The Essential Dimension of Low Dimensional Tori via Lattices

Gareth Case

Department of Mathematics and Statistics

Lancaster University

A thesis presented for the degree of

Doctor of Philosophy

May 2019

Declaration

I declare that the present thesis was prepared by me and none of its contents were obtained by means that are against the law. I also declare that the present thesis is a part of a Ph.D. Programme at Lancaster University. This thesis has never before been a subject of any procedure of obtaining an academic degree.

Gareth Case

May 2019

Acknowledgements

A Ph.D. thesis may seem like a solitary undertaking, but there are many people that go in to making it a reality; here is a small subset I would like to single out.

Firstly, to my supervisor, Dr Mark MacDonald, for his ever-present encouragement and guidance. There was always time in his busy schedule for a friendly meeting to discuss my half-baked mathematical ideas, offering a great deal of clarity with a thoughtful question or comment. I am lucky to have had a supervisor from whom I have learned such a lot, not solely in mathematics, but in effective teaching and presenting. I will take these skills with me as I leave Lancaster, and for that I will be forever grateful. To my external examiner Professor Martin Liebeck, thank you for your patience and time; your input improved this thesis considerably. To my internal examiner, and bee-keeping HDC chair Dr Nadia Mazza, who always gave insightful comments and direction for study. Your feedback in the viva was invaluable. To my loving parents, your constant support and wise words kept the boat on course, through both calm and turbulent waters. Lastly to my wife, Faron. Thanks for being the Sam to my Frodo; I dedicate this thesis to you. I will always remember your sage advice on how one should go about eating an elephant.

Abstract

The essential dimension, $\mathrm{ed}_k(G)$, of an algebraic group G is an invariant that measures the complexity of G-torsors over fields. The correspondence between algebraic tori and finite subgroups of $\mathrm{GL}_n(\mathbb{Z})$ means one can establish bounds on $\mathrm{ed}_k(T)$ of an algebraic torus T by studying the action of the corresponding subgroup of $\mathrm{GL}_n(\mathbb{Z})$ acting on the character lattice $T^* \cong \mathbb{Z}^n$. Specifically, the action has a combinatorial property called the *symmetric p-rank*; this thesis is written to explore this notion, giving bounds on the essential dimension, and its p-local version the essential p-dimension, of algebraic tori and related groups.

Contents

Chapter 1

Introduction

The essential dimension was introduced formally in 1997 by Buhler and Reichstein [6] in their work on finite Galois field extensions with a given Galois group. It has subsequently been defined for a variety of algebraic objects, and the value of the essential dimension is often connected with profound results about that underlying object. In general, the essential dimension is difficult to calculate and the task is split into finding upper and lower bounds. Lower bounds are often given by the essential p-dimension, a p-local version which is usually easier to calculate.

This thesis aims to calculate the essential (p)-dimension of various algebraic groups, specifically algebraic tori and extensions of small finite groups by algebraic tori. The groundwork for this was laid in [28, Corollary 5.1] where it was was shown that the essential p-dimension of algebraic tori could be calculated as a result of data on the Galois group action on its character lattice, known as the *symmetric p-rank*. This property was calculated in [30] for the actions of the Weyl groups on character lattices

of maximal tori in semisimple algebraic groups, which in turn gave bounds on the wider question of $\mathrm{ed}_k(G)$ for semisimple algebraic groups G.

This thesis roughly takes the following trajectory. Chapter 2 introduces the necessary foundations in algebraic groups, Galois cohomology and lattices. Algebraic groups are viewed from a scheme-theoretic viewpoint, following [37], and the essential dimension is introduced and discussed in Chapter 3. The original work in this thesis can be found in the final two chapters; Chapter 4 is dedicated to calculating the symmetric p-rank, with a special emphasis on complex reflection groups of degree 3 or more. For each such group $\mathcal{G}$, there is shown to be a natural choice of lattice L defined such that $\mathcal{G}$ acts as a symmetry of L. The symmetric p-ranks are calculated by studying the geometry of L, and Table 4.2 summarises these results. The symmetric p-ranks of the automorphism group of the Leech lattice are also found, in Table 4.5. Also included is an implementation of a method given by Merkurjev [33, Thm. 4.3] (see also Proposition 4.0.6) in MAGMA, which finds the values of the symmetric p-ranks of the automorphism group of every irreducible finite maximal subgroup (up to conjugacy) of $\mathrm{GL}_n(\mathbb{Z})$, for $n \leq 9$, which is shown in Table 4.1. The code for this algorithm can be found in Appendix C.1.1.

Finally, Chapter 5 shifts the focus of study to extensions of some small finite groups by algebraic tori. Here, the value of the symmetric p-rank provides a valuable bound on the essential (p)-dimension of such groups, but gaining the exact value is a more substantial task and requires a subtle approach. For certain small finite groups $F = \{\mathcal{C}_p, \mathcal{C}_{p^2}, \mathcal{C}_2 \times \mathcal{C}_2, D_{2p}\}$ (p prime), the essential (p)-dimension is calculated for all extensions of F by algebraic tori, subject to some conditions of the base field.

Chapter 2

Preliminaries

2.1 Algebraic schemes

This chapter lays the groundwork in algebraic groups, lattices and cohomology that is necessary for the topics covered in the rest of this work. It should be noted that none is the author's own work, and comes directly from several sources; namely [37] on algebraic groups, [26] and [8] on lattices, and [5] and [43] on group and Galois cohomology. The author has endeavoured to approach topics in the language of category theory, definitions in this area can be found in [31].

For a field k, the category of k-algebras, $\mathbf{Alg_k}$, has as objects finitely generated commutative algebras over k, and morphisms all k-algebra homomorphisms. If A is an object in $\mathbf{Alg}_k$, the topological space $X := \mathrm{Spec}(A)$ is defined as the set of prime ideals $\mathfrak{p}$ in A, endowed with the Zariski topology. To each open subset $U \subset \mathrm{Spec}(A)$ can be associated a multiplicative subset of A, $S_U := A \setminus \bigcup\{\mathfrak{p} \mid \mathfrak{p} \in U\}$. Localising

A at S_U, $S_U^{-1}A := \{\frac{a}{s} \mid a \in A,\ s \in S_U\}$ gives an object in $\mathbf{Alg}_k$. This k-algebra is denoted by $\mathcal{O}_X(U)$ for the open subset $U \subset X$, and endows X with a *sheaf* of k-algebras $\mathcal{O}_X$.

An *affine algebraic scheme over* k is a topological space X endowed with a sheaf of k-algebras $\mathcal{O}_X$, that is isomorphic to $\mathrm{Spec}(A)$ for some k-algebra $A \in \mathbf{Alg_k}$, called the *coordinate algebra* of X. A morphism of affine algebraic schemes $f : X \to Y$ is a continuous map and a collection of ring homomorphisms, one for each open subset $U \subset Y$, $\varphi_U : \mathcal{O}_Y(U) \to \mathcal{O}_X(f^{-1}(U))$ such that for two open subsets $U_1 \subset U_2$ of Y, the following diagram commutes

$$\begin{array}{ccc} \mathcal{O}_Y(U_2) & \xrightarrow{\varphi_{U_2}} & \mathcal{O}_X(f^{-1}(U_2)) \\ \downarrow & & \downarrow \\ \mathcal{O}_Y(U_1) & \xrightarrow{\varphi_{U_1}} & \mathcal{O}_X(f^{-1}(U_1)). \end{array} \tag{2.1}$$

For each $f \in A$, the subset $D(f) := \{\mathfrak{p} \mid f \notin \mathfrak{p}\}$ of $\mathrm{Spec}(A)$ are the *principal open sets* and form a base for the topology on $\mathrm{Spec}(A)$.

Proposition 2.1.1. [36, Proposition 3.14] *There is a contravariant equivalence of categories between the category of finitely generated k-algebras $\mathbf{Alg_k}$ and the category of affine algebraic schemes over k, $\mathbf{Sch}_{aff}$.*

Proof. If $\alpha : A \to B$ is a morphism of finitely generated k-algebras, then it induces a unique map $\alpha^* : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$; $\mathfrak{p} \mapsto \alpha^{-1}(\mathfrak{p})$. This is well defined (the preimage of a prime ideal is prime) and continuous as $(\alpha^*)^{-1}(D(f)) = D(\alpha(f))$. The functor $A \mapsto \mathrm{Spec}(A)$ is therefore fully faithful, so induces an equivalence of categories between $\mathbf{Alg_k}$ and its image under Spec, which by definition is $\mathbf{Sch}_{\mathrm{aff}}$. □

Using these affine pieces, one builds the notion of an *algebraic scheme*, which is a topological space X with a sheaf of k-algebras $\mathcal{O}_X$, such that there exists a finite collection of open subsets (or *covering*) U_i of X, where the U_i are affine algebraic schemes, and $\bigcup U_i = X$. The notion of a morphism of algebraic schemes naturally extends from that of affine algebraic schemes in (2.1).

Example 2.1.2. Consider the affine plane without the origin, $V := \mathbb{A}^2 \setminus \{0\}$. Then there is no k-algebra A such that $V = \mathrm{Spec}(A)$. However, there exists affine algebraic schemes $V_x := \mathbb{A}^1 \setminus \{0\} = \mathrm{Spec}(k[x,y]/(x))$ and $V_y := \mathbb{A}^1 \setminus \{0\} = \mathrm{Spec}(k[x,y]/(y))$, that cover V, so V is an algebraic scheme.

Given a k-algebra R, and K/k a field extension of k, $R_K := K \otimes R$ defines an algebra over K. For a scheme X over k, this enables the definition of a new sheaf of K-algebras, $K \otimes_k \mathcal{O}_X(U)$ for all open subsets U, so the scheme X has the structure of an algebraic scheme over K, denoted X_K. This construction defines a functor, $X \mapsto X_K$ which takes an algebraic scheme over k to a scheme over K. For instance, if X is affine, then $X := \mathrm{Spec}(A) \to X_K := \mathrm{Spec}(K \otimes A)$.
The *height* of a prime ideal $\mathfrak{p}$ is the greatest length, n, of a chain of distinct prime ideals

$$\mathfrak{p} = \mathfrak{p}_n \supset \ldots \supset \mathfrak{p}_0 = \{0\}.$$

The *Krull dimension* of $A \in \mathbf{Alg}_k$ is the supremum of the heights of all prime ideals $\mathfrak{p} \subset A$. Likewise, the dimension of an algebraic scheme X over k is the length n, of the largest chain of distinct closed irreducible subschemes of X, and for affine $X = \mathrm{Spec}(A)$, it is clear that the Krull dimension of A and the dimension of X correspond. Indeed if $U \subset X$ is any open set of X, then $\dim(X) = \dim(U)$, so the

dimension of any algebraic scheme X, $\dim(X)$ is equal to the Krull dimension of A, where $\mathrm{Spec}(A) \subset X$ is an open set in X.

A point in a scheme $x \in X$ over k lies in an open neighbourhood $U \subset X$, so $x \in U = \mathrm{Spec}(A)$ corresponds to some prime ideal $\mathfrak{p} \subset A$, $A \in \mathbf{Alg}_k$. If $A_\mathfrak{p}$ denotes the localisation of A at $\mathfrak{p}$, then the *residue field* of x, $k(x)$ is defined as

$$k(x) := A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}. \tag{2.2}$$

This definition does not depend on the choice of the open neighbourhood and for a field K/k, x is *K-rational* if $k(x) \subset K$. The transcendence degree of $k(x)$ over k gives the Krull dimension of the corresponding prime ideal (see [20, pp. 87-88]) so also $\dim(X) = \sup \mathrm{tr.deg}(k(x))$ for x running over X.

For any k-algebra R, the *set of points of R in the scheme X* is defined by

$$X(R) := \mathrm{Hom}(\mathrm{Spec}(R), X), \tag{2.3}$$

in the category of algebraic schemes, **Sch** (see [37, A.16, pp. 494]). If $X := \mathrm{Spec}(A)$ is affine, then $X(R) = \mathrm{Hom}(\mathrm{Spec}(R), \mathrm{Spec}(A)) = \mathrm{Hom}_{\mathrm{alg}}(A, R)$ due to Proposition 2.1.1. This leads to the identification of algebraic schemes to their *functor of points*. A functor $\mathcal{F} : \mathcal{C} \to \mathbf{Set}$ is *representable* if there exists an $A \in \mathcal{C}$ such that $\mathcal{F}$ is naturally isomorphic to the Hom functor $h^A := \mathrm{Hom}(-, A)$. Yoneda's Lemma ([31, pp.61]) implies that the functor from $\mathbf{Alg_k}$ to **Set** that sends $R \mapsto X(R)$ is fully faithful, so an algebraic scheme X is defined up to unique isomorphism by this functor and thus can be identified as a representable functor $\mathcal{F} : \mathbf{Alg_k} \to \mathbf{Set}$.

An algebraic scheme X is *separated* if the image of the diagonal $\Delta : X \to X \times$

X; $\Delta(x) \mapsto (x, x)$ is closed, and *reduced* if the elements of $\mathcal{O}_X$ contain no non-zero nilpotent elements. X is *geometrically reduced* if $X_{\overline{k}} := X \otimes \overline{k}$ is reduced for $\overline{k}$ the algebraic closure of k and an *algebraic variety* is a scheme which is both separated and geometrically reduced.

If $X \in \mathbf{Sch}_{\text{aff}}$ then there exists some k-algebra $A = k[T_1, \ldots, T_n]/(f_1, \ldots, f_m)$ such that $X = \text{Spec}(A)$ and a point x is *smooth* if the derivatives $\frac{\partial f_i}{\partial t_j}$, $1 \leq i \leq m$, $1 \leq j \leq n$ are not all zero. If this is true for all $x \in X$, then X is also said to be smooth. More generally, an algebraic scheme is smooth if each point has an open neighbourhood which is a smooth affine scheme.

2.2 Algebraic groups

A separated algebraic scheme G is an *algebraic group* if there exists morphisms that bestow on G the structure of a group. That is to say there exists an identity element $e \in G$, and morphisms $\mu : G \times G \to G$; $\mu(x, y) \mapsto xy$ and $\iota : G \to G$; $\iota(x) \mapsto x^{-1}$ that obey the usual group axioms. As an algebraic scheme, an algebraic group G gives a representable functor $\mathcal{F} : \mathbf{Alg_k} \to \mathbf{Set}$, where $R \mapsto G(R)$. Extending to a functor $R \mapsto (G(R), \mu(R))$ gives an identification of G as a functor $\mathbf{Alg_k} \to \mathbf{Grp}$. In this sense, G is called a *group functor*.

Remark 2.2.1. The underlying scheme needs to be separated otherwise elements of the form gh^{-1} would not be closed in G.

The underlying scheme is a finite union of irreducible components, and the component containing the identity element is denoted by G°. If $G^\circ = G$, (i.e. the underlying

scheme is irreducible), then the group is *connected*.

The multiplication map μ on an affine algebraic group corresponds to the *comultiplication map* on the coordinate algebra $\mathcal{O}(G)$ of G, $\Delta : \mathcal{O}(G) \to \mathcal{O}(G) \otimes \mathcal{O}(G)$. This gives the coordinate algebra the structure of a *Hopf* algebra, which is an algebra over k with the following algebra morphisms

$$\Delta : A \to A \otimes A \tag{2.4}$$

$$\iota : A \to A \tag{2.5}$$

$$\epsilon : A \to k. \tag{2.6}$$

These are the co-multiplication, co-inverse and co-unit maps which satisfy certain properties on A that mirror the group axioms on G. Just as a k-algebra defines an affine algebraic scheme, if A is a Hopf algebra k, then $\mathrm{Spec}(A)$ defines an affine algebraic group and likewise the representable functor $\mathbf{Alg_k} \to \mathbf{Grp}$ defined by $R \mapsto \mathrm{Hom}(A, R^\times)$ is the functor of points of the algebraic group $G(R)$. Morphisms of algebraic groups are simply morphisms of algebraic schemes, that are also homomorphisms of groups.

The following are some important basic examples of algebraic groups that will be referred to throughout. For V a vector space of dimension n over k, the group $\mathrm{GL}(V)$ is defined as the group of k-linear automorphisms of V. This defines an affine algebraic group, as $\mathrm{GL}(V) = \mathrm{Spec}(k[T_1, \ldots T_n]/\det(T_i))$. In the language of group functors, $\mathrm{GL}(V)$ has the following description,

$$R \mapsto \mathrm{Aut}_R(V_R), \tag{2.7}$$

where $\mathrm{Aut}_R(V)$ is all R-linear automorphisms of V. If $n \geq 1$ is an integer, one can define the n-th roots of unity as an algebraic group,

$$\mu_n = \mathrm{Spec}(k[T]/(T^n - 1)). \tag{2.8}$$

The Hopf algebra has comultiplication map given by $\Delta(T) = T \otimes T$, and it is the group functor $R \mapsto \{r \in R \mid r^n = 1\}$.

The last example is the multiplicative group, $\mathbb{G}_m$, which consists of the multiplicative elements of the underlying field. The underlying Hopf algebra is $k[T, T^{-1}]$, with the same comultiplication map as μ_n. As a group functor, $R \mapsto R^\times$.

Example 2.2.2. All abstract finite groups give rise to an algebraic group. Indeed, if F is such a group, then $F_k := \mathrm{Spec}(\underbrace{k \times \cdots \times k}_{|F| \text{ times}})$. F_k is the following functor of points $R \mapsto \mathrm{Hom}(\pi_0(\mathrm{Spec}(R)), F)$, where $\pi_0(X)$ is the variety whose points correspond to the connected components of X, known as the *variety of connected components* of X.

Remark 2.2.3. Note that μ_m and the constant algebraic group associated to $\mathbb{Z}/m\mathbb{Z}$ are not the same as algebraic groups. To illustrate, suppose m is a prime. If the field is algebraically closed, then these are isomorphic as groups. However, $|\mu_m(K)| = 1$ and $|(\mathbb{Z}/m\mathbb{Z})(K)| = m$ for all fields K of characteristic dividing m.

A representation of an algebraic group G is a vector space V and a morphism $\rho : G \to \mathrm{GL}(V)$. Analogously to regular groups, a representation (V, ρ) is equivalent to an action of the group on a module; in this case, for all k-algebras, there is an action of $G(R)$ on the module $R \otimes V$. This module induces a co-action on the co-module of

$\mathcal{O}(G)$, which is a map $\phi : V \to V \otimes \mathcal{O}(G)$, linear over k, such that

$$(\mathrm{id}_V \otimes \Delta) \circ \phi = (\phi \otimes \mathrm{id}_{\mathcal{O}(G)}) \circ \phi, \tag{2.9}$$

$$(\mathrm{id}_V \otimes \epsilon) \circ \phi = \mathrm{id}_V. \tag{2.10}$$

In the special case where $V = k$, then a representation $\chi : G \to \mathbb{G}_m$ is a *character*. The set of characters of an algebraic group G is denoted G^*, and has the structure of an abelian group; with the sum of χ and χ' given by

$$(\chi + \chi')(g) = \chi(g)\chi'(g). \tag{2.11}$$

2.3 Multiplicative groups

If M is a finitely generated abelian group, then the group algebra $k[M]$ has the structure of a Hopf algebra, by defining the maps $\Delta(m) \to m \otimes m$, $\epsilon(m) \to 1$ and $\iota(m) \to m^{-1}$ for $m \in M$, and extending linearly on the whole of $k[M]$. This defines a functor from finitely generated abelian groups to affine algebraic groups $\mathrm{Diag}(M) := \mathrm{Spec}(k[M])$. Algebraic groups isomorphic to $\mathrm{Diag}(M)$ are called *diagonalisable*.

Example 2.3.1. Take $M = \mathbb{Z}/n\mathbb{Z}$. Then $k[M] \simeq k[T]/(T^n - 1)$, so $\mathrm{Diag}(M) = \mu_n$, (see 2.8). If $M = \mathbb{Z}$, then $k[M] \simeq k[T, T^{-1}]$ and $\mathrm{Diag}(M) = \mathbb{G}_m$.

Proposition 2.3.2. *If M_1 and M_2 are two finitely generated abelian groups,*

$$\mathrm{Diag}([M_1 \oplus M_2]) = \mathrm{Diag}(M_1) \times \mathrm{Diag}(M_2). \tag{2.12}$$

Proof. Note $k[M_1 \oplus M_2] = k[M_1] \oplus k[M_2]$, and under the contravariant equivalence in Proposition 2.1.1, $\mathrm{Spec}(A \oplus B) = \mathrm{Spec}(A) \times \mathrm{Spec}(B)$. □

Remark 2.3.3. Every diagonalisable group can be constructed from the two featured in Example 2.3.1 simply by using Proposition 2.3.2, along with the structure theorem of finitely generated abelian groups; all finite rank abelian groups are of the form $M := (\bigoplus \mathbb{Z}^m) \oplus (\bigoplus \mathbb{Z}/n_i\mathbb{Z})$ [14, Thm. 13.5].

Theorem 2.3.4. [37, Thm. 14.9] *There exists a contravariant equivalence of categories between finitely generated abelian groups and diagonalisable groups, given by the functor* Diag *and its quasi-inverse $G \to G^*$.*

Proof. By Proposition 2.3.2 and Remark 2.3.3, it is sufficient to check the case when M_i are $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$. Here is a list of possibilities that is easy to verify, where the left hand side are abstract group homomorphisms, and the right are morphisms of algebraic groups.

$$\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}) \cong \mathbb{Z} \cong \mathrm{Hom}(\mathbb{G}_m, \mathbb{G}_m),$$
$$\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z} \cong \mathrm{Hom}(\mu_n, \mathbb{G}_m),$$
$$\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) \cong \{1\} \cong \mathrm{Hom}(\mathbb{G}_m, \mu_n),$$
$$\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/d\mathbb{Z} \cong \mathrm{Hom}(\mu_m, \mu_n),$$

where $d = \gcd(m, n)$, and the elements in $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})$ and $\mathrm{Hom}(\mathbb{G}_m, \mu_n)$ are the identity maps. In general, for any choice of M, the homomorphisms have the form $\phi_n(x) = nx$ for some suitable n. Under Diag, this homomorphism becomes $\mathrm{Diag}(\phi)(x) = x^n$, which is the required bijection between $\mathrm{Hom}(M_1, M_2)$ and $\mathrm{Hom}(\mathrm{Diag}(M_1), \mathrm{Diag}(M_2))$. The functor Diag is therefore fully faithful, and is essentially surjective by the definition of diagonalisable groups.

□

An affine algebraic group G over k is called *multiplicative* if $G_{k_{\mathrm{sep}}}$ is diagonalisable. If G is a connected multiplicative group, then $G_{k_{\mathrm{sep}}} \simeq \mathbb{G}_m^n$ for some n, and G is an *algebraic torus*. A torus G *splits* over K if $G_K \simeq \mathbb{G}_m^n$ and K is a *splitting field* of G. The value of n is the *rank* of the torus.

Example 2.3.5. Set $k = \mathbb{R}$. There are two 1 dimensional tori over $\mathbb{R}$; the split torus $G(\mathbb{R}) = \mathbb{R}^\times$, and the *anisotropic* torus, $G(\mathbb{R}) = \{z \in \mathbb{C}^\times \mid z\overline{z} = 1\}$. Both groups have $G(\mathbb{C}) \simeq \mathbb{C}^\times$. Note that the split torus is the multiplicative group, and the anisotropic torus is the unit circle $\mathbb{T}^1 \subset \mathbb{C}$.

As the characters of a split torus are given by points of $\mathbb{Z}^r$, then any representation is given by some subset of $\mathbb{Z}^r$. These characters of $\mathbb{G}_m^r$ also form a basis of the coordinate algebra $\mathcal{O}(\mathbb{G}_m^r) = k[T_1, T_1^{-1}, \ldots T_r, T_r^{-1}]$.
For a non split torus G, define G^* as the group of morphisms $G_{k_{\mathrm{sep}}} \to \mathbb{G}_{m,k_{\mathrm{sep}}}$, where k_{sep} is the separable closure of k. This character lattice has an action of $\Gamma := \mathrm{Gal}(k_{\mathrm{sep}}/k)$ which offers an extension of Theorem 2.3.4 to an equivalence between $\Gamma := \mathrm{Gal}(k_{\mathrm{sep}}/k)$-modules and groups of multiplicative type, though first it is necessary to consider the topology on Γ.

For L/k a Galois field extension, the Galois group $\mathrm{Gal}(L/k)$ is an inverse limit of the finite groups $\mathrm{Gal}(K/k)$, where $k \subseteq K \subseteq L$, and K/k is a finite Galois extension of k. This group is endowed with the Krull topology, where the open sets are the subgroups $\mathrm{Gal}(k_{\mathrm{sep}}/K)$.

The action of an arbitrary topological group Γ on a module M is *continuous* if the mapping $\Gamma \times M \to M$ is continuous. If M is endowed with the discrete topology, then this is equivalent to saying every element of M is fixed by some open subset of Γ. If Γ is a Galois group, this simply means for every element $m \in M$ there exists some K/k Galois extension such that m is fixed by $\mathrm{Gal}(k_{\mathrm{sep}}/k)$.

Corollary 2.3.6. [37, Theorem 14.17] *There is an antiequivalence of categories between algebraic groups over k of multiplicative type and finitely generated abelian groups with a continuous action of $\Gamma := \mathrm{Gal}(k_{sep}/k)$.*

Proof. Suppose M is a finitely generated abelian group, with continuous action of Γ. Using the categorical equivalence in Corollary 2.3.6, $\mathrm{Spec}(k_{\mathrm{sep}}[M])$ is a diagonalisable group, so $\mathrm{Spec}(k[M])$ is a group of multiplicative type.

Conversely, suppose G is of multiplicative type over k. Every $\chi \in \mathrm{Hom}(G_{k_{\mathrm{sep}}}, \mathbb{G}_{m,k_{\mathrm{sep}}})$ is defined over some finite field extension K/k, so is fixed by some open subgroup $\mathrm{Gal}(k_{\mathrm{sep}}, K)$. Thus under the discrete topology, the action of Γ on G^* is continuous. □

As a group functor, the multiplicative group defined in the above theorem is

$$R \mapsto \mathrm{Hom}(\mathrm{Spec}(k[M]), (R \otimes_k k_{\mathrm{sep}})^{\times}), \tag{2.13}$$

where R is a k-algebra, and the morphisms are in the category of algebraic groups. In general, if K is a field extension, $k_{\text{sep}} \supseteq K/k$, then G_K can be identified as the functor of points $G_K = \text{Hom}(G^*, k_{\text{sep}})_{\text{Gal}(K/k)}$, the group of morphisms $G^* \to k_{\text{sep}}$ that commute with the action of Γ_K. Recall the two tori over $\mathbb{R}$ in Example 2.3.5.

Example 2.3.7. The character group of $\mathbb{C}^\times$ is $\mathbb{Z}$, which has precisely one non-trivial automorphism, $m \mapsto -m$. The action of $\Gamma = \text{Gal}(\mathbb{C}/\mathbb{R})$ is complex conjugation, so the group of morphisms that commute with this action satisfy

$$\sigma \cdot \chi(m) = \chi(\sigma(m))$$
$$\overline{\chi(m)} = \chi(m)^{-1}.$$

This is simply the collection of $z \in \mathbb{C}^\times$ that satisfy $\overline{z}z = 1$. Thus the rank 1 tori in Example 2.3.5 are recovered.

Corollary 2.3.8. *There exists an antiequivalence of categories between algebraic tori over k and torsion-free $\mathbb{Z}$-modules with continuous action by* $\text{Gal}(k_{sep}/k)$.

Proof. The finitely generated torsion-free $\mathbb{Z}$-modules (*i.e.* $\mathbb{Z}^n$) correspond to the split tori under the Diag functor, this is just the restriction of Corollary 2.3.6 to this case. □

Remark 2.3.9. Suppose T is a torus over k, so $\Gamma = \text{Gal}(k_{\text{sep}}/k)$ acts on $T^* = \mathbb{Z}^n$. Although Γ is usually a profinite group, it factors through a finite group of automorphisms of T^*, called the *decomposition group* of T, denoted by A_T. Explicitly, there exists a morphism $\pi : \Gamma \to \text{Aut}(\mathbb{Z}^n)$, and $A_T := \pi(\Gamma)$.

2.4 $\mathcal{G}$-lattices

A *lattice* L is a free $\mathbb{Z}$-module of finite rank, along with a symmetric positive definite bilinear form $L \times L \to \mathbb{Z}$. When L has an action by a finite group $\mathcal{G}$ that preserves the bilinear form, it is a *$\mathcal{G}$-lattice*. A $\mathcal{G}$-lattice yields an integral representation of $\mathcal{G}$

$$\phi : \mathcal{G} \to \mathrm{GL}(L) \simeq \mathrm{GL}_n(\mathbb{Z}). \tag{2.14}$$

It is often useful to study how "similar" two lattices are. For instance, two $\mathcal{G}$-lattices L, L' are *isomorphic* if there is a group isomorphism $\varphi : L \to L'$ that preserves the bilinear form. For coarser equivalences, it is necessary to consider the bilinear forms over other rings, by considering $L \otimes_{\mathbb{Z}} R$ as an R-module, or $R[\mathcal{G}]$-module for $\mathcal{G}$-lattices. One such important ring is the localisation of $\mathbb{Z}$ at a prime p

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z},\ p \not| \, b \right\} \subset \mathbb{Q}.$$

$L_{(p)}$ is used to denoted $L \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$, and two lattices L, L' are *locally isomorphic* if $L_{(p)} \simeq L'_{(p)}$ for all primes p. The set of isomorphism classes of the $L_{(p)}$ is the *genus* of L, and the notation $L \vee L'$ means L and L' have the same genus.

Let L be a $\mathcal{G}$-lattice of rank n, with bilinear form $\langle , \rangle$ and $\mathbb{Z}$-basis $\{e_i\}$. The *dual* of L is defined as

$$L^* := \{m \in \mathbb{R}^n \mid \langle m, l \rangle \in \mathbb{Z} \mid \text{for all } l \in L\}. \tag{2.15}$$

Clearly $L \subset L^*$, and the dual L^* can be identified as $\mathrm{Hom}(L, \mathbb{Z})$ via the maps $m \mapsto \phi_m$, where $\phi_m(x) = \langle m, x \rangle$, and $\varphi \mapsto (m_1, \ldots, m_n) \in L^*$, where $m_i := \varphi(e_i)$ for the basis

in $L \simeq \mathbb{Z}^n$. L^* is a lattice; it has a $\mathbb{Z}$-basis given by $(e_1^*, \ldots e_n^*)$, where $\langle e_i^*, e_j \rangle = \delta_{i,j}$ and if B and B^* are the matrices formed by the bases $\{e_i\}$ and $\{e_i^*\}$ respectively. L^* is also a $\mathcal{G}$-lattice; $\mathcal{G}$-acts on $\phi \in \mathrm{Hom}(L, \mathbb{Z})$ by $g \cdot \phi(l) := \phi(g^{-1} \cdot l)$.

