August 2017

Algebraic Tori: A Computational Approach

Armin Jamshidpey
The University of Western Ontario

Supervisor
Prof. Nicole Lemire and Prof. Eric Schost
The University of Western Ontario

Graduate Program in Mathematics

A thesis submitted in partial fulfillment of the requirements for the degree in Doctor of Philosophy

Abstract

The rationality problem for algebraic tori is well known. It is known that any algebraic torus is unirational over its field of definition. The first purpose of this work is to solve rationality problem for 5 dimensional stably rational algebraic tori with an indecomposable character lattice. In order to do so, we have studied the associated character lattices of the mentioned algebraic tori. For each character lattice L, either we see the lattice as an associated lattice to a root system (of which rationality of its corresponding algebraic torus is known) or we find a reduced component of L so that we can relate rationality of the associated algebraic torus to lower dimensions. Using these two main methods from [23], we solve rationality problem in some cases.

The second problem of which we are concerned with here, is to give a constructive proof for the No Name Lemma. Let G be a finite group, K be a field, L be a permutation G-lattice with the standard basis and $K[L]$ be the group algebra of L over K. The No Name Lemma asserts that the invariant field of the quotient field of $K[L]$, $K(L)^G$ is a purely transcendental extension of K^G. In other words, there exist $y_1, \ldots, y_n$ which are algebraically independent over K^G such that $K(L)^G \cong K^G(y_1, \ldots, y_n)$. For a Galois extension K/F with $G = \mathrm{Gal}(K/F)$ we have introduced $\mathcal{Y} = \{y_1, \ldots, y_n\} \subset K[L]^G$ with desired properties. Moreover, $\mathcal{Y}$ can be used to get a concrete description of $K[L]^G$. For a sign permutation G-lattice L, a more general argument is given so that we can concretely find a transcendence basis of $K(L)^G$ over K^G. Since the coordinate ring (resp. the rational function field) of an algebraic torus is given as invariant ring (resp. field), $K[L]^G$ (resp. $K(L)^G$) where L is the character lattice of the algebraic torus, the given proof can be used to construct the group ring or rational function field of a quasi split algebraic torus.

Keywords: Algebraic tori, multiplicative invariant, No Name Lemma.

Acknowledgment

I would like to express my sincere gratitude to my supervisors, Nicole Lemire and Eric Schost, for their continuous support. Their guidance helped me in all the time of research and writing of my dissertation.

Huge thanks go to Mark Giesbrecht and George Labahn, for accepting me in the Symbolic Computation Group in department of computer science at the University of Waterloo. My special thanks to Dan Christensen for his support during my studies at UWO.

Special thanks go to Lex Renner, who taught me the first notions of algebraic groups, for all his support during my studies and for his invaluable suggestions as a member of my examination board.

I kindly thank the examination board, Gregor Kemper, Marc Moreno Maza and Ajneet Dhillon for their careful reading and their invaluable suggestions.

I am thankful to my friends in the math department at UWO and to my fellow labmates in SCG at Waterloo. Many thanks to Dinesh Valluri and Jasmin Omanovic for many mathematical and non-mathematical conversations, Asghar Ghorbanpour, Javad Rastegari, Masoud Ataei, Javad Doliskani, Chandra Rajamani, Octavian Mitrea, Shahab Azarfar and Ahmed Ashraf. Thanks to my officemate Mohsen Mollahajiaghaei for all the conversations, friendship and companion during these years of hard work.

My heartfelt regard goes to my parents in law, sisters in law, Laya and Sara for their love and moral support.

My deepest gratitute goes to my lovely wife, Leili. I am truly appreciative of all she has done for me over the years. I could not have reached my goals without her help and support. She has been with me all these years and has made them the best years of my life.

At last but not least, to my parents, thanks for your unconditional love and support. During my life you were always there for me, day and night, and never gave up on me even for one moment. If it was not for my older brother Arash's suggestions I would have missed a lot of great opportunities during my life. So my warmest thanks go to Arash for all his guidance and support. I would also like to thank my younger brother Aryo for his love and support.

To my wife

Contents

List of Figures

List of Tables

List of Appendices

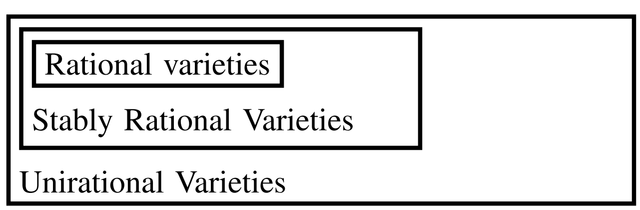
Chapter 1

Introduction

An interesting problem in algebraic geometry is the rationality problem, i.e. for a given algebraic variety, determine if it is rational or not. A more general problem is to classify algebraic varieties up to birational isomorphism classes.

In order to simplify the classification, we try to find coarser classes. Thus we define stable rationality and unirationality. Although these are geometric notions, in some cases there is a nice translation of these to algebraic language and this is the key to give a partial solution to the simplified problem.

But what do we mean by rationality? If X is an algebraic variety, we say X is rational if it is birationally isomorphic to $\mathbb{A}^n$ for some n. For a coarser class, we say that X is stably rational if $X \times \mathbb{A}^n$ is rational (for some n). We call X unirational if there exist a finite degree dominant rational map from $\mathbb{A}^n$ (for some n) to X.



To understand classes we need to find some birational invariants (properties which hold for all elements in a birational class) of algebraic varieties. A birational invariant of algebraic varieties is dimension. Another one is the function field of varieties which belong to the same class. Our approach here is to study the function fields.

In this dissertation we study two problems about algebraic tori. The first one is to examine rationality of 5 dimensional algebraic tori which are known to be stably rational. The other problem is finding an explicit algebraic description of quasi split algebraic tori. In what follows we briefly explain the mentioned problems and known results.

An algebraic F-torus T is an algebraic group defined over a field F, which is a torus over an algebraic closure $\bar{F}$. Since a torus is a finite product of $\mathbb{G}_m$ into itself, we say T splits over $\bar{F}$. In general $\bar{F}$ is not the smallest field such that T splits over it. It is known that an algebraic F-torus T splits over a finite Galois extension of F. If T splits over K/F and $G = \mathrm{Gal}(K/F)$, then G is called the splitting group of T.

The rationality problem for an algebraic torus is to determine whether a given algebraic torus is rational (stably rational or unirational). Algebraic tori are in some sense the simplest algebraic groups, so it is reasonable to solve the difficult problem of rationality in these cases. Our approach to solve the problem is to use the relation between algebraic tori and multiplicative invariants.

Assume L is a free $\mathbb{Z}$-module of finite rank (i.e. a lattice) and G is a finite group acting by automorphism on L. This type of action is called a multiplicative action. If R is a commutative unital ring, we can extend the action on L to an action on $R[L]$ (the group ring of L over R). Now L becomes a multiplicative group in $R[L]$. The multiplicative invariants are the invariant elements in $R[L]$ under the action of G.

Multiplicative invariants occur in different contexts such as centers and prime ideals of group algebras, representation rings of Lie algebras and rationality problems. Since we are interested in the rationality problem, we present Noether's problem here. Assume K/F is a rational field extension i.e. $K = F(x_1, \ldots, x_n)$ where x_i's are algebraically independent over F. Moreover, assume that a group G acts on K by automorphism and maps F to itself. Noether's rationality problem asks under what conditions the extension K^G/F^G is also rational. The origin of the problem goes back to some problems in constructive Galois theory (see [29] and [17]). The special case of multiplicative G-fields (here, $K(L)$ for some lattice L with a multiplicative action of G) for a finite group G has received particular attention. One of the main reasons of this attention is the connection of multiplicative invariants with algebraic tori.

There is a duality between the category of algebraic tori which split by G and G-lattices (a lattice equipped with a G action). For a given algebraic torus T with splitting group G, its character module $\mathrm{Hom}(T, \mathbb{G}_m)$ is a G-lattice. If L is a G-lattice, then $\mathrm{Spec}(K[L]^G)$ is an algebraic torus with splitting group G.

On the other hand having a G-lattice L means we have

$$G \longrightarrow \mathrm{GL}(L) \cong \mathrm{GL}(n, \mathbb{Z}),$$

where n is the rank of L. If G is a finite group acting on L then the image of G inside $\mathrm{GL}(n,\mathbb{Z})$ (under the representation map) is a finite subgroup of $\mathrm{GL}(n,\mathbb{Z})$. Also if G is a finite subgroup of $\mathrm{GL}(n,\mathbb{Z})$ then it acts naturally by multiplication on the standard basis of $\mathbb{Z}^n$ which gives a G-lattice. The dualities explained for a fixed Galois extension K/F with Galois group G, are summarized as

$$\{\text{isomorphism classes of } n \text{ dimensional algebraic tori}\}$$

$$\updownarrow$$

$$\{\text{isomorphism classes of } G\text{-lattices of rank } n\}$$

$$\updownarrow$$

$$\{\text{conjugacy classes of finite subgroups of } \mathrm{GL}(n,\mathbb{Z})\}.$$

By a celebrated theorem by Jordan [18], the number of finite subgroups of $\mathrm{GL}(n,\mathbb{Z})$ is finite (up to conjugacy) for any natural number n. This means that up to isomorphism, we have finitely many algebraic tori in each dimension. When we say a finite subgroup of $\mathrm{GL}(n,\mathbb{Z})$ or a G-lattice is rational, we mean their corresponding algebraic torus is rational. An algebraic torus T is called hereditarily rational if all subgroups of the group associated to T are rational.

In order to classify birational classes of algebraic tori, one should first find non-conjugate finite subgroups G in $\mathrm{GL}(n,\mathbb{Z})$. The information about finite subgroups of $\mathrm{GL}(n,\mathbb{Z})$ for n up to 4 is contained in the GAP package CrystCat. The GAP package Carat contains all finite subgroups of $\mathrm{GL}(n,\mathbb{Z})$, for n up to 6.

As we mentioned before, one of the problems we are concerned with here, is the rationality problem for 5 dimensional algebraic tori. In order to present the main results in rationality problem for algebraic tori we need to present some information first.

The GAP ID of finite subgroups of $\mathrm{GL}(n,\mathbb{Z})$ for $n \leq 4$ is used frequently in classification of 4 and 5 dimensional algebraic tori. A group with GAP ID (n,m,i,j) is the finite subgroup of $\mathrm{GL}(n,\mathbb{Z})$ of the jth $\mathbb{Z}$-class of the ith $\mathbb{Q}$-class of the mth crystal system. In [15] the authors introduced Carat ID. A group with Carat ID (n,i,j) is the finite subgroup of $\mathrm{GL}(n,\mathbb{Z})$ of the ith $\mathbb{Z}$-class of the jth $\mathbb{Q}$-class.

It is known that any algebraic tori is unirational over its field of definition. The rationality problem for one dimensional tori is straight forward. Voskresenskii showed that all two dimensional algebraic tori are rational (see [44]). He used a geometric argument to show this result.

In [21], Kunyavski solved the rationality problem for algebraic tori of dimension 3. He proved that except for 15 algebraic tori, the rest of them are rational. Moreover he proved that the exceptional algebraic tori are not stably rational (see Table 1.1).

GAP ID	Structure	#G	GAP ID	Structure	#G	GAP ID	Structure	#G
(3,3,1,3)	C_2^2	4	(3,4,7,2)	$D_8 \times C_2$	16	(3,7,5,3)	$S_4 \times C_2$	48
(3,3,3,3)	C_2^3	8	(3,7,2,2)	$A_4 \times C_2$	24	(3,7,5,2)	$S_4 \times C_2$	48
(3,4,4,2)	D_8	8	(3,7,3,3)	S_4	24	(3,4,3,2)	$C_4 \times C_2$	48
(3,4,6,3)	D_8	8	(3,7,3,2)	S_4	24	(3,3,3,4)	C_2^3	8
(3,7,1,2)	A_4	12	(3,7,4,2)	S_4	24	(3,7,2,3)	$A_4 \times C_2$	24

Table 1.1: Non-rational groups of rank 3.

Hoshi and Yamasaki classified algebraic tori of dimension 4 and 5 up to stable rationality [15]. Their proof is based on computations using GAP. In dimension 4, there are 487 (up to isomorphism) algebraic tori which are stably rational. In [23], Lemire proved that in dimension 4, all stably rational algebraic tori are rational, except for possibly ten of them. In dimension five, there are 311 stably rational algebraic tori, found by Hoshi and Yamasaki, with indecomposable character lattices. In [15] stable rationality of the 311 was proven by considering maximal groups among them.

We have studied the rationality of the mentioned groups in Chapter 3. Our approach to solve the rationality problem is similar to the approach used in [23]. We apply two main methods on lattices associated to the mentioned 311 groups. The first method is to see them as an isomorphic copy of a lattice which corresponds to a known rational torus. The second method is to find a short exact sequence of lattices with a specific condition on the cokernel. For a G-lattice L, we are interested in finding a short exact sequence of lattices

$$0 \longrightarrow M \longrightarrow L \longrightarrow P \longrightarrow 0$$

where P is a G-lattice (preferably of rank 1) such that there exist a $\mathbb{Z}$-basis of P which is permuted by G. It is known that the existence of such sequence shows that $K(L)^G$ is rational over $K(M)^G$ and rationality of $K(M)^G$ over F implies rationality of $K(M)^G$ over F as desired.

There are cases of which none of the above ideas work. In some of those cases, we have considered subgroups for which the above methods work. We have provided some information in the cases for which the rationality is unknown yet (see Section 3.3.17).

The rationality results of Chapter 3 are summarized in Table 1.2. The groups presented in Table 1.2 are hereditarily rational.

CARAT ID	Group Structure	#G	Description.
[5, 942, 1]	Imf(5, 1, 1)	3840	The root lattice of B_5
[5, 953, 4]	S_6	720	The root lattice of A_5
[5, 726, 4]	$C_2^4 \rtimes S_4$	384	reduced component [4, 32, 21, 1]
[5, 911, 4]	S_5	120	reduced component [4, 31, 4 , 1]
[5, 341, 6]	$D_8 \times S_3$	48	reduced component [4, 20, 17, 2]
[5, 531, 13]	$C_2 \times S_4$	48	reduced component [4, 25, 9 , 2]
[5, 245, 12]	$C_2^2 \times S_3$	24	reduced component [4, 14, 10, 2]
[5, 81, 54]	$C_2 \times D_8$	16	reduced component [4, 13, 7 , 5]
[5, 389, 4]	D_{12}	12	reduced component [4, 21, 3 , 2]
[5, 901, 3]	D_{10}	10	reduced component [4, 27, 3 , 1]
[5, 22, 14]	$C_2 \times C_2 \times C_2$	8	reduced component [4, 6 , 1 , 9]
[5, 98, 28]	D_8	8	reduced component [4, 13, 3 , 3]
[5, 99, 57]	D_8	8	reduced component [4, 12, 4 , 7]
[5, 174, 2]	S_3	6	reduced component [4, 17, 1 , 3]
[5, 174, 5]	S_3	6	reduced component [4, 17, 1 , 2]
[5, 18, 28]	$C_2 \times C_2$	4	reduced component [4, 4 , 3 , 4]
[5, 19, 14]	$C_2 \times C_2$	4	reduced component [4, 5 , 1 , 10]
[5, 57, 8]	C_4	4	reduced component [4, 7 , 1 , 2]
[5, 164, 2]	C_3	3	reduced component [4, 11, 1 , 1]
[5, 6, 3]	C_2	2	reduced component [4, 2 , 2 , 2]

Table 1.2: Hereditarily rational groups among 311 indecomposable stably rational groups found by Hoshi and Yamasaki.

A G-lattice L, is called permutation (resp. sign permutation) if it has a $\mathbb{Z}$-basis which is permuted (resp. up to sign changes) by G. In chapter 4 we will see that a G-lattice of rank n is a permutation lattice if and only if G is conjugate to a subgroup of $\mathbb{S}_n$ where

$$\mathbb{S}_n = \langle \sigma = \left[\begin{array}{c|c} 0 & 1 \\ \hline I_{n-1} & 0 \end{array}\right], \tau = \left[\begin{array}{cc|c} 0 & 1 & \\ 1 & 0 & 0 \\ \hline \multicolumn{2}{c|}{0} & I_{n-2} \end{array}\right] \rangle.$$

Among algebraic tori there are families with permutation or sign permutation character lattices. An algebraic torus with a permutation character lattice is called quasi split. These two families are known to be rational. Although computationally we do not have an efficient algorithm to decide whether a given lattice is permutation, the structure of a quasi split torus is well understood.

The No Name Lemma asserts that if L is a permutation G-lattice and K is a G-field , then $K(L)^G$ is rational over K^G. This shows that a quasi split torus is rational. Providing a concrete proof for the No Name Lemma is another problem which is solved in this dissertation. The proof is based on a generalization of the Moore determinant [13, Section 1.3].

For $G \leq \mathrm{GL}(n,\mathbb{Z})$, let L_G be the G-lattice of rank n, generated by the standard basis $\{e_i\}_{i=1}^n$, where $(e_i)_j = \delta_{ij}$. For a field K, the group algebra $K[L]$ is isomorphic to the ring of Laurent polynomials over K, i.e. $K[x_1^{\pm 1},\ldots,x_n^{\pm 1}]$ and G acts both on K and L. For $g \in G$, $ge_i = \sum_{j=1}^n c_{ij}e_j$ for some $c_{ij} \in \mathbb{Z}$. The action of g on x_i is given by $gx_i = \prod_{j=1}^n x_j^{c_{ij}}$.

Assume G is the Galois group of K/F and T_G is the algebraic torus associated to L_G. The coordinate ring of T_G is $K[L_G]^G \cong K[x_1^{\pm 1},\ldots,x_n^{\pm 1}]^G$. The invariant field of the quotient field of $K[L_G]$, $K(L_G)^G \cong K(x_1,\ldots,x_n)^G$ is the rational function field of T_G. It is known that T_G is rational if and only if $K(L_G)^G$ is rational over F_G.

Theorem 1. *Let $G \leq \mathbb{S}_n \leq \mathrm{GL}(n,\mathbb{Z})$ and L_G be the lattice corresponding to G as defined above, which is a permutation lattice with the standard basis. Let K/F be a finite Galois extension with Galois group G. Let $\alpha \in K$ be a normal element for the Galois extension K/F.*

$$K[L]^G \cong K[x_1^{\pm 1}, x_2^{\pm 1},\ldots,x_n^{\pm 1}]^G = F[y_1,\ldots,y_n]_{x_1\cdots x_n}$$

where y_i is given by

$$S = \sum_{\sigma\in G}\sigma \in \mathbb{Z}[G]$$
$$y_i = S(\alpha x_i) \quad \textit{for} \;\; 1 \leq i \leq n.$$

Theorem 2. *Let $G \leq \mathrm{GL}(n,\mathbb{Z})$ and L_G be the lattice corresponding to G as defined above. Assume L_G is a sign permutation lattice with the standard basis. Let K/F be a finite Galois extension with Galois group G. Let $\alpha \in K$ be a normal element for the Galois extension K/F. Then $K(x_1,\ldots,x_n)^G$ is rational over F with transcendence basis $y_1,\ldots,y_n$ where $y_i = S(\alpha(1+x_i)^{-1})$ and $S = \sum_{g\in G} g \in \mathbb{Z}[G]$.*

The constructiveness of the proof can be turned into an algorithm to find the rational function field and the coordinate ring of a quasi split algebraic tori.

Chapter 2

Preliminaries

This chapter is devoted to covering the necessary background for studying the rationality problem for algebraic tori and the other results proven in chapter 4.

Definition 1. [37, Examples 3, 4] Any ring R determines the ringed space (Spec(R), $\mathscr{O}$) where $\mathscr{O}$ is the structure sheaf. We call (Spec(R), $\mathscr{O}$) an affine scheme.

Definition 2. [39, Tag 01IJ] A *scheme* is a locally ringed space with the property that every point has an open neighbourhood which is an affine scheme. A *morphism of schemes* is a morphism of locally ringed spaces.

Definition 3. [39, Tag 01RS] Let X, Y be schemes.

1. Let $f : U \to Y$, $g : V \to Y$ be morphisms of schemes defined on dense open subsets U, V of X. We say that f is *equivalent* to g if $f|_W = g|_W$ for some $W \subset U \cap V$ dense open in X.

2. A *rational map from X to Y* is an equivalence class for the equivalence relation defined in (1).

Definition 4. [39, Tag 020C] Let k be a field. A *variety* is a scheme X over k such that X is integral and the structure morphism $X \to \text{Spec}(k)$ is separated and of finite type.

For simplicity we define rationality notions for varieties.

Definition 5. A rational mapping $\varphi : X \to Y$ such that it has a rational inverse, is called a birational isomorphism.

Now we can define a rational variety.

Definition 6. Let k be a field and X be a k-variety. We say X is k-rational (or simply rational) if there exists a birational isomorphism $X \xrightarrow{\sim} \mathbb{A}^n$.

In general for a given variety it is not easy to say if it is rational or not, so as usual we try some relaxed notions of rationality to give an approximation of rationality.

Definition 7. With the assumptions of the previous definition we say X is stably k-rational if there exists a birational isomorphism

$$\varphi : X \times \mathbb{A}^n \xrightarrow{\sim} \mathbb{A}^m$$

where $n \leqslant m$.

Definition 8. A morphism $\varphi : X \to Y$ between two varieties is said to be dominant if $\varphi(X)$ is dense in Y.

Definition 9. Again with above assumptions X is k-unirational if there exist a dominant rational map

$$\varphi : \mathbb{A}^n \to X.$$

We can see

$$\textit{rationality} \Rightarrow \textit{stably rationality} \Rightarrow \textit{unirationality}. \tag{2.1}$$

Now we want to translate these notions to algebraic equivalents so we can deal with them more easily. In order to do so, we define rationality (stable rationality, unirationality) of a field extension. After doing that we say a variety is rational (resp. stably rational or unirational) if the function field of the variety is rational (resp. stably rational or unirational) over the base field. In the below definitions assume K/k is a finitely generated field extension.

Definition 10. K is said to be rational over k, if $K \cong k(x_1, \ldots, x_n)$ for some algebraically independent $x_1, \ldots, x_n$ over k.

Definition 11. K is called stably rational over k, if $K(y_1, \ldots, y_m)$ is rational over k for some algebraically independent elements $y_1, \ldots, y_m$ over K.

Here we define another rationality type for which we did not give a geometric equivalent since Saltman first defined it algebraically.

Definition 12. K is called retract rational if it contains a k-algebra R satisfying the following:
i) K be the quotient field of R.
ii) the identity map $id : R \to R$ factors through a localized polynomial ring over k.

Definition 13. K is called unirational over k if

$$k \subseteq K \subseteq k(x_1, \ldots, x_n)$$

for some algebraically independent elements $x_1, \ldots, x_n$ over k.

Another useful notion is stable isomorphism. Let G be a group and F and F' be two G-fields (i.e. fields equipped with a G action). We say F and F' are stably isomorphic as G-fields if

$$F(x_1, \ldots, x_r) \cong F'(y_1, \ldots, y_s)$$

We note that letting $G = \{1\}$ we can get the stable isomorphism for fields. Having next proposition in hand, it is easy to see that

$$\text{rationality} \Rightarrow \text{stable rationality} \Rightarrow \text{retract rationality} \Rightarrow \text{unirationality}.$$

Proposition 14. *[25, Theorem 9.3.3] Let F/K and E/K be field extensions.*
(a) If F and E be stably isomorphic over K and F/K be retract rational, then E/K is retract rational.
(b) If F/K is stably rational then it is also retract rational.

Later on when we provide some more machinery, we can see these inclusions easier for algebraic tori.

None of the above implications are reversible in general. In other words we have varieties (one can see same statement for their function fields) which are unirational but not retract rational, there are retract rational examples which are not stably rational and there are stably rational varieties which are not rational.

2.1 G-Lattices

It is known that there is a duality between algebraic tori and G-lattices. In order to be able to discuss the duality, we briefly introduce G-lattices in this section. For a more detailed discussion see [25, Chapters 1 and 2].

A lattice is a free $\mathbb{Z}$-module of finite rank. As a $\mathbb{Z}$-module, it is isomorphic to $\mathbb{Z}^n$ for some n. If we have a group G, we can endow the lattice with an action of G. If G acts on a lattice L by automorphisms i.e. there exists

$$G \longrightarrow GL(M) \cong \mathrm{GL}(n, \mathbb{Z}),$$

we say L is a G-lattice. We can equivalently say that G-lattices are free $\mathbb{Z}$-modules of finite rank which is also $\mathbb{Z}[G]$-modules, for $\mathbb{Z}[G]$ the integral group ring over G. A G-equivariant, $\mathbb{Z}$-linear map between G-lattices is called a homomorphism of G-lattices.

For a given G-lattice L we define

$$L^G = \{l \in L : g.l = l, \quad \forall g \in G\}.$$

Example 15. Let $G = D_8 = \langle r, s : r^4 = s^2 = 1, rs = sr^{-1} \rangle$ be the dihedral group of order 8 and $L = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2$ be a lattice. The following can be checked to be an injective group homomorphism.

$$\rho : G \longrightarrow \mathrm{GL}_2(\mathbb{Z})$$

$$r \longrightarrow \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

$$s \longrightarrow \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

This gives a G-lattice, L. Since $g.x = \rho(g)(x)$ the action on the basis $\{e_1, e_2\}$ is given by

$$r \cdot e_1 = e_2$$

$$r \cdot e_2 = -e_1$$

$$s \cdot e_1 = -e_1$$

$$s \cdot e_2 = e_2$$

We can see that $L^G = 0$. G-lattices L with $L^G = 0$ are called effective.

Now let R be an arbitrary commutative (unital) ring. For any G-lattice L we can form the group algebra $R[L]$ and the action of G on L can be extended to an action on $R[L]$. The subalgebra of all G-invariant elements in $R[L]$

$$R[L]^G = \{l \in R[L] : g.l = l, \ \ \forall g \in G\}$$

is called the multiplicative invariant algebra. Studying this algebra is the subject of multiplicative invariant theory.

The group algebra $R[L]$ of a G-lattice, is isomorphic to the Laurent polynomial algebra $R[x_1^{\pm 1}, x_2^{\pm 1}, \ldots, x_n^{\pm 1}]$ and the lattice itself becomes a multiplicative subgroup of all monomials.

Going back to the previous example we can write $R[L] \cong R[x_1^{\pm 1}, x_2^{\pm 1}]$ and the multiplicative action is given by

$$r \cdot x_1 = x_2, \quad r \cdot x_2 = x_1^{-1}, \quad s \cdot x_1 = x_1^{-1}, \quad s \cdot x_2 = x_2$$

If L and L' are two G-lattices then $\mathrm{Hom}_{\mathbb{Z}}(L, L')$, the set of all $\mathbb{Z}$-linear maps from L to L', is a G-lattice with the following action

$$(g.f)(m) = g.(f(g^{-1}.m)).$$

For $L' = \mathbb{Z}$ (with trivial action of G), we get the G-lattice $L^* = \mathrm{Hom}_{\mathbb{Z}}(L, \mathbb{Z})$ which is called the dual lattice of L.

Suppose L is a G-lattice and H is a subgroup of G. L can be considered as an H-lattice. The new H-lattice is called restricted and is denoted by $L \downarrow_H^G$.

Assume H is a finite index subgroup of G and L is an H-lattice. The G module $\mathbb{Z}[H] \otimes_{\mathbb{Z}[G]} L$ is a G-lattice which is called the induced G-lattice and is denoted by $L \uparrow_H^G$.

Definition 16. A G-lattice L is called a permutation lattice if there exists a $\mathbb{Z}$ -basis X for L such that, G acts as permutation group on X. We denote L by $\mathbb{Z}[X]$.

Example 17. Let H be a finite index subgroup of a group G and $G/H = \{g_1H, g_2H, \ldots, g_nH\}$ be a complete representative set of left cosets of H in G. Then $\mathbb{Z}[G/H]$ is a G-lattice with the action $g.g_iH = (gg_i)H$. It is easy to see that G acts as a permutation group on the basis so it is a permutation lattice.

It is known that the permutation G-lattice $\mathbb{Z}[G/H]$ is isomorphic to $\mathbb{Z}\uparrow_H^G$.

Lemma 18. *[5, Proposition 10.28] If L is a H-lattice and H is a subgroup of G of finite index, then*

$$L^* \uparrow_H^G \cong (L \uparrow_H^G)^*.$$

Lemma 19. *[25, Section 2.2] A G-lattice L is a permutation lattice if and only if $L \cong \bigoplus_H \mathbb{Z}[G/H]$ where H is a finite index subgroup of G.*

Since the trivial H-lattice $\mathbb{Z}$ is self dual, as a corollary of the above lemmas we can conclude that, any permutation lattice is self dual.

It is important to notice that direct sum (and tensor product) of permutation lattices is still permutation.

Definition 20. We call a G-lattice L, decomposable if there are nontrivial G-lattices L_1 and L_2 such that $L \cong L_1 \oplus L_2$. L is called indecomposable if it is not decomposable.

If L is decomposable then it is reducible, but the converse is not true for lattices.

Definition 21. A G-lattice L is called reducible if L has a nontrivial G-invariant subspace M such that L/M is torsion free. L is called irreducible if it is not reducible.

Now let L and L' are two G-lattices. L and L' are stably permutation equivalent if and only if there exist permutation lattices P and P' such that

$$L \oplus P \cong L' \oplus P'.$$

In fact the above notion defines an equivalence relation on G-lattices. We denote the equivalence class of L by $[L]$.

