MATHEMATICS OF COMPUTATION
https://doi.org/10.1090/mcom/3469
Article electronically published on September 12, 2019

RATIONALITY PROBLEM FOR NORM ONE TORI IN SMALL DIMENSIONS

SUMITO HASEGAWA, AKINARI HOSHI, AND AIICHI YAMASAKI

Abstract. We classify stably/retract rational norm one tori in dimension $n-1$ for $n=2^e$ ($e\geq 1$) as a power of 2 and $n=12,14,15$. Retract non-rationality of norm one tori for primitive $G\leq S_{2p}$ where p is a prime number and for the five Mathieu groups $M_n\leq S_n$ ($n=11,12,22,23,24$) is also given.

1. Introduction

Let L be a finite Galois extension of a field k and let $G=\mathrm{Gal}(L/k)$ be the Galois group of the extension L/k. Let $M=\bigoplus_{1\leq i\leq n}\mathbb{Z}\cdot u_i$ be a G-lattice with a $\mathbb{Z}$-basis $\{u_1,\ldots,u_n\}$, i.e., finitely generated $\mathbb{Z}[G]$-module which is $\mathbb{Z}$-free as an abelian group. Let G act on the rational function field $L(x_1,\ldots,x_n)$ over L with n variables $x_1,\ldots,x_n$ by

$$\sigma(x_i)=\prod_{j=1}^{n}x_j^{a_{i,j}},\quad 1\leq i\leq n \tag{1}$$

for any $\sigma\in G$, when $\sigma(u_i)=\sum_{j=1}^{n}a_{i,j}u_j$, $a_{i,j}\in\mathbb{Z}$. The field $L(x_1,\ldots,x_n)$ with this action of G will be denoted by $L(M)$. There is the duality between the category of G-lattices and the category of algebraic k-tori which split over L (see [Ono61, Section 1.2], [Vos98, page 27, Example 6]). In fact, if T is an algebraic k-torus, then the character group $X(T)=\mathrm{Hom}(T,\mathbb{G}_m)$ of T may be regarded as a G-lattice. Conversely, for a given G-lattice M, there exists an algebraic k-torus T which splits over L such that $X(T)$ is isomorphic to M as a G-lattice.

The invariant field $L(M)^G$ of $L(M)$ under the action of G may be identified with the function field of the algebraic k-torus T. Note that the field $L(M)^G$ is always k-unirational (see [Vos98, page 40, Example 21]). Tori of dimension n over k correspond bijectively to the elements of the set $H^1(\mathcal{G},\mathrm{GL}_n(\mathbb{Z}))$ where $\mathcal{G}=\mathrm{Gal}(k_{\mathrm{s}}/k)$ since $\mathrm{Aut}(\mathbb{G}_m^n)=\mathrm{GL}_n(\mathbb{Z})$. The k-torus T of dimension n is determined uniquely by the integral representation $h:\mathcal{G}\to\mathrm{GL}_n(\mathbb{Z})$ up to conjugacy, and the group $h(\mathcal{G})$ is a finite subgroup of $\mathrm{GL}_n(\mathbb{Z})$ (see [Vos98, page 57, Section 4.9]).

Let K/k be a separable field extension of degree n and let L/k be the Galois closure of K/k. Let $G=\mathrm{Gal}(L/k)$ and $H=\mathrm{Gal}(L/K)$. The Galois group G

Received by the editor January 1, 2019, and, in revised form, April 14, 2019, May 14, 2019, and May 26, 2019.

2010 *Mathematics Subject Classification.* Primary 11E72, 12F20, 13A50, 14E08, 20C10, 20G15.

Key words and phrases. Rationality problem, algebraic tori, stably rational, retract rational, flabby resolution.

This work was partially supported by JSPS KAKENHI Grant Numbers 25400027, 16K05059, 19K03418.

may be regarded as a transitive subgroup of the symmetric group S_n of degree n. Let $R^{(1)}_{K/k}(\mathbb{G}_m)$ be the norm one torus of K/k, i.e., the kernel of the norm map $R_{K/k}(\mathbb{G}_m) \to \mathbb{G}_m$ where $R_{K/k}$ is the Weil restriction (see [Vos98, page 37, Section 3.12]). The norm one torus $R^{(1)}_{K/k}(\mathbb{G}_m)$ has the Chevalley module $J_{G/H}$ as its character module and the field $L(J_{G/H})^G$ as its function field where $J_{G/H} = (I_{G/H})^\circ = \mathrm{Hom}_{\mathbb{Z}}(I_{G/H}, \mathbb{Z})$ is the dual lattice of $I_{G/H} = \mathrm{Ker}\ \varepsilon$ and $\varepsilon : \mathbb{Z}[G/H] \to \mathbb{Z}$ is the augmentation map (see [Vos98, Section 4.8]). We have the exact sequence $0 \to \mathbb{Z} \to \mathbb{Z}[G/H] \to J_{G/H} \to 0$ and $\mathrm{rank}_{\mathbb{Z}}(J_{G/H}) = n-1$. Write $J_{G/H} = \bigoplus_{1\le i\le n-1} \mathbb{Z}x_i$. Then the action of G on $L(J_{G/H}) = L(x_1, \ldots, x_{n-1})$ is of the form (1).

Let K be a finitely generated field extension of a field k. A field K is called *rational over* k (or k*-rational* for short) if K is purely transcendental over k, i.e., K is isomorphic to $k(x_1, \ldots, x_n)$, the rational function field over k with n variables $x_1, \ldots, x_n$ for some integer n. K is called *stably* k*-rational* if $K(y_1, \ldots, y_m)$ is k-rational for some algebraically independent elements $y_1, \ldots, y_m$ over K. Two fields K and K' are called *stably* k*-isomorphic* if $K(y_1, \ldots, y_m) \simeq K'(z_1, \ldots, z_n)$ over k for some algebraically independent elements $y_1, \ldots, y_m$ over K and $z_1, \ldots, z_n$ over K'. When k is an infinite field, K is called *retract* k*-rational* if there is a k-algebra R contained in K such that (i) K is the quotient field of R, and (ii) the identity map $1_R : R \to R$ factors through a localized polynomial ring over k, i.e., there is an element $f \in k[x_1, \ldots, x_n]$, which is the polynomial ring over k, and there are k-algebra homomorphisms $\varphi : R \to k[x_1, \ldots, x_n][1/f]$ and $\psi : k[x_1, \ldots, x_n][1/f] \to R$ satisfying $\psi\circ\varphi = 1_R$ (cf. [Sal84]). K is called k*-unirational* if $k \subset K \subset k(x_1, \ldots, x_n)$ for some integer n. It is not difficult to see that "k-rational" $\Rightarrow$ "stably k-rational" $\Rightarrow$ "retract k-rational" $\Rightarrow$ "k-unirational".

The 1-dimensional algebraic k-tori, i.e., the trivial torus $\mathbb{G}_m$ and the norm one torus $R^{(1)}_{K/k}(\mathbb{G}_m)$ with $[K : k] = 2$, are k-rational. Voskresenskii [Vos67] showed that all the 2-dimensional algebraic k-tori are k-rational. Kunyavskii [Kun90] classifies rational (resp., stably rational, retract rational) algebraic k-tori in dimension 3. Hoshi and Yamasaki [HY17, Theorem 1.9, Theorem 1.12] classify stably rational (resp., retract rational) algebraic k-tori in dimensions 4 and 5.

Let S_n (resp., A_n, D_n, C_n) be the symmetric (resp., the alternating, the dihedral, the cyclic) group of degree n of order $n!$ (resp., $n!/2$, $2n$, n). Let $F_{pm} \simeq C_p \rtimes C_m \le S_p$ be the Frobenius group of order pm where $m \mid p-1$. Let nTm be the mth transitive subgroup of S_n (see Butler and McKay [BM83] for $n \le 11$, Royle [Roy87] for $n = 12$, Butler [But93] for $n = 14, 15$, and [GAP]).

The rationality problem for norm one tori $R^{(1)}_{K/k}(\mathbb{G}_m)$ is investigated by [EM75], [CTS77], [Hür84], [CTS87], [LeB95], [CK00], [LL00], [Flo], [End11], [HY17], and [HY]. In the previous papers [HY17] and [HY], a classification of stably/retract rational norm one tori $R^{(1)}_{K/k}(\mathbb{G}_m)$ in dimension $p-1$ where p is a prime number and in dimension $n \le 10$ is given except for the following three cases: (i) $G = \mathrm{PSL}_2(\mathbb{F}_{2^e})$ where $p = 2^e + 1 \ge 17$ is a Fermat prime; (ii) $G = 9T27 \simeq \mathrm{PSL}_2(\mathbb{F}_8)$; (iii) $G = 10T11 \simeq A_5 \times C_2$.

The first main results of this paper are Theorems 1.1 and 1.2 which classify stably/retract rational norm one tori $R^{(1)}_{K/k}(\mathbb{G}_m)$ in dimension $n-1$ for $n = 2^e$ ($e \ge 1$) and $n = 10, 12, 14, 15$. Note that there exist 45 (resp., 301, 63, 104) transitive groups $10Tm$ (resp., $12Tm$, $14Tm$, $15Tm$) of degree 10 (resp., 12, 14, 15). The case $n=10$ in Theorem 1.2(1) was solved by [HY, Theorem 1.11] except for $G = 10T11 \simeq A_5 \times C_2$.

