right)d^2X^4$$
$$- \frac{(a - b^2 + 1)(2ac - 1)\big(4ac(c + 1) - 1\big)d^3}{2^5(a + 1)^2(a - b + 1)}X^2 + \frac{(a - b^2 + 1)^2\big(4ac(c + 1) - 1\big)^2d^4}{2^{10}(a + 1)^3(a - b + 1)^2}$$

is a generic polynomial over $\mathbb{Q}$ for $\mathbf{G}_{64}$, when a, b, c, d are regarded as independent parameters.

Next we study the descent from $\mathbf{C}_8$ to $\mathbf{D}_8$, which is slightly more difficult since $\mathbf{D}_8$ is not a normal subgroup of $\mathbf{G}_{64}$. We observe that the action of $\beta_{_D}$ on $\mathbb{Q}(\underline{x})^{\langle\alpha\rangle} = \mathbb{Q}(c_1, \dots, c_5)$ is described simply as

$$\beta_{_D} : (c_1, c_2, c_3, c_4, c_5) \mapsto (-c_1, c_2, -c_3, c_4, c_5).$$

Put

$$a_d := \frac{2c_1}{c_3}, \quad b_d := \frac{c_1c_2}{c_3}, \quad c_d := c_4, \quad d_d := c_2c_5.$$

One then sees that these are all invariant under $\beta_{_D}$. Also one sees that

$$c_4 = c_d, \quad c_5 = \frac{a_d}{2b_d}, \quad c_1 = \frac{a_dc_3}{2}, \quad c_2 = \frac{2b_d}{a_d},$$

so that $\mathbb{Q}(c_1, \dots, c_5) = \mathbb{Q}(a_d, b_d, c_d, d_d, c_3)$. Furthermore we see that $\beta_{_D}(c_3) = -c_3$ implies $[\mathbb{Q}(a_d, b_d, c_d, d_d, c_3) : \mathbb{Q}(a_d, b_d, c_d, d_d)] = 2$; hence we conclude that $\mathbb{Q}(\underline{x})^{\mathbf{D}_8} = \mathbb{Q}(a_d, \dots, d_d)$. Now from (13) we have

$$a_f = -\frac{a_d^2 - 2b_d^2 + a_d^2c_d^2}{c_d^2(a_d^2 - 2b_d^2 + 2c_d^2)}, \quad b_f = \frac{1}{2c_d}, \quad c_f = \frac{c_d - b_d}{2b_d}, \quad d_f = d_d.$$

Substituting these into (14) and then replacing a_d, b_d, c_d, d_d by a, b, c, d, we obtain the following:

Theorem 4.9. *The polynomial*

$$\begin{aligned} F_{\mathbf{D}_8}(a,b,c,d;X) \;=\; & X^8 - dX^6 + \Bigg(\frac{a^2(b^2-c^2-1)}{4(a^2-2)b^2} \\ & + \frac{(a^2-b^2+c^2-1)^2\big(4b^2(b-c)+a^2\big(c+b^2c+c^3-2b(c^2+1)\big)\big)}{2^4(a^2-2)b^2\big(a^2+b^2(c-2)-(c-1)^2c\big)(b^2-c^2-1)} \Bigg) d^2X^4 \\ & - \frac{a^2(a^2-b^2+c^2-1)^2\big(2b(b-c)+a^2\big((b-c)c-1\big)\big)d^3}{2^5(a^2-2)^2b^3\big(a^2+b^2(c-2)-(c-1)^2c\big)}X^2 \\ & - \frac{a^4(a^2-b^2+c^2-1)^4(a^2-2b^2+2c^2)d^4}{2^{10}(a^2-2)^3b^4\big(a^2+b^2(c-2)-(c-1)^2c\big)^2} \end{aligned}$$

is a generic polynomial over $\mathbb{Q}$ for $\mathbf{D}_8$, when a,b,c,d are regarded as independent parameters.

Finally we study the descent from $\mathbf{C}_8$ to $\mathbf{QD}_8$. Observe that the action of β_Q on $\mathbb{Q}(\underline{x})^{\langle\alpha\rangle} = \mathbb{Q}(c_1,\dots,c_5)$ is described simply as

$$\beta_Q : (c_1,c_2,c_3,c_4,c_5) \mapsto (-c_1,-c_2,c_3,c_4,-c_5).$$

Put

$$a_q := \frac{c_2}{c_1}, \quad b_q := \frac{c_4}{c_1^2+1}, \quad c_q := \frac{c_3c_4}{c_1^2+1}, \quad d_q := c_2c_5.$$

One then sees that these are all invariant under β_Q. Also one sees that

$$c_3 = \frac{c_q}{b_q}, \quad c_2 = \frac{d_q}{c_5}, \quad c_4 = b_q + \frac{b_qd_q^2}{a_q^2c_5^2}, \quad c_1 = \frac{d_q}{a_qc_5},$$

from which it follows that $\mathbb{Q}(c_1,\dots,c_5) = \mathbb{Q}(a_q,b_q,c_q,d_q,c_5)$. Furthermore we see that $\beta_Q(c_5) = -c_5$ implies $[\mathbb{Q}(a_q,b_q,c_q,d_q,c_5) : \mathbb{Q}(a_q,b_q,c_q,d_q)] = 2$; hence we conclude that $\mathbb{Q}(\underline{x})^{\mathbf{QD}_8} = \mathbb{Q}(a_q,b_q,c_q,d_q)$. Now from (13) we have

$$\begin{cases} a_f = \dfrac{(a_q^2-2b_q^2-c_q^2)(2b_q^2+c_q^2+2)}{(a_q^2+2)^2b_q^2}, \\ b_f = \dfrac{a_q^2-2b_q^2-c_q^2}{2(a_q^2+2)b_q}, \\ c_f = \dfrac{-2a_q-2a_qb_q^2+2c_q+a_q^2c_q-a_qc_q^2}{2a_q(2b_q^2+c_q^2+2)}, \\ d_f = d_q. \end{cases}$$

We substitute these expressions into (14) and replace a_q,b_q,c_q,d_q by a,b,c,d. Then we obtain the following:

Theorem 4.10. *The polynomial*

$$\begin{aligned} F_{\mathbf{QD}_8}(a,b,c,d;X) &= X^8 - dX^6 + \Bigg(\frac{a^2(b^2+1)-c^2}{2a^2(2b^2+c^2+2)} \\ &\quad + \frac{\big(4b^2+a^2(b^2-1)+c^2\big)^2\big(c^2+a^2(b^2+c^2+1)-ac(2b^2+c^2+2)\big)}{8a^2\big(a^2(b^2+1)-c^2\big)(2b^2+c^2+2)\big(a^2(b-1)^2+4b^3+(2b-1)c^2\big)}\Bigg)d^2X^4 \\ &\quad - \frac{(a-c)\big(4b^2+a^2(b^2-1)+c^2\big)^2d^3}{2^4a^3(2b^2+c^2+2)\big(a^2(b-1)^2+4b^3+(2b-1)c^2\big)}X^2 \\ &\quad + \frac{(a^2-2b^2-c^2)\big(4b^2+a^2(b^2-1)+c^2\big)^4d^4}{2^8a^4(a^2+2)(2b^2+c^2+2)^2\big(a^2(b-1)^2+4b^3+(2b-1)c^2\big)^2} \end{aligned}$$

is a generic polynomial over $\mathbb{Q}$ *for* $\mathbf{QD}_8$*, when* a, b, c, d *are regarded as independent parameters.*

5. A $\mathbb{Q}$-versal polynomial for C_8

It has been known since the 1970s that NP for $\mathbf{C}_8/\mathbb{Q}$ has a negative answer (cf. [EM], [Vos1], [Len]). Saltman [Sal1] gave an explanation of this fact using Grunwald-Wang's theorem, which asserts that there is no $\mathbf{C}_8$-extension $K/\mathbb{Q}$ such that $K\otimes_{\mathbb{Q}}\mathbb{Q}_2$ is the unramified field extension of degree 8 over $\mathbb{Q}_2$.

It seems that after these results there has been no substantial development to the problem of describing the set of *all* $\mathbf{C}_8$-extensions of an arbitrary field of characteristic zero.

Applying the results of the previous section we shall give a fairly complete answer to this problem.

