RATIONALITY PROBLEM FOR NORM ONE TORI, II

SUMITO HASEGAWA, AKINARI HOSHI, AND AIICHI YAMASAKI

Abstract. We give a stably and retract rational classification of norm one tori of dimension \( n - 1 \) for \( n = 2^e \) \((e \geq 1)\) is 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.

Contents

1. Introduction  
2. Preliminaries: rationality problem for algebraic tori and flabby resolution  
3. Proof of Theorem 1.1  
4. Proof of Theorem 1.2  
5. Proof of Theorem 1.3 Theorem 1.4 and Theorem 1.6  
6. References

1. Introduction

Let \( L \) be a finite Galois extension of a field \( k \) and \( G = \text{Gal}(L/k) \) 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

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

for any \( \sigma \in \mathbb{G} \), where \( \sigma(u_i) = \sum_{j=1}^{n} a_{i,j}u_j \), \( a_{i,j} \in \mathbb{Z} \). 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 \( X(T) = \text{Hom}(T, \mathbb{G}_m) \) 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 \( H^1(G, \mathbb{G}_m) \) where \( G = \text{Gal}(k_n/k) \) since \( \text{Aut}(\mathbb{G}_m^n) = \text{GL}_n(\mathbb{Z}) \). The \( k \)-torus \( T \) of dimension \( n \) is determined uniquely by the integral representation \( h : G \rightarrow \text{GL}_n(\mathbb{Z}) \) up to conjugacy, and the group \( h(G) \) is a finite subgroup of \( \text{GL}_n(\mathbb{Z}) \) (see [Vos98] page 57, Section 4.9]).

Let \( K/k \) be a separable field extension of degree \( n \) and \( L/k \) be the Galois closure of \( K/k \). Let \( G = \text{Gal}(L/k) \) and \( H = \text{Gal}(L/K) \). The Galois group \( G \) may be regarded as a transitive subgroup of the symmetric group \( S_n \) of degree \( n \). Let \( R_{K/k}(\mathbb{G}_m) \) be the norm one torus of \( K/k \), i.e. the kernel of the norm map \( R_{K/k}(\mathbb{G}_m) \rightarrow \mathbb{G}_m \) where \( R_{K/k} \) is the Weil restriction (see [Vos98] page 37, Section 3.12]). The norm one torus \( R_{K/k}(\mathbb{G}_m) \) has the Chevalley module \( J_{K/H} \) as its character module and the field \( L(J_{K/H})^G \) as its function field where \( J_{K/H} = (I_{G/H})^\circ \) is the dual lattice of \( I_{G/H} = \text{Ker} \varepsilon \) and \( \varepsilon : \mathbb{Z}[G/H] \rightarrow \mathbb{Z} \) is the augmentation map (see [Vos98] Section 4.8]). We have the exact sequence \( 0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Z}[G/H] \rightarrow J_{K/H} \rightarrow 0 \) and \( \text{rank}_\mathbb{Z}(J_{K/H}) = n - 1 \). Write \( J_{K/H} = \oplus_{1 \leq i \leq n} \mathbb{Z}x_i \). Then the action of \( G \) on \( L(J_{K/H}) = L(x_1, \ldots, x_{n-1}) \) is nothing but \( (1) \).

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 \textit{stably $k$-isomorphic} if $K(y_1, \ldots, y_m) \cong K'(z_1, \ldots, z_n)$ 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 \textit{retracted $k$-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 $\varphi : R \to k[x_1, \ldots, x_n]/[f] \rightarrow R$ satisfying $\psi \circ \varphi = 1_R$ (cf. [Sal84]). $K$ is called \textit{$k$-universal} if $K \subset k(x_1, \ldots, x_n)$ for some integer $n$. It is not difficult to see that “$k$-universal” $\Rightarrow$ “stably $k$-rational” $\Rightarrow$ “retract $k$-rational” $\Rightarrow$ “$k$-universal”.

The 1-dimensional algebraic $k$-tori, i.e. the trivial torus $G_m$ and the norm one torus $R_{K/k}^{1}(G_m)$ with $[K : k] = 2$, are $k$-rational. Voskresenskii [Vos67] showed that all the 2-dimensional algebraic $k$-tori are $k$-rational. A rational (stably rational, retract rational) classification of 3-dimensional $k$-tori is given by Kunyavskii [Kun90]. A stably and retract rational classification of algebraic $k$-tori of dimension 4 and 5 is given by Hoshi and Yamasaki [HY17] Theorem 1.9, Theorem 1.12.

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 $F_{pm} \cong C_p \times C_m \leq S_p$ be the Frobenius group of order $pm$ where $m | p - 1$. Let $nTm$ be the $m$-th 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]). The rationality problem for norm one tori $R_{K/k}^{1}(G_m)$ is investigated by [EM75], [CTS77], [Hir84], [CTS87], [LeB95], [CK00], [LL00], [Pla], [End11], [HY17] and [HY]. In the previous papers [HY17] and [HY], a stably retract rational classification of norm one tori $R_{K/k}^{1}(G_m)$ of dimension $p - 1$ where $p$ is a prime number and of dimension $n \leq 5$ is given except for the following three cases: (i) $G = \text{PSL}_2(\mathbb{F}_p)$ where $p = 2^r + 1$ is a Fermat prime; (ii) $G = 9T27 \simeq \text{PSL}_2(\mathbb{F}_8)$; (iii) $G = 10T11 \simeq A_5 \times C_2$.

The first main results of this paper are Theorem 1.1 and Theorem 1.2 which give a stably and retract rational classification of norm one tori $R_{K/k}^{1}(G_m)$ of dimension $n - 1$ for $n = 2^r (e \geq 1)$ and $n = 10, 12, 14, 15$ respectively. 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 $G = 10T11 \simeq A_5 \times C_2$.

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

\textbf{Theorem 1.2.} Let $K/k$ be a separable field extension of degree $n$ and $L/k$ be the Galois closure of $K/k$. Assume that $G = \text{Gal}(L/k)$ is a transitive subgroup of $S_n$ and $H = \text{Gal}(L/K)$ with $[G : H] = n$. Then a stably and retract rational classification of norm one tori $T = R_{K/k}^{1}(G_m)$ of 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 $10T11 \simeq C_{10}$, $10T2 \simeq D_5$, $10T3 \simeq D_{10}$, $10T11 \simeq A_5 \times C_2$;
   (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 $12T11 \simeq C_{12}$, $12T7 \simeq C_3 \times C_4$, $12T11 \simeq C_4 \times S_3$;
   (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 $14T4 \simeq F_{42}$, $14T5 \simeq F_{21} \times C_2$, $14T7 \simeq F_{42} \times C_2$, $14T16 \simeq \text{PSL}_3(\mathbb{F}_2) \times C_2$, $14T19 \simeq \text{PSL}_4(\mathbb{F}_2) \times C_2$, $14T46 \simeq S_7$, $14T47 \simeq A_7 \times C_2$, $14T49 \simeq S_7 \times C_2$;
   (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 $15T1 \simeq C_{15}$, $15T2 \simeq D_{15}$, $15T3 \simeq D_5 \times C_3$, $15T4 \simeq S_3 \times C_5$, $15T5 \simeq A_5$, $15T7 \simeq A_5 \times S_5$, $15T16 \simeq A_5 \times C_3 \simeq GL_2(\mathbb{F}_4)$, $15T23 \simeq A_5 \times S_5$;
   (ii) $T$ is not stably $k$-rational but retract $k$-rational for $15T6 \simeq C_{15} \times C_4$, $15T8 \simeq F_{20} \times C_3$, $15T10 \simeq S_5$, $15T11 \simeq F_{20} \times S_3$, $15T22 \simeq (A_5 \times C_3) \times C_2 \simeq GL_2(\mathbb{F}_4) \times C_2$, $15T24 \simeq S_5 \times C_3$, $15T29 \simeq S_5 \times S_5$;
   (iii) $T$ is not retract $k$-rational for $15Tm$ with $9 \leq m \leq 104$ and $m \neq 10, 11, 16, 22, 23, 24, 29$. 

