# 行政院國家科學委員會專題研究計畫　期中進度報告

## 逆 Galois 問題與有理性問題(2/3)

計畫類別：個別型計畫
計畫編號：NSC92-2115-M-002-014-
執行期間：92 年 08 月 01 日至 93 年 07 月 31 日
執行單位：國立臺灣大學數學系暨研究所

計畫主持人：康明昌

報告類型：精簡報告
報告附件：出席國際會議研究心得報告及發表論文
處理方式：本計畫可公開查詢

中　華　民　國 93 年 4 月 23 日

Available at WWW.MATHEMATICSWEB.ORG
POWERED BY SCIENCE DIRECT
Advances in Mathematics 181 (2004) 321–352
ADVANCES IN Mathematics
http://www.elsevier.com/locate/aim

# Rationality problem of $GL_4$ group actions

Ming-Chang Kang

*Department of Mathematics, National Taiwan University, Taipei 106, Taiwan, ROC*

Received 1 May 2001; accepted 19 November 2002

Communicated by Melvin Hochster

**Abstract**

Let $K$ be any field which may not be algebraically closed, $V$ be a four-dimensional vector space over $K$, $\sigma \in GL(V)$ where the order of $\sigma$ may be finite or infinite, $f(T) \in K[T]$ be the characteristic polynomial of $\sigma$. Let $\alpha$, $\alpha\beta_1$, $\alpha\beta_2$, $\alpha\beta_3$ be the four roots of $f(T) = 0$ in some extension field of $K$.

**Theorem 1.** *Both $K(V)^{\langle\sigma\rangle}$ and $K(\mathbb{P}(V))^{\langle\sigma\rangle}$ are rational* (= *purely transcendental*) *over $K$ if at least one of the following conditions is satisfied*: (i) *char* $K = 2$, (ii) *$f(T)$ is a reducible or inseparable polynomial in $K[T]$*, (iii) *not all of $\beta_1, \beta_2, \beta_3$ are roots of unity*, (iv) *if $f(T)$ is separable irreducible, then the Galois group of $f(T)$ over $K$ is not isomorphic to the dihedral group of order* 8 *or the Klein four group.*

**Theorem 2.** *Suppose that all $\beta_i$ are roots of unity and $f(T) \in K[T]$ is separable irreducible.* (a) *If the Galois group of $f(T)$ is isomorphic to the dihedral group of order* 8, *then both $K(V)^{\langle\sigma\rangle}$ and $K(\mathbb{P}(V))^{\langle\sigma\rangle}$ are not stably rational over $K$.* (b) *When the Galois group of $f(T)$ is isomorphic to the Klein four group, then a necessary and sufficient condition for rationality of $K(V)^{\langle\sigma\rangle}$ and $K(\mathbb{P}(V))^{\langle\sigma\rangle}$ is provided.* (See Theorem 1.5. for details.)



*MSC:* primary 13A50; 14E08; 12G05

*Keywords:* Rationality; Noether's problem; Multiplicative actions; Algebraic tori

## 1. Introduction

Let $K$ be any field, $K(x_1, \ldots, x_n)$ be a rational function field of $n$ variables over $K, \sigma$ be a $K$-automorphism acting on $K(x_1, \ldots, x_n)$ by

$$\sigma : x_1 \mapsto x_2 \mapsto \cdots \mapsto x_n \mapsto x_1.$$

*E-mail address:* kang@math.ntu.edu.tw.

0001-8708/$ - see front matter © 2003 Elsevier Science (USA). All rights reserved.
doi:10.1016/S0001-8708(03)00067-7

It was asked by Emmy Noether [14] that whether the fixed field $K(x_1, \dots, x_n)^{\langle\sigma\rangle}$ is rational (= purely transcendental) over $K$. Around 1960s Masuda showed that $\mathbb{Q}(x_1, \dots, x_n)^{\langle\sigma\rangle}$ was rational if $n = 2, 3, 4, 5, 6, 7, 11$ [12]. The first counter-example to Noether's problem was constructed by Swan [18] who showed that $\mathbb{Q}(x_1, \dots, x_n)^{\langle\sigma\rangle}$ was not rational if $n = 47, 113, 233$. For a survey of Noether's problem and related topics, see Swan's paper [19].

Swan's counter-example for $n = 47$ uses the arithmetic of $\mathbb{Q}(\zeta_{23})$ whose class number is not one; note that $\mathbb{Q}(\zeta_{23})$ is the first cyclotomic field not of class number one. Later Lenstra gave a complete solution of the rationality problem of $K(x_1, \dots, x_n)^{\langle\sigma\rangle}$, in particular, that of $\mathbb{Q}(x_1, \dots, x_n)^{\langle\sigma\rangle}$ [11]. As Lenstra pointed out, those integers $n$ such that $n < 47$ and $\mathbb{Q}(x_1, \dots, x_n)^{\langle\sigma\rangle}$ was not rational were $n = 8, 16, 24, 32, 40$ [11, (7.3) Corollary]. A new proof of the non-rationality of $\mathbb{Q}(x_1, \dots, x_8)^{\langle\sigma\rangle}$ and similar cases was found by Saltman [15, Theorem 5.11]. Saltman's proof used a result of Shianghaw Wang, which corrected a mistake in Grunwald's Theorem.

Using the non-rationality of $\mathbb{Q}(x_1, \dots, x_8)^{\langle\sigma\rangle}$, it was shown that both the fixed fields $\mathbb{Q}(y_1, y_2, y_3, y_4)^{\langle\sigma\rangle}$ and $\mathbb{Q}(z_1, z_2, z_3)^{\langle\sigma\rangle}$ were not rational over $\mathbb{Q}$ [1, Example 2.3] where

$$\sigma : y_1 \mapsto y_2 \mapsto y_3 \mapsto y_4 \mapsto -y_1, z_1 \mapsto z_2 \mapsto z_3 \mapsto -1/(z_1 z_2 z_3).$$

Being led by the above examples, we would like to find the rationality of $k(x_1, \dots, x_n)^{\langle\sigma\rangle}$ where $\sigma \in GL_n(K)$ and $n \leqslant 4$. Here are the answers:

**1.1. Theorem** (Noether [14,13]). *If $G$ is any subgroup of $GL_2(K)$, then $K(x_1, x_2)^G$ is rational over $K$.*

**1.2. Theorem** (Ahmad et al. [1, Theorems 4.1 and 4.3]). *Let $K$ be any field.*

(1) *If $\sigma \in GL_3(K)$, then both $K(x_1, x_2, x_3)^{\langle\sigma\rangle}$ and $K(x_1/x_3, x_2/x_3)^{\langle\sigma\rangle}$ are rational over $K$.*

(2) *If $\sigma$ is a $K$-automorphism on $K(x_1, x_2, x_3)$ defined by*

$$\sigma(x_j) = \sum_{1 \leqslant i \leqslant 3} a_{ij} x_i + b_j \quad \text{for } 1 \leqslant j \leqslant 3,$$

*where $a_{ij}, b_j \in K$ and $\det(a_{ij}) \neq 0$, then $K(x_1, x_2, x_3)^{\langle\sigma\rangle}$ is rational over $K$.*

(3) *If $\sigma$ is a $K$-automorphism on $K(x_1, x_2)$ defined by*

$$\sigma(x_1) = (a_1 x_1 + b_1)/(c_1 x_1 + d_1), \quad \sigma(x_2) = (a_2 x_2 + b_2)/(c_2 x_2 + d_2),$$

*where $a_i, b_i, c_i, d_i \in K$ and $a_i d_i - b_i c_i \neq 0$ for $1 \leqslant i \leqslant 2$, then $K(x_1, x_2)^{\langle\sigma\rangle}$ is rational over $K$.*

What we shall prove in this paper are the following theorems:

**1.3. Theorem.** *Let $K$ be any field which may not be algebraically closed, $V$ be a four-dimensional vector space over $K$, $\sigma \in GL(V)$ where the order of $\sigma$ may be finite or infinite, $f(T) \in K[T]$ be the characteristic polynomial of $\sigma$. Let $\alpha, \alpha\beta_1, \alpha\beta_2, \alpha\beta_3$ be the four roots of $f(T) = 0$ in some extension field of $K$. Then both $K(V)^{\langle\sigma\rangle}$ and $K(\mathbb{P}(V))^{\langle\sigma\rangle}$ are rational over $K$, if at least one of the following conditions is satisfied*:

(i) *char $K = 2$*,
(ii) *$f(T)$ is a reducible or inseparable polynomial in $K[T]$*,
(iii) *not all of $\beta_1, \beta_2, \beta_3$ are roots of unity*,
(iv) *if $f(T)$ is a separable irreducible polynomial in $K[T]$ and $G$ denotes the Galois group of $f(T)$ over $K$, then $G$ is not isomorphic to $D_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$ where $D_4$ denotes the dihedral group of order 8 and $\mathbb{Z}_n$ denotes the cyclic group of order $n$.*

**1.4. Theorem.** *Let the notations be the same as in Theorem* 1.3. *Suppose that all the $\beta_i$ are roots of unity for $1 \leqslant i \leqslant 3$, $f(T) \in K[T]$ is separable irreducible and the Galois group $G$ is isomorphic to $D_4$. Then*

(i) *char $K \neq 2$ and $f(T) = (T^2 - \alpha^2)(T^2 - \alpha^2\beta^2)$, i.e. $\{\beta_1, \beta_2, \beta_3\} = \{\beta, -\beta, -1\}$, with $4 | ord(\beta)$.*
(ii) *both $K(V)^{\langle\sigma\rangle}$ and $K(\mathbb{P}(V))^{\langle\sigma\rangle}$ are not stably rational over $K$.*

**1.5. Theorem.** *Let the notations be the same as in Theorem* 1.3. *Suppose that all the $\beta_i$ are roots of unity for $1 \leqslant i \leqslant 3$, $f(T) \in K[T]$ is separable irreducible and the Galois group $G$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.*

*Define integers $n_1, n_2, m_1, m_2, d, k, i$ as follows: $n_j = ord(\beta_j)$, $d = \gcd\{n_1, n_2\}$, $n_j = dm_j$ for $1 \leqslant j \leqslant 2$, $\beta_1^{m_1} = \beta_2^{km_2}$. Let $\tau = (\alpha, \alpha\beta_1)(\alpha\beta_2, \alpha\beta_3) \in G$, i.e. $\tau(\alpha) = \alpha\beta_1$, $\tau(\alpha\beta_1) = \alpha$, $\tau(\alpha\beta_2) = \alpha\beta_3$, $\tau(\alpha\beta_3) = \alpha\beta_2$. Define an integer $i$ by $\tau(\beta_2) = \beta_2^i$. Define $a, b, c$ by $i + 1 = da$, $i - 1 = m_2 b$, $2k = cd - m_1 b$. In case $d = 1$, it is understood that $k = 0$; otherwise, $k$ is uniquely determined modulo $d$ and $i$ is uniquely determined modulo $n_2$. Then*

(i) *$a, b, c$ are integers and* $\gcd\{b, d\} = 1$ *or* 2;
(ii) *char $K \neq 2$*;
(iii) *$K(V)^{\langle\sigma\rangle}$ (resp. $K(\mathbb{P}(V))^{\langle\sigma\rangle}$) is rational over $K$ if and only if any one of the following conditions is satisfied*:
   (1) *not both of $b$ and $d$ are even integers*,
   (2) $b \equiv d \equiv 2 \pmod 4$ *and* $a + c \equiv 0 \pmod 2$,
   (3) $b \equiv 0 \pmod 4$, $d \equiv 2 \pmod 4$ *and* $m_1 + m_2 \equiv 0 \pmod 2$,
   (4) $b \equiv 2 \pmod 4$, $d \equiv 0 \pmod 4$ *and* $a + c \equiv 0 \pmod 2$.

If $K(V)^{\langle\sigma\rangle}$ (*resp.* $K(\mathbb{P}(V))^{\langle\sigma\rangle}$) *is not rational over* $K$, *it is not stably rational over* $K$. *Explicitly, the non-rational cases are the situations*:

$(1)'$ $b \equiv d \equiv 2 \pmod 4$ *and* $a + c \equiv 1 \pmod 2$,
$(2)'$ $b \equiv 0 \pmod 4$, $d \equiv 2 \pmod 4$, *and* $m_1 + m_2 \equiv 1 \pmod 2$,
$(3)'$ $b \equiv 2 \pmod 4$, $d \equiv 0 \pmod 4$ *and* $a + c \equiv 1 \pmod 2$.

A special case of Theorem 1.5 is the following.

**1.6. Theorem.** *Let the notations be the same as in Theorem* 1.3. *Suppose that all the* $\beta_i$ *are roots of unity for* $1 \leqslant i \leqslant 3$, $f(T) \in K[T]$ *is separable irreducible and the Galois group* $G$ *is isomorphic to* $\mathbb{Z}_2 \times \mathbb{Z}_2$. *If the subgroup* $\{\beta_1, \beta_2, \beta_3\}$ *is generated by one of* $\{\beta_1, \beta_2, \beta_3\}$, *then* $\{\beta_1, \beta_2, \beta_3\} = \{\beta, \beta^j, \beta^{1-j}\}$ *for some integer* $j$. *Let* $n = ord(\beta)$. *Then*

(i) $2j(j-1)$ *is divisible by* $n$;
(ii) $K(V)^{\langle\sigma\rangle}$ (*resp.* $K(\mathbb{P}(V))^{\langle\sigma\rangle}$) *is rational over* $K$ *if and only if* $2j(j-1)/n$

*is an even integer. If* $K(V)^{\langle\sigma\rangle}$ (*resp.* $K(\mathbb{P}(V))^{\langle\sigma\rangle}$) *is not rational over* $K$, *it is not stably rational over* $K$.

*In particular, if* $\{\beta_1, \beta_2, \beta_3\} = \{\beta, -\beta, -1\}$, *then* $K(V)^{\langle\sigma\rangle}$ (*resp.* $K(\mathbb{P}(V))^{\langle\sigma\rangle}$) *is not stably rational over* $K$ *if and only if* $ord(\beta)$ *is divisible by* 4. *If* $K(V)^{\langle\sigma\rangle}$ (*resp.* $K(\mathbb{P}(V))^{\langle\sigma\rangle}$) *is stably rational over* $K$, *it is rational over* $K$.

As applications we get the following Theorems 1.7 and 1.8.

**1.7. Theorem.** *Let* $K$ *be any field,* $\sigma$ *be a* $K$*-automorphism on* $K(x_1, x_2, x_3, x_4)$ *defined by*

$$\sigma : x_1 \mapsto x_2 \mapsto x_3 \mapsto x_4 \mapsto (-a^2/b)x_1 + ax_3,$$

*where* $a, b \in K \backslash \{0\}$. *Then both* $K(x_1, x_2, x_3, x_4)^{\langle\sigma\rangle}$ *and* $K(x_1/x_4, x_2/x_4, x_3/x_4)^{\langle\sigma\rangle}$ *are rational over* $K$ *if at least one of the following conditions is satisfied*:

(i) *char* $K = 2$;
(ii) *no root of the equation* $T^4 - (b-2)T^2 + 1 = 0$ *is a root of unity*;
(iii) *at least one of* $b^2 - 4b$, $a + (2a/\sqrt{b})$, $a - (2a/\sqrt{b})$ *is in* $K^2$;
(iv) $b - 4 \in K^2$.