Theorem 1.1. *Let K/k be a separable field extension of degree n and let L/k be the Galois closure of K/k. Let $G = \mathrm{Gal}(L/k)$ be a transitive subgroup of S_n where $n = 2^e$ $(e \geq 1)$ and $H = \mathrm{Gal}(L/K)$ with $[G : H] = n$. Then $R^{(1)}_{K/k}(\mathbb{G}_m)$ is stably k-rational if and only if $G \simeq C_n$. Moreover, if $R^{(1)}_{K/k}(\mathbb{G}_m)$ is not stably k-rational, then it is not retract k-rational.*

Theorem 1.2. *Let K/k be a separable field extension of degree n and let L/k be the Galois closure of K/k. Let $G = \mathrm{Gal}(L/k)$ be a transitive subgroup of S_n and $H = \mathrm{Gal}(L/K)$ with $[G : H] = n$. Then a classification of stably/retract rational norm one tori $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ in dimension $n-1$ for $n = 10, 12, 14, 15$ is given as follows:*

(1) *The case* $10Tm$ $(1 \leq m \leq 45)$.
 (i) *T is stably k-rational for $10T1 \simeq C_{10}$, $10T2 \simeq D_5$, $10T3 \simeq D_{10}$, $10T11 \simeq A_5 \times C_2$;*
 (ii) *T is not stably but retract k-rational for $10T4 \simeq F_{20}$, $10T5 \simeq F_{20} \times C_2$, $10T12 \simeq S_5$, $10T22 \simeq S_5 \times C_2$;*
 (iii) *T is not retract k-rational for $10Tm$ with $6 \leq m \leq 45$ and $m \neq 11, 12, 22$.*

(2) *The case* $12Tm$ $(1 \leq m \leq 301)$.
 (i) *T is stably k-rational for $12T1 \simeq C_{12}$, $12T5 \simeq C_3 \rtimes C_4$, $12T11 \simeq C_4 \times S_3$;*
 (ii) *T is not retract k-rational for $12Tm$ with $1 \leq m \leq 301$ and $m \neq 1, 5, 11$.*

(3) *The case* $14Tm$ $(1 \leq m \leq 63)$.
 (i) *T is stably k-rational for $14T1 \simeq C_{14}$, $14T2 \simeq D_7$, $14T3 \simeq D_{14}$;*
 (ii) *T is not stably k-rational but retract k-rational for $14T4 \simeq F_{42}$, $14T5 \simeq F_{21} \times C_2$, $14T7 \simeq F_{42} \times C_2$, $14T16 \simeq \mathrm{PSL}_3(\mathbb{F}_2) \rtimes C_2$, $14T19 \simeq \mathrm{PSL}_3(\mathbb{F}_2) \times C_2$, $14T46 \simeq S_7$, $14T47 \simeq A_7 \times C_2$, $14T49 \simeq S_7 \times C_2$;*
 (iii) *T is not retract k-rational for $14Tm$ with $6 \leq m \leq 63$ and $m \neq 7, 16, 19, 46, 47, 49$.*

(4) *The case* $15Tm$ $(1 \leq m \leq 104)$.
 (i) *T is stably k-rational for $15T1 \simeq C_{15}$, $15T2 \simeq D_{15}$, $15T3 \simeq D_5 \times C_3$, $15T4 \simeq S_3 \times C_5$, $15T5 \simeq A_5$, $15T7 \simeq D_5 \times S_3$ $15T16 \simeq A_5 \times C_3 \simeq \mathrm{GL}_2(\mathbb{F}_4)$, $15T23 \simeq A_5 \times S_3$;*
 (ii) *T is not stably k-rational but retract k-rational for $15T6 \simeq C_{15} \rtimes C_4$, $15T8 \simeq F_{20} \times C_3$, $15T10 \simeq S_5$, $15T11 \simeq F_{20} \times S_3$, $15T22 \simeq (A_5 \times C_3) \rtimes C_2 \simeq \mathrm{GL}_2(\mathbb{F}_4) \rtimes C_2$, $15T24 \simeq S_5 \times C_3$, $15T29 \simeq S_5 \times S_3$;*
 (iii) *T is not retract k-rational for $15Tm$ with $9 \leq m \leq 104$ and $m \neq 10, 11, 16, 22, 23, 24, 29$.*

The second main result of this paper is the following.

Theorem 1.3. *Let K/k be a separable field extension of degree n and let L/k be the Galois closure of K/k. Let $G = \mathrm{Gal}(L/k)$ be a transitive subgroup of S_n and $H = \mathrm{Gal}(L/K)$ with $[G : H] = n$. Assume that $n = q+1$ where $q = l^e \equiv 1 \pmod 4$*

is an odd prime power and $\mathrm{PSL}_2(\mathbb{F}_q) \leq G \leq \mathrm{P\Gamma L}_2(\mathbb{F}_q) \simeq \mathrm{PGL}_2(\mathbb{F}_q) \rtimes C_e$. *Then* $R^{(1)}_{K/k}(\mathbb{G}_m)$ *is not retract k-rational.*

As a consequence of Theorem 1.3, we will show Theorem 1.4 which gives a classification of stably/retract rational norm one tori $R^{(1)}_{K/k}(\mathbb{G}_m)$ in dimension $n-1$ where $n = 2p$, p is a prime number and $G = \mathrm{Gal}(L/k) \leq S_{2p}$ is primitive.

Theorem 1.4. *Let p be a prime number, let K/k be a separable field extension of degree $2p$, and let L/k be the Galois closure of K/k. Assume that $G = \mathrm{Gal}(L/k)$ is a primitive subgroup of S_{2p} and $H = \mathrm{Gal}(L/K)$ with $[G : H] = 2p$. Then $R^{(1)}_{K/k}(\mathbb{G}_m)$ is not retract k-rational.*

More precisely, $R^{(1)}_{K/k}(\mathbb{G}_m)$ is not retract k-rational for the following primitive groups $G \leq S_{2p}$:

(i) $G = S_{2p}$ *or* $G = A_{2p} \leq S_{2p}$;
(ii) $G = S_5 \leq S_{10}$ *or* $G = A_5 \leq S_{10}$;
(iii) $G = M_{22} \leq S_{22}$ *or* $G = \mathrm{Aut}(M_{22}) \simeq M_{22} \rtimes C_2 \leq S_{22}$ *where* M_{22} *is the Mathieu group of degree 22;*
(iv) $\mathrm{PSL}_2(\mathbb{F}_q) \leq G \leq \mathrm{P\Gamma L}_2(\mathbb{F}_q) \simeq \mathrm{PGL}_2(\mathbb{F}_q) \rtimes C_e$ *where* $2p = q + 1$ *and* $q = l^e$ *is an odd prime power.*

Remark 1.5. For the reader's convenience, we give a list of non-solvable primitive groups $G = nTm \leq S_n$ of degree $n = 10, 12, 14, 15$:

(i) $10T7 \simeq A_5$, $10T13 \simeq S_5$, $10T26 \simeq \mathrm{PSL}_2(\mathbb{F}_9) \simeq A_6$, $10T30 \simeq \mathrm{PGL}_2(\mathbb{F}_9)$, $10T31 \simeq M_{10}$, $10T32 \simeq S_6$, $10T35 \simeq \mathrm{P}\Gamma L_2(\mathbb{F}_9)$, $10T44 \simeq A_{10}$, $10T45 \simeq S_{10}$.
(ii) $12T179 \simeq \mathrm{PSL}_2(\mathbb{F}_{11})$, $12T218 \simeq \mathrm{PGL}_2(\mathbb{F}_{11})$, $12T272 \simeq M_{11}$, $12T295 \simeq M_{12}$, $12T300 \simeq A_{12}$, $12T301 \simeq S_{12}$.
(iii) $14T30 \simeq \mathrm{PSL}_2(\mathbb{F}_{13})$, $14T39 \simeq \mathrm{PGL}_2(\mathbb{F}_{13})$, $14T62 \simeq A_{14}$, $14T63 \simeq S_{14}$.
(iv) $15T20 \simeq A_6$, $15T28 \simeq S_6$, $15T47 \simeq A_7$, $15T72 \simeq A_8 \simeq \mathrm{PSL}_4(\mathbb{F}_2)$, $15T103 \simeq A_{15}$, $15T104 \simeq S_{15}$.

We also give the following result for the five Mathieu groups $M_n \leq S_n$ where $n = 11, 12, 22, 23, 24$:

Theorem 1.6. *Let K/k be a separable field extension of degree n and let L/k be the Galois closure of K/k. Let $G = \mathrm{Gal}(L/k)$ be a transitive subgroup of S_n and $H = \mathrm{Gal}(L/K)$ with $[G : H] = n$. Assume that $n = 11$, 12, 22, 23, or 24 and G is isomorphic to the Mathieu group M_n of degree n. Then $R^{(1)}_{K/k}(\mathbb{G}_m)$ is not retract k-rational.*

We organize this paper as follows. In Section 2, we prepare some basic tools to prove stably/retract rationality of algebraic tori. In Section 3, we will give the proof of Theorem 1.1. In Section 4, we will give the proof of Theorem 1.2. Finally, we give the proof of Theorems 1.3, 1.4, and 1.6 in Section 5.

We note that the proofs of Theorems 1.2, 1.4, and 1.6 are given by applying GAP algorithms which are available from `https://www.math.kyoto-u.ac.jp/~yamasaki/Algorithm/RatProbNorm1Tori/` although the proofs of Theorems 1.1 and 1.3 are given by a purely algebraic way.

2. Preliminaries: Rationality problem for algebraic tori and flabby resolution

We recall some basic facts of the theory of flabby (flasque) G-lattices (see Colliot-Thélène and Sansuc [CTS77], Swan [Swa83], Voskresenskii [Vos98, Chapter 2], Lorenz [Lor05, Chapter 2], and Swan [Swa10]).

Definition 2.1. Let G be a finite group and let M be a G-lattice (i.e., finitely generated $\mathbb{Z}[G]$-module which is $\mathbb{Z}$-free as an abelian group).

(i) M is called a *permutation* G-lattice if M has a $\mathbb{Z}$-basis permuted by G, i.e., $M \simeq \bigoplus_{1\le i\le m} \mathbb{Z}[G/H_i]$ for some subgroups $H_1, \ldots, H_m$ of G.
(ii) M is called a *stably permutation* G-lattice if $M \oplus P \simeq P'$ for some permutation G-lattices P and P'.
(iii) M is called *invertible* (or *permutation projective*) if it is a direct summand of a permutation G-lattice, i.e., $P \simeq M \oplus M'$ for some permutation G-lattice P and a G-lattice M'.
(iv) M is called *flabby* (or *flasque*) if $\widehat{H}^{-1}(H, M) = 0$ for any subgroup H of G where $\widehat{H}$ is the Tate cohomology.
(v) M is called *coflabby* (or *coflasque*) if $H^1(H, M) = 0$ for any subgroup H of G.