There are numerous ways to construct new lattices from two given lattices. If L is a $\mathcal{G}_L$-lattice and M a $\mathcal{G}_M$-lattice, then the direct sum $L \oplus M := \{(l, m) |\ l \in L,\ m \in M\}$ is a $\mathcal{G}_L \times \mathcal{G}_M$-lattice. There also exists the *tensor product*, $L \otimes_{\mathbb{Z}} M$,which has elements of the form

$$L \otimes_{\mathbb{Z}} M := \sum_{i,j} \alpha_{i,j}(e_i \otimes f_j), \tag{2.16}$$

for $\alpha_{i,j} \in \mathbb{Z}$ and $\mathbb{Z}$-bases $\{e_i\}$ of L and $\{f_i\}$ of M. As $-l \otimes m = l \otimes -m$, $L \otimes_{\mathbb{Z}} M$ has a faithful action by the *central product*, $\mathcal{G}_L \times \mathcal{G}_M/(-1, -1)$. This will be discussed in more detail in Section 4.1.3.

A lattice L' is *adjacent* to a lattice L if they share the same bilinear form, rank, and there exists some collection $v_i \in L'$ such that L' is generated by L and v_i. Also as $L \leqslant L'$, and r is the index of L in L', $r := [L' : L]$, then L' is denoted L^{+r}. A collection of adjacent lattices forms a partially ordered set and is called a *family*. Such families often share the same lattice automorphism group, though occasionally there can be additional automorphisms for certain family members.

Example 2.4.1. The D_n root lattice comprises all points

$$\{(x_1, \ldots, x_n) \mid \textstyle\sum x_i \in 2\mathbb{Z}\},$$

along with the standard inner product. The regular integer lattice, I_n is an adjacent lattice, generated as a $\mathbb{Z}$-module by D_n and the vector $(1, 0, \ldots, 0)$. The third family member, $D_n^{+4} = D_n^*$, is generated by I_n and the following two vectors $(\frac{1}{2}, \ldots, \frac{1}{2})$,

$(\frac{1}{2}, \ldots, \frac{1}{2}, -\frac{1}{2})$. The family is the following poset $D_n \leqslant I_n \leqslant D_n^{+4}$. They all share the same automorphism group $C_2 \wr S_n$ (where $\wr$ denotes the wreath product), barring dimension 4, where D_4 has an extra automorphism of order 3 (known as *triality*).

If a $\mathcal{G}$-lattice L has a $\mathbb{Z}$-basis that is permuted by $\mathcal{G}$, then it is a *permutation* $\mathcal{G}$-lattice, and two $\mathcal{G}$-lattices L and L' are *stably permutation equivalent* if there exists some permutation lattices P, P' such that $L \oplus P \simeq L' \oplus P'$, (here $\mathcal{G}$ acts with the diagonal action). Denote $[L]$ as the stably permutation class of L, and if $[L] = [0]$, then L is a *stably permutation* lattice. In fact the stably permutation class of $L \oplus L'$ only depends on the respective classes of L and L' (see [26, 2.3, pp.34]) so the set of classes is a monoid, which is denoted $\mathrm{SP}_{\mathcal{G}}$. A $\mathcal{G}$-lattice L is *invertible* (sometimes called *permutation projective*) if $[L]$ is an invertible element of $\mathrm{SP}_{\mathcal{G}}$.

As mentioned in Remark 2.3.9, the set of characters $T^* = \mathrm{Hom}(T, \mathbb{G}_m)$ of an algebraic torus T over k form a copy of $\mathbb{Z}^n$ with an action of the decomposition group A_T; a finite subgroup of the Galois group $\mathrm{Gal}(k_{\mathrm{sep}}/k)$. The set of *cocharacters* of T is the set $T_* = \mathrm{Hom}(\mathbb{G}_m, T)$, which has a natural pairing with T^*; $\langle\ ,\ \rangle\ T^* \times T_* \to \mathbb{Z}$; $\langle \chi, \lambda \rangle = \chi \circ \lambda \in (\mathbb{G}_m)^* = \mathbb{Z}$, for $\chi \in T^*$, $\lambda \in T_*$. The cocharacter lattice is canonically isomorphic to the dual of the character lattice; as $T_* = \mathrm{Hom}(\mathbb{G}_m, T) = \mathrm{Hom}(\mathrm{Diag}(\mathbb{Z}), \mathrm{Diag}(L)) = \mathrm{Hom}(T^*, \mathbb{Z})$, under the contravariant equivalence Diag. Therefore $T^* \subset T_*$, and restricting this bilinear form to $T^* \times T^*$, gives a bilinear form on T^*, and it is thus T^* is an A_T-lattice.

Certain lattice properties of the A_T-lattice T^* correspond to properties of the algebraic torus T. For instance, T is *quasi-split* if T^* is permutation, and is *special* if T^* is invertible. An important example of this occurs when the group $\mathcal{G}$ is a p-group. A morphism of algebraic groups $\phi : G \to Q$ is an *isogeny* if ϕ is surjective and has finite

kernel, and further if the kernel has order prime to p, then it is a *p-isogeny.*

Proposition 2.4.2. [27, Lemma 9.1] *Let $\mathcal{G}$ be a p-groups. For two $\mathcal{G}$-lattices L, L',* $\mathrm{Diag}(L)$ *and* $\mathrm{Diag}(L')$ *are p-isogeneous if and only if $L \vee L'$.*

Proof. If $L \vee L'$, then there exists an isomorphism $\phi : L_{(p)} \to L'_{(p)}$. As $L \subset L_{(p)}$, and ϕ is surjective, $\phi(L)$ has finite, prime to p index inside $\frac{1}{n}L'$ for some n prime to p. As $\mathcal{G}$-modules, $L' \simeq \frac{1}{n}L'$, so by restricting to L, there exists an injective morphism $\phi : L \to L'$ that has a finite cokernel of size prime to p. Under the functor Diag, this results in a surjective morphism $\mathrm{Diag}(\phi) : \mathrm{Diag}(L') \to \mathrm{Diag}(L)$ with kernel finite and order prime to p, so $\mathrm{Diag}(\phi)$ is a p-isogeny.
If $\mathrm{Diag}(L') \to \mathrm{Diag}(L)$ is a p-isogeny, then likewise under the quasi-inverse, there exists an injective morphism $\phi : L \to L'$ with finite cokernel of order prime to p. The resulting exact sequence, when tensored with $\mathbb{Z}_{(p)}$ is

$$1 \longrightarrow L_{(p)} \longrightarrow L'_{(p)} \longrightarrow \mathrm{coker}(\phi)_{(p)} \longrightarrow 1, \tag{2.17}$$

but $\mathrm{coker}(\phi)$ has order prime to p and therefore vanishes, giving the required isomorphism. □

Automorphisms of lattices are always finite subgroups of $\mathrm{GL}_n(\mathbb{Z})$ (see 2.14). In fact, there are finitely many of these subgroups, a fact which has been known since the 19^{th} century.

Theorem 2.4.3. [23] *For a given n, there are finitely many conjugacy classes of finite subgroups of* $\mathrm{GL}_n(\mathbb{Z})$.

Although finite, the number of finite subgroups of $\mathrm{GL}_n(\mathbb{Z})$ grows rapidly with n, so attempts at a classification focus on the maximal subgroups that are irreducible (as integral representations). These irreducible maximal finite subgroups of $\mathrm{GL}_n(\mathbb{Z})$ are completely classified up to $\mathrm{GL}_n(\mathbb{Z})$-conjugacy for ranks 1 to 10 and primes up to 23, and up to $\mathrm{GL}_n(\mathbb{Q})$-conjugacy for all ranks up to 31. There exists databases of such groups in the computer algebra systems GAP and MAGMA, and these groups, along with descriptions of the lattices for which these symmetries appear as the full automorphism group, can be found in the first two of a series of papers by Conway and Sloane [10], [11].

Definition 2.4.4. Let L be a $\mathcal{G}$-lattice, and $\phi : \mathcal{G} \to \mathrm{GL}(L)$ the corresponding integral representation of $\mathcal{G}$. The *symmetric rank* of ϕ is defined as

$$\mathrm{SymRank}(\phi) := \min\{|\Lambda|\} \tag{2.18}$$

where the minimum runs over all generating subsets $\Lambda \subset L$ that are invariant under $\mathcal{G}$.

A p-local version of this is the symmetric p-rank. For a prime p, a subset Λ is said to *p-generate* L if it generates a full rank sub-lattice of L that has index prime to p.

Definition 2.4.5. Using the same definitions as Definition 2.4.4, let Γ_p be a Sylow p-subgroup of $\mathcal{G}$. The *symmetric p-rank* of ϕ is defined as

$$\mathrm{SymRank}(\phi; p) := \min\{|\Lambda|\} \tag{2.19}$$

where the minimum runs over all p-generating subsets $\Lambda \subset L$ that are invariant under

Γ_p.

Example 2.4.6. Suppose L is a $\mathcal{G}$-lattice, where $\mathcal{G}$ contains an element that acts on L as -1. Then $\mathrm{SymRank}(\phi; 2) \geq 2 \cdot \mathrm{rank}(L)$, as any 2-generating invariant set decomposes as $X = X' \amalg -X'$, where $|X'| \geq \mathrm{rank}(L)$.

Remark 2.4.7. The symmetric (p)-rank is defined for a specific integral representation of a finite group $\mathcal{G}$; though often this representation is implicitly defined. For notational convenience, given a $\mathcal{G}$-lattice L, and $\mathcal{H} \leqslant \mathcal{G}$, then $\mathrm{SymRank}(\widehat{\mathcal{H}}; p) := \mathrm{SymRank}(\phi|_{\mathcal{H}}; p)$.

Often the group $\mathcal{G}$ is implicit, either when comparing $\mathcal{G}$-lattices across a fixed $\mathcal{G}$, or when $\mathcal{G} = \mathrm{Aut}(L)$, the full automorphism group of L. In these cases the notation $\mathrm{SymRank}(\phi; p)$ is replaced by $\mathrm{SymRank}(L; p)$, though this notation will be clearly defined in each such instance.

2.5 Group cohomology

The following introduction on group cohomology follows [5]. For $\mathcal{G}$ a finite group, and M a $\mathcal{G}$-module, define the following set of maps

$$C^n(\mathcal{G}, M) = \{f : \mathcal{G}^n \to M\}. \tag{2.20}$$

Together with the differential map $\partial^{n+1} : C^n(\mathcal{G}, M) \to C^{n+1}(\mathcal{G}, M)$ defined by

$$\partial^{n+1}(f)(g_1, \ldots, g_{n+1}) = g_1 \cdot f(g_2, \ldots, g_{n+1}) + \tag{2.21}$$

$$\sum_{i=1}^{n} (-1)^i f(g_1, \ldots, g_{i-1}, g_i g_{i+1}, \ldots, g_{n+1}) + (-1)^{n+1} f(g_1, \ldots, g_n) \tag{2.22}$$

forms a cochain complex, and the following set of n-cocycles and n-coboundaries respectively,

$$Z^n(\mathcal{G}, M) = \ker \partial^{n+1},$$

$$B^n(\mathcal{G}, M) = \begin{cases} 0 & n = 0 \\ \text{Im } \partial^n & n \geq 1. \end{cases}$$

The cohomology group of $\mathcal{G}$ with coefficients in M with degree n is defined as

$$H^n(\mathcal{G}, M) = Z^n(\mathcal{G}, M)/B^n(\mathcal{G}, M). \tag{2.23}$$

The following descriptions of the low degree cohomology groups follow immediately from the definitions.

$$H^0(\mathcal{G}, M) = M^{\mathcal{G}}, \tag{2.24}$$

$$Z^1(\mathcal{G}, M) = \{f : G \to M \mid f(gh) = g \cdot f(h) + f(g) \text{ for all } g, h \in \mathcal{G}\}, \tag{2.25}$$

$$B^1(\mathcal{G}, M) = \{f : G \to M \mid f(g) = gm - m \text{ for some } m \in M\}, \tag{2.26}$$

the latter two being known as the crossed homomorphisms, and the principal crossed homomorphisms respectively. The group $H^2(\mathcal{G}, M)$ gives information on the *exten-*

sions of $\mathcal{G}$ by M, which are the groups E which fit into the exact sequence of groups

$$1 \longrightarrow M \longrightarrow E \longrightarrow \mathcal{G} \longrightarrow 1. \tag{2.27}$$

Two extensions E_1 and E_2 are *equivalent* if there exists an isomorphism $\sigma : E_1 \to E_2$, and the following diagram commutes

$$\begin{array}{ccccccccc} 1 & \longrightarrow & M & \longrightarrow & E_1 & \longrightarrow & \mathcal{G} & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & M & \longrightarrow & E_2 & \longrightarrow & \mathcal{G} & \longrightarrow & 1. \end{array}$$

The group $H^2(\mathcal{G}, M)$ specifies the classes of extension, up to equivalence. If $c \in H^2(\mathcal{G}, M)$ is a 2-cocycle, and define E as the set of formal pairs $\{(g, m) \,|g \in \mathcal{G}, m \in M\}$, with binary product

$$(g_1, m_1)(g_2, m_2) = (g_1 g_2, c(g_1, g_2) m_1 (g_1 \cdot m_2)), \tag{2.28}$$

and a pair of 2-cocycles give isomorphic extensions when their difference lies in $Z^2(\mathcal{G}, M)$.

When $\mathcal{G}$ is a finite cyclic group, $H^2(\mathcal{G}, M)$ is particularly easy to calculate.

Proposition 2.5.1.

If there exists a short exact sequence of $\mathcal{G}$-modules

$$1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1, \tag{2.29}$$

then this induces a long exact sequence (of cohomology groups)

$$1 \longrightarrow A^{\mathcal{G}} \longrightarrow B^{\mathcal{G}} \longrightarrow C^{\mathcal{G}} \longrightarrow H^1(\mathcal{G}, A) \longrightarrow H^1(\mathcal{G}, B) \longrightarrow H^1(\mathcal{G}, C) \cdots, \qquad (2.30)$$

which extends to the right through the H^i. If M is non-abelian, then it is possible to make sense of $H^i(\mathcal{G}, M)$ for $i = 0, 1$, using the same definitions as (2.24). M is referred to as a $\mathcal{G}$-*group* in this case. Note the H^i may not in general be groups, though as the trivial cocycle always exists, they are pointed sets, so kernels can be defined. Thus the long exact sequence of cohomology in (2.30) is also valid here, up to H^1.

Group cohomology can be extended to topological groups and algebraic groups in a natural manner. Recall from (2.3.4) that an action of a topological group Γ on M is continuous if the mapping $\Gamma \times M \to M$ is a continuous map, which is equivalent to $M = \bigcup_{U \subset \Gamma} M^U$ for the open subgroups $U \subset \Gamma$. In general, if E is a topological space under the discrete topology, with a continuous action by Γ, then it is a Γ-*set*. If E also has the structure of a group or module then it is a Γ-group or module, respectively. If M is a Γ-module, then restricting the cochain complex at (2.20) to continuous maps $f : \Gamma \to M$, along with the same differential gives the right analogue to the finite group case. The same definitions of H^i apply here, and when Γ is a Galois group, these are the *Galois cohomology* groups.

Finally, for algebraic groups, analogous definitions give rise to the *Hochschild cohomology*. If G is an algebraic group over k, a commutative algebraic group M is a G-module if for all k-algebras R, $M(R)$ is a $G(R)$-module. The group $C^n(G, M)$ is then defined as the set of all maps of set-valued functors between G^n and M,

specifically if G has coordinate ring A, then $C^n(G, M) = M(A^{\otimes n})$. Using the same definitions of the differential, the cohomology groups are denoted $H_0^i(G, M)$, the i^{th} Hochschild cohomology group.

2.6 Galois cohomology and twisted forms

A fundamental question in Galois theory is given a pair of "objects" A and B defined over a field k (such as k-algebras or algebraic varieties), and a Galois extension K/k such that there is a K-isomorphism $\phi : A_K \to B_K$ (B is a K-*form* of A) in what sense are A_k and B_k the same? Certainly it is not true that there exists a k-isomorphism $A_k \to B_k$; indeed this is only true if there exists a $\mathrm{Gal}(K/k)$-invariant K-isomorphism $A_K \to B_K$, which takes k points in A to k-points in B. The Galois cohomology group $H^1(\Gamma, \mathrm{Aut}_K(A))$ (see (2.23), along with the suitable definition of the cochain map described at the end of Section 2.5) measures in some sense the obstructions to creating such isomorphisms, and will be explored in the following section. The definitions and results are from [43], and the discussion will give some insight in to the bijection between the forms of an algebraic object A and the classes of $H^1(\Gamma, \mathrm{Aut}_K(A))$. Let $\Gamma := \mathrm{Gal}(K/k)$, G a Γ-group and F a Γ-set, which also has an action of G. G is said to act on F *compatibly* with Γ if $\sigma \cdot (g \cdot f) = \sigma(g) \cdot \sigma(f)$ for all $g \in G$, $f \in F$, $\sigma \in \Gamma$.

Definition 2.6.1. [43, pp. 46] A right (resp. left) principal homogeneous space, or right (resp. left) *torsor* over G is a non-empty Γ-set P, on which G acts on the right (resp. left) compatibly with Γ such that for each pair x, $y \in P$, there exists a unique $g \in G$ such that $y = x \cdot g$.

Unpacking the definition, if P is a (right) torsor over G, then for any $\sigma \in \Gamma$, there must exist some corresponding $g_\sigma \in G$ such that $\sigma \cdot x = x \cdot (g_\sigma)$ for all $x \in P$. The map $\sigma \mapsto g_\sigma$ is a 1-cocycle; for σ, $\tau \in \Gamma$, $g_{\sigma\tau}$ is the unique element in G such that $\sigma\tau(x) = x \cdot (g_{\sigma\tau})$. As $\sigma\tau(x) = \sigma(x \cdot g_\tau) = \sigma(x) \cdot \sigma(g_\tau)$, then $g_{\sigma\tau} := g_\sigma \sigma(g_\tau)$, satisfying the 1-cocycle condition.
On the other hand, given a cocycle $g \in Z^1(\Gamma, G)$, then defining a copy of G with a new action of Γ, $\sigma * g = g_\sigma \sigma(g)$, gives a principal homogeneous space P, with G acting on the right by translations.

Proposition 2.6.2. [43, Prop. 33] *Let* $\Gamma := \mathrm{Gal}(K/k)$*, and* G *be a* Γ*-group. There exists a bijection between the set of principal homogeneous spaces over* G *and* $H^1(\Gamma, G)$*.*

The connection between *principal homogeneous spaces* and *forms* $A_K \to B_K$ can now be elucidated. In general, if A is an object over a field k, and K/k a Galois field extension, then $\mathrm{Aut}_K(A)$ is a Γ-group that acts on A in a compatible way. If A is an object over k, then define an equivalence relation on $P \times A$, where $(x, a) \sim (x \cdot g, g^{-1}a)$ for $g \in G$. The resulting quotient $(P \times A)/\sim$ is a Γ-set, and has a bijection with A. This is the *twisting of* A *by* P and yields a form of A. Conversely, the set of K-isomorphisms between two forms $A \to B$ is a principal homogeneous space.
The term "object" has hitherto been used to denote some algebraic structure defined over a field, that is functorial over field extensions and has a definable group of automorphisms. Propositions 1 and 5 in [43, pp.122–123] assert the existence of a bijection between the forms of A and the classes $H^1(\Gamma, \mathrm{Aut}_K(A))$ for A a k-vector space and a (quasi-projective) algebraic variety respectively. Of specific interest is when $\mathrm{Aut}_K(A)$ is an algebraic group, and it is useful to consider how $H^1(\mathrm{Gal}(k_{\mathrm{sep}}/K), \mathrm{Aut}_{k_{\mathrm{sep}}}(A))$

changes as K runs over Galois field extensions of K/k_{sep}. To this end, the notation is amended, and if G is an algebraic group, where $G := \text{Aut}(A)$, then the group $H^1(\text{Gal}(k_{\text{sep}}/K), \text{Aut}_{k_{\text{sep}}}(A))$ is instead written as $H^1(K, G)$. The *Galois cohomology functor* is the following

$$\mathcal{F} : \mathbf{Fields}_k \to \mathbf{Set}$$
$$K \mapsto H^1(\text{Gal}(k_{\text{sep}}/K, G).$$

Example 2.6.3. [43, 1.2(b), pp.143] A central algebra over k is a finite-dimensional, associative, unital algebra over k that satisfies $Z(A) = k$, and a simple algebra is one that has no non-trivial proper two sided ideals. The central simple algebras are the twisted forms of the matrix algebra $M_n(k)$, and as $\text{PGL}_n := \text{Aut}(M_n)$, the set $H^1(K, \text{PGL}_n)$ is the set of K-isomorphism classes of central simple algebras.

Example 2.6.4. [43, 1.2(c), pp.143] Let q be a quadratic form on a k-vector space V. Then $\text{Aut}_K(V) = O(q)$, the orthogonal group that preserves the quadratic form q. This is an algebraic group, and therefore $H^1(K, O(q))$ classifies all quadratic forms that become isometric to q over the field extension K_{sep}.

2.7 Extensions of finite groups by tori

In the previous discussion (for instance Remark 2.3.9), $\mathcal{G}$-lattices appeared when studying the action of $\text{Gal}(k_{\text{sep}}/k)$ on some torus T over k. This section will now explore a situation where a similar link to $\mathcal{G}$-lattices appears; extensions of finite groups by tori. For the rest of this chapter, T is a split torus over a field k. If

L is an F-lattice for some finite group F, then F acts on the characters of the torus $T := \mathrm{Diag}(L) := \mathrm{Spec}(k[L])$. These characters form a basis of the coordinate algebra of T, $\mathcal{O}(T)$, so induces an action on the torus itself, given by homomorphisms $\theta : F \to \mathrm{Aut}_k(T)$. As the group F defines an algebraic group (the constant group scheme F_k, see Example 2.2.2) then it is possible to construct an exact sequence of algebraic groups

$$1 \longrightarrow T \longrightarrow G \xrightarrow{\pi} F \longrightarrow 1, \tag{2.31}$$

where $G(R) = T(R) \times F(R)$ as sets for all k-algebras R, and G acts on T by conjugation in the same way as $\pi(G) = F$.

One such group G is the *semidirect product* $T \rtimes F : \mathrm{Alg}_k \to \mathrm{Grp}$, which is endowed with the following product, for $t, t' \in T(R)$, $f, f' \in F(R)$,

$$(t, f) \cdot (t', f') = (t\theta(f)(t'), ff').$$

In this case, the exact sequence *splits*, meaning there exists a morphism of algebraic groups $s : F \to G$ such that $\pi \circ s$ is the identity.

It is important to note that the definition of an extension of F by T not only depends on T and F, but crucially on the chosen action of F on T, which will be implied by the action of F on T^*. The notation of the base field is now dropped, and the symbol F either denotes the abstract group, or the constant group scheme F_k associated, depending on the setting.

As T is abelian with an action of F, it has the structure of an F-module. As a result, algebraic groups G that satisfy (2.31) are classified up to isomorphism by the elements of the group $\mathrm{Ext}^1(F; T)$ ([SGA3, XVII. pp.367]). This is an abelian group, with the

binary operation being the *Baer sum*. Two extensions create a new extension by a pullback under the diagonal map $F \to F \times F$, and then a pushforward along the multiplication map $T \times T \to T;\ (t_1, t_2) \mapsto t_1 t_2$.
The following are some useful lemmas on the structure of $\mathrm{Ext}^1(F;T)$.

Lemma 2.7.1. [SGA3, XVII, Lemma 5.2.4] $\mathrm{Ext}^1(F;T)$ *has* m *torsion, where* m *equals the order of* F*.*

Recall the definition of an isogeny from Section 2.4.

Lemma 2.7.2. [2, pp. 7] *Define* m_T *as the isogeny* $T \to T\ ;\ x \mapsto x^m$*, and define* $T[m] := \ker(m_T)$*. Then* $\mathrm{Ext}^1(F;T) \leq \mathrm{Ext}^1(F;T[m])$*.*

Proof. The isogeny m_T yields the exact sequence

$$1 \longrightarrow T[m] \longrightarrow T \xrightarrow{m_T} T, \tag{2.32}$$

applying $\mathrm{Ext}(F;-)$ to (2.32) leads to a long exact sequence

$$\ldots \mathrm{Ext}^1(F;T[m]) \longrightarrow \mathrm{Ext}^1(F;T) \xrightarrow{(m_T)_*} \mathrm{Ext}^1(F;T) \ldots, \tag{2.33}$$

and Lemma 2.7.1 says any extension class $\gamma \in \mathrm{Ext}^1(F;T)$ is annihilated by m, i.e. $m\gamma = 0$. Then $m\gamma$ can be identified as the $(m_T)_*(\gamma)$, the pushout of γ by m_T, and using the exact sequence in (2.33), every $\gamma \in \mathrm{Ext}^1(F,T)$ is the image of some $\gamma' \in \mathrm{Ext}^1(F, T[m])$. □

The aim of the following discourse is to show that, for a split torus T, and a

constant group scheme F, there is a canonical bijection between $\mathrm{Ext}^1(F;T)$ and $H^2(F;T(k))$, where H^i denotes the (abstract) group cohomology of the finite group F and $T(k)$ the group of k-rational points of T.

The extension in (2.31) is *Hochschild* if it admits a *scheme*-theoretic section, a map of schemes $s : F \to G$ such that $\pi \circ s$ is the identity on F. Two Hochschild extensions G and G' are equivalent if there exists a morphism of algebraic groups $f : G \to G'$ such that the following diagram commutes

$$\begin{array}{ccccccccc} 1 & \longrightarrow & T & \longrightarrow & G & \xrightarrow{\pi} & F & \longrightarrow & 1 \\ & & \downarrow & & \downarrow{\scriptstyle f} & & \downarrow & & \\ 1 & \longrightarrow & T & \longrightarrow & G' & \xrightarrow{\pi'} & F & \longrightarrow & 1. \end{array} \tag{2.34}$$

Lemma 2.7.3. *Let T be an F-module. Then there exists a bijection between the set of Hochschild extensions up to equivalence of F by T and the Hochschild cohomology group $H^2_0(F;T)$.*

Proof. Suppose G is a Hochschild extension, and $s : F \to G$ the section. Then define $c : F \times F \to T$ as the preimage in T of $s(f_1)s(f_2)s(f_1f_2)^{-1}$. This defines a 2-cocycle, and similarly given a 2-cocycle $c : F \times F \to T$, the group functor $T(R) \times F(R)$ with multiplication for all $t_i \in T(R)$, $f_i \in F(R)$,

$$(t_1, f_1)(t_2, f_2) := (c(f_1, f_2)t_1(f_1 \cdot t_2), f_1f_2) \tag{2.35}$$

defines a Hochschild extension, with section $s(f_1) = (1, f_1)$ for all k-algebras R. □

This is reminiscent of the case for abstract groups, where there is a canonical bijection between H^2 of the abstract group cohomology, and the group (up to equiv-

alence) of extensions Ext^1, but in the setting of algebraic groups some extensions aren't necessarily Hochschild.

Example 2.7.4. Consider the following extension of algebraic groups over a perfect field of characteristic not 2.

$$1 \longrightarrow \{\pm 1\} \longrightarrow \mathbb{G}_m \xrightarrow{\sigma} \mathbb{G}_m \longrightarrow 1, \tag{2.36}$$

where σ is the squaring map $z \mapsto z^2$. No section exists, so this is not Hochschild. A section $s : \mathbb{G}_m \to \mathbb{G}_m$ would imply σ defines an isomorphism of schemes, which is false.

In the case of a finite group by split torus however, all extensions have a scheme-theoretic section. The exact sequence (2.31) endows G with the structure of a torsor over F, where T takes the place of Γ in Definition 2.6.1, viewed as a topological group under the *étale topology*. The group $H^1_{\text{ét}}(F;T)$ classifies these torsors over F. Rather than give an exposition on étale cohomology here, the reader is referred to [16, Chap. 5]. The reason for this omission is due to the following, which is a consequence of [41, Thm. 14].

Proposition 2.7.5. *$H_{ét}(F;T)$ has d-torsion, where d is the degree of the splitting field of T.*

If an extension gives a set valued section, then the torsor is trivial, (as there exists an isomorphism of schemes $T \times F \to G$). This therefore gives rise to the following

short exact sequence, which is a rewording of [SGA3, XVII. App. I.3.1],

$$0 \longrightarrow H_0^2(F_k; T) \longrightarrow \mathrm{Ext}^1(F; T) \longrightarrow H_{\text{ét}}(F_k; T). \tag{2.37}$$

In (2.36), σ defined a non-trivial torsor $\mathcal{C}_2$-torsor $\mathbb{G}_m \to \mathbb{G}_m$ where $\mathcal{C}_2$ acts as $\{\pm 1\}$, so the corresponding extension was not Hochschild.

Proposition 2.7.6. *Denote by F_k the constant group scheme associated to the finite abstract group F, and M a F_k-module. There is a canonical bijection between the Hochschild cohomology $H_0^i(F_k, M)$ and the abstract group cohomology $H^i(F, M(k))$.*

Proof. It is sufficient to simply show a bijection between $C(F_k, M)$, the maps of set valued functors, and $C^i(F, M(k))$, the set of maps between the abstract groups. For the former, $C(F_k, M) = M(A)$ where $A = k^{|F|}$, the coordinate ring of F_k. $C(F, M(k))$ is given by the identification of the elements of F to the k-points of M, so there are bijections of sets $C(F, M(k)) \xrightarrow{\simeq} M(k^{|F|}) \xrightarrow{\simeq} C(F_k, M)$. As this is preserved through taking products of F, the chain complexes are thus equivalent. □

Corollary 2.7.7. *Let T be a split torus, and F a finite group. There exists a canonical bijection between the elements of* $\mathrm{Ext}^1(T; F)$ *and the abstract group cohomology $H^2(T(k); F)$.*

Proof. As T is split, $H_{\text{ét}}(F_k; T)$ is trivial, so $H_0^2(F_k; T) \simeq \mathrm{Ext}^1(F; T)$. Proposition 2.7.6 gives an isomorphism between the Hochschild cohomology group of algebraic groups $H_0^2(F; T)$, and the abstract group cohomology $H^2(F; T(k))$. □

Example 2.7.8. Take $F = \mathcal{C}_2$, $T = \mathbb{G}_m$, so $T^* = \mathbb{Z}$. The action of $\mathcal{C}_2$ on T^* sends $x \mapsto -x$, and on T sends $z \mapsto z^{-1}$. $T[2] \simeq \mathcal{C}_2$, and $H^2(F, T[2]) = H^2(\mathcal{C}_2, \mathcal{C}_2) =$

$\mathbb{Z}/2\mathbb{Z}$. There are thus two isomorphism classes of extensions with the following matrix representations. Embed $\mathbb{G}_m$ in GL_2 by sending $z \mapsto \mathrm{diag}(z, z^{-1})$, so F acts by sending elements in T to their inverse. There are two choices of element $g \in \mathrm{GL}_2$ such that $gtg^{-1} = t^{-1}$, $\left(\begin{smallmatrix} 0 & a \\ a^{-1} & 0 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 0 & a \\ -a^{-1} & 0 \end{smallmatrix}\right)$. These matrices are in the preimage under π of the non-trivial element of F. The first of these is the split case, so the finite group F can be identified as a subgroup of G. The second choice gives rise to the non-split case, so corresponds to the non-trivial element of $H^2(F;T)$, which is the following 2-cocycle

$$c(g, g') = \begin{cases} -1 & g = g' \neq e \\ 1 & \text{otherwise.} \end{cases} \tag{2.38}$$

There is no copy of F in the non-identity component of G, and $F \neq F' = \left\langle \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \right\rangle$, so $T \cap F' = \left\langle \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \right\rangle = \mathcal{C}_2$.