Definition 22. A G-lattice L is called stably permutation if $[L] = [0]$ i.e. there exist permutation lattices P and P' such that

$$L \oplus P \cong P'$$

We can also define addition on the set of all equivalence classes of stably permutation equivalence relation. For G-lattices L and L', define

$$[L] + [L'] = [L \oplus L']$$

Note that it is well defined.

Having this addition on the set of equivalence classes turns the set to an additive monoid which we denote it by SP_G. This is obviously a commutative monoid with $[0]$ as the identity.

Definition 23. A G-lattice is called permutation projective or invertible if its corresponding class in SP_G is invertible. i.e. there exists an L' such that $[L] + [L'] = [0]$.

The above definition says, there are P and P' permutation lattices such that $L \oplus L' \oplus P \cong P'$. So L is invertible if and only if L is a direct summand of a permutation lattice.

Let G be a finite group. Let us denote the Tate cohomology functor by $\hat{H}^i(G, .)$ (for $i \in \mathbb{Z}$) (See [4, Chapter 6]). Here we are just interested in $\hat{H}^{\pm 1}(G, .)$.

Definition 24. A G-lattice L is $\hat{H}^i$- trivial if $\hat{H}^i(H, L) = 0$ for all $H \leqslant G$.

Definition 25. We call a G-lattice L, flasque (coflasque) if it is $\hat{H}^{-1}$- trivial ($\hat{H}^1$- trivial).

Lemma 26. *[25, Page 36] Let L be a G-lattice then*

$$\hat{H}^i(G, L) \cong \hat{H}^{-i}(G, L^*).$$

Definition 27. An exact sequence of G-lattices

$$0 \longrightarrow L \longrightarrow P \longrightarrow F \longrightarrow 0$$

is called a flasque resolution of L, if P is a permutation lattice and F is flasque. Similarly, we can define a coflasque resolution of L as

$$0 \longrightarrow C \longrightarrow P \longrightarrow L \longrightarrow 0$$

where C is coflasque.

Theorem 28. *[25, Lemma 2.6.1] For any given G-lattice L, there exists a coflasque (flasque) resolution. Furthermore, if*

$$0 \longrightarrow C \longrightarrow P \longrightarrow L \longrightarrow 0$$

and

$$0 \longrightarrow C' \longrightarrow P' \longrightarrow L \longrightarrow 0$$

are two coflasque resolutions of L, then $[C] = [C']$ *(statement is true for flasque resolutions).*

Lemma 29. *[25, Lemma 2.5.1] Permutation projective G-lattices are both flasque and coflasque.*

We can see that in particular permutation lattices are flasque and coflasque. As an example one can consider the augmentation map

$$\varepsilon_{G/H} : \mathbb{Z}[G/H] \to \mathbb{Z}$$

$$gH \to 1$$

Let $I_{G/H} = Ker\varepsilon_{G/H}$. We can obtain the below exact sequence

$$0 \to I_{G/H} \xrightarrow{i} \mathbb{Z}[G/H] \xrightarrow{\varepsilon_{G/H}} \mathbb{Z} \to 0.$$

Considering the dual sequence where $J_{G/H} = I^*_{G/H}$ we get

$$0 \to \mathbb{Z} \to \mathbb{Z}[G/H] \to J_{G/H} \to 0.$$

Note that $\mathbb{Z}$ and $\mathbb{Z}[G/H]$ are both flasque and coflasque.

In general there is a construction for finding a coflasque resolution of a given lattice L. Let

$$P = \bigoplus_H L^H \uparrow_H^G .$$

where H ranges through all subgroups of G. It can be shown that P is a permutation G-lattice . On the other hand we can extend the inclusion

$$L^H \to L$$

to a G-equivariant epimorphism

$$\phi : P \twoheadrightarrow L$$

with $\phi(P^H) = L^H$ for all $H \leq G$. Now letting $C = \ker\phi$ we obtain an exact sequence

$$0 \to C \to P \to L \to 0.$$

Still we need to check if C is a coflasque G-lattice. By applying the cohomology functor to the above sequence we get

$$\cdots \to P^H \to L^H \to H^1(H, C) \to H^1(H, P) \to \cdots$$

But we know that $H^1(H, P) = 0$. Since ϕ is a surjection from P^H to L^H, we conclude that $H^1(H, C) = 0$.

Definition 30. Let L be a G-lattice. The flasque class of L, which is denoted by $[L]^{fl}$ is $[F] \in \mathrm{SP}_G$ where F is the cokernel in any flasque resolution of L.

We write

$$L \sim_{fl} L' \iff [L]^{fl} = [L']^{fl}$$

Note that $[0]^{fl} = [0]$ and $[L \oplus L']^{fl} = [L]^{fl} + [L']^{fl}$, since the direct sum of two flasque resolutions for L and L' is a flasque resoulution for $L \oplus L'$.

Definition 31. A G-lattice L which $L \sim_{fl} 0$ is called quasi-projective i.e. L is quasi projective if and only if there exists a flasque resolution for L

$$0 \longrightarrow L \longrightarrow P \longrightarrow Q \longrightarrow 0$$

where Q is a permutation G-lattice.

In order to summarize important facts about lattices we can mention the below diagram

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

2.2 Root Systems and Their Associated Lattices

In this brief section we define root systems and present the root lattice of A_n. For a more detailed discussion we invite the reader to see [2], [16, Chapter 3].

Assume V is a vector space over $\mathbb{R}$ and V^* be its dual. Suppose $\langle ., . \rangle : V^* \times V \to \mathbb{R}$ denote the usual evaluation pairing.

Definition 32. A subset $\Phi \subset V$ is called a reduced root system in V if it satisfies the following properties,

i. Φ is finite, $0 \notin \Phi$ and $V = \langle \Phi \rangle_{\mathbb{R}}$.

ii. $\forall v \in \Phi$ there exists $\hat{v} \in V^*$ such that $\langle \hat{v}, v \rangle = 2$ and the reflection $s_v(u) = u - \langle \hat{v}, u \rangle v$ maps Φ to itself.

iii. $\forall v \in \Phi$, $\langle \hat{v}, \Phi \rangle \subset \mathbb{Z}$.

iv. $v \in \Phi \Rightarrow 2v \notin \Phi$

A root system Φ in V is called irreducible, if it is not possible to write $V = V_1 \oplus V_2$ ($V_i \neq 0$) and $\Phi = \Phi_1 \cup \Phi_2$ and root systems Φ_i in V_i. The irreducible reduced root systems are well understood and classified. We only need the root systems of types A_n ($n \geq 1$) and B_n ($n \geq 2$).

Definition 33. The automorphism group of a reduced root system Φ in V is denoted by $\mathrm{Aut}(\Phi)$ and is defined as

$$\mathrm{Aut}(\Phi) = \{g \in \mathrm{GL}(V) : g(\Phi) \subset \Phi\}.$$

Moreover, the Weyl group of Φ is denoted by $W(\Phi)$ and is generated by s_v defined in Definition 32[ii] i.e.

$$W(\Phi) = \langle s_v : v \in \Phi \rangle.$$

Note that $W(\Phi) \subset \mathrm{Aut}(\Phi)$ and $\mathrm{Aut}(\Phi)$ is a finite group.

Definition 34. A subset Δ of a root system $\Phi \subset V$ is called a base for Φ if

- Δ is a basis of V
- $u \in \Phi \Rightarrow u = \sum_{\delta\in\Delta} c_\delta \delta$ or $u = -\sum_{\delta\in\Delta} c_\delta \delta$ where c_δ are non negative integers.

Definition 35. The root lattice $L(\Phi)$ of a root system Φ is defined by

$$L(\Phi) = \mathbb{Z}\Phi = \{\sum_{v\in\Phi} c_v v : c_v \in \mathbb{Z}\}.$$

We are just interested in types A_n, and B_n. Let V denote the nullspace of the linear map $\mathbb{R}^{n+1} \to \mathbb{R}$ sending the standard basis $\{e_i\}_{i=1}^{n+1}$ of $\mathbb{R}^{n+1}$ to one. One can verify that

$$\Phi = \{e_i - e_j : i \neq j, 1 \leq i, j \leq n+1\}$$

is a root system in V, and it is called the root system of type A_n. The set $\{e_i - e_{i+1}\}_{i=1}^{n}$ is a base of Φ.

The Weyl group of Φ, $W(A_n)$, is S_{n+1} and it acts on Φ by its standard action on e_i's, i.e

$$\forall g \in S_{n+1}, \quad g(e_i) = e_{g(i)}.$$

Moreover, the automorphism group of Φ is $\mathrm{Aut}(\Phi) = C_2 \times S_{n+1}$ where $C_2 =< \sigma >$ is the cyclic group of order two. σ acts on Φ by multiplication with -1.

The root lattice $\mathbb{Z}A_n$ is given by

$$\{\sum_{i=1}^{n} c_i e_i : c_i \in \mathbb{Z}, \ \sum_i c_i = 0\} = \langle e_1 - e_2, \ldots, e_n - e_{n+1}\rangle_{\mathbb{Z}}.$$

The root lattice of A_n can be given as the kernel of the augmentation map. Identify S_n as $\mathrm{Stab}_{\mathrm{S}_{n+1}}(n+1)$ of S_{n+1}. It is clear that $\mathbb{Z}[\mathrm{S}_{n+1}/\mathrm{S}_n]$ is isomorphic to the permutation S_{n+1}-lattice $\oplus_i \mathbb{Z}e_i$ with $g \in \mathrm{S}_{n+1}$ acting by $g(e_i) = e_{g(i)}$. The kernel of the augmentation map $\varepsilon : \oplus_i \mathbb{Z}e_i \to \mathbb{Z}$, $\varepsilon(e_i) \to 1$, is $\mathbb{Z}A_n$.

For the root system of type B_n let $V = \mathbb{R}^n$ $(n \geq 2)$. One can verify that $\Phi = \{\alpha : (\alpha, \alpha) = 1 \text{ or } 2\}$ is a root system in V and it is called the root system of type B_n. The set $\{e_i - e_{i+1}\}_{i=1}^{n-1} \cup \{e_n\}$ is a basis of Φ. The Weyl group of Φ, $W(B_n)$ is $C_2^n \rtimes \mathrm{S}_n$ (the wreath product) where C_2 is the cyclic group of order two and S_n is the symmetric group of order n. For more detail see [16, Chapter 3].

Proposition 36. *[25, Proposition 1.1] Let Φ be an irreducible reduced root system not of type C_4 and $L = L(\Phi)$ be its root lattice. the action of* $\mathrm{Aut}(\Phi)$ *on L realizes* $\mathrm{Aut}(\Phi)$ *as a maximal finite subgroup of* $\mathrm{GL}(L)$.

2.3 Algebraic Groups

In this small section the aim is to introduce the main definitions of algebraic groups and algebraic tori. For a more detailed discussion see [16, Chapter 2], [1, Chapter 1] and [44, Chapter 1].

Theorem 37. *[45, Page 5] Let F be a functor from k-algebras to sets. If the elements in $F(R)$ correspond to solutions in R of some family of equations, there is a k-algebra A and a natural correspondence between $F(R)$ and $\mathrm{Hom}_k(A, R)$. The converse also holds.*

Such an F is called representable and we say A represents F. An affine group scheme is a representable functor from category of k-algebras to category of groups (see [45, Chapter 1] or [44, Chapter 1]). An affine group scheme, G is called algebraic, if its representing algebra is finitely generated.

Example 38. GL_n is the affine algebraic group scheme represented by $\mathrm{Spec}(\mathbb{Z}[x_{11}, \ldots, x_{nn}, D^{-1}])$ where $D = \det(x_{ij})$. $\mathrm{GL}_n(K)$ is the set of all invertible matrices in $M_{nn}(K)$.

Example 39. Since we can embed S_n(symmetric group of order n) into GL_n, it is an algebraic group. More precisely for $\sigma \in \mathrm{S}_n$ we can send it to the action of σ on I_n. Furthermore applying Cayley's theorem, we see that any finite group is an algebraic group.

Example 40. We denote GL_1 by $\mathbb{G}_m$ (where m refers to multiplicative). $\mathbb{G}_m$ is represented by $\mathrm{Spec}(\mathbb{Z}[x, x^{-1}])$. $\mathbb{G}_a$ is the algebraic group represented by $\mathbb{Z}[x]$. Another way to look at $\mathbb{G}_a$ is given by below embedding:

$$x \longrightarrow \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2$$

From now on when we say algebraic group we mean an affine algebraic group. We call a map $f : G \longrightarrow G'$ a morphism of algebraic groups if it is a morphism of varieties and homomorphism of groups. A character of an algebraic group is $\chi : G \longrightarrow \mathbb{G}_m$ which is a morphism of algebraic groups. It is well known that the set of characters of an algebraic group form an abelian group and it is denoted by $\chi(G)$.

In the simplest terms, an algebraic torus over a field k, is an algebraic group which over $\bar{k}$ it looks like a torus i.e. it will be the product of some copies of $\mathbb{G}_m$. In order to define an algebraic torus more formally we need the following definition.

Definition 41. Let F/K be a field extension and X be a K-scheme. We say a K-scheme Y is an F/K-form of X if the following holds(as F-schemes)

$$X \otimes F \cong Y \otimes F$$

if $F = \bar{K}$ we say Y is a K-form.

Now an algebraic torus is a an algebraic group, which is a K-form of $\mathbb{G}_m^d$ for some d.

The Weil restriction is a functor such that for any field extension K/F and any affine group scheme, G over K, produces an F-group scheme $R_{K/F}(G)$. If A is a K-algebra, then $R_{K/F}(G)(A) = G(A \otimes_F K)$ (see [44, Section 1.3.12]).

The simplest example of an algebraic torus is $\mathbb{G}_m$. Another well understood example is $R_{K/F}(\mathbb{G}_m)$ where $R_{K/F}$ is the Weil restriction for a Galois extension K/F.

Definition 42. [44, Example 19] An algebraic torus representable as a direct product of groups of the form $R_{K/F}(\mathbb{G}_m)$ is called a quasi split torus.

We say that an algebraic group G, is diagonalizable if the coordinate ring of G, can be spanned by its character group. This is equivalent to say G is isomorphic to a subgroup of D_n (consisting of diagonal matrices) for some $n > 0$.

Later on when we want to see the duality between algebraic tori and G-lattices we will use it.

Theorem 43. *[1, Page 114] The following are equivalent:*
a) T is an n dimensional torus.
b) T is a connected diagonalizable group of dimension n.
c) T is a diagonalizable group and $\chi(T) = \mathbb{Z}^n$.

Remark. A quasi split torus is characterized by the condition that its character lattice is a permutation lattice.

2.4 Duality Between Algebraic Tori and G-lattices

As mentioned before there is a duality between category of algebraic tori split by a G-Galois extension and category of G-lattices. In this section we want to briefly take a look at the duality. For more discussion see [44, Section 3.4].

Let Y be a k-form of a k-scheme X. A field $k \subseteq F$ is called a splitting field of Y if

$$X \otimes_k F \cong Y \otimes_k F.$$

It turns out that there exists a separable extension of k, which is a splitting field of Y. Let k_s be the separable closure of k and G be the absolute Galois group of k_s/k.

Let T be an algebraic k-torus which splits over k_s and G as above. Also let $\hat{T}$ be the character group of T. One can see that there is an action of G by means of automorphisms on $\hat{T}$. Let the action be given by the representation

$$h : G \to \mathrm{Aut}(\hat{T}).$$

Note that h is continuous, $\mathrm{Aut}(\hat{T})$ has the discrete topology and G is compact (in the profinite topology). Hence the image of G is compact in $\mathrm{Aut}(\hat{T})$. This obviously implies that $h(G)$ is a finite subgroup of $\mathrm{Aut}(\hat{T})$. This is telling us the kernel of h, which is acting trivially, is of finite index in G. Let $H = \ker h$ and assume F is the fixed field of k_s under the action of H. Hence $H = \mathrm{Gal}(k_s/F)$. Note that the quotient $G/H \cong \mathrm{Gal}(F/k)$ and F/k is a finite Galois extension.

Since everything can be reduced to the finite case, let us take a closer look at it. Let T be an algebraic torus over K and let L be a finite Galois extension of K such that T splits over L. Assume that the Galois group of L/K is $G = \mathrm{Gal}(L/K)$. In the light of Theorem 43 we know that the character group of T is a lattice and we can endow it with the action of Galois group. In other words for any algebraic torus of dimension n, we have $\mathrm{Hom}(T, \mathbb{G}_m)$ as a G-lattice.

On the other hand for a given G-lattice M, $\mathrm{Spec}(L[M]^G)$ is an algebraic torus. In this case $L[M]^G$ is the coordinate ring of the torus.

Lemma 44. *Suppose V is a vector space over a field F and $W \neq 0$ is a non-empty subset of V. If any F-linear function $\phi : V \to F$ annihilating W, is zero, then W contains an F-basis of V.*

Proof. Assume any linear map from V to F which annihilates W, is zero. If W does not contain a basis of V then $V \setminus \mathrm{span}_F(W)$ is nonempty. Let $t \neq 0$ be an arbitrary element of $V \setminus \mathrm{span}_F(W)$. We can extend $\{t\}$ to B, a F-basis for V. Now we define a linear map $\phi : V \to F$ such that $\phi(t) = 1$ and $\forall v \in B \setminus \{t\},\ \ \phi(v) = 0$. It is clear that $W \subset \mathrm{span}_F(B \setminus \{t\})$. Hence ϕ is a linear map annihilating W which is nonzero and this is a contradiction. □

The main key to this correspondence is the below proposition.

Proposition 45. *[38] (Speiser's Lemma) Let V be an F-vector space and G be a finite group which acts faithfully on F and acts on V by the property*

$$\forall l \in F, v \in V and\ \ g \in G \quad g.(lv) = (g.l)(g.v)$$

i.e. V is a G-module with above property. Then V^G contains an F-basis for V.

Now let T be an algebraic K-torus which splits over a Galois extension F and $G = \mathrm{Gal}(F/K)$. Considering its character group M we get a G-lattice. We can construct an algebraic torus out of M by considering $\mathrm{Spec}(F[M]^G)$ with coordinate ring $F[M]^G$.

We note that T is diagonalizable (Theorem 43), so over F, its coordinate ring is $F[M]$. Applying the proposition to $F[M]^G$ we see that

$$F[M]^G \otimes_K F \cong F[M]$$

So over F, T and $\mathrm{Spec}(F[M]^G)$ has the same coordinate ring.

Up to now we know that there is a one to one correspondence between algebraic tori split by a G-Galois extension and G-lattices or equivalently integral representations of G. In other words for an algebraic K-torus T of dimension n, which splits over finite Galois extension F with $G = \mathrm{Gal}(F/K)$, T is determined by $h : G \longrightarrow \mathrm{GL}(n, \mathbb{Z})$. We call $h(G)$ the splitting group of T, which is a finite subgroup of $\mathrm{GL}(n, \mathbb{Z})$. So in order to classify algebraic tori of dimension n over k, we have to investigate in all conjugacy classes of finite subgroups of $\mathrm{GL}(n, \mathbb{Z})$. As we mentioned earlier Jordan proved that the number of finite subgroups of $\mathrm{GL}(n, \mathbb{Z})$ for any n, up to conjugacy, is finite.

2.5 Basic Results

In this section we present some important results about rationality problem for algebraic tori. Before presenting the results we need the following definition to avoid repeating the same assumptions.

Definition 46. If G is a finite subgroup of $\mathrm{GL}(n, \mathbb{Z})$, then the corresponding lattice to G which is denoted by L_G is the rank n lattice generated by the standard basis, i.e. $L_G = \langle e_i : i = 1, \ldots, n\rangle_{\mathbb{Z}}$ where $(e_i)_j = \delta_{ij}$. The action of G on L_G is given by multiplication from right on the e_i's. Moreover, if $G \cong \mathrm{Gal}(K/F)$ for some finite Galois extension K/F then $K[L_G] \cong K[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$, that is the Laurent polynomial ring, and $K(L_G)$ which is the quotient field of $K[L_G]$ is isomorphic to $K(x_1, \ldots, x_n)$ (x_i's are algebraically independent over K) are equipped with an action of G as

- G acts as Galois group on K
- $\forall g \in G,\ \ g(x_i) = \prod_{j=1}^{j=n} x_j^{a_{ij}}$ where a_{ij}'s are given by $g(e_i) = \sum_{j=1}^{j=n} a_{ij} e_j$.

Also T_G is the corresponding algebraic torus to L_G i.e. T_G is an algebraic torus defined on F which splits over K, with character lattice L_G.

By the duality explained before, $K(L_G)^G$ is the rational function field of T_G. From now on we work with finite subgroups of $\mathrm{GL}(n, \mathbb{Z})$ (up to conjugacy) and when we consider their corresponding lattice (or algebraic torus), L_G (T_G), we mean the lattice (algebraic torus) defined in Definition 46.

Theorem 47. *[38] (No Name Lemma) Let M be a permutation G-lattice and F be a G-field. Then $F(M)^G$ is rational over F^G.*

Proof. Let $\{x_1, \ldots, x_n\}$ be a $\mathbb{Z}$-basis which is permuted by G and $V = \sum_{i=1}^{n} Fx_i$ be a F vector space. Applying Proposition 45 to V, we find $y_1, \ldots, y_n \in V^G$ such that $V = \sum_{i=1}^{n} Fy_i$. This implies $F(M) = F(x_1, \ldots, x_n) = F(y_1, \ldots, y_n)$. Hence

$$F(M)^G = F(y_1, \ldots, y_n)^G = F^G(y_1, \ldots, y_n).$$

□

Note that if $G = \mathrm{Gal}(F/K)$, then $F^G = K$. For another version of the No Name Lemma see [9].

Theorem 48. *[25, Proposition 9.5.1] Assume L is a sign permutation G-lattice and F is a G-field. Then $F(M)^G$ is rational over F^G.*

The rationality problem for algebraic tori of dimension one was concrete. For dimension two Voskresenskii used a geometric method to prove the below result.

Theorem 49. *[42] Any 2 dimensional algebraic torus over k, is k-rational.*

We talked about the duality between category of algebraic tori and category of G-lattice. Having the duality in hand one may ask how to interpret the notions from one side to the other side. One of the important results about translating the facts about the rationality of algebraic tori, into the language of G-lattices is given below.

Theorem 50. *[43] Let M and M' be two G-lattices and F/K be a finite Galois extension with Galois Group G. Then $[M]^{fl} = [M']^{fl}$ if and only if $F(M)^G$ and $F(M')^G$ are stably isomorphic.*

The next two results give us necessary and sufficient conditions for stable rationality and retract rationality in terms of G-lattices. Having these two criteria gives us some control over the birational classification of algebraic tori of small dimension.

Theorem 51. *[25, Theorem 9.5.4] Let M be a G-lattice and F/K be a finite Galois extension with Galois group G. $[M]^{fl}$ is invertible if and only if $F(M)^G$ is retract K-rational.*

Theorem 52. *[10, Theorem 1.6]Let M be a G-lattice and F/K be a finite Galois extension with Galois group G. $[M]^{fl} = 0$ if and only if $F(M)^G$ is stably K-rational.*

The above two theorems can be used to see any stably rational algebraic torus is retract rational.

The following two theorems classifies algebraic tori of dimension 4 and 5 up to stable rationality. In [15] the authors gave a complete classification of mentioned tori, however they did not say anything about rationality of tori of dimension 4 and 5. The main idea of their work was to investigate the last 3 results above, by means of computer algebra system, GAP.

Theorem 53. *[15, Theorem 1.9] Let F/K be a finite Galois extension with Galois Group $G \leqslant \mathrm{GL}(4,\mathbb{Z})$. Assume G acts on $L = F(x_1, x_2, x_3, x_4)$ as above. (For tables of the below subgroups see [15, Page 4])*
(i) L^G is stably K-rational if G is (up to conjugacy) one of a list of 487 subgroups of $\mathrm{GL}(4,\mathbb{Z})$.
(ii) L^G is not stably but retract K-rational if G is (up to conjugacy) one of a list of 7 subgroups of $\mathrm{GL}(4,\mathbb{Z})$.
(iii) L^G is not retract K-rational if G is (up to conjugacy) one of a list of 216 subgroups of $\mathrm{GL}(4,\mathbb{Z})$.

In 2015, Lemire showed that except for possibly ten, all stably rational groups found by Hoshi and Yamasaki are rational (see [23]).

Theorem 54. *[15, Theorem 1.12] Let F/K be a finite Galois extension with Galois Group $G \leqslant \mathrm{GL}(5,\mathbb{Z})$. Assume G acts on $L = F(x_1, x_2, x_3, x_4, x_5)$ as above. (for tables of below subgroups see [15, Pages 134-144])*
(i) L^G is stably K-rational if G is (up to conjugacy) one of a list 3051 subgroups of $\mathrm{GL}(5,\mathbb{Z})$.
(ii) L^G is not stably but retract K-rational if G is (up to conjugacy) one of a list 25 subgroups of $\mathrm{GL}(5,\mathbb{Z})$.
(iii) L^G is not retract K-rational if G is (up to conjugacy) one of a list of 3003 subgroups of $\mathrm{GL}(5,\mathbb{Z})$.

There are examples of varieties which are stably rational but not rational. So in general being stably rational is not the same as being rational. However, there is a conjecture about the equivalence of stable rationality and rationality for algebraic tori.

Conjecture. [44, Section 2.6.1] Any stably rational algebraic torus is rational.

According to Theorem 54 we know all stably rational algebraic tori of dimension 5. However, the theorem does not say anything about rationality of those tori. An interesting problem is to find all rational tori between 3051 mentioned tori in the theorem.

We call $G \leq \mathrm{GL}(n,\mathbb{Z})$ irreducible (resp. indecomposable), if the corresponding lattice to G be irreducible (resp. indecomposable).

2.6 Families of Rational Algebraic Tori

In the next chapter, we investigate on rationality of stably rational algebraic tori of dimension 5. We will try to reduce their rationality to the rationality of some well understood algebraic torus. In this small section we present some families of algebraic tori which are rational, so that we can relate our algebraic tori to one of these families. It is already mentioned that every n dimensional algebraic torus has a corresponding finite subgroup of $\mathrm{GL}(n,\mathbb{Z})$. In order to study the rationality of algebraic tori, we study its corresponding group. We would rather to consider maximal groups and prove rationality for their subgroups, instead of proving it case by case. The following definitions are borrowed from [23].

Definition 55. Let L be a G-lattice for $G \leq \mathrm{GL}(n, \mathbb{Z})$. If all algebraic tori with character lattice $L \downarrow_H^G$ and splitting group H are rational, for any subgroup $H \leq G$, then we call L hereditarily rational.

Definition 56. If T is an algebraic torus and L is its corresponding lattice, then T is called hereditarily rational if L is hereditarily rational.

By Theorem 47, a quasi-split torus is rational. For a permutation G-lattice L and any subgroup $H \leq G$, since $L \downarrow_H^G$ is a permutation lattice, the corresponding torus to $L \downarrow_H^G$ is rational. In other words a quasi split torus is hereditarily rational. Simillarly by Theorem 48 and above argument for (a sign permutation lattice), we conclude that any algebraic torus with a sign permutation character lattice is hereditarily rational.

In particular this is true for an algebraic torus with character lattice the root lattice $\mathbb{Z}B_n$ as an $W(B_n)$-lattice. It is also known that any rank n sign permutation lattice, is isomorphic to the restriction of $\mathbb{Z}B_n$ to a subgroup of $W(B_n)$.

Proposition 57. *[24, Proposition 1.5] Suppose P is a permutation projective G-lattice and G is the Galois group of a finite Galois extension, K/F. If*

$$0 \longrightarrow M \longrightarrow L \longrightarrow P \longrightarrow 0$$

is an exact sequence of G-lattices, then the fields $K(L)^G$ and $K(M \oplus P)^G$ are isomorphic over F.

One can use the above proposition and Theorem 47 to conclude the following theorem.

Theorem 58. *[24, Proposition 1.6] Suppose P is a permutation G-lattice and G is the Galois group of a finite Galois extension, K/F. If*

$$0 \longrightarrow M \longrightarrow L \longrightarrow P \longrightarrow 0$$

is an exact sequence of G-lattices, then $K(L)^G$ is rational over $K(M)^G$.

An important corollary of the above theorem will be used frequently in chapter 3, in order to prove the rationality of algebraic tori.

Corollary 59. *Suppose P is a permutation G-lattice and G is the Galois group of a finite Galois extension, K/F. If*

$$0 \longrightarrow M \longrightarrow L \longrightarrow P \longrightarrow 0$$

is an exact sequence of G-lattices and $K(M)^G$ is rational over F, then $K(L)^G$ is rational over F.

In [44, Section 2.4.8] the author has shown that any algebraic torus with an augmentation ideal lattice is hereditarily rational. More precisely let T be an algebraic torus defined over F and splits over K and $G = \mathrm{Gal}(K/F)$. Assume the character lattice of T is I_X (the kernel of the augmentation map), and $\mathbb{Z}[X]$ is a G-permuattion lattice, where

$$0 \longrightarrow I_X \longrightarrow \mathbb{Z}[X] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0 \tag{2.2}$$

is an exact sequence and $\varepsilon : \mathbb{Z}[X] \to \mathbb{Z}$, $x \to 1$ is the augmentation map. The exact sequence (2.2) corresponds to the exact sequence of F algebraic tori

$$0 \longrightarrow \mathbb{G}_m \longrightarrow R_{K_1/F}(\mathbb{G}_m) \times \cdots \times R_{K_t/F}(\mathbb{G}_m) \longrightarrow T \longrightarrow 0$$

where K_i/F (for $i = 1, \ldots, t$) are intermediate fields of K/F and K/K_i is Galois. Now $T = \prod_{i=1}^{t} R_{K_i/F}(\mathbb{G}_m)/\mathbb{G}_m$ and is rational. We note that for any subgroup H of G, $I_X \downarrow_H^G$ is also an augmentation ideal. Hence an algebraic tori with augmentation ideal character lattice is hereditarily rational.