Lemma 2.2 (Lenstra [Len74, Propositions 1.1 and 1.2]; see also Swan [Swa83, Section 8])**.** *Let E be an invertible G-lattice.*

(i) *E is flabby and coflabby.*
(ii) *If C is a coflabby G-lattice, then any short exact sequence $0 \to C \to N \to E \to 0$ splits.*

Definition 2.3 (see [EM75, Section 1], [Vos98, Section 4.7])**.** Let $\mathcal{C}(G)$ be the category of all G-lattices. Let $\mathcal{S}(G)$ be the full subcategory of $\mathcal{C}(G)$ of all permutation G-lattices and let $\mathcal{D}(G)$ be the full subcategory of $\mathcal{C}(G)$ of all invertible G-lattices. Let

$$\mathcal{H}^i(G) = \{M \in \mathcal{C}(G) \mid \widehat{H}^i(H, M) = 0 \text{ for any } H \le G\} \ (i = \pm 1)$$

be the class of "$\widehat{H}^i$-vanish" G-lattices where $\widehat{H}^i$ is the Tate cohomology. Then we have the inclusions $\mathcal{S}(G) \subset \mathcal{D}(G) \subset \mathcal{H}^i(G) \subset \mathcal{C}(G)$ $(i = \pm 1)$.

Definition 2.4. We say that two G-lattices M_1 and M_2 are *similar* if there exist permutation G-lattices P_1 and P_2 such that $M_1 \oplus P_1 \simeq M_2 \oplus P_2$. We denote the similarity class of M by $[M]$. The set of similarity classes $\mathcal{C}(G)/\mathcal{S}(G)$ becomes a commutative monoid (with respect to the sum $[M_1] + [M_2] := [M_1 \oplus M_2]$ and the zero $0 = [P]$ where $P \in \mathcal{S}(G)$).

Theorem 2.5 (Endô and Miyata [EM75, Lemma 1.1], Colliot-Thélène and Sansuc [CTS77, Lemma 3]; see also [Swa83, Lemma 8.5], [Lor05, Lemma 2.6.1])**.** *For any G-lattice M, there exists a short exact sequence of G-lattices $0 \to M \to P \to F \to 0$ where P is permutation and F is flabby.*

Definition 2.6. The exact sequence $0 \to M \to P \to F \to 0$ as in Theorem 2.5 is called a *flabby resolution* of the G-lattice M. $\rho_G(M) = [F] \in \mathcal{C}(G)/\mathcal{S}(G)$ is called *the flabby class* of M, denoted by $[M]^{fl} = [F]$. Note that $[M]^{fl}$ is well-defined: if $[M] = [M']$, $[M]^{fl} = [F]$, and $[M']^{fl} = [F']$, then $F \oplus P_1 \simeq F' \oplus P_2$ for some permutation G-lattices P_1 and P_2, and therefore $[F] = [F']$ (cf. [Swa83, Lemma 8.7]). We say that $[M]^{fl}$ is *invertible* if $[M]^{fl} = [E]$ for some invertible G-lattice E.

For G-lattice M, it is not difficult to see

$$\begin{array}{ccccccc} \text{permutation} & \Rightarrow & \text{stably permutation} & \Rightarrow & \text{invertible} & \Rightarrow & \text{flabby and coflabby} \\ & & \Downarrow & & \Downarrow & & \\ & & [M]^{fl} = 0 & \Rightarrow & [M]^{fl} \text{ is invertible.} & & \end{array}$$

The above implications in each step cannot be reversed (see, for example, [HY17, Section 1]).

Let L/k be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/k)$ and let M be a G-lattice. The flabby class $\rho_G(M) = [M]^{fl}$ plays a crucial role in the rationality problem for $L(M)^G$ as follows (see Voskresenskii's fundamental book [Vos98, Section 4.6] and Kunyavskii [Kun07]; see also, e.g., Swan [Swa83], Kunyavskii [Kun90, Section 2], Lemire, Popov, and Reichstein [LPR06, Section 2], Kang [Kan12], and Yamasaki [Yam12]).

Theorem 2.7 (Endô and Miyata, Voskresenskii, Saltman)**.** *Let L/k be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/k)$. Let M and M' be G-lattices.*

(i) (Endô and Miyata [EM73, Theorem 1.6]). *$[M]^{fl} = 0$ if and only if $L(M)^G$ is stably k-rational.*

(ii) (Voskresenskii [Vos74, Theorem 2]). *$[M]^{fl} = [M']^{fl}$ if and only if $L(M)^G$ and $L(M')^G$ are stably k-isomorphic.*

(iii) (Saltman [Sal84, Theorem 3.14]). *$[M]^{fl}$ is invertible if and only if $L(M)^G$ is retract k-rational.*

Lemma 2.8 (Swan [Swa10, Lemma 3.1])**.** *Let $0 \to M_1 \to M_2 \to M_3 \to 0$ be a short exact sequence of G-lattices with M_3 invertible. Then the flabby class $[M_2]^{fl} = [M_1]^{fl} + [M_3]^{fl}$. In particular, if $[M_1]^{fl}$ is invertible, then $-[M_1]^{fl} = [[M_1]^{fl}]^{fl}$.*

Definition 2.9. Let G be a finite subgroup of $\mathrm{GL}_n(\mathbb{Z})$. *The G-lattice M_G with* $\mathrm{rank}_{\mathbb{Z}}(M_G) = n$ is defined to be the G-lattice with a $\mathbb{Z}$-basis $\{u_1, \ldots, u_n\}$ on which G acts by $\sigma(u_i) = \sum_{j=1}^{n} a_{i,j} u_j$ for any $\sigma = [a_{i,j}] \in G$.

Lemma 2.10 (see [CTS77, Remarque R2, page 180], [HY17, Lemma 2.17])**.** *Let G be a finite subgroup of $\mathrm{GL}_n(\mathbb{Z})$ and let M_G be the corresponding G-lattice as in Definition* 2.9. *Let $H \leq G$ and $\rho_H(M_H)$ be the flabby class of M_H as an H-lattice.*

(i) *If $\rho_G(M_G) = 0$, then $\rho_H(M_H) = 0$.*

(ii) *If $\rho_G(M_G)$ is invertible, then $\rho_H(M_H)$ is invertible.*

3. Proof of Theorem 1.1

In order to prove Theorem 1.1, we show the following two theorems.

Theorem 3.1. *Let $n = p^e$ be a prime power and let G be a transitive subgroup of S_n. Let $G_p = \mathrm{Syl}_p(G)$ be a p-Sylow subgroup of G. Then G_p is a transitive subgroup of S_n.*

Proof. Let H be the stabilizer of one of the letters in G and let H_p be a p-Sylow subgroup of H with $H_p \leq G_p$. Because $[G : H] = n$ and p does not divide both $[H : H_p]$ and $[G : G_p]$, we have $[G_p : H_p] = n = p^e$. Hence $H_p = G_p \cap H$ becomes the stabilizer of one of the letters in G_p and $G_p \leq S_n$ is transitive. $\square$

Theorem 3.2. *Let $n = 2^e$ be a power of 2 and let G be a transitive subgroup of S_n. Let $G_2 = \mathrm{Syl}_2(G)$ be a 2-Sylow subgroup of G. If $G_2 \simeq C_n$, then $G \simeq C_n$.*

Proof. Let H be the stabilizer of one of the letters in G. We should show that $H = 1$ because $[G : H] = n$. We will prove $H = 1$ by induction in e. When $e = 1$, the assertion holds. For e, we assume that $G_2 = \langle\sigma\rangle \simeq C_n$ where $n = 2^e$. Without loss of generality, we may assume that $\sigma = (1 \cdots n) \in S_n$.

There exist $(n-1)!$ elements of order n in S_n which are conjugate in S_n. Let $Z_{S_n}(G_2)$ be the centralizer of G_2 in S_n and let$N_{S_n}(G_2)$ be the normalizer of G_2 in S_n. Then we see that $Z_{S_n}(G_2) = G_2 \simeq C_n$ and $N_{S_n}(G_2) = C_n \rtimes \mathrm{Aut}(C_n) \simeq \mathbb{Z}/2^e\mathbb{Z} \rtimes (\mathbb{Z}/2^e\mathbb{Z})^\times$. We also have $G_2 = Z_G(G_2) \leq N_G(G_2) \leq G$. Because $N_G(G_2)$ is also a 2-group, we obtain that $Z_G(G_2) = N_G(G_2) = G_2$.

Let $A = \{x \in G \mid \mathrm{ord}(x) = n\}$ be the set of elements of order n in G and let $A_2 = \{x \in G_2 \mid \mathrm{ord}(x) = n\} = \{\sigma^i \mid i\text{: odd}\}$ be the set of elements of order n in G_2. If $g \in G_2$, then $gag^{-1} = a$ for any $a \in A_2$. If $g \in G \setminus G_2$, then $gA_2g^{-1} \cap A_2 = \emptyset$ because $N_G(G_2) = G_2$. Note that $g_1A_2g_1^{-1} = g_2A_2g_2^{-1}$ if and only if $g_2^{-1}g_2 \in G_2$. Hence we have $|A| = |A_2| \cdot [G : G_2] = 2^{e-1} \cdot |H| = |G|/2$. This implies that $A = \{x \in G \mid \mathrm{sgn}(x) = -1\}$.

We claim that if $h(j) = k$ $(h \in H)$, then $j \equiv k \pmod 2$. Suppose not. Then there exists $\sigma^{j-k} \in A_2$ such that $\sigma^{j-k}h(j) = j$. But this is impossible because $\mathrm{sgn}(\sigma^{j-k}h) = -1$ and hence $\mathrm{ord}(\sigma^{j-k}h) = n$. This claim implies that $\langle\sigma^2, H\rangle$ acts on $2\mathbb{Z}/n\mathbb{Z} = \{2, 4, \ldots, n\}$.

On the other hand, $\langle\sigma^2, H\rangle \leq G \cap A_n$ because $\mathrm{sgn}(\sigma^2) = \mathrm{sgn}(h) = 1$ $(h \in H)$. We also see $\langle\sigma^2, H\rangle = G \cap A_n$ because $[\langle\sigma^2, H\rangle : H] = n/2$.

Remember that $|H| = [G : G_2]$ is odd. The restriction $G \cap A_n|_{2\mathbb{Z}/n\mathbb{Z}}$ of $G \cap A_n$ into $2\mathbb{Z}/n\mathbb{Z}$ seems to be a transitive subgroup of $S_{2\mathbb{Z}/n\mathbb{Z}} = S_{\{2,4,\ldots,n\}}$ whose 2-Sylow subgroup is $\langle\sigma^2\rangle|_{2\mathbb{Z}/n\mathbb{Z}}$. By the assumption of induction, we have $H|_{2\mathbb{Z}/n\mathbb{Z}} = 1$. Similarly, we get $H|_{1+2\mathbb{Z}/n\mathbb{Z}} = 1$. Therefore, we conclude that $H = 1$. $\square$

Proof of Theorem 1.1. Take a transitive subgroup $G = \mathrm{Gal}(L/k) \leq S_n$ $(n = 2^e)$ and $H = \mathrm{Gal}(L/K)$ with $[G : H] = n$. By Theorem 3.1, the 2-Sylow subgroup $G_2 = \mathrm{Syl}_2(G)$ of G is a transitive subgroup of S_n.