Chapter 3

Essential dimension

The intuition behind the essential dimension of an algebraic object is "how many algebraically independent parameters are required to describe that object?". First defined for finite groups in [6] by Buhler and Reichstein, the definition of $\mathrm{ed}_k(S_n)$ is roughly equivalent to the minimum number of parameters required to describe a polynomial of degree n. This was then generalised to any finite group, where the essential dimension was given by the minimal dimension with which a faithful representation can be "compressed" (see Section 3.2). Essential dimension has since been defined for a variety of other algebraic objects including algebraic groups, firstly in [40] for algebraic groups over fields of characteristic 0 and subsequently more generally in [1], by defining the essential dimension using category theory and G-torsors. This will be the path followed in this chapter, additionally making use of the survey paper [34], which synthesises the various viewpoints.

3.1 Definition

Let k be a field. The category $\mathbf{Fields}_k$ consists of field extensions of k, with morphisms as field homomorphisms over k. Suppose $\mathcal{F}$ is a covariant functor $\mathbf{Fields}_k \to \mathbf{Set}$ and K/k a field extension. For an intermediate field extension, $K/K_0/k$, with morphism $\alpha : K_0 \to K$, an element $x \in \mathcal{F}(K)$ is *defined over* K_0 if x is in the image of $\mathcal{F}(\alpha) : \mathcal{F}(K_0) \to \mathcal{F}(K)$ (so there exists $x_0 \in \mathcal{F}(K_0)$ such that $\mathcal{F}(\alpha)(x_0) = x$). In this case the field K_0 is a *field of definition* of x.
The *essential dimension* of x is the following

$$\mathrm{ed}_k(x) := \min \text{ tr. } \deg_k(K_0) \tag{3.1}$$

amongst all fields of definition of x, K_0.

Definition 3.1.1. [1, Def. 1.2] For a functor $\mathcal{F} : \mathbf{Fields}_k \to \mathbf{Set}$,

$$\mathrm{ed}_k(\mathcal{F}) := \max \mathrm{ed}_k(x), \tag{3.2}$$

over all field extensions K/k and all $x \in \mathcal{F}(K)$.

The idea is to define the essential dimension of an algebraic object by choosing a suitable functor. For example, given a scheme X, a natural choice would be the associated functor of points $X(K)$, which gives the K-rational points of X. In this case the essential dimension recovers the usual definition of dimension.

Proposition 3.1.2. [1, Prop. 1.17] *For an algebraic scheme X defined over k,*

$$\mathrm{ed}_k(X) = \dim(X).$$

Proof. The discussion in Section 2.1 showed that if $x \in X(K)$ for K/k, then the residue field $k(x) \subset K$. Therefore, $\mathrm{ed}_k(x) = \mathrm{tr.deg}_k(k(x))$. Thus

$$\begin{aligned} \mathrm{ed}_k(X) &= \max\{\mathrm{tr.deg}_k(k(x))\} \\ &= \dim(X), \end{aligned}$$

where the maximum is taken over all $x \in X(K)$, K/k. □

For any $\mathcal{F} : \mathbf{Fields}_k \to \mathbf{Set}$, if there exists some scheme X such that for every K/k there is a surjection of sets $X(K) \to \mathcal{F}$, (called here a *surjection of functors* $X \to \mathcal{F}$) then X is called a *classifying scheme*, and from the definition of $\mathrm{ed}_k(\mathcal{F})$ and the earlier proposition,

$$\mathrm{ed}_k(\mathcal{F}) \leq \dim(X). \tag{3.3}$$

Definition 3.1.3. Let G be an algebraic group over k. The essential dimension of G is the essential dimension of the covariant first Galois cohomology functor $K \to H^1(K, G)$ associated to G,

$$\mathrm{ed}_k(G) := \mathrm{ed}_k(H^1(-, G)). \tag{3.4}$$

The choice of this functor for algebraic groups is thus a measure of the complexity of classes of G-torsors over $\mathrm{Spec}(k)$ when taking different field extensions of k. This is often a difficult number to calculate and the quest is usually divided between finding upper and lower bounds.

3.2 Upper bounds

Firstly defined are the "scheme theoretic" version of group actions; the definitions and results in this section are from [1]. For a scheme S (which will be referred to now as a *base scheme*), then a morphism of schemes $T \to S$, along with T form an *S-scheme*. If X is such an S-scheme, and G is an algebraic group which is also an S-scheme, then one can form the pullback along S, $G \times_S X$. *G acts on X* if there is a morphism of S-schemes $G \times_S X \to X$, given by $(g, x) \mapsto x \cdot g$, such that the usual properties of group actions hold. The scheme X is thus a *G-scheme*, and the *scheme-theoretic* stabilizer G_x for $x \in X$ is given by the pullback

$$\begin{array}{ccc} G_x & \longrightarrow & G \times_S \{x\} \\ \downarrow & & \downarrow \\ \mathrm{Spec}(k(x)) & \xrightarrow{x} & X. \end{array} \tag{3.5}$$

If the scheme theoretic stabilizer of all points $x \in X$ is trivial, then like with abstract groups, G acts *freely* on X. If for some open subset $U \subset X$, G_x is trivial for all $x \in U$, then G is said to act *generically freely* on X.

If a linear representation of G is generically free, then the scheme U/G is a classifying scheme for $\mathrm{ed}_k(G)$, so gives rise to the following upper bound.

Proposition 3.2.1. [1, Prop. 4.11] *Suppose V is a vector space over k such that G acts on V linearly and generically-freely. Then*

$$\mathrm{ed}_k(G) \leq \dim(V) - \dim(G). \tag{3.6}$$

Remark 3.2.2. If G is a finite group, then a faithful representation V is automatically generically free, as G acts freely on the dense open set $V \backslash S$, where $S := \bigcup_{g \neq 1} S_g$, $S_g := \{x \in V \mid g \cdot x = x\}$.

Proposition 3.2.3. [SGA3, V, Theorem 8.1] *A G-scheme over k is generically free if and only if there is a non empty dense subscheme $U \subset X$ and a G-torsor $U \to Y$ with Y a variety over k.*

The G-torsor is defined by the choice of $U \to Y$, but this can be made suitably generic by taking the *generic fiber*, which is the pullback along $X \to Y$ and the generic point $\mathrm{Spec}(k(Y)) \to Y$, (corresponding to the prime ideal $\{0\}$).
Torsors in turn give rise to classifying schemes. Suppose $f : X \to Y$, with Y irreducible, is a G-torsor. Then $Y \to H^1(-, G)$ gives a classifying scheme subject to some conditions on f; for any infinite field extension k'/k and any principal homogeneous space P' of G over k'/k, the set of points $y \in Y(k)$ such that P is isomorphic to the fiber $f^{-1}(y)$ must be dense in Y. In this case $f : X \to Y$ is *classifying for G*. As before, any torsor classifying for G can be made generic by taking the corresponding generic fiber, and the generic fiber of a classifying torsor is the *generic torsor* of G.
From (3.3) the essential dimension is bounded by the minimum dimension of a classifying scheme. A *rational* map $f : X \dashrightarrow Y$ is a set of maps $f : U \to Y$, for U non-empty open set of X, where $f_1 : U_1 \to Y = f_2 : U_2 \to Y$ if $f_1(U') = f_2(U')$ for

some $U' \subset U_1 \cap U_2$. A *compression* of a G-torsor $f : X \to Y$ is a torsor $f' : X' \to Y'$ such that the following square commutes

$$\begin{array}{ccc} X & \overset{g}{\dashrightarrow} & X' \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f'} \\ Y & \overset{h}{\dashrightarrow} & Y', \end{array} \tag{3.7}$$

where g is a G-equivariant dominant (i.e. $f(X)$ is dense in Y), rational map $X \dashrightarrow X'$, and a h a rational map $Y \dashrightarrow Y$.

Lemma 3.2.4. [1, Lemma 6.13] *A compression $f' : X' \to Y'$ of a classifying torsor $f : X \to Y$ is also classifying.*

The essential dimension of a torsor, $\mathrm{ed}_k(f)$ is defined as $\min\{\dim(\mathrm{X}')\}$ across all compressions $f : X \to Y$ to $f' : X' \to Y'$. The essential dimension of a classifying torsor of an algebraic group is in fact equal to the essential dimension of the group itself.

Proposition 3.2.5. [1, Cor 6.16] *For an algebraic group G over k, $\mathrm{ed}_k(G) = \mathrm{ed}_k(f)$, where f is the generic torsor of G.*

The properties of a classifying torsor $f : X \to Y$ are mirrored in the properties of X; X must have that for every generically free G-scheme X' with $F(X')^G$ infinite and every dense open G-invariant set $U \subset X$, there is a G-equivariant rational morphism $X' \dashrightarrow U$. Such G-schemes X are called *versal*.

Example 3.2.6. [19, Sec. 5] Let V be a generically free representation of G, and X a G-scheme such that $F(X)^G$ is infinite and $U \subset V$ is non empty and G-invariant. A

representation V of G is a versal G-variety, and if G acts generically freely on V, this recovers the result in Proposition 3.2.1.

Example 3.2.7. Suppose V is a generically free representation of an algebraic group G, such that G also acts generically freely on $\mathbb{P}(V)$. Then $V \dashrightarrow \mathbb{P}(V)$ is a G-compression, so $\mathrm{ed}_k(G) \leq \dim(\mathbb{P}(V)) = \dim(V) - 1$.

In [40], the notion of essential dimension for algebraic groups was defined purely on the minimum dimension of a compression of a generically free G-variety. This was over characteristic 0, and in this case is equivalent to the definitions via compressions of G-torsors in [1], which this discourse has followed. The survey paper [34] synthesises both these viewpoints.

Proposition 3.2.8. [1, Thm. 6.19] *Suppose H is a subgroup of an algebraic group G over k. Then*

$$\mathrm{ed}_k(H) + \dim(H) \leq \mathrm{ed}_k(G) + \dim(G) \tag{3.8}$$

Proof. For V a generically free representation of G, and an open subset $U \subset V$ then $U \to U/G$ is a classifying torsor. Then there exists a G-compression

$$\begin{array}{ccc} U & \overset{g}{\dashrightarrow} & X \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f'} \\ U/G & \overset{h}{\dashrightarrow} & Y, \end{array} \tag{3.9}$$

where $\mathrm{ed}_k(G) = \dim(Y)$. As G acts generically freely on U and X, so does H. Similarly, as g is G-equivariant, it is also H-equivariant, so $U \to U/H$ must also have

a compression to $X \to Y$. Therefore

$$\begin{aligned} \mathrm{ed}_k(H) &\leq \dim(X) - \dim(H) \\ &= \mathrm{ed}_k(G) + \dim(G) - \dim(H). \end{aligned}$$

□

Note this implies for finite groups $\mathcal{H} \leq \mathcal{G}$, $\mathrm{ed}_k(\mathcal{H}) \leq \mathrm{ed}_k(\mathcal{G})$.

3.3 Lower bounds

Throughout, p denotes a prime integer. A useful lower bound on the essential dimension is given by the essential p-dimension, which is a p-local version of the essential dimension that is usually easier to find. A field extension K/k is *prime to* p if it is a finite extension, and $[K : k]$ is prime to p. The following are p-local versions of the earlier definitions so the set up is exactly as before. $\mathcal{F}$ is a functor $\mathbf{Fields}_k \to \mathbf{Set}$ with K/k a field extension. An element $x \in \mathcal{F}(K)$ is *p-defined* over a field K_0/k if there are morphisms $K_0 \to K'$ and $K \to K'$ in $\mathbf{Fields}_k$ for some field K'/k and an element $x_0 \in F(K_0)$ such that K'/K is a prime to p extension and x is in the image of $\mathcal{F}(K_0) \to \mathcal{F}(K')$. The *essential p-dimension* of x is then

$$\mathrm{ed}_k(x; p) := \min \text{ tr. } \deg_k(K_0) \tag{3.10}$$

amongst all fields K_0, such that x is p-defined over K_0. The essential p-dimension of $\mathcal{F}$ is therefore

$$\mathrm{ed}_k(\mathcal{F}; p) := \max \mathrm{ed}_k(x; p), \tag{3.11}$$

over all field extensions K/k and elements $x \in \mathcal{F}(K)$.

The essential p-dimension effectively disregards any data from fields K/k where $[K : k]$ is prime to p, and the essential dimension can be seen as a specific case of the essential p-dimension, by setting $p = 0$ (a "prime to 0" extension of K being only K itself). If an element x is defined over K_0, then it is p-defined over K_0, so $\mathrm{ed}_k(x; p) \leq \mathrm{ed}_k(x)$, so from its definition, $\mathrm{ed}_k(\mathcal{F}; p) \leq \mathrm{ed}_k(\mathcal{F})$.

When G is a finite p-group, the essential p-dimension is much easier to calculate.

Theorem 3.3.1. [24, Theorem 4.1] *Let G be a finite p-group, k a field of characteristic not p that contains a primitive p^{th} root of unity. Then*

$$\mathrm{ed}_k(G; p) = \mathrm{ed}_k(G) = \min \dim(V) \tag{3.12}$$

where the minimum runs over all faithful representations V of G over k.

There is also the following useful lemma.

Lemma 3.3.2. [35, Lemma 4.1] *Let G' be a closed subgroup of a smooth algebraic group G defined over k, where* $\mathrm{char}(k) \neq p$. *If the index $[G : G']$ is finite and prime to p, then* $\mathrm{ed}_k(G'; p) = \mathrm{ed}_k(G; p)$.

3.4 Essential p-dimension of algebraic tori

A split torus $T = (k^\times)^r$ has essential dimension 0, as the standard representation is generically free. However, if T is non-split then the value of the essential p-dimension follows from a combinatorial property of the underlying character lattice. Suppose T is a torus over k, so $T_{k_{\text{sep}}}$ is a split torus. Then the representations of $T_{k_{\text{sep}}}$ are of the form

$$V = \bigoplus_{\chi \in T^*_{k_{\text{sep}}}} V_\chi, \tag{3.13}$$

because $T_{k_{\text{sep}}}$ is abelian. However, not all representations of $T_{k_{\text{sep}}}$ descend to representations on T_k.

Proposition 3.4.1. [37, Thm. 14.22] *Let T be an algebraic torus over k. Define $\Gamma := \text{Gal}(k_{sep}/k)$. The irreducible representations of T are in one-to-one correspondence with orbits of Γ acting on $T^*_{k_{sep}}$.*

Proof. A representation $\rho_{k_{\text{sep}}} : T_{k_{\text{sep}}} \to k^\times_{\text{sep}}$ is defined over k if and only if it commutes with the action of Γ. As Γ acts by permuting the characters in $T^*_{k_{\text{sep}}}$, a representation must contain the orbit of the character under the action Γ. □

Let X be a $\mathbb{Z}\mathcal{G}$-module, with $\mathcal{G}$ a finite group. A *p-presentation* is a map of $\mathbb{Z}\mathcal{G}$-modules $\phi : P \to X$, where P is a permutation $\mathbb{Z}\mathcal{G}$-module, and the cokernel is finite and of order prime to p. A p-presentation $\phi : P \to X$ is the same as giving a surjective map $\phi_{(p)} : P \to X_{(p)}$, where $X_{(p)} := X \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$.

Theorem 3.4.2. [28, Corollary 5.1] *Let G be a group of multiplicative type over k, K/k be a finite Galois splitting field of G, and Γ_p be a Sylow p-subgroup of $\text{Gal}(K/k)$.*

Then

$$\mathrm{ed}_k(G;p) = \min \operatorname{rank}(\ker \phi), \tag{3.14}$$

where the minimum is taken over all p-presentations $\phi : P \to G^*$ of G^*, viewed as a $\mathbb{Z}\Gamma_p$-module.

Recall the definition of the decomposition group of an algebraic torus from (see Remark 2.3.9).

Corollary 3.4.3. *Let T be an algebraic torus defined over k, whose splitting field K/k has p power degree. Define $\psi_T : A_T \to T^*$ as the integral representation of the decomposition group of T. Then*

$$\mathrm{ed}_k(T;p) = \mathrm{SymRank}(\psi_T;p) - \dim(T) \tag{3.15}$$

Proof. From Theorem 3.4.2, it suffices to show that the minimum rank of the kernel of a p-presentation is equal to $\mathrm{SymRank}(\psi_T;p) - \dim(T)$. Given $\Delta \subset T^*$, a Γ_p-invariant subset which p-generates T^*, the image of the canonical map $\phi : \mathbb{Z}[\Delta] \to L$ is qT^*, for some q prime to p, therefore ϕ is a p-presentation, and $\operatorname{rank}(\ker \phi) = \operatorname{rank}(\mathbb{Z}[\Delta]) - \operatorname{rank}(T^*) = \mathrm{SymRank}(\psi_T;p) - \dim(T)$. Conversely, given a p-presentation, $\phi : P \to T^*$, pick a Γ_p-invariant $\mathbb{Z}$-basis $\Delta \subset P$. Then $\phi(\Delta)$ generates qT^*, where q is prime to p. □

Remark 3.4.4. An algebraic group G over k is *special* if $H^1(K,G) = 0$ for all field extensions K/k. If a torus T is special, then clearly $\mathrm{ed}_k(T;p) = 0$ for all $p > 0$.

A large amount of the original work in this thesis comes in Chapter 4,which is an exploration of the symmetric p-ranks of various lattices. The symmetric p-ranks of the automorphism groups of many low rank lattices can be found in Table 4.1, which, due to Theorem 3.4.2 gives the values of $\mathrm{ed}_k(T)$ for many low rank-tori. See 4.1 for more information on the choice of lattices and a discussion on the results found.

3.5 Essential dimension of extensions of algebraic tori

For the final section in this chapter, $\mathrm{ed}_k(G)$ is explored for groups G which are extensions of finite groups by tori. See Section 2.7 for a more robust introduction to these groups and how to classify such extensions. Whereas the essential dimension for p-groups and algebraic tori are given exactly by the dimensions of certain representations, the situation here is a little harder. These groups have been studied before, owing to the fact that, if G is a connected semisimple group whose centre is finite, and N is the normalizer of a maximal torus $T \leq G$, then

$$\mathrm{ed}_k(N) \geq \mathrm{ed}_k(G).$$

See [40, Prop 4.3] (in this instance the proof doesn't rely on k having characteristic 0). This was employed by Meyer and Reichstein in [35] for calculating bounds on $\mathrm{ed}_k(\mathrm{PGL}_n)$, and by MacDonald in [30] for calculating bounds on the values of $\mathrm{ed}_k(G;p)$ for semisimple groups G.

For split extensions, there exists a simple lower bound.

Proposition 3.5.1. *Let $G := T \rtimes F$, T an algebraic torus, F a finite group, over a field k. Then* $\mathrm{ed}_k(F) \leq \mathrm{ed}_k(G)$.

Proof. G is a split extension, so the following

$$F \longrightarrow T \rtimes F \longrightarrow F, \tag{3.16}$$

composes to the identity. Applying the Galois cohomology functor, this induces the sequence

$$H^1(k, F) \longrightarrow H^1(k, T \rtimes F) \longrightarrow H^1(k, F), \tag{3.17}$$

which also composes to the identity, meaning $H^1(k, T \rtimes F) \to H^1(k, F)$ is a surjection. □

Recall from Corollary 3.2.1 that the essential dimension of an algebraic group is bounded above by the dimension of a generically free representation.

Proposition 3.5.2. [35, Lemma 3.2] *Let G satisfy (2.31), and suppose W is a faithful representation of F and V is a representation of G which is generically free on its restriction to T. Then $V \times W$ is a generically free representation of G.*

Proof. Remark 3.2.2 shows that a faithful action by a finite group (constant group scheme) is generically free, so it acts freely on a dense open subset $U_W \subset W$ so $\mathrm{Stab}_G(U_W) = T$. T acts freely on a dense open subset $U_V \subset V$, $\mathrm{Stab}_T(U_V) = \{1\}$ therefore $\mathrm{Stab}_G(U_W \times U_V) = \mathrm{Stab}_G(U_V) \cap \mathrm{Stab}_G(U_W) = \mathrm{Stab}_T(U_V) = 1$, so G acts freely on an open dense subset of $V \times W$. □

This next lemma assumes no restrictions on the base field k. Recall that for a representation of torus $T \to \mathrm{GL}(V)$ V splits into one dimensional irreducible representations, or *weight spaces* $V = \bigoplus_{\lambda \in \Delta} V_\lambda$, for $\Delta \subset T^*$ (the set of weights). The action of T on these weight spaces by multiplication, in a generalisation of the notion of eigenspaces.

Lemma 3.5.3. [18, Lemma 2.3] *Let G be a group over k satisfying (2.31). Suppose G acts on a vector space V such that*

1. *Every weight of V has multiplicity 1, and*
2. *For Ω the set of weights of V, F acts faithfully on the kernel of the map $\psi : \bigoplus_{\omega \in \Omega} \mathbb{Z} \to T^*;\ n_\omega \mapsto \sum_\omega n_\omega \omega$.*

If T acts faithfully on V resp. $\mathbb{P}(V)$ (the projectivisation of V), then G acts generically freely on V resp. $\mathbb{P}(V)$.

The second condition will be denoted K_F, so an invariant subset of $\Lambda \subset T^*$ "satisfies K_F" if F acts faithfully on the kernel of the map $\mathbb{Z}[\Lambda] \to T^*$.

Example 3.5.4. An easy non-trivial example where the second part fails in Lemma 3.5.3 is for the root lattice $A_2 = \{(\alpha, \beta, -\alpha - \beta) \mid \alpha, \beta \in \mathbb{Z}\}$. If $T := \mathrm{Diag}(A_2)$, and $F := \mathcal{C}_3$ which permutes $\Delta := \{\alpha,\ \beta,\ -\alpha - \beta\}$, then the map $\psi : \mathbb{Z}[\Delta] \to T^*$ has kernel $\langle (1,1,1) \rangle$, which is fixed under the action of F.

Additionally to the symmetric p-ranks calculated in Table 4.1, the condition K_F is checked on each of the generating subsets, using an algorithm implemented in GAP.

Code for this can be found in Appendix C.2.1.

In order to calculate the essential p-dimension, often a change of base field is necessary.

Definition 3.5.5. A field K is *p-special* if every finite extension of K has degree a power of p. Every field k has some algebraic field extension $k^{(p)}$ that is p-special, called the p-special closure of k.

Some results on the essential p-dimension are defined for a smooth algebraic group. The following lemma shows that by replacing k by a p-special closure gives a smooth algebraic group with the same essential p-dimension.

Lemma 3.5.6. [29, Lemma 2.1] *A group G defined over $k^{(p)}$ is smooth, and for any field k,* $\mathrm{char}(k) \neq p$, $\mathrm{ed}_k(G;p) = \mathrm{ed}_{k^{(p)}}(G;p)$.

A linear representation $\phi : G \to \mathrm{GL}(V)$ is *p-generically free* (respectively, *p-faithful*) if $\ker\phi$ is finite of order prime to p, and ϕ descends to a generically free (respectively, faithful) representation of $G/\ker\phi$.

Theorem 3.5.7. [29, Thm. 1.1] *Let G be a group over a p-special field of characteristic not p satisfying (2.31) such that F is a finite p-group. Then*

$$\min \dim(\rho) - \dim(G) \leq \mathrm{ed}_k(G;p) \leq \min \dim(\mu) - \dim(G), \tag{3.18}$$

where the minima are taken over all p-faithful linear representations ρ and all p-generically free representations μ of G respectively.

If the group is a torus, the lower and upper bounds are equal ([28, Lemma 2.5]) and likewise with finite groups, (see Remark 3.2.2).

The gap between the p-faithful and p-generically free representations is a difficult one to narrow, and is the cause of the difference in bounds that occur in Chapter 5. Even the very simple case explored in Example 2.7.8 has a difference between the two bounds.

Example 3.5.8. An easy example of a p-faithful representation which fails to be p-generically free can be found for the group $G := \mathrm{Diag}(A_{p-1}) \rtimes \mathcal{C}_p$, where $\mathrm{Diag}(A_{p-1})$, the torus of root datum of Lie type A_{p-1} (when $p = 2$, this group is O_2). The dimension p representation of G which embeds $\mathrm{Diag}(A_{p-1})$ in $\mathbb{G}_m^p$ as the matrix $\mathrm{diag}\{(t_1, \ldots, t_{p-1}, t_1^{-1} \ldots t_{p-1}^{-1})\}$, and $\mathcal{C}_p$ as $p \times p$ permutation matrices is not generically free. The generic point $(\alpha_1, \ldots, \alpha_p)$, $\alpha_i \neq 0$ is stabilised by

$$\begin{pmatrix} 0 & \frac{\alpha_1}{\alpha_2} & 0 & \cdots \\ \vdots & 0 & \ddots & 0 \\ 0 & \cdots & 0 & \frac{\alpha_{p-1}}{\alpha_p} \\ \frac{\alpha_1}{\alpha_p} & 0 & \cdots & 0 \end{pmatrix}.$$

Chapter 4

The symmetric p-rank

This chapter is an exploration of the symmetric p-ranks of some integral representations (see Definition 2.4.5). To give an idea of the values the symmetric p-rank can take, Table 4.1 contains the symmetric p-ranks of the automorphism groups of all irreducible maximal finite subgroups of $\mathrm{GL}_n(\mathbb{Z})$ up to dimension 9. The descriptions of the lattices used are from [11], and the symmetric p-rank is calculated using an algorithm implemented in MAGMA.

For lattices associated to root systems, the symmetric p-ranks of both the full automorphism group and Weyl group, (along with any intermediate groups between the two) was completed in [30] (Tables I–III). These calculations gave bounds on the essential dimension of simple algebraic groups, (see Section 3.5).

Weyl groups appear naturally as the symmetries of the root lattices for the root datum of algebraic groups, though they fall into a more general class of groups; complex reflection groups. Though there isn't a canonical way to embed them in a root lattice,

as with Weyl groups, they do appear as symmetries in other lattices. For instance, the symmetry group of the Coxeter-Todd lattice has as an index 2 subgroup the complex reflection group $(\mathcal{C}_6 \rtimes \mathrm{PSU}_4(\mathbb{F}_3)) \rtimes \mathcal{C}_2$ (known as *Mitchell's group*). The lattices associated to the some of the complex refection groups will be explored, and their symmetric p-ranks calculated, in Table 4.2. The chapter concludes with the calculation of the symmetric p-rank for a particularly famous lattice; the Leech lattice.
The following example highlights how different the value of the symmetric p-ranks can be, even among lattices of the same family with the same automorphism groups.

Example 4.0.1. The integer lattice I_n is generated by the standard basis vectors $\{e_i\}$ and has automorphism group $\mathcal{C}_2 \wr S_n$, which acts by permuting the coordinates and multiplying each entry by ± 1. For $p > 2$, $\mathrm{SymRank}(I_n; p) = n$, as the standard basis vectors are permuted under the action of S_n. As the -1 action is included in the Sylow 2-subgroup, then $\mathrm{SymRank}(I_n; 2) = 2n$, achieved by taking the invariant set $\pm e_i$.
The lattice D_n^* is generated by the standard basis vectors along with $\frac{1}{2}\sum e_i$, so any element in D_n^* must have entries either all integers, or all half integers. The full automorphism group is the same, and the vectors $\{e_i\}$ generate a full rank sublattice of index 2. Therefore, for $p > 2$, $\mathrm{SymRank}(D_n^*; p) = n$. However, for $p = 2$, any 2-generating set must include a coordinate with a half integer, so all entries must be a half integer. Under the Sylow 2-subgroup (which includes an action of $\pm$ on each entry), this vector must have orbit size of at least 2^n. The orbit of $(\frac{1}{2}, \ldots, \frac{1}{2})$ generates D_n^* and has size 2^n, so $\mathrm{SymRank}(D_n^*; 2) = 2^n$. This is can be interpreted geometrically, where the generating set is the 2^n vertices of a unit hypercube, and the smaller 2-generating set as the midpoints of the $2n$ faces of the hypercube of edge

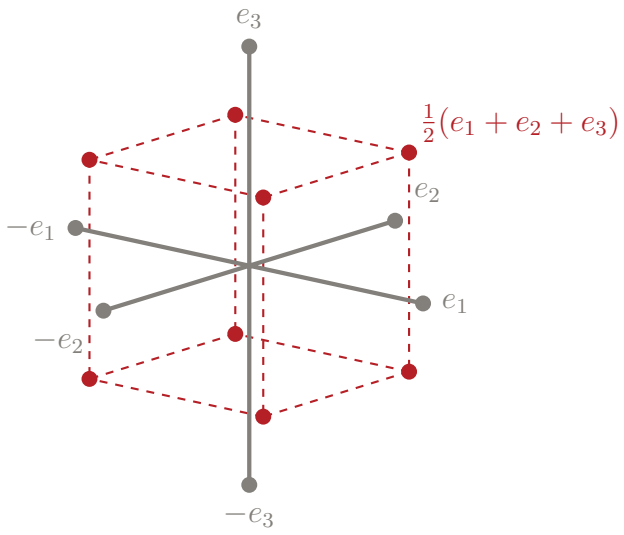


Figure 4.1: Two subsets of the D_3^* lattice, invariant under the action of its Sylow 2-subgroup. The subset containing $\frac{1}{2}(e_1+e_2+e_3)$ has size $2^n = 8$ generates the lattice, whereas the set $\{\pm e_i\}$ has size $2n = 6$ and generates an index 2 sublattice.

length 2.

The symmetric p-rank behaves well with taking direct products, the proof of which relies on Nakayama's Lemma.

Lemma 4.0.2. Nakayama's Lemma [12, §5.7] *Let R be a commutative ring, with Jacobson radical $\mathscr{J}$, and M a torsion-free R-module. Define $\overline{m}$ as the image of $m \in M$ under the surjection $M \to M/\mathscr{J}M$. If $\{m_i\} \in M$ are such that their images $\overline{m_i}$ generate $M \to M/\mathscr{J}M$, then the m_i generate M.*

The *augmentation ideal* I of the group ring $R := \mathbb{Z}\mathcal{G}$ is the kernel of the map $R \to \mathbb{Z}$; $\sum_i \alpha_i g_i \mapsto \sum_i \alpha_i$.

Lemma 4.0.3. [12, Cor. 5.25] *When $\mathcal{G}$ is a p-group, and R is the group ring $\mathbb{Z}\mathcal{G}$, the*

Jacobson radical of the ring $R_{(p)} := R \otimes \mathbb{Z}_{(p)}$ is the ideal generated by $(p + I)$, where I is the augmentation ideal.