It is worth mentioning that passing to dual lattices in 2.2 we get

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}[X] \xrightarrow{\varepsilon} J_X \longrightarrow 0$$

where $J_X = I_X^*$ is called Chevalley module. The corresponding algebraic torus to J_X has interesting properties and is called norm one torus. Chevalley was the first one who discovered that norm one torus is not necessarily rational.

The following lemma was used in [23] to show that a given G-lattice is isomorphic to $J_{G/H}$.

Lemma 60. *[23, Remark 4.1] Let L be a G-lattice. If there exist $x \in L$ such that,*

- $\langle G.x \rangle_{\mathbb{Z}} = L$
- $\mathrm{Stab}_G(x) = H$
- $\sum_{g \in G} gx = 0$,

then $L \cong J_{G/H}$.

Chapter 3

Rationality Problem for Five Dimensional Algebraic Tori

In 2012 Hoshi and Yamasaki published a paper [15] in which they classified algebraic tori of dimensions 4 and 5 up to stable rationality. Their classification is based on computing the flasque classes of algebraic tori in GAP. They showed that in rank 5, there are exactly 311 indecomposable G-lattices which are stably rational. More precisely they showed their stable rationality by finding the maximal groups and proved stable rationality of their subgroups. The following table presents the maximal groups they found.

Number	CARAT ID	G	$\#G$
1	$(5,942,1)$	$\mathrm{Imf}(5,1,1)$	3840
2	$(5,953,4)$	S_6	720
3	$(5,726,4)$	$C_2^4 \rtimes S_4$	384
4	$(5,919,4)$	$C_2 \times S_5$	240
5	$(5,801,3)$	$C_2 \times (S_3^2 \rtimes C_2)$	144
6	$(5,655,4)$	$D_8^2 \rtimes C_2$	128
7	$(5,911,4)$	S_5	120
8	$(5,946,2)$	S_5	120
9	$(5,946,4)$	S_5	120
10	$(5,947,2)$	S_5 ,	120
11	$(5,337,12)$	$D_8 \times S_3$	48
12	$(5,341,6)$	$D_8 \times S_3$	48
13	$(5,531,13)$	$C_2 \times S_4$	48
14	$(5,533,8)$	$C_2 \times S_4$	48
15	$(5,623,4)$	$C_2 \times S_4$	48
16	$(5,245,12)$	$C_2^2 \times S_3$	24
17	$(5,81,42)$	$C_2 \times D_8$	16
18	$(5,81,48)$	$C_2 \times D_8$	16

Table 3.1: The maximal 18 groups in the 311 cases found by Hoshi and Yamasaki in [15].

In 2015 Lemire [23], proved that, except for possibly ten of the 4 dimensional stably rational algebraic tori found by Hoshi and Yamasaki, all of them are rational. The rationality of the ten exceptional cases is still unknown. The author did not use any computer based arguments except for finding generating sets of groups and lattices of subgroups in GAP. The rationality results we are presenting are based on the ideas used in [23]. We present algorithms which may be applied to character lattices of algebraic tori, in order to investigate their rationality. These algorithms provide machinery to reduce the rationality problem in a specific dimension to lower dimensions.

From now on we will call the groups mentioned in Table 3.1 respectively G_1 to G_{18}. L_G represents the corresponding G-lattice to a finite subgroup of $\mathrm{GL}(n,\mathbb{Z})$, G, as defined in Definition 46. When we say a group or a lattice is rational we mean their corresponding algebraic torus is rational. By a decomposable (matrix) group, we mean its corresponding lattice is decomposable. We say G' is the dual group of G if G' is the corresponding group to the dual of L_G.

In this chapter we will investigate the rationality of $G_1,\ldots,G_{18}$. In some cases, we prove that the group is hereditarily rational. There are two main methods that we will use, both of which were used in [23]. The first method is reducing the rationality of a five dimensional torus to rationality in lower dimensions. The second one is to see them as lattices of which the rationality is known.

3.1 GAP: Carat and CrystCat

GAP [11] stands for Groups, Algorithms, Programming, and is a computer algebra system for computations in discrete algebra with emphasis on computations in group theory. GAP is an open source system which is accessible directly or in SAGE [8]. GAP provides various packages for computations in matrix groups and representation theory. For our purposes we need Carat and CrystCat packages of GAP.

The GAP package Carat provides functions of the stand-alone programs of *CARAT*, which is a package for the computations related to crystallographic groups. Carat contains the catalog of all conjugacy classes of finite subgroups of $\mathrm{GL}(n,\mathbb{Z})$ for n up to six. More precisely the Carat package gives access to all $\mathbb{Q}$-classes and $\mathbb{Z}$-classes and maximal classes over $\mathbb{Z}$ (for the number of these classes see Table 3.2).

Remark. The $\mathbb{Q}$-classes are conjugacy classes over $\mathbb{Q}$. We note that some $\mathbb{Z}$-classes may belong to the same conjugacy class over the rationals.

n	# conjugacy classes of finite subgroups of $\mathrm{GL}(n,\mathbb{Z})$	# conjugacy classes of maximal finite subgroups of $\mathrm{GL}(n,\mathbb{Z})$	# conjugacy classes of finite subgroups over $\mathbb{Q}$
1	2	1	2
2	13	2	10
3	73	4	32
4	710	9	227
5	6079	17	955
6	85308	39	7103

Table 3.2: Numbers of conjugacy classes which are accessible in Carat.

It is worth mentioning that Carat contains information about crystallographic groups which we will not use. The CrystCat Package in GAP also provides a catalog of crystallographic groups up to dimension 4. The catalog mostly covers the data in [3]. CrystCat and Carat are complement of each other.

The GAP ID, (n,m,l,k) of a finite subgroup G of $\mathrm{GL}(n,\mathbb{Z})$ means that G is of rank n and belongs to k-th $\mathbb{Z}$ class of the l-th $\mathbb{Q}$-class of the m-th crystal system. This works for $2 \leq n \leq 4$. Hoshi and Yamasaki wrote a GAP code using the Carat package to have easy access to the j-th $\mathbb{Z}$-class of the i-th $\mathbb{Q}$-class group of rank n. They called this Carat ID. The GAP scripts written by Hoshi and Yamasaki are available from http://www.math.h.kyoto-u.ac.jp/ yamasaki/Algorithm/

The algorithms introduced in the next section are implemented in GAP (needs some functions from the codes written by Hoshi and Yamasaki) and the code is available from

https://github.com/armin-jamshidpey/Algebraic-Tori

Since the actions of matrix groups in GAP are considered from right, throughout this chapter we work with row vectors instead of columns. One may also use the columns by considering the dual groups.

3.2 Reduction Algorithms

Assume

$$0 \to M \to L_G \to N \to 0$$

is a short exact sequence of G-lattices such that N is a permutation projective G-lattice. If K/F is a finite Galois extension with $G \cong \mathrm{Gal}(K/F)$, then by Theorem (58), $K(L_G)^G$ is rational over $K(M)^G$. Thus, rationality of $K(M)^G$ over F implies rationality of $K(L_G)^G$ over F.

Suppose L_G is an indecomposable G-lattice. In this section, we present methods to examine the possibility of existence of such a short exact sequence for L_G, with N a permutation G-lattice.

Although sign permutation lattices are not permutation projective, constructing a short exact sequence of G-lattices

$$0 \to M \to L_G \to N \to 0$$

where N is a rank one sign permutation G-lattice might help to determine rationality of the associated algebraic torus to L_G. Note that existence of such a sequence does not directly imply rationality. However, under some conditions the rationality may be concluded.

The goal of this section is to provide tools to get exact sequences mentioned above for a given indecomposable G-lattice. The idea behind all of the methods is a simple fact which we explain briefly here.

A lattice L_G, is reducible as a G-lattice if and only if $\mathbb{Q}L_G = L_G \otimes_{\mathbb{Z}} \mathbb{Q}$ has a proper $\mathbb{Q}[G]$-submodule W of dimension $0 < m < n$. Let L_G be a G-lattice of rank n and W is an m dimensional proper $\mathbb{Q}[G]$-submodule of $\mathbb{Q}L_G$. Then $L_G \cap W$ is a sublattice of L_G of rank m such that $\mathbb{Q}(L_G \cap W) = W$. Then

$$0 \to L_G \cap W \to L_G \to L_G/(L_G \cap W) \to 0$$

is a short exact sequence of G-lattices. Note that this implies in particular that $L_G/(L_G \cap W)$ is torsion free so that a $\mathbb{Z}$-basis of $L_G \cap W$ can be extended to a $\mathbb{Z}$-basis of L_G.

In the next paragraphs we are specifically looking for an $n-1$ dimensional proper $\mathbb{Q}[G]$-submodule of $\mathbb{Q}L_G$.

If we start with the dual lattice L_G^*, and we are able to find a rank 1 permutation sublattice of L_G^*, we get

$$0 \to \mathbb{Z} \to L_G^* \to M \to 0,$$

where $M = L_G^*/\mathbb{Z}$ is of rank $n-1$. Then by dualizing the sequence we have

$$0 \to M^* \to L_G \to \mathbb{Z} \to 0$$

as desired.

Now, we explain how to find a permutation rank one sublattice of L_G^*. In order to get a one dimensional $\mathbb{Q}[G]$-submodule of $\mathbb{Q}L_G^*$, we use the eigenspaces of the transposes of a generating set of G. Let $\{\sigma_1, \ldots, \sigma_m\}$ be the transposes of a generating set of G and let $G^* = \langle \sigma_1, \ldots, \sigma_m \rangle$. Suppose E_{1,σ_i} is the left nullspace of $\sigma_i - I$ over $\mathbb{Q}$. We define

$$E_1 = E_{1,\sigma_1} \cap \cdots \cap E_{1,\sigma_n}.$$

Note that G^* acts trivially on E_1. If $E_1 \neq 0$ then we can choose a nonzero vector $u \in E_1$. Let $u = (\frac{a_1}{b_1}, \frac{a_2}{b_2}, \ldots, \frac{a_n}{b_n}) \in E_1$ such that $\gcd(a_i, b_i) = 1$. If $m = \operatorname{lcm}(b_1, \ldots, b_n)$ then $mu = (a_1', \ldots, a_n') \in \mathbb{Z}^n$. If $\gcd(a_1', \ldots, a_n') = d$ then $v = \frac{m}{d}u \in L_G \cap E_1$ and the gcd of its entries is 1.

As a consequence, we can extend $\{v\}$ to a $\mathbb{Z}$-basis of L_G^*. A general algorithm to do this extension is given by Magliveras et al in [27]; GAP also has a function which does the job. In most of the cases that we will see in the next section, v had a ± 1 as an entry, which makes the basis extension so simple: if v_j is ± 1 then $\{e_1, \ldots, e_{j-1}, e_{j+1}, \ldots, e_n, v\}$ forms a $\mathbb{Z}$-basis for L_G^*.

Since it is possible to extend v to a basis for the lattice L_G^*, there exists a change of basis matrix T in $\mathrm{GL}(n, \mathbb{Z})$ such that

$$T\sigma_i T^{-1} = \left[\begin{array}{c|c} \delta_i & * \\ \hline 0 & 1 \end{array}\right]$$

for some $\delta_i \in \mathrm{GL}(n-1, \mathbb{Z})$. Since we consider the finite subgroups of $\mathrm{GL}(n, \mathbb{Z})$ up to conjugacy, we can work with $G' = TG^*T^{-1}$. By considering the first $n-1$ vectors of the standard basis of the G'-lattice $L_{G'}$ (which is isomorphic to L_G^*), can form the G'-lattice M such that $L_{G'}/\mathbb{Z} = M$ and we get

$$0 \longrightarrow \mathbb{Z} \longrightarrow L_{G'} \longrightarrow M \longrightarrow 0.$$

By dualizing the sequence we get

$$0 \longrightarrow M^* \longrightarrow L_{G'}^* \longrightarrow \mathbb{Z} \longrightarrow 0.$$

Note that $L^*_{G'}$ is isomorphic to L_G.

The explained method above is presented as an algorithm here.

Algorithm 1 Fixed Point Algorithm

Input: A finite subgroup G of $\mathrm{GL}(n,\mathbb{Z})$, given by its generators $\{\sigma_1,\ldots,\sigma_m\}$.

Output: A matrix $T \in \mathrm{GL}(n,\mathbb{Z})$ such that $T\sigma_i^t T^{-1} = \left[\begin{array}{c|c} \delta_i & * \\ \hline 0 & 1 \end{array}\right]$ where $\delta_i \in \mathrm{GL}(n-1,\mathbb{Z})$, and sublattices M, N such that $0 \longrightarrow N \longrightarrow L^*_G \longrightarrow M \longrightarrow 0$ is an exact sequence of lattices.

$E \leftarrow \left[\ \sigma_1^t - I \mid \sigma_2^t - I \mid \cdots \mid \sigma_n^t - I\ \right]$
$W \leftarrow$ LeftNullspace(E)
if W is not zero then
    choose a nonzero $v \in W$
    if $v \notin \mathbb{Z}^n$
        find $c \in \mathbb{Z}$ s.t $cv \in \mathbb{Z}^n$ and $\gcd(cv) = 1$
        $v \leftarrow cv$
    end if
    apply the algorithm in [27] to extend v to a basis $B = \{\beta_1,\ldots,\beta_{n-1}, v\}$ for L_G
    $T \leftarrow \begin{bmatrix}\beta_1 & \cdots & \beta_{n-1} & v\end{bmatrix}^t$
    $N \leftarrow \mathbb{Z}v$
    $M \leftarrow L/N$
    return M, N, T
    end if
else
    return fail
end if

Remark. If the algorithm returns a matrix T then for $\sigma \in \{\sigma_1^t,\ldots,\sigma_m^t\}$,

$$T\sigma T^{-1} = \sigma'$$

where

$$\sigma' = \left[\begin{array}{c|c} \delta & * \\ \hline 0 & 1 \end{array}\right].$$

for some $\delta \in \mathrm{GL}(n-1,\mathbb{Z})$. More precisely

$$T\sigma = \sigma' T$$

and the last row of $T\sigma$ is nothing but $v\sigma = v$. This implies that the last row of $\sigma' = [0\ \ldots\ 0\ 1]$.

Example 1. Let $G \leq \mathrm{GL}(4, \mathbb{Z})$ be generated by

$$\begin{bmatrix} 0 & -1 & 0 & 0 \\ -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & -1 \\ 0 & -1 & -1 & 0 \end{bmatrix}.$$

The transposes are

$$\sigma = \begin{bmatrix} 0 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 \\ 0 & -1 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{bmatrix} \text{ and } \tau = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & -1 & -1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{bmatrix}.$$

Then the $E_{1,\sigma}$ is the left nullspace of

$$\sigma - I_4 = \begin{bmatrix} -1 & -1 & 1 & 1 \\ -1 & -2 & 1 & 1 \\ 0 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}.$$

One can verify that

$$\{\begin{bmatrix} 1 & -1 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & -1 & 0 & 1 \end{bmatrix}\}$$

is a basis for $E_{1,\sigma}$. Similarly $E_{1,\tau}$ is the left nullspace of

$$\tau - I_4 = \begin{bmatrix} -1 & -1 & 0 & 0 \\ 1 & -1 & -1 & -1 \\ 0 & 0 & -1 & -1 \\ 0 & 0 & -1 & -1 \end{bmatrix}$$

and it is generated by $\begin{bmatrix} 0 & 0 & -1 & 1 \end{bmatrix}$.

It is not hard to see $\begin{bmatrix} 0 & 0 & -1 & 1 \end{bmatrix} \in E_{1,\sigma}$. Thus

$$E_1 = E_{1,\sigma} \cap E_{1,\tau} = \langle \begin{bmatrix} 0 & 0 & -1 & 1 \end{bmatrix} \rangle$$

and $\begin{bmatrix} 0 & 0 & -1 & 1 \end{bmatrix} \in L$. Now

$$\{\begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & -1 & 1 \end{bmatrix}\}$$

forms a $\mathbb{Z}$-basis for L. The change of basis matrix T is

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{bmatrix}$$

Hence

$$T\sigma T^{-1} = \left[\begin{array}{ccc|c} 0 & -1 & 2 & 1 \\ -1 & -1 & 2 & 1 \\ 0 & -1 & 1 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right]$$

$$T\sigma T^{-1} = \left[\begin{array}{ccc|c} 0 & -1 & 0 & 0 \\ 1 & 0 & -2 & -1 \\ 0 & 0 & -1 & -1 \\ \hline 0 & 0 & 0 & 1 \end{array}\right]$$

Now by dualizing we get

$$\left[\begin{array}{ccc|c} 0 & -1 & 0 & 0 \\ -1 & -1 & -1 & 0 \\ 2 & 2 & 1 & 0 \\ \hline 1 & 1 & 0 & 1 \end{array}\right] \quad \text{and} \quad \left[\begin{array}{ccc|c} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & -2 & -1 & 0 \\ \hline 0 & -1 & -1 & 1 \end{array}\right]$$

as a generating set for a conjugate of G. By defining $M \subset L_G$ generated by e_1, e_2 and e_3 the following exact sequence will be obtained

$$0 \longrightarrow M \longrightarrow L_G \longrightarrow \mathbb{Z} \longrightarrow 0$$

We call the above process the fixed point algorithm. One can generalize it as follows. Assume $E_{\lambda,\sigma}$ be the left kernel of $\sigma - \lambda I$ over the rationals. Now define $E_{\pm 1,\sigma}$ to be the set $\{E_{1,\sigma}, E_{-1,\sigma}\}$. Assume $E_{\pm 1,G}$ is the Cartesian product of $E_{\pm 1,\sigma}$ for all $\sigma \in G^*$, i.e.

$$E_{\pm 1,G} = E_{\pm 1,\sigma_1} \times \cdots \times E_{\pm 1,\sigma_n}.$$

If there exist $A \in E_{\pm 1,G}$ such that $W = \bigcap_{B \in A} B \neq 0$, then we can find a nonzero $v \in L_G^* \cap W$. As we have seen in the fixed point algorithm, we can extend a multiple of v to a $\mathbb{Z}$-basis for L_G^*. Then we can get a change of basis matrix T, such that

$$T\sigma_i T^{-1} = \left[\begin{array}{c|c} \delta_i & * \\ \hline 0 & \pm 1 \end{array}\right]$$

for some $\delta_i \in \mathrm{GL}(n-1, \mathbb{Z})$. Thus by a similar argument we can use the new representative of the conjugacy class of G^* to form an equivalent lattice and similarly by choosing the first $n-1$ elements of the standard basis of $L_{G'}$ we can produce

$$0 \longrightarrow \mathbb{Z}^- \longrightarrow L_{G'} \longrightarrow M \longrightarrow 0.$$

By dualizing the sequence we get

$$0 \longrightarrow M^* \longrightarrow L_{G'}^* \longrightarrow \mathbb{Z}^- \longrightarrow 0.$$

Again note that $L^*_{G'}$ is isomorphic to L_G.

This process will be called the sign fixed point algorithm and it is presented as an algorithm here.

Algorithm 2 Sign Fixed Point Algorithm

Input: A finite subgroup G of $\mathrm{GL}(n,\mathbb{Z})$, given by its generators $\{\sigma_1,\ldots,\sigma_m\}$.

Output: A matrix $T \in \mathrm{GL}(n,\mathbb{Z})$ such that $T\sigma_i^t T^{-1} = \left[\begin{array}{c|c} \delta_i & * \\ \hline 0 & 1 \end{array}\right]$ where $\delta_i \in \mathrm{GL}(n-1,\mathbb{Z})$, and sublattices M, N such that $0 \longrightarrow N \longrightarrow L^*_G \longrightarrow M \longrightarrow 0$ is an exact sequence of lattices.

1: for g in $\{\sigma_1^t,\ldots,\sigma_m^t\}$ do
    $E_g \leftarrow$ the set of left nullspaces of $g \pm I$ over $\mathbb{Q}$
  end do
2: $E \leftarrow E_{\sigma_1^t} \times E_{\sigma_2^t} \times \cdots \times E_{\sigma_m^t}$
3: $W \leftarrow 0$
4: while $W = 0$ and $E \neq \emptyset$ do
    $A \leftarrow$ a random element of E
    $W \leftarrow \bigcap_{a\in A} a$
    $E \leftarrow E \setminus A$
  end do
5: if W is not zero then
    choose a nonzero $v \in W$
    if $v \notin \mathbb{Z}^n$
      find $c \in \mathbb{Z}$ s.t $cv \in \mathbb{Z}^n$ and $\gcd(cv) = 1$
      $v \leftarrow cv$
    end if
    apply the algorithm in [27] to extend v to get a basis $B = \{\beta_1,\ldots,\beta_{n-1},v\}$ for L
    $T \leftarrow \begin{bmatrix}\beta_1 & \cdots & \beta_{n-1} & v\end{bmatrix}^t$
    $N \leftarrow \mathbb{Z}v$
    $M \leftarrow L/N$
    return M, N, T
    end if
  else
    return fail
  end if

Example 2. Let $G \leq \mathrm{GL}(4, \mathbb{Z})$ be generated by

$$\begin{bmatrix} -1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ -1 & 1 & 0 & 1 \end{bmatrix}.$$

The transposes are

$$\sigma = \begin{bmatrix} -1 & 0 & -1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{bmatrix} \text{ and } \tau = \begin{bmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 1 \end{bmatrix}.$$

Then

$$\sigma - I_4 = \begin{bmatrix} -2 & 0 & -1 & 0 \\ 1 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & -1 \end{bmatrix}$$

$$\sigma + I_4 = \begin{bmatrix} 0 & 0 & -1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 2 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$\tau - I_4 = \begin{bmatrix} -1 & 0 & 0 & -1 \\ 1 & -1 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & -1 & 0 \end{bmatrix}$$

$$\tau + I_4 = \begin{bmatrix} 1 & 0 & 0 & -1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & -1 & 2 \end{bmatrix}.$$

By computing the left nullspaces we get

$$E_{1,\sigma} = \langle [0, 0, 1, 0], [1, 1, 0, 1] \rangle$$

$$E_{-1,\sigma} = \langle [[2, 0, 1, 0], [1, -1, 0, 1]] \rangle$$

$$E_{1,\tau} = \langle [-1, -1, -1, 1] \rangle$$

$$E_{-1,\tau} = \langle [1, -1, 1, 1] \rangle$$

So

$$E_{1,\sigma} \cap E_{1,\tau} = 0$$

$$E_{1,\sigma} \cap E_{-1,\tau} = 0$$
$$E_{-1,\sigma} \cap E_{1,\tau} = \langle [1,1,1,-1] \rangle$$
$$E_{-1,\sigma} \cap E_{-1,\tau} = 0$$

Let $W = E_{-1,\sigma} \cap E_{1,\tau}$. So $[1,1,1,-1] \in L \cap W$ is extendable to a basis for L by vectors

$$[1,0,0,0]\,,\ [0,1,0,0] \text{ and } [0,0,1,0]$$

and the corresponding transformation is

$$T = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & -1 \end{bmatrix}$$

$$\sigma' = T\sigma T^{-1} = \begin{bmatrix} 0 & 1 & -1 & -1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

$$\tau' = T\tau T^{-1} = \begin{bmatrix} 0 & 0 & -1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & -1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Now by dualizing we get

$$\left[\begin{array}{ccc|c} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ -1 & 1 & 1 & 0 \\ \hline -1 & 0 & 1 & -1 \end{array}\right] \text{ and } \left[\begin{array}{ccc|c} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ -1 & 1 & 0 & 0 \\ \hline 0 & 0 & -1 & 1 \end{array}\right]$$

as a generating set for a conjugate of G. By defining $M \subset L_G$ generated by e_1, e_2 and e_3 the following exact sequence will be obtained

$$0 \longrightarrow M \longrightarrow L_G \longrightarrow \mathbb{Z}^- \longrightarrow 0.$$

In general to get a $\mathbb{Q}[G]$-submodule W of $\mathbb{Q}L$, where $L = L_G$ is a G-lattice, one can use the decomposition of $\mathbb{Q}L$ (provided that it is decomposable). It is not always easy to find the decomposition of a $\mathbb{Q}[G]$-module. The most well-known tool for module decomposition is the meataxe algorithm. The algorithm was first introduced by Parker in [31] in order to check irreducibility of a finite dimensional module over a finite field and finding explicit submodules in case of reducibility. Later on Parker extended the idea of the meataxe algorithm to characteristic zero (see [32]). His algorithm can be used to decompose an integral representation of a finite group. In [33], the authors provided machinery which enables us to decompose $\mathbb{Q}[G]$-modules up to dimension 200. So there are algorithms which give the decomposition over $\mathbb{Q}$. We invite the reader to see [26] and [14] for more details.

Assume $G \leq \mathrm{GL}(n, \mathbb{Z})$ is finite and $\mathbb{Q}L = L \otimes_{\mathbb{Z}} \mathbb{Q}$ is the $\mathbb{Q}$-vector corresponding space to L. If $\mathbb{Q}L$ is a decomposable $\mathbb{Q}[G]$-module, then there exists a change of basis matrix such that generators of the $\mathbb{Q}$-class of G can be written as block diagonal matrices

$$T\sigma_i T^{-1} = \left[\begin{array}{c|c} \delta_i & 0 \\ \hline 0 & \gamma_i \end{array}\right]$$

where $\delta_i \in \mathrm{GL}(m, \mathbb{Q})$ and $\gamma_i \in \mathrm{GL}(m', \mathbb{Q})$ for some $m, m' \in \mathbb{Z}$. Let $\{e_1, \ldots, e_m, e_{m+1}, \ldots, e_{m+m'}\}$ be the standard basis for $\mathbb{Q}L$. The $\mathbb{Q}M$ and $\mathbb{Q}N$ generated respectively by $\{e_1, \ldots, e_m\}$ and $\{e_{m+1}, \ldots, e_{m+m'}\}$ are invariant (set wise) under the action of G and $\mathbb{Q}L = \mathbb{Q}M \oplus \mathbb{Q}N$. Now $T^{-1}(\mathbb{Q}M)$ is a G-stable subspace and

$$M = L \cap T^{-1}(\mathbb{Q}M)$$

is G stable. Then we get

$$0 \longrightarrow M \longrightarrow L \longrightarrow L/M \longrightarrow 0$$

as an exact sequence of lattices.

The above idea can be turned into an algorithm. In order to do so, one need to compute the decomposition of $\mathbb{Q}L$ (meataxe or any other algorithm can be applied). If in the previous step the change of basis, namely T, to get the decomposition is not computed, it should be done next. The next step is to choose a component of the decomposition, say $\mathbb{Q}M$ and a basis of it. After that, $M = T^{-1}(\mathbb{Q}M) \cap L$ is a sublattice of L. The last step is to extend a basis of M to L (see [27] for an algorithm).

Here is an example which shows the above idea in practice. The $\mathbb{Q}$-class of the group is presented from the list of $\mathbb{Q}$-classes in rank 4 provided in [15].