($\Rightarrow$) Assume that $G \not\simeq C_n$. By Theorem 3.2, we have $G_2 \not\simeq C_n$. Hence $[J_{G_2/H_2}]^{fl}$ is not invertible by Endô and Miyata [EM75, Theorem 1.5] and Endô [End11, Theorem 2.1] where H_2 is the 2-Sylow subgroup of H. Because G_2 is transitive in S_n, it follows from Lemma 2.10(ii) that $[J_{G/H}]^{fl}$ is not invertible. Hence $R^{(1)}_{K/k}(\mathbb{G}_m)$ is not retract k-rational.

($\Leftarrow$) By Endô and Miyata [EM75, Theorem 2.3], if $G \simeq C_n$, then $R^{(1)}_{K/k}(\mathbb{G}_m)$ is stably k-rational. $\square$

Example 3.3 (The case $nTm \leq S_n$ where $n = 2^e$)**.** (1) When $n = 4$, there exist 5 transitive subgroups $4Tm \leq S_4$ $(1 \leq m \leq 5)$: $4T1 \simeq C_4$, $4T2 \simeq C_2 \times C_2$, $4T3 \simeq D_4$, $4T4 \simeq A_4$, $4T5 \simeq S_4$.

(2) When $n = 8$, there exist 50 transitive subgroups of $8Tm \leq S_8$ $(1 \leq m \leq 50)$. There exist 5 groups $G = 8Tm$ $(1 \leq m \leq 5)$ with $|G| = 8$ (see Butler and McKay [BM83], [GAP]): $8T1 \simeq C_8$, $8T2 \simeq C_4 \times C_2$, $8T3 \simeq (C_2)^3$, $8T4 \simeq D_4$, $8T5 \simeq Q_8$.

(3) When $n = 16$, there exist 1954 transitive subgroups of $16Tm \leq S_{16}$ $(1 \leq m \leq 1954)$. There exist 14 groups $G = 16Tm$ $(1 \leq m \leq 14)$ with $|G| = 16$ (see [HHY, Example 3.4]): $16T1 \simeq C_{16}$, $16T2 \simeq C_4 \times (C_2)^2$, $16T3 \simeq (C_2)^4$, $16T5 \simeq C_4 \times C_4$, $16T5 \simeq C_8 \times C_2$, $16T6 \simeq M_{16}$, $16T7 \simeq Q_8 \times C_2$, $16T8 \simeq C_4 \rtimes C_4$,

$16T9 \simeq D_4 \times C_2$, $16T10 \simeq (C_4 \times C_2) \rtimes C_2$, $16T11 \simeq (C_4 \times C_2) \rtimes C_2$, $16T12 \simeq QD_8$, $16T13 \simeq D_8$, $16T14 \simeq Q_{16}$.

(4) When $n = 32$, there exist 2801324 transitive subgroups of $32Tm \leq S_{32}$ $(1 \leq m \leq 2801324)$ (see Cannon and Holt [CH08]).

4. Proof of Theorem 1.2

Let K/k be a separable field extension of degree n and let L/k be the Galois closure of K/k. Let $G = \mathrm{Gal}(L/k)$ be a transitive subgroup of S_n and $H = \mathrm{Gal}(L/K)$ with $[G : H] = n$. We may assume that H is the stabilizer of one of the letters in G, i.e., $L = k(\theta_1, \ldots, \theta_n)$ and $K = L^H = k(\theta_i)$ where $1 \leq i \leq n$.

Let nTm be the mth transitive subgroup of S_n (see Butler and McKay [BM83] for $n \leq 11$, Royle [Roy87] for $n = 12$, Butler [But93] for $n = 14, 15$, and [GAP]).

We provide the following GAPalgorithm to certify whether $F = [J_{G/H}]^{fl}$ is invertible (resp., zero) (see also Hoshi and Yamasaki [HY17, Chapter 5]). Some related programs are available from `https://www.math.kyoto-u.ac.jp/~yamasaki/Algorithm/RatProbNorm1Tori/`.

Algorithm 4.1 (see Hoshi and Yamasaki [HY17, Chapter 5 and Chapter 8])**.**

(0) Construction of the Chevalley module $J_{G/H}$ (see [HY17, Chapter 8]):

`Norm1TorusJ(`n, m`)` returns $J_{G/H}$ for $G = nTm \leq S_n$ and H is the stabilizer of one of the letters in G.

(1) Whether $F = [J_{G/H}]^{fl}$ is invertible:

`IsInvertibleF(Norm1TorusJ(`n, m`))` returns true (resp., false) if $[J_{G/H}]^{fl}$ is invertible (resp., not invertible) for $G = nTm \leq S_n$ and H is the stabilizer of one of the letters in G (see [HY17, Section 5.2]).

(2) Possibility for $F = 0$ where $F = [J_{G/H}]^{fl}$:

`PossibilityOfStablyPermutationF(Norm1TorusJ(`m, n`))` returns a basis $\mathcal{L} = \{l_1, \ldots, l_s\}$ of possible solutions space $\{(a_1, \ldots, a_r, b_1)\}$ $(a_i, b_1 \in \mathbb{Z})$ (see also [HY17, Section 5.4]) to

$$\bigoplus_{i=1}^{r} \mathbb{Z}[G/H_i]^{\oplus a_i} \ \simeq \ F^{\oplus(-b_1)}$$

for $G = mTn \leq S_n$, H is the stabilizer of one of the letters in G and $F = [J_{G/H}]^{fl}$. In particular, if all the b_1's are even, then we can conclude that $F = [J_{G/H}]^{fl} \neq 0$.

(3) Verification of $F = 0$ where $F = [J_{G/H}]^{fl}$:

`FlabbyResolutionLowRankFromGroup((Norm1TorusJ(`n, m`)TransitiveGroup(`n, m`)).actionF` returns a suitable flabby class $F = [J_{G/H}]^{fl}$ of $J_{G/H}$ with low rank for $G = nTm \leq S_n$ and H is the stabilizer of one of the letters in G by using the backtracking techniques. Repeating the algorithm, by defining $[J_{G/H}]^{fl^n} := [[J_{G/H}]^{fl^{n-1}}]^{fl}$ inductively, $[J_{G/H}]^{fl} = 0$ is provided if we may find some n with $[J_{G/H}]^{fl^n} = 0$ (this method is slightly improved to the `flfl` algorithm; see [HY17, Section 5.3]).

Proof of Theorem 1.2*.* We may assume that H is the stabilizer of one of the letters in G (see the first paragraph of Section 4).

(1) The case $10Tm$ $(1 \leq m \leq 45)$.

By [HY, Theorem 1.11], we should show that T is stably k-rational for $10T11 \simeq A_5 \times C_2$. For $10T11$, by Algorithm 4.1(3), we may take $F = [J_{G/H}]^{fl}$ with

$\mathrm{rank}_{\mathbb{Z}}(F)=31$, $F'=[F]^{fl}$ with $\mathrm{rank}_{\mathbb{Z}}(F')=13$ and $F''=[F']^{fl}$ with $F''=[\mathbb{Z}]=0$. This implies that $F=0$ and hence T is stably k-rational (see [HHY, Example 4.2]).

(2) The case $12Tm$ $(1\leq m\leq 301)$.

(2-1) The case where K/k is Galois: $1\leq m\leq 5$. For $12T1\simeq C_{15}$, $12T2\simeq C_6\times C_2$, $12T3\simeq D_6$, $12T4\simeq A_4$, $12T5\simeq C_3\rtimes C_4$, K/k is a Galois extension. By Endô and Miyata [EM75, Theorem 2.3], T is stably k-rational for $12T1$, $12T5$. By Endô and Miyata [EM75, Theorem 1.5], T is not retract k-rational for $12T2$, $12T3$, $12T4$.

(2-2) The case where K/k is not Galois: $6\leq m\leq 301$.

Case 1 $(m=11)$. For $12T11\simeq C_4\times S_3$, by Algorithm 4.1(3), we may take $F=[J_{G/H}]^{fl}$ with $\mathrm{rank}_{\mathbb{Z}}(F)=17$, $F'=[F]^{fl}$ with $\mathrm{rank}_{\mathbb{Z}}(F')=4$ and F' is permutation. This implies that $F=0$ and hence T is stably k-rational (see [HHY, Example 4.3]). (We note that $12T1\leq 12T5\leq 12T11$.)

Case 2 $(m\neq 11)$. By using the command `List([1..301],x->Filtered([1..x], y->IsSubgroup(TransitiveGroup(12,x), TransitiveGroup(12,y))))` in GAP [GAP] (see also [HHY, Example 4.4] for the case where $n=14$), we obtain the inclusions $12Tm\leq 12Tm'$ among the groups $G=12Tm$ with minimal groups $12Tm$ where $m\in I_{12}:=\{2,3,4,7,8,9,12,15,16,17,19,29,30,31,32,33,34,36,40,41,46,47,57,58,59,60,61,63,64,65,66,68,69,70,73,74,75,76,89,91,93,96,99,100,102,105,107,160,162,166,171,172,173,179,181,182,183,207,212,216,246,254,272,278,295\}$.

By using the command
`Filtered(List(ConjugacyClassesSubgroups(TransitiveGroup(12,`m`)),] Representative), x->Length(Orbits(x,[1..12]))=1)`, we also see the following inclusions for $12Tm$ with $m\in I_0:=\{207,212,216,254,272,278,295\}$ (see [HHY, Example 4.3], we may reduce these cases which take more computational time and resources):

$12T166\leq 12T207, 12T254$,
$12T46\leq 12T212, 12T216, 12T272$,
$12T17\leq 12T278$,
$12T2\leq 12T295$.

By the inclusion of $G=12Tm$ above and Lemma 2.10(ii), it is enough to check that $[J_{G/H}]^{fl}$ is not invertible for $I_{12}\setminus I_0$. By Algorithm 4.1(1), we obtain that $[J_{G/H}]^{fl}$ is not invertible and hence, by Theorem 2.7(iii), T is not retract k-rational for $m\in I_{12}\setminus I_0$ (see [HHY, Example 4.3]).