5.1. **Main result.** We have seen that the fixed field under $\mathbf{C}_8 = \langle\alpha\rangle$ is generated by $c_1, \dots, c_5$, which satisfy a single equation (7). On the other hand, we saw in the proof of Proposition 4.4 that $\mathbb{Q}(c_1, \dots, c_5) = \mathbb{Q}(c_2, a_m, b_m, c_m, d_m)$. From (9) one can rewrite equation (7) as

$$\begin{aligned} V(a_m,b_m,c_m,e_m) &:= (a_m^2+b_m^2-c_m^2) - 2\,e_m^2(a_m^2+b_m^2+1) = 0, \\ e_m &:= \frac{1}{c_2} = \frac{x_1x_2+x_2x_3-x_1x_4+x_3x_4}{x_1^2+x_2^2+x_3^2+x_4^2}. \end{aligned} \tag{15}$$

Now we view our $\mathbb{Q}$-generic $\mathbf{M}_{16}$-polynomial $F_{\mathbf{M}_{16}}(a,b,c,d;X)$, obtained in (11), as defined over the fixed field $\mathbb{Q}(a_m, b_m, c_m, d_m, e_m)$ under $\mathbf{C}_8$. The crucial point is that a_m, b_m, c_m, d_m are not free parameters here, but are subject to the relation $V(a_m, b_m, c_m, e_m) = 0$. This amounts to saying that in order to regard it as a $\mathbf{C}_8$-polynomial over $\mathbb{Q}(a_m, b_m, c_m, d_m, e_m)$, the value $R(a_m, b_m, c_m)$ should be a nonzero square, where we put

$$R(a_m,b_m,c_m) := \frac{2(a_m^2+b_m^2-c_m^2)}{a_m^2+b_m^2+1} \qquad (= 4\,e_m^2\,).$$

Thus we have the following result, which is one of the main results of this paper:

Theorem 5.1. *Let* K *be a field of characteristic zero, and suppose for* $a, b, c, d \in K$ *that* $R(a,b,c)$ *is a nonzero square while* a^2+b^2 *is a nonsquare element in* $K^\times$*. Then* $F_{\mathbf{M}_{16}}(a,b,c,d;X)$ *is an irreducible* $\mathbf{C}_8$*-polynomial over* K*, and the splitting*

field contains $K(\sqrt{a^2+b^2})$ as its unique quadratic subextension. Furthermore, $F_{\mathbf{M}_{16}}(a,b,c,d;X)$ with the condition $R(a,b,c)$ to be a nonzero square is a versal polynomial for $\mathbf{C}_8$ over $\mathbb{Q}$ in the sense of [BR]*, so that any $\mathbf{C}_8$-extension of K is obtained in this way.*

Proof. We first observe that $a_m^2+b_m^2$ is written as an element of $\mathbb{Q}(\underline{x})$ by

$$a_m^2+b_m^2=\frac{c_1^2+1}{c_4^2}=q_m^2,\quad q_m:=\frac{x_1x_2+x_2x_3-x_1x_4+x_3x_4}{x_1x_2-x_2x_3+x_1x_4+x_3x_4}$$

with $\alpha(q_m)=-q_m$. It follows that $\mathbb{Q}(\underline{x})^{\langle\alpha^2\rangle}=\mathbb{Q}(a_m,b_m,c_m,d_m,e_m,q_m)$, over which $\mathbb{Q}(\underline{x})$ is a $\mathbf{C}_4$-extension and that $F_{\mathbf{M}_{16}}(a_m,b_m,c_m,d_m;X)$ splits into the product of two factors of degree 4. Since this polynomial is already known to be an irreducible $\mathbf{C}_8$-polynomial over $\mathbb{Q}(a_m,b_m,c_m,d_m,e_m)=\mathbb{Q}(\underline{x})^{\langle\alpha\rangle}$, we see that this is the only way through which it becomes reducible. Now let L/K be any $\mathbf{C}_8$-extension whose Galois group is generated by σ. Then by the normal basis theorem one finds $\bar{x}_1\in L$, which together with $\bar{x}_2=\sigma(\bar{x}_1)$, $\bar{x}_3=\sigma^2(\bar{x}_1)$, $\bar{x}_3=\sigma^3(\bar{x}_1)$ generates an irreducible $\mathbb{Q}[\sigma]$-module on which $\sigma^4=-id$. One can define from $\bar{x}_1,\dots,\bar{x}_4$ those elements $\bar{c}_1,\dots,\bar{c}_5$ and $\bar{a}_m,\bar{b}_m,\bar{c}_m,\bar{d}_m$ in the same way as above without making denominators vanish, since there are infinitely many choices of $\bar{x}_1$. Thus we obtain a specialized polynomial $F_{\mathbf{M}_{16}}(\bar{a}_m,\bar{b}_m,\bar{c}_m,\bar{d}_m;X)\in K[X]$ whose splitting field over K is obviously $K(\bar{x}_1)=L$. This completes the proof. □

It should be noted that $F_{\mathbf{M}_{16}}(a,b,c,d;X)$ can further degenerate. Indeed one can show from the results of the previous section that $F_{\mathbf{M}_{16}}(a,b,c,d;X)$ is reducible and is a product of two factors of degree 4 if and only if a^2+b^2 is a square in K. Putting $a=m^2-n^2$, $b=2mn$, we indeed have the following decomposition:

$$F_{\mathbf{M}_{16}}(m^2-n^2,2mn,c,d;X)=F_4(m,n,c,d;X)F_4(n,m,-c,d;X),$$

where

$$F_4(m,n,c,d;X)=X^4-\frac{d(m^2+n^2+c)}{2(m^2+n^2)}X^2 + \frac{d^2n^2\big((m^2+n^2)^2-1\big)^2(m^2+n^2+c)^2}{16(m^2+n^2)^3\big((m^2+n^2)^2-4mn+1\big)\big((m^2+n^2)^2+1\big)}.$$

Recall that, for a quadratic extension $K=k(\sqrt{m})$ of k to be the subfield of a $\mathbf{C}_4$-extension of k, it is necessary and sufficient that m is a sum of two nonzero squares of k: $m=a^2+b^2$ for some $a,b\in k^\times$ (cf. [Ser], Theorem 1.2.4). From the above discussion we obtain a similar criterion for K to be extended to a $\mathbf{C}_8$-extension of k.

Corollary 5.2. *Let $K=k(\sqrt{a^2+b^2})$ be a quadratic extension of a field k of characteristic zero. For the existence of a $\mathbf{C}_8$-extension of k containing K, it is necessary and sufficient that there exists $c\in k^\times$ for which $R(a,b,c)$ is a nonzero square in k.*

Remark 5.3. From Corollary 5.2 we obtain, without using the Kronecker-Weber theorem, that for $k=\mathbb{Q}$ the discriminant of the quadratic field K which can be embedded in a $\mathbf{C}_8$-extension consists of only primes 2, and $p\equiv 1 \pmod 8$. This fact corresponds to the Grunwald-Wang theorem, which asserts that the unramified $\mathbf{C}_8$-extension L_2 over $\mathbb{Q}_2$ cannot be the splitting field of a $\mathbf{C}_8$-polynomial in $\mathbb{Q}[X]$. On the other hand, we find a solution $a_m=2$, $b_m=1$, $c_m=\sqrt{-7}$, $e_m=1$ in $\mathbb{Q}_2$

to (15) for which $\mathbb{Q}_2(\sqrt{a_m^2+b_m^2})/\mathbb{Q}_2$ is unramified. Hence L_2 is the splitting field of $F_{\mathbf{M}_{16}}(2,1,\sqrt{-7},d_m;X)$ over $\mathbb{Q}_2$.