Example 3. Consider the group G generated by

$$\sigma = \begin{bmatrix} 0 & 0 & -1 & 0 & 1 \\ -1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & -1 \\ 0 & 0 & -1 & 0 & 0 \end{bmatrix} \text{ and } \tau = \begin{bmatrix} -1 & 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 \\ 1 & -1 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

The $\mathbb{Q}$-class of G is accessible in the list of rank 4 groups in [15] by the name cryst4[149]. The generators of the $\mathbb{Q}$-class are

$$\sigma' = \left[\begin{array}{ccc|cc} 0 & 0 & 1 & 0 & 0 \\ 1 & -1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right] \text{ and } \tau' = \left[\begin{array}{ccc|cc} 1 & -1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 & -1 \end{array}\right].$$

Considering the orders of matrices we can figure out there exist an invertible integral matrix T such that

$$T\sigma T^{-1} = \sigma'$$

$$T\tau T^{-1} = \tau'.$$

Assume 25 indeterminates $t_{00}, \ldots, t_{44}$ and the matrix

$$T = \begin{bmatrix} t_{00} & t_{01} & t_{02} & t_{03} & t_{04} \\ t_{10} & t_{11} & t_{12} & t_{13} & t_{14} \\ t_{20} & t_{21} & t_{22} & t_{23} & t_{24} \\ t_{30} & t_{31} & t_{32} & t_{33} & t_{34} \\ t_{40} & t_{41} & t_{42} & t_{43} & t_{44} \end{bmatrix}.$$

Then

$$T \cdot \begin{bmatrix} 0 & 0 & -1 & 0 & 1 \\ -1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & -1 \\ 0 & 0 & -1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & -1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \cdot T$$

$$T \cdot \begin{bmatrix} -1 & 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 \\ 1 & -1 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & -1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 & -1 \end{bmatrix} \cdot T.$$

The transformation T can be found by solving (and replacing parameters) the linear system obtained from above equations as

$$T = \begin{bmatrix} -1 & 1 & -2 & 1 & 1 \\ -1 & 2 & -1 & 0 & -1 \\ 0 & -1 & -1 & -1 & 0 \\ 1 & -2 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 & 1 \end{bmatrix}.$$

Define $\mathbb{Q}M = \langle e_1, e_2, e_3 \rangle_{\mathbb{Q}}$, since

$$T^{-1} = \begin{bmatrix} -\frac{1}{4} & \frac{1}{4} & -\frac{1}{4} & \frac{1}{4} & \frac{3}{4} \\ -\frac{1}{4} & \frac{1}{4} & -\frac{1}{4} & -\frac{1}{4} & \frac{1}{4} \\ -\frac{1}{4} & -\frac{1}{4} & -\frac{1}{4} & -\frac{1}{4} & -\frac{1}{4} \\ \frac{1}{2} & 0 & -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & -\frac{1}{2} & 0 & -\frac{1}{2} & 0 \end{bmatrix}$$

we have

$$T^{-1}(e_1) = \left[-\frac{1}{4}, \frac{1}{4}, -\frac{1}{4}, \frac{1}{4}, \frac{3}{4}\right]$$
$$T^{-1}(e_2) = \left[-\frac{1}{4}, \frac{1}{4}, -\frac{1}{4}, -\frac{1}{4}, \frac{1}{4}\right]$$
$$T^{-1}(e_3) = \left[-\frac{1}{4}, -\frac{1}{4}, -\frac{1}{4}, -\frac{1}{4}, -\frac{1}{4}\right]$$

Hence $T^{-1}(\mathbb{Q}M) = \langle \left[-\frac{1}{4}, \frac{1}{4}, -\frac{1}{4}, \frac{1}{4}, \frac{3}{4}\right], \left[-\frac{1}{4}, \frac{1}{4}, -\frac{1}{4}, -\frac{1}{4}, \frac{1}{4}\right], \left[-\frac{1}{4}, -\frac{1}{4}, -\frac{1}{4}, -\frac{1}{4}, -\frac{1}{4}\right] \rangle_{\mathbb{Q}}$ Now

$$M = L \cap T^{-1}(\mathbb{Q}M) = \langle \begin{bmatrix} 1 & 0 & 1 & 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & 1 & 1 \end{bmatrix} \rangle_{\mathbb{Z}}$$

By extending the above basis of M to a basis of L (by adding $[0, 0, 1, 0, 0]$ and $[0, 0, 0, 0, 1]$) and forming the change of basis matrix we get

$$S = \begin{bmatrix} 1 & 0 & 1 & 0 & -1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

which gives

$$\begin{bmatrix} 1 & 0 & 1 & 0 & -1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & -1 & 0 & 1 \\ -1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & -1 \\ 0 & 0 & -1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 0 & -1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}^{-1} = \left[\begin{array}{ccc|cc} 0 & 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ \hline 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & -1 & 0 \end{array}\right]$$

$$\begin{bmatrix} 1 & 0 & 1 & 0 & -1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 \\ 1 & -1 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 0 & -1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}^{-1} = \left[\begin{array}{ccc|cc} 0 & 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & 1 & -1 \end{array}\right]$$

Now we can get the following exact sequence of lattices

$$0 \longrightarrow M \longrightarrow L \longrightarrow L/M \longrightarrow 0.$$

3.3 Rationality Problem for 5 Dimensional Indecomposable Stably Rational Algebraic Tori

Up to now we have presented some algorithms to reduce a lattice and form exact sequences of specific type. In this section we apply those algorithms to the 18 indecomposable lattices which are maximal in the set of indecomposable stably rational rank 5 lattices found in [15].

In some cases instead of applying any algorithm we interpret the lattice as a root lattice of a root system. The general idea is to identify the given lattice as a lattice in one of the hereditarily rational families of lattices. We also try to reduce some lattices to one of those families.

There are also cases where our reduction does not provide enough information to decide about the rationality. In these cases we reduce the lattice and provide some information which may help to decide about their rationality. There are also irreducible lattices among the 18 maximal ones. A partial lattice of maximal subgroups of the irreducible cases is provided so that our algorithms work for maximal subgroups.

Throughout this section for a finite subgroup $G \leq \mathrm{GL}(n, \mathbb{Z})$, the corresponding algebraic torus and the corresponding lattice (see Definition 46) is denoted respectively by T_G and L_G. When we say a group is rational or a lattice is rational we mean the corresponding algebraic torus is rational.

3.3.1 Case G_1

G_1 is one of the 7 maximal indecomposable finite subgroups of $\mathrm{GL}(5, \mathbb{Z})$. This is the automorphism group of root system B_5. So we can recognize the lattice as $(\mathbb{Z}(B_5), \mathrm{Aut}(B_5))$. This lattice is hereditarily rational (see [23]).

Alternatively by looking at the generators of G_1

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

One can also see that the corresponding lattice is sign permutation which implies rationality of L_{G_1}

3.3.2 Case G_2

This is a group isomorphic to S_6. Following [23] we show that the dual lattice is isomorphic to Chevalley module J_{S_6/S_5}. The group G_2 is generated by

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & -1 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & 1 & 0 & 0 & -1 \\ 0 & -1 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & -1 & 0 \end{bmatrix}.$$

The dual lattice corresponds to the group generated by

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & -1 & 1 & 1 & -1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix} \text{ and } B = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & -1 & 1 & 1 & -1 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

The following computations show that e_1 is a cyclic generator of $L^*_{G_2}$.

$$e_1B = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & -1 & 1 & 1 & -1 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

$$e_1B^2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ -1 & 1 & -1 & -1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & -1 & 0 & 0 & 0 \end{bmatrix}$$

$$e_1B^3 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} -1 & 1 & -1 & -1 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 1 & -1 & -1 & 1 \end{bmatrix}$$

$$e_1B^3A = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} -1 & 1 & -1 & -1 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & -1 & 1 & 1 & -1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Now we have to make sure that the stabilizer subgroup of e_1 is isomorphic to S_5.

```
gap> GD2:= GroupByGenerators([A,B]);
<matrix group with 2 generators>

gap> S:= Stabilizer(GD2 ,e1);
<matrix group with 6 generators>

gap> StructureDescription(S);
"S5"
```

The last step is to check if $\sum_{g\in H} e_1.g = 0$

```
gap> n:= [0,0,0,0,0];
0
gap> for g in GD2 do n:= n + (e1*g); od;
gap> n;
[ 0, 0, 0, 0, 0 ]
```

This shows that the lattice is isomorphic to J_{S_6/S_5} and its dual is isomorphic to the augmentation ideal I_{S_6/S_5}. This implies that G_2 is hereditarily rational.

3.3.3 Case G_3

The order of group suggests that there is a relation between the lattice and the rank 4 lattice for $\mathbb{Z}B_4$. The group is generated by

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 \\ -1 & 0 & -1 & 0 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ -1 & -1 & 0 & -1 & 0 \end{bmatrix}.$$

The dual group is generated by

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

By applying algorithm(1) we get the change of basis matrix

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & -1 \end{bmatrix}$$

Now changing the basis and dualizing gives us the group

$$\left[\begin{array}{cccc|c} 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 1 & 1 & 0 & 1 \end{array}\right] \text{ and } \left[\begin{array}{cccc|c} 0 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 & 1 \end{array}\right]$$

This yields the following exact sequence of lattices

$$0 \longrightarrow M \longrightarrow L_{G_3} \longrightarrow \mathbb{Z} \longrightarrow 0$$

where M corresponds to H generated by

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

GAP ID for the above group is

```
gap> G3info:= Rank1PermQuot(G3);;
gap> G3info.ZClassSubLat;
[ 4, 32, 21, 1 ]
```

In [23] the author has proved the corresponding lattice to [4, 32, 21, 1] is $\mathbb{Z}B_4$ which is hereditarily rational. This proves that T_{G_3} is hereditarily rational.

Alternatively one can see from the above generators of H, that M is a sign permutation lattice which is hereditarily rational.

3.3.4 Case G_4

The group is generated by

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

The dual group is generated by

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

Algorithm (2) produces the change of basis matrix

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & -1 & -1 & 2 \end{bmatrix}$$

With the above transformation we can see the new representative for G_4 is generated by

$$\left[\begin{array}{cccc|c} 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 \end{array}\right] \text{ and } \left[\begin{array}{cccc|c} -1 & 1 & 0 & 1 & 0 \\ -1 & 0 & -1 & -1 & 0 \\ 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & -1 & -1 \end{array}\right]$$

Now by considering M_{G_4} to be the corresponding lattice to

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

we can produce

$$0 \longrightarrow M_{G_4} \longrightarrow L_{G_4} \longrightarrow \mathbb{Z}^- \longrightarrow 0.$$

M_{G_4} corresponds to [4,31,7,1]. The generators of [4,31,7,1] are

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 \\ 1 & 0 & 0 & -1 \\ 1 & -1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & -1 \\ -1 & 0 & 1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}$$

The generators of the dual group are

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 1 & 1 & 1 & 1 \\ -1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix}$$

$e := [1, 0, 0, 0]$

$$e \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \end{bmatrix} = [1, 1, 1, 1]$$

$$e\begin{bmatrix} 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 1 & 1 & 1 & 1 \\ -1 & 0 & 0 & 0 \end{bmatrix} = [0,-1,0,0]$$

$$e\begin{bmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix} = [0,0,-1,0]$$

```
gap> H:= GDual(MatGroupZClass(4,31,7,1));;
gap> S:= Stabilizer(H,e);
<matrix group with 15 generators>
gap> StructureDescription(S);
"S4"
gap> n:= [0,0,0,0];
[ 0, 0, 0, 0 ]
gap> for h in H do n:= n + e*h; od; n;
[ 0, 0, 0, 0 ]
```

which shows M is the Chevalley module J_{S_5/S_4}, thus its dual lattice is hereditarily rational. However, since L_{G_4}/M_{G_4} is sign permutation, we can not conclude rationality of G_4.

3.3.5 Case G_5

The group is generated by

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

The generators of the group corresponding to the dual lattice are

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

Algorithm (2) produces the change of basis matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & -1 & 0 \end{bmatrix}$$

With the above transformation we can see the new generators for G_4 are given by

$$\left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 \end{array}\right], \left[\begin{array}{cccc|c} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ \hline 0 & 0 & -1 & -1 & 1 \end{array}\right] \text{ and } \left[\begin{array}{cccc|c} -1 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 & -1 \end{array}\right]$$

Now by considering M_{G_5} to be the lattice corresponding to the grouop generated by

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{bmatrix}\begin{bmatrix} -1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

we can produce

$$0 \longrightarrow M_{G_5} \longrightarrow L_{G_5} \longrightarrow \mathbb{Z}^- \longrightarrow 0.$$

The corresponding group to M_{G_5} has GAP ID [4,29,9,2].

3.3.6 Case G_6

The group is generated by

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

The group corresponding to the dual lattice is generated by

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

Algorithm (2) produces the change of basis matrix

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & -1 \end{bmatrix}$$

With the above transformation we can see the new generators for G_6 are given by

$$\left[\begin{array}{cccc|c} 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 \end{array}\right] \left[\begin{array}{cccc|c} 0 & -1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & -1 \end{array}\right] \text{ and } \left[\begin{array}{cccc|c} -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ \hline 1 & 0 & 0 & 0 & 1 \end{array}\right]$$

Now by considering M_{G_6} to be the corresponding lattice to , H, generated by

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

we can produce

$$0 \longrightarrow M_{G_6} \longrightarrow L_{G_6} \longrightarrow \mathbb{Z}^- \longrightarrow 0.$$

M_{G_6} is a sign permutation lattice and therefore hereditarily rational. However, since L_{G_6}/M_{G_6} is sign permutation, we can not conclude rationality of G_6.

3.3.7 Case G_7

The group is generated by

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

The group corresponding to the dual lattice is generated by

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

Algorithm (1) produces the change of basis matrix

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & -1 & -1 & 2 \end{bmatrix}$$

With the above transformation we can see the new representative for G_7 is generated by

$$\left[\begin{array}{cccc|c} 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 \end{array}\right] \text{ and } \left[\begin{array}{cccc|c} 0 & 0 & 1 & 1 & 0 \\ 0 & -1 & 0 & -1 & 0 \\ -1 & -1 & -2 & -2 & 0 \\ 0 & 2 & 1 & 2 & 0 \\ \hline 0 & -1 & -1 & -1 & 1 \end{array}\right]$$

Now by considering M_{G_7} to be the corresponding lattice to the group generated by

$$\begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & -1 & 0 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & -1 & 0 & -1 \\ -1 & -1 & -2 & -2 \\ 0 & 2 & 1 & 2 \end{bmatrix}$$

we can produce

$$0 \longrightarrow M_{G_7} \longrightarrow L_{G_7} \longrightarrow \mathbb{Z} \longrightarrow 0.$$

On the other hand the GAP ID of M_{G_7} is given as

```
gap> G7info:= Rank1PermQuot(G7);;
gap> G7info.ZClassSubLat;
[ 4, 31, 4, 1 ]
```

The dual of [4,31,4,1], H, is isomorphic to S_5 and can be generated by

$$\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ -1 & -1 & -1 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & 1 \\ -1 & -1 & -1 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

For $e_1 = [1\ 0\ 0\ 0]$,

$$e_1 \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ -1 & -1 & -1 & -1 \end{bmatrix} = [0\ 0\ 1\ 0]$$

$$e_1 \begin{bmatrix} 0 & 0 & 0 & 1 \\ -1 & -1 & -1 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} = [0\ 0\ 0\ 1]$$

$$e_1 \begin{bmatrix} 0 & 0 & 0 & 1 \\ -1 & -1 & -1 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ -1 & -1 & -1 & -1 \end{bmatrix} = [-1\ -1\ -1\ -1]$$

The stabilizer subgroup of e_1 in H can be calculated as

```
 gap> S:= Stabilizer(H,e);
<matrix group with 7 generators>
gap> StructureDescription(S);
"S4"
```

Moreover,

```
 gap> n:= [0,0,0,0];
[ 0, 0, 0, 0 ]
gap> for h in H do n:= n + e*h; od; n;
[ 0, 0, 0, 0 ]
```

which shows the corresponding lattice to H is the Chevalley module J_{S_5/S_4} Alternatively in [23] the author has proved that [4,31,7,1] is hereditarily rational. Using GAP we can verify that [4,31,4,1] (up to conjugacy) is a subgroup of [4,31,7,1]. This proves rationality of T_{G_7}.

3.3.8 Cases G_8, G_9 and G_{10}

It is well known that a representation ρ is absolutely irreducible if and only if $\langle \chi_\rho, \chi_\rho \rangle = 1$ where χ_ρ is the corresponding character to ρ. Since the groups are of small order, 120, we can test if $\langle \chi_\rho, \chi_\rho \rangle$ is one or not. We recall

$$\langle \chi_\rho, \chi_\rho \rangle = \frac{1}{n} \sum_{\sigma \in G} (tr(\sigma)^2)$$

where $G \leq \mathrm{GL}(n, \mathbb{Q})$ and $|G| = n$.

```
gap> n:= 0;
0
```

```
gap> for g in AsList(G8) do
> n:= n+ (1/Size(G8))*Trace(g)^2;
> od;
gap> n;
1

gap> n:= 0;
0
gap> for g in AsList(G9) do
> n:= n+ (1/Size(G9)) *Trace(g)^2;
> od;
gap> n;
1

gap> n:= 0;
0
gap> for g in AsList(G10) do
> n:= n+ (1/Size(G10))*Trace(g)^2;
> od;
gap> n;
1
```

Since all 3 groups are irreducible, we consider their maximal subgroups up to conjugacy and check if their maximal subgroups are reducible. In case that a maximal subgroup is irreducible we consider its maximal subgroups again and continue this process.

Figures 3.1, 3.2 and 3.3 respectively present lattices of subgroups of G_8, G_9 and G_{10}. These are not the complete lattices of the mentioned groups. We just considered the lattices up to the level where algorithm one returns an output. Appendix (a) is devoted to show that the shaded groups are hereditarily rational.

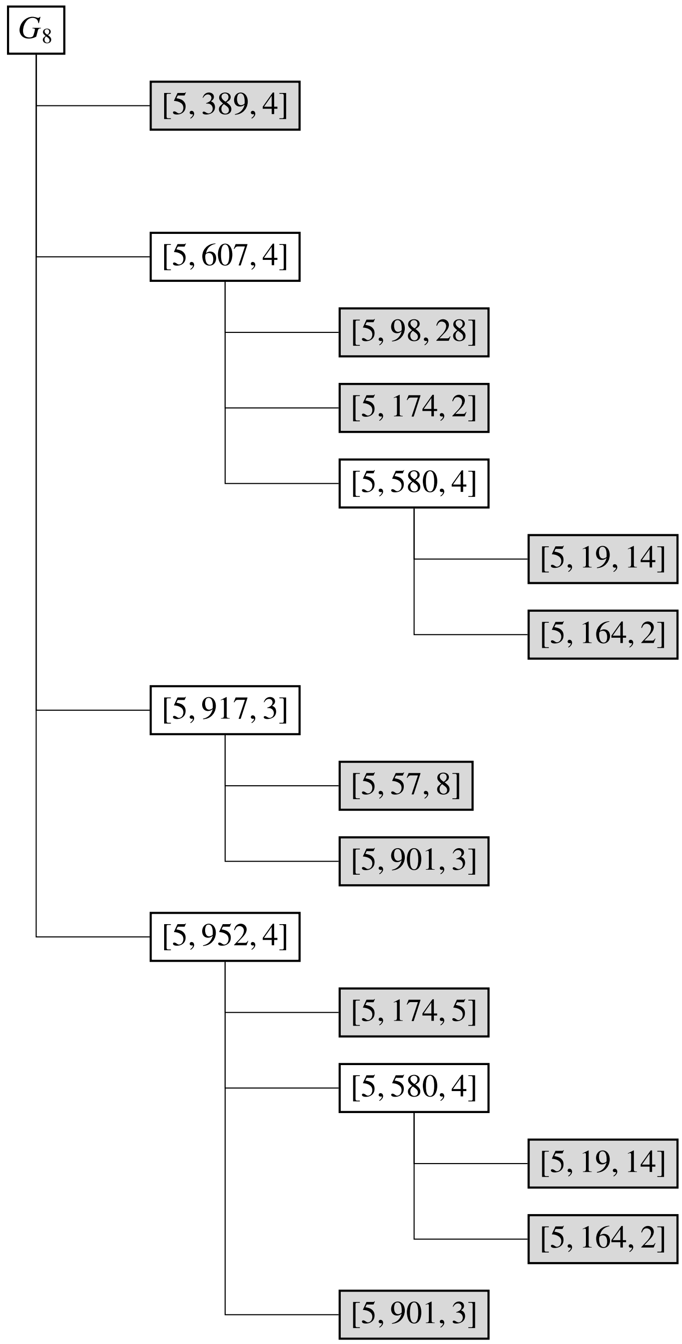


Figure 3.1: Conjugacy classes of subgroups of G_8. Algorithm (1) works for the gray ones.

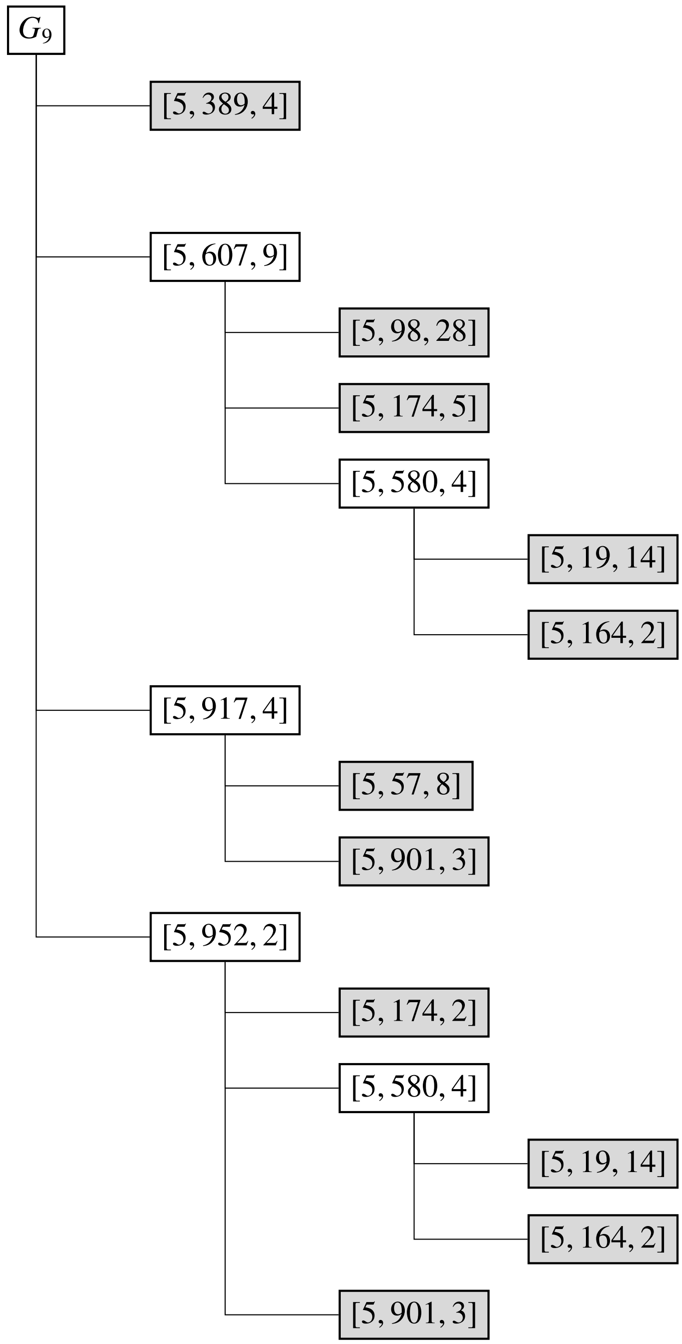


Figure 3.2: Conjugacy classes of subgroups of G_9. Algorithm (1) works for the gray ones.

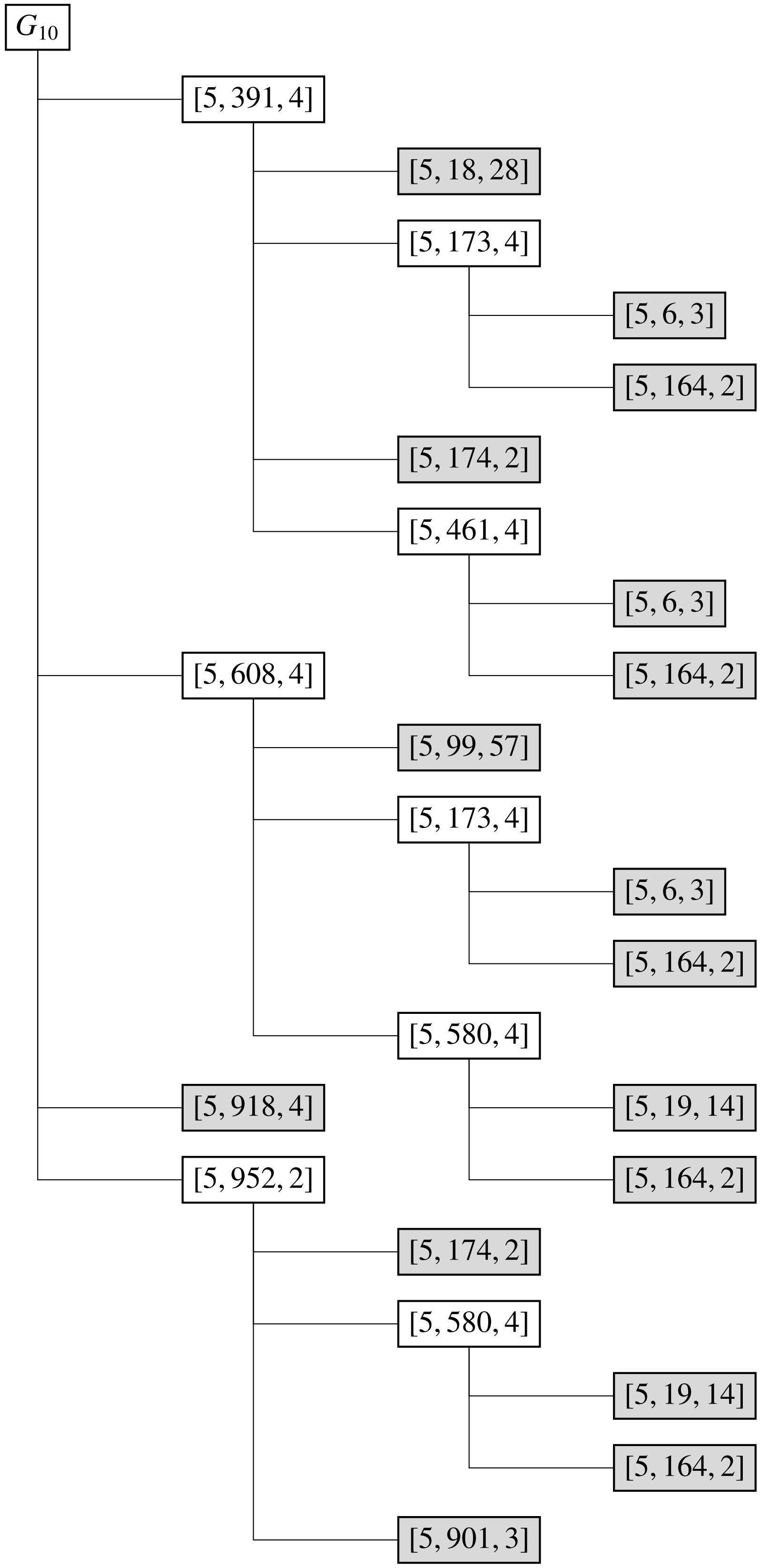


Figure 3.3: Conjugacy classes of subgroups of G_{10}. Algorithm (1) works for the gray ones.

3.3.9 Case G_{11}

The group is generated by

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

The dual group is generated by

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

Algorithm (2) produces the change of basis matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & -1 & -2 & -2 & 2 \end{bmatrix}$$

With the above transformation we can see a new representative for G_{11} is generated by

$$\left[\begin{array}{cccc|c} -1 & -1 & -1 & -1 & 0 \\ 0 & 2 & 1 & 2 & 0 \\ 0 & 1 & 2 & 2 & 0 \\ 0 & -2 & -2 & -3 & 0 \\ \hline 0 & 1 & 1 & 1 & -1 \end{array}\right] \left[\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ \hline 0 & 0 & 0 & 0 & -1 \end{array}\right] \text{ and } \left[\begin{array}{cccc|c} -1 & 0 & 0 & 0 & 0 \\ 2 & 0 & 2 & 1 & 0 \\ 2 & 1 & 2 & 2 & 0 \\ -2 & 0 & -3 & -2 & 0 \\ \hline 1 & 0 & 1 & 1 & 1 \end{array}\right]$$

Now by considering $M_{G_{11}}$ to be the corresponding lattice to the group H generated by

$$\begin{bmatrix} -1 & -1 & -1 & -1 \\ 0 & 2 & 1 & 2 \\ 0 & 1 & 2 & 2 \\ 0 & -2 & -2 & -3 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \text{ and } \begin{bmatrix} -1 & 0 & 0 & 0 \\ 2 & 0 & 2 & 1 \\ 2 & 1 & 2 & 2 \\ -2 & 0 & -3 & -2 \end{bmatrix}$$

we can produce

$$0 \longrightarrow M_{G_{11}} \longrightarrow L_{G_{11}} \longrightarrow \mathbb{Z}^- \longrightarrow 0.$$

H GAP ID is [4,20,20,4]. A generating set for [4,20,20,4] is given by

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

As we can see its corresponding lattice decompose into 2 rank two lattices which are hereditarily rational.

3.3.10 Case G_{12}

The group is isomorphic to $D_8 \times S_4$ and is generated by

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & -1 & 0 & -1 \\ 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & -1 & -1 & -1 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \end{bmatrix}.$$

Its dual is generated by

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

Algorithm(1) provides the matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & -1 & -2 & -2 & 2 \end{bmatrix}$$

as our desired change of basis which gives us a new representative for the conjugacy class of G_{12}, namely the group generated by

$$\left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 \\ 0 & 2 & 1 & 2 & 0 \\ 0 & -3 & 0 & -2 & 0 \\ \hline 0 & 1 & 0 & 1 & 1 \end{array}\right] \left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 0 \\ -2 & -1 & -2 & -2 & 0 \\ -2 & -2 & -1 & -2 & 0 \\ 2 & 2 & 2 & 3 & 0 \\ \hline -1 & -1 & -1 & -1 & 1 \end{array}\right] \text{ and } \left[\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 0 \\ 0 & -2 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 2 & -1 & 0 & 0 \\ \hline 0 & -1 & 0 & 0 & 1 \end{array}\right]$$

Now we can define $M_{G_{12}}$ to be the corresponding lattice to the group generated by

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 2 & 1 & 2 \\ 0 & -3 & 0 & -2 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ -2 & -1 & -2 & -2 \\ -2 & -2 & -1 & -2 \\ 2 & 2 & 2 & 3 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & -2 & 0 & -1 \\ 0 & -1 & 0 & 0 \\ 0 & 2 & -1 & 0 \end{bmatrix}$$

we get the following exact sequence for $L_{G_{12}}$

$$0 \longrightarrow M_{G_{12}} \longrightarrow L_{G_{12}} \longrightarrow \mathbb{Z} \longrightarrow 0$$

The ZClass of $M_{G_{12}}$ is given by GAP as

```
gap> G12info:= Rank1PermQuot(G12);;
gap> G12info.ZClassSubLat;
[ 4, 20, 17, 2 ]
```

A generating set of [4,20,17,2] is given by

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & -1 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

and its corresponding lattice is decomposable to rank 2 lattices which we know their rationality. Thus, $M_{G_{12}}$ is hereditarily rational and this implies that $T_{G_{12}}$ is hereditarily rational.