(3) The case $14Tm$ $(1\leq m\leq 63)$.

(3-1) The case where K/k is Galois: $m=1,2$. For $14T1\simeq C_{14}$ and $14T2\simeq D_7$, K/k is a Galois extension. By Endô and Miyata [EM75, Theorem 2.3], T is stably k-rational for $14T1$ and $14T2$.

(3-2) The case where K/k is not Galois: $3\leq m\leq 63$.

Case 1 $(m=3)$. For $14T3\simeq D_{14}$, by Algorithm 4.1(1), we obtain that $[J_{G/H}]^{fl}$ is invertible and hence T is retract k-rational by Theorem 2.7(iii). By Algorithm 4.1(3), we may take $F=[J_{G/H}]^{fl}$ with $\mathrm{rank}_{\mathbb{Z}}(F)=17$ and $F'=[F]^{fl}=\mathbb{Z}^2$ which is permutation. This implies that $F=0$ and hence T is stably k-rational by Theorem 2.7(i) (see [HHY, Example 4.4]).

Case 2 ($m=4,5,7,16,19,46,47,49$). By Algorithm 4.1(1), we see that $[J_{G/H}]^{fl}$ is invertible and hence T is retract k-rational by Theorem 2.7(iii) for $m=4,5,7,16,19,46,47,49$. For $m=4,5,16$, by Algorithm 4.1(2), we see that $[J_{G/H}]^{fl}\neq 0$ and hence T is not stably k-rational (see [HHY, Example 4.4]). By Lemma 2.10(i) and the inclusions $14T4\leq 14T7, 14T46$ and $14T5\leq 14T19\leq 14T47\leq 14T49$, we have $[J_{G/H}]^{fl}\neq 0$ and hence T is also not stably k-rational for $m=7,19,46,47,49$.

Case 3 ($6\leq m\leq 63$ and $m\neq 7,16,19,46,47,49$). By using the command `List([1..63],x->Filtered([1..x],y->IsSubgroup(TransitiveGroup(14,x), TransitiveGroup(14,y))))` in GAP [GAP] (see [HHY, Example 4.4]), we get the inclusions $14Tm\leq 14Tm'$ among the groups $G=14Tm$ with minimal groups $14Tm$ where $m\in I_{14}:=\{6,8,10,12,26,30\}$.

By the inclusion of $G=14Tm$ above and Lemma 2.10(ii), it is enough to show that $[J_{G/H}]^{fl}$ is not invertible for $m\in I_{14}$. By Algorithm 4.1(1), we see that $[J_{G/H}]^{fl}$ is not invertible and hence T is not retract k-rational for $m\in I_{14}$ (see [HHY, Example 4.4]).

(4) The case $15Tm$ ($1\leq m\leq 104$).

(4-1) The case where K/k is Galois: $m=1$. For $15T1\simeq C_{15}$, K/k is a Galois extension. It follows from Endô and Miyata [EM75, Theorem 2.3] that T is stably k-rational for $15T1$.

(4-2) The case where K/k is not Galois: $2\leq m\leq 104$.

Case 1 ($m=2,3,4$). For $15T2\simeq D_{15}, 15T3\simeq D_5\times C_3, 15T4\simeq S_3\times C_5$, it follows from Endô [End11, Theorem 3.1] that T is stably k-rational for $15T2, 15T3, 15T4$.

Case 2 ($m=5,7,10,16,23$). By Algorithm 4.1(1), we see that $[J_{G/H}]^{fl}$ is invertible and hence T is retract k-rational for $m=5,7,16,23$.

For $15T5\simeq A_5$, by Algorithm 4.1(3), we get $F=[J_{G/H}]^{fl}$ with $\mathrm{rank}_{\mathbb{Z}}(F)=21$ and $F'=[F]^{fl}=\mathbb{Z}$. This implies that $F=0$ and hence T is stably k-rational (see [HHY, Example 4.5]).

For $15T7\simeq D_5\times S_3, 15T16\simeq A_5\times C_3, 15T23\simeq A_5\times S_3$, it is enough to prove that $[J_{G/H}]^{fl}=0$ for $G=15T23$ because $15T7\leq 15T23$, $15T16\leq 15T23$ and Lemma 2.10(i). By Algorithm 4.1(3), we obtain that $F=[J_{G/H}]^{fl}$ with $\mathrm{rank}_{\mathbb{Z}}(F)=27$, $F'=[F]^{fl}$ with $\mathrm{rank}_{\mathbb{Z}}(F')=8$ and $F''=[F']^{fl}$ with $F''=\mathbb{Z}$. This implies that $F=0$ and hence T is stably k-rational (see [HHY, Example 4.5]).

For $15T10\simeq S_5$, by Algorithm 4.1(2), we obtain that $[J_{G/H}]^{fl}\neq 0$ and hence T is not stably k-rational (see [HHY, Example 4.5]).

Case 3 ($m=6,8,11,22,24,29$). For $15T6\simeq C_{15}\rtimes C_4$, $15T8\simeq F_{20}\times C_3$, it follows from Endô [End11, Theorem 3.1] that $[J_{G/H}]^{fl}$ is invertible and $[J_{G/H}]^{fl}\neq 0$. Hence T is not stably but retract k-rational.

For $m=11,22,24,29$, by Algorithm 4.1(1), we see that $[J_{G/H}]^{fl}$ is invertible and hence T is retract k-rational. By Lemma 2.10(i) and the inclusions $15T6\leq 15T11, 15T22, 15T29$, and $15T8\leq 15T24$, we obtain that $[J_{G/H}]^{fl}\neq 0$ and hence T is not stably k-rational for $m=11,22,24,29$.

Case 4 ($9\leq m\leq 104$ and $m\neq 10,11,16,22,23,24,29$). By using the command `List([1..104],x->Filtered([1..x],y->IsSubgroup(TransitiveGroup(15,x), TransitiveGroup(15,y))))` in GAP [GAP] (see also [HHY, Example 4.4] for the case where $n=14$), we obtain the inclusions $15Tm\leq 15Tm'$ among the groups $G=15Tm$ with minimal groups $15Tm$ where $m\in I_{15}:=\{9,15,20,26\}$.

By the inclusions of groups $G = 15Tm$ above and Lemma 2.10(ii), it is enough to show that $[J_{G/H}]^{fl}$ is not invertible for $m \in I_{15}$. By Algorithm 4.1(1), we obtain that $[J_{G/H}]^{fl}$ is not invertible and hence T is not retract k-rational for $m \in I_{15}$ (see [HHY, Example 4.5]). □

We give GAP [GAP] computations in the proof of Theorem 1.2 for $n = 10, 12, 14, 15$ in the arXiv version of this paper [HHY, Examples 4.2 to 4.5] (see [HY17, Chapter 5] for the explanation of the functions). Some related programs are available at `https://www.math.kyoto-u.ac.jp/~yamasaki/Algorithm/RatProbNorm1Tori/`.

5. Proof of Theorems 1.3, 1.4, and 1.6

Proof of Theorem 1.3. We may assume that H is the stabilizer of one of the letters in G (see the first paragraph of Section 4).

Step 1. It is enough to show that $F = [J_{G/H}]^{fl}$ is not invertible for $G = \mathrm{PSL}_2(\mathbb{F}_q)$ because $\mathrm{PSL}_2(\mathbb{F}_q) \leq G \leq \mathrm{P\Gamma L}_2(\mathbb{F}_q)$ and Lemma 2.10(ii). The group $G = \mathrm{PSL}_2(\mathbb{F}_q)$ acts on $\mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}$ via linear fractional transformation. Let $\mathbb{F}_q^\times = \langle u \rangle$. Then $\mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q^\times \cup \{0\} \cup \{\infty\}$ and $\mathbb{F}_q^\times = \{1, -1, \sqrt{-1}, -\sqrt{-1}, u^i, -u^i, u^{-i}, -u^{-i} \mid 1 \leq i \leq \frac{q-5}{4}\}$ because $q \equiv 1 \pmod 4$.

Step 2. Take a subgroup $V_4 = \langle \sigma, \tau \rangle \simeq C_2 \times C_2 \leq G = \mathrm{PSL}_2(\mathbb{F}_q)$ as

$$\sigma = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \ \tau = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

The action of $V_4 = \langle \sigma, \tau \rangle$ on $\mathbb{P}^1(\mathbb{F}_q)$ is given as $\sigma : x \mapsto -x$ and $\tau : x \mapsto -1/x$. This action induces the action of V_4 on $J_{G/H}$ given by

$$\begin{aligned}
&\sigma : e_1 \leftrightarrow e_{-1},\ e_{\sqrt{-1}} \leftrightarrow e_{-\sqrt{-1}},\ e_{u^i} \leftrightarrow e_{-u^i},\ e_{-u^{-i}} \leftrightarrow e_{u^{-i}},\ e_0 \mapsto e_0,\ e_\infty \mapsto e_\infty,\\
&\tau : e_1 \leftrightarrow e_{-1},\ e_{\pm\sqrt{-1}} \mapsto e_{\pm\sqrt{-1}},\ e_{u^i} \leftrightarrow e_{-u^{-i}},\ e_{-u^i} \leftrightarrow e_{u^{-i}},\ e_0 \leftrightarrow e_\infty,\\
&\sigma\tau : e_{\pm 1} \mapsto e_{\pm 1},\ e_{\sqrt{-1}} \leftrightarrow e_{-\sqrt{-1}},\ e_{u^i} \leftrightarrow e_{u^{-i}},\ e_{-u^i} \leftrightarrow e_{-u^{-i}},\ e_0 \leftrightarrow e_\infty
\end{aligned}$$

where $B = \{e_1, e_{-1}, e_{\sqrt{-1}}, e_{-\sqrt{-1}}, e_{u^i}, e_{-u^i}, e_{u^{-i}}, e_{-u^{-i}}, e_0 \mid 1 \leq i \leq \frac{q-5}{4}\}$ is a $\mathbb{Z}$-basis of $J_{G/H}$ and

$$e_\infty := -\sum_{j \in \mathbb{F}_q} e_j.$$

By Lemma 2.10(ii), we should show that $[M]^{fl}$ is not invertible where $M = J_{G/H}|_{V_4}$ is a V_4-lattice with $\mathrm{rank}_{\mathbb{Z}}(M) = q = n - 1$.