*If char* $K \neq 2$, $b^2 - 4b$, $a + (2a/\sqrt{b})$, $a - (2a/\sqrt{b}) \notin K^2$ *and* $\beta$ *is a root of* $T^4 - (b-2)T^2 + 1 = 0$ *with* $ord(\beta) = n < \infty$, *then* $K(x_1, x_2, x_3, x_4)^{\langle\sigma\rangle}$ (*resp.*

$K(x_1/x_4, x_2/x_4, x_3/x_4)^{\langle\sigma\rangle}$) *is not stably rational over* $K$ *if and only if either* (1) $b \in K^2$ *and* $4|n$, *or* (2) $b$ *and* $b-4 \notin K^2$.

**1.8. Theorem.** *Let* $K$ *be any field,* $\sigma$ *be a* $K$*-automorphism on* $K(x_1, x_2, x_3, x_4)$ *defined by*

$$\sigma : x_1 \mapsto x_2 \mapsto x_3 \mapsto x_4 \mapsto -ax_1,$$

*where* $a \in K\backslash\{0\}$. *Then* $K(x_1, x_2, x_3, x_4)^{\langle\sigma\rangle}$) (*resp.* $K(x_1/x_4, x_2/x_4, x_3/x_4)^{\langle\sigma\rangle}$) *is rational over* $K$ *if and only if at least one of the following conditions is satisfied,* (i) *char* $K = 2$; (ii) $-a \in K^2$; (iii) $4a \in K^4$; (iv) $-1 \in K^2$. *If* $K(x_1, x_2, x_3, x_4)^{\langle\sigma\rangle}$ (*resp.* $K(x_1/x_4, x_2/x_4, x_3/x_4)^{\langle\sigma\rangle}$) *is not rational over* $K$, *it is not stably rational over* $K$.

**1.9. Theorem.** *Let* $K$ *be any field,* $\sigma$ *be a* $K$*-automorphism on* $K(x_1, x_2, x_3, x_4)$ *defined by*

$$\sigma(x_j) = \sum_{1 \leqslant i \leqslant 4} a_{ij}x_i + b_j \quad \textit{for } 1 \leqslant j \leqslant 4,$$

*where* $a_{ij}, b_j \in K$ *and* det $(a_{ij}) \neq 0$. *Let* $f(T)$ *be the characteristic polynomial of* $(a_{ij}) \in GL_4(K)$. *Then* $K(x_1, x_2, x_3, x_4)^{\langle\sigma\rangle}$ *is rational over* $K$ *except for the case* $f(1) \neq 0$ *and* $f(T)$ *is the minimal polynomial of* $(a_{ij})$. *If* $f(1) \neq 0$ *and* $f(T)$ *is the minimal polynomial of* $(a_{ij})$, *then there exist* $y_1, y_2, y_3, y_4 \in K + \sum_{1 \leqslant i \leqslant 4} K \cdot x_i$ *such that* $K + \sum_{1 \leqslant i \leqslant 4} K \cdot x_i = K + \sum_{1 \leqslant i \leqslant 4} K \cdot y_i$ *and*

$$\sigma(y_j) = \sum_{1 \leqslant i \leqslant 4} a_{ij}y_i \quad \textit{for } 1 \leqslant j \leqslant 4.$$

Note that, if $a = 1$ in Theorem 1.8, we find that $K(x_1, x_2, x_3, x_4)^{\langle\sigma\rangle}$ is rational over $K$ if and only if char $K = 2$, or $\sqrt{-1} \in K$, or $\sqrt{2} \in K$, or $\sqrt{-2} \in K$; and therefore the non-rational examples mentioned at the beginning of this section is just a special case of this conclusion. Finally we remark that, besides Theorem 1.3, there is yet another direction of generalization for Theorem 1.2, which will appear in a forthcoming paper [7]:

**1.10. Theorem.** *Let* $K$ *be any field,* $G$ *any solvable subgroup of* $GL_3(K)$. *Then both* $K(x_1, x_2, x_3)^G$ *and* $K(x_1/x_3, x_2/x_3)^G$ *are rational over* $K$.

It may be interesting to point out that Castelnuovo–Zariski's Theorem for rational algebraic surfaces requires that the base field $K$ is algebraically closed [23] while the rationality of $K(x_1/x_3, x_2/x_3)^G$ in Theorem 1.10 is valid for any $K$, in particular those non-closed fields.

In case $f(T)$ is separable and irreducible, the strategy of proving Theorem 1.2 is to use Galois descent and to reduce the problem to two-dimensional algebraic tori [1]. We use similar techniques to prove the main results of this paper. However, in this situation, not all three-dimensional algebraic tori are rational. Thanks are due to Kunyavskii who provided a birational classification of all three-dimensional algebraic tori [10]. In this sense we may regard the birational class of the three-dimensional algebraic torus associated to $K(\mathbb{P}(V))^{\langle\sigma\rangle}$ is the obstruction to the rationality of $K(V)^{\langle\sigma\rangle}$ and $K(\mathbb{P}(V))^{\langle\sigma\rangle}$. If $f(T)$ is inseparable or reducible, we will resort to other methods to solve the rationality problem; see Theorems 2.7 and 2.8 for details. In the formulation of Theorems 1.3–1.6, it is important to determine the Galois group of the quartic polynomial $f(T)$. We would mention that the paper [9] provides some handy criteria to determine the Galois group of a quartic polynomial. Finally, we would remark that Saltman has developed a method to determine whether an algebraic torus is retract rational [16, Theorem 3.14; 17, Section 2]; this method is particularly effective if we try to prove an algebraic torus is not stably rational.

We shall organize this paper as follows. In Section 2 the rationality of $K(V)^{\langle\sigma\rangle}$ and $K(\mathbb{P}(V))^{\langle\sigma\rangle}$ will be established if $f(T)$ is reducible or inseparable. The proof of Theorem 1.3 will be finished in Section 3. We shall prove Theorem 1.4 in Section 4. The proof of Theorem 1.5 will be presented in Section 5. Section 6 will contain the proof of Theorems 1.6–1.8. In the last section, Section 7, we shall prove Theorem 1.9 together with another application.

**Standing notations.** In this paper, $K$ will always stand for a field; it is unnecessary to assume *char* $K=0$ or $K$ is algebraically closed. If $V$ is a vector space over $K$, $K(V)$ and $K(\mathbb{P}(V))$ will denote the function fields of $V$ and $\mathbb{P}(V)$ respectively; taking a basis $x_1,\dots,x_n$ for $V^*$ (the dual space of $V$), $K(V)$ (resp. $K(\mathbb{P}(V))$) is nothing but the field $K(x_1,\dots,x_n)$ (resp. $K(x_1/x_n, x_2/x_n,\dots,x_{n-1}/x_n)$). We shall denote by $K(x_1,\dots,x_n)$ the rational function field of $n$ variables over $K$, i.e. $x_1,x_2,\dots,x_n$ are algebraically independent over $K$. ($K(x,y)$ is defined similarly.)

If $\sigma\in GL(V)$, then $\sigma$ acts on $K(V)$ and $K(\mathbb{P}(V))$ in a natural way; thus we may consider the fixed subfields $K(V)^{\langle\sigma\rangle}$ and $K(\mathbb{P}(V))^{\langle\sigma\rangle}$ of $K(V)$ and $K(\mathbb{P}(V))$, respectively. In particular, If $\sigma=(a_{ij})_{1\leqslant i,j\leqslant n}\in GL_n(K)$, then $\sigma$ acts on $K(x_1,\dots,x_n)$ by $\sigma(x_j)=\sum_i a_{ij}x_i$ for $1\leqslant j\leqslant n$.

A field extension $L$ of $K$ is called rational over $K$ if it is purely transcendental over $K$; $L$ is called stably rational over $K$ if $L(y_1,\dots,y_m)$ is rational over $K$ for some $y_1,\dots,y_m$ which are algebraically independent over $L$.

If $\varepsilon$ is an element of a group $G, ord(\varepsilon)$ will denote the order of $\varepsilon$; for $g_1,g_2,\dots,g_m\in G$, $\langle g_1,g_2,\dots,g_m\rangle$ denotes the subgroup generated by $g_1,g_2,\dots,g_m$. If $G$ is the Galois group of a quartic equation $f(T)=0$ over a field $K$ and $\alpha_1,\alpha_2,\alpha_3,\alpha_4$ are the four roots of $f(T)=0$, then we may regard $G$ as a subgroup of $S_4$, the symmetric group on $\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\}$; for an element $\tau\in G$, the expression $\tau=(\alpha_1,\alpha_2)(\alpha_3,\alpha_4)$ means that $\tau(\alpha_1)=\alpha_2, \tau(\alpha_2)=\alpha_1, \tau(\alpha_3)=\alpha_4, \tau(\alpha_4)=\alpha_3$.

## 2. The reducible and inseparable cases

We recall several results which will be used repeatedly throughout this paper.

**2.1. Theorem** (Hajja and Kang [6, Theorem 1]). *Let $G$ be a finite group acting on $L(x_1, \ldots, x_n)$, the rational function field of $n$ variables over a field $L$. Suppose that*

(i) *for any $\sigma \in G, \sigma(L) \subset L$;*
(ii) *the restriction of the actions of $G$ to $L$ is faithful;*
(iii) *for any $\sigma \in G$,*

$$\begin{pmatrix} \sigma(x_1) \\ \vdots \\ \sigma(x_n) \end{pmatrix} = A(\sigma) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + B(\sigma),$$

*where $A(\sigma) \in GL_n(L)$ and $B(\sigma)$ is an $n \times 1$ matrix over $L$.*

*Then there exist $z_1, \ldots, z_n \in L(x_1, \ldots, x_n)$ such that $L(x_1, \ldots, x_n) = L(z_1, \ldots, z_n)$ with $\sigma(z_i) = z_i$ for any $\sigma \in G$, any $1 \leqslant i \leqslant n$.*

**2.2. Theorem** (Ahmad et al. [1, Theorem 3.1]). *Let $G$ be a group acting on $L(x)$, the rational function field of one variable over a field $L$. Suppose that, for any $\sigma \in G, \sigma(L) \subset L$ and $\sigma(x) = a_\sigma \cdot x + b_\sigma$ for some $a_\sigma, b_\sigma \in L$ with $a_\sigma \neq 0$. Then $L(x)^G = L^G$ or $L^G(f(x))$ where $f(x) \in L[x]$ is of positive degree.*

**2.3. Theorem** (Ahmad et al. [1, Proposition 3.2]). *Let $K$ be any field, $V$ a finite-dimensional vector space over $K$ and $G$ any subgroup of $GL(V)$. If $K(\mathbb{P}(V))^G$ is rational over $K$, then $K(V)^G$ is rational over $K$ also.*

**2.4. Theorem.** *Let $K$ be any field, $\sigma$ be a $K$-automorphism of $K(x, y)$ defined by $\sigma(x) = a/x$, $\sigma(y) = b/y$ where $a \in K \backslash \{0\}$, $b = c(x + (a/x)) + d$ such that $c, d \in K$ and at least one of $c$ and $d$ is non-zero. If $u$ and $v$ are defined by*

$$u = \frac{x - (a/x)}{xy - (ab/xy)}, \quad v = \frac{y - (b/y)}{xy - (ab/xy)}, \tag{2.1}$$

*then $K(x, y)^{\langle \sigma \rangle} = K(u, v)$ and*

$$x + (a/x) = (-bu^2 + av^2 + 1)/v, \quad y + (b/y) = (bu^2 - av^2 + 1)/u,$$

$$xy + (ab/xy) = (-bu^2 - av^2 + 1)/uv. \tag{2.2}$$

**Proof.** Define $u$ and $v$ by (2.1). Then it is straightforward to verify that (2.2) is valid no matter what $a$ and $b$ may be.

We shall prove that $K(x,y)^{\langle\sigma\rangle}=K(u,v)$ if $a$ and $b$ are required as in the statement of the theorem.

From (2.2), we get

$$(x+(a/x))v=\{-c(x+(a/x))-d\}u^2+av^2+1,$$

$$(x^2+a)v=-c(x^2+a)u^2+x(du^2+av^2+1).$$

Thus $[K(x,u,v)\colon K(u,v)]\leqslant 2$.

Again using (2.2) we find that

$$y+(b/y)=A, \tag{2.3}$$

$$xy+(ab/xy)=B, \tag{2.4}$$

where $A=(bu^2-av^2+1)/u$ and $B=(-bu^2-av^2+1)/uv$. Regard (2.3) and (2.4) as linear equations with coefficients in $K(x,u,v)$ and in unknowns $y$ and $1/y$. Thus solve (2.3) and (2.4) within the field $K(x,u,v)$. It follows $y\in K(x,u,v)$. Hence $K(x,y)=K(x,u,v)$.

Since $K(u,v)\subset K(x,y)^{\langle\sigma\rangle}\subset K(x,y)=K(x,u,v)$ and $[K(x,u,v):K(u,v)]\leqslant 2=[K(x,y):K(x,y)^{\langle\sigma\rangle}]$, it follows that $K(u,v)=K(x,y)^{\langle\sigma\rangle}$. $\square$

**Remark.** The case when $a,b\in K\backslash\{0\}$ in Theorem 2.4 was proved by Giles and McQuillan [2] without exhibiting the generators of $K(x,y)^{\langle\sigma\rangle}$; the generators $u$ and $v$ in (2.1) and the formula of $x+(a/x),\ldots$ in (2.2), valid only for the case $a,b\in K\backslash\{0\}$, were proved in [5, (2.7) Lemma].

We shall use results of the birational classification of algebraic tori due to Voskresenskii [21] and Kunyavskii [10]. We refer to the monograph of Voskresenskii [22] for general notions of algebraic tori. Here we just give an algebraic formulation of the function field of an algebraic torus defined over a field $K$: Let $L$ be a finite Galois extension of $K$ with Galois group $G$, $L(x_1,\ldots,x_n)$ be the rational function field of $n$ variable over $L$, and $\rho: G\to GL_n(\mathbb{Z})$ be a group homomorphism. Then the action of $G$ on $L$ can be extended to $L(x_1,\ldots,x_n)$ by

$$\tau(x_j)=\prod_{i=1}^{n}x_i^{n_{ij}},$$

where $\rho(\tau)=(n_{ij})\in GL_n(\mathbb{Z})$ for any $\tau\in G$. The fixed field $L(x_1,\ldots,x_n)^G$ is the function field of some $n$-dimensional algebraic torus defined over $K$ and split by $L$.

**2.5. Theorem** (Voskresenskii [21]). *All two-dimensional algebraic tori are rational.*

**Remark.** The birational classification of three-dimensional algebraic tori is proved by Kunyavskii [10]. See [10, Theorem 1] for the details.