S. HASEGA WA, A. HOSHI, AND A. YAMASAKI
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 $L/k$ be the Galois closure of $K/k$. Let $G = \text{Gal}(L/k)$ be a transitive subgroup of $S_n$ and $H = \text{Gal}(L/K)$ with $[G : H] = n$. Assume that $n = q + 1$ where $q = l^r \equiv 1 \pmod{4}$ is an odd prime power and $\text{PSL}_2(\mathbb{F}_q) \leq G \leq \text{PGL}_2(\mathbb{F}_q) \cong \text{PGL}_2(\mathbb{F}_q) \rtimes C_e$. Then $R_{K/k}^{(1)}(G_m)$ is not retract $k$-rational.

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

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

More precisely, $R_{K/k}^{(1)}(G_m)$ 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 $G = \text{Aut}(M_{22}) \simeq M_{22} \rtimes C_2 \leq S_{22}$ where $M_{22}$ is the Mathieu group of degree 22;
(iv) $\text{PSL}_2(\mathbb{F}_q) \leq G \leq \text{PGL}_2(\mathbb{F}_q) \cong \text{PGL}_2(\mathbb{F}_q) \rtimes C_e$ where $2p = q + 1$ and $q = l^r$ 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) $10T7 \simeq A_5$, $10T13 \simeq S_5$, $10T26 \simeq \text{PSL}_2(\mathbb{F}_9) \simeq A_6$, $10T30 \simeq \text{PGL}_2(\mathbb{F}_9)$, $10T31 \simeq M_{10}$, $10T32 \simeq S_6$, $10T35 \simeq \text{PGL}_2(\mathbb{F}_9)$, $10T44 \simeq A_{18}$, $10T45 \simeq S_{10}$.

(ii) $12T179 \simeq \text{PSL}_2(\mathbb{F}_{11})$, $12T218 \simeq \text{PGL}_2(\mathbb{F}_{11})$, $12T272 \simeq M_{11}$, $12T295 \simeq M_{12}$, $12T300 \simeq A_{12}$, $12T301 \simeq S_{12}$.

(iii) $14T30 \simeq \text{PSL}_2(\mathbb{F}_{13})$, $14T39 \simeq \text{PGL}_2(\mathbb{F}_{13})$, $14T62 \simeq A_{14}$, $14T63 \simeq S_{14}$.

(iv) $15T20 \simeq A_6$, $15T28 \simeq S_6$, $15T47 \simeq A_7$, $15T72 \simeq A_8 \simeq \text{PSL}_4(\mathbb{F}_2)$, $15T103 \simeq A_{15}$, $15T104 \simeq S_{15}$.

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 $L/k$ be the Galois closure of $K/k$. Let $G = \text{Gal}(L/k)$ be a transitive subgroup of $S_n$ and $H = \text{Gal}(L/K)$ 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 $R_{K/k}^{(1)}(G_m)$ is not retract $k$-rational.

We organize this paper as follows. In Section 2 we prepare some basic tools to prove stably and 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 Theorem 1.3, Theorem 1.4 and Theorem 1.6 in Section 5.

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

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

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 \cite{CTS77}, Swan \cite{Swa83}, Voskresenskii \cite{Vos98} Chapter 2], Lorenz \cite{Lor03} Chapter 2], Swan \cite{Swa10}.

**Definition 2.1.** Let $G$ be a finite group and $M$ 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. $M \simeq \oplus_{1 \leq i \leq m} \mathbb{Z}[G/H_i]$ 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 $\tilde{H}^{-1}(H, M) = 0$ for any subgroup $H$ of $G$ where $\tilde{H}$ is the Tate cohomology.

(v) $M$ is called coflabbly (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 $C(G)$ be the category of all $G$-lattices. Let $S(G)$ be the full subcategory of $C(G)$ of all permutation $G$-lattices and $D(G)$ be the full subcategory of $C(G)$ of all invertible $G$-lattices. Let
\[ \mathcal{H}^i(G) = \{ M \in C(G) \mid \mathring{H}^i(H, M) = 0 \text{ for any } H \leq G \} \quad (i = \pm 1) \]
be the class of “$\mathring{H}^i$-vanish” $G$-lattices where $\mathring{H}^i$ is the Tate cohomology. Then we have the inclusions $S(G) \subset D(G) \subset \mathcal{H}^i(G) \subset C(G) \quad (i = \pm 1)$.

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 (Endo and Miyata [EM75] Lemma 1.1, Colliot-Thélène and Sansuc [CTS77] Lemma 3), see also [Swa83] Lemma 8.5, [Lor03] 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 $[M]^{fl}$. 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. Swan [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
\[
\text{permutation } \Rightarrow \text{ stably permutation } \Rightarrow \text{ invertible } \Rightarrow \text{ flabby and coflabby}
\]

\[
[M]^{fl} = 0 \quad \Rightarrow \quad [M]^{fl} \text{ is invertible.}
\]

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 $G = \text{Gal}(L/k)$ and $M$ be a $G$-lattice. The flabby class $\rho_G(M) = [M]^{fl}$ plays 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], Yamasaki [Yam12]):

Theorem 2.7 (Endo and Miyata, Voskresenskii, Saltman). Let $L/k$ be a finite Galois extension with Galois group $G = \text{Gal}(L/k)$. Let $M$ and $M'$ be $G$-lattices.
(i) (Endo and Miyata [EM75] 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 $-[M_1]^{fl} = [[M_2]^{fl}]^{fl}$.

Definition 2.9. Let $G$ be a finite subgroup of $\text{GL}_n(\mathbb{Z})$. The $G$-lattice $M_G$ with 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 $\text{GL}_n(\mathbb{Z})$ and $M_G$ be the corresponding $G$-lattice as in Definition 2.7. 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 \ref{thm:main}}

In order to prove Theorem \ref{thm:main}, we show the following two theorems.