Step 3. We will construct a coflabby resolution $0 \to F^\circ \to P^\circ \to M^\circ \to 0$ where P° is permutation V_4-lattice and F° is coflabby V_4-lattice with $\mathrm{rank}_{\mathbb{Z}}(F^\circ) = 5$.

Step 3-1. The actions of σ and τ on M are represented as matrices

$$\left(\begin{array}{cccc|cccc|ccc|c}
0 & 1 & & & & & & & & & & \\
1 & 0 & & & & & & & & & & \\
 & & 0 & 1 & & & & & & & & \\
 & & 1 & 0 & & & & & & & & \\
\hline
 & & & & 0 & 1 & 0 & 0 & & & & \\
 & & & & 1 & 0 & 0 & 0 & & & & \\
 & & & & 0 & 0 & 0 & 1 & & & & \\
 & & & & 0 & 0 & 1 & 0 & & & & \\
\hline
 & & & & & & & & \ddots & & & \\
 & & & & & & & & & \ddots & & \\
 & & & & & & & & & & \ddots & \\
\hline
 & & & & & & & & & & & 1
\end{array}\right),$$

$$\left(\begin{array}{cccc|cccc|ccc|c}
0 & 1 & & & & & & & & & & \\
1 & 0 & & & & & & & & & & \\
 & & 1 & 0 & & & & & & & & \\
 & & 0 & 1 & & & & & & & & \\
\hline
 & & & & 0 & 0 & 0 & 1 & & & & \\
 & & & & 0 & 0 & 1 & 0 & & & & \\
 & & & & 0 & 1 & 0 & 0 & & & & \\
 & & & & 1 & 0 & 0 & 0 & & & & \\
\hline
 & & & & & & & & \ddots & & & \\
 & & & & & & & & & \ddots & & \\
 & & & & & & & & & & \ddots & \\
\hline
-1 & -1 & -1 & -1 & 1 & -1 & -1 & -1 & -1 & \cdots & -1 & -1
\end{array}\right).$$

Let $B^* = \{e_1^*, e_{-1}^*, e_{\sqrt{-1}}^*, e_{-\sqrt{-1}}^*, e_{u^i}^*, e_{-u^i}^*, e_{u^{-i}}^*, e_{-u^{-i}}^*, e_0^* \mid 1 \leq i \leq \frac{q-5}{4}\}$ be the dual basis of B. By the definition, B^* is a $\mathbb{Z}$-basis of the G-lattice $I_{G/H} = (J_{G/H})^\circ$. The action of $V_4 = \langle \sigma, \tau \rangle$ on M° is given by

$$\begin{aligned}
&\sigma : e_1^* \leftrightarrow e_{-1}^*,\ e_{\sqrt{-1}}^* \leftrightarrow e_{-\sqrt{-1}}^*,\ e_{u^i}^* \leftrightarrow e_{-u^i}^*,\ e_{-u^{-i}}^* \leftrightarrow e_{u^{-i}}^*,\ e_0^* \mapsto e_0^*,\\
&\tau : e_1^* \leftrightarrow e_{-1}^* - e_0^*,\ e_{\pm\sqrt{-1}}^* \leftrightarrow e_{\pm\sqrt{-1}}^* - e_0^*,\ e_{u^i}^* \leftrightarrow e_{-u^{-i}}^* - e_0^*,\ e_{-u^i}^*\\
&\qquad\qquad \leftrightarrow e_{u^{-i}}^* - e_0^*,\ e_0^* \mapsto -e_0^*,\\
&\sigma\tau : e_{\pm 1}^* \leftrightarrow e_{\pm 1}^* - e_0^*,\ e_{\pm\sqrt{-1}}^* \leftrightarrow e_{\mp\sqrt{-1}}^* - e_0^*,\ e_{u^i}^* \leftrightarrow e_{u^{-i}}^* - e_0^*,\ e_{-u^i}^*\\
&\qquad\qquad \leftrightarrow e_{-u^{-i}}^* - e_0^*,\ e_0^* \mapsto -e_0^*
\end{aligned}$$

(this action corresponds to the transposed matrices of the above matrices).

We define the permutation V_4-lattice P° of $\mathrm{rank}_{\mathbb{Z}}(P^\circ) = q+5 = n+4$ with $\mathbb{Z}$-basis

$$v_1 := v(e_1^*),\ v_2 := v(e_{-1}^*),\ v_3 := v(e_1^* - e_0^*), v_4 := v(e_{-1}^* - e_0^*),\ v_5 := v(e_1^* + e_{-1}^* - e_0^*),$$
$$v_6 := v(e_{\sqrt{-1}}^*), v_7 := v(e_{-\sqrt{-1}}^*), v_8 := v(e_{\sqrt{-1}}^* - e_0^*), v_9 := v(e_{-\sqrt{-1}}^* - e_0^*),$$
$$v_{10} := v(e_{\sqrt{-1}}^* + e_{-\sqrt{-1}}^* - e_0^*),$$
$$v_{i,1} := v(e_{u^i}^*), v_{i,2} := v(e_{-u^i}^*), v_{i,3} := v(e_{u^{-i}}^* - e_0^*),$$
$$v_{i,4} := v(e_{-u^{-i}}^* - e_0^*) \quad (1 \le i \le \tfrac{q-5}{4})$$

where V_4 acts on P° by $g(v(m^*)) = v(g(m^*))$ $(m^* \in M^\circ, g \in V_4)$:

$$\sigma : v_1 \leftrightarrow v_2,\ v_3 \leftrightarrow v_4,\ v_5 \mapsto v_5,\ v_6 \leftrightarrow v_7,\ v_8 \leftrightarrow v_9,\ v_{10} \mapsto v_{10},\ v_{i,1} \leftrightarrow v_{i,2},\ v_{i,3} \leftrightarrow v_{i,4},$$
$$\tau : v_1 \leftrightarrow v_4,\ v_2 \leftrightarrow v_3,\ v_5 \mapsto v_5,\ v_6 \leftrightarrow v_9,\ v_7 \leftrightarrow v_8,\ v_{10} \mapsto v_{10},\ v_{i,1} \leftrightarrow v_{i,4},\ v_{i,2} \leftrightarrow v_{i,3},$$
$$\sigma\tau : v_1 \leftrightarrow v_3,\ v_2 \leftrightarrow v_4,\ v_5 \mapsto v_5,\ v_6 \leftrightarrow v_8,\ v_7 \leftrightarrow v_9,\ v_{10} \mapsto v_{10},\ v_{i,1} \leftrightarrow v_{i,3},\ v_{i,2} \leftrightarrow v_{i,4}.$$

Step 3-2. We define a V_4-homomorphism $f : P^\circ \to M^\circ$, $v(m^*) \mapsto m^*$ $(m^* \in M^\circ)$. Then f is surjective. We define a V_4-lattice F° as $F^\circ = \mathrm{Ker}(f)$. Then we obtain an exact sequence $0 \to F^\circ \to P^\circ \to M^\circ \to 0$ with $\mathrm{rank}_{\mathbb{Z}}(F^\circ) = 5$.

Step 3-3. We will check that F° is coflabby. In order to prove this assertion, we should check that $\widetilde{f} = f|_{H^0(W,P^\circ)} : H^0(W, P^\circ) \to H^0(W, M^\circ)$ is surjective (hence $H^1(W, F^\circ) = 0$) for any $W \le V_4$ where $H^0(W, P^\circ) = \widehat{Z}^0(W, P^\circ) = (P^\circ)^W$ (see also [HY17, Chapter 2]).

Step 3-3-1 ($W = V_4 = \langle \sigma, \tau \rangle$). By the orbit decomposition of the action of V_4 on P°,

$$\{v_1 + v_2 + v_3 + v_4, v_5, v_6 + v_7 + v_8 + v_9, v_{10}, v_{i,1} + v_{i,2} + v_{i,3} + v_{i,4} \mid 1 \le i \le \tfrac{q-5}{4}\}$$

is a $\mathbb{Z}$-basis of $(P^\circ)^{V_4}$. We also see that

$$\{e_1^* + e_{-1}^* - e_0^*, e_{\sqrt{-1}}^* + e_{-\sqrt{-1}}^* - e_0^*, e_{u^i}^* + e_{-u^i}^* + e_{u^{-i}}^* + e_{-u^{-i}}^* - 2e_0^* \mid 1 \le i \le \tfrac{q-5}{4}\}$$

is a $\mathbb{Z}$-basis of $(M^\circ)^{V_4}$. Hence $\widetilde{f}$ is surjective because

$$\begin{aligned}\widetilde{f} : {}& v_1 + v_2 + v_3 + v_4 \mapsto 2(e_1^* + e_{-1}^* - e_0^*),\ v_5 \mapsto e_1^* + e_{-1}^* - e_0^*,\\ & v_6 + v_7 + v_8 + v_9 \mapsto 2(e_{\sqrt{-1}}^* + e_{-\sqrt{-1}}^* - e_0^*),\ v_{10} \mapsto e_{\sqrt{-1}}^* + e_{-\sqrt{-1}}^* - e_0^*,\\ & v_{i,1} + v_{i,2} + v_{i,3} + v_{i,4} \mapsto e_{u^i}^* + e_{-u^i}^* + e_{u^{-i}}^* + e_{-u^{-i}}^* - 2e_0^* \quad (1 \le i \le \tfrac{q-5}{4}).\end{aligned}$$

Step 3-3-2 ($W = \langle \sigma \rangle$). The set

$$\{v_1 + v_2, v_3 + v_4, v_5, v_6 + v_7, v_8 + v_9, v_{10}, v_{i,1} + v_{i,2}, v_{i,3} + v_{i,4} \mid 1 \le i \le \tfrac{q-5}{4}\}$$

becomes a $\mathbb{Z}$-basis of $(P^\circ)^{\langle\sigma\rangle}$ and

$$\{e_1^* + e_{-1}^*, e_{\sqrt{-1}}^* + e_{-\sqrt{-1}}^*, e_{u^i}^* + e_{-u^i}^*, e_{u^{-i}}^* + e_{-u^{-i}}^*, e_0^* \mid 1 \le i \le \tfrac{q-5}{4}\}$$

is a $\mathbb{Z}$-basis of $(M^\circ)^{\langle\sigma\rangle}$. Hence $\widetilde{f}$ is surjective because

$$\begin{aligned}\widetilde{f} : {}& v_1 + v_2 \mapsto e_1^* + e_{-1}^*, v_5 \mapsto e_1^* + e_{-1}^* - e_0^*,\ v_6 + v_7 \mapsto e_{\sqrt{-1}}^* + e_{-\sqrt{-1}}^*,\\ & v_{i,1} + v_{i,2} \mapsto e_{u^i}^* + e_{-u^i}^*,\ v_{i,3} + v_{i,4} \mapsto e_{u^{-i}}^* + e_{-u^{-i}}^* - 2e_0^* \quad (1 \le i \le \tfrac{q-5}{4}).\end{aligned}$$