From now on till the end of this section, $V$ is assumed to be a four-dimensional vector space over $K$, $\sigma \in GL(V)$ and $f(T) \in K[T]$ the characteristic polynomial of $\sigma$. In order to establish the rationality of $K(V)^{\langle\sigma\rangle}$ and $K(\mathbb{P}(V))^{\langle\sigma\rangle}$, it suffices to establish the rationality of $K(\mathbb{P}(V))^{\langle\sigma\rangle}$ because of Theorem 2.3.

**2.6. Lemma.** *If $K$ is a field with char $K = 2$ and $f(T) = T^4 + a \in K[T]$, then both $K(V)^{\langle\sigma\rangle}$ and $K(\mathbb{P}(V))^{\langle\sigma\rangle}$ are rational over $K$.*

**Proof.** *Case* 1: *$f(T)$ is the minimal polynomial of $\sigma$.* By the rational canonical form of $\sigma$, we can find a basis $v_1, v_2, v_3, v_4$ of $V^*$ such that

$$\sigma : v_1 \mapsto v_2 \mapsto v_3 \mapsto v_4 \mapsto av_1.$$

Define

$$x_1 = v_3/v_1, \quad x_2 = v_4/v_2, \quad x_3 = v_2/v_1, \quad u = x_2/x_1.$$

Then $K(\mathbb{P}(V)) = K(x_1, x_2, x_3)$ and

$$\sigma : x_1 \mapsto x_2 \mapsto a/x_1, \quad x_3 \mapsto x_1/x_3, \quad u \mapsto a/(x_2^2 u),$$

$$\sigma^2 : x_1 \mapsto a/x_1, \quad x_2 \mapsto a/x_2, \quad x_3 \mapsto ux_3, \quad u \mapsto 1/u.$$

By Theorem 2.4, $K(x_1, x_2, x_3)^{\langle\sigma^2\rangle} = K(x_1, x_2, (1+u)x_3)^{\langle\sigma^2\rangle} = K(x_1, x_2)^{\langle\sigma^2\rangle}((1+u)x_3) = K(y_1, y_2, (1+u)x_3)$ where

$$y_1 = \frac{x_1 - (a/x_1)}{x_1x_2 - (a^2/x_1x_2)}, \quad y_2 = \frac{x_2 - (a/x_2)}{x_1x_2 - (a^2/x_1x_2)}.$$

Define

$$z_1 = a(y_1 + y_2), \quad z_2 = y_1/(y_1 + y_2), \quad z_3 = z_2(1+u)x_3.$$

Then $K(y_1, y_2, (1+u)x_3) = K(z_1, z_2, z_3)$ and

$$\sigma : z_1 \mapsto a/z_1, \quad z_2 \mapsto z_2 + 1, \quad z_3 \mapsto (z_1 + (a/z_1))/z_3.$$

Now $K(z_1, z_2, z_3) = K(z_1, z_3, z)$ for some $z$ with $\sigma(z) = z$ by Theorem 2.1. Thus $K(z_1, z_2, z_3)^{\langle\sigma\rangle} = K(z_1, z_3)^{\langle\sigma\rangle}(z)$ is rational over $K$ by Theorem 2.4.

*Case* 2: *$f(T)$ is not the minimal polynomial of $\sigma$.* Thus $f(T)$ is reducible. Either $f(T)$ has a linear factor in $K[T]$ or $f(T) = (T^2 + b)^2$ for some $b \in K$ with $b^2 = a$.

In the first situation, $K(\mathbb{P}(V))^{\langle\sigma\rangle}$ is rational by Case 1 of the proof of the following Theorem 2.7 (under a more general situation). Thus, it remains to consider the latter situation. In this situation, we may assume that $T^2+b$ is irreducible and is the minimal polynomial of $\sigma$.

Thus we may find a basis $v_1, v_2, w_1, w_2$ of $V^*$ such that

$$\sigma : v_1 \mapsto v_2 \mapsto bv_1, \quad w_1 \mapsto w_2 \mapsto bw_1.$$

Define

$$x = v_2/v_1, \quad y = w_1/v_1, \quad z = w_2/v_2.$$

Then $K(\mathbb{P}(V)) = K(x, y, z)$ and

$$\sigma : x \mapsto b/x, y \mapsto z \mapsto y.$$

Since $K(x)^{\langle\sigma\rangle}$ is rational by Lüroth's Theorem, it follows that $K(x, y, z)^{\langle\sigma\rangle}$ is rational by Theorem 2.1. $\square$

**2.7. Theorem.** *If $K$ is any field and $f(T)$ is a reducible polynomial in $K[T]$, then $K(\mathbb{P}(V))^{\langle\sigma\rangle}$ is rational over $K$.*

**Proof.** *Case* 1: *$f(T) = (T - \alpha)g(T)$ for some $\alpha \in K$.* Then $V^*$ has an eigenvector with eigenvalue $\alpha$. Thus we may find a basis $v_1, v_2, v_3, v_4$ of $V^*$ such that $\sigma(v_1) = \alpha v_1$. Define

$$x_1 = v_2/v_1, \quad x_2 = v_3/v_1, \quad x_3 = v_4/v_1.$$

Then

$$\sigma(x_j) = \sum_{1 \leqslant i \leqslant 3} a_{ij}x_i + b_i \quad \text{for } 1 \leqslant j \leqslant 3,$$

where $(a_{ij})_{1 \leqslant i,j \leqslant 3} \in GL_3(K)$ and $b_j \in K$. Hence $K(x_1, x_2, x_3)^{\langle\sigma\rangle}$ is rational over $K$ by Theorem 1.2 (2).

*Case* 2: *$f(T) = g_1(T)g_2(T)$ where $g_1(T)$ and $g_2(T)$ are distinct monic irreducible polynomial of degree* 2. By linear algebra, $V^*$ decomposes into *a* direct sum of two invariant two-dimensional subspaces, i.e. there exists a basis $v_1, v_2, v_3, v_4$ of $V^*$ such that $\sigma(v_i) \in K \cdot v_1 + K \cdot v_2$ for $1 \leqslant i \leqslant 2$, and $\sigma(v_j) \in K \cdot v_3 + K \cdot v_4$ for $3 \leqslant j \leqslant 4$. Define

$$x_1 = v_2/v_1, \quad x_2 = v_4/v_3, \quad x_3 = v_3/v_1.$$

Then $K(\mathbb{P}(V)) = K(x_1, x_2, x_3)$ and $\sigma(x_3) = \lambda x_3$ for some $\lambda \in K(x_1, x_2)$. By Theorem 2.2 the rationality of $K(x_1, x_2, x_3)^{\langle\sigma\rangle}$ follows from that of $K(x_1, x_2)^{\langle\sigma\rangle}$. However, $K(x_1, x_2)^{\langle\sigma\rangle}$ is rational over $K$ by Theorem 1.2(3).

*Case* 3: *$f(T) = g(T)^2$, where $g(T)$ is a monic irreducible polynomial.* If $g(T)$ is inseparable, then *char* $K = 2$ and $g(T) = T^2 + b$ for some $b \in K \backslash \{0\}$. Thus $f(T) = T^4 + b^2$. This situation has been treated in Lemma 2.6.

Thus we may assume that $g(T)$ is separable irreducible.

If the minimal polynomial of $\sigma$ is $g(T)$, then $V^*$ decomposes into a direct sum of two invariant two-dimensional subspaces. This situation can be treated as the above Case 2.

Thus, we may assume that $f(T) = g(T)^2$ is the minimal polynomial of $\sigma$ and $g(T)$ is separable irreducible.

Let $g(T) = (T - \alpha)(T - \beta)$ and $L = K(\alpha)$. Let $G = \langle \tau \rangle$ be the Galois group of $L$ over $K$. Then $\tau(\alpha) = \beta$.

Choose a vector $v \in V^*$ such that $v, \sigma(v), \sigma^2(v), \sigma^3(v)$ is a basis of $V^*$.

The action of $\sigma$ on $V^*$ is extended to $V^* \otimes_K L$ by $\sigma(\alpha) = \alpha$, and the action of $\tau$ on $L$ is extended to $V^* \otimes_K L$ by $\tau(v) = v$ for any $v \in V^*$.

In $V^* \otimes_K L$, define

$$v_2 = (\sigma - \beta)^2 v, \quad v_4 = (\sigma - \alpha)^2 v,$$

$$v_1 = (\sigma - \alpha) v_2, \quad v_3 = (\sigma - \beta) v_4.$$

Then

$$\sigma : v_1 \mapsto \alpha v_1, \quad v_2 \mapsto \alpha v_2 + v_1, \quad v_3 \mapsto \beta v_3, \quad v_4 \mapsto \beta v_4 + v_3.$$

Define

$$x_1 = v_2/v_1, \quad x_2 = v_4/v_3, \quad x_3 = v_3/v_1.$$

Then

$$K(\mathbb{P}(V)) = L(\mathbb{P}(V \otimes_K L))^{\langle \tau \rangle} = L(x_1, x_2, x_3)^{\langle \tau \rangle}$$

and

$$\sigma : x_1 \mapsto x_1 + (1/\alpha), \quad x_2 \mapsto x_2 + (1/\beta), \quad x_3 \mapsto \lambda x_3,$$

where $\lambda = \beta/\alpha$.

Note that $\tau(v_2) = \tau(\sigma - \beta)^2(v) = (\sigma - \alpha)^2 \tau(v) = (\sigma - \alpha)^2 v = v_4$, $\tau(v_1) = \tau(\sigma - \alpha) v_2 = (\sigma - \beta)\tau(v_2) = (\sigma - \beta) v_4 = v_3$. We find that

$$\tau : \alpha \leftrightarrow \beta, \quad v_1 \leftrightarrow v_3, \quad v_2 \leftrightarrow v_4, \quad x_1 \leftrightarrow x_2, \quad x_3 \mapsto 1/x_3.$$

If $char\, K = 0$, define $y = (\alpha x_1 - \beta x_2)/(\alpha - \beta)$. Then $\sigma(y) = \tau(y) = y$. Hence $L(x_1, x_2, x_3)^{\langle \sigma \rangle} = L(x_2, x_3)^{\langle \sigma \rangle}(y)$. Using Theorem 2.2 we get $L(x_2, x_3)^{\langle \sigma \rangle} = L(x_3)^{\langle \sigma \rangle} = L(x_3^n)$ or $L$ depending on whether $ord(\lambda) = n$ or $ord(\lambda) = \infty$ in $L \backslash \{0\}$. Now, if $L(x_3)^{\langle \sigma \rangle} = L$, then $K(\mathbb{P}(V))^{\langle \sigma \rangle} = L(x_1, x_2, x_3)^{\langle \tau, \sigma \rangle} = \{L(x_1, x_2, x_3)^{\langle \sigma \rangle}\}^{\langle \tau \rangle} = L^{\langle \tau \rangle} = K$. If $L(x_3)^{\langle \sigma \rangle} = L(x_3^n)$, then $K(\mathbb{P}(V))^{\langle \sigma \rangle} = \{L(x_1, x_2, x_3)^{\langle \sigma \rangle}\}^{\langle \tau \rangle} = L(x_3^n)^{\langle \tau \rangle} = L(z)^{\langle \tau \rangle} = K(z)$ where $z = (\alpha - \beta)\{(1 - x_3^n)/(1 + x_3^n)\}$. In both cases, $K(\mathbb{P}(V))^{\langle \sigma \rangle}$ is rational.

Now consider the case $char\, K = p > 0$.

Suppose that $ord(\lambda) = \infty$ in $L \backslash \{0\}$.

Using Theorem 2.2 again, we have $L(x_1,x_2,x_3)^{\langle\sigma\rangle} = L(x_1,x_2)(x_3)^{\langle\sigma\rangle} = L(x_1,x_2)^{\langle\sigma\rangle}$.

It is easy to verify that $L(x_1,x_2)^{\langle\sigma\rangle} = L(y_1,y_2)$ where

$$y_1 = x_1^p - (1/\alpha^{p-1})x_1, \quad y_2 = \alpha x_1 - \beta x_2. \tag{2.5}$$

Note that

$$\tau(y_2) = -y_2 \quad \text{and} \quad \tau(y_1) = (\alpha/\beta)^p y_1 - (1/\beta^p)(y_2^p - y_2). \tag{2.6}$$

By Theorem 2.1, find $z \in L(y_1,y_2)$ such that $L(y_1,y_2) = L(y_2,z)$ with $\tau(z) = z$. Hence $L(y_1,y_2)^{\langle\tau\rangle} = L(y_2,z)^{\langle\tau\rangle} = L^{\langle\tau\rangle}(y,z) = K(y,z)$ where $y = (\alpha-\beta)y_2$, is rational over $K$.

It remains to solve the case $ord(\lambda) = n$, i.e. $\lambda$ is a primitive $n$th root of unity.

Note that $p \nmid n$; and $p \mid ord(\sigma)$ because $x_1 \mapsto x_1 + (1/\alpha)$ is of order $p$.

Then $L(x_1,x_2,x_3)^{\langle\sigma^p\rangle} = L(x_1,x_2,x_3^n)$. Thus $L(x_1,x_2,x_3)^{\langle\sigma\rangle} = L(x_1,x_2,x_3^n)^{\langle\sigma\rangle} = L(x_1,x_2)^{\langle\sigma\rangle}(x_3^n) = L(y_1,y_2,x_3^n)$ where $y_1$ and $y_2$ are defined by the same formula as in (2.5). The action of $\tau$ on $y_1$ and $y_2$ are the same as (2.6).

$$y_3 = 1/(1+x_3^n).$$

Then $\tau(y_3) = -y_3 + 1$. By Theorem 2.1, find $y_0 \in L(y_1,y_2,y_3)$ such that $L(y_1,y_2,y_3) = L(y_1,y_2,y_0)$ with $\tau(y_0) = y_0$.

Now $K(\mathbb{P}(V))^{\langle\sigma\rangle} = L(\mathbb{P}(V\otimes_K L))^{\langle\tau,\sigma\rangle} = \{L(x_1,x_2,x_3)^{\langle\sigma\rangle}\}^{\langle\tau\rangle} = L(y_1,y_2,x_3^n)^{\langle\tau\rangle} = L(y_1,y_2)^{\langle\tau\rangle}(y_0)$. The rationality of $L(y_1,y_2)^{\langle\tau\rangle}$ follows by the same way as above. Hence the result. $\square$

**2.8. Theorem.** *Let $K$ be a field with $char\, K = 2$ and $f(T) = T^4 + bT^2 + a \in K[T]$. Then both $K(V)^{\langle\sigma\rangle}$ and $K(\mathbb{P}(V))^{\langle\sigma\rangle}$ are rational over $K$.*

**Proof.** The situation when $b = 0$ or $f(T)$ is reducible is treated in Lemma 2.6 and Theorem 2.7. Thus we may assume that $b \neq 0$ and $f(T)$ is irreducible.

Let $T^2 + bT + a = (T-\alpha)(T-\beta)$ and $L = K(\alpha)$. Let $G = \langle\tau\rangle$ be the Galois group of $L$ over $K$. Then $\tau(\alpha) = \beta$.