5.2. **Example 1: Kummer extensions.** As a typical example of Theorem 5.1, we describe how the Kummer extensions can be recovered from a specialization of $F_{\mathbf{M}_{16}}(a,b,c,d;X)$. Thus we assume that the base field K contains the primitive root ζ of unity of order 8, and $L=K(\theta)$ is a $\mathbf{C}_8$-extension of K with $\mathrm{Gal}(L/K)=\langle\sigma\rangle$ such that $\sigma(\theta)=\zeta\theta$ and $m:=\theta^8$ is a nonsquare element of $K^\times$. Our aim is to find $a_\theta, b_\theta, c_\theta, d_\theta$ and e_θ in K satisfying $V(a_\theta,b_\theta,c_\theta,e_\theta)=0$ such that L is the splitting field of $F_{\mathbf{M}_{16}}(a_\theta,b_\theta,c_\theta,d_\theta;X)$ over K. For this purpose we put

$$y_1 := \theta+\theta^3+\theta^5,$$

and

$$y_i := \sigma^{i-1}(y_1),\ i=2,3,4.$$

Then it follows that

$$\sigma : (y_1,y_2,y_3,y_4) \longmapsto (y_2,y_3,y_4,-y_1).$$

Also we see that $L=K(\theta)=K(y_1,y_2,y_3,y_4)$. Let $a_\theta,b_\theta,c_\theta,d_\theta,e_\theta$ be the elements of K obtained by substituting $x_i=y_i$ $(i=1,\dots,4)$ in the expression (10), (15) of a_m,b_m,c_m,d_m,e_m. By direct computations we obtain

$$\begin{aligned}&(a_\theta,b_\theta,c_\theta,d_\theta,e_\theta)\\ &=\left(\frac{\zeta^2(m+1)(m^2-m+1)}{2m},\ \frac{(m-1)(m^2+m+1)}{2m},\ \zeta^2,\ 8m,\ \frac{\zeta(\zeta^2-1)}{2}\right).\end{aligned}$$

In particular we have $V(a_\theta,b_\theta,c_\theta,e_\theta)=0$. The polynomial $F_{\mathbf{M}_{16}}(a_\theta,b_\theta,c_\theta,d_\theta;X)$ now becomes

$$\begin{aligned}F(m;X)=X^8-8mX^6+4m(3m-5)X^4\\ +8m(m^2-m-1)X^2-m(m^2+m+1)^2,\end{aligned}$$

which splits completely in $L[X]$ as

$$F(m;X) \;=\; \prod_{i=0}^{7}\left(X-(\zeta^i\theta+\zeta^{3i}\theta^3+\zeta^{5i}\theta^5)\right).$$

Also we have

$$R(a_\theta,b_\theta,c_\theta) \;=\; 2 \;=\; \left(\sqrt{2}\right)^2 \in (K^\times)^2$$

and

$$a_\theta^2+b_\theta^2 \;=\; -m \in K^\times\setminus(K^\times)^2.$$

It follows that $F(m,X)=F_{\mathbf{M}_{16}}(a_\theta,b_\theta,c_\theta,d_\theta;X)$ is a $\mathbf{C}_8$-polynomial over K, and the splitting field of it is $K(y_1,y_2,y_3,y_4)=K(\theta)=L$.

5.3. **Example 2.** Here we shall give a simple family of $\mathbf{C}_8$-polynomials with two parameters and illustrate how one can recover its splitting field by a specialization of $F_{\mathbf{M}_{16}}(a,b,c,d;X)$.

We start by putting $(a,b,c)\to(4a,a^2,2a^3)$ in the polynomial $F_{\mathbf{G}_{128}}(a,b,c,d;X)$ given by (4). This gives a simple polynomial with two parameters

$$F(a,d;X) \;:=\; X^8-4aX^6+5a^2X^4-2a^3X^2+d.$$

Proposition 5.4. *$F(a,d;X)$ is a family of $\mathbf{G}_0$-polynomials. More precisely, the splitting field of $F(a,d;X)$ over $\mathbb{Q}(a,d)$ is a $\mathbf{G}_0$-extension that is not regular over $\mathbb{Q}$.*

Proof. Suppose s is a zero of $F(a,d;X)$ so that $F(a,d;s)=0$. Then solving this equation in d we have $d=s^2(a-s^2)^2(2a-s^2)$. Substitution of this expression gives a decomposition

$$F(a,d;X) \quad := \quad (X^2-s^2)(X^2+s^2-2a)\Big(X^4-2aX^2+(s^2-a)^2\Big),$$

from which we see that the splitting field has degree $8\times 4=32$ over $\mathbb{Q}(a,d)$. Also if we put $t=\sqrt{2a-s^2}$, then we see that

$$a \,=\, \frac{1}{2}(s^2+t^2), \quad d \,=\, \frac{1}{4}\Big(s^2t^2\big(s^2-t^2\big)^2\Big),$$

and the zeros of $F(a,d;X)$ are

$$\left\{\pm s, \quad \pm t, \quad \pm\frac{s-t}{\sqrt{2}}, \quad \pm\frac{s+t}{\sqrt{2}}\right\}.$$

It follows that the splitting field is $\mathbb{Q}(\sqrt{2},s,t)$, which is not a regular extension over $\mathbb{Q}$. Finally one can check that the following maps $\alpha,\beta_{_D},\beta_{_Q},\beta_{_M}$ are automorphisms of $\mathbb{Q}(\sqrt{2},s,t)/\mathbb{Q}(a,d)$,

$$\begin{cases} \alpha : (s,t,\sqrt{2}) \mapsto \left(\dfrac{s-t}{\sqrt{2}}, \dfrac{s+t}{\sqrt{2}}, -\sqrt{2}\right), \\ \beta_{_D} : (s,t,\sqrt{2}) \mapsto (-t,-s,-\sqrt{2}), \\ \beta_{_Q} : (s,t,\sqrt{2}) \mapsto (-t,-s,\sqrt{2}), \\ \beta_{_M} : (s,t,\sqrt{2}) \mapsto (s,t,-\sqrt{2}), \end{cases}$$

which satisfy

$$\alpha^8=1, \quad \beta_{_D}\alpha\beta_{_D}^{-1}=\alpha^{-1}, \quad \beta_{_Q}\alpha\beta_{_Q}^{-1}=\alpha^3, \quad \beta_{_M}\alpha\beta_{_M}^{-1}=\alpha^5.$$

It follows that the Galois group of $\mathbb{Q}(\sqrt{2},s,t)/\mathbb{Q}(a,d)$ is isomorphic to $\mathbf{G}_0$. □

Observe that, if we put $d=2e^2$ with $e=\dfrac{1}{2\sqrt{2}}\Big(st(s^2-t^2)\Big)$, then we have

$$\alpha(e)=\beta_{_D}(e)=e, \quad \beta_{_Q}(e)=\beta_{_M}(e)=-e.$$

This implies the following:

Corollary 5.5. *The polynomial*

$$F(a,2e^2;X) \quad = \quad X^8-4aX^6+5a^2X^4-2a^3X^2+2e^2$$

is a $\mathbf{D}_8$-polynomial over $\mathbb{Q}(a,e)$.

Now we further make a specialization by the replacement

$$a\mapsto 2q, \quad e\mapsto \frac{q^2\big((p-1)^2-2\big)}{p^2+1},$$

which gives the polynomial

$$H(p,q;X) \quad = \quad X^8-8qX^6+20q^2X^4-16q^3X^2+\frac{2q^4(p^2-2p-1)^2}{(p^2+1)^2}.$$

Proposition 5.6. *$H(p,q;X)$ is a family of $\mathbf{C}_8$-polynomials. More precisely, the splitting field of $H(p,q;X)$ over $\mathbb{Q}(p,q)$ is a $\mathbf{C}_8$-extension containing $\mathbb{Q}(\sqrt{2})$.*

Proof. One can regard p, q as elements of $\mathbb{Q}(\sqrt{2}, s, t)$. Namely it is easy to find the expressions

$$q = \frac{1}{4}(s^2+t^2), \quad p = \frac{s^2+2st-t^2+\sqrt{2}(s^2-t^2)}{s^2-t^2-2st(\sqrt{2}+1)}.$$

It follows that $\mathbb{Q}(\sqrt{2}, s, t)^{\langle\alpha\rangle} = \mathbb{Q}(p,q)$, which proves the assertion. □

Our next aim is to recover $H(p,q;X)$ or its splitting field from the $\mathbb{Q}$-versal polynomial $F_{\mathbf{M}_{16}}(a,b,c,d;X)$. Actually, it turns out that one cannot obtain $H(p,q;X)$ directly from $F_{\mathbf{M}_{16}}(a,b,c,d;X)$ by specialization of the parameters. Instead, we put $x_1 := s^3$ and look at the $\langle\alpha\rangle$-orbit of x_1. This orbit is given by

$$\begin{aligned}&\{x_1, \dots, x_4, -x_1, \dots, -x_4\}\\ &= \left\{s^3, \frac{(s-t)^3}{2\sqrt{2}}, t^3, \frac{(s+t)^3}{2\sqrt{2}}, -s^3, -\frac{(s-t)^3}{2\sqrt{2}}, -t^3, -\frac{(s+t)^3}{2\sqrt{2}}\right\},\end{aligned}$$

and from (10) we have expressions for a_m, b_m, c_m, d_m by s, t, and then by p, q using elimination. The result is