Recall that for a subset of a $\mathcal{G}$-lattice, $\Delta \subset L$, a morphism $f : \mathbb{Z}[\Delta] \to L$ is a *p-presentation* if and only if the composition $f_{(p)} : \mathbb{Z}[\Delta] \to L \to L_{(p)}$ is surjective.
If L is a $\mathcal{G}$-lattice, where $\mathcal{G}$ is a p-group, then consider the surjection $L \to \overline{L} := L/(pL + IL)$. Any p-generating $\mathcal{G}$-invariant subset splits into disjoint $\mathcal{G}$-orbits $\Delta = \coprod \Delta_i$. For any point $l \in L$, the elements in the orbit of l under $\mathcal{G}$ belongs to the same equivalence class modulo $p + I$; $g \cdot l = (g - e) \cdot l + l$ and as $g - e \in I$, $\overline{l} = \overline{g \cdot l}$. Therefore $\mathcal{G}$ acts trivially on $\overline{L}$, and the image $\overline{\Delta_i}$ has rank 1. Nakayama's Lemma states that a basis of $\overline{L}$ gives a basis of $L_{(p)}$, which under the map $L \to L_{(p)}$ gives a p-generating set.

Proposition 4.0.4. *Let L, M be $\mathcal{G}_L$-, $\mathcal{G}_M$-lattices, and ϕ_L, ϕ_M be the corresponding integral representations. Then*

$$\mathrm{SymRank}(\phi_{L\oplus M}; p) = \mathrm{SymRank}(\phi_L; p) + \mathrm{SymRank}(\phi_M; p), \tag{4.1}$$

where $\phi_{L\oplus M}$ is the representation $\mathcal{G}_L \times \mathcal{G}_M \to \mathrm{GL}(L \oplus M)$.

Proof. Firstly, the group $\mathcal{G}_L \times \mathcal{G}_M$ acts on $(l, m) \in L \oplus M$ by $(g_l, g_m) \cdot (l, m) = (g_L \cdot l, g_M \cdot m)$. Define Γ_L and Γ_M as Sylow p-subgroups of $\mathcal{G}_L$, $\mathcal{G}_M$ respectively. If $\Delta_L \subset L$, $\Delta_M \subset M$ are p-generating and Γ_L-(resp. Γ_M-)invariant, then $\Delta_L \oplus \Delta_M \subset L \oplus M$ must be p-generating and $\Gamma_L \times \Gamma_M$-invariant. Therefore

$$\mathrm{SymRank}(\phi_{L\oplus M}; p) \leq \mathrm{SymRank}(\phi_L; p) + \mathrm{SymRank}(\phi_M; p).$$

To prove the opposite inequality, it will be shown that any p-generating $(\Gamma_L \times \Gamma_M)$-invariant subset $\Delta \subset L \oplus M$ can be replaced by some $(\Gamma_L \times \Gamma_M)$-invariant subset Δ' such that

1. $|\Delta'| \leq |\Delta|$
2. $\mathrm{Span}_{\mathbb{Z}}(\Delta') \supseteq \mathrm{Span}_{\mathbb{Z}}(q\Delta)$ for some $q \in \mathbb{Z}$ prime-to-p.
3. $\Delta' = \{(l_i, 0)\} \cup \{(0, m_i)\}$ for non zero $l_i \in L$, $m_i \in M$.

If this was the case, then $|\Delta'| \geq \mathrm{SymRank}(L; p) + \mathrm{SymRank}(M; p)$, so

$$\mathrm{SymRank}(\phi_{L\oplus M}; p) \geq \mathrm{SymRank}(\phi_L; p) + \mathrm{SymRank}(\phi_M; p).$$

To show such a Δ' exists, consider the image of Δ under the surjection $L \oplus M \to \overline{L \oplus M}$. As it is a surjection, and Δ p-generates $L \oplus M$, $\overline{\Delta}$ must generate $\overline{L \oplus M}$ as a $\mathbb{F}_p$-vector space. Take an orbit $\Delta_i \subseteq \Delta$. Then $\overline{\Delta_i}$ is a rank 1 element $(l, m) \in \overline{L \oplus M}$. As $\overline{\Delta}$ generates $\overline{L \oplus M}$, either $(l, 0) \in \mathrm{Span}_{\mathbb{F}_p}(\overline{\Delta})$ or $(0, m) \in \mathrm{Span}_{\mathbb{F}_p}(\overline{\Delta})$ (or neither). If the former is true, then define Δ_i' by replacing an orbit representative $(l', m') \in \Delta_i$ by $(0, m')$, and by $(l', 0)$ otherwise. Then Δ' is such that $\overline{\Delta'}$ still generates $\overline{L}$. Also, as the size of the $(\mathcal{G}_L \times \mathcal{G}_M)$-orbit of (l, m) is greater than the size of the orbit of either $(l, 0)$ or $(0, m)$, $|\Delta_i'| \leq |\Delta_i|$. Repeating this process for an orbit representative of each orbit in Δ gives a Δ' such that $\overline{\Delta}$ generates $\overline{L}$, and $|\Delta'| \leq |\Delta|$. By Nakayama's Lemma, Δ' must generate $(L \oplus M)_{(p)}$, so $\mathbb{Z}[\Delta'] \to (L \oplus M)_{(p)}$ is surjective and Δ' p-generates L. Therefore, Δ' satisfies the three conditions outlined and the result follows. $\square$

Remark 4.0.5. Note that if instead L and M are $\mathcal{G}$-lattices, then it is easy to check that the same argument holds for the symmetric p-rank of $\phi : \mathcal{G} \to L \oplus M$, where $\mathcal{G}$ acts diagonally.

4.0.1 A method of Merkurjev

If L is a $\mathcal{G}$-lattice, define $\overline{L} := L/(pL + IL)$, where I is the augmentation ideal of $\mathbb{Z}\mathcal{G}$, and p a prime. Fix a Sylow p-subgroup $\Gamma_p \leq \mathcal{G}$. For a subgroup $\mathcal{H}$ of Γ_p, $\overline{L^{\mathcal{H}}}$ is the canonical image of the $\mathcal{H}$-fixed points of L in $\overline{L}$. Define the following for $k \in \mathbb{N}$,

$$V_k := \coprod_{\mathcal{H} \leq \Gamma_p} \overline{L^{\mathcal{H}}} \tag{4.2}$$

where the union ranges over all $\mathcal{H}$ where $[\Gamma_p : \mathcal{H}] \mid p^k$. There is a natural inclusion

$$0 =: V_{-1} \subseteq V_0 \subset \ldots V_r = \overline{L}, \tag{4.3}$$

where $|\Gamma_p| = p^r$.

Proposition 4.0.6. [33, Thm. 4.3] *Let L be a $\mathcal{G}$-lattice. Using the definition of V_k at (4.2),*

$$\mathrm{SymRank}(L, p) = \sum_{k=0}^{r} (\mathrm{rank}(V_k) - \mathrm{rank}(V_{k-1}))p^k \tag{4.4}$$

Using this algorithm is practical when $\Gamma_p \leq \mathcal{G}$ is small, however computing through the extensive list of all subgroups is computationally impossible as Γ_p gets large. It was implemented in MAGMA by the author (see Appendix C.1.1) to find the values of the symmetric p-rank in Table 4.1. This algorithm takes as an input a lattice L

from the database `IntegralMatrixGroupDatabase()` in MAGMA, and firstly finds the subspaces $V_k \subset \overline{L}$. Using the formula (4.4), it then outputs the symmetric p-ranks of $\mathrm{Aut}(L)$, for all p that divide the order of $\mathrm{Aut}(L)$.

4.0.2 The Smith Normal Form

The Smith Normal Form (see [14, § 12.3]) can be used to determine if a subset $X \subset \mathbb{Z}^n$ generates $\mathbb{Z}^n$. If A is an $M \times n$ matrix over $\mathbb{Z}$, then there exists invertible matrices P_1 and P_2 such that $P_1 A P_2 = D$, where D is a diagonal matrix whose n non-zero entries α_i satisfy $\alpha_i | \alpha_{i+1}$ for $1 \leq i < n$. These α_i are the *elementary divisors*, and are unique up to multiplication by ± 1. D is the *Smith Normal Form* of A. A map ϕ is *p-surjective* if $|\mathrm{coker}(\phi)|$ is prime to p.

Proposition 4.0.7. *Let $X \subset \mathbb{Z}^n$ of size m, and A is the $m \times n$ matrix whose rows are the elements of X. Then X generates (resp. p-generates) $\mathbb{Z}^n$ if and only if* $\det(D) = \pm 1$ *(resp. q, where q is prime to p), where D is the Smith Normal Form of A.*

Proof. A is a $\mathbb{Z}$-linear transformation $\mathbb{Z}^m \to \mathbb{Z}^n$, and if A is (p)-surjective, X (p)-generates the lattice. As the P_i are isomorphisms of $\mathbb{Z}^m$ and $\mathbb{Z}^n$, then D is (p-)surjective if and only if A is (p)-surjective. However, D is a diagonal matrix defined over $\mathbb{Z}$, so is surjective if and only if its entries are ± 1, and is p-surjective if and only if its entries are all prime to p. □

Lemma 4.0.8. [30, Lemma 1.14] *Let $\phi : F \to \mathrm{GL}(L)$ be an integral representation, $L' \subset L$ is a sublattice of index prime-to-p, then*

$$\mathrm{SymRank}(\phi; p) = \mathrm{SymRank}(\phi|_{L'}; p).$$

Proof. Suppose X is a minimal invariant set that generates a sublattice of L' of index prime-to-p, X is an invariant p-generating set of L, so $\mathrm{SymRank}(\phi; p) \leq \mathrm{SymRank}(\phi|_{L'}; p)$. Now suppose X is a minimal invariant p-generating set of L, then cX for $c = [L : L']$ is a p-generating invariant set inside L', so $\mathrm{SymRank}(\phi; p) \geq \mathrm{SymRank}(\phi|_{L'}; p)$ □

4.1 Tables of symmetric p-ranks

To give an idea of the values of the symmetric p-ranks, Table 4.1 gives the values of the symmetric p-ranks of the full automorphism groups of each irreducible maximal finite subgroup of $\mathrm{GL}_n(\mathbb{Z})$. The descriptions of the following lattices are from [11], and the naming convention used there will be followed. Recall that for a lattice L, the following notation L^{+r} denotes a lattice of the same family, where $[L^{+r} : L] = r$ (see 2.4.1). These values were calculated using the algorithm in Section 4.0.1; the code for this can be found in Appendix C.1.1. Lastly, the column labelled K_F denotes the primes p for which the invariant p-generating set satisfies the condition K_F (see Lemma 3.5.3). The symbol "-" is used for when the lattice has no symmetry of that order, and "o" for when the lattice has a symmetry of that order, but the symmetric p rank is equal to the rank.

L	$\lvert\mathrm{Aut}(L)\rvert$	Symmetric p-rank				K_F
		$p=2$	$p=3$	$p=5$	$p=7$	
A_1	2	2	-	-	-	-
I_2	2^3	4	-	-	-	-
A_2	$2^2 \cdot 3$	4	3	-	-	-
I_3	$2^4 \cdot 3$	6	o	-	-	-
A_3		8	o	-	-	2
A_3^{+4}		8	o	-	-	2
D_4	$2^7 \cdot 3^2$	16	9	-	-	2, 3
$A_2 \otimes I_2$	$2^5 \cdot 3^2$	8	6	-	-	-
A_4	$2^4 \cdot 3 \cdot 5$	8	o	5	-	-
A_4^{+5}		8	o	5	-	-
I_4	$2^7 \cdot 3$	8	o	-	-	-
$A_2 \otimes A_2$	$2^4 \cdot 3^2$	8	9	-	-	3
I_5	$2^8 \cdot 3 \cdot 5$	10	o	o	-	-
D_5		16	o	o	-	2
D_5^{+4}		32	o	o	-	2
A_5	$2^5 \cdot 3^2 \cdot 5$	16	6	o	-	2, 3
A_5^{+2}		12	9	o	-	2, 3
A_5^{+3}		16	6	o	-	2
A_5^{+6}		12	6	o	-	2
I_6	$2^{10} \cdot 3^2 \cdot 5$	12	o	o	-	-
D_6		32	o	o	-	2
D_6^{+4}		64	o	o	-	2
$I_3 \otimes A_2$	$2^7 \cdot 3^4$	12	9	-	-	2
E_6	$2^8 \cdot 3^4 \cdot 5$	32	27	o	-	2, 3
E_6^{+3}		32	27	o	-	2, 3
A_6	$2^5 \cdot 3^2 \cdot 5 \cdot 7$	12	o	o	7	-
A_6^{+7}		12	o	o	7	-
$Q_6(1)$	$2^4 \cdot 3 \cdot 7$	16	o	-	7	2
$Q_6(4)$	$2^4 \cdot 3 \cdot 5$	16	o	o	-	2
$Q_6(4)^{+2}$		12	o	o	-	
$Q_6(4)^{+4}$		16	o	o	-	2

L	$\lvert\mathrm{Aut}(L)\rvert$	Symmetric p-rank				K_F
		$p=2$	$p=3$	$p=5$	$p=7$	
$A_3 \otimes I_2$	$2^9 \cdot 3^2$	16	o	-	-	2
$A_3^{+4} \otimes I_2$		16	o	-	-	-
D_6^{+2}	$2^9 \cdot 3^2 \cdot 5$	32	o	o	-	2
$A_3 \otimes A_2$	$2^5 \cdot 3^2$	16	9	-	-	2
$A_3^{+4} \otimes A_2$		16	9	-	-	2
I_7	$2^{11} \cdot 3^2 \cdot 5 \cdot 7$	14	o	o	o	-
D_7		40	o	o	o	2
D_7^{+4}		128	o	o	o	2
E_7	$2^{10} \cdot 3^4 \cdot 5 \cdot 7$	64	27	o	o	2, 3
E_7^{+2}		40	27	o	o	2, 3
A_7	$2^8 \cdot 3^2 \cdot 5 \cdot 7$	32	o	o	o	2
A_7^{+8}		16	o	o	o	2
I_8	$2^{15} \cdot 3^2 \cdot 5 \cdot 7$	16	o	o	o	-
D_8		64	o	o	o	2
D_8^{+4}		256	o	o	o	2
$D_4 \otimes I_2$	$2^{15} \cdot 3^4$	32	18	-	-	2, 3
E_8	$2^{14} \cdot 3^5 \cdot 5^2 \cdot 7$	128	81	25	o	2, 3, 5
$D_4 \otimes A_2$	$2^8 \cdot 3^3$	32	27	-	-	2, 3
$(D_4 \otimes A_2)^{+2}$	$2^7 \cdot 3^2$	32	12	-	-	2, 3
$(D_4 \otimes A_2)^{+4}$		64	27	-	-	2, 3
$(D_4 \otimes A_2)^{+8}$		24	12	-	-	2, 3
$I_4 \otimes A_2$	$2^{11} \cdot 3^5$	16	12	-	-	-
$(I_4 \otimes A_2)^{+3}$	$2^8 \cdot 3^5$	16	81	-	-	3
$(I_4 \otimes A_2)^{+27}$		16	27	-	-	27
$A_4 \otimes I_2$	$2^9 \cdot 3^2 \cdot 5^2$	16	o	10	-	-
$A_4^{+5} \otimes I_2$		16	o	o	-	-
$(A_4 \otimes I_2)^{+5}$	$2^8 \cdot 3^2 \cdot 5^2$	16	o	25	-	5
$Q_8(1)$	$2^7 \cdot 3^2 \cdot 5^2$	64	18	25	-	2, 3, 5
$A_4 \otimes A_2$	$2^5 \cdot 3^2 \cdot 5$	16	12	10	-	-
$A_4^{+5} \otimes A_2$		16	12	10	-	-

L	$\lvert\mathrm{Aut}(L)\rvert$	Symmetric p-rank				K_F
		$p=2$	$p=3$	$p=5$	$p=7$	
$Q_8(3)$	$2^5 \cdot 3 \cdot 7$	16	9	-	o	-
$Q_8(3)^{+3}$		16	9	-	o	-
$Q_8'(3)$		16	9	-	o	-
$Q_8'(3)^{+3}$		16	9	-	o	-
A_8	$2^8 \cdot 3^4 \cdot 5 \cdot 7$	16	27	o	o	3
A_8^{+9}		16	9	o	o	-
$A_2 \otimes A_2 \otimes I_2$	$2^9 \cdot 3^4$	16	18	-	-	3
$A_2^{\otimes 3}$	$2^5 \cdot 3^4$	16	27	-	-	3
I_9	$2^{16} \cdot 3^4 \cdot 5 \cdot 7$	18	o	o	o	-
D_9		32	o	o	o	2
D_9^*		512	o	o	o	2
A_9	$2^9 \cdot 3^4 \cdot 5^2 \cdot 7$	20	o	25	o	2, 5
A_9^{+2}		64	o	25	o	2, 5
A_9^{+5}		32	o	10	o	2
$A_9^{+10} = A_9^*$		32	o	10	o	2
$A_3 \otimes I_3$	$2^{13} \cdot 3^4$	24	o	-	-	2
$(A_3 \otimes I_3)^{+2}$		32	o	-	-	2
$(A_3 \otimes I_3)^{+4}$		128	o	-	-	2
$(A_3 \otimes I_3)^{+16}$		64	o	-	-	2
$(A_3 \otimes I_3)^{+32}$		128	o	-	-	2
$(A_3 \otimes I_3)^{+64}$		24	o	-	-	2
$A_3 \otimes A_3$	$2^8 \cdot 3^2$	32	o	-	-	2
$(A_3 \otimes A_3)^{+4096}$		32	o	-	-	2
$(A_3 \otimes A_3)^{+2}$	$2^{12} \cdot 3^2$	64	o	-	-	2
$(A_3 \otimes A_3)^{+2048}$		48	o	-	-	2
$A_3 \otimes A_3^*$	$2^7 \cdot 3^2$	32	o	-	-	2
$Q_9(5)$	$2^5 \cdot 3^2 \cdot 5$	24	o	10	-	2
$Q_9(5)^*$		24	o	10	-	2

Table 4.1: Symmetric p-ranks of automorphism groups of lattices up to dimension 9.

Remark 4.1.1. The lattice named "D_4" in Table 4.1 could also be called "F_4"; the $\mathbb{Z}$-span of the vectors of these root systems give equivalent lattices. The full automorphism group of this lattice is the Weyl group $W(F_4)$, of size 1152, and $W(D_4)$ is an index 6 subgroup inside $W(F_4)$.

For lattices of the form $L \otimes_{\mathbb{Z}} M$, the symmetric p-rank of the automorphism group is multiplicative except for when $p = 2$, when it is half the product of the individual symmetric 2-ranks. Recall from Section 2.4, the group $\mathrm{Aut}(L \otimes_{\mathbb{Z}} M)$ always contains the central product

$$(\mathrm{Aut}(L) \times \mathrm{Aut}(M))/(-1,-1).$$

For $p = 2$, if L and M are $\mathcal{G}_L$-, $\mathcal{G}_M$- lattices, both with a non-trivial action of -1, then the central product dictates that $(-1,1) = (1,-1)$, and the definition of the tensor product gives $r(l \otimes m) = (rl \otimes m) = (l \otimes rm)$ for $r \in \mathbb{Z}$, $l \in L$, $m \in M$. Therefore if $\Delta_L \coprod -\Delta_L$ and $\Delta_M \coprod -\Delta_M$ are 2-generating invariant sets of L and M, then $(\Delta_L \coprod \Delta'_L) \otimes (\Delta_M \coprod -\Delta_M) = (\Delta_L \coprod -\Delta_L) \otimes \Delta_M$, which gives a 2-generating and invariant subset. This is a strictly $p = 2$ phenomenon.

4.2 Complex reflection groups

A linear transformation g of a vector space V over a field F of characteristic 0 is a *reflection* if $[V, g] := \mathrm{Im}(\mathrm{Id} - g)$ has dimension 1. Intuitively, these are transformations that fix some hyperplane in V, and groups generated by reflections are consequently

called reflection groups. The *root* of a reflection g is any non-zero vector in $[V, g]$.

Let V be a complex vector space of dimension n, equipped with a positive definite hermitian form $(-,-) : V \times V \to \mathbb{C}$. An isometry g is a transformation that preserves this form (that is, $(u, v) = (g \cdot u, g \cdot v)$, and the unitary group, $U(V)$ is the group of isometries of V. Any finite reflection group $\mathcal{G}$ of V preserves some hermitian form (take $(u, v) := \sum_{g \in \mathcal{G}} (gu, gw)$), so is a subgroup of $U(V)$ after picking an appropriate hermitian form. As any two forms are equivalent over $\mathbb{C}$, $U(V)$ is unique up to conjugacy in $\mathrm{GL}(V)$ so $\mathcal{G}$ appears as a subgroup of $U(V)$ under the regular hermitian form$\langle , \rangle$, given by $\langle (u_1, \ldots, u_n), (v_1, \ldots, v_n) \rangle = u_1\overline{v_1} + \ldots u_n\overline{v_n}$, where $\overline{v_i}$ denotes complex conjugation, and $(u_1, \ldots, u_n)$, $(v_1, \ldots, v_n) \in \mathbb{C}^n$.

Groups $\mathcal{G}$ that are generated by complex reflections of some complex vector space V are called *complex reflection groups*, (sometimes unitary reflection groups in the literature) and if $\mathcal{G}$ is a finite subgroup of $U(V)$ with V irreducible, then $\mathcal{G}$ is an irreducible complex reflection group. These are the building blocks of all complex reflection groups, and were classified by Shephard and Todd in 1954. It was shown that the irreducible complex reflection groups belong either to a family $G(m, n, p)$ or are one of 34 exceptional groups. The description of the complex reflection groups can be found in [25], the reader is referred there and [4] for an introduction to the subject.

If N is the normalizer of a split torus T over a field k, $\mathrm{char}(k) \neq p$ in a semisimple algebraic group G, then define $\widehat{T}$ as the integral representation of the Weyl group $W \simeq N/T$ acting on the character lattice T^*. Theorem 1.10 in [30] asserts the following

$$\max\{\mathrm{SymRank}(\widehat{T}; p)\} - \dim(T), \mathrm{ed}(F; p)\} \leq \mathrm{ed}(N; p) \tag{4.5}$$

and

$$\mathrm{ed}(N;p) \leq \mathrm{SymRank}(\widehat{T};p) - \dim(T) + \mathrm{ed}(F;p). \tag{4.6}$$

Also, if the condition K_F was satisfied, then the lower bound was an equality. Due to the surjection of Galois cohomology $H^1(k,N) \twoheadrightarrow H^1(k,G)$, see [43, III.4.3 Lemma 6] together with [1, Lemma 1.3] the symmetric p-rank was calculated for each case, and this gave bounds on the essential p-dimension of G.

The aim of the following is to attempt something similar for some complex reflection groups, though there does exist some issues upon stepping outside the realm of Weyl groups.

Firstly, there is not necessarily a canonical choice for a root lattice; complex root systems form *complex lattices*, which are free $\mathscr{J}$-modules for some suitable ring $\mathscr{J} \subset \mathbb{C}$. However, often complex reflection groups appear as low index subgroups inside an irreducible maximal finite subgroup of $\mathrm{GL}_n(\mathbb{Z})$; this phenomenon is explored in Section 4.2.2.

Secondly, (4.5–4.6) relies on the construction of a representation of dimension equal to the symmetric p-rank; this was realised due to the representation of highest weight, which can only be applied in the case of algebraic groups. However, there does always exist a representation of this dimension for the split extension $T \rtimes W$ for a W action on T^*, and the arguments used in (4.5–4.6) can be applied to this group. For completeness, a proof is provided in Theorem 4.2.1, but note that the arguments are not the author's own.

Moreover, there doesn't exist an analogue of a semisimple algebraic group that has a complex reflection group as its Weyl group. Although there certainly does exist the group $T \rtimes W$ of which one can attain bounds on the essential p-dimension, this group

isn't a normalizer of a split torus inside some larger algebraic group.

The story doesn't quite end there however; the search for such analogues has lead to much fruitful mathematics, including the study of *Spetses*, where certain unipotent characters seem to evidence a mysterious algebraic structure that behaves like an analogue of semisimple algebraic groups for complex reflection groups, see [3] for more details.

Theorem 4.2.1. *Let L be a W-lattice for some finite group W, with $\phi_W : W \to \mathrm{GL}(L)$ the integral representation, and define the split torus $T := \mathrm{Diag}(L)$ over k, $\mathrm{char}(k) \neq p$. There exists the following bounds on $\mathrm{ed}_k(T \rtimes W; p)$,*

$$\max\{\mathrm{SymRank}(\phi_W; p)\} - \dim(T), \mathrm{ed}_k(W; p)\} \leq \mathrm{ed}_k(T \rtimes W; p)$$

and

$$\mathrm{ed}_k(T \rtimes W; p) \leq \mathrm{SymRank}(\phi_W; p) - \dim(T) + \mathrm{ed}_k(W; p).$$

If the p-generating subset of L satisfies K_F (see Lemma 3.5.3), then the lower bound is an equality.

Proof. Let Γ_p be a Sylow p-subgroup of W. Using Lemma 3.5.6 and replacing k by $k^{(p)}$, means the value of the essential p-dimension of the groups remains unchanged, and the groups are smooth. Then by Lemma 3.3.2, $\mathrm{ed}_k(T \rtimes W; p) = \mathrm{ed}_k(T \rtimes \Gamma_p; p)$, and $\mathrm{ed}_k(W; p) = \mathrm{ed}_k(\Gamma_p; p)$ so replace W by Γ_p. For the lower bound, as the extension is split, we can apply Proposition 3.5.1, so $\mathrm{ed}_k(\Gamma_p; p) \leq \mathrm{ed}_k(T \rtimes \Gamma_p; p)$. Also, suppose V is a p-faithful representation of $T \rtimes \Gamma_p$, which decomposes into weight spaces $\{V_\lambda \mid \lambda \in \Delta\}$ for a subset $\Delta \subset L = T^*$. As V is p-faithful, the elements in Δ

generate a sublattice of $L = T^*$ of index that is finite and prime to p (as shown in the proof of Corollary 3.4.3). As Γ_p permutes the weight spaces, Δ would also have to be invariant under Γ_p, hence $\dim(V) = |\Delta| \geq \mathrm{SymRank}(\phi_W; p)$. Applying the lower bound of Theorem 3.5.7 gives $\mathrm{SymRank}(\phi_W; p) - \dim(T) \leq \mathrm{ed}_k(T \rtimes W; p)$. If the subset Δ satisfies the condition K_F, then this is bound is an equality, by Lemma 3.5.3.

For the upper bound, let Δ be a minimal p-generating, Γ_p-invariant subset of L. Then there exists a p-faithful representation V_Δ of $T \rtimes \Gamma_p$ of dimension $|\Delta|$, given by $V_\Delta := \mathrm{Span}_k\{(v_\lambda) \mid \lambda \in \Delta\}$. The finite group group Γ_p acts by permuting the basis elements, $g : v_\lambda \mapsto v_{g\cdot\lambda}$, for all $g \in \Gamma_p$, $\lambda \in \Delta$, and T acts by $t : v_\lambda \mapsto \lambda(t)v_\lambda$ for any $t \in T$ and $v_\lambda \in V_\lambda$ (see [35, pp. 473]). This action on the basis $\{v_\lambda \mid \lambda \in \Delta\}$, is then extend linearly to the whole of V_Δ. If K_F is satisfied, then by Lemma 3.5.3 it is p-generically free, and if not, as Γ_p is a p-group, there exists a faithful representation V_Γ of Γ_p of dimension $\mathrm{ed}_k(\Gamma_p; p)$ (from Theorem 3.3.1) and by Proposition 3.5.2, $V_\Delta \times V_\Gamma$ is p-generically free of dimension $|\Delta| + \mathrm{ed}_k(W; p)$. □

Example 4.2.2 shows how to use the tables for calculating these bounds.

The symmetric p-ranks of lattices associated to complex reflection groups of rank 3 or greater (those which can be easily attributed to complex root systems) can be found in Table 4.2. and the essential p-dimension of the complex reflection groups themselves was studied in [15]. Remarkably it turns out to be equal to the number of fundamental invariants of W that divide p. The list for each of the complex reflection groups considered here is given in Table A.1 in Appendix A.

As a guide for Table 4.2, Σ denotes the complex root system (defined in 4.2.1), $\Lambda(\Sigma)_{\mathrm{real}}$

gives the lattice that contains that complex reflection group via the construction outlined in 4.2.2, along with the index of the complex reflection group in the full automorphism group of that lattice. The column labelled K_F denotes at which p the condition K_F is satisfied (see Lemma 3.5.3). The condition is not satisfied mostly in the cases where $\mathrm{SymRank}(\phi_L; p) = \mathrm{rank}(L)$ so $0 \leq \mathrm{ed}_k(G; p) \leq 1$, for G satisfying (2.31). As the only algebraic groups with essential dimension 0 are connected [40, Theorem 5.4], in this case $\mathrm{ed}_k(G; p) = 1$. To elucidate how to use Tables 4.2 and A.1 in conjunction with Theorem 4.2.1, consider the following example.

Example 4.2.2. Take the complex reflection group $\mathcal{J}_3^{(4)}$. For each prime considered, assume $\mathrm{char}(k) \neq p$. The corresponding lattice $Q_6(1)$ contains $W(\mathcal{J}_3^{(4)})$ as an index 2 subgroup (more information on this group is given in 4.3.2). The symmetric 2-rank of both the Weyl group and the larger full automorphism group is 16, and as K_F is satisfied for $p = 2$, $\mathrm{ed}(T \rtimes W(\mathcal{J}_3^{(4)}); 2) = 10$. The symmetric 3-rank is equal to the rank, and as mentioned previously $T \rtimes W(\mathcal{J}_3^{(4)})$ is not connected, its essential 3-dimension is therefore 1. Finally, the symmetric 7-rank is 7, so $1 \leq \mathrm{ed}(T \rtimes W(\mathcal{J}_3^{(4)}); 7) \leq 2$. In fact, as a $\mathcal{C}_7$-lattice, $Q_6(1) \simeq A_6$ (the A_6 root lattice) so $\mathrm{ed}_k(T \rtimes W(\mathcal{J}_3^{(4)}); 7) = \mathrm{ed}_k(\mathrm{Diag}(A_6) \rtimes \mathcal{C}_7; 7) = 2$ (see the beginning of 5.3 for an explanation of this figure).

Remark 4.2.3. Comparing Table 4.2 of symmetric p-ranks with Table A.1, some relationships appear. Firstly, $\mathrm{ed}_k(W; p) = 0$ precisely when the group W has no p-symmetry and if $\mathrm{ed}_k(W; p) = 1$, then the symmetric p-rank is either equal to the rank, or in the case of $p = 7$, the nearest multiple of p greater than the rank. For $\mathrm{ed}_k(W; p) = n \geq 2$, the value of the symmetric p-rank is always greater than p^n.