**Theorem 3.1.** Let n = p^r be a prime power and G be a transitive subgroup of S_n. Let G_p = 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 H_p be a p-Sylow subgroup of H with H_p ≤ 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^r. Hence H_p = G_p ∩ H becomes the stabilizer of one of the letters in G_p and G_p ≤ S_n is transitive. ∎

**Theorem 3.2.** Let n = 2^e be a power of 2 and G be a transitive subgroup of S_n. Let G_2 = Syl_2(G) be a 2-Sylow subgroup of G. If G_2 ∼= C_n, then G ∼= 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 σ \rangle ∼= C_n where n = 2^e. Without loss of generality, we may assume that σ = (1 \cdots n) ∈ 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 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 ∼= C_n and N_{S_n}(G_2) = C_n ∝ Aut(C_n) ∼= \mathbb{Z}/2^e\mathbb{Z} × (\mathbb{Z}/2^e\mathbb{Z})^×. We also have G_2 = Z_G(G_2) ≤ N_G(G_2) ≤ 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 ∈ G | ord(x) = n\} be the set of elements of order n in G and A_2 = \{x ∈ G_2 | ord(x) = n\} = \{σ^1 | i: odd\} be the set of elements of order n in G_2. If g ∈ G_2, then gag^{-1} = a for any a ∈ A_2. If g ∈ G \setminus G_2, then gag^{-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 ∈ G_2. Hence we have |A| = |A_2| ∩ |G : G_2| = 2^{e−1}. |H| = |G|/2. This implies that A = \{x ∈ G | sgn(x) = 1\}.

We claim that if h(j) = k (h ∈ H), then j ≡ k (mod 2). Suppose not. Then there exists σ^{j-k}h(j) = j. But this is impossible because sgn(σ^{j-k}h) = −1 and hence ord(σ^{j-k}h) = n. This claim implies that \langle σ^2, H \rangle acts on 2\mathbb{Z}/n\mathbb{Z} = \{2, 4, \ldots, n\}.

On the other hand, \langle σ^2, H \rangle ≤ G ∩ A_n because sgn(σ^2) = sgn(h) = 1 (h ∈ H). We also see \langle σ^2, H \rangle = G ∩ A_n because [(σ^2, H) : H] = n/2.

Remember that |H| = |G : G_2| is odd. The restriction G ∩ A_n ≼ \mathbb{Z}/n\mathbb{Z} into 2\mathbb{Z}/n\mathbb{Z} seems to be a transitive subgroup of S_{2\mathbb{Z}/n\mathbb{Z}} whose 2-Sylow subgroup is \langle σ^2 \rangle ≼ \mathbb{Z}/n\mathbb{Z}. By the assumption of induction, we have H_{1+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. ∎

**Proof of Theorem \ref{thm:main}**. Take a transitive subgroup G = Gal(L/k) ≤ S_n (n = 2^e) and H = Gal(L/K) with [G : H] = n. By Theorem \ref{thm:main}, the 2-Sylow subgroup G_2 = Syl_2(G) of G is a transitive subgroup of S_n.

(⇒) Assume that G \not∼= C_n. By Theorem \ref{thm:main}, we have G_2 \not∼= C_n. Hence [J_{G_2/H}] is not invertible by Endo and Miyata [EM75, Theorem 1.5] and Endo [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 \ref{lem:main} (ii) that [J_{G/H}] is not invertible. Hence R_{K/k}(G_m) is not retract k-rational.

(⇐) By Endo and Miyata [EM75, Theorem 2.3], if G ∼= C_n, then R_{K/k}^{(1)}(G_m) is stably k-rational. ∎

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

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

(3) When n = 16, there exist 1954 transitive subgroups of 16Tm ≤ S_16 (1 ≤ m ≤ 1954). There exist 14 groups G = 16Tm (1 ≤ m ≤ 14) with |G| = 16 (see Example \ref{ex:main}): 16T1 ∼= C_{16}, 16T2 ∼= C_4 × (C_2)^2, 16T3 ∼= (C_2)^4, 16T5 ∼= C_4 × C_4, 16T5 ∼= C_2 × C_2, 16T6 ∼= M_{16}, 16T7 ∼= Q_8 × C_2, 16T8 ∼= C_4 × C_4, 16T9 ∼= D_4 × C_2, 16T10 ∼= (C_2 × C_2) × C_2, 16T11 ∼= (C_4 × C_2) × C_2, 16T12 ∼= QD_8, 16T13 ∼= D_8, 16T14 ∼= Q_{16}.

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

**Example 3.4** (Computations for 16Tm ≤ S_16). For G = 16Tm ≤ S_16, Theorem \ref{thm:main} and Theorem \ref{thm:main} can be checked by GAP as follows:

```gap
gap> NrTransitiveGroups(16); # the number of transitive subgroups G=16Tm <= S16
1954

gap> Sy16:=List([1..1954],x->SylowSubgroup(TransitiveGroup(16,x),2));;
```
4. Proof of Theorem 1.2

Let $K/k$ be a separable field extension of degree $n$ and $L/k$ be the Galois closure of $K/k$. Let $G = \text{Gal}(L/k)$ be a transitive subgroup of $S_n$ and $H = \text{Gal}(L/K)$ 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 $m$-th transitive subgroup of $S_n$ (see Butler and McKay [BMS] for $n \leq 11$, Royle [Roy] for $n = 12$, Butler [But] for $n = 14, 15$ and [GAP]).

We provide the following GAP algorithm to certify whether $F = [J_G/H]^f$ 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]):
NormTorusJ(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 $F = [J_G/H]^f$ is invertible:
IsInvertibleF(NormTorusJ(n,m)) returns true (resp. false) if $[J_G/H]^f$ 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 $F = [J_G/H]^f$:
PossibilityOfStablyPermutationF(NormTorusJ(n,m)) returns a basis $\mathcal{L} = \{1, \ldots, l_s\}$ 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

$$\bigoplus_{i=1}^r \mathbb{Z}[G/H_1]^{\oplus a_i} \cong F^{\oplus (-b_1)}$$

for $G = nTm \leq S_n$, $H$ is the stabilizer of one of the letters in $G$ and $F = [J_G/H]^f$. In particular, if all the $b_1$’s are even, then we can conclude that $F = [J_G/H]^f \neq 0$.

(3) Verification of $F = 0$ where $F = [J_G/H]^f$:
FlabbyResolutionLowRankFromGroup(NormTorusJ(n,m),TransitiveGroup(n,m)).actionF returns a suitable flabby class $F = [J_G/H]^f$ 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 $[J_G/H]^{f_n} := [[J_G/H]^{f_{n-1}}][f_1]$ inductively, $[J_G/H]^{f_n} = 0$ is provided if we may find some $n$ with $[J_G/H]^{f_n} = 0$ (this method is slightly improved to the flit algorithm, see [HY17, Section 5.3]).

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 3).

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

By [HY17, 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 $F = [J_G/H]^f$ with rank$_{\mathbb{Z}}(F) = 31$, $F' = [F]^f$ with rank$_{\mathbb{Z}}(F') = 13$ and $F'' = [F']^f$ with $F'' = [\mathbb{Z}] = 0$. This implies that $F = 0$ and hence $T$ is stably k-rational (see 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 $12T1 \simeq C_{15}$, $12T2 \simeq C_6 \times C_2$, $12T3 \simeq D_6$, $12T4 \simeq A_4$, $12T5 \simeq C_3 \times C_4$, $K/k$ is a Galois extension. By Endo and Miyata [EM75, Theorem 2.3], $T$ is stably $k$-rational for $12T1$, $12T5$. By Endo 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 $\text{rank}_{\mathbb{Z}}(F) = 17$, $F' = [I_{G/H}]^{fl}$ with $\text{rank}_{\mathbb{Z}}(F') = 4$ and $F'$ is permutation. This implies that $F = 0$ and hence $T$ is stably $k$-rational (see 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 Example 4.3 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 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 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 Endo 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 $\text{rank}_{\mathbb{Z}}(F) = 17$ and $F' = [I_{G/H}]^{fl} \cong \mathbb{Z}^2$ which is permutation. This implies that $F = 0$ and hence $T$ is stably $k$-rational by Theorem $2.7$ (i) (see Example 4.3).