3.3.11 Case G_{13}

A generating set of G_{13} is

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 1 \\ 0 & -1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & 1 & 0 & 1 & -1 \\ 0 & -1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 1 \\ 0 & -2 & 0 & 0 & 1 \end{bmatrix}$$

The dual group is generated by

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 1 & -1 & -1 & -1 & -2 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

By algorithm (1) we have the following transformation matrix

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix}$$

which provides the new generators of the representative of the conjugacy class of G_{13} as

$$\left[\begin{array}{cccc|c} 0 & -1 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 \end{array}\right] \text{ and } \left[\begin{array}{cccc|c} -1 & 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ -2 & 0 & -1 & 2 & 0 \\ -2 & 0 & 0 & 1 & 0 \\ \hline 1 & 0 & 1 & -1 & 1 \end{array}\right]$$

Now by defining $M_{G_{13}}$ to be the corresponding lattice to the group generated by

$$\begin{bmatrix} 0 & -1 & 0 & 1 \\ -1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} -1 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ -2 & 0 & -1 & 2 \\ -2 & 0 & 0 & 1 \end{bmatrix}$$

we can get

$$0 \longrightarrow M_{G_{13}} \longrightarrow L_{G_{13}} \longrightarrow \mathbb{Z} \longrightarrow 0.$$

On the other hand GAP returns the GAP ID of $M_{G_{13}}$ as

```
gap> G13info:= Rank1PermQuot(G13);;
gap> G13info.ZClassSubLat;
[ 4, 25, 9, 2 ]
```

In [23] the author has proved that [4,25,9,2] is hereditarily rational which means $T_{G_{13}}$ is hereditarily rational.

3.3.12 Case G_{14}

A generating set of G_{14} is

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

The dual group is generated by

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

By algorithm (1) we have the following transformation matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & -1 & 1 & 1 \end{bmatrix}$$

which provides the new representative of the conjugacy class of G_{14} as

$$\left[\begin{array}{cccc|c} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ -1 & 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & -1 & 0 \\ \hline 1 & 0 & 1 & 1 & 1 \end{array}\right] \text{ and } \left[\begin{array}{cccc|c} 0 & 1 & 1 & 1 & 0 \\ -1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ \hline 0 & 0 & 1 & 1 & 1 \end{array}\right]$$

Now by defining $M_{G_{14}}$ to be the corresponding lattice to the group generated by

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

we can get

$$0 \longrightarrow M_{G_{14}} \longrightarrow L_{G_{14}} \longrightarrow \mathbb{Z} \longrightarrow 0.$$

On the other hand GAP returns the GAP ID of $M_{G_{14}}$ as

```
gap> G14info:= Rank1PermQuot(G14);;
gap> G14info.ZClassSubLat;
[ 4, 25, 8, 5 ]
```

In [23] it is shown that the subgroups of [4,25,8,5] are rational except for possibly 8 subgroups

$[4,6,2,11], [4,12,4,13], [4,13,2,6], [4,13,3,6], [4,13,7,12], [4,24,4,6], [4,25,4,5], [4,25,8,5].$

Each of the above groups corresponds to a subgroup of G_{14} and except for them, the rest are rational.

3.3.13 Case G_{15}

The group G_{15} is isomorphic to $C_2 \times S_4$ and is generated by

$$\begin{bmatrix} 0 & 0 & -1 & 0 & 1 \\ -1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & -1 \\ 0 & 0 & -1 & 0 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} -1 & 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 \\ 1 & -1 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

This is the G-lattice discussed in Example 3. So the information is being recalled from that example.

$$T = \begin{bmatrix} 1 & 0 & 1 & 0 & -1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

which provides a new representative of the conjugacy class of G_{15} as the group generated by

$$\left[\begin{array}{ccc|cc} 0 & 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ \hline 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & -1 & 0 \end{array}\right] \text{ and } \left[\begin{array}{ccc|cc} 0 & 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & 1 & -1 \end{array}\right].$$

Now we can define $M = \langle e_1, e_2, e_3 \rangle_{\mathbb{Z}} \subset L_{G_{15}}$ to get

$$0 \longrightarrow M \longrightarrow L_{G_{15}} \longrightarrow L/M \longrightarrow 0.$$

One can see that L/M is a rank 2 lattice which is the corresponding lattice to the group, H generated by

$$\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}.$$

H is isomorphic to S_3 and its corresponding lattice is not even sign permutation. We can consider maximal subgroups of G_{15} as we did for the irreducible lattices.

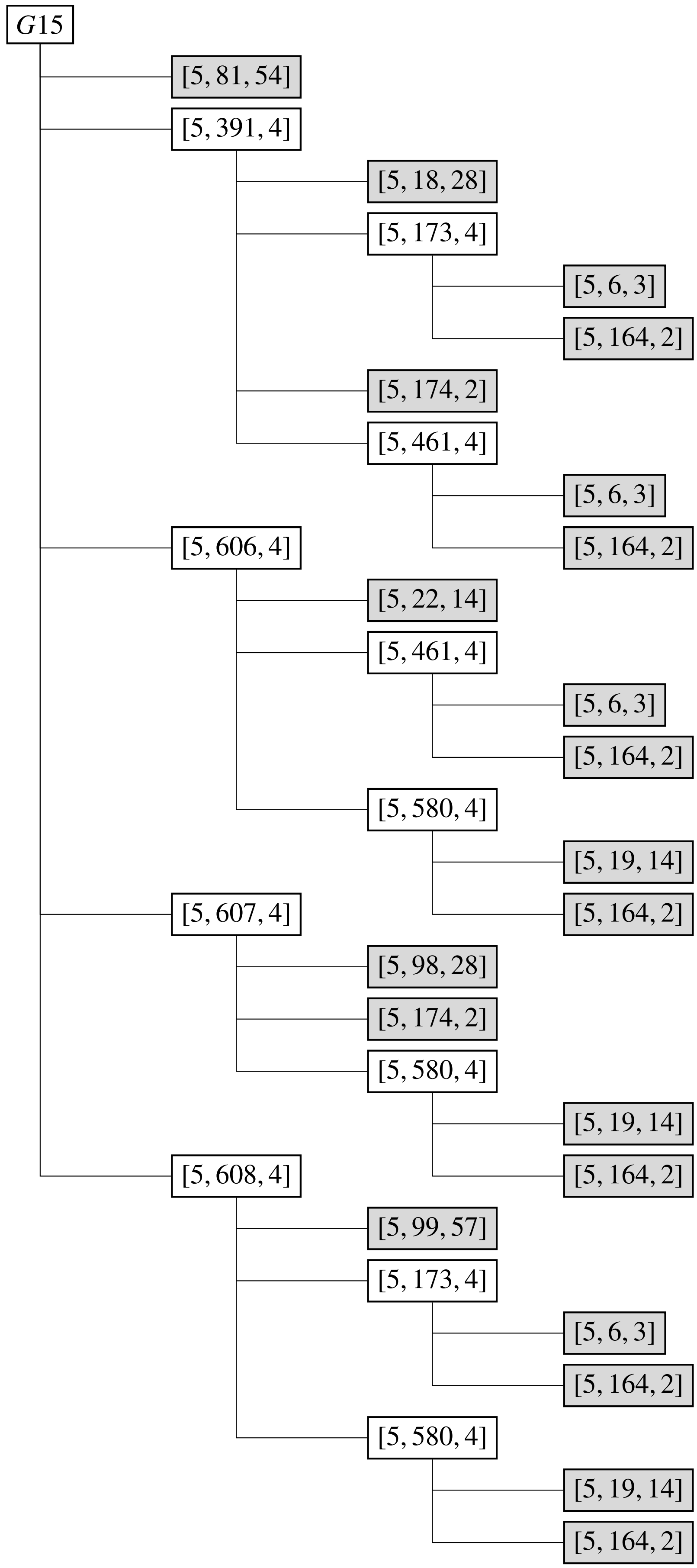


Figure 3.4: Conjugacy classes of subgroups of G_{15}. Algorithm (1) works for the gray ones.

3.3.14 Case G_{16}.

A generating set of G_{16} is

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

The dual group is generated by

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

By algorithm (1) we have the following transformation matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

which provides the new generators of the representative of the conjugacy class of G_{16} as

$$\left[\begin{array}{cccc|c} 1 & -1 & -1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ \hline 0 & -1 & -1 & 1 & 1 \end{array}\right] \left[\begin{array}{cccc|c} 1 & -1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & -1 & -1 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ \hline 0 & -1 & -1 & 0 & 1 \end{array}\right] \text{ and } \left[\begin{array}{cccc|c} -1 & 0 & 1 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

Now by defining $M_{G_{16}}$ to be the corresponding lattice to the group generated by

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

we can get

$$0 \longrightarrow M_{G_{16}} \longrightarrow L_{G_{16}} \longrightarrow \mathbb{Z} \longrightarrow 0.$$

On the other hand GAP returns the GAP ID of $M_{G_{16}}$ as

```
gap> G16info:= Rank1PermQuot(G16);;
gap> G16info.ZClassSubLat;
[ 4, 14, 10, 2 ]
```

In [23] it is shown that [4, 31, 7, 1] is hereditarily rational. Using GAP one can verify that [4,14,10,2] (up to conjugacy) is a subgroup of [4,31,7,1] which means $T_{G_{16}}$ is hereditarily rational.

3.3.15 Case G_{17}

A generating set of G_{17} is

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

The dual group is generated by

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

By algorithm (1) we have the following transformation matrix

$$\begin{bmatrix} 1 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

which provides the new generators of the representative of the conjugacy class of G_{17} as

$$\left[\begin{array}{cccc|c} 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ \hline -1 & 0 & -1 & 0 & 1 \end{array}\right] \left[\begin{array}{cccc|c} -2 & 0 & 0 & -1 & 0 \\ 1 & -1 & 0 & 1 & 0 \\ 1 & 0 & -1 & 1 & 0 \\ 3 & 0 & 0 & 2 & 0 \\ \hline -3 & 0 & 0 & -1 & 1 \end{array}\right] \text{ and } \left[\begin{array}{cccc|c} 1 & 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 \\ 0 & -3 & 0 & 1 & 0 \\ \hline 0 & 2 & 0 & 0 & 1 \end{array}\right]$$

Now by defining $M_{G_{17}}$ to be the corresponding lattice to the group generated by

$$\begin{bmatrix} 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} -2 & 0 & 0 & -1 \\ 1 & -1 & 0 & 1 \\ 1 & 0 & -1 & 1 \\ 3 & 0 & 0 & 2 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & -3 & 0 & 1 \end{bmatrix}$$

we can get

$$0 \longrightarrow M_{G_{17}} \longrightarrow L_{G_{17}} \longrightarrow \mathbb{Z} \longrightarrow 0.$$

On the other hand GAP returns the GAP ID of $M_{G_{17}}$ as

```
gap> G17info:= Rank1PermQuot(G17);;
gap> G17info.ZClassSubLat;
[ 4, 13, 7, 12 ]
```

In [23] it is shown that the subgroups of [4,13,7,12] are rational except for possibly 5 subgroups

$$[4,6,2,11], [4,12,4,13], [4,13,2,6], [4,13,3,6], [4,13,7,12]$$

Each of the above groups corresponds to a subgroup of G_{17} and except for them, the rest are rational.

3.3.16 Case G_{18}

A generating set of G_{18} is

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

The dual group is generated by

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

By algorithm (1) we have the following transformation matrix

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & -1 & 1 & -1 \end{bmatrix}$$

which provides the new generators of the representative of the conjugacy class of G_{18} as

$$\left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 \end{array}\right] \left[\begin{array}{cccc|c} 0 & -1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 1 & -1 & -1 & 0 & 0 \\ -1 & 1 & 0 & -1 & 0 \\ \hline -1 & 1 & 1 & -1 & 1 \end{array}\right] \text{ and } \left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 \\ \hline 0 & -1 & 0 & 0 & 1 \end{array}\right]$$

Now by defining $M_{G_{18}}$ to be the corresponding lattice to the group generated by

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 1 & -1 & -1 & 0 \\ -1 & 1 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{bmatrix}$$

we can get

$$0 \longrightarrow M_{G_{18}} \longrightarrow L_{G_{18}} \longrightarrow \mathbb{Z} \longrightarrow 0.$$

On the other hand GAP returns the GAP ID of $M_{G_{18}}$ as

```
gap> G18info:= Rank1PermQuot(G18);;
gap> G18info.ZClassSubLat;
[ 4, 13, 7, 12 ]
```

In [23] it is shown that the subgroups of [4,13,7,12] are rational except for possibly 5 subgroups

$$[4, 6, 2, 11], [4, 12, 4, 13], [4, 13, 2, 6], [4, 13, 3, 6], [4, 13, 7, 12]$$

Each of the above groups corresponds to a subgroup of G_{18} and except for them, the rest are rational.

3.3.17 Conclusion

The 18 maximal indecomposable stably rational lattices found in [15] are divided into 4 families. The first family are the ones interpreted as lattices of root systems which are hereditarily rational. The second family contains all lattices on which Algorithm 1 will not fail. The third family contains lattices on which Algorithm 2 does not fail while Algorithm 1 fails. The last family contains all lattices on which either, both Algorithms 1 and 2 fail but still the general idea of reduction works, or they are irreducible.

All lattices of the first family are hereditarily rational. The second family contains lattices of which after reduction, rationality of the reduced component is unknown. By arguments in the previous sections we have proved the following theorem.

Theorem 4. *The groups presented in Table 3.3 are hereditarily rational.*

CARAT ID	Group Structure	#G	Description.
$(5,942,1)$	$\mathrm{Imf}(5,1,1)$	3840	The root lattice of B_5
$(5,953,4)$	S_6	720	The root lattice of A_5
$(5,726,4)$	$C_2^4 \rtimes S_4$	384	reduced component $[4,32,21,1]$
$(5,911,4)$	S_5	120	reduced component $[4,31,4,1]$
$(5,341,6)$	$D_8 \times S_3$	48	reduced component $[4,20,17,2]$
$(5,531,13)$	$C_2 \times S_4$	48	reduced component $[4,25,9,2]$
$(5,245,12)$	$C_2^2 \times S_3$	24	reduced component $[4,14,10,2]$

Table 3.3: Hereditarily rational groups among the maximal 18 groups found in [15].

The exceptional cases of the second family are presented in Table 3.4. In each case the reduced component is stably rational as proved in [15]. Their rationality is unknown yet. In [23] the author has proved that subgroups of $[4,25,8,5]$ are rational except for possibly

$$[4,6,2,11], [4,12,4,13], [4,13,2,6], [4,13,3,6], [4,13,7,12], [4,24,4,6], [4,25,4,5], [4,25,8,5].$$

There will be precisely one subgroup of G_{14} with each of the dimension 4 reduced components in the above list, so except for possibly those subgroups of G_{14} the rest are rational. The exceptional cases are presented in Table 3.5.

From the above list

$$[4,6,2,11], [4,12,4,13], [4,13,2,6], [4,13,3,6], [4,13,7,12]$$

are subgroups of $[4,13,7,12]$ which means we have the same problem for cases G_{17} and G_{18}. Hence except for possibly the subgroups of G_{17} and G_{18} associated to above list their rest of subgroups are rational. For the exceptional cases see Table 3.6 and Table 3.7.

CARAT ID	Group Structure	#G	Description.
$(5,533,8)$	$C_2 \times S_4$	48	reduced component $[4,25,8,5]$
$(5,81,42)$	$C_2 \times D_8$	16	reduced component $[4,13,7,12]$
$(5,81,48)$	$C_2 \times D_8$	16	reduced component $[4,13,7,12]$

Table 3.4: Groups among 18 maximals which are reduced but rationality of rank 4 sublattice is unknown

CARAT ID	Group Structure	#G	Description.
$(5,32,52)$	$C_2 \times C_2 \times C_2$	8	reduced component [4, 6, 2, 11]
$(5,99,53)$	D_8	8	reduced component [4, 12, 4, 13]
$(5,103,22)$	$C_4 \times C_2$	8	reduced component [4, 13, 2, 6]
$(5,98,22)$	D_8	8	reduced component [4, 13, 3, 6]
$(5,81,50)$	$C_2 \times D_8$	16	reduced component [4, 13, 7, 12]
$(5,522,15)$	S_4	24	reduced component [4, 24, 4, 6]
$(5,521,15)$	S_4	24	reduced component [4, 25, 4, 5]
$(5,533,8)$	$C_2 \times S_4$	48	reduced component [4, 25, 8, 5]

Table 3.5: Subgroups of G_{14} that have associated tori which are stably rational but whose rationality is unknown.

CARAT ID	Group Structure	#G	Description.
$(5,32,49)$	$C_2 \times C_2 \times C_2$	8	reduced component [4, 6, 2, 11]
$(5,99,52)$	D_8	8	reduced component [4, 12, 4, 13]
$(5,103,16)$	$C_4 \times C_2$	8	reduced component [4, 13, 2, 6]
$(5,98,16)$	D_8	8	reduced component [4, 13, 3, 6]
$(5,81,42)$	$C_2 \times D_8$	16	reduced component [4, 13, 7, 12]

Table 3.6: Subgroups of G_{17} that have associated tori which are stably rational but whose rationality is unknown.

CARAT ID	Group Structure	#G	Description.
$(5,32,46)$	$C_2 \times C_2 \times C_2$	8	reduced component [4, 6, 2, 11]
$(5,99,54)$	D_8	8	reduced component [4, 12, 4, 13]
$(5,103,24)$	$C_4 \times C_2$	8	reduced component [4, 13, 2, 6]
$(5,98,24)$	D_8	8	reduced component [4, 13, 3, 6]
$(5,81,48)$	$C_2 \times D_8$	16	reduced component [4, 13, 7, 12]

Table 3.7: Subgroups of G_{18} that have associated tori which are stably rational but whose rationality is unknown.

Theorem 5. *All subgroups of G_{14}, G_{17} and G_{18} are rational except for possibly the subgroups in Table 3.5, Table 3.6 and Table 3.7.*

There are 4 cases, namely G_4, G_5, G_6 and G_{11}, in which after the reduction we get a rank one sign permutation lattice (more information is given in Table 3.8). The same also happened in some subgroups of irreducible lattices (see Table 3.9). It is possible that these groups are hereditarily rational, but we do not currently have a proof. One possible approach to prove rationality in these cases may be the following argument.

Assume L is a lattice in the third family, that is, there exists an exact sequence of lattices such that

$$0 \longrightarrow M \longrightarrow L \longrightarrow \mathbb{Z}^{-} \longrightarrow 0$$

Moreover assume M is a hereditarily rational. Using a flasque resolution of L we have

$$\begin{array}{ccccccccc} & & & & 0 & & & & \\ & & & & \downarrow & & & & \\ 0 & \longrightarrow & M & \longrightarrow & L & \longrightarrow & \mathbb{Z}^{-} & \longrightarrow & 0 \\ & & & & \downarrow & & & & \\ & & & & P & & & & \\ & & & & \downarrow & & & & \\ & & & & Q & & & & \\ & & & & \downarrow & & & & \\ & & & & 0 & & & & \end{array}$$

Suppose K/F is a finite Galois extension and $G = \mathrm{Gal}(K/F)$. We note that by the No Name Lemma we obtain $K(P)^G = K(y_1, \ldots, y_t)$ and $K(M)^G = F(x_1, \ldots, x_{n-1})$ is implied by rationality of M. Now if there exist a permutation lattice Q' such that $P \subset M \oplus Q'$ (or even if $L \subset M \oplus Q'$) then $K(L)^G \subset K(M)(Q')^G$ which implies unirationality of $K(L)^G$ over $K(M)^G$. Now Lüroth's theorem implies rationality of $K(L)^G$ over F.

$$\begin{array}{c} K(M \oplus Q')^G = K(M)^G(z_1, \ldots, z_s) \\ | \\ K(P)^G = K(y_1, \ldots, y_t) \\ | \\ K(L)^G = K(M)(\mathbb{Z}^{-})^G \\ | \\ K(M)^G = F(x_1, \ldots, x_{n-1}) \\ | \\ F \end{array}$$

The following table summarizes the information about reduction of lattices in the third family.

CARAT ID	G	$\#G$	Description.
$(5,919,4)$	$C_2 \times S_5$	240	reduced component $[4,31,7,1]$
$(5,801,3)$	$C_2 \times (S_3^2 \rtimes C_2)$	144	reduced component $[4,29,9,2]$
$(5,655,4)$	$D_8^2 \rtimes C_2$	128	reduced component $[4,32,17,1]$
$(5,337,12)$	$D_8 \times S_3$	48	reduced component $[4,20,20,4]$

Table 3.8: The groups corresponding to maximal stably rational tori of dimension 5 whose associated lattices are indecomposable and have a rank 1 sign quotient.

For the last family we have considered their maximal subgroups and we could not decide about the rationality of the groups presented in the following table.

Theorem 6. *All groups in Table 3.10 are hereditarily rational. That is, all subgroups of* G_8*,* G_9*,* G_{10} *and* G_{15} *except for possibly the subgroups in Table 3.9 are hereditarily rational.*

A proof of Theorem 6 is provided in Appendix A.

Carat ID	G	$\#G$	Description
$[5,173,4]$	S_3	6	reduced comp. $[4,17,1,1]$, rank 1 sign perm. quot.
$[5,391,4]$	D_{12}	12	reduced comp. $[4,21,3,1]$ rank 1 sign perm. quot.
$[5,461,4]$	$C_2^2 \times S_3$	24	reduced comp.$[3,6,7,1]$, quot $[2,4,4,1]$
$[5,580,4]$	A_4	12	reduced comp.$[3,7,1,1]$, quot $[2,4,1,1]$
$[5,606,4]$	$C_2 \times A_4$	24	reduced comp. $[3,7,2,1]$, quot $[2,4,1,1]$
$[5,607,4]$	S_4	24	reduced comp. $[3,7,4,1]$, quot $[2,4,2,1]$
$[5,607,9]$	S_4	24	reduced comp. $[3,7,4,1]$, quot $[2,4,2,2]$
$[5,608,4]$	S_4	24	reduced comp.t $[3,7,3,1]$, quot $[2,4,2,1]$
$[5,917,3]$	$C_5 \rtimes C_4$	20	reduced comp. $[4,31,1,1]$ rank 1 sign perm. quot.
$[5,917,4]$	$C_5 \rtimes C_4$	20	reduced comp. $[4,31,1,1]$ rank 1 sign perm. quot.
$[5,623,4]$	$C_2 \times S_4$	48	reduced comp. $[3,7,5,1]$, quot $[2,4,2,1]$
$[5,952,2]$	A_5	60	absolutely irreducible
$[5,952,4]$	A_5	60	absolutely irreducible
$[5,946,2]$	S_5	120	absolutely irreducible
$[5,946,4]$	S_5	120	absolutely irreducible
$[5,947,2]$	S_5	120	absolutely irreducible

Table 3.9: Subgroups of G_8, G_9, G_{10} and G_{15} that have associated tori which are stably rational but whose rationality is unknown.

The following table present the reduced components of the subgroups mentioned in Theorem 6.

Number	CARAT ID	G	$\#G$	Description.
1	$[5,6,3]$	C_2	2	[4, 2, 2, 2]
2	$[5,18,28]$	$C_2 \times C_2$	4	[4, 4, 3, 4]
3	$[5,19,14]$	$C_2 \times C_2$	4	[4, 5, 1, 10]
4	$[5,22,14]$	$C_2 \times C_2 \times C_2$	8	[4, 6, 1, 9]
5	$[5,57,8]$	C_4	4	[4, 7, 1, 2]
6	$[5,81,54]$	$C_2 \times D_8$	16	[4, 13, 7, 5]
7	$[5,98,28]$	D_8	8	[4, 13, 3, 3]
8	$[5,99,57]$	D_8	8	[4, 12, 4, 7]
9	$[5,164,2]$	C_3	3	[4, 11, 1, 1]
10	$[5,174,2]$	S_3	6	[4, 17, 1, 3]
11	$[5,174,5]$	S_3	6	[4, 17, 1, 2]
12	$[5,389,4]$	D_{12}	12	[4, 21, 3, 2]
13	$[5,901,3]$	D_{10}	10	[4, 27, 3, 1]
14	$[5,918,4]$	$C_5 \rtimes C_4$	20	[4, 31, 1, 2]

Table 3.10: Hereditarily rational subgroups of G_8, G_9, G_{10} and G_{15}.

Remark. The union of the set of groups in Table 3.9 and the set of subgroups of the groups in Table 3.10, is the set of all subgroups of G_8, G_9, G_{10} and G_{15}.

Appendix B presents tables of conjugacy classes of indecomposable subgroups of $\mathrm{GL}(5,\mathbb{Z})$ which correspond to stably rational tori of dimension 5 from Hoshi and Yamasaki's list. From this list, those stably rational tori of dimension 5 whose rationality is unknown are listed.

Chapter 4

Algebraic Construction of Quasi-Split Tori

There are several applications of algebraic tori, for instance in cryptography and coding theory, see [28, Chapter 8], [19] and [36]. For practical purposes, the applications use split tori, that is $T = \mathbb{G}_m^d$ for some positive d. Split tori are used primarily due to the simplicity of calculations in this case. To make computations efficient and effective, one needs to be able to define coordinate rings and function fields of algebraic tori in an explicit manner.

As we saw in the second chapter, an algebraic torus is defined without using an ideal of a polynomial ring. Even the function field (resp. coordinate ring) of a general algebraic torus is defined as the field of invariants of a field (resp. ring of) under the action of some finite group. Considering the fact that these invariants are multiplicative, it is not easy to find these invariants in general. To the best of the author's knowledge, there are only a few algorithms for finding the multiplicative invariants (see [20] and [25]). The results presented in this chapter allow us to find multiplicative invariants in the particular cases where the lattice is permutation or sign permutation.

Indeed, in this chapter we present results concerning the construction of algebraic function field and coordinate ring of quasi split tori. The first section is devoted to a brief discussion of permutation lattices. In the second section, a constructive proof of the No Name Lemma is presented. This can be used to find an explicit transcendence basis of the rational function field of a quasi split torus. The final section presents a similar result for finding the function field of an algebraic torus with sign permutation lattice.

Throughout this chapter, for a given finite group $G \leq \mathrm{GL}(n, \mathbb{Z})$, L_G represents the lattice corresponding to G and T_G is the algebraic torus corresponding to G in the sense of Definition 46. $T_{G,F}$ denotes the algebraic torus associated to G, which is defined over a field F and splits over a Galois extension of F, K where $G = \mathrm{Gal}(K/F)$. Hence, G acts on $K(L_G) \cong K[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$

and $K(L_G) \cong K(x_1, \ldots, x_n)$ as in Definition 46.

4.1 Generalities

In this section, we briefly take a look at our main ingredients to present the results in the later sections. In order to give a concrete proof of the No Name Lemma, we will use a permutation basis of a given permutation lattice. Hence in the first subsection the problem of finding a permutation basis is discussed. A normal element of a given Galois extension is the other thing we will need. A brief discussion on normal element and normal basis of Galois extensions are provided.

4.1.1 Characterization of Permutation Lattices

In Chapter 2 we saw that for a given finite subgroup of $G \leq \mathrm{GL}(n, \mathbb{Z})$, the rational function field and the coordinate ring of $T_{G,F}$ are respectively given by $K(x_1, \ldots, x_n)^G$ and $K[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]^G$ (see Definition 46).

In general for a given G-lattice, we do not have a method to determine if the lattice is permutation or not. Let us take a closer look at the structure of permutation lattices to get some ideas.

The following lemma characterizes permutation lattices. Let $\mathbb{S}_n$ be the group generated by

$$\sigma = \left[\begin{array}{c|c} 0 & 1 \\ \hline I_{n-1} & 0 \end{array}\right] \text{ and } \tau = \left[\begin{array}{cc|c} 0 & 1 & \\ 1 & 0 & 0 \\ \hline \multicolumn{2}{c|}{0} & I_{n-2} \end{array}\right].$$

One can see $\mathbb{S}_n$ is the group of all permutation matrices.

Lemma 1. *Let $G \leq \mathrm{GL}(n, \mathbb{Z})$ be finite. The G-lattice corresponding to G is a permutation lattice if and only if G is conjugate to one of the subgroups of $\mathbb{S}_n$.*

Proof. ($\Rightarrow$) Assume that $G = \langle \sigma_i : 1 \leq i \leq m \rangle$ and that L_G has the standard basis $\{e_1, \ldots, e_n\}$. If L_G is a permutation lattice, then there exists a basis $W = \{\alpha_1, \ldots, \alpha_n\} \subset L_G$ such that G acts as permutation on W i.e. for any $\sigma \in G$ and $1 \leq i \leq n$

$$\alpha_i \cdot \sigma = \alpha_{s_i}$$

for some $s_i \in \{1, \ldots, n\}$. By defining $T = \begin{bmatrix} \alpha_1 & \cdots & \alpha_n \end{bmatrix}^t$, the above equations imply

$$T\sigma = P_\sigma T \text{ and thus } T\sigma T^{-1} = P_\sigma$$

where P_σ is a permutation matrix of size n. Note that since W forms a basis for L_G, T is invertible. The group P generated by $\{P_\sigma : \sigma \in \{\sigma_1, \ldots, \sigma_m\}\}$ is clearly a subgroup of $\mathbb{S}_n$ and

$TGT^{-1} = P$, which means that G and P are conjugate in $\mathrm{GL}(n, \mathbb{Z})$.
($\Leftarrow$) is obvious. □

The proof of the last lemma is simply saying that if a lattice is a permutation lattice then we can find an invertible matrix (change of basis matrix) such that TGT^{-1} is a subgroup of $\mathrm{GL}(n, \mathbb{Z})$ generated by permutation matrices.