(16)

$$\begin{cases} a_m = -\dfrac{3}{8}\dfrac{(p^4-6p^2+1)}{(p^2+1)^2} \\ \qquad\qquad \cdot \dfrac{(23p^4+36p^3+46p^2-36p+23)(31p^4+4p^3+62p^2-4p+31)}{\big(505(p^8+1)+1848(p^7+p^5-p^3-p)+2932(p^6+p^2)+1206p^4\big)}, \\ b_m = -\dfrac{3}{8}\dfrac{(p^2-2p-1)^4}{(p^2+1)^2} \\ \qquad\qquad \cdot \dfrac{(41p^4-36p^3+82p^2+36p+41)}{\big(505(p^8+1)+1848(p^7+p^5-p^3-p)+2932(p^6+p^2)+1206p^4\big)}, \\ c_m = -\dfrac{9}{40}\dfrac{(p^4-6p^2+1)}{(p^2+1)^2}, \\ d_m = 80q^3. \end{cases}$$

Now substituting these expressions we find that $F_{\mathbf{M}_{16}}(a_m, b_m, c_m, d_m; X^3)$ is decomposed into a product of $H(p,q;X)$ and a factor of degree 16. Thus we have shown that the splitting field of $H(p,q;X)$ is obtained as that of a specialization (16) of $F_{\mathbf{M}_{16}}(a,b,c,d;X)$. Also we can show the following equalities:

$$\begin{aligned} R(a_m, b_m, c_m) &= \frac{2(a_m^2+b_m^2-c_m^2)}{1+a_m^2+b_m^2} = \left(\frac{3}{5}\cdot\frac{p^2-2p-1}{p^2+1}\right)^2, \\ a_m^2+b_m^2 &= 2\left(\frac{3}{8}\cdot\frac{p^2-2p-1}{p^2+1}\right)^2. \end{aligned}$$

6. The group $\mathbf{G}_0$ in the Cremona group of dimension 2

6.1. **GNP for $\mathbf{G}_0$ in $\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(x,y)$.** Here we describe how the group $\mathbf{G}_0$, as well as $\mathbf{G}_{32}$, $\mathbf{G}_{64}$, can be realized as a subgroup of the Cremona group $\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(x,y)$, and discuss briefly the Generalized Noether's problem (GNP) for its subgroups. We

should remark that this is not to rephrase the results of section 3. For example, we see that the following $\mathbb{Q}$-automorphism

$$\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(x,y) \ni \alpha \ : \ (x,y) \longmapsto \left(y, \frac{x+1}{-x+1}\right) \tag{17}$$

has order 8. Nevertheless, as we shall show in Theorem 6.2 below, the fixed field $\mathbb{Q}(x,y)^{\langle\alpha\rangle}$ is rational over $\mathbb{Q}$. This means that there exists a positive answer of the General Noether's Problem for $\mathbf{C}_8/\mathbb{Q}$ in dimension two. The linear fractional transformations

$$\delta_x : x \longmapsto \frac{x+1}{-x+1}, \qquad \iota_x : x \longmapsto -x$$

satisfy $\delta_x^4 = \iota_x^2 = 1$, $\iota_x\delta_x\iota_x^{-1} = \delta_x^{-1}$; hence we have $\langle\delta_x, \iota_x\rangle \cong \mathbf{D}_4$. Indeed it is not difficult to show that any subgroup of $\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(x) \cong \mathrm{PGL}_2(\mathbb{Q})$ isomorphic to $\mathbf{D}_4$ is conjugate to $\langle\delta_x, \iota_x\rangle$. Let $\langle\delta_y, \iota_y\rangle$ be a copy of this group in $\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(y)$, and let $\tau : (x,y) \longmapsto (y,x)$ be the transposition. We then see that these five automorphisms together generate a subgroup $\mathbf{G}_{128}$ of a 2-group of order $2^7 = 128$ in $\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(x,y)$:

$$\mathbf{G}_{128} \ := \ \langle \delta_x,\ \iota_x,\ \delta_y,\ \iota_y,\ \tau\rangle \ \cong \ (\mathbf{D}_4 \times \mathbf{D}_4) \rtimes \mathbf{C}_2.$$

In $\mathbf{G}_{128}$ we find the following elements of order 2:

$$\begin{cases} \beta_D \ := \ \iota_y\iota_x\delta_x^{-1} : (x,y) \longmapsto \left(\dfrac{x+1}{x-1}, -y\right), \\ \beta_Q \ := \ \delta_y^2\iota_y\delta_x\iota_x : (x,y) \longmapsto \left(\dfrac{x+1}{x-1}, \dfrac{1}{y}\right), \\ \beta_M \ := \ \delta_y^2 : (x,y) \longmapsto \left(x, \dfrac{-1}{y}\right), \end{cases}$$

which commute with each other and generate a group isomorphic to Klein's four group. Furthermore we have

$$\beta_{_D}\alpha\beta_{_D}^{-1} = \alpha^{-1}, \quad \beta_{_Q}\alpha\beta_{_Q}^{-1} = \alpha^3, \quad \beta_{_M}\alpha\beta_{_M}^{-1} = \alpha^5,$$

where $\alpha = \alpha_x\tau$ is an element of order 8 as in (17). Thus we have

$$\langle\alpha\rangle \cong \mathbf{C}_8, \quad \langle\alpha, \beta_{_D}\rangle \cong \mathbf{D}_8, \quad \langle\alpha, \beta_{_Q}\rangle \cong \mathbf{QD}_8, \quad \langle\alpha, \beta_{_M}\rangle \cong \mathbf{M}_{16},$$

so that $\langle\alpha, \beta_{_D}, \beta_{_Q}, \beta_{_M}\rangle$ is a realization of $\mathbf{G}_0$ in the Cremona group $\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(x,y)$ of dimension two.

We shall now study the fixed field under $\langle\alpha\rangle$. First note that α^4 is an involution $(x,y) \mapsto (-1/x, -1/y)$.

The fixed field under this type of involution has been known to be rational, with an explicit set of generators given by several authors (e.g., [Haj2]). Namely we have the following.

Lemma 6.1. *Let k be a field of characteristic zero and $k(X,Y)$ be the rational function field over k with two variables X, Y and let α be a k-involution of $k(X,Y)$ given by*

$$\alpha \quad : \quad \begin{cases} X \longmapsto m_1/X, \\ Y \longmapsto m_2/Y, \end{cases}$$

with $m_1, m_2 \in k^\times$. Then the fixed field of $k(X, Y)$ under this involution is

$$k^{\langle\alpha\rangle} \quad = \quad k\left(\frac{X^2Y^2 - m_1m_2}{Y(X^2 - m_1)}, \frac{X(Y^2 - m_2)}{Y(X^2 - m_1)}\right).$$

Proof. Put $u := \frac{X^2Y^2-m_1m_2}{Y(X^2-m_1)}$, $v := \frac{X(Y^2-m_2)}{Y(X^2-m_1)}$. We see immediately that u, v are fixed by α, so that $k(u, v) \subseteq k^{\langle\alpha\rangle}$. On the other hand, it follows from $u - Xv = m_2/Y$, $Y = m_2/(u - Xv)$ that $k(X, Y) = k(X, u, v)$, and also that X satisfies the quadratic equation $uvX^2 - (u^2 + m_1 - m_2)X + uvm_1 = 0$. We now have $[k(X, Y) : k(u, v)] = [k(X, u, v) : k(u, v)] = 2$; hence $k^{\langle\alpha\rangle} = k(u, v)$. □

Applying Lemma 6.1, we have $\mathbb{Q}(x, y)^{\langle\alpha^4\rangle} = \mathbb{Q}(s_0, t_0)$ where

$$s_0 = \frac{x^2y^2 - 1}{y(x^2 + 1)}, \quad t_0 = \frac{x(y^2 + 1)}{y(x^2 + 1)}.$$