Σ	$\Lambda(\Sigma)_{\text{real}}$	$[\mathrm{Aut}(\Lambda) : W(\Sigma)]$	$\mathrm{SymRank}(\phi_L; p)$				K_F
			$p = 2$	$p = 3$	$p = 5$	$p = 7$	
$\mathcal{H}_3$	$Q_6(4)$	2	16	o	o	-	2
	$Q_6(4)^{+2}$		12	o	o	-	-
	$Q_6(4)^{+4}$		16	o	o	-	2
$\mathcal{J}_3^{(4)}$	$Q_6(1)$	2	16	o	-	7	2
$\mathcal{L}_3$	E_6	$2^5 \cdot 5$	16	27	-	-	2, 3
$\mathcal{M}_3$		$2^4 \cdot 5$	16	27	-	-	2, 3
$\mathcal{J}_3^{(5)}$	Q_{12}	2^2	32	54	o	-	2, 3
$\mathcal{F}_4$	D_4	1	16	9	-	-	2, 3
$\mathcal{H}_4$	$Q_8(1)$	2	64	18	25	-	2, 3, 5
$\mathcal{N}_4$	E_8	$2^5 \cdot 3^4 \cdot 5 \cdot 7$	64	o	10	-	2
$\mathcal{O}_4$		$2^4 \cdot 3^3 \cdot 5 \cdot 7$	128	18	10	-	2
$\mathcal{L}_4$		$2^7 \cdot 5 \cdot 7$	16	81	o	-	2, 3
$\mathcal{K}_5$	Q_{10}	2	128	81	o	-	2, 3
$\mathcal{K}_6$	K_{12}	2	128	243	o	14	2, 3
$\mathcal{E}_6$	E_6	2	32	27	o	-	2, 3
	E_6^{+3}		32	27	o	-	2, 3
$\mathcal{E}_7$	E_7	1	64	27	o	o	2, 3
	E_7^{+2}		40	27	o	o	2, 3
$\mathcal{E}_8$	E_8	1	128	81	25	o	2, 3, 5

Table 4.2: Symmetric p-ranks of lattices associated to complex reflection groups.

4.2.1 Complex lattices and root systems

Let F be a finite abelian extension of $\mathbb{Q}$, and $\mathscr{J}$ the intersection of F and the set of all algebraic integers, called the *ring of integers of F*. A $\mathscr{J}$*-lattice* is a collection of n linearly independent vectors in F^n, along with all their $\mathscr{J}$-linear combinations. Any submodule of a free $\mathscr{J}$-module is itself free if $\mathscr{J}$ is a principal ideal domain, and although this isn't necessarily the case *a priori* in practice, the specific $\mathscr{J}$ considered are indeed principal ideal domains. This leads to a natural generalisation of root systems for complex reflection groups, see [25, Def. 1.43].

Definition 4.2.4. [25] A $\mathscr{J}$-root system in a vector space V over F, with hermitian inner product $(-,-)$ is a pair (Σ, f), where Σ is a finite subset of V, $f: \Sigma \to \mathscr{J}^\times$ a function such that

1. Σ spans V and $0 \notin \Sigma$,
2. for all $\alpha \in \Sigma$ and $\lambda \in F$, $\lambda\alpha \in \Sigma$ if and only if $\lambda \in \mathscr{J}^\times$,
3. for all $\alpha \in \Sigma$ and $\lambda \in \mathscr{J}^\times$, $f(\lambda\alpha) = f(\alpha) \neq 1$,
4. for all $\alpha, \beta \in \Sigma$, the Cartan coefficient

$$\langle a \mid b \rangle = (1 - f(\beta))\frac{(\alpha, \beta)}{(\beta, \beta)}$$

   belongs to $\mathscr{J}$,

5. for all $\alpha, \beta \in \Sigma$, $r_{\alpha,f(\alpha)}(\beta) := \beta - (1 - f(\alpha))\dfrac{(v, f(\alpha))}{(\alpha, \alpha)}a \in \Sigma$ and $f(r_{\alpha,f(\alpha)}(\beta)) = f(\beta)$.

The group generated by the reflections $\{r_\alpha \mid \alpha \in (\Sigma, f)\}$, is denoted $W(\Sigma, f)$, and is called (in slightly confusing nomenclature) the Weyl group of the system. It will be shown later that many of the irreducible complex reflection groups are indeed Weyl groups of some complex root system. A notable difference between this and the "real" case is the fact that these reflections can have order greater than 2.

The complex lattice $\Lambda(\Sigma)$ is formed of the $\mathscr{J}$-linear combinations of the root system Σ; this gives a suitable generalisation of the root lattice of a real root system for complex reflection groups. From these "complex lattices" it is often possible to define a real counterpart; a free $\mathbb{Z}$-module, exhibiting the same symmetry as its complex counterpart. Throughout this chapter, define $\lambda = \frac{1}{2}(-1+\sqrt{-7})$ and $\sigma = \frac{1}{2}(-1+\sqrt{5})$, and the instances of $\mathscr{J}$ used in this chapter will be $\mathbb{Z}[\alpha] \in \mathbb{C}$, where α is one of $\{\lambda, \sigma, \zeta_p\}$, where ζ_p is a primitive p^{th} root of unity. To each of these α is assigned an involution; for a non real α, it is complex conjugation $x \mapsto \overline{x}$, otherwise $x \in \mathbb{Z}[\sigma]$, and the involution is $x \mapsto x'$, where $(a + b\sqrt{5})' = a - b\sqrt{5}$.

$\mathscr{J}$	$\zeta_3 = \omega = e^{\frac{2\pi i}{3}}$	$\lambda = \frac{1}{2}(-1+\sqrt{-7})$	$\sigma = \frac{1}{2}(-1+\sqrt{5})$
Involution	$\overline{\omega} = \omega^2 = -1-\omega$	$\overline{\lambda} = -1-\lambda$	$\sigma' = -\sigma - 1$

Table 4.3: Reference table for lattices associated to complex reflection groups.

4.2.2 $\Lambda(\Sigma)_{\mathbf{real}}$

There are different ways to obtain a real lattice $L \simeq \mathbb{Z}^n$ from a complex root system, or complex lattice Λ. Ideally, there would be a canonical choice, such that the automorphisms $\mathrm{GL}(L)$ are the same as $\mathrm{GL}(\Lambda)$. The following construction from [8, §2.6]

defines a real lattice Λ_{real}, from a complex lattice Λ. Firstly, for ω or λ, a complex $\mathscr{J}$-lattice vector $(x_1, \ldots, x_n) \in \Lambda$, defines a lattice vector

$$(\text{Re}(x_1), \text{Im}(x_1), \ldots, \text{Re}(x_n), \text{Im}(x_n)) \in \mathbb{Z}^{2n}. \tag{4.7}$$

For $\alpha = \sigma \in \mathbb{R}$, this lattice vector is instead

$$(x_1, \ldots, x_n, x_1', \ldots x_n'). \tag{4.8}$$

The integer combinations of these vectors give the elements of the rank $2n$ $\mathbb{Z}$-lattice, Λ_{real}, with inner product given by the Hermitian form

$$\begin{aligned}(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) &= \text{Re}(x_1\overline{y}_1 + \ldots x_n\overline{y_n}) \\ &= \frac{1}{2}(x_1\overline{y_1} + \overline{x_1}y_1 + \ldots + x_n\overline{y_n} + \overline{x_n}y_n)\end{aligned} \tag{4.9}$$

for $\alpha = \zeta_p$ or λ, and

$$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) = \frac{1}{2}(x_1y_1 + \ldots + x_ny_n + x_1'y_1' + \ldots x_n'y_n') \tag{4.10}$$

for $\alpha = \sigma$.

The lattice Λ_{real} is very closely related to its complex counterpart, and notably if $\mathcal{G}$ is a group of automorphisms of a complex $\mathscr{J}$-lattice Λ, (so comprised of elements of $\text{GL}_n(\mathscr{J})$), then $\mathcal{G}$ is a group of automorphisms of Λ_{real} as a subgroup of $\text{GL}_{2n}(\mathbb{Z})$. However these groups are often not isomorphic, as extra automorphisms of Λ_{real} creep in, for instance complex conjugation.

Example 4.2.5. Define $\omega := e^{\frac{2\pi i}{3}}$, and Λ a $\mathbb{Z}[\omega]$-lattice. Multiplication by ω gives an

order 3 automorphism of Λ that leaves no non-zero fixed points of Λ, which induces an order 3 automorphism of Λ_{real}. In fact if L is a real lattice, with a fixed-point-free automorphism of order 3, then $L = \Lambda_{\text{real}}$ for a $\mathbb{Z}[\omega]$-lattice Λ.

Now define $\theta := \omega - \overline{\omega} = \sqrt{-3}$. The element θ generates a prime ideal, indeed there exists an isomorphism of rings

$$\mathbb{Z}[\omega]/\theta\mathbb{Z}[\omega] \simeq \mathbb{Z}/3\mathbb{Z}. \tag{4.11}$$

The modulo 3 structure of Λ_{real} is the modulo θ-structure of Λ.

As a concrete example, the root lattice A_2 is Λ_{real} for $\Lambda := \mathbb{Z}[\omega]$. The automorphisms of $\mathbb{Z}[\omega]$ are multiplication by -1 and ω, which generate the cyclic group of order 6. This group sits as an index 2 subgroup of $\text{Aut}(A_2)$, with the extra symmetry coming from complex conjugation.

4.3 Symmetric p-ranks of lattices of complex reflection groups

For a complex root system Σ over $\mathscr{J}$, the $\mathscr{J}$-linear combinations of the roots form a $\mathscr{J}$-lattice, denoted by $\Lambda(\Sigma)$. Using the construction Λ_{real} on $\Lambda(\Sigma)$ returns lattices that contain $W(\Sigma)$ as a group of automorphisms.

This has a varied effect, in some cases $\Lambda(\Sigma)_{\text{real}}$ returns a previously known root lattice (either E_6, E_6^* or E_8), and the index of $W(\Sigma)$ in the full automorphism group is large. However in other cases $\Lambda(\Sigma)_{\text{real}}$ is a genuinely "new" lattice, that contains $W(\Sigma)$ as

a subgroup of small index, usually extended to the full automorphism group by an outer automorphism such as complex conjugation.

For some complex root systems, the ring of integers for Σ is $\mathbb{Q}$ (these are the groups more usually referred to as Weyl groups). In this case, the definition of Λ_{real} is simply the root lattice A_n, D_n or E_n, though embedded as

$$(l_1, \ldots l_n) \mapsto (l_1, 0, l_2, \ldots, l_n, 0).$$

For the remainder of this section, each complex root system of degree 3 or greater will be taken in turn. A description of the root system Σ, along with $W(\Sigma)$ is given, and the construction of the real lattice $\Lambda(\Sigma)_{\text{real}}$. By studying these groups, the value of each of the symmetric p-ranks of both $W(\Sigma)$ and the full automorphism group $\text{Aut}(\Lambda)_{\text{real}}(\Sigma)$ will be calculated and given, leading to the results in Table 4.2. Also, for each root system Σ, the Coxeter diagram $W(\Sigma)$ is given, see [4] for a description of these.

4.3.1 $\mathcal{H}_3$

Let $\tau := \frac{1+\sqrt{5}}{2}$, the golden ration, and $\sigma := \frac{1}{\tau} = \tau - 1$. The root system $\mathcal{H}_3 \in \mathbb{R}^3$ is formed by taking the 30 cyclic permutations of $(\pm 2, 0, 0)$ and $(\pm 1, \pm\tau, \pm\sigma)$. The reflections in these roots form the complex reflection group $W(\mathcal{H}_3) \cong \mathcal{C}_2 \times A_5$, which is the symmetry group of the icosahedron.

$\Lambda(\mathcal{H}_3)$ is the set of $\mathbb{Z}[\sigma]$ linear combinations of the roots of $\mathcal{H}_3$, and $\Lambda(\mathcal{H}_3)_{\text{real}}$ (as defined in Section 4.2) is the real rank 6 lattice $Q_6(4)$. The bilinear form on this

Figure 4.2: Coxeter diagram of $W(\mathcal{H}_3)$.

lattice is the following

$$(x_1, y_1, z_1) \cdot (x_2, y_2, z_2) = \frac{1}{2}(x_1x_2 + y_1y_2 + z_1z_2 + x_1'x_2' + y_1'y_2' + z_1'z_2'). \tag{4.12}$$

Embedding in $\mathbb{R}^3$, the roots of $\mathcal{H}_3$ form the midpoints of the edges of an icosahedron and under the bilinear form (4.12) have norm 4. These form the minimal vectors of the lattice $Q_6(4)$ ([11, pp. 46]), a member of the family of 3 lattices $Q_6^{+r}(4)$ all sharing the same bilinear form and automorphism group. The other two lattices have minimal vectors that correspond to the faces and vertices of the icosahedron.

The 20 faces of the icosahedron (equivalently the vertices of the dodecahedron) are given by the cyclic permutations of the coordinates $(\pm 1, \pm 1, \pm 1)$ and $(0, \pm\tau, \pm\sigma)$, and this gives rise to the 20 minimal vectors, with norm 3, of the lattice $Q_6^{+2}(4)$.

The lattice $Q_6^{+4}(4)$ has 24 minimal vectors, which are given by by two labellings of the 12 vertices of the icosahedron. The first set of 12 vertices, labelled $\{v_\infty, v_0, \ldots v_4\}$ are the cyclic permutations of $(0, \pm\sigma, \pm 1)$. The second labelling is the set $\{w_i\}$, where $w_i := \tau v_i$. Together, the corresponding vectors in $\mathbb{Z}^6$ of $\{v_i\}$ and $\{w_i\}$ form the 24 minimal vectors, with norm $\frac{5}{2}$, of the lattice $Q_6^{+4}(4)$.

It is possible to define the vectors of the other lattices in terms of v_i and w_i coordinates, as $Q_6(4) = \langle \pm v_i \pm v_j, \pm w_i \pm w_j \rangle$, and $Q_6^{+2}(4)$ is generated by differences between certain pairs of v_i and w_i. The containment is as follows

$$Q_6(4) \subset Q_6(4)^{+2} \subset Q_6(4)^{+4}. \tag{4.13}$$

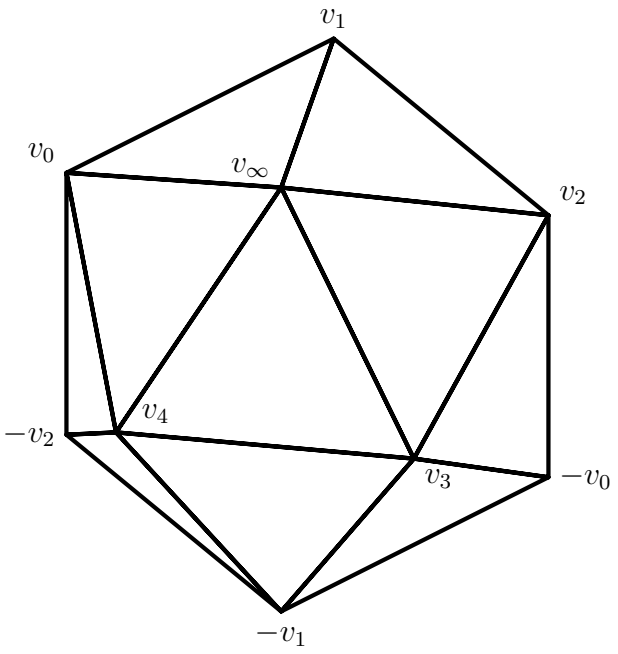


Figure 4.3: Position of $v_i \in Q_6^{+r}(4)$.

Using the characterisation via points on the icosahedron makes it very easy to un-

v_∞	$(\sigma, 1, 0)$
v_1	$(0, \sigma, -1)$
v_3	$(1, 0, \sigma)$

v_0	$(-\sigma, 1, 0)$
v_2	$(1, 0, -\sigma)$
v_4	$(0, \sigma, 1)$

Table 4.4: Coordinates of $v_i \in Q_6^{+r}(4)$.

derstand the automorphism group of $Q_6^{+r}(4)$. The group $\mathcal{C}_2 \times A_5$, is the group of symmetries of the icosahedron, and naturally this group leaves the sets $\{v_i\}$ and $\{w_i\}$ invariant. This extends to the full automorphism group by adding the conjugation map,

$$(x, y, z) \mapsto (x', z', y'). \tag{4.14}$$

where $(a + b\sqrt{5})' = a - b\sqrt{5}$, and this interchanges the sets $\{v_i\}$ and $\{w_i\}$. This automorphism group contains $W(\mathcal{H}_3)$ as an index 2 subgroup.

Remark 4.3.1. The notation for these lattices comes from [11, pp. 46], and the reason that the index of the vertices runs from $\{0, \ldots 4, \infty\}$ is due to the fact that the symmetries of icosahedron act on v_i exactly as the natural action of $\mathrm{PSL}_2(5)$ on $\mathbb{P}^1(\mathbb{F}_5)$.

The sets $\{v_i\}$ and $\{w_i\}$ satisfy linear relations called the *icosahedral* relations, the first of which says that $\sqrt{5}$ times any point is equal to the sum of all its adjacent points, for instance

$$\begin{aligned} v_0 + \ldots + v_4 &= \sqrt{5}v_\infty, \\ w_0 + \ldots + w_4 &= \sqrt{5}w_\infty. \end{aligned} \tag{4.15}$$

In particular, this means

$$\begin{aligned} v_0 + \ldots + v_4 + v_\infty &= v_\infty + \sqrt{5}v_\infty \\ &= 2(\tau v_\infty) \\ &= 2w_0. \end{aligned}$$

Similarly, $w_0 + \ldots + w_4 - w_\infty = 2v_\infty$. So the sets $\{v_i\}$ and $\{w_i\}$ each generate a full rank sublattice of index 2.

The second set of relations is that the sum of two adjacent v_i's equals the sum of the two corresponding adjoining w_i (the next closest two vertices to that common edge).

For instance,

$$v_\infty + v_4 = w_0 + w_3, \qquad v_\infty + v_2 = w_1 + w_3.$$

The Sylow 2-subgroup of $W(\mathcal{H}_3)$ is $\mathcal{C}_2^3$, and is generated by the symmetries that multiply each coordinate by -1. These are reflections in three mutually orthogonal planes with rectangles given by the vertices $\pm\{v_\infty, v_0\}$, $\pm\{v_1, v_4\}$ and $\pm\{v_2, v_3\}$. By adding the conjugation map (4.14), this generates $\mathrm{Syl}_2(\mathrm{Aut}(Q_6^{+r}(4))$, and this outer automorphism gives the Sylow 2-subgroup structure $\mathcal{C}_2 \times D_8$, D_8 being the dihedral group of order 8.

For $L = Q_6^{+2}(4)$, let ϕ_L be the integral representation of $\mathrm{Aut}(L)$, and $\phi_L|_{W(\mathcal{H}_3)}$ the restriction to the index 2 subgroup $W(\mathcal{H}_3)$.

Proposition 4.3.2. *For* $L = Q_6^{+2}(4)$, $\mathrm{SymRank}(\phi_L; 2) = \mathrm{SymRank}(\phi_L|_{W(\mathcal{H}_3)}; 2) = 12$ *for* $i = 1, 2$.

Proof. As mentioned previously, there exists an element $g \in W(\mathcal{H}_3)$ such that $\phi_L(g) = -1$, so $\mathrm{SymRank}(\phi_L|_{W(\mathcal{H}_3)}; 2) \geq \mathrm{SymRank}(\phi_L|_{W(\mathcal{H}_3)}; 2) \geq 12$. The orbit of $w_\infty - v_0 = (\tau, \sigma, 0)$ has size 12, and is formed by all the cyclic permutations of $(\pm\tau, \pm\sigma, 0)$. We claim that this subset generates L. The remaining 8 minimal vectors are $(\pm 1, \pm 1, \pm 1)$, and

$$(\tau, -\sigma, 0) + (-\sigma, 0, \tau) + (0, \tau, -\sigma) = (1, 1, 1).$$

Therefore all minimal vectors can be attained with appropriate choice of $\pm$ multiples of the coordinates. Therefore $12 \leq \mathrm{SymRank}(\phi_L|_{W(\mathcal{H}_3)}; 2) \leq \mathrm{SymRank}(\phi_L; 2) \leq 12$. □

Lemma 4.3.3. *Any vector* $x = (a_1 + b_1\sigma, a_2 + b_2\sigma, a_3 + b_3\sigma) \in Q_6(4)$ *satisfies* $\sum a_i \equiv \sum b_i \equiv 0 \bmod 2$.

Proof. The minimal vectors of $Q_6(4)$ are cyclic permutations of $(\pm 2, 0, 0)$ and $(\pm 1, \pm\sigma, \pm\tau)$. As $\tau = 1 + \sigma$, these satisfy the above condition. This property is preserved under addition, so applies to all elements in $Q_6(4)$. □

For the symmetric 2-ranks of the next two lattices, consider the map $\mathbb{Z}[\sigma] \mapsto \mathbb{F}_2^2$, where which takes an element to its class modulo $2\mathbb{Z}[\sigma]$. This extends to a map on the whole lattice, which will be denoted by f.

$$f : L \to \mathbb{F}_2^6. \tag{4.16}$$

Lemma 4.3.4. *If* $x = (\alpha_1, \alpha_2, \alpha_3) \in Q_6(4)$ *has orbit size less than 8 under the action of* $\mathcal{C}_2^3$, *or if* $x \in Q_6(4)^{+4}$ *has orbit size less than 4, then* $f(x) = 0$.

Proof. Firstly, for $\alpha \in [1, \sigma, \tau]$, neither $(\alpha, \alpha, 0)$, nor its cyclic permutations are in $Q_6(4)$, and similarly, $(\alpha, 0, 0)$ nor its cyclic permutations are in either $Q_6(4)$ nor $Q_6(4)^{+4}$. These all have norm less than 4, contradicting the minimality of the minimal vectors of $Q_6(4)^{+r}$. As the cyclic permutations of $(2, 0, 0)$ and $(2\sigma, 0, 0)$ are in $Q_6(4)^{+r}$ $r = 0, 4$, this in turn implies that the cyclic permutations of $(\alpha_1, \alpha_2, 0) \notin Q_6(4)$, and $(\alpha, 0, 0) \notin Q_6(4)^{+r}$, $r = 0, 4$ for $\alpha_i \not\equiv 0 \bmod 2\mathbb{Z}[\sigma]$.
The group $\mathcal{C}_2^3$ acts by -1 on each entry, so if $x = (\alpha_1, \alpha_2, \alpha_3) \in Q_6(4)$ has orbit size less than 8 under $\mathcal{C}_2^3$, then $\alpha_i = 0$ for some i, and the previous argument shows the other entries must be in $2\mathbb{Z}[\sigma]$, and a similar argument works for $Q_6(4)^{+4}$, so $f(x) = 0$

in all cases. □

Proposition 4.3.5. *Let $L = Q_6(4)$. Then*

$$\mathrm{SymRank}(\phi_L; 2) = \mathrm{SymRank}(\phi_L|_{W(\mathcal{H}_3)}; 2) = 16.$$

Proof. If X is a 2-generating set, invariant under $\mathcal{C}_2^3$, then it contains two elements $x = (\alpha_1, \alpha_2, \alpha_3)$, $y = (\beta_1, \beta_2, \beta_3) \in X$ with $\alpha_1 \not\equiv \beta_1 \not\equiv 0 \bmod 2\mathbb{Z}[\sigma]$, as $\mathbb{Z}[\sigma]/2\mathbb{Z}[\sigma] \simeq \mathbb{F}_2^2$. The action of $\mathcal{C}_2^3$ leaves the equivalence class of each entry invariant so they must have different orbits and Lemma 4.3.4 implies both x and y have orbit size 8. It remains to find a size 16 generating set, invariant under $\mathcal{C}_2^3$, and the conjugating map. Notice that the minimal vectors are split into 4 orbits of size 16, 8, 4 and 2, with representatives $(\tau, 1, \sigma)$, $(1, \sigma, \tau)$, $(0, 2, 0)$ and $(2, 0, 0)$ respectively. The size 16 orbit generates the lattice, as each of the other representatives can be found by integer linear combinations of elements of the orbit of $(\tau, 1, \sigma)$. Specifically,

$$\begin{aligned}
(1, \sigma, \tau) &= (\tau, -1, \sigma) + \overline{(\tau, 1, -\sigma)} \ (= (-\sigma, \tau, 1)), \\
(2, 0, 0) &= (1, \sigma, \tau) + (1, -\sigma, -\tau), \\
(0, 2, 0) &= (\tau, 1, \sigma) + (-\tau, 1, -\sigma).
\end{aligned}$$

The other elements of the orbits are achieved by using the linearity of the group action. So $16 \leq \mathrm{SymRank}(\phi_L|_{W(\mathcal{H}_3)}; 2) \leq \mathrm{SymRank}(\phi_L; 2) = 16) \leq 16$. □

Proposition 4.3.6. *Let $L = Q_6^{+4}(4)$. Then*

$$\mathrm{SymRank}(\phi_L; 2) = \mathrm{SymRank}(\phi_L|_{W(\mathcal{H}_3)}; 2) = 16.$$

Proof. As mentioned previously, the group $\mathcal{C}_2^3$ leaves invariant the equivalence class modulo $2\mathbb{Z}[\sigma]$ of the entries of $x \in L$. Consider the morphism $f : L \to (\mathbb{F}_2)^6$, where the entry of each vector is taken to its equivalence class modulo $2\mathbb{Z}[\omega]$. The image of L has rank at least 4; the images of $\{(\sigma, 1, 0), (0, \sigma, 1), (1, 0, \sigma), (1, 0, \tau)\}$ forming a linearly independent set. A set that 2-generates L must therefore generate its image under f. The group $\mathcal{C}_3^2$ acts trivially on $(\mathbb{F}_2)^6$, and by Lemma 4.3.4 any $x \in L$ with orbit size 2 or smaller has trivial image under this map, a set that must generate $f(L)$ must have size 4, each with a distinct orbit of size 4. Therefore a 2-generating invariant set must have size 16 at least.

The set $\pm\{v_2, v_3, w_0, w_\infty\} \cup \pm\{v_0, v_\infty, w_2, w_3\}$ has size 16 and is invariant under $\mathcal{C}_2^3$ and the conjugating map. It generates the whole lattice, as the rest of the minimal vectors ($\pm\{v_1, v_4, w_1, w_4\}$) are given from the following adjacency/adjoining relations,

$$v_0 + v_2 = w_\infty + w_1$$

$$v_1 + v_\infty = w_0 + w_2$$

$$v_4 + v_\infty = w_0 + w_3$$

$$v_0 + v_\infty = w_1 + w_4.$$

Therefore $16 \leq \mathrm{SymRank}(\phi_L|_{W(\mathcal{H}_3)}; 2) \leq \mathrm{SymRank}(\phi_L; 2) = 16) \leq 16$. □

For $p = 3$ and 5, both Sylow p-subgroups are $\mathcal{C}_p$. For $p = 3$ it is the rotation around a triangular face, (choosing for example the rotation $v_\infty \mapsto v_3 \mapsto v_4$ is the cyclic permutation of the coordinates $[x, y, z]$), and the order 5 automorphism is given by the rotation around any vertex.

Proposition 4.3.7. *For* $L = Q_6(4)^{+r}$, $\mathrm{SymRank}(\phi_L; 3) = 6$.

Proof. Take the Sylow 3-subgroup to be the rotation about the face given by the vertices $\{v_\infty, v_3, v_4\}$. For $Q_6(4)^{+4}$, the set $\{v_\infty, v_3, v_4, v_1, v_0, v_2\}$ is invariant. This contains all points v_i, up to -1 sign, so generates a sublattice of index 2, so 3-generates. Lemma 4.0.8 gives the symmetric 3-ranks of the other lattices. □

Proposition 4.3.8. *For* $L = Q_6(4)^{+r}$, $\mathrm{SymRank}(\phi_L; 5) = 6$

Proof. Take the Sylow 5-subgroup to be the rotation about the vertex v_∞. It is sufficient to find a fixed point of this rotation, and together with an appropriate orbit of 5 minimal vectors gives an invariant generating set. For $Q_6(4)^{+4}$, the set $\{v_\infty, v_3, v_4, v_1, v_0, v_2\}$ is invariant. This contains all points v_i, up to -1 sign, so generates a sublattice of index 2, so 5-generates. Again using Lemma 4.0.8 gives the symmetric 5-rank. □

4.3.2 $\mathcal{J}_3^{(4)}$

The roots of the root system $\mathcal{J}_3^{(4)}$ are the cyclic permutations of the following

$$(\pm 2, 0, 0),\ (\pm\lambda, \pm 1, \pm 1) \text{ and } (0, \pm\mu, \pm\mu), \tag{4.17}$$

where $\lambda := \frac{-1+\sqrt{7}i}{2}$, and $\mu := \overline{\lambda}$; the roots of the quadratic $x^2 + x + 2$. The corresponding complex reflection group $W(\mathcal{J}_3^{(4)})$ is isomorphic to $\mathcal{C}_2 \times \mathrm{PSL}_2(\mathbb{F}_7)$, which is the automorphism group of the Klein quartic, the second smallest nonabelian simple group. $\Lambda(\mathcal{J}_3^{(4)})$ is the complex rank 3 $\mathbb{Z}[\lambda]$-lattice generated by the roots of $\mathcal{J}_3^{(4)}$, and

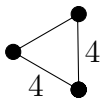


Figure 4.4: Coxeter diagram of $W(\mathcal{J}_3^{(4)})$.

the rank 6 lattice $Q_6(1)$ is the name given to the real lattice, $\Lambda(\mathcal{J}_3^{(4)})_{\text{real}}$. The group $W(\mathcal{J}_3^{(4)}) \simeq \mathcal{C}_2 \times \mathrm{PSL}_2(\mathbb{F}_7)$ of order $2^4 \cdot 3 \cdot 7$, [25, pp. 160] and this is an index 2 subgroup inside $\mathrm{Aut}(Q_6(1))$ [11, pp. 45].

The Sylow 2-subgroup of $W(\mathcal{J}_3^{(4)})$ has order 2^4, generated by ± 1 on each coordinate, along with an order 2 reflection which acts by swapping the last two entries. One can see this acts on the set of minimal vectors. The Sylow 3-subgroup acts by cyclically permuting the entries. As usual, denote by ϕ_L^1 and ϕ_L^2 as the integral representations of $W(\mathcal{J}_3^{(4)})$ and $\mathrm{Aut}(Q_6(1))$ respectively.

Lemma 4.3.9. *For* $(a_1 + b_1\lambda, a_2 + b_2\lambda, a_3 + b_3\lambda) \in Q_6(1)$, a_i, $b_i \in \mathbb{Z}$,

$$a_1 + b_1 \equiv a_2 + b_2 \equiv a_3 + b_3 \bmod 2, \text{ and} \tag{4.18}$$

$$\sum a_i \equiv 0 \bmod 2. \tag{4.19}$$

Proof. Note that both these properties are preserved under addition; it remains to show they are both true for the minimal vectors, which is easy to check, using that $[0, \mu, \mu] = [0, -1 - \lambda, -1 - \lambda]$. □

Proposition 4.3.10. *For* $L = Q_6(1)$, $\mathrm{SymRank}(\phi_L^i; 2) = 16$.