However, to the best of the author's knowledge there is no general algorithm to determine if a given lattice is permutation. We mention here a naive approach, and where it fails.

For a given group $G \leq \mathrm{GL}(n, \mathbb{Z})$ with m generators one can always form a matrix T with n^2 indeterminates $x_{11}, \ldots, x_{nn}$ as entries, then form

$$\begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nn} \end{bmatrix} \sigma = P_\sigma \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nn} \end{bmatrix},$$

for σ a generator of G and P_σ the corresponding permutation matrix. This gives n^2 equations in n^2 variables. Since we can do the same for any generator of G, one can form a linear system of $m \times n^2$ equations with n^2 variables. We can always solve the system over rationals. If the system has no solution over $\mathbb{Q}$, it has no solutions over $\mathbb{Z}$ as well. However, there are two difficulties in this approach. The first problem is the choice of the permutation matrices P_σ, as it is not obvious how to choose appropriate candidates. The second problem happens when the system has a solution set over $\mathbb{Q}$ of positive dimension. In this case, we need to find a solution over the integers in such a way that T has determinant in $\{\pm 1\}$. Finding a solution of this type is a hard problem to which we offer no solution.

Since we are not looking for a solution to solve the mentioned decision problem for lattices, we assume our groups are subgroups of $\mathbb{S}_n$. This assures us that the lattice we are working with is a permutation lattice with the standard basis. We also note that since conjugate subgroups of $\mathrm{GL}(n, \mathbb{Z})$ correspond to isomorphic lattices, with our assumption we are discussing isomorphism classes of permutation lattices. We also know that isomorphic lattices correspond to isomorphic algebraic tori.

4.1.2 Normal Basis Theorem

Suppose K/F is a finite Galois extension with $G = \mathrm{Gal}(K/F)$. The purpose of this section is to provide some information about a specific type of basis for K as a F-vector space. We are interested in a basis on which the action of G permutes the elements, it will play a central role in the results of this chapter.

Definition 2. Assume K/F is a finite Galois extension and $G = \{\sigma_1, \ldots, \sigma_n\}$ is the Galois group of K/F. An element $\alpha \in K$ is called normal if $B = \{\sigma_1(\alpha), \ldots, \sigma_n(\alpha)\}$ is an F-basis for K, and we call B a normal basis of K over F.

The existence of a normal basis for a finite Galois extension was proven in [30] and [7].

Theorem 3. *[22, Theorem 6.13.1] (Normal Basis Theorem) Let K/F be a finite Galois extension of degree n. Let $\sigma_1, \ldots, \sigma_n$ be the elements of the Galois group G. Then there exists an element $\alpha \in K$ such that $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ form a basis of K over F.*

There are different proofs for the normal basis theorem. The following argument, which is part of one of the proofs, gives a concrete way to find a normal basis for a given finite Galois extension.

Assume K/F is a finite Galois extension and $G = \{\sigma_1, \ldots, \sigma_n\}$ is the Galois group of K/F. We are looking for an element $x \in K$ such that, if $\sum_{i=1}^n c_i\sigma_i(x) = 0$ (for $c_i \in F$), then $c_i = 0$ for each i. Let $\{\beta_1, \ldots, \beta_n\}$ be an F-basis for K. For indeterminates $x_1, \ldots, x_n$ we can write $x = x_1\beta_1 + \cdots + x_n\beta_n$.

For $\sigma \in \{\sigma_1, \ldots, \sigma_n\}$, if $\sum_{i=1}^n c_i\sigma_i(x) = 0$, then $\sigma^{-1}(\sum_{i=1}^n c_i\sigma_i(x)) = \sum_{i=1}^n c_i\sigma^{-1}\sigma_i(x) = 0$. Thus we have

$$\begin{bmatrix} \sigma_1^{-1}\sigma_1(x) & \sigma_1^{-1}\sigma_2(x) & \cdots & \sigma_1^{-1}\sigma_n(x) \\ \sigma_2^{-1}\sigma_1(x) & \sigma_2^{-1}\sigma_2(x) & \cdots & \sigma_2^{-1}\sigma_n(x) \\ \vdots & \vdots & \cdots & \vdots \\ \sigma_n^{-1}\sigma_1(x) & \sigma_n^{-1}\sigma_2(x) & \cdots & \sigma_n^{-1}\sigma_n(x) \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} = 0$$

So it is enough to show that the above matrix, we call it $A(x)$, is invertible for some x. Replacing x by $x_1\beta_1 + \cdots + x_n\beta_n$ we get

$$A(x) = A(x_1, \ldots, x_n) = \begin{bmatrix} \sigma_1^{-1}\sigma_1(\sum_{i=1}^n x_i\beta_i) & \sigma_1^{-1}\sigma_2(\sum_{i=1}^n x_i\beta_i) & \cdots & \sigma_1^{-1}\sigma_n(\sum_{i=1}^n x_i\beta_i) \\ \sigma_2^{-1}\sigma_1(\sum_{i=1}^n x_i\beta_i) & \sigma_2^{-1}\sigma_2(\sum_{i=1}^n x_i\beta_i) & \cdots & \sigma_2^{-1}\sigma_n(\sum_{i=1}^n x_i\beta_i) \\ \vdots & \vdots & \cdots & \vdots \\ \sigma_n^{-1}\sigma_1(\sum_{i=1}^n x_i\beta_i) & \sigma_n^{-1}\sigma_2(\sum_{i=1}^n x_i\beta_i) & \cdots & \sigma_n^{-1}\sigma_n(\sum_{i=1}^n x_i\beta_i) \end{bmatrix}$$

and $\det(A) \in K[x_1, \ldots, x_n]$. We just need to find $(a_1, \ldots, a_n) \in F^n$ so that $\det(A)(a_1, \ldots, a_n) \neq 0$. It is possible to show the existence of such element in F^n. Indeed this gives a complete proof of the theorem. Since we just wanted to explain a way to find a normal element, we skip the proof of existence (see [22, Theorem 6.13.1]).

The above argument gives a randomized method to find a normal element for a given extension by choosing $x_1, \ldots, x_n$ at random. There are better algorithms for finding a normal element. For an algorithm in characteristic zero see [12], in positive characteristic, see [41], [34].

4.2 Construction of Quasi Split Tori

We have already seen the duality between algebraic tori and lattices. For a given $G \leq \mathrm{GL}(n, \mathbb{Z})$ although we know $K(T_{G,F}) \cong K(x_1, \ldots, x_n)^G$ and $K[T_{G,F}] \cong K[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]^G$, it is given as a field (or ring) of multiplicative invariants, and we do not have a generating set for them. We are interested in finding the multiplicative invariants in a concrete way.

There are many algorithms for finding the invariant rings for polynomial invariants. We invite the reader to consult [6] and [40]. However, for multiplicative invariants the algorithmic side is not explored that much. We invite the reader to consult [20] and [35] for some results.

In this section, we focus on a specific family of algebraic tori, namely quasi split tori. For this family we present machinery to construct rational function fields and coordinate rings. The lattice corresponding to a quasi split algebraic torus is a permutation lattice. The rationality of this kind of algebraic tori has been known for a long time. Since a quasi-split torus of dimension d is rational over the base field, its function field is generated as a field by d elements which are algebraically independent over the base field.

When L_G is a permutation lattice, by the No Name Lemma, $K(T_{G,F})$ is a rational extension of F, i.e. there exist $y_1, \ldots, y_n \in K[x_1, \ldots, x_n]$ such that

$$K(x_1, \ldots, x_n)^G = F(y_1, \ldots, y_n)$$

and $y_1, \ldots, y_n$ are algebraically independent over F.

The existence of y_i's is related to the existence of a permutation basis for L_G. Hence having such a basis, enables us to construct the transcendence basis we are looking for.

From the discussion of the previous section, we know that for a given permutation G-lattice, it is not easy to find a basis on which G acts permutations. Hence, we will assume that G is given as a subgroup of the group $\mathbb{S}_n$ generated by

$$\left[\begin{array}{c|c} 0 & 1 \\ \hline I_n & 0 \end{array}\right] \text{ and } \left[\begin{array}{cc|c} 0 & 1 & \multirow{2}{*}{0} \\ 1 & 0 & \\ \hline \multicolumn{2}{c|}{0} & I_{n-2} \end{array}\right]$$

so that the corresponding G-lattice L is a permutation (by Lemma 1). We note that conjugate subgroups of $\mathrm{GL}(n, \mathbb{Z})$ correspond to isomorphic algebraic tori.

Remark. Assume S_n is the symmetric group generated by $\sigma = (1\ 2\ \ldots\ n)$ and $\tau = (1\ 2)$. Now the above generators of $\mathbb{S}_n$ can be seen as the images of I_n, under the action of σ and τ on its rows which gives an isomorphism between S_n and $\mathbb{S}_n$. This shows that the action of $\delta \in \mathrm{S}_n$ on e_i, an element of the standard basis of $L_{\mathbb{S}_n}$, is given by $\delta(e_i) = e_{\delta^{-1}(i)}$ and similarly if we are dealing with $K(x_1, \ldots, x_n) \cong K(L_{\mathbb{S}_n})$, we have $\delta(x_i) = x_{\delta^{-1}(i)}$ by Definition 46.

We need one more component to construct $T_{G,F}$. The last component is a finite Galois extension of a field F. In other words one needs to solve the inverse Galois problem for the pair (G, F) since it is not the purpose of this thesis, we assume K/F is a finite Galois extension and the action of G on a basis of K over F is given.

By the No Name Lemma, we know that the rational function field of $T_{G,F}$ is purely transcendental over F, so the final step is to find a transcendence basis of $K(T_{G,F})$ over F. By the proof of the No Name Lemma provided in chapter two, one can see that it all comes down to finding a basis for V, the K-vector space generated by $\{x_1, \ldots, x_n\}$, which is also a generating set for $K(L_G)$ being permuted by G.

Let us see the above ideas in the following concrete example.

Example 4. Suppose $G = \langle \sigma = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \rangle$, so $n = 2$. G is isomorphic to the cyclic group of order two. We can take $F = \mathbb{Q}$ and $K = \mathbb{Q}(i)$ as our extension; then $\sigma(i) = -i$. Now $M = \langle e_1, e_2 \rangle_{\mathbb{Z}}$ is a permutation G-lattice, so that $K(M) = K(x_1, x_2)$. It can be verified that

$$y_1 = x_1 + x_2 \ \text{ and } \ y_2 = ix_1 - ix_2$$

are in V^G and generate V so

$$K(M)^G = K(x_1, x_2)^G = K^G(y_1, y_2) = \mathbb{Q}(y_1, y_2)$$

The following theorem solves the problem of finding a transcendence basis in the special case where $G = \mathbb{S}_n$. Later on we present a general result which works for any subgroup of $\mathbb{S}_n$.

Theorem 5. *Suppose $G = \mathbb{S}_n$, L_G is its corresponding G-lattice (with the action in Remark 4.2) and $\mathrm{S}_n = \mathrm{Gal}(K/\mathbb{Q})$ where K is the splitting field of an irreducible polynomial $f \in \mathbb{Q}[x]$. Assume $R = \{r_1, \ldots, r_n\}$ is the set of all roots of f in K such that for $s \in \mathrm{S}_n$, $s(r_i) = r_{s(i)}$ and A be the sum of elements of R. The generators of the rational function field of the corresponding algebraic torus, is given explicitly by*

$$K(L_G)^G = K(x_1, \ldots, x_n)^G = \mathbb{Q}(y_1, \ldots, y_n)$$

where

$$S = \sum_{\delta \in G} \delta \in \mathbb{Z}[G]$$

$$y_1 = x_1 + x_2 + \cdots + x_n$$

$$y_i = S(r_i x_i) \ \ , i = 2, \ldots, n.$$

Moreover the coefficient of x_k in y_i for $1 \le i \le n-1$ is given by:

$$c_k = \begin{cases} (n-1)!r_i & k = i \\ (n-2)!(A - r_i) & k \neq i \end{cases}$$

Proof. Suppose $\{x_1, \ldots, x_n\}$ is a basis which is being permuted by G. As discussed in Remark 4.2, we can consider L_G as a S_n lattice with the action mentioned in Remark 4.2. That is for $\delta \in S_n$, $\delta(x_i) = x_{\delta^{-1}(i)}$. By the proofs of Speiser's lemma and the No Name Lemma we know that $K(M)^G$ is rational over $\mathbb{Q}$ i.e. there exist y_is such that $K(M)^G \cong \mathbb{Q}(y_1, \ldots, y_n)$. Let V be the K-vector space generated by x_is. We need to find $\{y_1, \ldots, y_n\} \subset SV$ such that $\{y_i\}$ generates V as a K-vector space.

Define $y_1 = x_1 + x_2 + \cdots + x_n$ and $y_i = S(r_i x_i)$ for $i = 2, \ldots, n$. So for $i = 1, \ldots, n-1$,

$$y_i = \sum_{\sigma \in S_n} r_{\sigma(i)} x_{\sigma^{-1}(i)} = \sum_{k=1}^{n} \sum_{\sigma^{-1}(i)=k} r_{\sigma(i)} x_k.$$

So $c_k = \sum_{\sigma \in S_n, \sigma^{-1}(i)=k} r_{\sigma(i)}$. If $k = i$, $\sigma^{-1}(i) = i$ implies $\sigma(i) = i$ and so $c_i = |\mathrm{Stab}_{S_n}(i)| r_i = (n-1)! r_i$. If $k \neq i$, then $\sigma^{-1}(i) = k$ implies that σ maps $\{1, \ldots, n\} - \{k\}$ bijectively to $\{1, \ldots, n\} - \{i\}$. So since $i \neq k$, $\sigma(i)$ can take on any value in $\{1, \ldots, n\} - \{i\}$. This shows that for $k \neq i$, we have

$$c_k = \sum_{j \neq i} |\{\sigma \in S_n, \sigma(k) = i, \sigma(i) = j\}| r_j = (n-2)!(A - r_i).$$

Also $(n-1)! r_i - (n-2)!(A - r_i) \neq 0$ since otherwise $r_i = \frac{A}{n}$ which is rational. Thus by considering $y_i - (n-2)!(A - r_i) y_1$ we get a multiple of x_i. This shows that $\{y_i\}$ has the desired property and we are done.

□

Remark. L_G in the previous theorem, is isomorphic to the permutation S_n lattice $\mathbb{Z}[S_n/S_{n-1}]$. For a geometric description of the corresponding algebraic torus see Examples 18 and 19 in [44].

Example 6. Let $G \leq \mathrm{GL}(3, \mathbb{Z})$ be generated by

$$\sigma = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \text{ and } \tau = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

This is obviously isomorphic to S_3.

$$\sigma^2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \text{ and } \sigma\tau = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \text{ and } \tau\sigma = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

Now the splitting field of $x^3 - 2$ is $\mathbb{Q}(\rho, \sqrt[3]{2})$, where ρ is a primitive third root of unity. The roots of $x^3 - 2$ are $\sqrt[3]{2}$, $\rho\sqrt[3]{2}$, $\rho^2\sqrt[3]{2}$. The Galois group of the extension is S_3 with the action

$$\sigma = \begin{cases} \sqrt[3]{2} \longrightarrow \rho\sqrt[3]{2} \\ \rho \longrightarrow \rho \end{cases} \qquad \tau = \begin{cases} \sqrt[3]{2} \longrightarrow \sqrt[3]{2} \\ \rho \longrightarrow \rho^2 \end{cases} \qquad \sigma^2 = \begin{cases} \sqrt[3]{2} \longrightarrow \rho^2\sqrt[3]{2} \\ \rho \longrightarrow \rho \end{cases}$$

$$\sigma\tau = \begin{cases} \sqrt[3]{2} \longrightarrow \rho\sqrt[3]{2} \\ \rho \longrightarrow \rho^2 \end{cases} \qquad \tau\sigma = \begin{cases} \sqrt[3]{2} \longrightarrow \rho^2\sqrt[3]{2} \\ \rho \longrightarrow \rho^2 \end{cases} .$$

We can provide the following table for the action of the symmetric group on x_is and the roots.

	1	σ	σ^2	τ	$\sigma\tau$	$\tau\sigma$
x_1	x_1	x_3	x_2	x_2	x_3	x_1
x_2	x_2	x_1	x_3	x_1	x_2	x_3
x_3	x_3	x_2	x_1	x_3	x_1	x_2
$\sqrt[3]{2}$	$\sqrt[3]{2}$	$\rho\sqrt[3]{2}$	$\rho^2\sqrt[3]{2}$	$\sqrt[3]{2}$	$\rho\sqrt[3]{2}$	$\rho^2\sqrt[3]{2}$
$\rho\sqrt[3]{2}$	$\rho\sqrt[3]{2}$	$\rho^2\sqrt[3]{2}$	$\sqrt[3]{2}$	$\rho^2\sqrt[3]{2}$	$\sqrt[3]{2}$	$\rho\sqrt[3]{2}$
$\rho^2\sqrt[3]{2}$	$\rho^2\sqrt[3]{2}$	$\sqrt[3]{2}$	$\rho\sqrt[3]{2}$	$\rho\sqrt[3]{2}$	$\rho^2\sqrt[3]{2}$	$\sqrt[3]{2}$

Let $r_1 = \rho\sqrt[3]{2}, r_2 = \rho^2\sqrt[3]{2}$ and $r_3 = \sqrt[3]{2}$. One can verify that for $g \in G$, $g(r_i) = r_{g(i)}$ and then we get

$$S = 1 + \sigma + \sigma^2 + \tau + \sigma\tau + \tau\sigma$$

$$y_0 = S(x_1 + x_2 + x_3) = 6(x_1 + x_2 + x_3)$$

$$y_1 = S(\rho\sqrt[3]{2}x_1) = 2\rho\sqrt[3]{2}x_1 + (\sqrt[3]{2} + \rho^2\sqrt[3]{2})x_2 + (\sqrt[3]{2} + \rho^2\sqrt[3]{2})x_3$$

$$y_2 = S(\rho^2\sqrt[3]{2}x_2) = (\sqrt[3]{2} + \rho\sqrt[3]{2})x_1 + 2\rho^2\sqrt[3]{2}x_2 + (\sqrt[3]{2} + \rho\sqrt[3]{2})x_3$$

Theorem 5 does not say anything about a proper subgroup of $\mathbb{S}_n$. Thus it can just be used to get explicit information about $T_{\mathbb{S}_n}$. In fact using a generic polynomial for S_n, one can construct $K/\mathbb{Q}$. Now we want to prove a general result which works for any subgroup of $\mathbb{S}_n$. The other difference of this result we are talking about with Theorem 5 is, the different descriptions of the field extension. In Theorem 5 we assumed the roots of a polynomial are given, but in the general case we will assume a normal element of the field extension is given. The following lemma is a generalization of the idea which is used in [13, Lemma 1.3.3] to prove that the Moore determinant is nonzero over an extension of a finite field. It is the main tool for a constructive proof of the No Name Lemma with some assumptions.

Remark. For a matrix M we denote its j-th column by M_j; an automorphism acts on a column by acting on its entries.

Let K/F be a finite Galois extension with finite Galois group G. Let $M \in M_{mn}(K)$, $m \leq n$. G acts on the columns of M, by acting on entries, that is for $g \in G$ and $M_j^T = \begin{bmatrix} m_{1j} & m_{2j} & \dots & m_{mj} \end{bmatrix}$, $g(M_j^T) = \begin{bmatrix} g(m_{1j}) & g(m_{2j}) & \dots & g(m_{mj}) \end{bmatrix}$. When we say that G permutes the columns of M transitively up to sign, we mean: There exists a homomorphism $\rho : G \longrightarrow S_n$, $\rho(g) = \rho_g$ such that $g(M_i) = (-1)^{s_g} M_{\rho_g(i)}$ for some $s_g \in \{0, 1\}$ for all $i = 1, \dots n$ and for each $1 \leq i \neq j \leq n$, there exists $g \in G$ such that $\rho_g(i) = j$. Note that the action of G on the columns of M is not required to be faithful.

Lemma 7. *Let K/F be a finite Galois extension with finite Galois group G. Let $M \in M_{mn}(K)$, $m \le n$ and assume that G permutes the columns of M transitively up to sign. Assume also that the entries of M_1 are F-linearly independent. Then the rows of M are K-linearly independent so that the rank of M over K is m.*

Proof. The proof is by induction on m. If $m = 1$, we need only to show that the unique row of M is non-zero. This is true since if $M_1 = [v_1]$, v_1 is F linearly independent and so non-zero. Since v_1 is the first entry in the only row of M, we are done.

Now assume that $m > 1$. To show that the rows of M are linearly independent over K, it is equivalent to show that the null space of M^T is trivial. We will show this by contradiction. Assume that there exists $\mathbf{0} \neq \mathbf{x} \in N(M^T) \subseteq K^m$. So $M^T\mathbf{x} = 0$. There exists some $x_k \neq 0$. Let $\mathbf{y} = \frac{1}{x_k}\mathbf{x} \in K^m$. Then $y_k = 1$ and $\mathbf{y} \in N(M^T)$, so $M^T\mathbf{y} = 0$. The ith component is $M_i^T\mathbf{y} = 0$, $i = 1, \ldots, n$. For each $g \in G$, we get $g(M_i^T\mathbf{y}) = g(M_i)^T g(\mathbf{y}) = \pm M^T_{\rho_g(i)} g(\mathbf{y}) = 0$ for all $i = 1, \ldots, n$ and so $M_j^T g(\mathbf{y}) = 0$ for all $j = 1, \ldots, n$, which shows that $g(\mathbf{y}) \in N(M^T)$. So $g(\mathbf{y}) - \mathbf{y} \in N(M^T)$. By assumption, the kth component of $g(\mathbf{y}) - \mathbf{y}$ is 0, and so $g(\hat{\mathbf{y}}) - \hat{\mathbf{y}} \in N(\hat{M}^T)$ where $\hat{\mathbf{y}} \in K^{m-1}$ is the vector $\mathbf{y}$ with the kth component removed and $\hat{M} \in M_{m-1,n}(K)$ is M with row k removed. Note that $\hat{M}$ has columns $\hat{M}_i$, $i = 1, \ldots, n$. Since M_1 has entries which are F-linearly independent, so does $\hat{M}_1$. Since the columns of M are permuted transitively up to sign changes by the action of G, so the columns of $\hat{M}$ are similarly permuted transitively up to sign changes. Since the inductive hypothesis applies to $\hat{M}$, we see that the rows of $\hat{M}$ are K-linearly independent, or equivalently $N(\hat{M}^T)$ is trivial. Since $g(\hat{\mathbf{y}}) - \hat{\mathbf{y}} \in N(\hat{M}^T) = \{0\}$ for all $g \in G$, we see that $\hat{\mathbf{y}} \in F^{m-1}$ and so $\mathbf{y} \in F^m$. But then $M_1^T\mathbf{y} = 0$ is equivalent to $\sum_{k=1}^m v_k y_k = 0$ which is a non-trivial F-dependence relation for the entries of the first column of M. By contradiction, the rows of M must be K-linearly independent and so $\operatorname{rank}(M) = m$. □

Remark. With the assumptions of Lemma 7, if $m = n$ then $\det M \neq 0$.

Theorem 8. *Let $G \le \mathbb{S}_n \le \mathrm{GL}(n, \mathbb{Z})$ and L_G be the lattice corresponding to G as defined in Definition 46, which is a permutation lattice with the standard basis. Assume that G acts transitively on the standard basis of L_G. Let K/F be a finite Galois extension with Galois group G. Let $\alpha \in K$ be a normal element for the Galois extension K/F. Then $K(x_1, \ldots, x_n)^G$ is rational over F with transcendence basis $y_1, \ldots, y_n$ where $y_i = S(\alpha x_i) = \sum_{j=1}^n \sum_{g\in G_{ij}} g(\alpha)x_j$, $i = 1, \ldots, n$, where $S = \sum_{g\in G} g \in \mathbb{Z}[G]$ and $G_{ij} = \{g \in G : g(x_i) = x_j\}$. Here $G_{ij} = g_{ij}\mathrm{Stab}_G(x_i)$, where g_{ij} is a fixed element of G_{ij}.*

Proof. Let $V = \sum_{i=1}^n Kx_i$. Then by Speiser's Lemma 45 there exists a K-basis for V contained in V^G. By the No Name Lemma, this K-basis gives a transcendence basis for $K(L_G)^G$.

We show that $y_i = S(\alpha x_i) = \sum_{g\in G} g(\alpha)g(x_i) \in V^G$, for $i = 1, \ldots, n$, is a K-basis for V. Let $G_{ij} = \{g \in G : g(x_i) = x_j\}$. Since the action of G on L_G is transitive, G_{ij} is non-empty for every

$1 \le i, j \le n$. Then

$$y_i = \sum_{j=1}^{n} \sum_{g \in G_{ij}} g(\alpha) x_j, \quad i = 1, \ldots, n.$$

Fix some $g_{ij} \in G$ with $x_j = g_{ij}(x_i)$. If $g \in G_{ij}$, then $g_{ij}^{-1} g(x_i) = x_i$ shows that $g \in g_{ij}\mathrm{Stab}_G(x_i)$. Since $g_{ij}\mathrm{Stab}_G(x_i) \subseteq G_{ij}$, we see that $G_{ij} = g_{ij}\mathrm{Stab}_G(x_i)$ is a left coset of $\mathrm{Stab}_G(x_i)$ in G.

To show that $\{y_1, \ldots, y_n\}$ is a K-basis of V, we show that the matrix M with ith row the coordinate vector for y_i with respect to the K-basis $\{x_1, \ldots x_n\}$ has rows which are linearly independent over K. The matrix M has entries $m_{ij} = \sum_{g \in G_{ij}} g(\alpha)$, $i, j = 1, \ldots, n$. We will apply Lemma 7 to show that M has K linearly independent rows and so the $y_1, \ldots, y_n$ form K-basis of V.

We need to check the hypothesis of the lemma are satisfied . First, let $\rho : G \longrightarrow \mathrm{S}_n$, $\rho(g) = \rho_g$ be the group homomorphism that corresponds to the action of G on the $\{x_1, \ldots, x_n\}$. Note that this is defined by the following rule: $\rho_g(i) = j$ if and only if $g(x_i) = x_j$ for all $1 \le i, j \le n$. We will show that the columns of M are permuted by the action of G. Let $h \in G$. Note that if $g \in G_{ij}$, then $hg \in G_{i\rho_h(j)}$. So

$$h(m_{ij}) = \sum_{g \in G_{ij}} hg(\alpha) = \sum_{\sigma \in G_{i\rho_h(j)}} \sigma(\alpha) = m_{i\rho_h}(j)$$

shows that $hM_j = M_{\rho_h(j)}$ for all $j = 1, \ldots, n$. So the action of G permutes the columns of M.

Secondly, the first column M_1 has entries

$$\{\sum_{g \in G_{i1}} g(\alpha), i = 1, \ldots, n\}.$$

Since α is a normal element of the Galois extension K/F with Galois group G, the set $\{g(\alpha) : g \in G\}$ is F linearly independent. Since $G = \sqcup_{i=1}^{n} G_{i1}$ is a disjoint union, the set

$$\{\sum_{g \in Gi1} g(\alpha), i = 1, \ldots, n\}$$

is F linearly independent.

So the lemma applies and we may conclude that $y_1, \ldots, y_n$ is a K-basis of V and so is an F transcendence basis of $K(L_G)^G$.