Choose a vector $v \in V^*$ such that $v, \sigma(v), \sigma^2(v), \sigma^3(v)$ is a basis of $V^*$.

The action of $\sigma$ (resp. $\tau$) on $V^*$ (resp. $L$) can be extended to $V^* \otimes_K L$ by $\sigma(\alpha) = \alpha$ (resp. $\tau(v) = v$ for any $v \in V^*$).

In $V^* \otimes_K L$, define

$$w_1 = \alpha v + \sigma^2(v), \quad w_2 = \alpha\cdot\sigma(v) + \sigma^3(v),$$

$$w_3 = \beta v + \sigma^2(v), \quad w_4 = \beta\cdot\sigma(v) + \sigma^3(v).$$

Then we find that

$$\sigma: w_1 \mapsto w_2 \mapsto \beta w_1, \quad w_3 \mapsto w_4 \mapsto \alpha w_3,$$

$$\tau: w_1 \leftrightarrow w_3, \quad w_2 \leftrightarrow w_4.$$

Define

$$x_1 = w_2/w_1, \quad x_2 = w_4/w_3, \quad x_3 = w_3/w_1.$$

Then

$$\sigma: x_1 \mapsto \beta/x_1, \quad x_2 \mapsto \alpha/x_2, \quad x_3 \mapsto x_2x_3/x_1,$$

$$\sigma^2: x_1 \mapsto x_1, \quad x_2 \mapsto x_2, \quad x_3 \mapsto \lambda x_3,$$

$$\tau: x_1 \mapsto x_2, \quad x_3 \mapsto 1/x_3,$$

where $\lambda = \alpha/\beta$.

We shall compute $K(\mathbb{P}(V))^{\langle\sigma\rangle} = \{L(x_1, x_2, x_3)^{\langle\sigma\rangle}\}^{\langle\tau\rangle}$.

*Case* 1: $ord(\lambda) = \infty$. $L(x_1, x_2, x_3)^{\langle\sigma\rangle} = \{L(x_1, x_2, x_3)^{\langle\sigma^2\rangle}\}^{\langle\sigma\rangle} = L(x_1, x_2)^{\langle\sigma\rangle} = L(y_1, y_2)$ where $y_1, y_2$ are defined by

$$y_1 = \frac{x_1 - (\beta/x_1)}{x_1x_2 - (\alpha\beta/x_1x_2)}, \qquad y_2 = \frac{x_2 - (\alpha/x_2)}{x_1x_2 - (\alpha\beta/x_1x_2)}. \tag{2.7}$$

Note that $\tau(y_1) = y_2$ and $\tau(y_2) = y_1$. It is clear that

$$\begin{aligned} L(y_1, y_2)^{\langle\tau\rangle} &= L(y_1 + y_2, \{y_1/(y_1 + y_2)\} + (\alpha/b))^{\langle\tau\rangle} \\ &= K(y_1 + y_2, \{y_1/(y_1 + y_2)\} + (\alpha/b)) \end{aligned}$$

is rational over $K$.

*Case* 2: $ord(\lambda) = n$. Note that $2 \nmid n$ because $char\, K = 2$.

$L(x_1, x_2, x_3)^{\langle\sigma\rangle} = \{L(x_1, x_2, x_3)^{\langle\sigma^2\rangle}\}^{\langle\sigma\rangle} = L(x_1, x_2, x_3^n)^{\langle\sigma\rangle} = L(x_1, x_2)^{\langle\sigma\rangle}(y_3)$ where $y_3 = (1 + u^n)x_3^n$ with $u = x_2/x_1$. Note that $\tau(y_3) = (u^n + u^{-n})/y_3$.

Define $w = u + (\lambda/u) \in L(x_1, x_2)^{\langle\sigma\rangle}$. From the binomial expansion of $w^n = (u + (\lambda/u))^n$, $w^{n-2} = (u + (\lambda/u))^{n-2}, \ldots$, it is easy to find that

$$u^n + u^{-n} = w^n + c_1\lambda w^{n-2} + c_2\lambda^2 w^{n-4} + \cdots + c_m\lambda^m w,$$

where $n = 2m + 1$ and $c_1, c_2, \ldots, c_m$ are either 0 or 1. Since $\lambda$ is in the finite field $\mathbb{F}_2(\lambda)$, it follows that $\lambda = \varepsilon^2$ for some $\varepsilon \in \mathbb{F}_2(\lambda)\backslash\{0\}$; and therefore $u^n + u^{-n} = w\theta^2$ for some

$\theta \in L(x_1, x_2)^{\langle\sigma\rangle}$. Since $\tau(u^n + u^{-n}) = u^n + u^{-n}$ and $\tau(w) = \lambda^{-1}w$, it follows that $\tau(\theta) = \varepsilon\theta$.

Define $z_1, z_2, z_3$ by

$$z_1 = \frac{u - (\lambda/u)}{ux_1 - (\lambda\beta/ux_1)}, \quad z_2 = \frac{x_1 - (\beta/x_1)}{ux_1 - (\lambda\beta/ux_1)}, \quad z_3 = y_3/\theta. \tag{2.8}$$

Then $L(x_1, x_2, x_3)^{\langle\sigma\rangle} = L(z_1, z_2, z_3)$ by Theorem 2.4. Moreover,

$$\tau : z_1 \mapsto \lambda^{-1}z_1/z_2, \quad z_2 \mapsto 1/z_2, \quad z_3 \mapsto \varepsilon^{-1}w/z_3.$$

Define $t_1, t_2, t_3$ by

$$t_1 = (1/(1+z_2)) + (\alpha/b), \quad t_2 = \varepsilon^{-1}z_1/(1+z_2),$$

$$t_3 = (t_1^2 + t_1 + (a/b^2))z_3.$$

By substituting the formula $u + (\lambda/u)$ in (2.2) of Theorem 2.4, then $L(z_1, z_2, z_3) = L(t_1, t_2, t_3)$ and $\tau(t_1) = t_1$, $\tau(t_2) = t_2$, $\tau(t_3) = A/t_3$ where

$$A = \{t_1^2 + t_1 + (a/b^2)\}\{(\varepsilon b + \varepsilon\alpha)t_2^2 + (\varepsilon + \varepsilon^{-1})t_1^2 + (\varepsilon + \varepsilon b^{-1}\alpha)\}.$$

Note that $\varepsilon b + \varepsilon\alpha, \varepsilon + \varepsilon^{-1}$, $\varepsilon + \varepsilon b^{-1}\alpha$ are fixed by $\tau$ and therefore belong to $K$.

We claim that $L(t_1, t_2, t_3)^{\langle\tau\rangle} = K(t_1, t_2, t_4, t_5)$ with the relation

$$t_4^2 + (b/a)t_4t_5 + (1/a)t_5^2 = b^2A/a. \tag{2.9}$$

In fact, letting $t_4 = t_3 + (A/t_3)$ and $t_5 = \alpha t_3 + (aA/\alpha t_3)$. The verification of the above claim will become straightforward.

We shall simplify relation (2.9):

$$(at_4/b)^2 + (at_4/b)t_5 + (a/b)^2t_5^2 = aA. \tag{2.10}$$

Multiply by $t_1^2 + t_1 + (a/b^2)$ both sides of (2.10). We get

$$\begin{aligned}&\{(at_4/b)^2 + (at_4/b)t_5 + (a/b^2)t_5^2\}\{t_1^2 + t_1 + (a/b^2)\}\\ &\quad = \{t_1^2 + t_1 + (a/b^2)\}^2\{(\varepsilon ab + \varepsilon a\alpha)t_2^2 + a(\varepsilon + \varepsilon^{-1})t_1^2 + (\varepsilon a + \varepsilon ab^{-1}\alpha)\}.\end{aligned}$$

The left-hand side of the above identity is

$$\begin{aligned}&((a/b)t_1t_4 + (a/b^2)t_5)^2 + ((a/b)t_1t_4 + (a/b^2)t_5)((a/b)t_4 + t_1t_5 + t_5)\\ &\quad + (a/b)^2((a/b)t_4 + t_1t_5 + t_5)^2.\end{aligned}$$

Since $\varepsilon \in \mathbb{F}_2(\lambda)$, which is a finite field, it follows that $\varepsilon = \rho^2$ for some $\rho \in \mathbb{F}_2(\lambda)\backslash\{0\}$. Thus $\varepsilon + \varepsilon^{-1} = \rho^{-2}(\varepsilon + 1)^2$. Note that $\rho^{-1}(\varepsilon + 1) \in K$.

Define $p, q, r$ by

$$p = ((a/b)t_1t_4 + (a/b^2)t_5)/(t_1^2 + t_1 + (a/b^2)),$$

$$q = ((a/b)t_4 + t_1t_5 + t_5)/(t_1^2 + t_1 + (a/b^2)),$$

$$r = \rho^{-1}(\varepsilon + 1)t_1.$$

Thus $L(t_1, t_2, t_3)^{\langle\tau\rangle} = K(t_2, p, q, r)$ with the relation

$$p^2 + pq + (a/b^2)q^2 = (\varepsilon ab + \varepsilon a\alpha)t_2^2 + ar^2 + (\varepsilon a + \varepsilon ab^{-1}\alpha). \tag{2.11}$$

The above relation (2.11) can be written as

$$p^2 + pq + a((q/b) + r)^2 = (\varepsilon ab + \varepsilon a\alpha)t_2^2 + (\varepsilon a + \varepsilon ab^{-1}\alpha). \tag{2.12}$$

It follows that $q \in K(t_2, p, (q/b) + r)$ by (2.12). Hence $K(\mathbb{P}(V))^{\langle\sigma\rangle} = L(t_1, t_2, t_3)^{\langle\tau\rangle} = K(t_2, p, (q/b) + r)$ is rational over $K$. $\square$

**2.9. Theorem.** *Let $K$ be any field. If $f(T)$ is inseparable, then $K(\mathbb{P}(V))^{\langle\sigma\rangle}$ is rational over $K$.*

**Proof.** If $f(T)$ is inseparable, then *char* $K = 2$ or 3. The case *char* $K = 2$ has been solved by Theorem 2.8. If *char* $K = 3$, then $f(T) = (T - b)(T^3 - a)$ for some $a, b \in K$. Thus $f(T)$ is reducible and we may apply Theorem 2.7. $\square$

## 3. The proof of Theorem 1.3

In this section except in 3.4, we assume the characteristic polynomial $f(T)$ is separable irreducible in $K[T]$.

Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be the roots of $f(T) = 0$, $L = K(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ and $G$ be the Galois group. Since elements of $G$ permute $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, we may regard $G$ as a subgroup of $S_4$ by: for any $\tau \in G$,

$$\tau(i) = j \quad \text{if and only if } \tau(\alpha_i) = \alpha_j.$$

Note that, as a subgroup of $S_4$, $G$ is one of $S_4$, $A_4$, or is conjugate of $D_4$, $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$ ($\mathbb{Z}_n$ stands for the cyclic group of order $n$).

We shall write the four roots $\alpha_1$, $\alpha_2$, $\alpha_3$, $\alpha_4$ of $f(T) = 0$ by $\alpha$, $\alpha\beta_1$, $\alpha\beta_2$, $\alpha\beta_3$ by assigning $\alpha$ to be any root $\alpha_j$ $(1 \leqslant j \leqslant 4)$. Define $N = K(\beta_1, \beta_2, \beta_3)$.

We shall indicate the main idea of our proof of Theorems 1.3–1.5 in the case when $f(T)$ is separable irreducible.

The group action of $\sigma$ on $V^*$ is extended to $V^* \otimes_K L$ by $\sigma(\alpha) = \alpha$ for any $\alpha \in L$. The group action of $G$ on $L$ is extended $V^* \otimes_K L$ by $\tau(v) = v$ for any $\tau \in G$, any $v \in V^*$.

Choose a vector $v \in V^*$ such that $v, \sigma(v), \sigma^2(v), \sigma^3(v)$ is a basis of $V^*$. Define $v_1, v_2, v_3, v_4 \in V^* \otimes_K L$ by

$$v_i := (\sigma - \alpha_1) \cdots (\widehat{\sigma - \alpha_i}) \cdots (\sigma - \alpha_4)(v).$$

Then $\sigma(v_i) = \alpha_i v_i$ and, for any $\tau \in G$, $\tau(v_i) = \tau(\sigma - \alpha_1) \cdots (\widehat{\sigma - \alpha_i}) \cdots (\sigma - \alpha_4)(v) = (\sigma - \alpha_{\tau(1)}) \cdots (\widehat{\sigma - \alpha_{\tau(i)}}) \cdots (\sigma - \alpha_{\tau(4)})(\tau(v)) = v_{\tau(i)}$.

Define

$$x_i = v_i / v_1, \quad \beta_i = \alpha_i / \alpha_1 \quad \text{for } 1 \leqslant i \leqslant 3.$$

Then

$$K(\mathbb{P}(V))^{\langle \sigma \rangle} = \{L(\mathbb{P}(V \bigoplus_K L))^G\}^{\langle \sigma \rangle} = \{L(x_1, x_2, x_3)^{\langle \sigma \rangle}\}^G,$$

and $\sigma(x_i) = \beta_i x_i$.

Let $\langle x_1, x_2, x_3 \rangle := \{x_1^{n_1} x_2^{n_2} x_3^{n_3} \in L(x_1, x_2, x_3) \backslash \{0\}\colon n_1, n_2, n_3 \in \mathbb{Z}\}$ and define the $G$-equivariant map $\Phi$ by

$$\begin{array}{rcl} \Phi : \langle x_1, x_2, x_3 \rangle & \to & L^\times \\ x_1^{n_1} x_2^{n_2} x_3^{n_3} & \mapsto & \sigma(x_1^{n_1} x_2^{n_2} x_3^{n_3}) / (x_1^{n_1} x_2^{n_2} x_3^{n_3}). \end{array}$$

Since $\langle x_1, x_2, x_3 \rangle$ is isomorphic to a free abelian group of rank three, it follows that $Ker\,\Phi$ is a free abelian group of rank $\leqslant 3$ with $G$ actions, i.e. $Ker\,\Phi = \langle M_1, \ldots, M_k \rangle$ for some monomials $M_1, \ldots, M_k$ with $k = rank(Ker\,\Phi)$. Now $L(x_1, x_2, x_3)^{\langle \sigma \rangle} = L(M_1, \ldots, M_k)$ and $L(M_1, \ldots, M_k)^G$ is the function field of some algebraic turns over $K$ split by $L$. Thus, we can apply results of the birational classification of algebraic tori due to Voskresenskii and Kunyavskii (Theorem 2.5 and [10]).