Proof. Suppose for a contradiction $X \subset Q_6(1)$ is a 2-generating invariant set with $|X| < 16$. By Lemma 4.3.9 there must exist $x = (a_1 + b_1\lambda, a_2 + b_2\lambda, a_3 + b_3\lambda) \in X$

whose entries satisfy $a_i + b_i \equiv 1 \bmod 2$ (as for instance $(\lambda, 1, 1) \in Q_6(1)$). As all entries must be non-zero, the orbit of x has size at least 8. If $|X| < 16$, then the orbit of x must then have size 8, and be invariant under the action of swapping the last two entries. It must have the form $x = (\alpha, \beta, \beta)$, α, $\beta \in \mathbb{Z}[\lambda]$; denote the orbit of x by $\mathcal{O}_x$.

All other elements $y = a_i + b_i\lambda \in X \setminus \mathcal{O}_x$ for $i \in 1, 2, 3$ must have orbit size 4 or less, and by the previous argument must have $(a_i + b_i)$ even. Inspecting orbit sizes, y is either equal to $(0, a, a)$ or a cyclic permutation of $(2a, 0, 0)$, $a \in \mathbb{Z}[\lambda]$. Therefore all elements $(\alpha_1, \alpha_2, \alpha_3) \in X$, $\alpha_i \in \mathbb{Z}[\lambda]$, are such that $\alpha_2 \equiv \alpha_3 \bmod 2\mathbb{Z}[\lambda]$, so for instance $(\mu, 0, \mu) \notin \mathrm{Span}_{\mathbb{Z}}(qX)$ for any odd q. Thus X is not 2-generating.

The orbits of $(\lambda, 1, 1)$ and $(0, \mu, \mu)$ have each size 8 and together generate $Q_6(1)$, which is also invariant under the action of $\mathrm{Syl}_2(\mathrm{Aut}(Q_6(1))$. This is verified in Appendix C.2.2, and therefore $16 \leq \mathrm{SymRank}(\phi_L^1; 2) \leq \mathrm{SymRank}(\phi_L^2; 2) \leq 16$. □

The symmetric 3-rank is very easy to find thanks to the following easy $\mathbb{Z}$-basis.

Proposition 4.3.11. *For $L = Q_6(1)$, $\mathrm{SymRank}(\phi_L; 3) = 6$*

Proof. The cyclic permutations of $[\lambda, 1, 1]$ and $[\lambda, -1, 1]$ form a $\mathbb{Z}[\lambda]$-basis for $Q_6(1)$. As $[\lambda, 1, 1] - [\lambda, 1, -1] = [0, 2, 0]$, and adding cyclic permutations of $(2, 0, 0)$ gives all coordinates of type $(\pm\lambda, \pm 1, \pm 1)$. Lastly, as $\lambda + \mu = -1$, $[0, \mu, \mu] = -[1, \lambda, 1] - [-1, 1, \lambda]$, and $[0, \mu, -\mu] = [1, 1, \lambda] - [1, \lambda, 1] - [0, 2, 0] + [0, 0, 2]$. □

Proposition 4.3.12. *For $L = Q_6(1)$, $\mathrm{SymRank}(\phi_L; 7) = 7$.*

Proof. There are only 3 indecomposable $\mathcal{C}_p$-lattices, for $p \leq 19$ (see [12, Thm 34.31 pp. 729]), which are; the trivial lattice $\mathbb{Z}$, the permutation lattice $\mathbb{Z}[\mathcal{C}_p]$ and the

root lattice A_{p-1}. $Q_6(1)$ has rank 6, and as the $\mathcal{C}_7$ acts non trivially, a $\mathcal{C}_7$-lattice, $Q_6(1) \simeq A_6$, so $\mathrm{SymRank}(Q_6(1); 7) = \mathrm{SymRank}(A_6(1); 7) = 7$. □

4.3.3 $\mathcal{L}_3$ and $\mathcal{M}_3$

The descriptions of these root systems Σ and the groups $W(\Sigma)$ are from [25, pp. 149, 162]. $\mathcal{L}_3$ is given by the permutations and ω^i multiples on each entry of $(\theta, 0, 0)$ and $(1, 1, 1)$, where $\theta = \omega - \omega^2 = \sqrt{-3}$, consisting of 36 points. These, along with their -1 multiples form the minimal vectors (of norm 3) of the lattice $\Lambda(\mathcal{L}_3)_{\mathrm{real}}$, which is in fact the root lattice E_6. The description of E_6 as this rank 3 $\mathbb{Z}[\omega]$-lattice is given in [8, pp. 126], therefore $W(\mathcal{L}_3)$ is those automorphisms $\mathrm{GL}_3(\mathbb{Z}[\omega])$ preserving the hermitian form. It has order $2^3 \cdot 3^4$, and is generated by the order 4 reflection

$$\frac{1}{\theta}\begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}, \tag{4.20}$$

along with permutation of the the entries, and $\mathrm{diag}\{(\omega^{a_1}, \omega^{a_2}, \omega^{a_3})\}$, $0 \leq a_i \leq 2$. This group is also the triple cover of the *Hessian* group.

Figure 4.5: Coxeter diagrams of $W(\mathcal{L}_3)$ and $W(\mathcal{M}_3)$.

The complex root system $\mathcal{M}_3$ is given by the points $(1, \omega, 0)$ under the action of the group $W(\mathcal{L}_3)$, which yields 27 vectors. This set, along with its -1 multi-

ples, form the 54 minimal vectors (of norm 2) of $\Lambda(\mathcal{M}_3)_{\text{real}}$, which is the lattice E_6^{+3}. One can see $\Lambda(\mathcal{L}_3)_{\text{real}}$ is a sublattice inside $\Lambda(\mathcal{M}_3)_{\text{real}}$, for instance $(1,1,1) = (1,-\omega,0)-(0,\omega,-\omega^2)+(0,1,-\omega)$. The group $W(\mathcal{M}_3)$ is generated by $W(\mathcal{L}_3)$, along with complex conjugation. An example of $\text{Syl}_2(W(\mathcal{L}_3))$ is generated by the element at (4.20), along with permutation of the last two coordinates, so is isomorphic to $\mathcal{C}_2 \times \mathcal{C}_4$. This is extended to $\text{Syl}_2(W(\mathcal{M}_3))$ by including complex conjugation.
Define $\phi_{\mathcal{L}_3} : W(\mathcal{L}_3) \to \text{GL}(E_6)$, $\phi_{\mathcal{M}_3} : W(\mathcal{M}_3) \to \text{GL}(E_6^{+3})$ as the respective integral representations; here the symmetric p-ranks of the full automorphism group $\text{Aut}(E_6)$ will not be covered, as that was calculated in [30].

Lemma 4.3.13. *The following set Δ 2-generates $\Lambda_{real}(\mathcal{L}_3)$,*

$$\begin{aligned}\Delta = \{&(1,\omega,1),(-\omega,-1,-\omega),(-1,-1,-\omega),\\ &(1,\omega^2,1),(\omega^2,\omega^2,1),(-1,-1,-\omega^2)\}.\end{aligned} \tag{4.21}$$

Proof. From the definition of $\mathcal{L}_3$, all $x \in \Lambda_{\text{real}}(\mathcal{L}_3) \subset (\mathbb{Z}[\omega])^3$. Set e_i as the standard basis vectors of $\mathbb{Z}^3$, and a_i, $1 \leq i \leq 6$ as the respective elements of Δ at (4.21). There exists the following relations

$$\begin{aligned} 3e_1 &= a_2 - a_3 + a_4 - a_5, & 3\omega e_1 &= -2a_2 + 2a_3 + a_4 - a_5,\\ 3e_2 &= a_1 - 2a_2 - a_4 + 2a_5 - 2a_6, & 3\omega e_2 &= a_1 + a_2 - a_4 - a_5 + a_6,\\ 3e_3 &= 2a_1 - 2a_2 + a_3 + 2a_5 - a_6, & 3\omega e_3 &= -a_1 + a_2 - 2a_3 - a_5 + 2a_6. \end{aligned}$$

Therefore Δ is a generating set for $(3\mathbb{Z}[\omega])^3$, and for any $l \in \Lambda_{\text{real}}(\mathcal{L}_3)$, $3l$ must be an integer linear combination of elements of Δ, so Δ 2-generates $\Lambda_{\text{real}}(\mathcal{L}_3)$, and therefore also $\Lambda_{\text{real}}(\mathcal{M}_3)$. □

Lemma 4.3.14. *Let $\mathcal{H} = \mathrm{Syl}_2(W(\mathcal{L}_3))$. Then $x \in \Lambda_{real}(\mathcal{L}_3)$ falls into one of three types under the action of $\mathcal{H}$, where $\alpha_i \in \mathbb{Z}[\omega]$,*

1. *$x = (0, \alpha_1, -\alpha_1)$ of orbit size 2,*
2. *$x = (\alpha_1, \alpha_2, \alpha_2)$ of orbit size 4,*
3. *all other cases, orbit size 8.*

Proof. $\mathcal{H}$ is generated by the elements A and B,

$$A := \frac{1}{\theta}\begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}, \qquad B := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}. \tag{4.22}$$

As $A^2 = -B$, one can express the elements of $\mathcal{H}$ as

$$\mathcal{H} = \{\mathrm{Id}_3, A, A^2, A^3, -\mathrm{Id}_3, -A, -A^2, -A^3\}. \tag{4.23}$$

$\mathcal{H}$ is isomorphic to $\mathcal{C}_4 \times \mathcal{C}_2$, so has 8 subgroups. Simply checking the spaces fixed by each of these subgroups and applying the orbit-stabilizer theorem yields the result. Here, $\alpha_i \in \mathbb{Z}[\omega]$.

Generators	Group	Fixed points
Id_3	$\{1\}$	$(\alpha_1, \alpha_2, \alpha_3)$
$-\mathrm{Id}_3$	$\mathcal{C}_2$	$(0, 0, 0)$
$-A^2$	$\mathcal{C}_2$	$(\alpha_1, \alpha_2, \alpha_2)$
A^2	$\mathcal{C}_2$	$(0, \alpha_1, -\alpha_1)$

Generators	Group	Fixed points
$-\mathrm{Id}_3,\ A^2$	$\mathcal{C}_2 \times \mathcal{C}_2$	$(0, 0, 0)$
A	$\mathcal{C}_4$	$(0, \alpha_1, -\alpha_1)$
$-A$	$\mathcal{C}_4$	$(0, 0, 0)$
$A, -\mathrm{Id}_3$	$\mathcal{C}_2 \times \mathcal{C}_4$	$(0, 0, 0)$

The only non-trivial calculation is the fixed points of A; though as A^2 fixes only the points $(0, \alpha_1, -\alpha_1)$, it suffices to check if A fixes those points, which indeed it does. □

Proposition 4.3.15. $\mathrm{SymRank}(\phi_{\mathcal{L}_3}; 2) = \mathrm{SymRank}(\phi_{\mathcal{M}_3}; 2) = 16$.

Proof. Set $L = \Lambda_{\mathrm{real}}(\mathcal{L}_3)$. Suppose X is a 2-generating subset of L such that $|X| < 16$. A consequence of Lemma 4.3.14 is that any $x = (\alpha_1, \alpha_2, \alpha_3) \in L$ with orbit size less than 8 has $\alpha_2 \equiv \alpha_3 \bmod 2\mathbb{Z}[\omega]$. As there exists elements in L with $\alpha_2 \not\equiv \alpha_3$, and as X is 2-generating, it must therefore contain at least one element with $\alpha_2 \not\equiv \alpha_3$, and thus an orbit of size 8. As $|X| < 16$, the remaining elements of X must lie in orbits of size less than 8. Denote by X' this set of remaining elements of X with orbit sizes less than 8.

Let A, B be the generators of the Sylow 2-subgroup $\mathcal{H}$ as in Lemma 4.3.14. Observe the following relations on A and B,

$$\mathrm{Id}_3 - A + A^2 - A^3 = 0,$$
$$A^2 + B = 0.$$

Therefore, each element in $\mathcal{H}$ can be written as a linear combination of Id_3, A and A^2; so an orbit of size 3 can have rank at most 3 (over $\mathbb{Z}$). L has rank 6, so the elements of X' must form a sublattice of rank 3 or greater, and as $-\mathrm{Id}_3 \in \mathcal{H}$, this means $|X'| \geq 2 \cdot \mathrm{rank}(X')$ so $|X'| \geq 6$. There are no orbits of size 1, (for instance, $-\mathrm{Id}_3$ fixes nothing) which means $|X'| = 6$, to ensure $|X| < 16$. The only orbits of size 2 are of the form $(0, \alpha_1, -\alpha_1)$, which form a sublattice of rank 2, $\mathbb{Z}$-spanned by

$(0,1,1)$ and $(0,\omega,\omega)$. If X' was solely comprised of elements of orbit size 2, it would have rank 2, which is impossible, so X' must be the union of an orbit of size 4 and an orbit of size 2.

Finally, we show that $\text{rank}(\overline{X}) < 6$, where $\overline{X}$ is the image of X modulo $2\mathbb{Z}[\omega]$. Suppose for a contradiction that $\text{rank}(\overline{X}) = 6$, and set $x = (\alpha_1, \alpha_2, \alpha_3) \in X$ as the element of orbit size 8, where $\alpha_2 \not\equiv \alpha_3$, $y = (\alpha_4, \alpha_5, \alpha_5) \in X$ as the element of orbit size 4 and $z = (0, \alpha_6, -\alpha_6) \in X$ of orbit size 2.

From the above arguments, for X to have rank 6, the set $\{x, A \cdot x, A^2 \cdot x, y, A \cdot y, z\}$ must be linearly independent, likewise their images modulo $2\mathbb{Z}[\omega]$ must be linearly independent for $\overline{X}$ to have rank 6. We have $x + A^2 \cdot x = (0, \alpha_2 - \alpha_3, -(\alpha_2 - \alpha_3)) \equiv (0, \overline{a}, \overline{a}) \bmod 2\mathbb{Z}[\omega]$ for some $\overline{a} \in \mathbb{Z}[\omega]/2\mathbb{Z}[\omega]$. As $\theta \equiv 1 \bmod 2\mathbb{Z}[\omega]$, $A \cdot y \equiv \theta A \cdot y = (\alpha_4 + 2\alpha_5, \alpha_4 - \alpha_5, \alpha_4 - \alpha_5)$. Therefore $y - A \cdot y \equiv y - \theta A \cdot y = (2\alpha_5, \alpha_4 - \alpha_5, \alpha_4 - \alpha_5) \equiv (0, \overline{b}, \overline{b}) \bmod 2\mathbb{Z}[\omega]$ for some $\overline{b} \in \mathbb{Z}[\omega]/2\mathbb{Z}[\omega]$.

As $\overline{X}$ has rank 6, we must assume that firstly $\alpha_4 \not\equiv \alpha_5 \bmod 2\mathbb{Z}[\omega]$, otherwise $y - A \cdot y \equiv (0,0,0)$. This also requires that $\overline{a} \not\equiv \overline{b}$, and both are not $\equiv 0$. This implies $\overline{x}$ and $\overline{y}$ must generate the space $\langle (0, \overline{1}, \overline{1}), (0, \overline{\omega}, \overline{\omega}) \rangle$. However, $\overline{z}$ must lie in this subspace, so $\overline{X}$ must have rank less than 6. If $\text{rank}(\overline{X}) < 6$, then X fails to 2-generate the lattice, and a 2-generating invariant set must have size at least 16. The orbits of the points in Lemma 4.21 give the size 16 set $\mathcal{H} \cdot \Delta = \Delta' \cup -\Delta'$, where

$$\Delta' = \{(1,\omega,1), (1,1,\omega), (\omega,1,\omega), (\omega,\omega,1), (1,\omega^2,1), (1,1,\omega^2), (\omega^2,\omega^2,1), (\omega^2,1,\omega^2)\}.$$

Therefore $\text{SymRank}(\Lambda_{\text{real}}(\mathcal{L}_3)) = 16$. As this subset is also invariant under conjugation, it is invariant under $\text{Syl}_2(W(\mathcal{M}_3)$ and as $\Lambda_{\text{real}}(\mathcal{L}_3)$ has index prime to 2 in

$\Lambda_{\text{real}}(\mathcal{M}_3)$, it must 2-generate that lattice too, so $\text{SymRank}(\Lambda_{\text{real}}(\mathcal{M}_3)) = 16$. □

Proposition 4.3.16. $\text{SymRank}(\phi_{\mathcal{L}_3}; 3) = \text{SymRank}(\phi_{\mathcal{M}_3}; 3) = 27$.

Proof. The Sylow 3-subgroups of $W(\mathcal{L}_3)$, $W(\mathcal{M}_3)$ and $W(E_6)$ are all isomorphic and are acting on the same lattice, so the symmetric 3-ranks are equal to those of E_6 and E_6^{+3} respectively, which are both 27 (given in [30]). □

4.3.4 $\mathcal{J}_3^{(5)}$

The root system $\mathcal{J}_3^{(5)}$ is defined over the ring $\mathbb{Z}[\sigma, \omega]$, and is given by the union of $\mathcal{H}_3$ (see section 4.3.1) and the $W(\mathcal{H}_3)$-orbit of the following point in $\mathbb{R}^3$

$$(\sigma + 1 + \omega, \sigma\omega - 1, 0),$$

which has size 60, for a combined total of 90 vectors in $\Lambda(\mathcal{J}_3^{(5)})$. The group $W(\mathcal{J}_3^{(5)})$

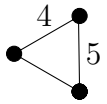


Figure 4.6: Coxeter diagram of $W(\mathcal{J}_3^{(5)})$.

is the *Valentiner* group, which is an extension of A_6 by $\mathcal{C}_3$. As it is a rank 3 root system in $\mathbb{Z}[\omega, \sigma] = \{a_1 + a_2\omega + a_3\sigma + a_4\omega\sigma \mid a_i \in \mathbb{Z}\}$ it must be embedded in $\mathbb{Z}^n$ with n at least $3 \cdot 4 = 12$.

$\Lambda(\mathcal{J}_3^{(5)})_{\text{real}}$, contains 2 extra automorphisms; given by $x \mapsto x'$ and $x \mapsto \overline{x}$ so the index of $W(\mathcal{J}_3^{(5)})$ in $\text{Aut}(\Lambda(\mathcal{J}_3^{(5)})_{\text{real}})$ is at least 4.

The GAP library does indeed contain a rank 12 lattice with $270 = 90 \cdot 3$ minimal vectors (corresponding to the ω-multiples of the points in $\mathcal{J}_3^{(5)}$) and $W(\mathcal{J}_3^{(5)})$ appears as an index 4 subgroup inside the full automorphism group. As a subgroup of $\mathrm{GL}_{12}(\mathbb{Z})$, it is studied in [39], though no description of the lattice structure has been found in the literature. This lattice will be denoted by Q_{12}, and the symmetric p-ranks have been found using the algorithm in 4.0.1, and the code, along with the description of Q_{12} in GAP can be found in Appendix C.2.2. The symmetric p ranks for $\mathcal{W}(\mathcal{J}_3^{(5)})$ and the full automorphism group of Q_{12} are identical, and are 64, 54, and 12 for $p = 2$, 3, 5 respectively.

4.3.5 $\mathcal{H}_4$

The roots of $\mathcal{H}_4$ are given by the even permutations of $(\pm 2, 0, 0, 0)$, $(\pm 1, \pm 1, \pm 1, \pm 1)$ and $(0, \pm 1, \pm\sigma \pm \tau)$. These are the 120 vertices of the 600-cell, a 4 dimensional regular polytope. The roots of $\mathcal{H}_4$ also can be described as quaternions known as the unit *icosians* via $(w, x, y, z) \mapsto \frac{1}{2}(w + xi + yj + zk)$. The group of unit quaternions SU_2 is a double cover of SO_3, and under this mapping the unit icosians form a double cover of A_5, called the binary icosahedral group. The lattice $\Lambda(\mathcal{H}_4)_{\mathrm{real}}$ is the rank 8 lattice

Figure 4.7: Coxeter diagram of $W(\mathcal{H}_4)$.

$Q_8(1)$ ([11, pp. 49]), which has 120 minimal vectors of norm 4, given by the roots of $\mathcal{H}_4$. This lattice is closely related to the E_8 lattice, in fact embedding $\mathcal{H}_4$ as a real lattice but changing the inner product to the standard inner product in $\mathbb{Z}^8$ gives the

E_8 lattice, and $Q_8(1)$ is an index 2 sublattice inside E_8.

For l, r unit quaternions, the map $[l, r] : p \mapsto lp\hat{r}$ (where $\hat{r}$ is quaternionic conjugation) then the point in $\mathbb{R}^4$ defined by the coefficients of $lp\hat{r}$ is the image of $(a, b, c, d) \in \mathbb{R}^4$ (where $p = a + bi + cj + dk$) under some 4 dimensional isometry. The rotations of the 600-cell can be expressed as all maps of the form $[l, r]$, where l, r are in the binary icosahedral group. As $[-l, -r] = [l, r]$, the group of rotations is the central product $L \times R/\{\pm 1\}$ ($L \simeq R \simeq 2.A_5$) of size $\frac{1}{2}(120.120) = 7,200$. This is extended to $W(\mathcal{H}_4)$ by including the *wreathing involution*, $t : q \mapsto \hat{q}$, which is the full symmetry group of the 600-cell, denoted $\{3, 3, 5\}$ of size 14,400. As usual, $W(\mathcal{H}_4)$ has index 2 inside $\mathrm{Aut}(Q_8(1))$, which is achieved by including the conjugation map $(w, x, y, z) \mapsto (w', x', z', y)$, (where $(a + b\sqrt{5})' = a - b\sqrt{5}$).

The Sylow 2-subgroup of $\mathrm{Aut}(Q_8(1))$ has size 2^7, and is generated by ± 1 multiplication on each coordinate, complex conjugation conjugation, and the Sylow 2-subgroup of the alternating group A_4, which can be taken as the group $\langle (12)(34), (13)(24) \rangle = \mathcal{C}_2 \times \mathcal{C}_2$.

Lemma 4.3.17. *For $(\alpha_1, \ldots, \alpha_4) \in \Lambda(\mathcal{H}_4)_{real}$, $\sum_i \alpha_i \equiv 0 \bmod 2$.*

Proof. All the minimal vectors satisfy this condition, and as it is preserved under addition and multiplication by σ, it holds for $\Lambda(\mathcal{H}_4)$. □

Lemma 4.3.18. *If $x = (\alpha_1, \ldots, \alpha_4) \in \Lambda(\mathcal{H}_4)_{real}$, $\alpha_i \in \mathbb{Z}[\sigma]$ with two entries zero, then $\alpha_i \in 2\mathbb{Z}[\sigma]$.*

Proof. Similarly to previous arguments, suppose x has two zero entries, and one or two entries odd. As the cyclic permutations of $(2, 0, 0, 0)$ and $(2\sigma, 0, 0, 0) \in L$, this

would imply either $(\alpha_i, \alpha_j, 0, 0)$ or $(\alpha_i, 0, 0, 0) \in \Lambda(\mathcal{H}_4)$ for α_i, $\alpha_j \in \{1, \sigma, 1+\sigma\}$, all of which have norm less than 4, so can't exist in L. Take for instance the norm of $(1+\sigma, 1+\sigma, 0, 0)$. Recall the norm at (4.10), and that $\tau = 1+\sigma$, so $|(1+\sigma, 1+\sigma, 0, 0)| = \frac{1}{2}((\tau)^2 + (\tau)^2 + \sigma^2 + \sigma^2) = \tau^2 + \sigma^2 = 3$. □

Denote by ϕ_L^1, ϕ_L^2 the integral representations of $W(\mathcal{H}_4)$ and $\mathrm{Aut}(Q_8(1))$ (which is $W(\mathcal{H}_4)$ along with the conjugating map).

Proposition 4.3.19. $\mathrm{SymRank}(\phi_L^i; 2) = 64$.

Consider the map $f : L \to \mathbb{F}_2^8$ which takes an element $(\alpha_1, \ldots, \alpha_4) \in L$ to its equivalence class modulo $2\mathbb{Z}[\sigma]$. The image of L has rank 6, with the images of

$$\{(0,1,\sigma,\tau), (1,0,\tau,\sigma), (\sigma,\tau,0,1), (\sigma,0,1,\tau), (1,\sigma,0,\tau), (1,1,1,1)\}$$

forming a linearly independent set. Let $\mathcal{C}_2^4$ be the group acting by ± 1 on each entry, which leaves $f(L)$ invariant, and if a set X 2-generates L, $f(X)$ must have rank at least 6.

Consider the orbit of $x = (\alpha_1, \ldots, \alpha_4) \in L$ under $\mathcal{H} := \langle (12)(34), (13)(24) \rangle$, the Sylow 2-subgroup of the alternating group A_4. The action of this group on x gives

$$\sum_{x \in \mathcal{H} \cdot x} x = \sum_{1}^{4} \alpha_i (1,1,1,1).$$

However Lemma 4.3.17 implies $\sum_i \alpha_i \equiv 0 \bmod 2$ so $f(\sum_{x \in \mathcal{H} \cdot x} x) = 0$. As $|\mathcal{H} \cdot x| = 4$, then $\mathrm{rank}(\mathcal{H} \cdot x) \leq 3$.

Any $x \in L$ with $f(x) \neq 0$ must have at most one zero entry by Lemma 4.3.18 so has

orbit size at least 8 under $\mathcal{C}_2^4$. Under the action of $\mathcal{H}$ and $\mathcal{C}_2^4$, such x fall into three categories:

1. Not fixed by any non-identity element of $\mathcal{H}$; these have orbit size at least $2^3 \cdot 2^2 = 32$ (under firstly $\mathcal{C}_2^4$ and then $\mathcal{H}$).

2. Fixed by a single non-trivial element of $\mathcal{H}$, so have no zero entries. These have orbit size orbit size $2^4 \cdot 2 = 32$.

3. Fixed by every element of $\mathcal{H}$. These also have no zero entries, so have orbit size $2^4 = 16$ (from the action of $\mathcal{C}_2^4$).

Suppose for a contradiction that $|X| < 64$. If X didn't contain an element of type (1), then there can be at most one orbit of an element of type (2) (of size 32) together with elements that are fixed by $\mathcal{H}$. Therefore the whole set would be fixed by some non-trivial element of $\mathcal{H}$ (and so any linear combination of the set would be fixed by some non-trivial element of $\mathcal{H}$) so wouldn't 2-generate L. Thus an orbit of the first type must exist in X, together with an orbit of an element fixed by $\mathcal{H}$. However from the previous discussion, the image of X under f in this case would have rank $3 + 1 = 4 < 6$ so its image can't generate $f(L)$ and 2-generate L. Therefore, such an X can't exist, so $\text{SymRank}(\phi^1; 2) \geq 64$.

A generating set of size 64 can be chosen, the orbit of $(\sigma, 0, 1, \tau)$ and its image under the conjugating map, $(\tau, 0, \sigma, 1)$. GAP verifies this generates the lattice in Appendix C.2.2. Therefore $\text{SymRank}(\phi_L^i; 2) = 64$.

Lemma 4.3.20. *The root system $\mathcal{H}_4$ contains the subsystem $A_2 \times A_2$.*

Proof. The sets

$$\{(1,1,1,1),(-1,-1,-1,1),(0,0,0,-2)\},$$
$$\{(-\tau,1,\sigma,0),(\sigma,-\tau,1,0),(1,\sigma,-\tau,0)\}$$

are mutually orthogonal and each set sums to 0. □

In particular, the Sylow 3-subgroup of $A_2 \times A_2$ is $\mathcal{C}_3 \times \mathcal{C}_3$, so can be identified as $\mathrm{Syl}_3(W(\mathcal{H}_4))$. The matrices for each generator can be identified as

$$A := \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad B := \frac{1}{2}\begin{pmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ 1 & 1 & 1 & -1 \end{pmatrix}. \tag{4.24}$$

This means that the orbit of any $x \in Q_8(1)$ under $\mathcal{C}_3 \times \mathcal{C}_3$ has rank at most 4.

Proposition 4.3.21. $\mathrm{SymRank}(Q_8(1);3) = 18$.

Proof. If $x \in A_2$, and fixed by the action of $\mathcal{C}_3$, then $x = 0$. Therefore, if $x \in A_2 \times A_2$, with orbit size less than 9, it is 0 on one of the A_2 components.
A 3-generating set in $Q_8(1)$ needs two elements in different copies of $A_2 \times A_2$, otherwise they would sit inside a rank 4 sublattice. As the action of $\mathcal{C}_3 \times \mathcal{C}_3$ leaves these $A_2 \times A_2$ invariant, and from the previous discussion, for these to 3-generate, they need to each have orbit size 9, therefore a 3-generating set needs size at least 18. There does exist an orbit size 18 that generates $Q_8(1)$, verified in Appendix C.2.2. □

Proposition 4.3.22. $\mathrm{SymRank}(Q_8(1); 5) = 25$.

Proof. $Q_8(1)$ is an index 2 sublattice of E_8, and as $|\mathrm{Syl}_5(W(E_8))| = |\mathrm{Syl}_5(W(\mathcal{H}_4))| = 25$, the groups must be the same. Using Lemma 4.0.8, $\mathrm{SymRank}(\phi_L; 5) = \mathrm{SymRank}(\phi_{E_8}; 5) = 25$. □

4.3.6 $\mathcal{N}_4$ & $\mathcal{O}_4$

The root systems $\mathcal{N}_4$ and $\mathcal{O}_4$ are defined over the ring of Gaussian integers $\mathbb{Z}[i]$. $\mathcal{N}_4$ is the $4^2 \cdot \binom{4}{2} = 96$ points given by the permutations $(2i^{a_1}, 2i^{a_2}, 0, 0)$ for $0 \leq a_i \leq 3$, along with the $4^3 = 64$ points $(1+i)(i^{a_1}, i^{a_2}, i^{a_3}, i^{a_4})$, $0 \leq k \leq 3$, $\sum a_i \equiv 0 \bmod 4$.
This is a subsystem of $\mathcal{O}_4$, which is given by the previous points, along with the 16 points given by the permutations of $(i^k(2+2i), 0, 0, 0)$, $0 \leq k \leq 3$, and the extra 64 points $(1+i)(i^{a_1}, i^{a_2}, i^{a_3}, i^{a_4})$, given by relaxing the condition on the a_i to $\sum a_i \equiv 0 \bmod 2$.
The lattice $\Lambda(\mathcal{O}_4)_{\mathrm{real}}$ is the E_8 root lattice ([25, pp. 110]), and as $\mathcal{N}_4$ is a subsystem of $\mathcal{O}_4$, it will be also embedded in E_8.
The group $W(\mathcal{N}_4)$ is given by multiplication by i on an even number of entries, permutation of the coordinates, and an action of $\mathcal{C}_5$, due to the embedding of A_4 in the root system, so has size $4^3 \cdot 4! \cdot 5 = 2^9 \cdot 3 \cdot 5 = 7680$. This is extended to $W(\mathcal{O}_4)$ by two extra elements; multiplication by $\mathrm{diag}\{(i^{k_1}, i^{k_2}, i^{k_3}, i^{k_4})\}$ where $\sum_i k_i \equiv 0 \bmod 2$, which gives an extra order 2 automorphism (for instance, the group element $g = \mathrm{diag}\{(-1, 1, 1, 1)\} \in W(\mathcal{O}_4)$, but $g \notin W(\mathcal{N}_4)$), and an extra automorphism of order 3 given by the subsystem D_4 that embeds in $\mathcal{O}_4$, so $W(\mathcal{O}_4) = 2 \cdot 3 \cdot |W(\mathcal{N}_4)| = 46080$.