□

Corollary 9. *With the assumptions of previous theorem except that we now assume that L_G is an arbitrary permutation G-lattice. Then $K(x_1, \ldots, x_n)^G$ is rational over F with transcendence basis $y_1, \ldots, y_n$ where $y_i = S(\alpha x_i) = \sum_{x_j \in Gx_i} \sum_{g \in G_{ij}} g(\alpha) x_j$, $i = 1, \ldots, n$ where $S = \sum_{g \in G} g \in \mathbb{Z}[G]$ and $Gx_i = \{gx_i : g \in G\}$ and $G_{ij} = \{g \in G : g(x_i) = x_j\}$. Here $G_{ij} = g_{ij}\mathrm{Stab}_G(x_i)$ where g_{ij} is a fixed element of G_{ij}.*

Proof. Let $P = L_G$ and $\mathbf{e}_1, \ldots, \mathbf{e}_n$ be a permutation basis of P corresponding to $x_1, \ldots, x_n$. Let $\mathbf{e}_{j_k} : k = 1, \ldots, r$ and correspondingly $x_{j_k} : k = 1, \ldots, r$ be a complete set of G orbit representatives on the $\mathbb{Z}$-basis for P and the indeterminates $x_1, \ldots, x_n$ respectively. Then $P_k = \oplus_{\mathbf{e}_i \in G\mathbf{e}_{j_k}} \mathbb{Z}\mathbf{e}_i$ is a transitive permutation G lattice for each $k = 1, \ldots, r$ and $K(P_k) = K(x_i : x_i \in Gx_{j_k})$. $P = \oplus_{k=1}^r P_k$ is a direct sum of transitive permutation G lattices. Then $K(P)^G$ is a composite of fields $K(P)^G = \prod_{k=1}^r K(P_k)$ and so $K(P)^G$ has transcendence basis $\{y_i : x_i \in Gx_{j_k}\}$ over F where for $x_i \in Gx_{j_k}$, we have $y_i = \sum_{x_j \in Gx_{j_k}} \sum_{g \in G_{ij}} g(\alpha)x_j$. Since $x_i \in Gx_{j_k}$, we see that $x_j \in Gx_{j_k}$ if and only if $x_j \in Gx_i$ so we may express

$$y_i = \sum_{x_j \in Gx_i} \sum_{g \in G_{ij}} g(\alpha)x_j$$

(Note also that in fact, G_{ij} is non-empty if and only if $x_j \in Gx_i$, so we could even write

$$y_i = \sum_{j=1}^{n} \sum_{g \in G_{ij}} g(\alpha)x_j$$

as before). At any rate $K(P)^G = F(y_i : x_i \in Gx_{j_k}, k = 1, \ldots, r) = F(y_1, \ldots, y_n)$ as required. □

Example 10. Let K be the splitting field of $x^4 - 2$ over $\mathbb{Q}$. Then $\mathrm{Gal}(K/\mathbb{Q}) \cong D_8$, $K = \mathbb{Q}(\sqrt[4]{2}, i)$ and $\{1, \theta, \theta^2, \theta^3, i, i\theta, i\theta^2, i\theta^3\}$ where $\theta = \sqrt[4]{2}$ is a $\mathbb{Q}$-basis for K. Moreover, let $G \leq \mathrm{GL}(4, \mathbb{Z})$ be generated by

$$r = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad \text{and} \quad s = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

One can verify that $G \cong D_8$. The action of r and s on the basis of K is given by

$$r(i) = i \quad r(\theta) = i\theta$$
$$s(i) = -i \quad s(\theta) = \theta$$

Now we define

$$\alpha_1 = \alpha = 1 + \theta + \theta^2 + \theta^3 + i + i\theta + i\theta^2 + i\theta^3$$

and claim that α is a normal element in K. In fact,

$$\alpha_2 = r(\alpha) = 1 - \theta - \theta^2 + \theta^3 + i + i\theta - i\theta^2 - i\theta^3$$

$$\alpha_3 = r^2(\alpha) = 1 - \theta + \theta^2 - \theta^3 + i - i\theta + i\theta^2 - i\theta^3$$

$$\alpha_4 = r^3(\alpha) = 1 + \theta - \theta^2 - \theta^3 + i - i\theta - i\theta^2 + i\theta^3$$

$$\alpha_5 = s(\alpha) = 1 + \theta + \theta^2 + \theta^3 - i - i\theta - i\theta^2 - i\theta^3$$

$$\alpha_6 = rs(\alpha) = 1 + \theta - \theta^2 - \theta^3 - i + i\theta + i\theta^2 - i\theta^3$$

$$\alpha_7 = r^2 s(\alpha) = 1 - \theta + \theta^2 - \theta^3 - i + i\theta - i\theta^2 + i\theta^3$$
$$\alpha_8 = r^3 s(\alpha) = 1 - \theta - \theta^2 + \theta^3 - i - i\theta + i\theta^2 + i\theta^3$$

and

$$\det \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 \end{bmatrix} = 4096,$$

which implies α is a normal element of K. Now we can define $y_i = S(\alpha x_i)$ where

$$S = 1 + r + r^2 + r^3 + s + sr + sr^2 + sr^3 \in \mathbb{Z}[D_8].$$

Finally,

$$K(x_1, x_2, x_3, x_4) = F(y_1, y_2, y_3, y_4).$$

It is also worth presenting the coordinate matrix of the y_i's, as a concrete example of Lemma 7. In order to do so, we need to know the action of G on the x_i's.

	1	r	r^2	r^3	s	sr	sr^2	sr^3
x_1	x_1	x_4	x_3	x_2	x_1	x_2	x_3	x_4
x_2	x_2	x_1	x_4	x_3	x_4	x_1	x_2	x_3
x_3	x_3	x_2	x_1	x_4	x_3	x_4	x_1	x_2
x_4	x_4	x_3	x_2	x_3	x_2	x_3	x_4	x_1

From the above table one can easily form the matrix

$$M = \begin{bmatrix} (1+s)(\alpha) & (r^3+sr)(\alpha) & (r^2+sr^2)(\alpha) & (r+sr^3)(\alpha) \\ (r+sr)(\alpha) & (1+sr^2)(\alpha) & (r^3+sr^3)(\alpha) & (r^2+s)(\alpha) \\ (r^2+sr^2)(\alpha) & (r+sr^3)(\alpha) & (1+s)(\alpha) & (r^3+sr)(\alpha) \\ (r^3+sr^3)(\alpha) & (r^2+s)(\alpha) & (r+sr)(\alpha) & (1+srr)(\alpha) \end{bmatrix}.$$

The action of r and s on the columns is

	r	s
M_1	M_4	M_1
M_2	M_1	M_4
M_3	M_2	M_2
M_4	M_3	M_3

As it has been mentioned above, we can apply Lemma 7 in order to compute the coordinate ring of an algebraic torus. The following theorem and its constructive proof can be turned into an efficient algorithm to compute the coordinate ring of an algebraic tori.

Theorem 11. *With the assumptions of Theorem 9*

$$K[L]^G \cong K[x_1^{\pm 1}, x_2^{\pm 1}, \ldots, x_n^{\pm 1}]^G = F[y_1, \ldots, y_n]_{x_1 \cdots x_n}$$

where y_i is given by

$$S = \sum_{\sigma \in G} \sigma \in \mathbb{Z}[G]$$

$$y_i = S(\alpha x_i) \quad \textit{for} \;\; 1 \le i \le n.$$

Proof. It is known that $K(L)$ is isomorphic to a Laurent polynomial ring. Also

$$K[x_1^{\pm 1}, x_2^{\pm 1}, \ldots, x_n^{\pm 1}] = K[x_1, \ldots, x_n]_{x_1 \cdots x_n}.$$

We are interested in $K[L]^G \cong \left(K[x_1^{\pm 1}, x_2^{\pm 1}, \ldots, x_n^{\pm 1}]\right)^G = (K[x_1, \ldots, x_n]_{x_1 \cdots x_n})^G$. By the proof of Theorem 9 we can see $K[x_1, \ldots, x_n] = K[y_1, \ldots, y_n]$. On the other hand since G permutes the x_i's, $x_1 \cdots x_n$ is invariant under the action of G, we can conclude

$$(K[x_1, \ldots, x_n]_{x_1 \cdots x_n})^G = (K[y_1, \ldots, y_n]_{x_1 \cdots x_n})^G$$

$$= K^G[y_1, \ldots, y_n]_{x_1 \cdots x_n} = F[y_1, \ldots, y_n]_{x_1 \cdots x_n}.$$

□

4.3 Algebraic tori with sign permutation character lattice

Permutation lattices are special examples of a larger family of lattices which is called sign permutation. As we have already seen in the second chapter, a sign permutation lattice is a G-lattice which has a $\mathbb{Z}$-basis which G permutes it up to sign changes. There is no known efficient algorithm which determines if a given lattice is sign permutation or not. It is also known that if T_G is a corresponding algebraic torus with sign permutation character lattice, then T_G is rational over the base field.

Before presenting the next theorem we recall the action on a sign permutation lattice. Let $G \le \mathrm{GL}(n, \mathbb{Z})$ be a finite subgroup. L_G, the corresponding lattice to G, is the lattice generated by $\{\mathbf{e}_i : i = 1, \ldots, n\}$ where $(\mathbf{e}_i)_j = \delta_{ij}$. G acts on L_G by multiplication from right. For a finite Galois extension K/F with $G \cong \mathrm{Gal}(K/F)$, $K(L) \cong K(x_1, \ldots, x_n)$ for algebraically independent x_i's over K, is a G field. G acts as Galois group on K and the action of $g \in G$ on x_i is given by

$$g(x_i) = \begin{cases} x_j & if \;\; g(\mathbf{e}_i) = \mathbf{e}_j \\ x_j^{-1} & if \;\; g(\mathbf{e}_i) = -\mathbf{e}_j \end{cases}.$$

Theorem 12. *Assume $G \leq \mathrm{GL}(n, \mathbb{Z})$ and the corresponding G-lattice, L_G (as in Definition 46), is sign permutation. Suppose that G acts transitively (up to sign) on L_G. Let K/F be a finite Galois extension with Galois group G. Let $\alpha \in K$ be a normal element for the Galois extension K/F. Then*

$$K(L_G)^G = K(x_1, \ldots, x_n)^G = F(y_1, \ldots, y_n),$$

where $S = \sum_{g \in G} g \in \mathbb{Z}[G]$ and $y_i = S(\alpha(1 + x_i)^{-1})$ for $i = 1, \ldots, n$.

Proof. We use the change of basis $z_i = (1 + x_i)^{-1}$. Now for $g \in G$,

$$g(z_i) = \begin{cases} z_j & \text{if } g(x_i) = x_j \\ 1 - z_j & \text{if } g(x_i) = x_j^{-1} \end{cases},$$

and $K(x_1, \ldots, x_n) = K(z_1, \ldots, z_n)$.

Define the K-vector space $V = K + \sum_{i=1}^{n} K z_i$. Similar to the permutation case, we need to find a K-basis for V which is contained in V^G. Let $S = \sum_{g \in G} g \in \mathbb{Z}[G]$ and $y_i = S(\alpha z_i)$ for $i = 1, \ldots, n$. We want to show that $\{1, y_1, \ldots, y_n\} \subset V^G$ is a K-basis for V.

For $i, j \in \{1, \ldots, n\}$, $G_{ij} = \{g \in G : g(z_i) = z_j \text{ or } g(z_i) = 1 - z_j\}$. Then, by the transitivity assumption, G_{ij} is non-empty for every $1 \leq i, j \leq n$. Moreover let $G_{ij}^{z_j} = \{g \in G : g(z_i) = z_j\}$ and $G_{ij}^{1-z_j} = \{g \in G : g(z_i) = 1 - z_j\}$ so that $G_{ij} = G_{ij}^{z_j} \sqcup G_{ij}^{1-z_j}$.

Let $\hat{M}$ be the coordinate matrix of $\{1, y_1, \ldots, y_n\}$ with respect to the K-basis $\{1, z_1, \ldots, z_n\}$. We have to show that $\det(\hat{M}) \neq 0$.

By definition,

$$\begin{aligned} y_i = S(\alpha z_i) &= \sum_j \Big(\sum_{g \in G_{ij}^{z_j}} g(\alpha) z_j + \sum_{g \in G_{ij}^{1-z_j}} g(\alpha)(1 - z_j) \Big) = \\ & \sum_j \Big(\sum_{g \in G_{ij}^{z_j}} g(\alpha) z_j + \sum_{g \in G_{ij}^{1-z_j}} g(\alpha) - \sum_{g \in G_{ij}^{1-z_j}} g(\alpha) z_j \Big) = \\ & \sum_j \sum_{g \in G_{ij}^{1-z_j}} g(\alpha) + \sum_j \Big(\sum_{g \in G_{ij}^{z_j}} g(\alpha) z_j - \sum_{g \in G_{ij}^{1-z_j}} g(\alpha) z_j \Big) = \\ & \sum_j \sum_{g \in G_{ij}^{1-z_j}} g(\alpha) + \sum_j \Big(\sum_{g \in G_{ij}^{z_j}} g(\alpha) - \sum_{g \in G_{ij}^{1-z_j}} g(\alpha) \Big) z_j \end{aligned}$$

For $i, j \in \{1, \ldots, n\}$, $m_{ij} = \sum_{g \in G_{ij}^{z_j}} g(\alpha) - \sum_{g \in G_{ij}^{1-z_j}} g(\alpha)$ and $c_i = \sum_j \sum_{g \in G_{ij}^{1-z_j}} g(\alpha)$. The matrix $\hat{M}$ is

$$\hat{M} = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ c_1 & m_{11} & \cdots & m_{1n} \\ \vdots & \vdots & \cdots & \vdots \\ c_n & m_{n1} & \cdots & m_{nn} \end{bmatrix}.$$

Define

$$M = \begin{bmatrix} m_{11} & \cdots & m_{1n} \\ \vdots & \cdots & \vdots \\ m_{n1} & \cdots & m_{nn} \end{bmatrix}.$$

Since $\det(\hat{M}) = \det(M)$, it is enough to show that the determinant of M is non-zero. In order to do so, we will apply Lemma 7 to show that M has K-linearly independent rows.

We need to check that the hypotheses of the lemma are satisfied. First, let $\rho : G \longrightarrow S_n$, $\rho(g) = \rho_g$ be the group homomorphism that corresponds to the action of G on the $\{z_1, \ldots, z_n\}$. Note that this is defined by the following rule: $\rho_g(i) = j$ if and only if $g(z_i) = z_j$ or $g(z_i) = 1 - z_j$ for all $1 \leq i, j \leq n$. We will show that the columns of M are permuted (up to a factor ± 1) by the action of G.

Let $h \in G$. Note that if $g \in G_{ij}$, then $hg \in G_{i\rho_h(j)}$. Hence $hG_{ij} \subseteq G_{i\rho_h(j)}$. On the other hand for any $g \in G_{i\rho_h(j)}$, $h^{-1}g(z_i) = z_j$ or $h^{-1}g(z_i) = 1 - z_j$ which implies $h^{-1}G_{i\rho_h(j)} \subseteq G_{ij}$ and $hG_{ij} = G_{i\rho_h(j)}$.

For $h \in G$ and $i, j \in \{1, \ldots, n\}$ we have

$$h(m_{ij}) = h(\sum_{g \in G_{ij}^{z_j}} g(\alpha) - \sum_{g \in G_{ij}^{1-z_j}} g(\alpha)) = \sum_{g \in G_{ij}^{z_j}} hg(\alpha) - \sum_{g \in G_{ij}^{1-z_j}} hg(\alpha)$$

On the other hand if $h(z_j) = z_{\rho_h(j)}$, then

$$m_{i\rho_h(j)} = \sum_{g \in G_{i\rho_h(j)}^{z_{\rho_h(j)}}} g(\alpha) - \sum_{g \in G_{i\rho_h(j)}^{1-z_{\rho_h(j)}}} g(\alpha) = \sum_{g \in G_{ij}^{z_j}} hg(\alpha) - \sum_{g \in G_{ij}^{1-z_j}} hg(\alpha).$$

To get the last equality we used the fact that $G_{i\rho_h(j)}^{z_{\rho_h(j)}} = hG_{ij}^{z_j}$ and $G_{i\rho_h(j)}^{1-z_{\rho_h(j)}} = hG_{ij}^{1-z_j}$.

If $h(z_j) = 1 - z_{\rho_h(j)}$, then

$$m_{i\rho_h(j)} = \sum_{g \in G_{i\rho_h(j)}^{z_{\rho_h(j)}}} g(\alpha) - \sum_{g \in G_{i\rho_h(j)}^{1-z_{\rho_h(j)}}} g(\alpha) = \sum_{g \in G_{ij}^{1-z_j}} hg(\alpha) - \sum_{g \in G_{ij}^{z_j}} hg(\alpha).$$

Similarly for the last equality we used the fact that $G_{i\rho_h(j)}^{z_{\rho_h(j)}} = hG_{ij}^{1-z_j}$ and $G_{i\rho_h(j)}^{1-z_{\rho_h(j)}} = hG_{ij}^{z_j}$.

In other words if $h \in G_{i\rho_h(j)}^{z_{\rho_h(j)}}$ then $h(m_{ij}) = m_{i\rho_h(j)}$ and if $h \in G_{i\rho_h(j)}^{1-z_{\rho_h(j)}}$ then $h(m_{ij}) = -m_{i\rho_h(j)}$, so $h(M_j) = \pm M_{\rho_h(j)}$.

Secondly, the first column M_1 has entries

$$\{\sum_{g \in G_{i1}^{z_1}} g(\alpha) - \sum_{g \in G_{i1}^{1-z_1}} g(\alpha), i = 1, \ldots, n\}$$

Since α is a normal element of the Galois extension K/F with Galois group G, the set $\{g(\alpha) : g \in G\}$ is F linearly independent. Since $G = \sqcup_{i=1}^n G_{i1} = \sqcup_{i=1}^n (G_{i1}^{z_1} \sqcup G_{i1}^{1-z_1})$ is a disjoint union, the set

$$\{\sum_{g\in G_{i1}^{z_1}} g(\alpha) - \sum_{g\in G_{i1}^{1-z_1}} g(\alpha), i = 1, \dots, n\}$$

is F-linearly independent.

So Lemma 7 applies and we may conclude that $1, y_1, \dots, y_n$ is a K-basis of V. So similarly to the proof of the No Name Lemma, $y_1, \dots, y_n$ is an F-transcendence basis of $K(L_G)^G$.

□

Corollary 13. *With the assumptions of previous theorem, assume now that L_G is an arbitrary sign permutation G-lattice. Then $K(x_1, \dots, x_n)^G$ is rational over F with transcendence basis $y_1, \dots, y_n$ where $y_i = S(\alpha(1 + x_i)^{-1})$ where $S = \sum_{g\in G} g \in \mathbb{Z}[G]$.*

Proof. Let $P = L_G$ and $\mathbf{e}_1, \dots, \mathbf{e}_n$ be a sign permutation basis of P corresponding to $x_1, \dots, x_n$. Let $\mathbf{e}_{j_k} : k = 1, \dots, r$ and correspondingly $x_{j_k} : k = 1, \dots, r$ be a complete set of G orbit representatives (up to a factor of ± 1) on the $\mathbb{Z}$-basis for P and the indeterminates $x_1, \dots, x_n$ respectively. Then $P_k = \oplus_{\mathbf{e}_i \in G\mathbf{e}_{j_k}} \mathbb{Z}\mathbf{e}_i$ is a transitive sign permutation G-lattice for each $k = 1, \dots, r$ and $K(P_k) = K(x_i : x_i \in Gx_{j_k}).P = \oplus_{k=1}^r P_k$ is a direct sum of transitive sign permutation G-lattices. Then $K(P)^G$ is a composite of fields $K(P)^G = \prod_{k=1}^r K(P_k)$ and so $K(P)^G$ has transcendence basis $\{y_i : x_i \in Gx_{j_k}\}$ over F. Hence $K(P)^G = F(y_i : x_i \in Gx_{j_k}, k = 1, \dots, r) = F(y_1, \dots, y_n)$ as required.

□

Example 14. Assume $G \leq \mathrm{GL}(3, \mathbb{Z})$ generated by

$$\sigma = \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix},$$

so that $G \cong C_4$. Suppose $K = \mathbb{Q}(\rho)$, where ρ is a primitive 5-th root of unity, $K/\mathbb{Q}$ is Galois, with $\mathrm{Gal}(K/\mathbb{Q}) \cong C_4$. Let x_1, x_2, x_3 be algebraically independent over K. We want to find $K(x_1, x_2, x_3)^G$. The action of G on the x_is and the 5-th roots of unity are given by

	id	σ	σ^2	σ^3
x_1	x_1	x_2^{-1}	x_1^{-1}	x_2
x_2	x_2	x_1	x_2^{-1}	x_1^{-1}
x_3	x_3	x_3^{-1}	x_3	x_3^{-1}
ρ	ρ	ρ^2	ρ^4	ρ^3
ρ^2	ρ^2	ρ^4	ρ^3	ρ
ρ^3	ρ^3	ρ	ρ^2	ρ^4
ρ^4	ρ^4	ρ^3	ρ	ρ^2

By defining

$$z_i = (1 + x_i)^{-1} \quad \text{for } 1 \le i \le 3,$$

the action of G on the z_is is given by

	id	σ	σ^2	σ^3
z_1	z_1	$1 - z_2$	$1 - z_1$	z_2
z_2	z_2	z_1	$1 - z_2$	$1 - z_1$
z_3	z_3	$1 - z_3$	z_3	$1 - z_3$

To form y_i we need $S = 1 + \sigma + \sigma^2 + \sigma^3$. Then

$$y_1 = S(\rho z_1) = \rho z_1 + \rho^2(1 - z_2) + \rho^4(1 - z_1) + \rho^3 z_2 = \rho^2 + \rho^4 + (\rho - \rho^4)z_1 + (\rho^3 - \rho^2)z_2$$

$$y_2 = S(\rho z_2) = \rho z_2 + \rho^2 z_1 + \rho^4(1 - z_2) + \rho^3(1 - z_1) = (\rho^3 + \rho^4) + (\rho^2 - \rho^3)z_1 + (\rho - \rho^4)z_2$$

$$y_3 = S(\rho z_3) = \rho z_3 + \rho^2(1 - z_3) + \rho^4 z_3 + \rho^3(1 - z_3) = (\rho^2 + \rho^3) + (\rho - \rho^2 - \rho^3 + \rho^4)z_3.$$

Just to compare with the proof of the Theorem 12, the matrix $\hat{M}$ is given

$$\hat{M} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ \rho^2 + \rho^4 & \rho - \rho^4 & \rho^3 - \rho^2 & 0 \\ \rho^3 + \rho^4 & \rho^2 - \rho^3 & \rho - \rho^4 & 0 \\ \rho^2 + \rho^3 & 0 & 0 & \rho - \rho^2 - \rho^3 + \rho^4 \end{bmatrix}$$

and

$$M = \begin{bmatrix} \rho - \rho^4 & \rho^3 - \rho^2 & 0 \\ \rho^2 - \rho^3 & \rho - \rho^4 & 0 \\ 0 & 0 & \rho - \rho^2 - \rho^3 + \rho^4 \end{bmatrix}.$$

One can verify the action of G on the columns of M is

	id	σ	σ^2	σ^3
M_1	M_1	$-M_2$	$-M_1$	M_2
M_2	M_2	M_1	$-M_2$	$-M_1$
M_3	M_3	$-M_3$	M_3	$-M_3$

Bibliography

[1] Armand Borel, *Linear algebraic groups*, second ed., Graduate Texts in Mathematics, vol. 126, Springer-Verlag, New York, 1991. MR 1102012 (92d:20001)

[2] N. Bourbaki, *éléments de mathématique. Fasc. XXXIV. Groupes et algèbres de Lie. Chapitre IV: Groupes de Coxeter et systèmes de Tits. Chapitre V: Groupes engendrés par des réflexions. Chapitre VI: systèmes de racines*, Actualités Scientifiques et Industrielles, No. 1337, Hermann, Paris, 1968. MR 0240238

[3] Harold Brown, Rolf Bülow, Joachim Neubüser, Hans Wondratschek, and Hans Zassenhaus, *Crystallographic groups of four-dimensional space*, Wiley-Interscience [John Wiley & Sons], New York-Chichester-Brisbane, 1978, Wiley Monographs in Crystallography. MR 0484179

[4] Kenneth S. Brown, *Cohomology of groups*, Graduate Texts in Mathematics, vol. 87, Springer-Verlag, New York, 1994, Corrected reprint of the 1982 original. MR 1324339 (96a:20072)

[5] Charles W. Curtis and Irving Reiner, *Methods of representation theory. Vol. I*, Wiley Classics Library, John Wiley & Sons, Inc., New York, 1990, With applications to finite groups and orders, Reprint of the 1981 original, A Wiley-Interscience Publication. MR 1038525

[6] Harm Derksen and Gregor Kemper, *Computational invariant theory*, enlarged ed., Encyclopaedia of Mathematical Sciences, vol. 130, Springer, Heidelberg, 2015, With two appendices by Vladimir L. Popov, and an addendum by Norbert A'Campo and Popov, Invariant Theory and Algebraic Transformation Groups, VIII. MR 3445218

[7] Max Deuring, *Galoissche Theorie und Darstellungstheorie*, Math. Ann. **107** (1933), no. 1, 140–144. MR 1512793

[8] The Sage Developers, *Sagemath, the Sage Mathematics Software System (Version 4.8)*, 2012, `http://www.sagemath.org`.

[9] Mátyás Domokos, *Covariants and the no-name lemma*, J. Lie Theory **18** (2008), no. 4, 839–849. MR 2523139

[10] Shizuo Endô and Takehiko Miyata, *Invariants of finite abelian groups*, J. Math. Soc. Japan **25** (1973), 7–26. MR 0311754 (47 #316)

[11] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.8.7*, 2017.

[12] Kurt Girstmair, *An algorithm for the construction of a normal basis*, J. Number Theory **78** (1999), no. 1, 36–45. MR 1706933

[13] David Goss, *Basic structures of function field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 35, Springer-Verlag, Berlin, 1996. MR 1423131

[14] Derek F. Holt, *The Meataxe as a tool in computational group theory*, The atlas of finite groups: ten years on (Birmingham, 1995), London Math. Soc. Lecture Note Ser., vol. 249, Cambridge Univ. Press, Cambridge, 1998, pp. 74–81. MR 1647414

[15] Akinari Hoshi and Aiichi Yamasaki, *Rationality problem for algebraic tori*, ArXiv. **1210.4525** (2012).

[16] James E. Humphreys, *Linear algebraic groups*, Springer-Verlag, New York-Heidelberg, 1975, Graduate Texts in Mathematics, No. 21. MR 0396773 (53 #633)

[17] Christian U. Jensen, Arne Ledet, and Noriko Yui, *Generic polynomials*, Mathematical Sciences Research Institute Publications, vol. 45, Cambridge University Press, Cambridge, 2002, Constructive aspects of the inverse Galois problem. MR 1969648

[18] Camille Jordan, *Memorie sur l'equivalence des formes*, J. Ecole Polytech, vol. 48, 1880.

[19] David Joyner, *Toric codes over finite fields*, Appl. Algebra Engrg. Comm. Comput. **15** (2004), no. 1, 63–79. MR 2142431

[20] Gregor Kemper, *Using extended Derksen ideals in computational invariant theory*, J. Symbolic Comput. **72** (2016), 161–181. MR 3369055

[21] B. È. Kunyavskiĭ, *Three-dimensional algebraic tori*, Investigations in number theory (Russian), Saratov. Gos. Univ., Saratov, 1987, Translated in Selecta Math. Soviet. **9** (1990), no. 1, 1–21, pp. 90–111. MR 1032541

[22] Serge Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. MR 1878556

[23] Nicole Lemire, *Four dimensional algebraic tori*, ArXiv: **1511.00315v3**.

[24] H. W. Lenstra, Jr., *Rational functions invariant under a finite abelian group*, Invent. Math. **25** (1974), 299–325. MR 0347788 (50 #289)

[25] Martin Lorenz, *Multiplicative invariant theory*, Encyclopaedia of Mathematical Sciences, vol. 135, Springer-Verlag, Berlin, 2005, Invariant Theory and Algebraic Transformation Groups, VI. MR 2131760 (2005m:13012)

[26] Klaus Lux and Herbert Pahlings, *Representations of groups*, Cambridge Studies in Advanced Mathematics, vol. 124, Cambridge University Press, Cambridge, 2010, A computational approach. MR 2680716

[27] Spyros S. Magliveras, Tran van Trung, and Wandi Wei, *Primitive sets in a lattice*, AUSTRALASIAN JOURNAL OF COMBINATORICS **40** (2008), 173–186.

[28] Edgar Martí nez Moro, Carlos Munuera, and Diego Ruano (eds.), *Advances in algebraic geometry codes*, Series on Coding Theory and Cryptology, vol. 5, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2008. MR 2516523

[29] Emmy Noether, *Gleichungen mit vorgeschriebener Gruppe*, Math. Ann. **78** (1917), no. 1, 221–229. MR 1511893

[30] ———, *Normalbasis bei Körpern ohne höhere Verzweigung*, J. Reine Angew. Math. **167** (1932), 147–152. MR 1581331

[31] R. A. Parker, *The computer calculation of modular characters (the meat-axe)*, Computational group theory (Durham, 1982), Academic Press, London, 1984, pp. 267–274. MR 760660

[32] Richard A. Parker, *An integral meataxe*, The atlas of finite groups: ten years on (Birmingham, 1995), London Math. Soc. Lecture Note Ser., vol. 249, Cambridge Univ. Press, Cambridge, 1998, pp. 215–228. MR 1647424

[33] Wilhelm Plesken and Bernd Souvignier, *Constructing rational representations of finite groups*, Experiment. Math. **5** (1996), no. 1, 39–47. MR 1412953

[34] A. Poli, *A deterministic construction for normal bases of abelian extensions*, Comm. Algebra **22** (1994), no. 12, 4751–4757. MR 1285704

[35] Marc Stetson Renault, *Computing generators for rings of multiplicative invariants*, ProQuest LLC, Ann Arbor, MI, 2002, Thesis (Ph.D.)–Temple University. MR 2704228

[36] Karl Rubin and Alice Silverberg, *Torus-based cryptography*, Advances in cryptology—CRYPTO 2003, Lecture Notes in Comput. Sci., vol. 2729, Springer, Berlin, 2003, pp. 349–365. MR 2093203

[37] I. R. Shafarevich, *Basic algebraic geometry*, study ed., Springer-Verlag, Berlin-New York, 1977, Translated from the Russian by K. A. Hirsch, Revised printing of Grundlehren der mathematischen Wissenschaften, Vol. 213, 1974. MR 0447223

[38] A. Speiser, *Zahlentheoretische Sätze aus der Gruppentheorie*, Math. Z. **5** (1919), no. 1-2, 1–6. MR 1544369

[39] The Stacks Project Authors, *stacks project*, http://stacks.math.columbia.edu, 2017.