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 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 Example 4.3), 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 Example 4.3).

(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 Endo 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 Endo [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 \( \langle J \rangle \) 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 \( F = \langle J \rangle \) with rank \( \mathbb{Z} \). This implies that \( F = 0 \) and hence \( T \) is stably \( k \)-rational.

For \( 15T7 \simeq D_5 \times S_3, 15T16 \simeq A_5 \times C_4, 15T23 \simeq A_5 \times S_3 \), it is enough to prove that \( [G/H]^{fl} = 0 \) for \( G = 15T23 \) because \( 15T7 \leq 15T23, 15T16 \leq 15T23 \) and Lemma 2.10 (i). By Algorithm 4.1 (3), we obtain that \( F = [J/H]^{fl} \) with rank \( \mathbb{Z} \). This implies that \( F = 0 \) and hence \( T \) is stably \( k \)-rational.

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

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

For \( m = 11, 22, 24, 29 \), by Algorithm 4.1 (1), we see that \( [J/H]^{fl} \) is invertible and hence \( T \) is retract \( k \)-rational. By Lemma 2.10 (i) and the inclusions \( 15T6 \leq 15T11, 15T22, 15T29, 15T8 \leq 15T24 \), we obtain that \( [J/H]^{fl} \neq 0 \) 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
\[
\text{List([1..104],x->Filtered([1..x],y->IsSubgroup(TransitiveGroup(15,x), TransitiveGroup(15,y))))}
\]
in GAP [GAP] (see also Example 4.4 for the case where \( n = 14 \)), we obtain the inclusions \( 15Tm \leq 15Tm' \) among the groups \( G = 15Tm \) with \( m \in I_{15} := \{ 9, 15, 20, 26 \} \).

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

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

Example 4.2 (Computations for \( 10T11 \leq S_{10} \)).

```
gap> Read("FlabbyResolutionFromBase.gap");

gap> J:=Norm1TorusJ(10,11);
< matrix group with 3 generators >
gap> StructureDescription(J);
"C2 x A5"
gap> IsInvertibleF(J); # 10T11 is retract k-rational
true
gap> T:=TransitiveGroup(10,11);
A(5)[x]2
gap> F:=FlabbyResolutionLowRankFromGroup(J,T).actionF;
<matrix group with 3 generators>
gap> Rank(F.1); # F is of rank 31
31
gap> F2:=FlabbyResolutionLowRankFromGroup(F,T).actionF;
<matrix group with 3 generators>
gap> Rank(F2.1); # [ F]^f1 is of rank 13
13
gap> F3:=FlabbyResolutionLowRankFromGroup(F2,T).actionF;
# 10T11 is stably k-rational because [ F]^f1=0
Group([ [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ])
```

Example 4.3 (Computations for $12Tm \leq S_{12}$).

gap> Read("FlabbyResolutionFromBase.gap");

gap> J:=Norm1TorusJ(12,11);
<matrix group with 3 generators>

gap> StructureDescription(J);
"C4 x S3"

gap> IsInvertibleF(J); # 12T11 is retract k-rational
true

gap> T:=TransitiveGroup(12,11);
S(3)[x]C(4)

gap> F:=FlabbyResolutionLowRankFromGroup(J,T).actionF;
<matrix group with 3 generators>

gap> Rank(F.1); # F is of rank 17
17

gap> F2:=FlabbyResolutionLowRankFromGroup(F,T).actionF;
<matrix group with 3 generators>

gap> Rank(F2.1); # [F]^fl is of rank 4
4

gap> GeneratorsOfGroup(F2);
[ [ 1, 0, 0, 0 ], [ 0, 1, 0, 0 ], [ 0, 0, 1, 0 ], [ 0, 0, 0, 1 ] ],
[ [ 1, 0, 0, 0 ], [ 0, 1, 0, 0 ], [ 0, 0, 1, 0 ], [ 0, 0, 0, 1 ] ],
[ [ 0, 1, 1, 2 ], [ 0, 1, 0, 0 ], [ 3, -3, -2, -6 ], [ -1, 1, 1, 3 ] ]

gap> F3:=FlabbyResolutionLowRankFromGroup(F2,T).actionF;
# 12T11 is stably k-rational because [F]^fl is permutation
[ ]

gap> IsInvertibleF(Norm1TorusJ(12,2)); # 12T2 is not retract k-rational
false

gap> IsInvertibleF(Norm1TorusJ(12,3)); # 12T3 is not retract k-rational
false

gap> IsInvertibleF(Norm1TorusJ(12,4)); # 12T4 is not retract k-rational
false

gap> IsInvertibleF(Norm1TorusJ(12,7)); # 12T7 is not retract k-rational
false

gap> IsInvertibleF(Norm1TorusJ(12,8)); # 12T8 is not retract k-rational
false

gap> IsInvertibleF(Norm1TorusJ(12,9)); # 12T9 is not retract k-rational
false

gap> IsInvertibleF(Norm1TorusJ(12,12)); # 12T12 is not retract k-rational
false

gap> IsInvertibleF(Norm1TorusJ(12,15)); # 12T15 is not retract k-rational
false

gap> IsInvertibleF(Norm1TorusJ(12,16)); # 12T16 is not retract k-rational
false

gap> IsInvertibleF(Norm1TorusJ(12,17)); # 12T17 is not retract k-rational
false

gap> IsInvertibleF(Norm1TorusJ(12,19)); # 12T19 is not retract k-rational
false

gap> IsInvertibleF(Norm1TorusJ(12,29)); # 12T29 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,30)); # 12T30 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,31)); # 12T31 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,32)); # 12T32 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,33)); # 12T33 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,34)); # 12T34 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,36)); # 12T36 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,40)); # 12T40 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,41)); # 12T41 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,46)); # 12T46 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,47)); # 12T47 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,57)); # 12T57 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,58)); # 12T58 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,59)); # 12T59 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,60)); # 12T60 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,61)); # 12T61 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,63)); # 12T63 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,64)); # 12T64 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,65)); # 12T65 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,66)); # 12T66 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,68)); # 12T68 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,69)); # 12T69 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,70)); # 12T70 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,73)); # 12T73 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,74)); # 12T74 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,75)); # 12T75 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,76)); # 12T76 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,89)); # 12T89 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,91)); # 12T91 is not retract k-rational
false

gap> IsInvertibleF(Norm1TorusJ(12,93)); # 12T93 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,96)); # 12T96 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,99)); # 12T99 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,100)); # 12T100 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,102)); # 12T102 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,105)); # 12T105 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,107)); # 12T107 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,160)); # 12T160 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,162)); # 12T162 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,166)); # 12T166 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,171)); # 12T171 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,172)); # 12T172 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,173)); # 12T173 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,179)); # 12T179 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,181)); # 12T181 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,182)); # 12T182 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,183)); # 12T183 is not retract k-rational
false
gap> IsInvertibleF(Norm1TorusJ(12,246)); # 12T246 is not retract k-rational
false