**3.1. Lemma.** *If $\langle \beta_1, \beta_2, \beta_3 \rangle$ is an infinite subgroup of $L \backslash \{0\}$, then $K(\mathbb{P}(V))^{\langle \sigma \rangle}$ is rational over $K$.*

**Proof.** From the above discussion, $Ker(\Phi)$ is a free abelian group of rank $\leqslant 2$. Since every two-dimensional algebraic torus is rational by Theorem 2.5 (and it is not difficult to show that the same conclusion is valid for every one-dimensional algebraic torus), it follows that $K(\mathbb{P}(V))^{\langle \sigma \rangle} = L(M_1, \ldots, M_k)^G$ is rational over $K$. $\square$

**3.2. Lemma.** *If $K = N$, then $G \simeq \mathbb{Z}_4$ and $K(\mathbb{P}(V))^{\langle \sigma \rangle}$ is rational over $K$.*

**Proof.** Since $L = K(\alpha, \beta_1, \beta_2, \beta_3) = N(\alpha) = K(\alpha)$, it follows that $[L : K] = 4$ and $G \simeq \mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.

If $G \simeq \mathbb{Z}_4$, then $K(\mathbb{P}(V))^{\langle\sigma\rangle}$ is rational over $K$ by Kunyavskii [10, Theorem 1]. We shall show that $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ will lead to a contradiction.

Suppose $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. Choose $\tau_1 \in G$ such that $\tau_1 = (\alpha, \alpha\beta_1)(\alpha\beta_2, \alpha\beta_3)$. Since $\beta_i \in N = K$, $\beta_i$ is fixed by $G$. It follows that $\alpha\beta_3 = \tau_1(\alpha\beta_2) = \tau_1(\alpha)\tau(\beta_2) = \alpha\beta_1 \cdot \beta_2$. Hence $\beta_3 = \beta_1\beta_2$.

Now choose $\tau_2 \in G$ with $\tau_2 = (\alpha, \alpha\beta_1\beta_2)(\alpha\beta_1, \alpha\beta_2)$. We get $\alpha\beta_1\beta_2 = \tau(\alpha) = \tau(\alpha\beta_1 \cdot \beta_1^{-1}) = \tau(\alpha\beta_1)\tau(\beta_1^{-1}) = \alpha\beta_2 \cdot \beta_1^{-1}$. Hence $\beta_1^2 = 1$. By similar arguments, we get $\beta_1^2 = 1$ also.

Hence $\beta_1 = \pm 1$, $\beta_2 = \pm 1$. Thus $f(T)$ cannot be a separable polynomial. A contradiction. $\square$

**3.3. Lemma.** *If $K \neq N$, then either $K(\mathbb{P}(V))^{\langle\sigma\rangle}$ is rational or $G \simeq D_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.*

**Proof.** For any $\tau \in G$, $\tau(\beta_i) = \tau(\alpha\beta_i/\alpha) = \tau(\alpha\beta_i)/\tau(\alpha) = (\alpha\beta_j)/(\alpha\beta_l) = \beta_j/\beta_l$ for some $j, l$. Thus $N = K(\beta_1, \beta_2, \beta_3)$ is normal over $K$. Because of Lemma 3.1 it suffices to consider the case $ord(\beta_i) < \infty$ for $1 \leqslant i \leqslant 3$. It follows that $N$ is an abelian extension of $K$.

If $\alpha \in N$, then $G$ is abelian. Hence $G \simeq \mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$. If $G \simeq \mathbb{Z}_4$, then $K(\mathbb{P}(V))^{\langle\sigma\rangle}$ is rational by Kunyavskii [10, Theorem 1].

If $\alpha \notin N$, then $L = N(\alpha)$. Thus $[N(\alpha) : N] = 2$ or 4. It follows that $G$ has a non-trivial normal subgroup $H$ such that $|H| = 2$ or 4, and $G/H$ is a non-trivial abelian group. Thus $G = S_4$ is impossible. If $G = A_4$, the $H$ should be the Klein four group in $A_4$ and $N = L^H$. Choose $\tau_1 \in H$ such that $\tau_1 = (\alpha, \alpha\beta_1)(\alpha\beta_2, \alpha\beta_3)$. We get $\beta_1 = \tau_1(\beta_1) = \tau_1(\alpha\beta_1/\alpha) = \tau_1(\alpha\beta_1)/\tau_1(\alpha) = \alpha/(\alpha\beta_1) = \beta_1^{-1}$. Hence $\beta_1^2 = 1$ and $\beta_1 = -1$. Similarly, take $\tau_2 = (\alpha, \alpha\beta_2)(\alpha\beta_1, \alpha\beta_3) \in H$; we will get $\beta_2 = -1$. Thus $f(T)$ would not be separable. A contradiction.

If follows that $G \simeq D_4$, $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$. The case $G \simeq \mathbb{Z}_4$ will ensure that $K(\mathbb{P}(V))^{\langle\sigma\rangle}$ is rational as before. $\square$

**3.4. Proof of Theorem 1.3.** Theorems 2.7 and 2.9 take care of situation (ii). Situation (iii) is covered by Lemma 3.1. By Lemmas 3.2 and 3.3 situation (iv) is ok. Because of (ii)–(iv), it follows that the remaining unsettled situation is the case: $f(T)$ is separable irreducible, $\langle \beta_1, \beta_2, \beta_3 \rangle$ is a finite group and the Galois group $G \simeq D_4$, or $\mathbb{Z}_2 \times \mathbb{Z}_2$. We shall show that it is necessary that $char\, K \neq 2$ in this situation (see Lemmas 4.1(i) and 5.1). Thus, if $char\, K = 2$, $K(\mathbb{P}(V))^{\langle\sigma\rangle}$ is rational over $K$, which is just situation (i). $\square$

## 4. Proof of Theorem 1.4

In this section we shall adopt the same notations as in Section 3. Throughout this section we shall assume that $f(T)$ is a separable irreducible polynomial in $K[T]$,

$\langle \beta_1, \beta_2, \beta_3 \rangle$ is a finite subgroup of $L \backslash \{0\}$ and the Galois group $G$ is equal to $D_4$ where $D_4 = \{id, (1234), (13)(24), (1432), (13), (24), (12)(34), (14)(23)\}$.

**4.1. Lemma.** (i) *$K \neq N$ and $N \neq L$, $char\, K \neq 2$, $\{\beta_1, \beta_2, \beta_3\} = \{-1, \beta, -\beta\}$.* (ii) *$(1234) = (\alpha, \alpha\beta, -\alpha, -\alpha\beta)$ or $(\alpha, -\alpha\beta, -\alpha, \alpha\beta)$; moreover, $(13)(24)$ leaves every element in $N$ fixed.*

**Proof.** By Lemma 3.2, $K \neq N$. Since $N$ is an abelian extension of $K$, while $G$ is not abelian, hence $N \neq L$.

Let $H$ be the Galois group of $L$ over $N$. Then $H \neq \{id\}$, $H \lhd G$ and $G/H$ is a non-trivial abelian group. Thus the only candidates for $H$ are: $\langle (1234) \rangle$, $\langle (13)(24), (12)(34) \rangle$, $\langle (13)(24), (13) \rangle$, $\langle (13)(24) \rangle$. In any case, $\tau_1 = (13)(24)$ belongs to $H$. (It can be shown that the situation $H = \langle (13)(24), (12)(34) \rangle$ or $\langle (13)(24), (13) \rangle$ is impossible. But we do not need this fact.)

Write $\tau_1 = (\alpha, \alpha\beta_1)(\alpha\beta_2, \alpha\beta_3)$ by indexing $\alpha_1 = \alpha$, $\alpha_2 = \alpha\beta_2$, $\alpha_3 = \alpha\beta_1$, $\alpha_4 = \alpha\beta_3$. Then $\alpha\beta_3 = \tau_1(\alpha\beta_2) = \tau_1(\alpha)\tau_2(\beta_2) = \alpha\beta_1 \cdot \beta_2$. Thus $\beta_3 = \beta_1\beta_2$. On the other hand, $\beta_1 = \tau_1(\beta_1) = \tau_1(\alpha\beta_1/\alpha_1) = \tau_1(\alpha\beta_1)/\tau_1(\alpha) = \alpha/(\alpha\beta_1) = \beta_1^{-1}$; hence $\beta_1 = -1$ and $char\, K \neq 2$ because $f(T)$ is separable and $\beta_1 = 1$ will be impossible. In conclusion, $\{\beta_1, \beta_2, \beta_3\} = \{-1, \beta, -\beta\}$ and $(13)(24) = (\alpha, -\alpha)(\alpha\beta, -\alpha\beta)$.

Let $\tau = (1234)$. Then $\tau^2 = (13)(24) = (\alpha, -\alpha)(\alpha\beta, -\alpha\beta)$. Thus $\tau = (\alpha, \alpha\beta, -\alpha, -\alpha\beta)$ or $(\alpha, -\alpha\beta, -\alpha, \alpha\beta)$. $\square$

**4.2. Lemma.** (i) $4 \mid ord(\beta)$.

(ii) *If $\beta^2 \neq -1$, then $f(T) = T^4 - aT^2 + (a^2/b) \in K[T]$ where $a, b \neq 0$ and $a = \alpha^2(1 + \beta^2)$, $b = (\beta + \beta^{-1})^2$. If $\beta^2 = -1$, then $f(T) = T^4 + a \in K[T]$ where $a = -\alpha^4$.*

**Proof.** By Lemma 4.1, write $f(T) = (T - \alpha)(T + \alpha)(T - \alpha\beta)(T + \alpha\beta)$. We will obtain (ii).

By Lemma 4.1, take $\tau = (\alpha, \alpha\beta, -\alpha, -\alpha\beta)$. (The case $\tau = (\alpha, -\alpha\beta, -\alpha, \alpha\beta)$ will lead to the same result.) Then $-\alpha = \tau(\alpha\beta) = \tau(\alpha)\tau(\beta) = \alpha\beta \cdot \tau(\beta)$. Hence $\tau(\beta) = -\beta^{-1}$. Thus $-\beta^{-1}$ is a conjugate of $\beta$ in $L$.

Since $\beta$ is a root of unity, all of its conjugates are of the form $\beta^j$ for some suitable $j$. It follows that $-\beta^{-1} = \beta^j$. Thus $-1 \in \langle \beta \rangle$. Denote $n = ord(\beta)$. Then $n$ is even. Write $n = 2m$. We shall show that $m$ is even.

Note that $\tau(\beta) = -\beta^{-1}$ and $\tau^2(\beta) = \tau(-\beta^{-1}) = -(-\beta^{-1})^{-1} = \beta$. Since $ord(\beta) = n$, then $-\beta^{-1} = \beta^{m-1}$. It follows that $\beta = \tau^2(\beta) = \tau(\tau(\beta)) = \tau(\beta^{m-1}) = \tau(\beta)^{m-1} = \beta^{(m-1)^2}$. Hence $(m-1)^2 = 1 \pmod{2m}$ and $2 \mid m$. $\square$

**4.3. Proof of Theorem 1.4.** Because of Lemmas 4.1 and 4.2, it remains to show that $K(\mathbb{P}(V))^{\langle \sigma \rangle}$ is not stably rational over $K$.

Recall that $\alpha_1 = \alpha$, $\alpha_2 = \alpha\beta$, $\alpha_3 = -\alpha$, $\alpha_4 = -\alpha\beta$ (in the proof of Lemma 4.1). Choose a vector $v \in V^*$ such that $v, \sigma(v), \sigma^2(v), \sigma^3(v)$ is a basis of $V^*$. Define

$v_1, v_2, v_3, v_4 \in V^* \otimes_K L$ by

$$v_i = (\sigma - \alpha_1)\cdots\widehat{(\sigma - \alpha_i)}\cdots(\sigma - \alpha_4)(v).$$

Then

$$\sigma(v_i) = \alpha_i v_i, \ \ \lambda(v_i) = v_{\lambda(i)} \quad \text{for any } \lambda \in G.$$

Define

$$x_i := v_{i+1}/v_i \quad \text{for } 1 \leqslant i \leqslant 3.$$

Then

$$\sigma : x_1 \mapsto \beta x_1, x_2 \mapsto -\beta^{-1}x_2, x_3 \mapsto \beta x_3,$$

$$\tau : \beta \mapsto -\beta^{-1}, v_1 \mapsto v_2 \mapsto v_3 \mapsto v_4 \mapsto v_1,$$

$$\rho : \beta \mapsto -\beta, v_2 \mapsto v_4 \mapsto v_2, v_1 \mapsto v_1, v_3 \mapsto v_3.$$

(Remember $\tau = (1234), \rho = (24)$. We take the possibility $\tau = (\alpha, \alpha\beta, -\alpha, -\alpha\beta)$ and $\rho = (\alpha\beta, -\alpha\beta)$. The discussion of other possibilities is similar.)

By Lemma 4.2, write $n = ord(\beta) = 4k$.

Then

$$L(x_1, x_2, x_3)^{\langle \sigma^2 \rangle} = L(x_1^{2k}, x_1x_2, x_3/x_1),$$

$$L(x_1, x_2, x_3)^{\langle \sigma \rangle} = L(y_1, y_2, y_3),$$

where

$$y_1 = x_1^n, \quad y_2 = x_2/x_1^{2k-1}, \quad y_3 = x_3/x_1.$$

Moreover,

$$\tau : y_1 \mapsto y_1^{2k-1}y_2^n, \quad y_2 \mapsto y_3/(y_1^{k-1}y_2^{2k-1}), \quad y_3 \mapsto 1/(y_1y_2^2y_3),$$

$$\rho : y_1 \mapsto y_1^{2k+1}y_2^ny_3^n, \quad y_2 \mapsto 1/(y_1^ky_2^{2k-1}y_3^{2k}), \quad y_3 \mapsto 1/(y_1y_2^2y_3).$$

Define $z_1, z_2, z_3$ by

$$z_1 = y_1y_3^{2k}, \quad z_2 = y_3^k/y_2, \quad z_3 = y_1y_2y_3^{k+1}.$$

Then $L(y_1, y_2, y_3) = L(z_1, z_2, z_3)$. With respect to $z_1, z_2, z_3$, the (multiplicative) actions of $\tau$ and $\tau\rho$ are given by

$$\begin{pmatrix} -1 & 0 & -1 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix},$$

which is the group action ($W_{13}$) in [20, p. 187]; this group action in turn is the group action ($U_4$) in Kunyavskii's list [10, p. 10]. By Kunyavskii's Theorem [10, Theorem 1], the fixed field $L(z_1, z_2, z_3)^G$ is not stably rational over $K$. $\square$

## 5. The proof of Theorem 1.5

In this section we shall adopt the same notations as in Section 3. Throughout this section we shall assume that $f(T)$ is a separable irreducible polynomial in $K[T]$, $\langle \beta_1, \beta_2, \beta_3 \rangle$ is a finite subgroup of $L\backslash\{0\}$ and the Galois group $G = \{id, (12)(34), (13)(24), (14)(23)\}$. By Lemma 3.2, it is necessary that $K \neq N$.