Figure 4.8: Coxeter diagrams of $W(\mathcal{N}_4)$ and $W(\mathcal{O}_4)$.

Lemma 4.3.23. *The entries of* $(\alpha_1, \dots \alpha_4) \in \Lambda(\Sigma)_{real}$ *for* $\Sigma = \mathcal{N}_4$, $\mathcal{O}_4$ *are equal modulo* $2\mathbb{Z}[i]$.

Proof. This is true for the points of both root systems and is preserved under addition, and multiplication by i. □

Proposition 4.3.24. $\mathrm{SymRank}(\phi_{\mathcal{N}_4}; 2) = 64$, $\mathrm{SymRank}(\phi_{\mathcal{O}_4}; 2) = 128$.

Proof. If X is a 2-generating set, then it must contain a vector with at least one odd entry, and by Lemma 4.3.23, all the entries are odd. For $W(\mathcal{N}_4)$, the orbit under the Sylow 2-subgroup of this vector has size at least 4^3, coming from the action of i^k on each entry. The $\mathrm{Syl}_2(W(\mathcal{N}_4))$-orbit of $(i+1)(1,1,1,1)$ has size 4^3 and generates $\Lambda_{\mathrm{real}}(\mathcal{N}_4)$; the relations $(2,2,0,0) = (1+i)(1,1,1,1)+(1+i)(-i,-i,-1,-1)$, $(2,2i,0,0) = 1+i(1,1,1,1)+(1+i)(-i,i,1,1)$ and their permutations show every vector in $\mathcal{N}_4$ can be written as an integer linear combination of this set. As the Sylow 2-subgroup is generated by the multiplication by i on three coordinates and the Sylow 2-subgroup of S_4 acting on the coordinates, this set is clearly invariant.
Similarly, the orbit of such a point under the Sylow 2-subgroup of $W(\mathcal{O}_4)$ has size $2 \cdot 4^3 = 128$, due to the order 2 automorphism (which again fixes only vectors with at least one zero entry). As this is the symmetric 2-rank of the $W(E_8)$ action on the E_8 root lattice, that must be an upper bound, so the result follows. □

The Sylow 3-subgroup of $W(\mathcal{N}_4)$ is just given by the order 3 permutation (1 2 3).

Proposition 4.3.25. $\mathrm{SymRank}(\phi_{\mathcal{N}_4}; 3) = 8$.

Proof. The set $4e_j$ and $4ie_j$ (where e_j are the standard basis vectors) clearly generate $(4\mathbb{Z}[i])^4$, and as all vectors $\alpha \in \Lambda_{\mathrm{real}}(\mathcal{N}_4)$ have coefficients in $\mathbb{Z}[i]$, 4α is contained in the $\mathbb{Z}$-span of $4e_j$ and $4ie_j$. These vectors also lie in $\Lambda_{\mathrm{real}}(\mathcal{N}_4)$, for instance

$$(4,0,0,0) = (2,2,0,0) + (2,0,2,0) - (0,2,2,0). \tag{4.25}$$

The rest can be obtained by taking suitable permutations and multiplying by i. Therefore, $4e_j$ and $4ie_j$ generate a sublattice of $\Lambda_{\mathrm{real}}(\mathcal{N}_4)$ of index dividing 4. The set $4e_j$ and $4ie_j$ is also invariant under the Sylow 3-subgroup and has size 8, so is a 3-generating size 8 set. □

The Sylow 3-subgroup of $W(\mathcal{N}_4)$ is inherited by virtue of a copy of D_4 living inside the root system.

Lemma 4.3.26. *There is an embedding of root systems $D_4 \subset \mathcal{O}_4$.*

Proof. As mentioned in Example 4.0.1, the D_4 root system consists (when multiplied each point by 2) of the 8 permutations $\pm(2,0,0,0)$ and the 16 points $(\pm 1, \pm 1, \pm 1, \pm 1)$. Multiplying by $(1+i)$ clearly embeds these 24 points in $\mathcal{O}_4$. □

From this description, $iD_4 := \{ix \mid x \in D_4\}$ is another copy of D_4, disjoint from the original.

Proposition 4.3.27. $\mathrm{SymRank}(\phi_{\mathcal{O}_4}; 3) = 18$.

Proof. As $D_4 \subset \mathcal{O}_4$, and the orders of the Sylow 3-subgroups of $W(D_4)$ and $W(\mathcal{O}_4)$ are equal (of order 9), then they are equal. Any 3-generating invariant set must have one element in the span of the copy of $D_4 \subset Q_8(1)$, and one in the copy iD_4, otherwise the $\mathbb{Z}$-span of the set would be rank at most 4. As this group leaves the D_4 system invariant, and the symmetric 3-rank of the automorphism group of the D_4 root lattice is 9, then the symmetric 3-rank must be at least $2 \cdot 9 = 18$. Finally, a similar argument to Proposition 4.3.25 shows that $D_4 \cup iD_4$ generates an index 4 lattice; $(2+i,0,0,0) + (2-i,0,0,0) = (4,0,0,0)$, and so on. Therefore $\text{SymRank}(\phi_{\mathcal{O}_4}; 3) = 18$. □

$\mathcal{N}_4$ (and by extension $\mathcal{O}_4$) contains A_4 as a subsystem ([25, pp. 109]); given by the following points and their -1 multiples:

$$\begin{gathered}(2,2i,0,0), \quad (2,0,2i,0), \quad (2,0,0,2i), \quad (0,2,-2,0),\\ (0,2,0,-2), \quad (0,0,2,-2), \quad (1+i)(1,1,1,1),\\ (1+i)(1,-1,-i,-i), (1+i)(1,-i,-1,-i), \quad (1+i)(1,-i,-i,-1).\end{gathered} \tag{4.26}$$

Embedding this system as disjoint copies A_4 and iA_4, as before, gives the symmetric 5-ranks.

Proposition 4.3.28. $\text{SymRank}(\phi_{\mathcal{N}_4}; 5) = \text{SymRank}(\phi_{\mathcal{O}_4}; 5) = 10$.

Proof. The system A_4 is a subsystem of $\mathcal{N}_4 \subset \mathcal{O}_4$, and as the Sylow 5-subgroups of $W(\mathcal{N}_4)$, $W(\mathcal{O}_4)$ and $W(A_4)$ are all isomorphic to $\mathcal{C}_5$.

Therefore, any orbit of a non-fixed point in $\Lambda(\mathcal{O}_4)_{\text{real}}$ under the orbit of the Sylow 5-subgroup has rank 4. Thus two orbits are needed, and $\text{SymRank}(\phi_{\mathcal{N}_4}; 5) =$

$\mathrm{SymRank}(\phi_{\mathcal{O}_4}; 5) \geq 10$. To show this upper bound is an equality, it is shown by GAP that the every group isomorphic to $\mathcal{C}_5$ in $W(E_8)$ has symmetric 5-rank ≤ 10, by finding 5-generating invariant sets, which can be found in Appendix C.2.2. $\square$

4.3.7 $\mathcal{L}_4$

In Section 4.3.3, the root system $\mathcal{L}_3$ is the set of the cyclic permutations and $\mathrm{diag}\{(\omega^{i_1}, \omega^{i_2}, \omega^{i_3})\}$ multiples of $(\theta, 0, 0)$ and $(1, 1, 1)$. Embed $\mathcal{L}_3$ inside $\mathbb{C}^4$ as the first three entries, then the root system $\mathcal{L}_4$ is given by the union of $\mathcal{L}_3$, and the $W(\mathcal{L}_3)$ orbit (acting on the first three coordinates) of $(0, 1, -1, -1)$ and $(0, 0, 0, \theta)$.
These form 120 roots, and along with their -1 multiples are the minimal vectors of $\Lambda(\mathcal{L}_4)_{\mathrm{real}}$, which is the description of the E_8 root lattice as a rank 4 $\mathbb{Z}[\omega]$-lattice.
$W(\mathcal{L}_4)$ has order $2^7 \cdot 3^5 \cdot 5$; the Sylow 2-group is given by multiplication by ± 1 on each coordinate, together with the Sylow 2-subgroup of the symmetric group S_4 acting on the coordinates. Similarly, the Sylow 3-subgroup acts by a multiplication of ω on each entry and by an order 3 permutation on the coordinates. The Sylow 5-subgroup acts by virtue of $A_4 \subset \mathcal{L}_4$.

Set ϕ_L as the integral representation of $W(\mathcal{L}_4)$ inside $\Lambda(\mathcal{L}_4)_{\mathrm{real}} \simeq E_8$.

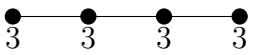


Figure 4.9: Coxeter diagram of $W(\mathcal{L}_4)$.

Proposition 4.3.29. $\mathrm{SymRank}(\phi_L; 2) = 16$.

Proof. Note that $\mathcal{L}_3 \subset \mathcal{L}_4$, $\mathrm{SymRank}(\phi_L; 2) \geq 16$. To achieve this lower bound, take the set $\pm\theta e_i$, $\pm\omega\theta e_i$ for $1 \leq i \leq 4$. This is invariant under the Sylow 2-subgroup of

$W(\mathcal{L}_4)$, and is 3 generating; indeed as $-\theta - 2\omega\theta = 3$, these vectors generate a lattice of index 3. □

The Sylow 3-subgroup is generated by multiplying each entry by ω, along with the Sylow 3-subgroup of the symmetric group S_4, which can be taken as a permutation of the first 3 coordinates. This has size 3^5, and comparing orders, $\mathrm{Syl}_3(W(E_8)) = \mathrm{Syl}_3(W(\mathcal{L}_4))$.

Proposition 4.3.30. $\mathrm{SymRank}(\phi_L; 3) = 81$.

Proof. As the Sylow 3-subgroups are the same, and $\Lambda(\mathcal{L}_4) = E_8$, so their symmetric 3-ranks are the same. □

4.3.8 $\mathcal{K}_5$ & $\mathcal{K}_6$.

As before, define $\omega := e^{\frac{2\pi i}{3}}$, and $\theta = \omega - \omega^2 = \sqrt{-3}$. The root system $\mathcal{K}_6$ is defined as the permutations of following points in $(\mathbb{Z}[\omega])^6$

$$\pm(\omega^i\theta, -\omega^j\theta, 0, \ldots, 0), \qquad \pm(\omega^{a_1}, \ldots, \omega^{a_6}), \tag{4.27}$$

where all powers are in $\{0, 1, 2\}$ and $\sum a_i \equiv 0 \bmod 3$. This contains $2 \cdot 3^2 \cdot \binom{6}{2} + 2 \cdot 3^5 = 756$ points. The system $\mathcal{K}_5$ is defined as all points in $\mathcal{K}_6$ orthogonal (under the Hermitian form) to $(1, 1, 1, 1, 1, 1)$. $\mathcal{K}_5$ thus consists of the permutations of

$$\pm\omega^i(\theta, -\theta, 0, 0, 0, 0) \qquad \pm (1, \omega, \omega^2, 1, \omega, \omega^2). \tag{4.28}$$

Therefore $\mathcal{K}_5$ consists of $2 \cdot 3 \cdot \binom{6}{2} + 2 \cdot \binom{6}{2} \cdot \binom{4}{2} = 270$ points.

The group $W(\mathcal{K}_6)$ is Mitchell's group, which has structure $\mathcal{C}_6 \rtimes (\mathrm{PSU}_4(\mathbb{F}_3) \rtimes \mathcal{C}_2)$, and has order $2^9 \cdot 3^7 \cdot 5 \cdot 7 = 39,191,040$, and $W(\mathcal{K}_5) = \mathcal{C}_2 \times \mathrm{PSU}_4(\mathbb{F}_2)$, of order $2^7 \cdot 3^4 \cdot 5 = 51,840$. The lattice $\Lambda(\mathcal{K}_6)_{\mathrm{real}}$ is the *Coxeter-Todd* lattice, K_{12} (see [9]),

Figure 4.10: Coxeter diagrams of $W(\mathcal{K}_6)$ & $W(\mathcal{K}_6)$.

a well-known lattice and the densest packing in 12 dimensions. The group $\mathrm{Aut}(K_{12})$ contains in addition the order 2 automorphism given by complex conjugation, so has order $2^{10} \cdot 3^7 \cdot 5 \cdot 7$.

The lattice $\Lambda(\mathcal{K}_5)_{\mathrm{real}}$ is not so well studied, though adjoining complex conjugation as an automorphism gives a maximal finite subgroup of $\mathrm{GL}_{10}(\mathbb{Z})$ called F_{31} in [44, pp. 344]. It is correspondingly found as the group `ImfMatrixGroup(10,4,1)` in the GAP database, though there is no explicit description as a lattice in its own right in the literature, so in Table 4.2 it is denoted by Q_{10}. For the following, the elements of $\Lambda(\mathcal{K}_5)_{\mathrm{real}}$ will be viewed as their respective elements inside $\Lambda(\mathcal{K}_6)_{\mathrm{real}}$.

The complex lattice $\Lambda(\mathcal{K}_6)$, and its real counterpart were explored in [9], where different descriptions (i.e. different $\mathbb{Z}[\omega]$-bases) are given. These make various subgroups of the automorphism group more apparent, and all yield an equivalent version of $\Lambda(\mathcal{K}_6)$. Firstly, the lattice $\Lambda(\mathcal{K}_6)_{\mathrm{real}}$ was called $\Lambda^{(3)}$ in [9, pp. 424]. Formally,

$$\Lambda^{(3)} := (\alpha_1, \ldots, \alpha_6)\ \alpha_i \in \mathbb{Z}[\omega], \quad \alpha_1 \equiv \ldots \equiv \alpha_6 \bmod \theta. \tag{4.29}$$

As the elements in $\mathcal{K}_5$ are orthogonal to $(1,\ldots,1)$, they additionally satisfy

$$\sum_i \mathrm{Re}(\alpha_i) = 0. \tag{4.30}$$

The Sylow 3-subgroup of $W(\mathcal{K}_6)$ has size 3^7, and is generated by the permutations (1 2 3) and (4 5 6), along with multiplying by $\mathrm{diag}\{(\omega^{a_1},\ldots\omega^{a_6})\}$, such that $\sum a_i = 0$. The Sylow 3-subgroup of $W(\mathcal{K}_5)$ has order 3^5; to identify this however, note that $W(\mathcal{K}_6)$ acts transitively on the minimal vectors of $\Lambda^{(3)}$ ([25, pp. 107]), so for any $x \in \mathcal{K}_6$, the points orthogonal to x make up the points of a copy of $\mathcal{K}_5$. Therefore, if one takes instead of $(1,\ldots,1)$ the point $(1,-1,0,0,0,0)$, a description of a new embedding of $\mathcal{K}_5$ appears,

$$\begin{aligned} \alpha_1 \equiv \ldots \equiv \alpha_6 \bmod \theta, \text{ where} \\ \alpha_1 + \overline{\alpha_1} + \alpha_2 + \overline{\alpha_2} = 0 \\ \Rightarrow \mathrm{Re}(\alpha_1 + \alpha_2) = 0. \end{aligned} \tag{4.31}$$

This is all points in $\mathcal{K}_6$ orthogonal to $(1,-1,0,0,0,0)$. The Sylow 3-subgroup of $W(\mathcal{K}_5)$ has order 3^5 ([25, pp. 166]) and can be identified as acting by ω^i on the last 4 entries of $(\alpha_1,\ldots\alpha_6)$, and the permutation (4 5 6).

As usual, set $\phi^1_{K_n}$, $\phi^2_{K_n}$ as the corresponding integral representations of $W(\mathcal{K}_n)$ and $\mathrm{Aut}(\Lambda(\mathcal{K}_n)_{\mathrm{real}})$.

Recall the isomorphism

$$\mathbb{Z}[\omega]/\theta\mathbb{Z}[\omega] \cong \mathbb{Z}/3\mathbb{Z}. \tag{4.32}$$

If $x \equiv \theta\Lambda$ in the complex lattice Λ, then the corresponding vector, $x_{\mathrm{real}} \in 3\Lambda_{\mathrm{real}}$.

Proposition 4.3.31. $\mathrm{SymRank}(\phi_{K_5}; 3) = 81$, $\mathrm{SymRank}(\phi^i_{K_6}; 3) = 243$.

Proof. A 3-generating subset $X \subset \Lambda(\mathcal{K}_n)_{\mathrm{real}}$ for $n = 5$ or 6, has at least one entry of an element $x \not\equiv 0 \bmod \theta$. By (4.29), all the entries of x are congruent modulo θ, so all are non-zero. For $W(\mathcal{K}_5)$, the action of ω^i on the last 4 entries leaves x with an orbit size at least 81, and similarly for $W(\mathcal{K}_5)$, the action of $\mathrm{diag}\{(\omega^{a_1}, \ldots \omega^{a_6})\}$ gives x orbit size at least $3^5 = 243$. This gives lower bounds for the respective symmetric 3-ranks.
In both these cases, there exists orbits of this size that generate the lattice; checked in GAP, (see Appendix C.2.2). □

For identifying the Sylow 2-subgroup, our attention is turned to the description of $\Lambda(\mathcal{K}_6)$ in a different $\mathbb{Z}[\omega]$-basis, denoted by $\Lambda^{(4)}$ in [9]. This is defined as the sets of 6-tuples of elements of $\mathbb{Z}[\omega]$, $(\alpha_1, \ldots, \alpha_6)$ such that

$$\alpha_1 \equiv \alpha_2 \equiv \ldots \equiv \alpha_6 \equiv m \bmod 2\mathbb{Z}[\omega], \tag{4.33}$$

$$\alpha_1 + \ldots + \alpha_6 \equiv 2\overline{\omega}m \bmod 4\mathbb{Z}[\omega]. \tag{4.34}$$

The minimal vectors in $\Lambda^{(4)}$ are the permutations of

$$\omega^i(2, 2, 0, 0, 0, 0), \qquad \omega^i(\theta, 1, \cdots, 1), \tag{4.35}$$

along with the action of $\mathrm{diag}\{(-1^{a_1}, \ldots -1^{a_6})\}$, where $\sum_i a_i = 0$. One can check the number of minimal vectors is correct; there are $\binom{6}{2} \cdot 4 \cdot 3 = 180$ of the first type, and $2^5 \cdot 6 \cdot 3 = 576$ making a total of 756 minimal vectors. The point $(1 \ldots, 1)$ under this

change of basis becomes $(2,2,0,0,0,0)$ (though as $W(\mathcal{K}_6)$ is transitive on the minimal vectors of $\Lambda(\mathcal{K}_6)_{\text{real}}$ any point will do), so $\mathcal{K}_5$ now describes the points satisfying (4.33) and (4.34), as well as satisfying the condition

$$\begin{aligned} \alpha_1 + \overline{\alpha_1} + \alpha_2 + \overline{\alpha_2} = 0 \\ \Rightarrow \mathrm{Re}(\alpha_1 + \alpha_2) = 0. \end{aligned} \tag{4.36}$$

These are the points $\pm\omega^i(2,-2,0,0,0,0)$, $\pm\omega^i(0,0,2,\pm 2,0,0)$, where the ± 2 can appear in any of the last 4 entries, and $\pm\omega^i(1,-1,\pm\theta,\pm 1,\pm 1,\pm 1)$, where there is an even number of minus signs, and θ can be in any of the last 4 entries. As a sanity check, there are $2\cdot 3 = 6$ vectors of the first type, $\binom{4}{2}\cdot 2^2\cdot 3 = 72$ of the second and $2^4\cdot 4\cdot 3 = 192$ of the third, which gives 270 minimal vectors.

From this description, the Sylow 2-subgroups of $W(\mathcal{K}_n)$ become apparent. Firstly taking $\mathcal{K}_6$, the symmetric group S_6 acts by permuting the entries, and the Sylow 2-subgroup of S_6 is $\mathcal{H} := \mathcal{C}_2 \times D_8$ (for example the group generated by (1 2), (1 3 2 4) and (5 6)). The Sylow 2-subgroup of $W(\mathcal{K}_6)$ is generated by this group, along with an even number of sign changes (an odd number would violate (4.34)). This has index 2 inside the Sylow 2-subgroup of $\mathrm{Aut}(K_{12})$ which also contains complex conjugation and so has order 2^{10}.

The Sylow 2-subgroup of $W(\mathcal{K}_5)$ is the subgroup of $\mathrm{Syl}_2(W(\mathcal{K}_6))$ that leaves $\mathcal{K}_5$ invariant. The element that doesn't satisfy this is (1 3 2 4), (though its square does) and any $\mathrm{diag}\{((-1)^{a_1},(-1)^{a_2},(-1)^{a_3},(-1)^{a_4},(-1)^{a_5},(-1)^{a_6})\}$ with $a_1 \not\equiv a_2$ modulo 2 (and of course $\sum_i a_i = 0$). Taking a quotient by these elements gives the Sylow 2-subgroup of $W(\mathcal{K}_5)$, with size 2^7. Take as the generators (1 2), (1 2)(3 4) and (5 6) (which gives an index 2 subgroup of $\mathcal{H}$) along with the group $\mathcal{C}_2^4$ that acts as

$\mathrm{diag}\{(-1^{a_1}, -1^{a_2}, -1^{a_3}, -1^{a_4}, -1^{a_5}, -1^{a_6})\}$, (with $\sum_i a_i = 0$, and $a_1 \equiv a_2 \bmod 2$). For $X \in \Lambda(\mathcal{K}_6)_{\mathrm{real}}$, define $X_\pm$ as the orbit of X under the action of $\mathrm{diag}\{((-1)^{n_1}, \ldots, (-1)^{n_6})\} \in W(\mathcal{K}_6)$.

Lemma 4.3.32. *Let $\mathcal{H}'$ be the 2-group in $W(\mathcal{K}_5)$ generated by* (1 2), (1 2)(3 4) *and* (5 6). *For $x = (\alpha_1, \ldots, \alpha_6) \in \mathcal{K}_5$, $\alpha_i \not\equiv 0 \bmod 2\mathbb{Z}[\sigma]$, denote by $X_\pm$ the orbit of x under the group generated by* $\mathrm{diag}\{((-1)^{n_1}, \ldots, (-1)^{n_6})\}$. *Then $|\mathcal{H}' \cdot X_\pm| \geq 4 \cdot |X_\pm|$.*

Proof. Suppose for a contradiction that instead $X_\pm$ is invariant under an index 2 subgroup of $\mathcal{H}'$. The size 4 subgroups of $\mathcal{H}'$ are going to comprise two or more of the transpositions (1 2), (3 4), (5 6). It can be assumed therefore that either $\alpha_3 = \pm\alpha_4$ or $\alpha_5 = \pm\alpha_6$ (or both), for α_i entries of x. Recall that $\alpha_i \equiv m \bmod 2\mathbb{Z}[\omega]$, and suppose (without loss of generality), $\alpha_3 = \pm\alpha_4$. From (4.34),

$$\alpha_1 + \alpha_2 + (\alpha_3 \pm \alpha_3) + \alpha_5 + \alpha_6 \equiv 2\overline{\omega} \bmod 4.$$

As $\mathrm{Re}(\alpha_1 + \alpha_2) = 0$, $\alpha_1 + \alpha_2 \equiv \omega \bmod 2\mathbb{Z}[\omega]$, so taking the coordinates modulo $2\mathbb{Z}[\omega]$,

$$\omega + \alpha_5 + \alpha_6 \equiv 0.$$

This contradicts $\alpha_5 \equiv \alpha_6 \bmod 2\mathbb{Z}[\omega]$, so the result follows. □

Proposition 4.3.33. $\mathrm{SymRank}(\phi^i_{\mathcal{K}_n}; 2) = 128$.

Proof. Recall that for $x \in \Lambda(\mathcal{K}_5)_{\mathrm{real}}$, all entries are equal modulo $2\mathbb{Z}[\sigma]$. For a set $X \subset \Lambda(\mathcal{K}_5)$ to be 2-generating, it must contain elements x, y where the x_i, $y_i \not\equiv 0 \bmod 2\mathbb{Z}[\sigma]$, and $x_i \not\equiv y_i \bmod 2\mathbb{Z}[\sigma]$. As the Sylow 2-subgroup of $W(\mathcal{K}_5)$ leaves this

equivalence class invariant, it must contain at least 2 orbits. Also, as all the entries are non-zero, they have orbit size 2^4 under the action of the -1 multiples. Lemma 4.3.32 implies the orbit is extended to size $2^6 = 64$ under the action of the permutations. As there needs to be two distinct orbits of size at least 64, $\mathrm{SymRank}(\phi^i_{\mathcal{K}_5}; 2) \geq 128$. There exists a generating invariant set of size 128 under the full Sylow 2-subgroup of $W(\mathcal{K}_6)$ (see Appendix C.2.2) and as $\mathcal{K}_5 \subset \mathcal{K}_6$, $\mathrm{SymRank}(\phi^i_{\mathcal{K}_n}; 2) = 2^7 = 128$. □

The permutation of order 5 (in either construction seen of Λ) gives a copy of $\mathrm{Syl}_5(\mathrm{Aut}(K_{12}))$.

Proposition 4.3.34. $\mathrm{SymRank}(\phi^i_{\mathcal{K}_5}; 5) = 10$, $\mathrm{SymRank}(\phi^i_{\mathcal{K}_6}; 5) = 12$.

Proof. As these are equal to the respective ranks of $\Lambda(\mathcal{K}_n)_{\mathrm{real}}$, it is sufficient to find p-generating sets of each size, found in GAP (see Appendix C.2.2). □

For $\mathrm{SymRank}(\phi^i_{\mathcal{K}}; 7) = 14$, another construction of Λ is used, $\Lambda^{(7)}$, [9, pp. 426]. Let $\alpha := 2 + 3\omega$, so $\alpha^2 - \alpha + 7 = 0$. Also, $\mathbb{Z}[\omega]/\alpha\mathbb{Z}[\omega] \simeq \mathbb{Z}/7\mathbb{Z}$, so α is a prime in $\mathbb{Z}[\omega]$. The lattice vectors of $\Lambda^{(7)}$ are $\{(x_0, \ldots, x_6) \mid x_i \in \mathbb{Z}[\omega]\}$ such that

$$x_0 \equiv \ldots \equiv x_6 \bmod \alpha, \tag{4.37}$$

$$\sum x_i = 0. \tag{4.38}$$

The group $\mathrm{Syl}_7(\mathrm{Aut}(\Lambda^{(7)}))$ acts by cyclically permuting these 7 entries. It has no fixed points, because if $(\alpha, \ldots, \alpha) \in \Lambda^{(7)}$, (4.38) implies $\alpha = 0$.

Proposition 4.3.35. $\mathrm{SymRank}(K_{12}; 7) = 14$

Proof. As mentioned previously, $\mathrm{Syl}_7(\mathrm{Aut}(\Lambda^{(7)})$ fixes no points, so fixes no points of K_{12}. Therefore the symmetric 7-rank is a multiple of 7, so $\mathrm{SymRank}(\phi^i_{\mathcal{K}}; 7) \geq 14$. Appendix C.2.2 shows a size 14 generating invariant set. □

4.4 The Leech lattice

The final part to this chapter is the calculation of the symmetric p-rank of the automorphism group of the Leech lattice, Λ_{24}. One of the most famous of all lattices, its automorphism group contains many simple sporadic groups, and Λ_{24} has numerous constructions. Some combinatorial results that are needed are proved using GAP, the code for which will appear in the proof. For $p = 2$ and 3, different descriptions of Λ_{24} are used which highlight the Sylow p-subgroups more readily, and these rely on the definition of the *Golay codes*.

4.4.1 The Golay Codes

A *linear code* C is a subspace of $\mathbb{F}_q^n$. The dimension of C is the dimension of the subspace, and the weight of a codeword $c \in C$, denoted $\mathrm{wt}(c)$, is defined as the number of non-zero entries of c. The minimum weight along all non-zero codewords is the *minimal distance* of the code word, and a triple $[n, k, d]$ denotes a code with length n (i.e. the dimension of $\mathbb{F}_q^n$), k the dimension of C, and d the minimal distance of C. For instance, the code $[n, n, 1]$ is simply all length n words $x \ldots x$, $x \in \mathbb{F}_q$.
The complete weight enumerator is a homogeneous polynomial which details the

number of codewords of each composition; for $\{x_i\}_{i\in\{1,\dots,q\}}$, it is the polynomial $\sum_{c\in C} x_1^{n_1(c)}\dots x_q^{n_q(c)}$, where $n_i(c)$ is the number of times the entry i appears in the codeword c.

Many lattices can be constructed from codewords; for instance the Coxeter-Todd lattice can be constructed using the *hexacode*, and the E_8 root lattice can be constructed using the *Hamming code*. A code has a group of automorphisms, and often if a code C is used in constructing a lattice L, then $\mathrm{Aut}(C)$ will appear as a subgroup of $\mathrm{Aut}(L)$. The following descriptions of the Golay codes and their automorphism groups can be found in [8, pp. 85].

The binary Golay code $\mathscr{C}_{23}$ is the $[23, 12, 7]$ code over $\mathbb{F}_2$, and after adding a zero-sum check digit becomes the *extended* binary Golay code, $\mathscr{C}_{24}$ which is the $[24, 12, 8]$ code over $\mathbb{F}_2$. Its complete weight enumerator is

$$x_1^{24} + 759x_1^{16}x_2^8 + 2576x_1^{12}x_2^{12} + 759x_1^8x_2^{16} + x_2^{24}. \tag{4.39}$$

The (extended) ternary Golay code $\mathscr{C}_{12}$, is the $[12, 6, 6]$ codeword over $\mathbb{F}_3$, with complete weight enumerator

$$x_1^{12} + x_2^{12} + x_3^{12} + 22(x_1^6x_2^6 + x_1^6x_3^6 + x_2^6x_3^6) + 220(x_1^6x_2^3x_3^3 + x_1^3x_2^6x_3^3 + x_1^3x_2^3x_3^6). \tag{4.40}$$

The automorphism group of $\mathscr{C}_{24}$ and $\mathscr{C}_{12}$ are the Mathieu groups M_{24}, M_{12} respectively, and define a *$\mathscr{C}$-set* as the set of coordinates where a codeword of $\mathscr{C}_{24}$ has entry 1.

The Leech lattice can now be defined as the following set, given in [8, pp. 133],

together with the standard inner product. The minimal vectors are the following

$$\frac{1}{\sqrt{8}}(\mp 3, \pm 1^{23}) \in \mathbb{R}^{24}, \tag{4.41}$$

where the upper signs form a $\mathscr{C}$-set. Λ_{24} is then the $\mathbb{Z}$-span of these vectors. Here, (a^n, b^m) means a point with n entries equal to a, and m entries equal to b. All lattice vectors have norm $16n$ for $n \in \mathbb{N}$, and there are a total of 196,560 minimal vectors of norm 16.