Step 3-3-3 ($W = \langle \tau \rangle$). The set

$$\{v_1 + v_4, v_2 + v_3, v_5, v_6 + v_8, v_7 + v_9, v_{10}, v_{i,1} + v_{i,4}, v_{i,2} + v_{i,3} \mid 1 \le i \le \tfrac{q-5}{4}\}$$

becomes a $\mathbb{Z}$-basis of $(P^\circ)^{\langle \tau \rangle}$ and

$$\{e_1^* + e_{-1}^* - e_0^*, e_{\sqrt{-1}}^* + e_{-\sqrt{-1}}^* - e_0^*, 2e_{-\sqrt{-1}}^* - e_0^*, e_{u^i}^* \\ + e_{-u^{-i}}^* - e_0^*, e_{u^{-i}}^* + e_{-u^i}^* - e_0^* \mid 1 \le i \le \tfrac{q-5}{4}\}$$

is a $\mathbb{Z}$-basis of $(M^\circ)^{\langle \tau \rangle}$. Hence $\widetilde{f}$ is surjective because

$$\widetilde{f} : v_5 \mapsto e_1^* + e_{-1}^* - e_0^*,\ v_7 + v_9 \mapsto 2e_{-\sqrt{-1}}^* - e_0^*,\ v_{10} \mapsto e_{\sqrt{-1}}^* + e_{-\sqrt{-1}}^* - e_0^*, \\ v_{i,1} + v_{i,4} \mapsto e_{u^i}^* + e_{-u^{-i}}^* - e_0^*,\ v_{i,2} + v_{i,3} \mapsto e_{-u^i}^* + e_{u^{-i}}^* - e_0^* \quad (1 \le i \le \tfrac{q-5}{4}).$$

Step 3-3-4 ($W = \langle \sigma\tau \rangle$). The set

$$\{v_1 + v_3, v_2 + v_4, v_5, v_6 + v_9, v_7 + v_8, v_{10}, v_{i,1} + v_{i,3}, v_{i,2} + v_{i,4} \mid 1 \le i \le \tfrac{q-5}{4}\}$$

becomes a $\mathbb{Z}$-basis of $(P^\circ)^{\langle \sigma\tau \rangle}$ and

$$\{e_1^* + e_{-1}^* - e_0^*, 2e_{-1}^* - e_0^*, e_{\sqrt{-1}}^* + e_{-\sqrt{-1}}^* - e_0^*, e_{u^i}^* + e_{u^{-i}}^* \\ - e_0^*, e_{-u^i}^* + e_{-u^{-i}}^* - e_0^* \mid 1 \le i \le \tfrac{q-5}{4}\}$$

is a $\mathbb{Z}$-basis of $(M^\circ)^{\langle \sigma\tau \rangle}$. Hence $\widetilde{f}$ is surjective because

$$\widetilde{f} : v_5 \mapsto e_1^* + e_{-1}^* - e_0^*,\ v_2 + v_4 \mapsto 2e_{-1}^* - e_0^*,\ v_{10} \mapsto e_{\sqrt{-1}}^* + e_{-\sqrt{-1}}^* - e_0^*, \\ v_{i,1} + v_{i,3} \mapsto e_{u^i}^* + e_{u^{-i}}^* - e_0^*,\ v_{i,2} + v_{i,4} \mapsto e_{-u^i}^* + e_{-u^{-i}}^* - e_0^* \quad (1 \le i \le \tfrac{q-5}{4}).$$

Step 4. We will prove that F is not invertible. By Step 3, we have an exact sequence $0 \to F^\circ \to P^\circ \to M^\circ \to 0$ where P° is permutation V_4-lattice and F° is coflabby V_4-lattice with $\mathrm{rank}_{\mathbb{Z}}(F^\circ) = 5$.

The set $\{w_1, w_2, w_3, w_4, w_5\}$ becomes a $\mathbb{Z}$-basis of F° where

$$w_1 = v_1 + v_4 - v_5,\ w_2 = v_2 - v_4 + v_8 + v_9 - v_{10},\ w_3 = v_3 + v_4 - v_5 - v_8 - v_9 + v_{10}, \\ w_4 = v_6 + v_9 - v_{10},\ w_5 = v_7 + v_8 - v_{10}.$$

The actions of σ and τ on F° are given by

$$\sigma : w_1 \mapsto w_2 + w_3,\ w_2 \mapsto w_1 - w_3,\ w_3 \mapsto w_3,\ w_4 \leftrightarrow w_5, \\ \tau : w_1 \mapsto w_1,\ w_2 \mapsto -w_1 + w_3 + w_4 + w_5,\ w_3 \mapsto w_1 + w_2 - w_4 - w_5,\ w_4 \leftrightarrow w_5$$

and they are represented as matrices

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

By taking the dual, we get the flabby resolution $0 \to M \to P \to F \to 0$ of M and the actions of σ and τ on F are represented as the following matrices (transposed matrices of the above):

$$S=\begin{pmatrix} 0 & 1 & 0 & 0 & 0\\ 1 & 0 & 0 & 0 & 0\\ 1 & -1 & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & 1\\ 0 & 0 & 0 & 1 & 0 \end{pmatrix},\quad T=\begin{pmatrix} 1 & -1 & 1 & 0 & 0\\ 0 & 0 & 1 & 0 & 0\\ 0 & 1 & 0 & 0 & 0\\ 0 & 1 & -1 & 0 & 1\\ 0 & 1 & -1 & 1 & 0 \end{pmatrix}.$$

In order to obtain $H^1(V_4,F)$, we should evaluate the elementary divisors of

$$(S-I\mid T-I)=\left(\begin{array}{ccccc|ccccc} -1 & 1 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0\\ 1 & -1 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0\\ 1 & -1 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0\\ 0 & 0 & 0 & -1 & 1 & 0 & 1 & -1 & -1 & 1\\ 0 & 0 & 0 & 1 & -1 & 0 & 1 & -1 & 1 & -1 \end{array}\right)$$

where I is the 5×5 identity matrix. Multiplying the regular matrix

$$Q=\begin{pmatrix} -1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1\\ 0 & -1 & 1 & 0 & 0\\ 1 & 0 & 1 & 0 & 0\\ 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

from the left, we have

$$Q\,(S-I\mid T-I)=\left(\begin{array}{ccccc|ccccc} 1 & -1 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0\\ 0 & 0 & 0 & 1 & -1 & 0 & 1 & -1 & 1 & -1\\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & -2 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right).$$

Hence we conclude that $H^1(V_4,F)=\mathbb{Z}/2\mathbb{Z}$. This implies that F is not invertible. $\square$

Let p be a prime number and let $G\leq S_{2p}$ be a primitive subgroup. Wielandt ([Wie56], [Wie64]) proved that G is doubly transitive if $2p-1$ is not a perfect square. Using the classification of finite simple groups, all doubly transitive finite groups are known (see Cameron [Cam81, Theorem 5.3] and also Dixon and Mortimer [DM96, Section 7.7]). On the other hand, by the O'Nan-Scott theorem (see Liebeck, Praeger, and Saxl [LPS88]), G must be almost simple, i.e., $S\leq G\leq \mathrm{Aut}(S)$ for some non-abelian simple group S. The socle $\mathrm{soc}(G)\lhd G$ of a group G was classified by Liebeck and Saxl [LS85, Theorem 1.1 (i), (iii)].

Theorem 5.1 (Liebeck and Saxl [LS85, Corollary 1.2]; see also [Sha97, Theorem 4.6], [DJ13, Proposition 5.5])**.** *Let p be a prime number and let $G\leq S_{2p}$ be a primitive subgroup. Then G is one of the following:*

(i) $G=S_{2p}$ *or* $G=A_{2p}\leq S_{2p}$*;*
(ii) $G=S_5\leq S_{10}$ *or* $G=A_5\leq S_{10}$*;*
(iii) $G=M_{22}\leq S_{22}$ *or* $G=\mathrm{Aut}(M_{22})\simeq M_{22}\rtimes C_2\leq S_{22}$ *where* M_{22} *is the Mathieu group of degree* 22*;*
(iv) $\mathrm{PSL}_2(\mathbb{F}_q)\leq G\leq \mathrm{P\Gamma L}_2(\mathbb{F}_q)\simeq \mathrm{PGL}_2(\mathbb{F}_q)\rtimes C_e$ *where* $2p=q+1$ *and* $q=l^e$ *is an odd prime power.*

Proof of Theorem 1.4. We may assume that H is the stabilizer of one of the letters in G (see the first paragraph of Section 4).

(i) follows from Cortella and Kunyavskii [CK00, Proposition 0.2] and Endô [End11, Theorem 5.2].

(ii) follows from Theorem 1.2(1) because $S_5 \simeq 10T13$ and $A_5 \simeq 10T7$.

For (iii), it is enough to show that $F = [J_{G/H}]^{fl}$ is not invertible for $G = M_{22} \leq S_{22}$. We see that there exists $G' \leq G$ such that $[J_{G/H}|_{G'}]^{fl}$ is not invertible. Indeed, we can find such G' which is isomorphic to $(C_2)^3$, Q_8, D_4 or $C_4 \times C_2$ (see [HHY, Example 5.2]). Hence it follows from Lemma 2.10(ii) that F is not invertible. This implies that T is not retract k-rational by Theorem 2.7(iii).

For (iv), we may assume that $p \geq 3$ (if $p = 2$, then $q = 3$ and $\mathrm{PSL}_2(\mathbb{F}_3) \simeq A_4$, $\mathrm{PGL}_2(\mathbb{F}_3) \simeq S_4$, see (i)). Then $q = 2p - 1 \equiv 1 \pmod 4$ because p is odd. Hence the assertion follows from Theorem 1.3 as a special case where $n = 2p$ and $q = l^e$. □

Proof of Theorem 1.6. The assertion for $n = 11$ and $n = 23$ follows from [HY, Theorem 1.9 (6)]. The assertion for $n = 12$ and $n = 22$ follows from Theorem 1.2(2)–(ii) and Theorem 1.4(iii), respectively.