We then see that α^2 transforms (x, y) to $\left(\frac{1+x}{1-x}, \frac{1+y}{1-y}\right)$; hence it induces an involution on $\mathbb{Q}(s_0, t_0)$ such that

$$\alpha^2 \quad : \quad \begin{cases} s_0 \ \longmapsto \ \dfrac{-2s_0(t_0 + 1)}{s_0^2 + t_0^2 - 1}, \\ t_0 \ \longmapsto \ \dfrac{s_0^2 - t_0^2 + 1}{s_0^2 + t_0^2 - 1}. \end{cases}$$

Putting

$$s := \frac{t_0 - 1}{s_0}, \quad t := \frac{t_0 + 1}{s_0} \qquad \left(s = \frac{y - x}{xy + 1}, \quad t = \frac{x + y}{xy - 1}\right),$$

one sees that $\mathbb{Q}(s_0, t_0) = \mathbb{Q}(s, t)$ and that the action of α^2 on s_2, t_2 is expressed simply as $\alpha^2 : (s, t) \mapsto (s, -1/t)$. It follows that $\mathbb{Q}(s, t)^{\langle\alpha^2\rangle} = \mathbb{Q}(p, q)$ where

(18)
$$p = s + 1, \quad q = \frac{1}{2}\Big(t - \frac{1}{t}\Big) \quad \left(p = \frac{xy - x + y + 1}{xy + 1}, \quad q = \frac{(x + y)^2 - (xy - 1)^2}{2(x + y)(xy - 1)}\right).$$

Now α induces an involution on $\mathbb{Q}(p, q)$ such that

$$\alpha \quad : \quad (p, q) \longmapsto \left(\frac{2}{p}, \frac{-1}{q}\right)$$

so that one can again apply Lemma 6.1. Thus we have proved the following assertion on GNP for $\mathbf{C}_8/\mathbb{Q}$ in contrast to the negative answers to NP and LNP (cf. Fact 1.6 in §1).

Theorem 6.2. *The fixed field of $\mathbb{Q}(x, y)$ under $\langle\alpha\rangle \cong \mathbf{C}_8$ is rational over $\mathbb{Q}$ and is equal to $\mathbb{Q}(x, y)^{\langle\alpha\rangle} = \mathbb{Q}(a_0, b_0)$, where a_0, b_0 are given by*

$$a_0 \ = \ \frac{p^2q^2 + 2}{q(p^2 - 2)}, \qquad b_0 \ = \ \frac{p(q^2 + 1)}{q(p^2 - 2)}. \tag{19}$$

We next study the action of $\beta_{D}, \beta_{Q}, \beta_{M}$ on various subfields of $\mathbb{Q}(x,y)$. From (18) we first see that they act on $\mathbb{Q}(s_0,t_0)=\mathbb{Q}(s,t)$ as

$$\beta_{D}:\begin{cases} s\longmapsto \dfrac{-s+1}{s+1},\\ t\longmapsto \dfrac{-t+1}{t+1},\end{cases}\quad \beta_{Q}:\begin{cases} s\longmapsto \dfrac{s+1}{s-1},\\ t\longmapsto \dfrac{t+1}{t-1},\end{cases}\quad \beta_{M}:\begin{cases} s\longmapsto \dfrac{-1}{s},\\ t\longmapsto \dfrac{-1}{t}.\end{cases}$$

Then from (18) we see that they transform p,q as

$$\beta_{D}:\begin{cases} p\longmapsto \dfrac{2}{p},\\ q\longmapsto \dfrac{1}{q},\end{cases}\quad \beta_{Q}:\begin{cases} p\longmapsto \dfrac{2(p-1)}{p-2},\\ q\longmapsto \dfrac{1}{q},\end{cases}\quad \beta_{M}:\begin{cases} p\longmapsto \dfrac{p-2}{p-1},\\ q\longmapsto q.\end{cases}$$

It is not difficult to see from (19) that β_{D},β_{Q} transform a_0,b_0 as

$$\beta_{D}:\begin{cases} a_0\longmapsto -a_0,\\ b_0\longmapsto -b_0,\end{cases}\qquad \beta_{Q}:\begin{cases} a_0\longmapsto \dfrac{(a_0-2b_0)^2+2}{a_0},\\ b_0\longmapsto \dfrac{a_0^2-3a_0b_0+2b_0^2+1}{a_0};\end{cases}$$

hence for $\beta_{M}=\beta_{D}\beta_{Q}$ we obtain

$$\beta_{M}\ :\ a_0\longmapsto -\frac{(a_0-2b_0)^2+2}{a_0},\quad b_0\longmapsto -\frac{a_0^2-3a_0b_0+2b_0^2+1}{a_0}.$$

Now we choose new generators a,b of $\mathbb{Q}(x,y)^{\langle\alpha\rangle}=\mathbb{Q}(a_0,b_0)$ as

$$a:=\frac{1}{b_0},\quad b:=\frac{a_0-b_0}{b_0}\qquad \Big(a=\frac{q(p^2-2)}{p(q^2+1)},\quad b=\frac{p^2q^2-pq^2-p+2}{p(q^2+1)}\Big).$$

Then we see that $\mathbb{Q}(x,y)^{\langle\alpha\rangle}=\mathbb{Q}(a,b)$ and $\beta_{D},\beta_{Q},\beta_{M}$ transform a,b as

$$\beta_{D}:\begin{cases} a\longmapsto -a,\\ b\longmapsto b,\end{cases}\quad \beta_{Q}:\begin{cases} a\longmapsto \dfrac{a(b+1)}{a^2+b^2-b},\\ b\longmapsto \dfrac{a^2-b+1}{a^2+b^2-b},\end{cases}\quad \beta_{M}:\begin{cases} a\longmapsto \dfrac{-a(b+1)}{a^2+b^2-b},\\ b\longmapsto \dfrac{a^2-b+1}{a^2+b^2-b}.\end{cases}\tag{20}$$

Proposition 6.3. *The fixed fields of $\mathbb{Q}(x,y)$ under $\langle\alpha,\beta_{D}\rangle$, $\langle\alpha,\beta_{Q}\rangle$, and $\langle\alpha,\beta_{M}\rangle$ are all rational over $\mathbb{Q}$. More precisely we have*

$$\mathbb{Q}(x,y)^{\langle\alpha,\beta_{D}\rangle}=\mathbb{Q}(a^2,b),\quad \mathbb{Q}(x,y)^{\langle\alpha,\beta_{Q}\rangle}=\mathbb{Q}(a_q,b_q),\quad \mathbb{Q}(x,y)^{\langle\alpha,\beta_{M}\rangle}=\mathbb{Q}(a_m,b_m),$$

where $a_q,b_q,a_m,b_m\in\mathbb{Q}(x,y)^{\langle\alpha\rangle}=\mathbb{Q}(a,b)$ are given by

$$\begin{aligned}(a_q,b_q)&=\Big(\frac{a(b+1)}{a^2+b^2+1},\frac{a^2-2b}{b^2-1}\Big),\\ (a_m,b_m)&=\Big(\frac{b-1}{a},\frac{a^2-2b}{a(b+1)}\Big).\end{aligned}\tag{21}$$

Proof. The assertion for $\langle\alpha,\beta_{D}\rangle$ is obvious. To prove the assertion for $\langle\alpha,\beta_{Q}\rangle$, first note from (20) that a_q,b_q are fixed by α,β_{Q}, so that $\mathbb{Q}(a_q,b_q)\subseteq\mathbb{Q}(a,b)^{\langle\alpha,\beta_{Q}\rangle}$. We then rewrite (21) as

$$a_q(a^2+b^2+1)-a(b+1)=0,\qquad b_q(b^2-1)-(a^2-2b)=0.$$

Eliminating a^2 we obtain an expression of a as an element of $\mathbb{Q}(b, a_q, b_q)$:

$$a = a_q(b_q b - b_q + b + 1).$$

It follows that $\mathbb{Q}(a, a_q, b_q) = \mathbb{Q}(a, b)$. Also by taking the resultant of them w.r.t. a, we obtain the equality

$$a_q^2(b_q b - b_q + b + 1)^2 - b_q b^2 + b_q - 2b = 0,$$

which shows that $[\mathbb{Q}(a,b) : \mathbb{Q}(a_q, b_q)] = 2 = [\mathbb{Q}(a,b) : \mathbb{Q}(a,b)^{\langle \alpha, \beta_{Q} \rangle}]$. This proves $\mathbb{Q}(x,y)^{\langle \alpha, \beta_{Q} \rangle} = \mathbb{Q}(a,b)^{\langle \alpha, \beta_{Q} \rangle} = \mathbb{Q}(a_q, b_q)$. The assertion for $\langle \alpha, \beta_{M} \rangle$ can be proved similarly, and we omit the details. □