**5.1. Lemma.** (i) *If $N \neq L$, then char $K \neq 2$ and $\{\beta_1, \beta_2, \beta_3\} = \{\beta, -\beta, -1\}$.*
(ii) *If $N = L$, then char $K = 0$.*

**Proof.** (i) Suppose that $N \neq L$. Since $[L : N] = 2$, let $\{id, \tau_1\}$ be the Galois group of $L$ over $N$. By reindexing $\beta_1, \beta_2, \beta_3$, we may assume that $\tau_1 = (\alpha, \alpha\beta_1)(\alpha\beta_2, \alpha\beta_3)$. Then $\alpha\beta_3 = \tau_1(\alpha\beta_2) = \tau_1(\alpha)\tau_1(\beta_2) = \alpha\beta_1 \cdot \beta_2$. Thus $\beta_3 = \beta_1\beta_2$; on the other hand, $\alpha\beta_2 = \tau_1(\alpha\beta_3) = \tau_1(\alpha)\tau_1(\beta_3) = \alpha\beta_1 \cdot \beta_1\beta_2$. Thus $\beta_1 = -1$ and *char* $K \neq 2$ because $f(T)$ is separable. Taking $\beta_2 = \beta$, we get $\{\beta_1, \beta_2, \beta_3\} = \{\beta, -\beta, -1\}$.

(ii) Write $\langle \beta_1, \beta_2, \beta_3 \rangle = \langle \zeta \rangle$. Note that $ord(\zeta) < \infty$. If $N = L$, then $L = K(\zeta)$.

Assume that *char* $K \neq 0$. Then $\zeta$ lies in some finite field and $K(\zeta)$ is necessarily a cyclic extension of $K$. A contradiction. $\square$

**5.2. Convention and definitions.** We shall denote $\alpha_1 = \alpha,\ \alpha_2 = \alpha\beta_1,\ \alpha_3 = \alpha\beta_2,\ \alpha_4 = \alpha\beta_3$, and $\tau_1 = (\alpha, \alpha\beta_1)(\alpha\beta_2, \alpha\beta_3),\ \tau_2 = (\alpha, \alpha\beta_2)(\alpha\beta_1, \alpha\beta_3),\ \tau_3 = (\alpha, \alpha\beta_3)(\alpha\beta_1, \alpha\beta_2)$.

Define integers $n_1, n_2, d, m_1, m_2$ by

$$ord(\beta_j) = n_j \quad \text{for } 1 \leqslant j \leqslant 2,$$

$$d = \gcd\{n_1, n_2\} \quad \text{and} \quad n_j = dm_j \quad \text{for } 1 \leqslant j \leqslant 2.$$

Since $\beta_2$ is a root of unity, it follows that $\tau_1(\beta_2) = \beta_2^i$ for some integer $i$. Note that $i$ is uniquely determined modulo $n_2$ and $\gcd\{i, n_2\} = 1$.

**5.3. Lemma.** (i) *$\beta_3 = \beta_1\beta_2^i$ and $\langle \beta_1 \rangle \cap \langle \beta_2 \rangle = \langle \beta_1^{m_1} \rangle = \langle \beta_2^{m_2} \rangle$.*
(ii) *$d \mid i + 1$ and $m_2 \mid i - 1$.*

**Proof.** Since $\tau_1(\beta_1) = \beta_1^{-1}$, thus $\alpha\beta_3 = \tau_1(\alpha\beta_2) = \tau_1(\alpha)\tau_1(\beta_2) = \alpha\beta_1 \cdot \beta_2^i$. Hence $\beta_3 = \beta_1\beta_2^i$.

Now $\alpha\beta_2 = \tau_3(\alpha\beta_1) = \tau_3(\alpha)\tau_3(\beta_1) = \alpha\beta_1 \cdot \beta_2^i \cdot \tau_3(\beta_1)$. It follows that $\beta_2^{1-i} = \beta_1 \cdot \tau_3(\beta_1) \in \langle \beta_1 \rangle$. Thus $\beta_2^{(1-i)n_1} = 1$. Hence $n_2 \mid (1-i)n_1$. Thus $m_2 \mid (1-i)m_1$. Since $\gcd\{m_1, m_2\} = 1$, hence $m_2 \mid 1 - i$.

Note that both $\beta_1^{m_1}$ and $\beta_2^{m_2}$ are primitive $d$th roots of unity. Hence $\langle \beta_1^{m_1} \rangle = \langle \beta_2^{m_2} \rangle$ and it is contained in $\langle \beta_1 \rangle \cap \langle \beta_2 \rangle$. The index of $\langle \beta_1^{m_1} \rangle$ in $\langle \beta_1 \rangle \cap \langle \beta_2 \rangle, [\langle \beta_1 \rangle \cap \langle \beta_2 \rangle : \langle \beta_1^{m_1} \rangle]$, divides both $m_1 = [\langle \beta_1 \rangle : \langle \beta_1^{m_1} \rangle]$ and $m_2 = [\langle \beta_2 \rangle : \langle \beta_2^{m_2} \rangle]$. Thus $[\langle \beta_1 \rangle \cap \langle \beta_2 \rangle : \langle \beta_1^{m} \rangle] = 1$, i.e. $\langle \beta_1 \rangle \cap \langle \beta_2 \rangle = \langle \beta_1^{m_1} \rangle$.

We may write $\beta_1^{m_1} = \beta_2^{km_2}$ for some integer $k$. Call $\zeta = \beta_1^{m_1}$. Recall that $\tau_1(\beta_1) = \beta_1^{-1}$ and $\tau_1(\beta_2) = \beta_2^i$. It follows that $\zeta^{-1} = \beta_1^{-m_1} = \tau_1(\beta_1^{m_1}) = \tau_1(\beta_2^{km_2}) = \beta_2^{ikm_2} = \zeta^i$. Thus $d \mid i+1$. $\square$

**5.4. Definition.** By Lemma 5.3, we define integers $a$ and $b$ by the relations: $i+1 = da$ and $i-1 = m_2 b$. In particular,

$$da - m_2 b = 2. \tag{5.1}$$

On the other hand, note that $\beta_1^{m_1}$ and $\beta_2^{m_2}$ are primitive $d$th roots of unity. If $d \geqslant 2$, there is an integer $k$ such that $\beta_1^{m_1} = \beta_2^{km_2}$. The integer $k$ is uniquely determined modulo $d$ and $\gcd\{k, d\} = 1$. If $d = 1$, we simply define $k = 0$.

**5.5.** Now we begin to prove Theorem 1.5.

Choose a vector $v \in V^*$ such that $v, \sigma(v), \sigma^2(v), \sigma^3(v)$ is a basis of $V^*$. Define $v_1, v_2, v_3, v_4 \in V^* \otimes_K L$ by

$$v_i = (\sigma - \alpha_1) \cdots (\widehat{\sigma - \alpha_i}) \cdots (\sigma - \alpha_4)(v).$$

Then $\sigma(v_i) = \alpha_i v_i$ for $1 \leqslant i \leqslant 4$.

Define $x_i = v_{i+1}/v_1$ for $1 \leqslant i \leqslant 3$. Then

$$\sigma : x_1 \mapsto \beta_1 x_1, \quad x_2 \mapsto \beta_2 x_2, \quad x_3 \mapsto \beta_3 x_3.$$

Since $\langle \beta_1, \beta_2 \rangle$ is a cyclic group of order $dm_1, m_2$, choose integers $r$ and $s$ such that $\beta := \beta_1^r \beta_2^s$ is a generator of $\langle \beta_1, \beta_2 \rangle$. We find that $\sigma(x_1^r x_2^s) = \beta x_1^r x_2^s$. Thus $\sigma$ is a faithful group action on $L(x_1, x_2, x_3)$ with order $dm_1 m_2$.

Define $y_1, y_2, y_3$ by

$$y_1 := x_1^{m_1}/x_2^{km_2}, \quad y_2 := x_2^{n_2}, \quad y_3 := x_3/(x_1 x_2^i).$$

Since the determinant of the "coefficient" matrix of $y_1, y_2, y_3$ with respect to $x_1, x_2, x_3$ is

$$det \begin{pmatrix} m_1 & 0 & -1 \\ -km_2 & n_2 & -i \\ 0 & 0 & 1 \end{pmatrix} = m_1 n_2 = ord(\sigma),$$

it follows that $[L(x_1, x_2, x_3) : L(y_1, y_2, y_3)] = ord(\sigma)$ and $L(x_1, x_2, x_3)^{\langle \sigma \rangle} = L(y_1, y_2, y_3)$. Moreover, the multiplicative subgroup $\langle y_1, y_2, y_3 \rangle$ of $\langle x_1, x_2, x_3 \rangle$ $(\subset L(x_1, x_2, x_3) \backslash \{0\})$ is invariant under the action of $G$ because it is the kernel of the following $G$-equivariant map

$$\Phi : \langle x_1, x_2, x_3 \rangle \to L \backslash \{0\},$$

$$x_1^{n_1} x_2^{n_2} x_3^{n_3} \to \beta_1^{n_1} \beta_2^{n_2} \beta_3^{n_3}.$$

The action of $G$ on $y_1, y_2, y_3$ is given by

$$\tau_1 : y_1 \mapsto y_1^{-1} y_2^{-ka} y_3^{-km_2},\ y_2 \mapsto y_2^{i} y_3^{n_2},\ y_3 \mapsto y_2^{-ab} y_3^{-i},$$

$$\tau_2 : y_1 \mapsto y_1 y_2^{c} y_3^{m_1},\ y_2 \mapsto y_2^{-1},\ y_3 \mapsto y_3^{-1},$$

where $c := (m_1 b + 2k)/d$.

Since $\langle y_1, y_2, y_3 \rangle$ is $G$-invariant, it follows that $c \in \mathbb{Z}$. In particular, the integers $m_1$, $k$, $b$, $c$, $d$ satisfy the relation

$$2k = cd - m_1 b. \tag{5.2}$$

**5.6. Lemma.** (i) $\gcd\{b, d\} = 2$ *if* $b \equiv d \equiv 2 \pmod 2$; $\gcd\{b, d\} = 1$ *otherwise*.
(ii) *The situation* $b \equiv 1 \pmod 2$ *and* $d \equiv 0 \pmod 2$ *will never happen*.
(iii) *If* $b \equiv 0 \pmod 2$ *and* $d \equiv 1 \pmod 2$, *then* $c \equiv 0 \pmod 2$; *if* $b \equiv d \equiv 1 \pmod 2$, *then* $c \equiv m_1 \pmod 2$.

**Proof.** (i) Note that $\gcd\{k, d\} = 1$. If $p$ is a prime factor of $\gcd\{b, d\}$, then $p = 2$ by (5.2). Thus $b \equiv d \equiv 0 \pmod 2$. It follows that $k = c(d/2) - m_1(b/2)$. Repeat the above argument. We find $\gcd\{d/2, b/2\} = 1$. Thus $\gcd\{d, b\} = 2$.

(ii) Assume that $b \equiv 1 \pmod 2$ and $d \equiv 0 \pmod 2$. By Definition 5.4 $i + 1 \equiv 0 \equiv m_2 \pmod 2$. On the other hand, $m_1 \equiv 0 \pmod 2$ by (5.2). Thus $2 \mid \gcd\{m_1, m_2\}$. A contradiction.

(iii) Both properties follow from (5.2). $\square$

**5.7. Theorem** (We continue the discussion in 5.5). *Suppose that not both b and d are even integers. Then* $K(\mathbb{P}(V))^{\langle \sigma \rangle}$ *is rational over* $K$.

**Proof.** Define $u$ and $v$ by

$$(u, v) = \begin{cases} (c/2, m_1/2), & \text{if } m_1 \text{ is even,} \\ ((c+b)/2, (m_1+d)/2), & \text{if } m_1 \text{ is odd.} \end{cases}$$

If $m_1$ is even, then $c$ is even by Lemma 5.6(iii). Note that $d$ is always odd by Lemma 5.6(ii). If $m_1$ is odd, then $m_1 + d$ and $c + d$ are even. In conclusion, $u$ and $v$ are integers.

Node that $ud - vb = k$.

Define $z_1 = y_1 y_2^u y_3^v$. Then $L(y_1, y_2, y_3) = L(z_1, y_2, y_3)$ and

$$\tau_1 : y_2 \mapsto y_2^i y_3^{n_2},\ \ y_3 \mapsto y_2^{-ab} y_3^{-i},\ \ z_1 \mapsto z_1^{-1},$$

$$\tau_2 : y_2 \mapsto y_2^{-1}, y_3 \mapsto y_3^{-1}, z_1 \mapsto \begin{cases} z_1 & \text{if } m_1 \text{ is even}, \\ z_1 y_2^{-b} y_3^{-d} & \text{if } m_1 \text{ is odd}. \end{cases}$$

*Case* 1: $m_1 \equiv 0 \pmod 2$. Define $z_0 := (1 - z_1)/1 + z_1$. Then $\tau_1(z_0) = -z_0,\ \tau_2(z_0) = z_0$. Thus $L(z_0) = L(z)$ for some $z$ with $\tau_1(z) = \tau_2(z) = z$ by Theorem 2.1.

We may regard $L(y_1, y_2, y_3)^G = L(z)(y_2, y_3)^G$ as the function field of a two-dimensional algebraic torus over $L(z)^G$. By Theorem 2.5, it is rational over $L(z)^G (= K(z))$. And therefore it is rational over $K$.

*Case* 2: $m_1 \equiv 1 \pmod 2$ and $m_2 \equiv 0 \pmod 2$. Since $d$ is always odd by Lemma 5.6(ii), hence $a$ is even by (5.1). It follows that $d(a/2) - b(m_2/2) = 1$.

Define

$$z_2 = z_1 y_2^{-b} y_3^{-d}, \quad z_3 = y_2^{a/2} y_3^{m_2/2}.$$

Then

$$\tau_1 : z_1 \mapsto z_1^{-1}, z_2 \mapsto z_2^{-1}, z_3 \mapsto z_3,$$

$$\tau_2 : z_1 \mapsto z_2, z_2 \mapsto z_1, z_3 \mapsto z_3^{-1}.$$

Define $z_0 := (1 - z_3)/(1 + z_3)$. Then $\tau_1(z_0) = z_0,\ \tau_2(z_0) = -z_0$. Thus $L(z_0) = L(z)$ for some $z$ with $\tau_1(z) = \tau_2(z) = z$ by Theorem 2.1.

We may regard $L(y_1, y_2, y_3)^G = L(z)(z_1, z_2)^G$ as the function field of a two-dimensional algebraic torus over $L(z)^G$. By Theorem 2.5, it is rational over $L(z)^G$ $(= K(z))$. And therefore it is rational over $K$.

*Case* 3: $m_1 \equiv 1 \pmod 2$ *and* $m_2 \equiv 1 \pmod 2$. Since $d$ is always odd by Lemma 5.6(ii), it follows that $n_1$ and $n_2$ are odd. Recall that $\tau_1(\beta_2) = \beta_2^i$. Without loss of generality, we may assume that $i$ is odd because, for the case $i$ is even, just consider $\tau_1(\beta_2) = \beta_2^{i+n_2}$. Thus, from Definition 5.4, we find that both $a$ and $b$ are even and $d(a/2) - m_2(b/2) = 1$.