gap> List(Filtered(List(ConjugacyClassesSubgroups(TransitiveGroup(12,207)),
> Representative),x->Length(Orbits(x,[1..12]))=1),Size);
[ 576, 1152 ]
gap> List(Filtered(List(ConjugacyClassesSubgroups(TransitiveGroup(12,212)),
> Representative),x->Length(Orbits(x,[1..12]))=1),Size);
[ 72, 72, 72, 72, 72, 144, 144, 648, 648, 1296 ]
gap> List(Filtered(List(ConjugacyClassesSubgroups(TransitiveGroup(12,216)),
> Representative),x->Length(Orbits(x,[1..12]))=1),Size);
[ 72, 72, 72, 72, 144, 144, 648, 648, 1296 ]
gap> List(Filtered(List(ConjugacyClassesSubgroups(TransitiveGroup(12,254)),
> Representative),x->Length(Orbits(x,[1..12]))=1),Size);
[ 576, 576, 1152, 1728, 3456 ]
gap> List(Filtered(List(ConjugacyClassesSubgroups(TransitiveGroup(12,272)),
> Representative),x->Length(Orbits(x,[1..12]))=1),Size);
[ 72, 72, 72, 144, 720, 7920 ]
gap> List(Filtered(List(ConjugacyClassesSubgroups(TransitiveGroup(12,278)),
> Representative),x->Length(Orbits(x,[1..12]))=1),Size);
Example 4.4 (Computations for $14Tm \leq S_{14}$).

gap> Read("FlabbyResolutionFromBase.gap");

gap> List([1..63],x->Filtered([1..x],y->IsSubgroup(TransitiveGroup(14,x),
> TransitiveGroup(14,y))));
[[1], [2], [1, 2, 3], [2, 4], [1, 5], [6], [1, 2, 3, 4, 5, 7],
[1, 8], [1, 6, 9], [10], [6, 11], [12], [1, 2, 3, 8, 13],
[1, 5, 8, 14], [1, 8, 15], [16], [1, 5, 10, 17],
[1, 5, 6, 9, 11, 18], [1, 5, 19], [1, 2, 3, 8, 12, 13, 20], [6, 21],
[12, 22], [12, 23], [1, 2, 3, 4, 5, 7, 8, 13, 14, 24],
[1, 2, 3, 8, 13, 15, 25], [26], [2, 6, 21, 27], [6, 21, 28],
[1, 6, 9, 21, 29], [30], [1, 2, 3, 8, 12, 13, 15, 20, 22, 25, 31],
[1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 20, 23, 24, 32], [6, 11, 33],
[6, 10, 11, 34], [6, 11, 21, 35], [12, 22, 23, 36],
[1, 2, 3, 4, 5, 7, 8, 13, 14, 15, 24, 25, 37],
[1, 2, 3, 6, 9, 21, 27, 28, 29, 38], [30, 39],
[2, 4, 6, 11, 21, 27, 35, 40], [6, 11, 21, 28, 35, 41],
[1, 5, 6, 9, 11, 18, 33, 42], [1, 5, 6, 9, 10, 11, 17, 18, 19, 34, 43],
[1, 5, 6, 9, 11, 18, 21, 29, 35, 44],
[1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 15, 20, 22, 23, 24, 25, 31, 32, 36, 37, 45],
[2, 4, 46], [1, 5, 19, 47],
[1, 2, 3, 4, 5, 6, 7, 9, 11, 18, 21, 27, 28, 29, 35, 38, 40, 41, 44, 48],
[1, 2, 3, 4, 5, 7, 19, 46, 47, 49], [6, 10, 11, 21, 23, 34, 35, 50],
[1, 5, 6, 9, 10, 11, 17, 18, 19, 21, 29, 33, 34, 35, 42, 43, 44, 50, 51],
[1, 5, 8, 14, 15, 16, 19, 52], [6, 10, 11, 21, 33, 34, 35, 50, 53],
[2, 4, 6, 10, 11, 21, 27, 33, 34, 35, 40, 46, 50, 53, 54],
[6, 10, 11, 21, 28, 33, 34, 35, 41, 50, 53, 55],
[1, 5, 6, 9, 10, 11, 17, 18, 19, 21, 29, 33, 34, 35, 42, 43, 44, 47, 50, 51, 53, 56],
[1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 17, 18, 19, 21, 27, 28, 29, 33, 34, 35, 38, 40, 41, 42, 43, 44, 46, 47, 48, 49, 50, 51, 53, 54, 55, 56, 57],
[1, 5, 8, 14, 15, 16, 19, 26, 47, 52, 58], [12, 22, 23, 36, 59],
[1, 2, 3, 4, 5, 7, 8, 13, 14, 15, 16, 19, 24, 25, 26, 37, 46, 47, 49, 52, 58, 60],
[1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 15, 16, 19, 20, 22, 23, 24, 25, 26, 31, 32, 36, 37, 45, 46, 47, 49, 52, 58, 59, 60, 61],
[6, 10, 11, 12, 21, 22, 23, 28, 30, 33, 34, 35, 36, 41, 50, 53, 55, 59, 62],
[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63]]

gap> IsInvertibleF(Norm1TorusJ(14,4)); # 14T4 is retract k-rational
true

gap> IsInvertibleF(Norm1TorusJ(14,5)); # 14T5 is retract k-rational
true
gap> IsInvertibleF(Norm1TorusJ(14,7)); # 14T7 is retract k-rational
true
gap> IsInvertibleF(Norm1TorusJ(14,16)); # 14T16 is retract k-rational
true
gap> IsInvertibleF(Norm1TorusJ(14,19)); # 14T19 is retract k-rational
true
gap> IsInvertibleF(Norm1TorusJ(14,46)); # 14T46 is retract k-rational
true
gap> IsInvertibleF(Norm1TorusJ(14,47)); # 14T47 is retract k-rational
true
gap> IsInvertibleF(Norm1TorusJ(14,49)); # 14T49 is retract k-rational
true