Now we consider the fixed field under $\langle \alpha, \beta_{D}, \beta_{Q}, \beta_{M} \rangle \cong \mathbf{G}_0$, which is the intersection of any two of $\mathbb{Q}(a^2, b), \mathbb{Q}(a_q, b_q), \mathbb{Q}(a_m, b_m)$. By inspection one sees from (20) that the following two elements belong to this field:

$$\begin{cases} a_f := a_m^2 = \dfrac{-2a_q^2 + 1}{a_q^2(b_q^2 + 1)} = \dfrac{(b-1)^2}{a^2}, \\ b_f := \dfrac{b_m}{a_m} = b_q = \dfrac{a^2 - 2b}{b^2 - 1}. \end{cases}$$

It follows that $[\mathbb{Q}(a_m, b_m) : \mathbb{Q}(a_f, b_f)] = 2 = [\langle \alpha, \beta_{D}, \beta_{Q}, \beta_{M} \rangle : \langle \alpha, \beta_{M} \rangle]$ from the first expression. Then one can show as the proof of Proposition 6.3 the following:

Proposition 6.4. *We have $\mathbb{Q}(x,y)^{\langle \alpha, \beta_{D}, \beta_{Q}, \beta_{M} \rangle} = \mathbb{Q}(a_f, b_f)$, so that it is rational over $\mathbb{Q}$.*

6.2. **Two-parameter H-polynomials for $H \subseteq \mathbf{G}_{128}$.** Finally we construct polynomials which correspond to the extensions $\mathbb{Q}(x,y)/\mathbb{Q}(x,y)^H$ for various subgroups H of $\mathbf{G}_{128}$. Let $R_\delta(x,y)$ be the union of the $\langle \delta_x, \iota_y \rangle$-orbit of x and the $\langle \delta_y, \iota_y \rangle$-orbit of y:

$$R_\delta(x,y) := \left\{ x,\ \frac{-1}{x},\ \frac{1+x}{1-x},\ \frac{x-1}{1+x},\ y,\ \frac{-1}{y},\ \frac{1+y}{1-y},\ \frac{y-1}{1+y} \right\},$$

and put

$$\mathrm{Aut}_{\mathbb{Q}} R_\delta(x,y) := \left\{ \varphi \in \mathrm{Aut}_{\mathbb{Q}} \mathbb{Q}(x,y) \,\middle|\, \varphi(R_\delta(x,y)) = R_\delta(x,y) \right\}.$$

The following lemma can be proved easily.

Lemma 6.5. *$\mathrm{Aut}_{\mathbb{Q}} R_\delta(x,y)$ is a group of order 2^5 generated by δ_x, δ_y and τ, and is isomorphic to $(\mathbf{C}_4 \times \mathbf{C}_4) \rtimes \mathbf{C}_2$.*

We put for simplicity $\mathbf{G}_{32} := \mathrm{Aut}_{\mathbb{Q}} R_\delta(x,y)$, and consider the monic separable polynomial $f(X)$ of degree 8 whose roots are elements of $R_\delta(x,y)$. Since $R_\delta(x,y)$ is stable under the transformation $z \mapsto -1/z$, one sees that $f(X)$ is expanded in the following form:

$$\begin{aligned} f(X) &= \prod_{\xi \in R_\delta(x,y)} \Big(X - \xi \Big) \\ &= X^8 - s_1 X^7 + s_2 X^6 - s_3 X^5 + s_4 X^4 + s_3 X^3 + s_2 X^2 + s_1 X + 1. \end{aligned}$$

A direct computation shows that the coefficients satisfy the equalities

$$s_3 + 7s_1 = 0, \quad s_4 + 2s_2 - 14 = 0.$$

We obtain from $f(X)$ the following polynomial:

$$(22)\quad F_{32}(s_1,s_2;X) := X^8 - s_1X^7 + s_2X^6 + 7s_1X^5 - 2(s_2-7)X^4 - 7s_1X^3 + s_2X^2 + s_1X + 1$$

with

$$\begin{cases} s_1 = \dfrac{(x+y)(xy-1)\big((xy-1)^2-(x+y)^2\big)}{xy(x^2-1)(y^2-1)}, \\ s_2 = \dfrac{(x^4-6x^2+1)(y^4-6y^2+1)}{xy(x^2-1)(y^2-1)} - 12. \end{cases}$$

Now we can show that (22) implies the following.

Proposition 6.6. *We have $\mathbb{Q}(x,y)^{\mathbf{G}_{32}} = \mathbb{Q}(s_1,s_2)$. $F_{32}(s_1,s_2;X) \in \mathbb{Q}(s_1,s_2)[X]$ is a $\mathbf{G}_{32}$-polynomial over $\mathbb{Q}(s_1,s_2)$, when s_1,s_2 are regarded as independent parameters.*

Note that $\mathbf{G}_{32}$ has $\langle \alpha, \beta_{M}\rangle \cong \mathbf{M}_{16}$ as a subgroup of index 2. In particular, one can express s_1, s_2 as a rational function of a_m, b_m as

$$(23)\quad \begin{cases} s_1 = s_1^M(a_m,b_m) := \dfrac{-8(a_m^2+b_m^2+2)}{b_m^3 - a_mb_m^2 + a_m + 3b_m}, \\ s_2 = s_2^M(a_m,b_m) := \dfrac{16(a_m^3 - a_m^2b_m + 3a_m + b_m)}{b_m^3 - a_mb_m^2 + a_m + 3b_m} - 12. \end{cases}$$

Hence from (22) we have

Corollary 6.7. *The polynomial*

$$F_{16}(a_m,b_m;X) := F_{32}(s_1^M(a_m,b_m), s_2^M(a_m,b_m);X)$$

is an $\mathbf{M}_{16}$-polynomial over $\mathbb{Q}(a_m,b_m) = \mathbb{Q}^{\langle \alpha,\beta_{M}\rangle}$ with independent parameters a_m, b_m.

Example 6.8. By specializing the parameters a_m, b_m of $F_{16}(a_m,b_m;X)$ as $(a_m,b_m) := (8/u, -8/u)$, we obtain the following simple polynomial over $\mathbb{Q}(u)$:

$$\begin{aligned} f_{16}^{(1)}(u;X) &:= F_{16}\Big(\frac{8}{u}, \frac{-8}{u}; X\Big) \quad \Big(= F_{32}(u,-28;X)\Big) \\ &= X^8 - uX^7 - 28X^6 + 7uX^5 + 70X^4 - 7uX^3 - 28X^2 + uX + 1. \end{aligned}$$

Y.-Y. Shen [She] studied the polynomial $f_{16}^{(1)}(u;X)$ from the viewpoint of constructing a system of fundamental units of a real octic number field that contains $\mathbb{Q}(\sqrt{2})$ (see also Shen-Washington [SW]). If we suppose that θ is a zero of $f_{16}^{(1)}(u;X)$ so that $f_{16}^{(1)}(u;\theta) = 0$, then we have

$$u = \frac{(\theta^4+4\theta^3-6\theta^2-4\theta+1)(\theta^4-4\theta^3-6\theta^2+4\theta+1)}{\theta(\theta+1)(\theta-1)(\theta^2+2\theta-1)(\theta^2-2\theta-1)}$$

and the zeros of $f_{16}^{(1)}(u;X)$ are

$$\left\{ \theta,\ \theta',\ \frac{\theta+1}{-\theta+1},\ \frac{\theta'+1}{-\theta'+1},\ \frac{-1}{\theta},\ \frac{-1}{\theta'},\ \frac{\theta-1}{\theta+1},\ \frac{\theta'-1}{\theta'+1} \right\},$$

where

$$\theta' := \frac{-(\sqrt{2}+1)\theta - 1}{\theta - (\sqrt{2}+1)}.$$

Thus the splitting field of $f_{16}^{(1)}(u;X)$ over $\mathbb{Q}(u)$ is $\mathbb{Q}(\sqrt{2},\theta)$, which is not a regular extension over $\mathbb{Q}$. The maps

$$\alpha \ : \ (\theta,\sqrt{2}) \ \mapsto (\theta',\sqrt{2}), \qquad \beta_{_M} \ : \ (\theta,\sqrt{2}) \ \mapsto (\theta,-\sqrt{2})$$

are automorphisms of $\mathbb{Q}(\sqrt{2},\theta)/\mathbb{Q}(u)$ that satisfy

$$\alpha^8 = 1, \qquad \beta_{_M}\,\alpha\,\beta_{_M}^{-1} = \alpha^5,$$

because $\alpha^2(\theta) = (\theta+1)/(-\theta+1)$, $\beta_{_M}(\theta') = -1/\theta'$. Hence the polynomial $f_{16}^{(1)}(u;X)$ is an $\mathbf{M}_{16}$-polynomial over $\mathbb{Q}(u)$ and is also a $\mathbf{C}_8$-polynomial over $\mathbb{Q}(\sqrt{2},u)$.