Define

$$z_2 = y_2^a y_3^{m_2}, \quad z_3 = y_2^{(b-a)/2} y_3^{(d-m_2)/2}.$$

Since the determinant of the "coefficient" matrix of $z_2$ and $z_3$ with respect to $y_2$ and $y_3$ is

$$det\begin{pmatrix} a & (b-a)/2 \\ m_2 & (d-m_2/2 \end{pmatrix} = 1,$$

it follows that $L(y_2, y_3) = L(z_2, z_3)$. Thus $L(y_1, y_2, y_3) = L(z_1, z_2, z_3)$ and

$$\tau_1 : z_1 \mapsto z_1^{-1}, z_2 \mapsto z_2, z_3 \mapsto z_2^{-1}z_3^{-1},$$

$$\tau_2 : z_1 \mapsto z_1 z_2^{-1} z_3^{-2}, z_2 \mapsto z_2^{-1}, z_3 \mapsto z_3^{-1}.$$

Define $u_1 = z_1$, $u_2 = z_3$, $u_3 = z_2^{-1}z_3^{-1}$. Then the (multiplicative) actions of $\tau_1$ and $\tau_1\tau_2$ with respect to $u_1$, $u_2$, $u_3$ are given by

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} -1 & 0 & 0 \\ 1 & 0 & -1 \\ -1 & -1 & 0 \end{pmatrix}$$

which is the group action $(W_{12})$ in [20, p. 174]; this group action in turn is of type (d) in [10, pp. 8–9]. Thus $L(u_1, u_2, u_3)^G$ is rational over $K$. $\square$

**5.8.** We will finish the proof of Theorem 1.5. We now assume that both $b$ and $d$ are even integers.

Since $\gcd\{k, d\} = 1$, it follows that $k$ is odd. From (5.1) and (5.2), it is easy to see: (i) if $b \equiv d \equiv 2 \pmod 4$, then $a + c \equiv m_1 + m_2 \pmod 2$; (ii) if $b \equiv 0 \pmod 4$, then $d \equiv 2 \pmod 4$ and $a \equiv c \equiv 1 \pmod 2$; (iii) if $d \equiv 0 \pmod 4$, then $b \equiv 2 \pmod 4$ and $m_1 \equiv m_2 \equiv 1 \pmod 2$.

We shall define integers $u$ and $v$ as follows:

If any one of the following conditions is valid: (i) if $b \equiv d \equiv 2 \pmod 4$ and $a + c \equiv 0 \pmod 2$, (ii) $b \equiv 0 \pmod 4$, $d \equiv 2 \pmod 4$ and $m_1 + m_2 \equiv 0 \pmod 2$ or (iii) $b \equiv 2 \pmod 4$, $d \equiv 0 \pmod 4$ and $a + c \equiv 0 \pmod 2$, then define

$$\text{(A)} \quad u = (a+c)/2, \quad v = (m_1 + m_2)/2.$$

If any one of the following conditions is valid: (i) if $b \equiv d \equiv 2 \pmod 4$ and $a + c \equiv 1 \pmod 2$, (ii) $b \equiv 0 \pmod 4$, $d \equiv 2 \pmod 4$ and $m_1 + m_2 \equiv 1 \pmod 2$ or (iii) $b \equiv 2 \pmod 4$, $d \equiv 0 \pmod 4$ and $a + c \equiv 1 \pmod 2$, then define

$$\text{(B)} \quad u = (2a + 2c + b)/4, \quad v = (2m_1 + 2m_2 + d)/4.$$

In both situations (A) and (B), we always have the relation: $ud - vb = k + 1$.

Define

$$z_1 = y_1 y_2^u y_3^v, \quad z_2 = y_2^a y_3^{m_2}, \quad z_3 = y_2^{b/2} y_3^{d/2}.$$

Then $L(y_1, y_2, y_3) = L(z_1, z_2, z_3)$ and

$$\tau_1 : z_2 \mapsto z_2, \quad z_3 \mapsto z_3^{-1}, \quad z_1 \mapsto z_2/z_1,$$

$$\tau_2 : z_2 \mapsto z_2^{-1}, \quad z_3 \mapsto z_3^{-1}, \quad z_1 \mapsto \begin{cases} z_1 z_2^{-1} & \text{if (A) holds,} \\ z_1 z_2^{-1} z_3^{-1} & \text{if (B) holds.} \end{cases}$$

*Case* 1: *Situation* (A) *holds*. Define $z_0 = (1 - z_3)/(1 + z_3)$. Then $\tau_1(z_0) = \tau_2(z_0) = -z_0$. Thus $L(z_0) = L(z)$ for some $z$ with $\tau_1(z) = \tau_2(z) = z$ by Theorem 2.1.

We may regard $L(y_1, y_2, y_3)^G = L(z)(z_1, z_2)^G$ as the function field of a two-dimensional algebraic torus over $L(z)^G$. By Theorem 2.5, it is rational over $L(z)^G (= K(z))$. And therefore it is rational over $K$.

*Case* 2: *Situation* (B) *holds*. Define

$$u_1 = z_3, \quad u_2 = z_1^{-1} z_2, \quad u_3 = z_1.$$

Then the actions of $\tau_1$ and $\tau_2$ with respect to $u_1, u_2, u_3$ are given by

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} -1 & 1 & -1 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}$$

which is the group action $(W_{14})$ in [20, p. 174]. This action in turn is the group action $(U_1)$ in Kunyavskii's list [10, p. 9]. By Kunyavskii's Theorem [10, Theorem 1], $L(u_1, u_2, u_3)^G$ is not stably rational over $K$. This finishes the proof of Theorem 1.5. $\square$

## 6. Special cases

**6.1. Lemma.** *Let the notations be the same as in Section* 3. *Assume that* $f(T) \in K[T]$ *is separable irreducible*, $\langle \beta_1, \beta_2, \beta_3 \rangle$ *is a finite group and the Galois group* $G = \{id, (12)(34), (13)(24), (14)(23)\}$.

(i) *If* $-1 \in \{\beta_1, \beta_2, \beta_3\}$, *then* $\{\beta_1, \beta_2, \beta_3\} = \{\beta, -\beta, -1\}$.

(ii) *If* $\{\beta_1, \beta_2, \beta_3\} = \{\beta_l, \beta_l^a, \beta_l^b\}$ *for some* $l$, *then* $\{\beta_1, \beta_2, \beta_3\} = \{\beta, \beta^j, \beta^{1-j}\}$ *for some integer* $j$ *and* $2j(j-1)$ *is divisible by* $n$ *where* $n = ord(\beta)$.

**Proof.** (i) Let $\beta_1 = -1$. Take $\tau = (\alpha, \alpha\beta_2)(\alpha\beta_1, \alpha\beta_3) \in G$. Then $\tau(\alpha) = \alpha\beta_2$ and $\alpha\beta_3 = \tau(\alpha\beta_1) = \tau(-\alpha) = -\tau(\alpha) = -\alpha\beta_2$. Hence $\beta_3 = -\beta_2$.

(ii) We may assume $l = 1$. Take $\tau_1 = (\alpha, \alpha\beta_1)(\alpha\beta_1^a, \alpha\beta_1^b) \in G$. Then $\tau_1(\beta_1) = \beta_1^{-1}$. Hence $\alpha\beta_1^b = \tau_1(\alpha\beta_1^a) = \tau_1(\alpha)\tau_1(\beta_1)^a = \alpha\beta_1 \cdot \beta_1^{-a}$. It follows that $b = 1 - a \pmod n$ where $n = ord(\beta)$ and $\beta = \beta_1$. Thus we may take $j = a$.

Take $\tau_2 = (\alpha, \alpha\beta^j)(\alpha\beta, \alpha\beta^{1-j}) \in G$. Then $\tau_2(\beta) = \tau_2(\alpha\beta/\alpha) = \tau_2(\alpha\beta)/\tau_2(\alpha) = (a\beta^{1-j})/(\alpha\beta^j) = \beta^{1-2j}$. It follows that $\alpha\beta = \tau_2(\alpha\beta^{1-j}) = \tau_2(\alpha)\tau_2(\beta)^{1-j} = \alpha\beta^j \cdot \beta^{(1-2j)(1-j)}$. Hence $1 = j + (1-2j)(1-j) \pmod n$, i.e. $2j(j-1) = 0 \pmod n$. $\square$

**6.2. Proof of Theorem 1.6.** *Step* 1: *Suppose that* $\{\beta_1, \beta_2, \beta_3\} = \{\beta, \beta^j, \beta^{1-j}\}$ *and* $n = ord(\beta)$.

Note that (i) is just Lemma 6.1(ii). It remains to prove (ii). Let $d = ord(\beta^j)$. Then $d \mid n$. Write $n = de$. It follows that $j = ej'$ for some integer $j'$ with gcd $\{j', d\} = 1$.

In the notations of Theorem 1.5 we find that

$$n_1 = n, \quad n_2 = d, \quad m_1 = e, \quad m_2 = 1.$$

Take $\tau_1 = (\alpha, \alpha\beta)(\alpha\beta^j, \alpha\beta^{1-j})$. Since $\tau_1(\beta) = \beta^{-1}$, it follows that $\tau_1(\beta^j) = \beta^{-j} = (\beta^j)^{-1}$. Thus the integer $i$ in 5.2 can be taken to be $-1$. By Definition 5.4, $a = 0$ and $b = -2$.

Since gcd $\{j', d\} = 1$, find integers $k$ and $s$ such that

$$kj' + sd = 1. \tag{6.1}$$

Then $\beta^{m_1} = \beta^e = \beta^{kj'e+sde} = (\beta^j)^k$. Thus this integer $k$ plays the same role of $k$ in Definition 5.4. Moreover, (5.2) becomes

$$cd = 2(k - e). \tag{6.2}$$

By (i) of Theorem 1.6, define an integer $x$ as follows: $2j(j-1) = nx$, or equivalently,

$$2j'(j-1) = dx. \tag{6.3}$$

We shall prove that $K(\mathbb{P}(V))^{\langle\sigma\rangle}$ is rational if and only if $x$ is an even integer.

*Case* 1: $d$ *is odd*. Apply Theorem 1.5(1). $K(\mathbb{P}(V))^{\langle\sigma\rangle}$ is rational. By (6.3), $x$ is even.

*Case* 2: $d$ *is even*. Let $2^t \| d$ where $t \geqslant 1$.

By (6.1), both $k$ and $j'$ are odd.

By (6.1) we get $kj'e + sde = e$. Thus $kj = e \pmod{2^t}$.

Now

$$\begin{aligned} x \text{ is even.} \quad &\Leftrightarrow 2^t \mid j-1 && \text{(by (6.3))} \\ &\Leftrightarrow k = kj \pmod{2^t} && (k \text{ is odd}) \\ &\Leftrightarrow k = e \pmod{2^t} && \\ &\Leftrightarrow c \text{ is even} && \text{(by (6.2)).} \end{aligned}$$

Applying Theorem 1.5(2), (4), $(1)'$ and $(3)'$, we find that $K(\mathbb{P}(V))^{\langle\sigma\rangle}$ is rational if and only if $x$ is even. Hence the result.

*Step* 2: *Suppose that* $\{\beta_1, \beta_2, \beta_3\} = \{\beta, -\beta, -1\}$ *and* $n = ord(\beta)$. If $n$ is odd, then $ord(-\beta) = 2n$; if $n$ is even, then $ord(-\beta) = n$ or $n/2$ (if $n/2$ is even). In any case, we write ord $(-\beta) = 2m$ and note that $4 \mid n$ if and only if $4 \mid 2m$.

Write $\{\beta_1, \beta_2, \beta_3\} = \{\beta, -\beta, -1\} = \{-\beta, (-\beta)^{m+1}, (-\beta)^{-m}\}$ and apply the result of Step 1. The integer $x$ is defined by $2(m+1)(-m) = 2mx$, i.e. $x = -(m+1)$. Thus $K(\mathbb{P}(V))^{\langle\sigma\rangle}$ is not stably rational $\Leftrightarrow x$ is odd $\Leftrightarrow m$ is even $\Leftrightarrow 4 \mid 2m \Leftrightarrow 4 \mid n$. This finishes the proof of Theorem 1.6. $\square$

Theorem 1.7 (resp. Theorem 1.8) is the application of Theorems 1.3, 1.4 and 1.6 to the case $f(T) = T^4 - aT^2 + (a^2/b)$ (resp. $f(T) = T^4 + a$). Before proving them, we recall a result which is part of the folklore in Galois theory:

**6.3. Theorem** (Kappe and Warren [9, Theorems 2 and 3]). *Let* $K$ *be a field of char* $K \neq 2$, $g(T) = T^4 - cT^2 + d \in K[T]$, *and* $G$ *be the Galois group of* $g(T)$ *over* $K$.

(i) $g(T)$ *is irreducible over* $K$. $\Leftrightarrow c^2 - 4d,\ c + 2\sqrt{d},\ c - 2\sqrt{d} \notin K^2$.

(ii) *Assume that* $g(T)$ *is irreducible. Then*

$$G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \Leftrightarrow d \in K^2,$$

$$G \simeq \mathbb{Z}_4 \Leftrightarrow d(c^2 - 4d) \in K^2,$$

$$G \simeq D_4 \Leftrightarrow d, d(c^2 - 4d) \notin K^2.$$

**6.4. Proof of Theorem 1.7.** The characteristic polynomial of $\sigma$ is $f(T) = T^4 - aT^2 + (a^2/b)$. The roots of $f(T) = 0$ are $\alpha$, $-\alpha$, $\alpha\beta$, $-\alpha\beta$ where $\alpha = \sqrt{ab + a\sqrt{b^2 - 4b}}/\sqrt{2b}$, $\beta = \sqrt{2b - 4 - 2\sqrt{b^2 - 4b}}/2$. Note that $\beta$ is root of $T^4 - (b-2)T^2 + 1 = 0$.

Conditions (i) and (ii) are consequences of Theorem 1.3(i) and (iii).

By Theorem 6.3, (iii) is equivalent to that $f(T)$ is reducible if *char* $K \neq 2$. Hence we may apply Theorem 1.3(i) and (ii).

By Theorem 6.3, (iv) is equivalent to $G \simeq \mathbb{Z}_4$ if char $K \neq 2$ and $f(T)$ is irreducible. Hence we may apply Theorem 1.3 (i), (ii) and (iv).

For the remaining part, $b \in K^2$ is equivalent to $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ and $b, b-4 \notin K^2$ is equivalent to $G \simeq D_4$ by Theorem 6.3. $\square$

**6.5.** The proof of Theorem 1.8 is similar to that of Theorem 1.7 and thus is omitted.

## 7. Applications

The method of the preceding sections can be applied to other situations. As illustrations, we shall give a proof of Theorems 1.9 and 7.3. We remark that similar ideas (besides a detailed analysis of eigenvalues) can be used to discuss the rationality of $K(x_1,x_2,x_3)^{\langle\sigma\rangle}$ where *char* $K \neq 2$, $\sigma(x_i) = (a_i x_i + b_i)/(c_i x_i + d_i)$ with $a_i d_i - b_i c_i \neq 0$ [8]; this problem is a generalization of a question solved by Saltman [17].