gap> PossibilityOfStablyPermutationF(Norm1TorusJ(14,4)); # 14T4 is not stably k-rational by Algorithm 4.1 (2)
[ [ 1, 1, 1, 1, -1, -1, 1, -2 ] ]
gap> PossibilityOfStablyPermutationF(Norm1TorusJ(14,5)); # 14T5 is not stably k-rational by Algorithm 4.1 (2)
[ [ 2, -1, 0, 3, 0, 1, 0, -1, -2 ] ]
gap> PossibilityOfStablyPermutationF(Norm1TorusJ(14,16)); # 14T16 is not stably k-rational by Algorithm 4.1 (2)
[ [ 1, 0, 0, 0, 0, 0, -3, 0, 2, 0, 1, 2, 2, 1, -4, 4 ], [ 0, 1, 0, 0, 0, -1, -1, 0, 1, 0, 1, 0, 1, 1, 0, -1, 0 ], [ 0, 0, 1, 0, 0, 0, -1, -1, -1, -2, 0, 0, 0, 1, 1, -1, 1 ], [ 0, 0, 0, 1, 0, 0, -1, 0, 0, 0, 0, 0, 1, 0, 1, -1, 1 ], [ 0, 0, 0, 0, 1, 0, 1, -1, 0, 0, -3, -1, -1, 2, 3, -1, 0 ] ]
Example 4.5 (Computations for $15Tm \leq S_{15}$).

```
gap> Read("FlabbyResolutionFromBase.gap");

gap> J:=Norm1TorusJ(15,5);
<matrix group with 2 generators>
gap> StructureDescription(J);
"A5"
gap> IsInvertibleF(J); # 15T5 is retract k-rational
true
gap> T:=TransitiveGroup(15,5);
A_5(15)
gap> F:=FlabbyResolutionLowRankFromGroup(J,T).actionF;
<matrix group with 2 generators>
gap> Rank(F.1); # F is of rank 21
21
gap> F2:=FlabbyResolutionLowRankFromGroup(F,T).actionF;
# 15T5 is stably k-rational because [F]^fl=0
Group([ [ [ 1 ] ], [ [ 1 ] ] ])

gap> J:=Norm1TorusJ(15,23);
<matrix group with 3 generators>
gap> StructureDescription(J);
"A5 x S3"
gap> IsInvertibleF(J); # 15T23 is retract k-rational
true
gap> T:=TransitiveGroup(15,23);
A(5)[x]S(3)
gap> F:=FlabbyResolutionLowRankFromGroup(J,T).actionF;
<matrix group with 3 generators>
gap> Rank(F.1); # F is of rank 27
27
gap> F2:=FlabbyResolutionLowRankFromGroup(F,T).actionF;
<matrix group with 3 generators>
gap> Rank(F2.1); # [F]^fl is of rank 8
8
gap> F3:=FlabbyResolutionLowRankFromGroup(F2,T).actionF;
# 15T23 is stably k-rational because [[F]^fl]^fl=0
Group([ [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ])

gap> IsInvertibleF(Norm1TorusJ(15,10)); # 15T10 is retract k-rational
true
gap> PossibilityOfStablyPermutationF(Norm1TorusJ(15,10));
# 15T10 is not stably k-rational by Algorithm 4.1 (2)
[ [ 1, 0, 0, 0, 0, 0, 8, 1, -2, 5, -3, 2, 2, 5, 0, -8, -10, -3, 8, -2 ], [ 0, 1, 0, 0, 0, -1, -1, 0, 0, -1, 0, 0, 0, 1, 1, 1, 0, -1, 0 ], [ 0, 0, 1, 0, 0, -2, 0, 0, -1, 1, 0, -1, -1, 0, 2, 2, 1, -2, 0 ], [ 0, 0, 0, 1, 0, 0, 12, 1, -3, 7, -5, 2, 3, 6, 0, -12, -14, -4, 12, -2 ], [ 0, 0, 0, 0, 1, 2, -2, 0, 1, -2, 2, -2, -1, -2, -2, 2, 4, 1, -2, 0 ]]

gap> IsInvertibleF(Norm1TorusJ(15,11)); # 15T11 is retract k-rational
true
The action of $1 \leq B$ where

Let $F$ and $PΓL$

Step 2. Take a subgroup $V$ and $M$.

By Lemma 2.10 (ii), we should show that $\psi \sigma$.

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 $G = PSL_2(\mathbb{F}_q)$ because $PSL_2(\mathbb{F}_q) \leq G \leq PGL_2(\mathbb{F}_q)$ and Lemma 2.10 (ii). The group $G = PSL_2(\mathbb{F}_q)$ 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 $\mathbb{F}_q^\times = \{1, -1, \sqrt{-1}, -\sqrt{-1}, u, -u, u^{-1}, -u^{-1} \mid 1 \leq i \leq \frac{q-3}{4}\}$ because $q \equiv 1 \pmod{4}$.

Step 2. Take a subgroup $V_4 = \langle \sigma, \tau \rangle \simeq C_2 \times C_2 \leq G = PSL_2(\mathbb{F}_q)$ as

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

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

$$\sigma : e_1 \leftrightarrow e_{-1}, \quad e_\sqrt{-1} \leftrightarrow e_{-\sqrt{-1}}, \quad e_u \leftrightarrow e_{-u}, \quad e_{-u} \leftrightarrow e_u, \quad e_0 \leftrightarrow e_0, \quad e_\infty \leftrightarrow e_\infty,$$

$$\tau : e_1 \leftrightarrow e_{-1}, \quad e_{\sqrt{-1}} \leftrightarrow e_{-\sqrt{-1}}, \quad e_u \leftrightarrow e_{-u}, \quad e_{-u} \leftrightarrow e_u, \quad e_0 \leftrightarrow e_{\infty},$$

$$\sigma \tau : e_{\pm 1} \leftrightarrow e_{\pm 1}, \quad e_{\sqrt{-1}} \leftrightarrow e_{-\sqrt{-1}}, \quad e_{u^i} \leftrightarrow e_{-u^i}, \quad e_{-u^i} \leftrightarrow e_{u^i}, \quad e_0 \leftrightarrow e_\infty$$

where $B = \{e_1, e_{-1}, e_{\sqrt{-1}}, e_{-\sqrt{-1}}, e_u, e_{-u}, e_{u^{-1}}, e_{-u^{-1}}, e_0 \mid 1 \leq i \leq \frac{q-5}{4}\}$ 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 $\text{rank}_\mathbb{Z}(M) = q = n-1$.

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

5. Proof of Theorem 1.3, Theorem 1.4 and Theorem 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 3-1. The actions of $\sigma$ and $\tau$ on $M$ are represented as matrices

\[
\begin{pmatrix}
0 & 1 & 0 \\
1 & 0 & 0 \\
0 & 0 & 1 \\
0 & 0 & 0
\end{pmatrix}
\quad \quad \quad
\begin{pmatrix}
0 & 1 & 0 \\
1 & 0 & 0 \\
0 & 0 & 1 \\
0 & 0 & 0
\end{pmatrix}
\]

Let $B^* = \{e_1^*, e_{-1}^*, e_{-\sqrt{5}}^*, e_{\sqrt{5}}^*, e_{-u}^*, e_{u}^*, e_{-u^*}^*, e_{u^*}^*, e_0^* \mid 1 \leq i \leq \frac{\sqrt{5}-1}{2}\}$ be the dual basis of $B$. By the definition, $B^*$ is a $\mathbb{Z}$-basis of the $G$-lattice $I_{G/H} = (J_{G/H})^o$. The action of $V_4 = \langle \sigma, \tau \rangle$ on $M^o$ is given by

\[
\sigma: e_1^* \leftrightarrow e_{-1}^*, \quad e_{-\sqrt{5}}^* \leftrightarrow e_{\sqrt{5}}^*, \quad e_u^* \leftrightarrow e_{-u}^*, \quad e_{-u^*}^* \leftrightarrow e_{u^*}^*, \quad e_0^* \leftrightarrow e_0^*,
\]

\[
\tau: e_1^* \leftrightarrow e_{-1}^*, \quad e_{-\sqrt{5}}^* \leftrightarrow e_{\sqrt{5}}^*, \quad e_u^* \leftrightarrow e_{-u}^*, \quad e_{-u^*}^* \leftrightarrow e_{u^*}^*, \quad e_0^* \leftrightarrow e_0^*,
\]

\[
\sigma \tau: e_{\pm 1}^* \leftrightarrow e_{\mp 1}^* - e_0^*, \quad e_{\pm \sqrt{5}}^* \leftrightarrow e_{\mp \sqrt{5}}^* - e_0^*, \quad e_u^* \leftrightarrow e_{-u}^*, \quad e_{-u^*}^* \leftrightarrow e_{u^*}^* - e_0^*, \quad e_0^* \leftrightarrow -e_0^*,