[40] Bernd Sturmfels, *Algorithms in invariant theory*, second ed., Texts and Monographs in Symbolic Computation, SpringerWienNewYork, Vienna, 2008. MR 2667486

[41] Joachim von zur Gathen and Mark Giesbrecht, *Constructing normal bases in finite fields*, J. Symbolic Comput. **10** (1990), no. 6, 547–570. MR 1087979

[42] V. E. Voskresenskiĭ, *On two-dimensional algebraic tori. II*, Izv. Akad. Nauk SSSR Ser. Mat. **31** (1967), 711–716. MR 0214597 (35 #5446)

[43] ______, *Stable equivalence of algebraic tori*, Izv. Akad. Nauk SSSR Ser. Mat. **38** (1974), 3–10. MR 0342515 (49 #7261)

[44] ______, *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]. MR 1634406 (99g:20090)

[45] William C. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Mathematics, vol. 66, Springer-Verlag, New York-Berlin, 1979. MR 547117 (82e:14003)

Appendix A

A Proof of Theorem 6

This chapter is devoted to a concrete proof of Theorem 3.10. We use simillar methods to the ones we already applied in chapter 3. After reducing the lattices we compare the sublattices with the rational ones introduced in [21] and [23].

A.1 (5,6,3)

The group is generated by

$$\begin{bmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \end{bmatrix}.$$

The corresponding lattice is sign permutation. This implies rationality of the corresponding torus.

A.2 (5,18,28)

The group is generated by

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

The corresponding lattice is a sign permutation lattice. Thus it is hereditarily rational.

A.3 (5,19,14)

The group is generated by

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

The dual group is generated by

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

Algorithm (2) produces the change of basis matrix

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

With the above transformation we can see the new representative is generated by

$$\left[\begin{array}{cccc|c} 0 & 0 & 1 & -1 & 0 \\ 0 & -1 & 0 & -2 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ \hline 0 & 1 & 0 & 1 & 1 \end{array}\right] \left[\begin{array}{cccc|c} 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 2 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ \hline 0 & 0 & 0 & -1 & 1 \end{array}\right]$$

Now by considering M to be the corresponding lattice to

$$\begin{bmatrix} 0 & 0 & 1 & -1 \\ 0 & -1 & 0 & -2 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 2 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

we can produce

$$0 \longrightarrow M \longrightarrow L \longrightarrow \mathbb{Z} \longrightarrow 0.$$

The corresponding group to M has GAP ID [4,5,1,10] and also can be generated by

$$\left[\begin{array}{ccc|c} 1 & 0 & -1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & -1 & 0 \\ \hline 0 & 0 & 0 & -1 \end{array}\right] \text{ and } \left[\begin{array}{ccc|c} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & -1 \end{array}\right]$$

So M decomposes into a direct sum of a rank one sign permutation lattice (which is hereditarily rational) and a rank 3 lattice given by a group, H, generated by

$$\left[\begin{array}{cc|c} 1 & 0 & -1 \\ 0 & 1 & -1 \\ \hline 0 & 0 & -1 \end{array}\right] \text{ and } \left[\begin{array}{cc|c} 0 & 1 & 0 \\ 1 & 0 & 0 \\ \hline 0 & 0 & 1 \end{array}\right]$$

Looking at the generators of H tells us we can form

$$0 \longrightarrow \mathbb{Z}^{-} \longrightarrow L_H \longrightarrow P \longrightarrow 0$$

where P is given by the group generated by

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Since P is a permutation lattice, by Corollary 59 we can conclude that [4,5,1,10] is hereditarily rational. This implies our desired result which is hereditarily rationality of (5,19,14).

A.4 (5,22,14)

The group is generated by

$$\left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & -1 \\ \hline 0 & 0 & 0 & 0 & -1 \end{array}\right], \left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ \hline 0 & 0 & 0 & 0 & 1 \end{array}\right] \text{ and } \left[\begin{array}{cccc|c} 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

Now we define P to be the lattice corresponding to, H, generated by

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

We can see the corresponding lattice to (5,22,14), L, fits into the following exact sequence

$$0 \longrightarrow \mathbb{Z}^{-} \longrightarrow L \longrightarrow P \longrightarrow 0.$$

and since P is permutation, by Corollary 59 we can conclude that L is hereditarily rational.

A.5 (5,57,8)

The group is generated by

$$\begin{bmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 & 0 \end{bmatrix}$$

and the corresponding lattice is a sign permutation lattice which is hereditarily rational.

A.6 (5,81,54)

The group is generated by

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

The dual group is generated by

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

Algorithm (2) produces the change of basis matrix

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & -2 & 1 & -1 & -1 \end{bmatrix}$$

With the above transformation we can see the new representative is generated by

$$\left[\begin{array}{cccc|c} 1 & 2 & 0 & 2 & 0 \\ 0 & -1 & 0 & -2 & 0 \\ 0 & 2 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ \hline 0 & 1 & 0 & 1 & 1 \end{array}\right], \left[\begin{array}{cccc|c} 0 & 2 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ \hline 0 & 1 & 0 & 0 & 1 \end{array}\right] \text{ and } \left[\begin{array}{cccc|c} 1 & -2 & -2 & -2 & 0 \\ 0 & 2 & 1 & 1 & 0 \\ 0 & -2 & -1 & -2 & 0 \\ 0 & -1 & -1 & 0 & 0 \\ \hline 0 & -1 & -1 & -1 & 1 \end{array}\right]$$

Now by considering M to be the corresponding lattice to

$$\begin{bmatrix} 1 & 2 & 0 & 2 \\ 0 & -1 & 0 & -2 \\ 0 & 2 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 2 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & -2 & -2 & -2 \\ 0 & 2 & 1 & 1 \\ 0 & -2 & -1 & -2 \\ 0 & -1 & -1 & 0 \end{bmatrix}$$

we can produce

$$0 \longrightarrow M \longrightarrow L \longrightarrow \mathbb{Z} \longrightarrow 0.$$

The generators of [4,13,7,5] (another representative of the corresponding conjugacy class to M) are

$$\left[\begin{array}{ccc|c} 0 & -1 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ \hline 0 & 0 & 0 & -1 \end{array}\right], \left[\begin{array}{ccc|c} 0 & 1 & -1 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & 0 & -1 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right] \text{ and } \left[\begin{array}{ccc|c} 0 & 0 & -1 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & -1 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right]$$

The generators of rank 3 lattice are

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

the CrystCatZClass of the former group is [3,4,6,4] which is rational by [21] and its subgroups are [3, 1, 1, 1], [3, 2, 1, 2], [3, 2, 2, 2], [3, 3, 1, 4], [3, 3, 2, 4], [3, 4, 2, 2] and [3, 4, 6, 4] where all of them are rational. This implies that (5, 81, 54) is hereditarily rational.

A.7 (5,98,28)

The group is generated by

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

The dual group is generated by

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

Algorithm (1) produces the change of basis matrix

$$\begin{bmatrix} 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 2 & -2 & -1 & 1 & -2 \end{bmatrix}$$

With the above transformation we can see the new representative is generated by

$$\left[\begin{array}{cccc|c} -6 & -5 & 0 & -2 & 0 \\ 5 & 4 & 0 & 2 & 0 \\ -3 & -3 & 1 & 0 & 0 \\ 5 & 5 & 0 & 1 & 0 \\ \hline 3 & 2 & 0 & 1 & 1 \end{array}\right] \text{ and } \left[\begin{array}{cccc|c} 5 & 6 & 0 & 0 & 0 \\ -4 & -5 & 0 & 0 & 0 \\ 1 & 2 & 0 & -1 & 0 \\ -3 & -4 & -1 & 0 & 0 \\ \hline -2 & -3 & 0 & 0 & 1 \end{array}\right]$$

Now by considering M to be the corresponding lattice to

$$\begin{bmatrix} -6 & -5 & 0 & -2 \\ 5 & 4 & 0 & 2 \\ -3 & -3 & 1 & 0 \\ 5 & 5 & 0 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 5 & 6 & 0 & 0 \\ -4 & -5 & 0 & 0 \\ 1 & 2 & 0 & -1 \\ -3 & -4 & -1 & 0 \end{bmatrix}$$

we can produce

$$0 \longrightarrow M \longrightarrow L \longrightarrow \mathbb{Z} \longrightarrow 0.$$

The generators of [4,13,3,3] are

$$\left[\begin{array}{ccc|c} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & -1 \end{array}\right] \left[\begin{array}{ccc|c} 0 & 0 & -1 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & -1 & 0 \\ \hline 0 & 0 & 0 & -1 \end{array}\right]$$

The generators of rank 3 lattice are

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

the GAP ID of the former group is [3,4,6,4] which is hereditarily rational by the argument given in the previous case. So (5,98,28) is hereditarily rational.

A.8 (5,99,57)

The group is generated by

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

The dual group is generated by

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

Algorithm (1) produces the change of basis matrix

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 2 & -1 & -1 & 1 \end{bmatrix}$$

With the above transformation we can see the new representative is generated by

$$\left[\begin{array}{cccc|c} 1 & -2 & 0 & -2 & 0 \\ -1 & 0 & 0 & 1 & 0 \\ 0 & 2 & 1 & 2 & 0 \\ 1 & -1 & 0 & -2 & 0 \\ \hline 0 & 1 & 0 & 1 & 1 \end{array}\right] \text{ and } \left[\begin{array}{cccc|c} -2 & -2 & -1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 \\ -1 & -2 & -1 & -1 & 0 \\ \hline 1 & 1 & 0 & 0 & 1 \end{array}\right]$$

Now by considering M to be the corresponding lattice to

$$\begin{bmatrix} 1 & -2 & 0 & -2 \\ -1 & 0 & 0 & 1 \\ 0 & 2 & 1 & 2 \\ 1 & -1 & 0 & -2 \end{bmatrix} \text{ and } \begin{bmatrix} -2 & -2 & -1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 0 \\ -1 & -2 & -1 & -1 \end{bmatrix}$$

we can produce

$$0 \longrightarrow M \longrightarrow L \longrightarrow \mathbb{Z} \longrightarrow 0.$$

The generators of [4,12,4,7] are

$$\left[\begin{array}{ccc|c} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & -1 \end{array}\right]\left[\begin{array}{ccc|c} 0 & 0 & -1 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & -1 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right]$$

The generators of rank 3 lattice are

$$\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 & -1 \\ 1 & 0 & -1 \\ 0 & 1 & -1 \end{bmatrix}$$

the GAP ID of the former group is [3,4,6,4] which is hereditarily rational by argument given in the previous case. So (5,99,57) is hereditarily rational.

A.9 (5,164,2)

The group is generated by

$$\left[\begin{array}{cc|ccc} -1 & 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 & 0 \end{array}\right]$$

The corresponding lattice decomposes into a rank 2 lattice which is hereditarily rational and a rank 3 sign permutation lattice which is also hereditarily rational. Hence (5,164,2) is hereditarily rational.

A.10 (5,174,2)

The group is generated by

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

The dual group is generated by

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

Algorithm (1) produces the change of basis matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & -1 & 0 & 0 & -1 \end{bmatrix}$$

With the above transformation we can see the new representative is generated by

$$\left[\begin{array}{cccc|c} 0 & -1 & 1 & 0 & 0 \\ -1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ \hline 0 & 0 & -1 & -1 & 1 \end{array}\right] \text{ and } \left[\begin{array}{cccc|c} -1 & 0 & 0 & -1 & 0 \\ 0 & -1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ \hline 1 & -1 & 0 & 0 & 1 \end{array}\right]$$

Now by considering M to be the corresponding lattice to

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

we can produce

$$0 \longrightarrow M \longrightarrow L \longrightarrow \mathbb{Z} \longrightarrow 0.$$

The generators of [4,17,13] are

$$\left[\begin{array}{cc|cc} -1 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & -1 \end{array}\right] \text{ and } \left[\begin{array}{cc|cc} -1 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \hline 0 & 0 & -1 & -1 \\ 0 & 0 & 1 & 0 \end{array}\right]$$

and the lattice decomposes into rank 2 lattices which we know they are hereditarily rational. This implies that (5,174,2) is hereditarily rational.

A.11 (5,174,5)

The group is generated by

$$\left[\begin{array}{cc|ccc} -1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{array}\right] \text{ and } \left[\begin{array}{cc|ccc} -1 & -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \end{array}\right]$$

and the lattice decomposes into a rank 2 lattice and a rank 3 sign permutation lattice, both of which are hereditarily rational. This implies that (5,174,5) is hereditarily rational.

A.12 (5,389,4)

The group is generated by

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

The dual group is generated by

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

Algorithm (1) produces the change of basis matrix

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & -1 \end{bmatrix}$$

With the above transformation we can see the new representative is generated by

$$\left[\begin{array}{cccc|c} 1 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ \hline 0 & 0 & -1 & 0 & 1 \end{array}\right] \text{ and } \left[\begin{array}{cccc|c} 0 & 0 & 0 & 1 & 0 \\ -1 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ \hline 0 & 0 & -1 & 0 & 1 \end{array}\right]$$

Now by considering M to be the corresponding lattice to

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

we can produce

$$0 \longrightarrow M \longrightarrow L \longrightarrow \mathbb{Z} \longrightarrow 0.$$

the above group is [4,21,3,2] which has the following subgroups [4, 1, 1, 1], [4, 3, 1, 3], [4, 5, 1, 1], [4, 11, 1, 1], [4, 17, 1, 2], [4, 17, 1, 3], [4, 21, 1, 1] and [4, 21, 3, 2] where all of them are rational.

A.13 (5,901,3)

The group is generated by

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

The dual group is generated by

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

Algorithm (1) produces the change of basis matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & -1 \end{bmatrix}$$

With the above transformation we can see the new representative is generated by

$$\left[\begin{array}{cccc|c} -1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & -1 & 0 \\ -1 & 0 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 & 1 \end{array}\right] \text{ and } \left[\begin{array}{cccc|c} -1 & 0 & 0 & -1 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 & 1 \end{array}\right]$$

Now by considering M to be the corresponding lattice to

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

we can produce

$$0 \longrightarrow M \longrightarrow L \longrightarrow \mathbb{Z} \longrightarrow 0.$$

The lattice M corresponds to [4,27,3,1] with subgroups [4, 1, 1, 1], [4, 3, 1, 3], [4, 27, 1, 1], [4, 27, 3, 1] where all of them are rational. So (5,901,3) is hereditarily rational.

A.14 (5,918,4)

The group is generated by

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

The dual group is generated by

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

Algorithm (1) produces the change of basis matrix

$$\begin{bmatrix} 0 & 1 & 1 & -2 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

With the above transformation we can see the new representative is generated by

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ -1 & 0 & -1 & 0 & 0 \\ -2 & 1 & -1 & 0 & 0 \\ 2 & 0 & 1 & 0 & 0 \\ -1 & 0 & -1 & 0 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} -1 & -1 & -1 & -1 & 0 \\ 1 & -1 & 1 & 0 & 0 \\ 1 & 1 & 2 & 2 & 0 \\ -1 & 0 & -2 & -1 & 0 \\ 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Now by considering M to be the corresponding lattice to

$$\begin{bmatrix} 1 & 0 & 1 & 1 \\ -1 & 0 & -1 & 0 \\ -2 & 1 & -1 & 0 \\ 2 & 0 & 1 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & 0 \\ 1 & 1 & 2 & 2 \\ -1 & 0 & -2 & -1 \end{bmatrix}$$

we can produce

$$0 \longrightarrow M \longrightarrow L \longrightarrow \mathbb{Z} \longrightarrow 0.$$

The lattice M corresponds to [4,31,1,2] which is a subgroup of [4, 31, 7, 1]. In [23] it is shown that [4, 31, 7, 1] is hereditarily rational and so is (5,918,4).

Appendix B

Related Lists to Rationality Results

Carat ID	Carat ID	Carat ID	Carat ID	Carat ID	Carat ID
(5, 18, 27)	(5, 19, 14)	(5, 22, 14)	(5, 23, 27)	(5, 28, 8)	(5, 28, 16)
(5, 28, 27)	(5, 30, 8)	(5, 30, 16)	(5, 30, 29)	(5, 30, 33)	(5, 31, 41)
(5, 31, 49)	(5, 32, 13)	(5, 32, 31)	(5, 32, 40)	(5, 32, 46)	(5, 32, 49)
(5, 32, 52)	(5, 32, 55)	(5, 32, 56)	(5, 32, 59)	(5, 37, 5)	(5, 37, 7)
(5, 38, 10)	(5, 39, 7)	(5, 74, 9)	(5, 74, 18)	(5, 75, 9)	(5, 75, 18)
(5, 75, 28)	(5, 75, 37)	(5, 75, 41)	(5, 78, 37)	(5, 78, 41)	(5, 81, 12)
(5, 81, 25)	(5, 81, 38)	(5, 81, 42)	(5, 81, 48)	(5, 81, 49)	(5, 81, 50)
(5, 81, 51)	(5, 81, 54)	(5, 82, 12)	(5, 82, 25)	(5, 84, 9)	(5, 84, 18)
(5, 92, 9)	(5, 92, 16)	(5, 98, 12)	(5, 98, 16)	(5, 98, 19)	(5, 98, 22)
(5, 98, 24)	(5, 98, 25)	(5, 98, 28)	(5, 99, 12)	(5, 99, 22)	(5, 99, 29)
(5, 99, 41)	(5, 99, 45)	(5, 99, 51)	(5, 99, 52)	(5, 99, 53)	(5, 99, 54)
(5, 99, 57)	(5, 100, 22)	(5, 100, 29)	(5, 101, 9)	(5, 101, 16)	(5, 101, 22)
(5, 102, 16)	(5, 102, 22)	(5, 103, 12)	(5, 103, 16)	(5, 103, 19)	(5, 103, 22)
(5, 103, 24)	(5, 103, 25)	(5, 103, 28)	(5, 106, 5)	(5, 108, 5)	(5, 108, 11)
(5, 108, 15)	(5, 110, 11)	(5, 110, 15)	(5, 114, 4)	(5, 117, 4)	(5, 117, 8)
(5, 117, 13)	(5, 117, 18)	(5, 118, 4)	(5, 118, 8)	(5, 120, 18)	(5, 120, 22)
(5, 121, 4)	(5, 121, 8)	(5, 121, 12)	(5, 122, 11)	(5, 126, 5)	(5, 131, 15)
(5, 131, 19)	(5, 133, 4)	(5, 133, 8)	(5, 133, 13)	(5, 133, 18)	(5, 137, 4)
(5, 138, 5)	(5, 138, 11)	(5, 156, 4)	(5, 160, 8)	(5, 161, 4)	(5, 161, 8)
(5, 162, 4)	(5, 162, 8)	(5, 222, 9)	(5, 222, 10)	(5, 223, 11)	(5, 223, 12)
(5, 224, 10)	(5, 225, 11)	(5, 225, 12)	(5, 226, 11)	(5, 226, 12)	(5, 226, 23)
(5, 226, 24)	(5, 227, 12)	(5, 230, 14)	(5, 230, 15)	(5, 231, 11)	(5, 231, 12)
(5, 232, 15)	(5, 242, 10)	(5, 243, 9)	(5, 243, 10)	(5, 245, 11)	(5, 245, 12)
(5, 267, 4)	(5, 268, 4)	(5, 271, 4)	(5, 272, 4)	(5, 275, 8)	(5, 277, 4)
(5, 292, 4)	(5, 293, 4)	(5, 302, 8)	(5, 304, 8)	(5, 306, 8)	(5, 307, 6)
(5, 308, 8)	(5, 308, 12)	(5, 337, 12)	(5, 341, 6)	(5, 389, 4)	(5, 390, 4)
(5, 391, 4)	(5, 391, 8)	(5, 392, 4)	(5, 404, 4)	(5, 409, 4)	(5, 410, 6)

(5, 413, 5)	(5, 414, 7)	(5, 416, 4)	(5, 424, 6)	(5, 426, 5)	(5, 434, 4)
(5, 435, 5)	(5, 436, 4)	(5, 461, 4)	(5, 462, 4)	(5, 465, 6)	(5, 501, 4)
(5, 519, 9)	(5, 519, 14)	(5, 520, 5)	(5, 520, 8)	(5, 520, 14)	(5, 521, 5)
(5, 521, 8)	(5, 521, 14)	(5, 521, 15)	(5, 522, 9)	(5, 522, 14)	(5, 522, 15)
(5, 524, 7)	(5, 529, 7)	(5, 529, 17)	(5, 531, 7)	(5, 531, 13)	(5, 531, 16)
(5, 533, 7)	(5, 533, 8)	(5, 537, 7)	(5, 538, 7)	(5, 541, 7)	(5, 580, 4)
(5, 606, 4)	(5, 607, 4)	(5, 607, 9)	(5, 608, 4)	(5, 608, 9)	(5, 623, 4)
(5, 623, 9)	(5, 640, 2)	(5, 641, 2)	(5, 644, 2)	(5, 645, 2)	(5, 655, 4)
(5, 656, 4)	(5, 665, 2)	(5, 666, 2)	(5, 668, 4)	(5, 670, 5)	(5, 671, 5)
(5, 672, 4)	(5, 674, 4)	(5, 684, 5)	(5, 687, 5)	(5, 689, 4)	(5, 696, 5)
(5, 700, 4)	(5, 703, 4)	(5, 704, 7)	(5, 704, 11)	(5, 705, 4)	(5, 705, 9)
(5, 705, 11)	(5, 706, 4)	(5, 706, 14)	(5, 707, 4)	(5, 709, 7)	(5, 710, 4)
(5, 711, 4)	(5, 713, 4)	(5, 715, 4)	(5, 726, 4)	(5, 742, 4)	(5, 750, 4)
(5, 750, 8)	(5, 753, 4)	(5, 754, 4)	(5, 754, 8)	(5, 756, 4)	(5, 758, 4)
(5, 760, 4)	(5, 760, 8)	(5, 762, 4)	(5, 763, 7)	(5, 763, 11)	(5, 773, 2)
(5, 774, 2)	(5, 785, 5)	(5, 801, 3)	(5, 822, 2)	(5, 823, 2)	(5, 846, 2)
(5, 852, 3)	(5, 853, 3)	(5, 854, 4)	(5, 855, 4)	(5, 856, 2)	(5, 869, 4)
(5, 870, 3)	(5, 889, 3)	(5, 890, 3)	(5, 891, 2)	(5, 892, 2)	(5, 900, 2)
(5, 901, 3)	(5, 902, 2)	(5, 904, 3)	(5, 909, 2)	(5, 910, 3)	(5, 910, 4)
(5, 911, 3)	(5, 911, 4)	(5, 912, 3)	(5, 912, 4)	(5, 917, 3)	(5, 917, 4)
(5, 918, 3)	(5, 918, 4)	(5, 919, 3)	(5, 919, 4)	(5, 926, 5)	(5, 926, 6)
(5, 931, 3)	(5, 931, 4)	(5, 933, 1)	(5, 934, 1)	(5, 935, 1)	(5, 936, 1)
(5, 937, 1)	(5, 938, 1)	(5, 939, 1)	(5, 940, 1)	(5, 941, 1)	(5, 942, 1)
(5, 943, 1)	(5, 944, 1)	(5, 945, 1)	(5, 946, 2)	(5, 946, 4)	(5, 947, 2)
(5, 947, 4)	(5, 951, 4)	(5, 952, 2)	(5, 952, 4)	(5, 953, 4)	

Table B.1: The 311 indecomposable stably rational 5 dimensional algebraic tori with an indecomposable character lattice.

Carat ID	Carat ID	Carat ID	Carat ID	Carat ID	Carat ID
(5, 31, 41)	(5, 31, 49)	(5, 32, 46)	(5, 32, 49)	(5, 32, 52)	(5, 38, 10)
(5, 39, 7)	(5, 78, 37)	(5, 78, 41)	(5, 81, 42)	(5, 81, 48)	(5, 81, 50)
(5, 98, 16)	(5, 98, 22)	(5, 98, 24)	(5, 99, 52)	(5, 99, 53)	(5, 99, 54)
(5, 100, 22)	(5, 100, 29)	(5, 102, 16)	(5, 102, 22)	(5, 103, 16)	(5, 103, 22)
(5, 103, 24)	(5, 110, 11)	(5, 110, 15)	(5, 118, 4)	(5, 118, 8)	(5, 120, 18)
(5, 120, 22)	(5, 122, 11)	(5, 131, 15)	(5, 131, 19)	(5, 160, 8)	(5, 162, 4)
(5, 162, 8)	(5, 224, 10)	(5, 227, 12)	(5, 232, 15)	(5, 242, 10)	(5, 267, 4)
(5, 271, 4)	(5, 275, 8)	(5, 292, 4)	(5, 302, 8)	(5, 304, 8)	(5, 306, 8)
(5, 337, 12)	(5, 390, 4)	(5, 391, 4)	(5, 392, 4)	(5, 404, 4)	(5, 410, 6)
(5, 414, 7)	(5, 416, 4)	(5, 424, 6)	(5, 426, 5)	(5, 434, 4)	(5, 435, 5)
(5, 465, 6)	(5, 521, 15)	(5, 522, 15)	(5, 533, 8)	(5, 607, 4)	(5, 608, 4)
(5, 623, 4)	(5, 641, 2)	(5, 645, 2)	(5, 655, 4)	(5, 666, 2)	(5, 670, 5)
(5, 671, 5)	(5, 674, 4)	(5, 703, 4)	(5, 704, 7)	(5, 704, 11)	(5, 706, 4)
(5, 706, 14)	(5, 709, 7)	(5, 710, 4)	(5, 715, 4)	(5, 753, 4)	(5, 754, 4)
(5, 754, 8)	(5, 758, 4)	(5, 763, 7)	(5, 763, 11)	(5, 774, 2)	(5, 801, 3)
(5, 822, 2)	(5, 846, 2)	(5, 852, 3)	(5, 854, 4)	(5, 856, 2)	(5, 869, 4)
(5, 870, 3)	(5, 889, 3)	(5, 890, 3)	(5, 891, 2)	(5, 910, 4)	(5, 912, 4)
(5, 917, 4)	(5, 919, 4)	(5, 926, 6)	(5, 946, 2)	(5, 946, 4)	(5, 947, 2)
(5, 952, 2)					

Table B.2: The cases among the 311 groups whose rationality is unknown (109 cases).

Carat ID	Carat ID	Carat ID	Carat ID	Carat ID	Carat ID
(5, 31, 41)	(5, 31, 49)	(5, 32, 46)	(5, 32, 49)	(5, 32, 52)	(5, 38, 10)
(5, 39, 7)	(5, 78, 37)	(5, 78, 41)	(5, 81, 42)	(5, 81, 48)	(5, 81, 50)
(5, 98, 16)	(5, 98, 22)	5, 98, 24)	(5, 99, 52)	(5, 99, 53)	(5, 99, 54)
(5, 100, 22)	(5, 100, 29)	(5, 102, 16)	(5, 102, 22)	(5, 103, 16)	(5, 103, 22)
(5, 103, 24)	(5, 110, 11)	(5, 110, 15)	(5, 118, 4)	(5, 118, 8)	(5, 120, 18)
(5, 120, 22)	(5, 122, 11)	(5, 131, 15)	(5, 131, 19)	(5, 160, 8)	(5, 162, 4)
(5, 162, 8)	(5, 224, 10)	(5, 227, 12)	(5, 232, 15)	(5, 242, 10)	(5, 267, 4)
(5, 271, 4)	(5, 275, 8)	(5, 292, 4)	(5, 302, 8)	(5, 304, 8)	(5, 306, 8)
(5, 337, 12)	(5, 390, 4)	(5, 391, 4)	(5, 392, 4)	(5, 404, 4)	(5, 410, 6)
(5, 414, 7)	(5, 416, 4)	(5, 424, 6)	(5, 426, 5)	(5, 434, 4)	(5, 435, 5)
(5, 465, 6)	(5, 521, 15)	(5, 522, 15)	(5, 533, 8)	(5, 641, 2)	(5, 645, 2)
(5, 655, 4)	(5, 666, 2)	(5, 670, 5)	(5, 671, 5)	(5, 674, 4)	(5, 703, 4)
(5, 704, 7)	(5, 704, 11)	(5, 706, 4)	(5, 706, 14)	(5, 709, 7)	(5, 710, 4)
(5, 715, 4)	(5, 753, 4)	(5, 754, 4)	(5, 754, 8)	(5, 758, 4)	(5, 763, 7)
(5, 763, 11)	(5, 774, 2)	(5, 801, 3)	(5, 822, 2)	(5, 846, 2)	(5, 852, 3)
(5, 854, 4)	(5, 856, 2)	(5, 869, 4)	(5, 870, 3)	(5, 889, 3)	(5, 890, 3)
(5, 891, 2)	(5, 910, 4)	(5, 912, 4)	(5, 917, 4)	(5, 919, 4)	(5, 926, 6)

Table B.3: The groups in the previous table on which Algorithm (2) works (102 cases).

Curriculum Vitae

Name:	Armin Jamshidpey
Post-Secondary Education and Degrees:	Western University London, Ontario, Canada 2013- 2017 Ph.D. Mathematics
	Visiting Ph.D. student at The University of Waterloo Waterloo, Ontario, Canada 2015- 2017
	Institute for advanced studies in Basic Sciences Zanjan, Iran 2010 - 2012 M.Sc. Mathematics
	Guilan University Rasht, Iran 2004 - 2009 B.Sc. Mathematics
Related Work Experience:	Teaching Assistant The University of Western Ontario 2013-2017
	Lecturer The University of Western Ontario Sep. 2016- Dec. 2016.