We can also obtain the following $\mathbf{M}_{16}$-polynomials over $\mathbb{Q}(u)$ with constant term one:

$$\begin{aligned} f_{16}^{(2)}(u;X) \ &:= \ F_{16}\Big(u-1,\frac{-u+2}{u};X\Big) \\ &= \ X^8 + 2u(u^2+2)(X^7-7X^5+7X^3-X) + 4(u^4-3)(X^6+X^2) \\ &\quad - 2(4u^4-19)X^4 + 1, \\ f_{16}^{(3)}(u;X) \ &:= \ F_{16}(u,1;X) \\ &= \ X^8 + 2(u^2+3)(X^7-7X^5+7X^3-X) \\ &\quad + 4(u^3-u^2+3u-2)(X^6+X^2) - 2(4u^3-4u^2+12u-15)X^4 + 1. \end{aligned}$$

Next we consider the case for $\mathbf{C}_8$. Since $\mathbf{C}_8$ is a subgroup of $\mathbf{M}_{16}$ with index 2, we obtain the following $\mathbf{C}_8$-polynomial over $\mathbb{Q}(a,b)$ by substituting (21) in the expression (23).

Corollary 6.9. *The polynomial*

$$F_8(a,b;X) \quad := \quad F_{32}(s_1(a,b),s_2(a,b);X)$$

with

$$\begin{cases} s_1(a,b) \ = \ \dfrac{-8a(b+1)(a^2+b^2+1)^2}{a^6+2a^4b^2+a^2b^4+4a^4-4b^4-12a^2b-8b^3-a^2+4b^2}, \\ s_2(a,b) \ = \ \dfrac{16(b+1)^2(a^4+2a^2b^2+b^4-4a^2-4b^2+4b-1)}{a^6+2a^4b^2+a^2b^4+4a^4-4b^4-12a^2b-8b^3-a^2+4b^2} - 12 \end{cases}$$

is a $\mathbf{C}_8$-polynomial over $\mathbb{Q}(a,b) = \mathbb{Q}(x,y)^{\langle\alpha\rangle}$, where we regard a,b as independent parameters.

We put $R_\delta^\pm(x,y) := R_\delta(x,y) \cup R_\delta(-x,-y)$ and define the group $\mathrm{Aut}_{\mathbb{Q}}R_\delta^\pm(x,y)$ similarly as $\mathrm{Aut}_{\mathbb{Q}}R_\delta(x,y)$:

$$\mathrm{Aut}_{\mathbb{Q}}R_\delta^\pm(x,y) \quad := \quad \Big\{\varphi \in \mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(x,y) \ \Big| \ \varphi(R_\delta^\pm(x,y)) = R_\delta^\pm(x,y)\Big\}.$$

The following lemma can be proved easily.

Lemma 6.10. *We have*

$$\mathrm{Aut}_{\mathbb{Q}}R_\delta^\pm(x,y) \quad = \quad \mathbf{G}_{128} \ = \ \langle \delta_x, \ \delta_y, \ \iota_x, \ \iota_y, \ \tau\rangle.$$

Let $g(X)$ be the monic separable polynomial of degree 16 whose roots are elements of $R_\delta^\pm(x,y)$. Then as for $f(X)$ one can express $g(X)$ as

$$\begin{aligned} g(X) \ &= \ \prod_{\xi\in R_\delta^\pm(x,y)} \Big(X-\xi\Big) \\ &= \ X^{16} + t_1X^{14} + t_2X^{12} + t_3X^{10} + t_4X^8 + t_3X^6 + t_2X^4 + t_1X^2 + 1, \end{aligned}$$

and one sees that the coefficients satisfy the equalities

$$22t_2 + 16t_3 + 7t_4 - 2002 = 0, \quad 11t_1 + 3t_3 + 2t_4 - 396 = 0.$$

It follows that $g(X)$ is expressed as

$$\begin{aligned} F_{128}(h_1, h_2; X) \ &= X^{16} + (h_1 - h_2)(X^{14} + X^2) + 2(h_1 + h_2 + 14)(X^{12} + X^4) \\ &\quad - (h_1 + 15h_2)(X^{10} + X^6) - 2(2h_1 - 14h_2 - 99)X^8 + 1 \end{aligned}$$

with

$$\begin{cases} h_1 \ = \ \dfrac{(x^8 + 14x^4 + 1)(y^8 + 14y^4 + 1)}{4x^2y^2(x^2 - 1)^2(y^2 - 1)^2}, \\ h_2 \ = \ \dfrac{(x^2 + 1)^4(y^2 + 1)^4}{4x^2y^2(x^2 - 1)^2(y^2 - 1)^2} - 4. \end{cases}$$

This implies the following.

Proposition 6.11. *We have* $\mathbb{Q}(x, y)^{\mathbf{G}_{128}} = \mathbb{Q}(h_1, h_2)$, *and* $F_{128}(h_1, h_2; X) \in \mathbb{Q}(h_1, h_2)[X]$ *is a* $\mathbf{G}_{128}$*-polynomial over* $\mathbb{Q}(h_1, h_2)$.

We note that $\mathbf{G}_{128}$ has the following subgroup of index 2 which contains $\mathbf{G}_{32}$:

$$\mathbf{G}_{64} \ := \ \langle \alpha, \ \beta_D, \ \beta_Q, \ \beta_M, \ \tau \rangle.$$

We see that the group $\mathbf{G}_{64}$ acts on $\mathbb{Q}(x, y)^{\mathbf{G}_{32}} = \mathbb{Q}(s_1, s_2)$ as $(s_1, s_2) \mapsto (-s_1, s_2)$, where s_1 and s_2 are defined in (22). Thus if we put

$$(r_1, r_2) \ := \ (s_1^2, s_2),$$

then we have $\mathbb{Q}(x, y)^{\mathbf{G}_{64}} = \mathbb{Q}(r_1, r_2)$. Also we can check the equalities

$$h_1 \ = \ \frac{12r_1 + r_2^2}{4}, \quad h_2 \ = \ \frac{16r_1 - 8r_2 + r_2^2}{4}.$$

Hence we have the following proposition:

Proposition 6.12. *We have* $\mathbb{Q}(x, y)^{\mathbf{G}_{64}} = \mathbb{Q}(r_1, r_2)$, *and the polynomial*

$$\begin{aligned} F_{64}(r_1, r_2; X) \ &:= \ F_{128}\left(\frac{12r_1 + r_2^2}{4}, \frac{16r_1 - 8r_2 + r_2^2}{4}; X\right) \\ &= X^{16} - (r_1 - 2r_2)(X^{14} + X^2) + (14r_1 - 4r_2 + r_2^2 + 28)(X^{12} + X^4) \\ &\quad - (63r_1 - 30r_2 + 4r_2^2)(X^{10} + X^6) + 2(50r_1 - 28r_2 + 3r_2^2 + 99)X^8 + 1 \end{aligned}$$

is a $\mathbf{G}_{64}$*-polynomial over* $\mathbb{Q}(r_1, r_2)$. *Also we have the equality*

$$F_{64}(s_1^2, s_2; X^2) \ = \ F_{32}(s_1, s_2; X)F_{32}(s_1, s_2; -X).$$

It is worth mentioning that $F_{128}(h_1, h_2; X)$, $F_{64}(r_1, r_2; X)$, $F_{32}(s_1, s_2; X)$ and $f_{16}^{(i)}(u; X)$ $(i = 1, 2, 3)$ are monic polynomials with constant term one, all other coefficients being simple integral polynomials in their parameters.