\]

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

We define the permutation $V_4$-lattice $P^o$ of $\text{rank}_2(P^o) = g + 5 = n + 4$ with $\mathbb{Z}$-basis

\[
v_1 := v(e_1^*), \quad v_2 := v(e_{-1}^*), \quad v_3 := v(e_{-\sqrt{5}}^*), \quad v_4 := v(e_{\sqrt{5}}^*), \quad v_5 := v(e_{u}^* - e_{-u}^*),
\]

\[
v_6 := v(e_{-u}^*), \quad v_7 := v(e_{u^*}^*), \quad v_8 := v(e_{-u^*}^*), \quad v_9 := v(e_{-\sqrt{5}}^* - e_{\sqrt{5}}^*), \quad v_{10} := v(e_{\sqrt{5}}^* + e_{-\sqrt{5}}^* - e_{u}^*),
\]

\[
v_{1,i} := v(e_{u}^*), \quad v_{1,2} := v(e_{-u}^*), \quad v_{1,3} := v(e_{u^*}^* - e_{-u^*}^*), \quad v_{1,4} := v(e_{-u^*}^* - e_{u^*}^*), \quad (1 \leq i \leq \frac{\sqrt{5}-1}{2})
\]

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

\[
\sigma: v_1 \leftrightarrow v_2, \quad v_3 \leftrightarrow v_4, \quad v_5 \leftrightarrow v_7, \quad v_6 \leftrightarrow v_8, \quad v_9 \leftrightarrow v_{10}, \quad v_{1,i} \leftrightarrow v_{i,2}, \quad v_{1,3} \leftrightarrow v_{i,4},
\]

\[
\tau: v_1 \leftrightarrow v_4, \quad v_2 \leftrightarrow v_3, \quad v_5 \leftrightarrow v_8, \quad v_6 \leftrightarrow v_7, \quad v_9 \leftrightarrow v_{10}, \quad v_{1,i} \leftrightarrow v_{i,2}, \quad v_{1,2} \leftrightarrow v_{i,3},
\]

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

Step 3-2. We define a $V_4$-homomorphism $f: P^o \rightarrow M^o, v(m^*) \mapsto m^* (m^* \in M^o)$. Then $f$ is surjective. We define a $V_4$-lattice $F^o$ as $F^o = \text{Ker}(f)$. Then we obtain an exact sequence $0 \rightarrow F^o \rightarrow P^o \rightarrow M^o \rightarrow 0$ with $\text{rank}_2(F^o) = 5$.

Step 3-3. We will check that $F^o$ is coflabby. In order to prove this assertion, we should check that $\tilde{f} = f|_{H^0(W, P^o)}: H^0(W, P^o) \rightarrow H^0(W, M^o)$ is surjective (hence $H^1(W, F^o) = 0$) for any $W \leq V_4$ where $H^0(W, P^o) \cong \tilde{H}^0(W, P^o) = (P^o)^W$ (see also [HYT] Chapter 2)).
Step 3-3-1. $W = V_4 = \langle \sigma, \tau \rangle$. By the orbit decomposition of the action of $V_4$ on $P^\circ$,

$$\{v_1 + v_2 + v_3 + v_4, v_5, v_6 + v_7 + v_8 + v_9, v_{10}, v_{11} + v_{12} + v_{13} + v_{14} \mid 1 \leq i \leq \frac{q-5}{4}\}$$

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

$$\{e_1^* + e_{-1}^* - e_0^*, e_1^* + e_{-1}^* - e_0^*, e_1^* + e_{-1}^* - e_0^*, e_1^* + e_{-1}^* - e_0^* \mid 1 \leq i \leq \frac{q-5}{4}\}$$

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

$$\bar{f} : v_1 + v_2 + v_3 + v_4 \mapsto 2(e_1^* + e_{-1}^* - e_0^*), \ v_5 \mapsto e_1^* + e_{-1}^* - e_0^*,$$

$$v_6 + v_7 + v_8 + v_9 \mapsto 2(e_1^* + e_{-1}^* - e_0^*), \ v_{10} \mapsto e_1^* + e_{-1}^* - e_0^*,$$

$$v_{11} + v_{12} + v_{13} + v_{14} \mapsto e_{-1}^* + e_{-1}^* - 2e_0^* \quad (1 \leq i \leq \frac{q-5}{4}).$$

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

$$\{v_1 + v_2, v_3 + v_4, v_5, v_6 + v_7 + v_8 + v_9, v_{10}, v_{11} + v_{12}, v_{13} + v_{14} \mid 1 \leq i \leq \frac{q-5}{4}\}$$

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

$$\{e_1^* + e_{-1}^* - e_0^*, e_1^* + e_{-1}^* - e_0^*, e_1^* + e_{-1}^* - e_0^*, e_1^* + e_{-1}^* - e_0^* \mid 1 \leq i \leq \frac{q-5}{4}\}$$

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

$$\bar{f} : v_1 + v_2 \mapsto e_1^* + e_{-1}^* - e_0^*, \ v_3 + v_4 \mapsto e_1^* + e_{-1}^* - e_0^*,$$

$$v_5 \mapsto e_{-1}^* + e_{-1}^* - 2e_0^*, \ v_{10} \mapsto e_{-1}^* + e_{-1}^* - 2e_0^* \quad (1 \leq i \leq \frac{q-5}{4}).$$

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

$$\{v_1 + v_2, v_3 + v_4, v_5, v_6 + v_7 + v_8 + v_9, v_{10}, v_{11} + v_{12}, v_{13} + v_{14} \mid 1 \leq i \leq \frac{q-5}{4}\}$$

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

$$\{e_1^* + e_{-1}^* - e_0^*, e_1^* + e_{-1}^* - e_0^*, e_1^* + e_{-1}^* - e_0^*, e_1^* + e_{-1}^* - e_0^* \mid 1 \leq i \leq \frac{q-5}{4}\}$$

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

$$\bar{f} : v_5 \mapsto e_1^* + e_{-1}^* - e_0^*, \ v_7 + v_9 \mapsto 2e_1^* + e_{-1}^* - e_0^*,$$

$$v_{11} + v_{13} \mapsto e_1^* + e_{-1}^* - e_0^*, \ v_{12} + v_{14} \mapsto e_{-1}^* + e_{-1}^* - e_0^* \quad (1 \leq i \leq \frac{q-5}{4}).$$

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

$$\{v_1 + v_3, v_2 + v_4, v_5, v_6 + v_7 + v_8 + v_9, v_{10}, v_{11} + v_{12}, v_{13} + v_{14} \mid 1 \leq i \leq \frac{q-5}{4}\}$$

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

$$\{e_1^* + e_{-1}^* - e_0^*, 2e_{-1}^* - e_0^*, 2e_{-1}^* - e_0^*, e_1^* + e_{-1}^* - e_0^*, e_{-1}^* + e_{-1}^* - e_0^* \mid 1 \leq i \leq \frac{q-5}{4}\}$$

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

$$\bar{f} : v_5 \mapsto e_1^* + e_{-1}^* - e_0^*, \ v_2 + v_4 \mapsto 2e_{-1}^* - e_0^*,$$

$$v_{11} + v_{13} \mapsto e_1^* + e_{-1}^* - e_0^*, \ v_{12} + v_{14} \mapsto e_{-1}^* + e_{-1}^* - e_0^* \quad (1 \leq i \leq \frac{q-5}{4}).$$

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 $P_\circ$ is permutation $V_4$-lattice and $F_\circ$ is coflabby $V_4$-lattice with rank$_{\mathbb{R}}(F_\circ) = 5$.

The set $\{w_1, w_2, w_3, w_4, w_5\}$ becomes a $Z$-basis of $F_\circ$ where

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

$$w_3 = v_3 + v_4 - v_5 - v_6 - v_7 + v_9 + v_{10},$$

$$w_4 = v_5 - v_7 + v_8 - v_{10},$$

The actions of $\sigma$ and $\tau$ on $F_\circ$ are given by

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