**7.1. Lemma** (Hajja [4]). *Let $K$ be any field, $\sigma \in GL_n(K)$, $f(T)$ be the characteristic polynomial of $\sigma$ such that $f(T)$ is the minimal polynomial of $\sigma$. Define an affine $K$-automorphism $\Phi$ on $K(x_1,\ldots,x_n)$ by*

$$\begin{pmatrix}\Phi(x_1)\\ \vdots \\ \Phi(x_n)\end{pmatrix} = \sigma\begin{pmatrix}x_1\\ \vdots \\ x_n\end{pmatrix} + \begin{pmatrix}b_1\\ \vdots \\ b_n\end{pmatrix}$$

*for some $b_i \in K$. If $f(1)\neq 0$, then $\Phi$ can be linearized. Explicitly, if $v$ is a vector in $\sum_{i=1}^n K\cdot x_i$ such that $v, \sigma(v), \ldots, \sigma^{n-1}(v)$ generate $\sum_{i=1}^n K\cdot x_i$ and define $v_i = \Phi^{i-1}(v)$ for $1\leqslant i\leqslant n$ then $\Phi(v_n) = (\sum_{i=1}^n a_{i-1}v_i) + c$ where $f(T) = T^n - \sum_{i=0}^{n-1} a_i T^i \in K[T]$ and $c\in K$; now define $y_1 = v - (c/f(1))$ and $y_i = \Phi^{i-1}(y_1)$ for $2\leqslant i\leqslant n$. It follows that $\Phi(y_n) = \sum_{i=1}^n a_{i-1}y_i$.*

**Proof.** The existence of $v$ follows from the assumption that $f(T)$ is the minimal polynomial of $\sigma$. All the rest are easy. $\square$

**7.2. Proof of Theorem 1.9.** *Case* 1: *$f(1)\neq 0$ and $f(T)$ is the minimal polynomial of $\sigma$.* Apply Lemma 7.1. Since $\sigma$ is similar to its rational normal form, we can transform the basis $y_1,\ldots,y_n$ in Lemma 7.1 to another one $z_1,\ldots,z_n$ such that $\Phi(z_j) = \sum a_{ij}z_i$ and $(a_{ij})$ is the linear part of the given affine automorphism.

*Case* 2: *$f(1) = 0$ and $f(T)$ is the minimal polynomial of $\sigma$.* By linear algebra, $\sigma$ is conjugate to one of the following matrices:

$$\begin{pmatrix}1&1&0&0\\0&1&1&0\\0&0&1&1\\0&0&0&1\end{pmatrix},\quad \begin{pmatrix}*&0&0&0\\0&1&1&0\\0&0&1&1\\0&0&0&1\end{pmatrix},\quad \left(\begin{array}{cc|cc} \multicolumn{2}{c|}{\multirow{2}{*}{$*$}} & 0&0\\ & & 0&0\\ \hline 0&0&1&1\\ 0&0&0&1\end{array}\right),\quad \left(\begin{array}{ccc|c} \multicolumn{3}{c|}{\multirow{3}{*}{$*$}} & 0\\ &&&0\\ &&&0\\ \hline 0&0&0&1\end{array}\right).$$

In any case, there exist $y_1,y_2,y_3,y_4 \in \sum_{i=1}^4 K\cdot x_i$ such that either $\Phi(y_4) = y_4 + y_3 + c$ or $\Phi(y_4) = y_4 + c$, where $c\in K$; moreover, $\Phi$ leaves $K + \sum_{i=1}^3 K\cdot y_i$ invariant.

Hence $K(x_1,x_2,x_3,x_4) = K(y_1,y_2,y_3,y_4)$ and $\Phi(K(y_1,y_2,y_3))\subset K(y_1,y_2,y_3)$ and $\Phi(y_4) = y_4 + u$ for some $u\in K(y_1,y_2,y_3)$. By Theorem 2.2 it suffices to prove that $K(y_1,y_2,y_3)^{\langle\Phi\rangle}$ is rational over $K$. But this follows from Theorem 1.2.

*Case* 3: *$f(T)$ is not the minimal polynomial of $\sigma$.* Thus $f(T)$ is not irreducible in $K[T]$.

*Case* 3.1: $f(1)\neq 0$. By Lemma 7.1, $\Phi$ can be linearized and the characteristic polynomial of the linearized automorphism $\Phi$ is the same $f(T)$. Since $f(T)$ is reducible, we may apply Theorem 1.3.

*Case* 3.2: $f(1) = 0$. By linear algebra, $\sigma$ is conjugate to one of the matrices

$$\left(\begin{array}{ccc|c} & & & * \\ & * & & * \\ & & & * \\ \hline 0 & 0 & 0 & 1 \end{array}\right), \quad \left(\begin{array}{cc|cc} \multicolumn{2}{c|}{\multirow{2}{*}{$*$}} & 0 & 0 \\ & & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right), \quad \left(\begin{array}{cc|cc} * & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{array}\right), \quad \left(\begin{array}{cc|cc} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{array}\right).$$

Apply similar arguments as in Case 2 to prove that $K(x_1, x_2, x_3, x_4)^{\langle\sigma\rangle}$ is rational. $\square$

**7.3. Theorem.** *Let $K$ be any field and $\sigma \in GL_5(K)$ be the form*

$$\sigma = \left(\begin{array}{cc|ccc} a_1 & a_2 & & & \\ b_1 & b_2 & & 0 & \\ \hline & & c_1 & c_2 & c_3 \\ & 0 & d_1 & d_2 & d_3 \\ & & e_1 & e_2 & e_3 \end{array}\right).$$

*If $\sigma$ acts on $K(x, y, z)$ by*

$$\sigma(x) = \frac{a_1 x + a_2}{b_1 x + b_2}, \quad \sigma(y) = \frac{c_1 y + c_2 z + c_3}{e_1 y + e_2 z + e_3}, \quad \sigma(z) = \frac{d_1 y + d_2 z + d_3}{e_1 y + e_2 z + e_3},$$

*then $K(x, y, z)^{\langle\sigma\rangle}$ is rational over $K$.*

**Proof.** Let $f(T)$ and $g(T)$ be the characteristic polynomials of

$$\begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} c_1 & c_2 & c_3 \\ d_1 & d_2 & d_3 \\ e_1 & e_2 & e_3 \end{pmatrix},$$

respectively.

*Case* 1: *$f(T)$ is reducible.* We can find $u \in K(x)$ such that $K(x) = K(u)$ and $\sigma(u) = \lambda u + \varepsilon$ for some $\lambda, \varepsilon \in K$. By Theorem 2.2, the rationality problem of $K(x, y, z)^{\langle\sigma\rangle}$ is reduced to that of $K(y, z)^{\langle\sigma\rangle}$, which is rational over $K$ by Theorem 1.2.

*Case* 2: *$g(T)$ is reducible.* Thus we may assume the action of $\sigma$ on $y$ and $z$ becomes

$$\sigma(y) = c_{11} y + c_{12} z + d_1, \quad \sigma(z) = c_{21} y + c_{22} z + d_2,$$

where $(c_{ij}) \in GL_2(K)$ and $d_1, d_2 \in K$. Let $h(T)$ be the characteristic polynomial of $(c_{ij})_{1 \leqslant i, j \leqslant 2}$.

*Case* 2.1: $h(1) \neq 0$. If $h(T)$ is not the minimal polynomial of $(c_{ij})_{1 \leqslant i, j \leqslant 2}$, then $(c_{ij})_{1 \leqslant i, j \leqslant 2}$ is a scalar matrix and $\sigma(y) = cy + d_1$, $\sigma(z) = cz + d_2$. Thus $K(x, y, z)^{\langle \sigma \rangle}$ is rational over $K$ by Theorem 2.2 and Lüroth's Theorem.

If $h(T)$ is the minimal polynomial of $(c_{ij})_{1 \leqslant i, j \leqslant 2}$, then we may linearize the action by Lemma 7.1. Therefore we may assume that $d_1 = d_2 = 0$. It follows that the action of $\sigma$ on $y/z$ and $z$ is given by

$$\sigma(y/z) = (c_{11}(y/z) + c_{12})/(c_{21}(y/z) + c_{22}), \quad \sigma(z) = uz,$$

where $u = c_{21}(y/z) + c_{22} \in K(y/z)$. Thus, the rationality of $K(x, y, z)^{\langle \sigma \rangle}$ is reduced to that of $K(x, y/z)^{\langle \sigma \rangle}$ by Theorem 2.2. The rationality of $K(x, y/z)^{\langle \sigma \rangle}$ follows from Theorem 1.2.

*Case* 2.2. $h(1) = 0$. Then the matrix $(c_{ij})_{1 \leqslant i, j \leqslant 2}$ is either diagonalizable or is conjugate to

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Thus, without loss of generality, we may assume that

$$\sigma(y) = c_1 y + d_1, \quad \sigma(z) = c_2 z + d_2$$

or

$$\sigma(z) = z + y + d_1, \quad \sigma(y) = y + d_2.$$

In either case, $K(x, y, z)^{\langle \sigma \rangle}$ is rational over $K$ because of Theorem 2.2.

*Case* 3: *Both $f(T)$ and $g(T)$ are irreducible and $f(T)$ is inseparable*. In this case, *char* $K = 2$, $g(T)$ is separable and $f(T) = T^2 - a$.

Let $L = K(\alpha_1, \alpha_2, \alpha_3)$ where $g(T) = (T - \alpha_1)(T - \alpha_2)(T - \alpha_3)$ and consider $K(x, y, z)^{\langle \sigma \rangle} = \{L(x, y, z)^{\langle \sigma \rangle}\}^G$ where $G$ is the Galois group of $L$ over $K$.

Applying standard arguments in the preceding sections, we can find $u, v, w \in L(x, y, z)$ such that $L(x, y, z) = L(u, v, w)$ and

$$\sigma(u) = a/u, \quad \sigma(v) = \lambda_1 v, \quad \sigma(w) = \lambda_2 w,$$

where $ord(\lambda_i)$ is either infinite or an odd integer because *char* $K = 2$.

Thus $L(x, y, z)^{\langle \sigma^2 \rangle} = L(u, M_1, M_2)$, $L(u, M)$ or $L(u)$ where $M_1$, $M_2$, $M$ are monomials in $v$ and $w$. Moreover, $M_1$, $M_2$, $M$ are fixed by $\sigma$. Hence $L(x, y, z)^{\langle \sigma \rangle} = L(u + (a/u), M_1, M_2)$, $L(u + (a/u), M)$ or $L(u + (a/u))$.

It follows that $\{L(x, y, z)^{\langle \sigma \rangle}\}^G$ is the function field of an algebraic torus of dimension $\leqslant 2$. Thus it is rational by Theorem 2.5.

*Case* 4: *Both $f(T)$ and $g(T)$ are irreducible and $g(T)$ is inseparable*. The case is similar to Case 3. Note that $K(y_1, y_2)^{\langle \sigma \rangle}$ is rational over $K$ if $\sigma(y_1) = y_2$, $\sigma(y_2) =$

$a/(y_1y_2)$ where $a \in K \backslash \{0\}$ by Hajja [3]. The rest of the proof is almost the same as in Case 3 and is omitted.

*Case* 5: *Both* $f(T)$ *and* $g(T)$ *are separable irreducible*. Let $L$ be the splitting field of $f(T)g(T)$ and $G$ be the Galois group of $L$ over $K$. Then $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_3, S_3$ or $\mathbb{Z}_2 \times S_3$ where $S_3$ is the symmetric group of degree 3.

Applying standard arguments in the preceding section, we get a function field of an algebraic torus of dimension $\leqslant 3$. If the dimension is $\leqslant 2$, we are finished because of Theorem 2.5. If it is a three-dimensional algebraic torus, apply [10, Theorem 1] because a three-dimensional algebraic torus is rational if the Galois group of its splitting field is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3, S_3$ or $\mathbb{Z}_2 \times S_3$. $\square$

## Acknowledgments

I thank the anonymous referee for pointing out several mistakes in the original manuscript and for providing many constructive suggestions.

## References

[1] H. Ahmad, M. Hajja, M. Kang, Rationality of some projective linear actions, J. Algebra 228 (2000) 643–658.
[2] W.B. Giles, D.L. McQuillan, A problem on rational invariants, J. Number Theory 1 (1969) 375–384.
[3] M. Hajja, Rationality of finite groups of monomial automorphisms of $K(X, Y)$, J. Algebra 109 (1987) 46–51.
[4] M. Hajja, A note on affine automorphisms, Comm. Algebra 18 (1990) 1535–1549.
[5] M. Hajja, M. Kang, Three-dimensional purely monomial group actions, J. Algebra 170 (1994) 805–860.
[6] M. Hajja, M. Kang, Some actions of symmetric groups, J. Algebra 177 (1995) 511–535.
[7] M. Kang, Solvable group actions on projective planes, preprint.
[8] M. Kang, Group actions on $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$, preprint.
[9] L. Kappe, B. Warren, An elementary test for the Galois group of a quartic polynomial, Amer. Math. Monthly 96 (1989) 133–137.
[10] B.E. Kunyavskii, Three-dimensional algebraic tori, Selecta Math. Soviet 9 (1990) 1–21.
[11] H.W. Lenstra Jr., Rational functions invariant under a finite abelian group, Invent. Math. 25 (1974) 299–325.
[12] K. Masuda, Application of the theory of the group of classes of projective modules to the existence problem of independent parameters of invariant, J. Math. Soc. Japan 20 (1968) 223–232.
[13] T. Miyata, Invariants of certain groups, I, Nagoya Math. J. 41 (1971) 69–73.
[14] E. Noether, Gleichungen mit vorgebshriebene Gruppe, Math. Ann. 78 (1916) 221–229.
[15] D.J. Saltman, Generic Galois extensions and problems in field theory, Adv. Math. 43 (1982) 250–283.
[16] D.J. Saltman, Retract rational fields and cyclic Galois extensions, Israel J. Math. 47 (1984) 165–215.
[17] D.J. Saltman, A nonrational field, answering a question of Hajja, in: M. Boulagouaz, J.-P. Tignol (Eds.), Algebra and Number Theory, Marcel Dekker, New York, 2000.

[18] R.G. Swan, Invariant rational functions and a problem of Steenrod, Invent. Math. 7 (1969) 148–158.
[19] R.G. Swan, Noether's problem in Galois theory, in: B. Srinivasan, J. Sally (Eds.), Emmy Neother in Bryn Mawr, Springer, New York, 1983.
[20] K. Tahara, On the finite subgroups of $GL(3,\mathbb{Z})$, Nagoya Math. J. 41 (1971) 169–209.
[21] V.E. Voskresenskii, On two-dimensional algebraic tori II, Math. USSR Izv. 1 (1967) 691–696.
[22] V.E. Voskresenskii, Algebraic Groups and their Birational Invariants, Translation of Mathematical Monographs, Vol. 179, Amer. Math. Soc., Providence, RI, 1998.
[23] O. Zariski, On Castelnuovo's criterion of rationality $p_a = P_2 = 0$ of an algebraic surface, Illinois J. Math. 2 (1958) 303–315.