References

[BR] J. Buhler and Z. Reichstein, *On the essential dimension of a finite group*, Compositio Math. **106** (1997) 159–179. MR1457337 (98e:12004)

[CHK] H. Chu, S. Hu, and M. Kang, *Noether's problem for dihedral 2-groups*, Comment. Math. Helv. **79** (2004) 147–159. MR2031703 (2004i:12004)

[DeM] F. R. DeMeyer, *Generic Polynomials*, J. Algebra **84** (1983) 441–448. MR723401 (85a:12007)

[DM] F. DeMeyer and T. McKenzie, *On generic polynomials*, J. Algebra **261** (2003) 327–333. MR1966633 (2003m:12007)

[EM] S. Endo and T. Miyata, *Invariants of finite abelian groups*, J. Math. Soc. Japan **25** (1973) 7–26. MR0311754 (47:316)

[GMS] S. Garibaldi, A. Merkurjev, and J.-P. Serre, *Cohomological Invariants in Galois Cohomology*, University Lecture Series 28, American Mathematical Society, Providence, RI, 2003. MR1999383 (2004f:11034)

[Haj1] M. Hajja, *A note on monomial automorphisms*, J. Algebra **85** (1993) 243–250. MR723077 (85k:12001)

[Haj2] M. Hajja, *Rationality of finite groups of monomial automorphisms of* $k(x, y)$, J. Algebra **109** (1987) 46–51. MR898335 (88j:12002)

[HK] M. Hajja and M. Kang, *Three-dimensional purely monomial group actions*, J. Algebra **170** (1994) 805–860. MR1305266 (95k:12008)

[Has] K. Hashimoto, *On Brumer's family of RM-curves of genus two*, Tohoku Math. J. (2) **52** (2000) 475–488. MR1793932 (2001k:14056)

[HH1] K. Hashimoto and A. Hoshi, *Families of cyclic polynomials obtained from geometric generalization of Gaussian period relations*, Math. Comp. **74** (2005) 1519–1530. MR2137015 (2005m:12003)

[HH2] K. Hashimoto and A. Hoshi, *Geometric generalization of Gaussian period relations with application to Noether's problem for meta-cyclic groups*, Tokyo J. Math. **28** (2005) 13–32. MR2149620 (2006c:12002)

[HT] K. Hashimoto and H. Tsunogai, *Generic Polynomials over* $\mathbb{Q}$ *with two parameters for the transitive groups of degree five*, Proc. Japan. Acad. Ser. A **79** (2003) 142–145. MR2022057 (2004i:12005)

[Hos] A. Hoshi, *Noether's problem for some meta-abelian groups of small degree*, Proc. Japan Acad. Ser. A **81** (2005) 1–6. MR2068482 (2005i:12004)

[JLY] C. Jensen, A. Ledet and N. Yui, *Generic polynomials. Constructive aspects of the inverse Galois problem*, Mathematical Sciences Research Institute Publications, vol. 45, Cambridge, 2002. MR1969648 (2004d:12007)

[Kan1] M. Kang, *Introduction to Noether's problem for dihedral groups*, Algebra Colloquium **11** (2004) 71–78. MR2058965

[Kan2] M. Kang, *Noether's problem for dihedral* 2*-groups II*, Pacific J. Math. **222** (2005) 301-316. MR2225074 (2007a:12003)

[Kem1] G. Kemper, *A constructive approach to Noether's problem*, Manuscripta Math. **90** (1996) 343–363. MR1397662 (97d:13005)

[Kem2] G. Kemper, *Generic polynomials are descent-generic*, Manuscripta Math. **105** (2001) 139–141. MR1885819 (2002k:12009)

[KM] G. Kemper and E. Mattig, *Generic polynomials with few parameters*, J. Symbolic Comput. **30** (2000) 843–857. MR1800681 (2001h:12006)

[Led1] A. Ledet, *Generic polynomials for quasi-dihedral, dihedral and modular extensions of order* 16, Proc. Amer. Math. Soc. **128** (1999) 2213–2222. MR1707525 (2000k:12003)

[Led2] A. Ledet, *On groups with essential dimension one*, J. Algebra **311** (2007) 31–37. MR2309876

[Len] H. W. Lenstra, *Rational functions invariant under a finite abelian group*, Invent. Math. **25** (1974) 299–325. MR0347788 (50:289)

[MM] G. Malle and B. H. Matzat, *Inverse Galois Theory*, Springer-Verlag, 1999. MR1711577 (2000k:12004)

[MiyT] T. Miyata, *Invariants of certain groups. I*, Nagoya Math. J. **41** (1971) 69–73. MR0272923 (42:7804)

[MiyK] K. Miyake, *Linear fractional transformations and cyclic polynomials*. Algebraic number theory (Hapcheon/Saga, 1996). Adv. Stud. Contemp. Math. (Pusan) **1** (1999) 137–142. MR1701914 (2000j:11159)

[Noe] E. Noether, *Gleichungen mit vorgeschriebener Gruppe*, Math. Ann. **78** (1918) 221–229. MR1511893

[Rik] Y. Rikuna, *Explicit constructions of generic polynomials for some elementary groups*, Galois theory and modular forms, 173–194, Dev. Math., 11, Kluwer Acad. Publ., Boston, MA, 2004. MR2059763 (2005f:12006)

[Sal1] D. J. Saltman, *Generic Galois extensions and problems in field theory*, Adv. Math., **43** (1982) 250–283. MR648801 (84a:13007)

[Sal2] D. J. Saltman, *Retract rational fields and cyclic Galois extensions*, Israel J. Math. **47** (1984), 165–215. MR738167 (85j:13008)

[Sch] L. Schneps, *On cyclic field extensions of degree* 8, Math. Scand. **71** (1992) 24–30. MR1216101 (94d:12004)

[Ser] J.-P. Serre, *Topics in Galois Theory*, Research Notes in Mathematics, **1**, Jones and Bartlett Publishers, Boston, MA, 1992. MR1162313 (94d:12006)

[She] Y.-Y. Shen, Unit groups and class numbers of real cyclic octic fields, Trans. Amer. Math. Soc. **326** (1991) 179–209. MR1031243 (91j:11092)

[SW] Y.-Y. Shen, L. C. Washington, A family of real 2^n-tic fields, Trans. Amer. Math. Soc. **345** (1994) 413–434. MR1264151 (95c:11125)

[Swa1] R. G. Swan, *Invariant rational functions and a problem of Steenrod*, Invent. Math. **7** (1969) 148–158. MR0244215 (39:5532)

[Swa2] R. G. Swan, *Noether's Problem in Galois Theory*, Emmy Noether in Bryn Mawr, 21–40, Springer-Verlag, 1983. MR713790 (84k:12013)

[Vos1] V. E. Voskresenskiĭ, *Fields of invariants of abelian groups*, (Russian) Uspehi Mat. Nauk **28** (1973) 77–102. English translation: Russian Math. Survey **28** (1973) 79–105. MR0392935 (52:13748)

[Vos2] V. E. Voskresenskiĭ, Algebraic groups and their birational invariants. Translations of Mathematical Monographs, 179. American Mathematical Society, Providence, RI, 1998. MR1634406 (99g:20090)

Department of Applied Mathematics, School of Fundamental Science and Engineering, Waseda University, 3–4–1 Ohkubo, Shinjuku-ku, Tokyo, 169–8555, Japan

E-mail address: khasimot@waseda.jp

Department of Mathematics, School of Education, Waseda University, 1–6–1 Nishi-Waseda, Shinjuku-ku, Tokyo, 169–8050, Japan

E-mail address: hoshi@ruri.waseda.jp

Department of Applied Mathematics, School of Fundamental Science and Engineering, Waseda University, 3–4–1 Ohkubo, Shinjuku-ku, Tokyo, 169–8555, Japan

E-mail address: rikuna@moegi.waseda.jp