$$\tau : w_1 \mapsto w_1, \ w_2 \mapsto -w_1 + w_3 + w_4 + w_5, \ w_3 \mapsto w_1 + w_2 - w_4 - w_5, \ w_4 \leftrightarrow w_5.$$
and they are represented as matrices

\[
\begin{pmatrix}
0 & 1 & 1 & 0 & 0 \\
1 & 0 & -1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0
\end{pmatrix}
\quad ,
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 \\
-1 & 0 & 1 & 1 & 1 \\
1 & 1 & 0 & -1 & -1 \\
0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0
\end{pmatrix}.
\]

By taking the dual, we get the flabby resolution

\[
0 \to M \to P \to F \to 0
\]

of $M$ and the actions of $\sigma$ and $\tau$ on $F$ are represented as the following matrices (transposed matrices of the above):

\[
S = \begin{pmatrix}
0 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 \\
1 & -1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0
\end{pmatrix},
T = \begin{pmatrix}
-1 & 1 & 0 & 0 & 0 \\
1 & -1 & 0 & 0 & 0 \\
0 & 0 & 0 & -1 & 1 \\
0 & 0 & 0 & 1 & -1 \\
0 & 0 & 0 & 0 & 1
\end{pmatrix}.
\]

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

\[
(S - I \mid T - I) = \begin{pmatrix}
-1 & 1 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\
1 & -1 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\
-1 & -1 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\
0 & 0 & 0 & -1 & 1 & 0 & 1 & -1 & -1 & 1 \\
0 & 0 & 0 & 1 & -1 & 0 & 1 & -1 & 1 & -1
\end{pmatrix}
\]

where $I$ is the $5 \times 5$ identity matrix. Multiply 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

\[
Q (S - I \mid T - I) = \begin{pmatrix}
1 & -1 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\
0 & 0 & 0 & 1 & -1 & 0 & 1 & -1 & 1 & -1 \\
0 & 0 & 0 & 0 & 0 & 2 & -2 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}
\]

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

Let $p$ be a prime number and $G \leq S_{2p}$ be a primitive subgroup. Wielandt ([Wie56, Wie61]) 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 O’Nan-Scott theorem (see Liebeck, Praeger and Saxl [LPS88]), $G$ must be almost simple, i.e. $S \leq G \leq \text{Aut}(S)$ for some non-abelian simple group $S$. The socle $\text{soc}(G) \vartriangleleft G$ 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 $G \leq S_{2p}$ 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 $G = \text{Aut}(M_{22}) \simeq M_{22} \times C_2 \leq S_{22}$ where $M_{22}$ is the Mathieu group of degree 22;
(iv) $\text{PSL}_2(\mathbb{F}_q) \leq G \leq \text{P}{\Gamma}L_2(\mathbb{F}_q) \simeq \text{PGL}_2(\mathbb{F}_q) \times C_e$ where $2p = q + 1$ and $q = l^e$ is an odd prime power.

**Proof of Theorem 5.1**. 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 Endo [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 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 $\text{PSL}_2(F_3) \simeq A_4$, $\text{PGL}_2(F_3) \simeq S_4$, 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 $q = l^r$.

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 Example 5.2). Then $[J_G]^{fl}$ is not invertible by Endo and Miyata [EM75, Theorem 1.5]. It follows from Lemma 2.10 (ii) that $[J_{G/H}]^{fl}$ is not invertible and hence $R_{K/k}(G_m)$ is not retract $k$-rational by Theorem 2.7 (iii).

Example 5.2 (Computations for $22T38 \simeq M_{22} \leq S_{22}$ and $M_{24} \leq S_{24}$).

gap> Read("FlabbyResolutionFromBase.gap");

gap> JM22:=Norm1TorusJ(22,38);
<matrix group with 2 generators>

gap> StructureDescription(JM22);
"M22"

gap> M22:=TransitiveGroup(22,38);

gap> M22s:=List(ConjugacyClassesSubgroups2(M22),Representative);;

gap> JM22s:=ConjugacyClassesSubgroups2FromGroup(JM22,M22);;

gap> JM22s8:=Filtered(JM22s,x->Size(x)=8);;

gap> Length(JM22s8);
12

gap> JM22s8false:=Filtered(JM22s8,x->IsInvertibleF(x)=false);;

# $[J_{G/H}\mid G']^{fl}$ is not invertible

gap> List(JM22s8false,StructureDescription);
[ "C2 x C2 x C2", "Q8", "D8", "C4 x C2" ]

gap> M24:=PrimitiveGroup(24,1);
M(24)

gap> M24s:=Filtered(List(ConjugacyClassesSubgroups2(M24),Representative),
> x->Length(Orbits(x,[1..24]))=1 and Size(x)=24);;

gap> M24s4:=Filtered(M24s,x->IdGroup(x)=[24,12]);;

gap> List(M24s4,StructureDescription);
[ "S4", "S4", "S4" ]

References

[But93] G. Butler, The transitive groups of degree fourteen and fifteen, J. Symbolic Comput. 16 (1993) 413–422.

[BM83] G. Butler, J. McKay, The transitive groups of degree up to eleven, Comm. Algebra 11 (1983) 863–911.

[Cam81] P. J. Cameron, Finite permutation groups and finite simple groups, Bull. London Math. Soc. 13 (1981) 1–22.

[CH08] J. J. Cannon, D. F. Holt, The transitive permutation groups of degree 32, Experiment. Math. 17 (2008) 307–314.

[CE56] H. Cartan, S. Eilenberg, Homological algebra, Princeton University Press, Princeton, N. J., 1956.

[CK00] A. Cortella, B. Kunyavskii, Rationality problem for generic tori in simple groups, J. Algebra 225 (2000) 771–793.

[CTS77] J.-L. Colliot-Thélène, J.-J. Sansuc, La R-équivalence sur les tores, Ann. Sci. École Norm. Sup. (4) 10 (1977) 175–229.

[CTS87] J.-L. Colliot-Thélène, J.-J. Sansuc, Principal homogeneous spaces under flasque tori: Applications, J. Algebra 106 (1987) 148–205.

[DM90] J. D. Dixon, B. Mortimer, Permutation groups, Graduate Texts in Mathematics, 163, Springer-Verlag, New York, 1996.

[DJ13] A. Džumčić, G. A. Jones, p-adic Hurwitz groups, J. Algebra 379 (2013) 179–207.

[End11] S. Endo, The rationality problem for norm one tori, Nagoya Math. J. 202 (2011) 83–106.

[EK17] S. Endo, M. Kang, Function fields of algebraic tori revisited, Asian J. Math. 21 (2017) 197–224.