Let $G = M_{24}$ be the Mathieu group of degree 24. Then there exists $G' \leq G \leq S_{24}$ which is transitive and isomorphic to S_4 (see [HHY, Example 5.2]). Then $[J_{G'}]^{fl}$ is not invertible by Endô and Miyata [EM75, Theorem 1.5]. It follows from Lemma 2.10(ii) that $[J_{G/H}]^{fl}$ is not invertible and hence $R^{(1)}_{K/k}(\mathbb{G}_m)$ is not retract k-rational by Theorem 2.7(iii). □

Acknowledgments

The authors would like to thank Ming-chang Kang and Shizuo Endô for giving them useful and valuable comments. They also thank the referee and the editor for crucial advice on how to organize the paper with the aid of computer algorithms.

References

[But93] G. Butler, *The transitive groups of degree fourteen and fifteen*, J. Symbolic Comput. **16** (1993), no. 5, 413–422, DOI 10.1006/jsco.1993.1056. MR1271082

[BM83] G. Butler and J. McKay, *The transitive groups of degree up to eleven*, Comm. Algebra **11** (1983), no. 8, 863–911, DOI 10.1080/00927878308822884. MR695893

[Cam81] P. J. Cameron, *Finite permutation groups and finite simple groups*, Bull. London Math. Soc. **13** (1981), no. 1, 1–22, DOI 10.1112/blms/13.1.1. MR599634

[CH08] J. J. Cannon and D. F. Holt, *The transitive permutation groups of degree 32*, Experiment. Math. **17** (2008), no. 3, 307–314. MR2455702

[CE56] H. Cartan and S. Eilenberg, *Homological Algebra*, Princeton University Press, Princeton, N. J., 1956. MR0077480

[CK00] A. Cortella and B. Kunyavskiĭ, *Rationality problem for generic tori in simple groups*, J. Algebra **225** (2000), no. 2, 771–793, DOI 10.1006/jabr.1999.8150. MR1741561

[CTS77] J.-L. Colliot-Thélène and J.-J. Sansuc, *La R-équivalence sur les tores* (French), Ann. Sci. École Norm. Sup. (4) **10** (1977), no. 2, 175–229. MR0450280

[CTS87] J.-L. Colliot-Thélène and J.-J. Sansuc, *Principal homogeneous spaces under flasque tori: applications*, J. Algebra **106** (1987), no. 1, 148–205, DOI 10.1016/0021-8693(87)90026-3. MR878473

[DM96] J. D. Dixon and B. Mortimer, *Permutation Groups*, Graduate Texts in Mathematics, vol. 163, Springer-Verlag, New York, 1996. MR1409812

[DJ13] A. Džambić and G. A. Jones, *p-adic Hurwitz groups*, J. Algebra **379** (2013), 179–207, DOI 10.1016/j.jalgebra.2013.01.007. MR3019251

[End11] S. Endô, *The rationality problem for norm one tori*, Nagoya Math. J. **202** (2011), 83–106, DOI 10.1215/00277630-1260459. MR2804547

[EK17] S. Endô and M.-C. Kang, *Function fields of algebraic tori revisited*, Asian J. Math. **21** (2017), no. 2, 197–224, DOI 10.4310/AJM.2017.v21.n2.a1. MR3672258

[EM73] S. Endô and T. Miyata, *Invariants of finite abelian groups*, J. Math. Soc. Japan **25** (1973), 7–26, DOI 10.2969/jmsj/02510007. MR0311754

[EM75] S. Endo, T. Miyata, *On a classification of the function fields of algebraic tori*, Nagoya Math. J. **56** (1975) 85–104. MR364203. Corrigenda: Nagoya Math. J. **79** (1980) 187–190. MR587418

[EM82] S. Endô and T. Miyata, *Integral representations with trivial first cohomology groups*, Nagoya Math. J. **85** (1982), 231–240. MR648425

[Flo] M. Florence, *Non rationality of some norm one tori*, preprint (2006).

[GAP] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.8.10; 2018. (http://www.gap-system.org).

[HHY] S. Hasegawa, A. Hoshi, and A. Yamasaki, *Rationality problem for norm one tori in small dimensions*, arXiv:1811.02145 (the arXiv version of this paper).

[HS97] P. J. Hilton and U. Stammbach, *A Course in Homological Algebra*, 2nd ed., Graduate Texts in Mathematics, vol. 4, Springer-Verlag, New York, 1997. MR1438546

[HKK14] A. Hoshi, M.-c. Kang, and H. Kitayama, *Quasi-monomial actions and some 4-dimensional rationality problems*, J. Algebra **403** (2014), 363–400, DOI 10.1016/j.jalgebra.2014.01.019. MR3166080

[HY17] A. Hoshi and A. Yamasaki, *Rationality problem for algebraic tori*, Mem. Amer. Math. Soc. **248** (2017), no. 1176, v+215, DOI 10.1090/memo/1176. MR3685951

[HY] A. Hoshi and A. Yamasaki, *Rationality problem for norm one tori*, arXiv:1811.01676.

[Hür84] W. Hürlimann, *On algebraic tori of norm type*, Comment. Math. Helv. **59** (1984), no. 4, 539–549, DOI 10.1007/BF02566365. MR780075

[Kan12] M.-c. Kang, *Retract rational fields*, J. Algebra **349** (2012), 22–37, DOI 10.1016/j.jalgebra.2011.10.024. MR2853623

[Kun90] B. E. Kunyavskii, *Three-dimensional algebraic tori*, Selecta Math. Soviet. **9** (1990) 1–21.

[Kun07] B. E. Kunyavskii, *Algebraic tori — thirty years after*, Vestnik Samara State Univ. (2007) 198–214.

[LL00] N. Lemire and M. Lorenz, *On certain lattices associated with generic division algebras*, J. Group Theory **3** (2000), no. 4, 385–405, DOI 10.1515/jgth.2000.031. MR1790337

[LPR06] N. Lemire, V. L. Popov, and Z. Reichstein, *Cayley groups*, J. Amer. Math. Soc. **19** (2006), no. 4, 921–967, DOI 10.1090/S0894-0347-06-00522-4. MR2219306

[LeB95] L. Le Bruyn, *Generic norm one tori*, Nieuw Arch. Wisk. (4) **13** (1995), no. 3, 401–407. MR1378805

[Len74] H. W. Lenstra Jr., *Rational functions invariant under a finite abelian group*, Invent. Math. **25** (1974), 299–325, DOI 10.1007/BF01389732. MR0347788

[LPS88] M. W. Liebeck, C. E. Praeger, and J. Saxl, *On the O'Nan-Scott theorem for finite primitive permutation groups*, J. Austral. Math. Soc. Ser. A **44** (1988), no. 3, 389–396. MR929529

[LS85] M. W. Liebeck and J. Saxl, *Primitive permutation groups containing an element of large prime order*, J. London Math. Soc. (2) **31** (1985), no. 2, 237–249, DOI 10.1112/jlms/s2-31.2.237. MR809945

[Lor05] M. Lorenz, *Multiplicative Invariant Theory*, Encyclopaedia of Mathematical Sciences, vol. 135, Springer-Verlag, Berlin, 2005. Invariant Theory and Algebraic Transformation Groups, VI. MR2131760

[Ono61] T. Ono, *Arithmetic of algebraic tori*, Ann. of Math. (2) **74** (1961), 101–139, DOI 10.2307/1970307. MR0124326

[Roy87] G. F. Royle, *The transitive groups of degree twelve*, J. Symbolic Comput. **4** (1987), no. 2, 255–268, DOI 10.1016/S0747-7171(87)80068-8. MR922391

[Sal84] D. J. Saltman, *Retract rational fields and cyclic Galois extensions*, Israel J. Math. **47** (1984), no. 2-3, 165–215, DOI 10.1007/BF02760515. MR738167

[Sha97] J. Shareshian, *On the Möbius number of the subgroup lattice of the symmetric group*, J. Combin. Theory Ser. A **78** (1997), no. 2, 236–267, DOI 10.1006/jcta.1997.2762. MR1445416

[Swa83] R. G. Swan, *Noether's problem in Galois theory*, Emmy Noether in Bryn Mawr (Bryn Mawr, Pa., 1982), Springer, New York-Berlin, 1983, pp. 21–40. MR713790

[Swa10] R. G. Swan, *The flabby class group of a finite cyclic group*, Fourth International Congress of Chinese Mathematicians, AMS/IP Stud. Adv. Math., vol. 48, Amer. Math. Soc., Providence, RI, 2010, pp. 259–269. MR2744226

[Vos67] V. E. Voskresenskiĭ, *On two-dimensional algebraic tori. II* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **31** (1967), 711–716. MR0214597

[Vos70] V. E. Voskresenskiĭ, *Birational properties of linear algebraic groups* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **34** (1970), 3–19. MR0262251

[Vos74] V. E. Voskresenskiĭ, *Stable equivalence of algebraic tori* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **38** (1974), 3–10. MR0342515

[Vos98] V. E. Voskresenskiĭ, *Algebraic Groups and Their Birational Invariants*, Translations of Mathematical Monographs, vol. 179, American Mathematical Society, Providence, RI, 1998. Translated from the Russian manuscript by Boris Kunyavski [Boris È. Kunyavskiĭ]. MR1634406

[Wie56] H. Wielandt, *Primitive Permutationsgruppen vom Grad* $2p$ (German), Math. Z. **63** (1956), 478–485, DOI 10.1007/BF01187953. MR0075200

[Wie64] H. Wielandt, *Finite Permutation Groups*, Translated from the German by R. Bercov, Academic Press, New York-London, 1964. MR0183775

[Yam12] A. Yamasaki, *Negative solutions to three-dimensional monomial Noether problem*, J. Algebra **370** (2012), 46–78, DOI 10.1016/j.jalgebra.2012.07.018. MR2966827

Graduate School of Science and Technology, Niigata University, Niigata 950-2181, Japan
Email address: `shasegawa@m.sc.niigata-u.ac.jp`

Department of Mathematics, Niigata University, Niigata 950-2181, Japan
Email address: `hoshi@math.sc.niigata-u.ac.jp`

Department of Mathematics, Kyoto University, Kyoto 606-8502, Japan
Email address: `aiichi.yamasaki@gmail.com`