The automorphism group of Λ_{24} is $\cdot 0 := \mathcal{C}_2 \times Co_1$, where Co_1 is a simple sporadic group of order $2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$. Co_1 was in fact discovered by virtue of being an automorphism group of this structure and contains many other simple sporadic groups. Set $\phi_\Lambda : \mathcal{C}_2 \times Co_1 \to \mathbb{Z}^{24}$ as the integral representation of the automorphism group of Λ_{24}. The following section takes each prime in turn and calculates the symmetric p-rank, using GAP to check various conditions on Λ_{24}.

p	2	3	5	7	11	13	23
SymRank$(\phi_\Lambda; p)$	32768	2187	125	49	24	26	24

Table 4.5: Symmetric p-ranks of the Leech lattice, Λ_{24}.

4.4.2 SymRank($\phi_\Lambda; 2$)

An equivalent definition of Λ_{24} ([8, pp.131]) is by the *even* and *odd* vectors, together with the standard inner product.

$$\frac{1}{\sqrt{8}}(\underline{0} + 2c + 4\underline{x}), \tag{4.42}$$

$$\frac{1}{\sqrt{8}}(\underline{1} + 2c + 4\underline{y}), \tag{4.43}$$

where $\underline{0}$ is the zero vector, $\underline{1} = (1^{24})$, $c \in \mathscr{C}_{24}$ with $1 \in \mathbb{F}_2$ being viewed as $1 \in \mathbb{Z}$, and $\underline{x} = (x_1, \ldots, x_{24})$, $\underline{y} = (y_1, \ldots, y_{24}) \in \mathbb{Z}^{24}$ such that

$$\sum x_i \equiv 0 \bmod 2, \qquad \sum y_i \equiv 1 \bmod 2.$$

Theorem 26 in [8, pp. 287] gives a subgroup $N < \mathrm{Aut}(\Lambda_{24})$ of index prime to 2. This group is isomorphic to $N := \mathcal{C}_2^{12} \rtimes M_{24}$, where $\mathcal{C}_2^{12}$ acts by -1 on an even number of entries of Λ_{24} and M_{24} acts as the group of automorphisms of the binary Golay code, so acts by permuting the entries of Λ_{24}. The following elements of M_{24} generate a Sylow 2-subgroup.

$$\begin{aligned}
\alpha_1 &:= (2,7)(3,16)(8,12)(9,11)(10,18)(15,20)(17,22)(21,23),\\
\alpha_2 &:= (2,8)(3,6)(4,16)(9,13)(10,22)(11,24)(14,19)(15,20),\\
\alpha_3 &:= (2,9)(7,15)(8,24)(10,13)(11,22)(12,14)(17,20)(18,19),\\
\alpha_4 &:= (1,6)(2,12,22,18)(3,23)(4,5)(7,10,17,8)(9,14,11,19)(13,20,24,15)(16,21).
\end{aligned} \tag{4.44}$$

A Sylow 2-subgroup of $\mathrm{Aut}(\Lambda_{24})$ is thus given by this group of permutations, along with multiplication by -1 on an even number of entries.

Lemma 4.4.1. *Suppose $x = (\alpha_1, \ldots, \alpha_{24})$, $\alpha_i \in \mathbb{Z}$ is an odd vector (as in 4.43).*

1. *There exists i, j such that $|\alpha_i| \neq |\alpha_j|$.*

2. *There must exist at least one α_i such that x has an odd number of entries equal to α_i.*

Proof. All lattice vectors in Λ_{24} must have norm that is a multiple of 16. For the first part, suppose on the contrary that $x = (\alpha, \ldots, \alpha) \in \Lambda_{24}$, where α is odd. Then $|(\pm\alpha, \ldots, \pm\alpha)| = 24 \cdot \alpha^2$, which does not divide 16. For the second part, choose i, j such that $|\alpha_i| \neq |\alpha_j|$ (which is possible by part 1). Define n_i as the number entries of x with value α_i. Then $\sum n_i = 24$, and $|x| = \sum n_i \alpha_i^2$. Now again suppose for a contradiction the n_i are all even. Certainly, not all the n_i can divide 16, as $\sum n_i = 24$, and a_i^2 are all odd. So $|x| = \sum n_i a_i^2$ does not divide 16. □

The next lemma is proved using GAP.

Lemma 4.4.2. *Let x be an odd vector (as in 4.43). Then the orbit of x under $H := \mathrm{Syl}_2(M_{24})$ has size at least 8.*

Proof. By Lemma 4.4.1, x has at least two different entries up to absolute value, and at least one of the entries appears an odd number of times. As the group M_{24} acts on x by permuting the entries, it is sufficient to show that the orbit of any vector of type $(0^{n_1}, 1^{n_2})$, n_i odd, is at least size 8 (here the only requirement is the two entries are different; regardless whether it lies in Λ_{24}). If a point contained any more entries, this orbit would only increase under the action of $\mathrm{Syl}_2(M_{24})$.

```
gap> M24:=MathieuGroup(24);;
gap> sylow2sbgp:=SylowSubgroup(M24,2);;
gap> gens:=GeneratorsOfGroup(sylow2sbgp);;
gap> gens:=List(gens,g->PermutationMat(g,24));;
#Redefining the generators so they act naturally on e_i.
gap> sylow2sbgp:=Group(gens);;
gap> ListOfMinima:=[];;
gap> for i in [1..12] do
>  j:=2*i-1; #j is all odd numbers up to 24.
>  odd_vectors:=Union(Combinations(IdentityMat(24,Rationals),j));
#finding combinations of odd numbers of e_i.
>  orbits:=OrbitsDomain(sylow2sbgp,odd_vectors);;
#decomposes into orbits under H
>  L:=List(orbits,o->Size(o));;
>  Add(ListOfMinima,(Minimum(L))); od; #for each collection,
finds minimum size of the orbits.
gap> Minimum(ListOfMinima); #minimum size of all orbits.
8
```

One such vector that achieves this minimum in Λ_{24} is $(1, \ldots, 1, -3)$. □

Proposition 4.4.3. $\mathrm{SymRank}(\phi_\Lambda; 2) = 2^{15} = 32768$

Proof. A set that 2-generates must contain at least one odd vector, say x, as no integer linear combination of even vectors can produce an odd vector. From the definition, x contains all odd entries, therefore no zero entries. Therefore, the orbit of x under $\mathcal{C}_2^{12}$ has size 2^{12}. Lemma 4.4.2 also stated that an odd vector up to absolute value

has minimum orbit size 8. As $\mathcal{C}_2^{12}$ acts trivially on vectors up to absolute value, the orbit of x has size at least $8 \cdot 2^{12} = 2^{15}$. So $\mathrm{SymRank}(\Lambda_{24}; 2) \geq 2^{15}$. Finally, we verify computationally if there exists an orbit of size 32768 that generates Λ_{24}. Here the function "SNFdet" calculates the determinant of the Smith Normal Form of an integer matrix M, thereby returning the index of the sublattice generated by the rows of M. See Appendix C.2.1 for the source code.

```
gap> DisplayImfInvariants(24,3);
#I Q-class 24.3:  Size = 2^22*3^9*5^4*7^2*11*13*23
#I   isomorphism type = C2.Co1
#I   elementary divisors = 1^24
#I   orbit size = 196560, minimal norm = 4
gap> G:=ImfMatrixGroup(24,3);;
gap> sylow2sbgp:=SylowSubgroup(G,2);;
gap> Id_24:=IdentityMat(24,Rationals);;
gap> min_vectors:=Orbit(G,Id_24[1],OnPoints);; #All minimal vectors.
gap> Size(min_vectors);
196560
gap> orbits:=OrbitsDomain(sylow2sbgp,min_vectors);; #Decomposes
minimal vectors in to orbits under the Sylow 2-subgroup.
gap> orbit_sizes:=List(orbits,o->Size(o));;
gap> smallsets:=orbits{Positions(L,32768)};; #Orbits of size 2^15.
gap> List(smallsets,o->SNFdet(o)); #If any of these equal 1, then an orbit
of size 2^15 generates the lattice.
[ 2, 1 ]
```

So there exists an orbit of size 32768 that generates the lattice. This vector is $(1, \cdots, 3)$ (the other vector of orbit size 2^{15} is an even vector of type $(2^8, 0^{16})$). $\square$

4.4.3 SymRank$(\phi_\Lambda; 3)$

The Leech lattice can also be viewed as a complex lattice over $\mathbb{Z}[\omega]$, using the (extended) *ternary code*, see 4.4.1. Recall that $\theta := \omega - \omega^2 = \sqrt{-3}$, and $\mathbb{Z}/3\mathbb{Z} \simeq \mathbb{F}_3 \simeq \mathbb{Z}[\omega]/\theta\mathbb{Z}[\omega]$. The complex Leech lattice $\Lambda_{12}^{(3)}$ ([8, 201]) can be defined as a rank 12 $\mathbb{Z}[\omega]$-module given by the following,

$$\underline{0} + \theta c + 3x, \quad \underline{1} + \theta c + 3y, \quad -\underline{1} + \theta c + 3z, \tag{4.45}$$

where $c \in \mathscr{C}_{12}$, $x = (x_1, \ldots, x_{12})$, $y = (y_1, \ldots, y_{12})$ and $z = (z_1, \ldots, z_{12})$.

$$\sum x_i \equiv 0 \bmod \theta, \quad \sum y_i \equiv 1 \bmod \theta \quad \sum z_i \equiv -1 \bmod \theta. \tag{4.46}$$

The Leech lattice $\Lambda_{24} = (\Lambda_{12}^{(3)})_{\text{real}}$, (giving the same description as 4.41 when multiplying all vectors by $\frac{\sqrt{2}}{3}$). The description of the Leech lattice as a $\mathbb{Z}[\omega]$-lattice provides many analogues with its description using the binary Golay code; most notably the action by the Sylow p-subgroup of Co_1 becomes apparent. Each codeword $c = (c_1, \ldots, c_{12}) \in \mathscr{C}_{12}$ gives an order 3 automorphism, $\text{diag}\{(\omega^{c_1}, \ldots, \omega^{c_{12}})\}$. This yields a group of isomorphism type $\mathcal{C}_3^6$, as $|\mathscr{C}_{12}| = 3^6$. Also, $\text{Aut}(\mathscr{C}_{12}) = M_{12}$, which permutes the codewords in the lattice vectors (4.45). Exactly analogous to the group N in the $p = 2$ case, the group generated by these automorphisms is $\mathcal{C}_3^6 \rtimes M_{12}$. Therefore the Sylow 3-subgroup is isomorphic to $\mathcal{C}_3^6 \rtimes \text{Syl}_3(M_{12})$. This has order 3^9, so is

the Sylow 3 -subgroup of $\cdot 0 = \mathrm{Aut}(\Lambda_{24})$. For instance, a set of generators of the Sylow 3-subgroup of M_{12} is

$$\begin{aligned} \alpha_1 &= (2,5,12)(3,11,4)(6,9,8), \\ \alpha_2 &= (1,9,4)(3,10,6)(7,8,11), \\ \alpha_3 &= (1,6,11)(3,7,9)(4,10,8). \end{aligned} \tag{4.47}$$

Note that this group leaves invariant the sets $(1,3,4,6,7,8,9,10,11)$ and $(2,5,12)$.

Proposition 4.4.4. $\mathrm{SymRank}(\phi_\Lambda; 3) = 3^7 = 2187$.

Proof. The vectors of type $\underline{0} + \theta c + 3x$ generate a sub-$\mathbb{Z}[\omega]$-lattice of index θ, so in order for the corresponding real lattice vectors to 3-generate the lattice, the set must contain one of the other vectors, say x_0. This lattice vector has all non-zero entries as the entries of any lattice vector are the same modulo θ, so under the action of $\mathcal{C}_3^6$ has orbit size 3^6. Now suppose for a contradiction x_0 is fixed under $\mathrm{Syl}_3(M_{12})$. From (4.47), x_0 must be some permutation of $(a, \ldots, a, b, b, b)$, for a, $b \in \mathbb{Z}[\omega]$. Note that if two entries are the same, say x_1 and x_2, then the corresponding c_i and y_i must be the same, as

$$\begin{aligned} \theta c_1 + 3y_1 &= \theta c_2 + 3y_2 \\ \theta c_1 - \theta^2 y_1 &= \theta c_2 - \theta^2 y_2 \\ c_1 - \theta y_1 &= c_2 - \theta y_2 \\ c_1 &= c_2, \end{aligned}$$

as $c_i \in \{0, 1, -1\}$, and thus $y_1 = y_2$. So for $x_0 = (a, \ldots, a, b, b, b)$, the corresponding vector y is of the form $(y_a, \ldots, y_a, y_b, y_b, y_b)$, so $\sum y_i = 9y_1 + 3y_2 \equiv 0 \bmod \theta$ contradicting (4.46). The orbit of x_0 must be at least size 3^7, and there does indeed exist orbits of that size that generate the lattice.

```
gap> G:=ImfMatrixGroup(24,3);;
gap> Id_24:=IdentityMat(24,Rationals);;
gap> sylow3sbgp:=SylowSubgroup(G,3);
<group of 24x24 matrices of size 19683 over Cyclotomics>
gap> min_vectors:=Orbit(G,Id_24[1],OnPoints);;
gap> Size(0);
196560
gap> orbits:=OrbitsDomain(sylow3sbgp,min_vectors);;
gap> sizes:=List(orbits,o->Size(o));;
gap> orbits:=orbits{Positions(sizes,2187)};;
gap> List(orbits,o->SNFdet(o));
[ 1, 3, 3, 1, 1, 1, 1, 1, 0, 0 ]
```

□

4.4.4 SymRank($\phi_\Lambda; p$) $p > 3$

The rest of the symmetric p-ranks are calculated using GAP. For $p = 5$ and 7, the arguments show that any element in an orbit of a particular size lies in a certain index p-sublattice.

Lemma 4.4.5. *If $x \in \Lambda_{24}$ has orbit size less than 125, then x lies in a sublattice Λ' such that $[\Lambda_{24} : \Lambda']$ is divisible by 5.*

Proof. The following GAP code finds a generating set of all orbits of size 25 or less, and finds the index of the sublattice it generates inside Λ_{24}.

```
gap> G:=ImfMatrixGroup(24,3);;
gap> sylow5sbgp:=SylowSubgroup(G,5);;
gap> conj_classes:=ConjugacyClassesSubgroups(sylow5sbgp);;
gap> L:=List(conj_classes,c->Size(c[1])>5);;
gap> conj_classes:=conj_classes{Positions(L,true)};;
gap> fixedpoints:=[];;
for g in conj_classes do
for h in g do
Add(fixedpoints,fixed_points(h));od;od;
gap> fixedpoints:=Union(fixedpoints);;
gap> GcdInt(SNFdet(fixedpoints),5);
5
```

The source code for any functions not in the GAP library used here can be found in Appendix C.2.1. □

Proposition 4.4.6. $\mathrm{SymRank}(\phi_\Lambda; 5) = 125$.

Proof. Lemma 4.4.5 shows that an invariant 5-generating set must contain an orbit of size 125 or greater, so $\mathrm{SymRank}(\phi_\Lambda; 5) = 125$. Indeed a size 125 orbit does generate

the lattice; the following code shows within the minimal vectors there exists 4 such generating orbits of size 125.

```
gap> min_vectors:=Orbit(G,IdentityMat(24,Rationals)[1],OnPoints);;
gap> orbits:=OrbitsDomain(sylow5sbgp,min_vectors);;
gap> size_of_orbits:=List(orbits,p->Size(p));;
gap> pos:=Positions(size_of_orbits,125);;
gap> list_of_indices:=List(orbits,p->SNFdet(p));;
gap> pos:=Positions(list_of_indices,1);
[ 25, 26, 27, 40 ]
```

□

Proposition 4.4.7. $\mathrm{SymRank}(\Lambda_{24}); 7) = 49$.

Proof. Firstly, if $x \in \Lambda_{24}$ is fixed by a non-trivial element of $\mathrm{Syl}_7(\mathrm{Aut}(\Lambda_{24}))$, then it lies in a sublattice of index divisible by 7.

```
gap> G:=ImfMatrixGroup(24,3);;
gap> sylow7sbgp:=SylowSubgroup(G,7);;
gap> J7:=ConjugacyClassesSubgroups(sylow7sbgp);;
for g in J7 do
for h in g do
Add(A,fixed_points(h));od;od;
gap> SNFdet(fix);
117649
```

As $117649 = 7^6$, there must exist an orbit of size 49 in an invariant, 7-generating set. Indeed, an orbit of size 49 does p-generate the lattice.

```
gap> 7genset:=Orbit(sylow7sbgp,IdentityMat(24,Rationals)[2],OnPoints);;
gap> Size(7genset);SNFdet(7genset);
49
8
```

□

Proposition 4.4.8. $\mathrm{SymRank}(\Lambda_{24}); 11) = \mathrm{SymRank}(\Lambda_{24}); 23) = 24$.

Proof. It suffices to show that for each p, an invariant p-generating set of size 24 exists and is invariant under the action of the Sylow p-subgroup.

```
gap> H11:=SylowSubgroup(G,11);;
gap> fixedpoints:=fixed_points(sylow11sbgp);;
gap> orbit_1:=Orbit(sylow11sbgp,IdentityMat(24,Rationals)[8],OnPoints);;
gap> orbit_2:=Orbit(sylow11sbgp,IdentityMat(24,Rationals)[17],OnPoints);;
gap> 11genset:=Union(Union(orbit_1,orbit_2),fixedpoints{[1,2]});;
gap> Size(11genset);SNFdet(11genset);
24
1
```

```
gap> sylow23sbgp:=SylowSubgroup(G,23);;
gap> fixedpoints:=fixed_points(sylow23sbgp);;
gap> Id_24:=IdentityMat(24,Rationals);;
```

```
gap> 23genset:=Union([fixedpoints[1]],
Orbit(sylow23sbgp,Id_24[1],OnPoints));;
gap> Size(23genset);SNFdet(23genset);
24
235
```

□

Proposition 4.4.9. $\mathrm{SymRank}(\Lambda_{24}); 13) = 26$.

Proof. The Sylow 13-subgroup fixes no point in Λ_{24}.

```
gap> fixed_points(SylowSubgroup(G,13));
[ ]
```

Therefore an invariant set must have size divisible by 13, and $\mathrm{SymRank}(\Lambda_{24}; 13) \geq 26$.

```
gap> orbit_1:=Orbit(sylow13sbgp,Id_24[1],OnPoints);;
gap> orbit_2:=Orbit(sylow13sbgp,Id_24[2],OnPoints);;
gap> 13genset:=Union(orbit_1,orbit_2);;
gap> Size(13genset);SNFdet(13genset);
26
1
```

□

Chapter 5

Essential dimension of extensions of small finite groups by tori

This chapter aims to take a finite group F, classify all possible extensions of F by algebraic tori and attain bounds on the essential (p)-dimension of these extensions. In order to classify all extensions, it is necessary to classify all algebraic tori with F-action, which is equivalent to classifying all finitely generated torsion-free $\mathbb{Z}F$-modules. In general this is a hopeless task, as most finite groups have wild (integral) representation type. For the purposes of finding the essential p-dimension of tori and extensions of finite groups by split tori, it is sufficient to classify lattices up to genus, confident in the fact that a decomposition of $\mathbb{Z}_{(p)}F$-modules is unique, by the Krull-Schimdt Theorem [12, Thm 36.0 pp. 768]. For certain F, this is achievable.

5.1 Groups of finite representation type

Recall that a lattice L is *indecomposable* if there exists no non-trivial lattices L_1, L_2 such that $L_1 \oplus L_2 \simeq L$.

Theorem 5.1.1. [22, Thm. 8] *Let $\mathcal{G}$ be a finite group. The number of indecomposable $\mathcal{G}$-lattices is finite if and only if, for each prime p dividing $|\mathcal{G}|$, the Sylow p-subgroups are cyclic order p or p^2.*

Such groups $\mathcal{G}$ are said to be of *finite representation type*, and are exclusively extensions of cyclic groups by cyclic groups. For instance, the groups $\mathcal{C}_m \rtimes \mathcal{C}_n$ for m, $n \in \mathbb{N}$, which include the dihedral groups D_{2n}. As well as being able to classify all torsion-free $\mathbb{Z}F$-modules, these groups possess other properties that will be useful for calculating the essential dimension of extensions of F by split tori. The following is a combination of several results, applied to the situation where F is a group of finite representation type.

Proposition 5.1.2. [5, pp.58] *Let F be a group of finite representation type. Then $H^2(F;T) = T^F/\mathrm{Im}(N_F(T))$, where T^F is the F-fixed points of T, and $N_F : T \to T$ is the norm map, $t \mapsto \sum_{g\in F} g \cdot t$.*

In particular, Corollary 2.7.7 gives us the group of extensions of F by T, $\mathrm{Ext}^1(F_k;T) = H^2(F;T(k)) = H^0(F;T(k)) = T(k)^F$, where $T(k)$ is the k-rational points of T, and $T(k)^F$ is its F-fixed points. Recall the short exact sequence at (2.31),

$$1 \longrightarrow T \longrightarrow G \xrightarrow{\pi} F \longrightarrow 1. \tag{5.1}$$

Proposition 5.1.3. *Let G be an algebraic group that satisfies (5.1), where $F = \mathcal{C}_n$, and assume the field k has characteristic not dividing n. For any F-invariant subset $\Delta \subset T^*$, there exists a representation of V_Δ of G, where $\dim(V_\Delta) = |\Delta|$, such that if Δ p-generates T^*, then V_Δ is p-faithful. If Δ also satisfies K_F, (see Lemma 3.5.3) then V_Δ is p-generically free.*

Proof. Δ splits into disjoint orbits $\Delta = \coprod \Delta_i$. Set $\lambda_i \in T$ as an orbit representative; either λ is fixed by a cyclic group or by nothing.

If $|\Delta_i| = n$, then there exist a representation of G given by

$$V_{\Lambda_i} := \mathrm{Ind}_T^G(\lambda_i), \tag{5.2}$$

which has dimension n.

If λ_i is fixed by a cyclic group then consider the subgroup $G_{\lambda_i} := \{g \in G \mid g \cdot \lambda_i = \lambda_i\}$. Indeed, there must exist some $r \in G_{\lambda_i}$ such that $r^n \subset T$, but $r^i \nsubseteq T$ for $1 \leq i < n$. The $\{r^i\}$ form a set of a coset representatives of G/T, so $G = T + rT + \ldots + r^{n-1}T$. Equivalently, for every $g \in G_{\lambda_i}$, there exists a unique i and t such that $g = r^i t$. Define $\rho : G_{\lambda_i} \to k^\times$ as $\rho(g) = \lambda(t)$, for this $g = r^i t$. This is a morphism of groups, as for g, $g' \in G_{\lambda_i}$,

$$\begin{aligned}
\rho(gg') &= \rho(r^i t r^j t') \\
&= \rho(r^{i+j} r^{-j} t r^j t') \\
&= \lambda_i(r^{-j} t r^j t') \quad \text{as } r^{-j} t r^j t' \in T.
\end{aligned}$$

$$= \lambda_i(r^{-j}tr^j)\lambda_i(t')$$
$$= \lambda_i(t)\lambda_i(t') \quad \text{as } r \text{ acts trivially on } \lambda_i.$$

The corresponding map on the coordinate algebras $\mathcal{O}(\mathbb{G}_m) \to \mathcal{O}(G)$ factors through $\mathcal{O}(T)$, and as λ is a character of T, this defines a comorphism, so ρ is indeed a morphism of algebraic groups thus a character of G_{λ_i}.

Now the representation

$$V_{\Lambda_i} := \mathrm{Ind}_{G_{\lambda_i}}^{G}(\rho), \tag{5.3}$$

is a representation of G of dimension $|\Delta_i|$. For $\Delta = \coprod \Delta_i$, using the representations defined above, $V_\Delta := \bigoplus V_{\Delta_i}$ gives a representation of G of dimension $|\Lambda|$.

For the last part, the proof is from [30, Lemma 1.11], and is true regardless of the choice of finite group F. Let M be the kernel of the representation $T \to \mathrm{GL}_{V_\Lambda}$, and $X_\Lambda = \langle \Delta \rangle$, the sublattice generated by Δ. The map $T \to \mathrm{GL}_{V_\Lambda}$ factors through $\mathrm{Diag}(X_\Lambda)$, and this acts faithfully on V_Δ. As Δ is p-generating, T^*/X_Λ is finite of order prime to p, and $\mathrm{Diag}(T^*/X_\Lambda) = M$ by the above discussion. Therefore the representation is p-faithful if and only if Δ p-generates. Likewise, if the representation V_Λ is p-faithful, the same argument implies Δ is p-faithful. Finally, Lemma 3.5.3 gives us that if Δ satisfies K_F, V_Λ is p-generically free. □

Proposition 5.1.4. *Let k be a field of characteristic not p, that contains a primitive $(p^r)^{th}$ root of unity. If G is an algebraic group over k that satisfies (5.1), where $\mathrm{Syl}_p(F) = \mathcal{C}_{p^r}$. Then*

$$\mathrm{SymRank}(\phi_{T^*}; p) - \dim(G) \leq \mathrm{ed}_k(G; p) \leq \mathrm{SymRank}(\phi_{T^*}; p) - \dim(G) + 1, \tag{5.4}$$

where ϕ_{T^*} is the integral representation $F \to T^*$. If a minimally generating, F-invariant set Λ has size $\mathrm{SymRank}(\phi_{T^*}; p)$*, then these bounds also hold true for* $\mathrm{ed}_k(G)$.

Proof. If $\pi : G \to F$ is the surjection in the exact sequence 5.1, and Γ_p the Sylow p-subgroup of F, then denote by G_{Γ_p} the preimage of Γ_p under π. Certainly, $[G : G_{\Gamma_p}] = [F : \Gamma_p]$ is finite and prime to p, and by Lemma 3.3.2, $\mathrm{ed}_k(G_{\Gamma_p}; p) = \mathrm{ed}_k(G; p)$. Therefore, it suffices to find bounds on $\mathrm{ed}_k(G_{\Gamma_p}; p)$, and by Lemma 3.5.6, k can be replaced by $k^{(p)}$.

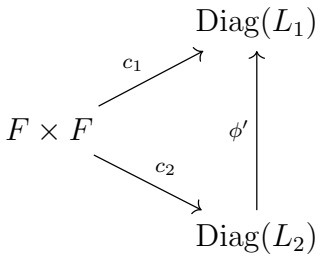
For the lower bound, it suffices to consider a minimal p-faithful representation V of G_{Γ_p}, by Theorem 3.5.7. As V is a representation of T, it decomposes into weight spaces, $\Delta \subset T^*$. As V is p-faithful on T, Δ must be p-generating, and as V is a representation of G_{Γ_p}, Δ must be invariant under the action of Γ_p. Therefore $\mathrm{SymRank}(\phi_{T^*}; p) \leq \dim(V)$. For a minimal p-generating Γ_p-invariant set $\Delta \subset T^*$, using the representation defined in Proposition 5.1.3 gives such a p-faithful representation.

Theorem 3.5.7 also gives an upper bound, and a p-generically free representation can be found by taking the faithful representation W of Γ_p of dimension one, and by Proposition 3.5.2, the representation $V_\Lambda \times W$ is p-generically free. If Δ is invariant under F, and generates T^*, then V_Δ is a generically free representation of G, so the last statement follows from $\mathrm{ed}_k(G; 2) \leq \mathrm{ed}_k(G)$, and $\mathrm{ed}_k(G) \leq \dim(V_\Delta) - \dim(G)$ (Proposition 3.2.1). □

Remark 5.1.5. The only algebraic groups of essential dimension 0 are connected (see [40, Theorem 5.4]) so if $\mathrm{SymRank}(\phi_{T^*}; p) = \mathrm{rank}(T^*)$, then G has essential dimension 1.

5.2 The category $\mathbf{Ext}_F$

The following section introduces a new category, $\mathbf{Ext}_F$. The objects of $\mathbf{Ext}_F$ are given by the data (L, c), where L is a $\mathbb{Z}F$-lattice and $c \in H^2(F; \mathrm{Diag}(L))$, where $\mathrm{Diag}(L)$ is a split torus. Morphisms are $\mathbb{Z}F$-morphisms $\phi : L_1 \to L_2$ (F-equivariant $\mathbb{Z}$-module homomorphisms), such that the following diagram commutes



where $\phi' := \mathrm{Diag}(\phi)$, so for $I \in \mathrm{Spec}(k[L_2])$, $\phi'(I) = \phi^{-1}(I) \in \mathrm{Spec}(k[L_1])$.

The data (L, c) defines a unique extension up to isomorphism, by Corollary 2.7.7. There is a natural notion of summing two objects in $\mathbf{Ext}_F$. Take (L_1, c_1), $(L_2, c_2) \in \mathbf{Ext}_F$. These define algebraic groups G_i, unique up to isomorphism of extension that fit in the short exact sequence (2.31). Define the sum, $G_1 \oplus_F G_2$, as the pullback along the diagonal map $\Delta : F \to F \times F$. Specifically, it is the universal object satisfying

$$\begin{array}{ccc} G_1 \oplus_F G_2 & \longrightarrow & F \\ \downarrow & & \downarrow \Delta \\ G_1 \times G_2 & \xrightarrow{\pi_1 \times \pi_2} & F \times F \end{array}$$

There is also a notion of decomposition. Recall that an F-lattice L is *indecomposable* if there exists no non-trivial lattices L_1, L_2 such that $L_1 \oplus L_2 \simeq L$. For any F-lattice, there exists a (not necessarily unique) decomposition $L = \bigoplus L_i$ into

indecomposable F-lattices L_i. This means the corresponding tori also decompose, $\mathrm{Diag}(L) = \prod \mathrm{Diag}(L_i)$ into *indecomposable tori*. With respect to the 2-cocycles c, define $c_i \in H^2(F; T_i)$ as the composition $\rho_i \circ c$, where ρ_i is the projection $T \to T_i$, so (L, c) decomposes to indecomposable factors (L_i, c_i). Although all lattices can be decomposed, they can in theory "lose" some information about the original extension (i.e. $c \neq \bigoplus c_i$). Therefore it is not a given that all extensions can be built up from indecomposable ones.

Proposition 5.2.1. *If F has finite representation type, and* $\mathrm{char}(k)$ *is coprime to $|F|$ then any object in $\mathbf{Ext}_F$ decomposes as a sum $\simeq G_1 \oplus_F \ldots \oplus_F G_n$, where the G_i are given by (L_i, c), and the L_i are indecomposable.*

Proof. Recall the definition of the norm map $N_F(T)$ in Proposition 5.1.2. F acts component-wise on $T_1 \times T_2$, so any element (t_1, t_2) fixed by F must also have $t_i \in T_i^F$. Conversely, if $t_i \in T_i^F$ for $i = 1, 2$ then $(t_1, t_2) \in (T_1 \times T_2)^F$.
Similarly, if $(t_1, t_2) \in \mathrm{Im}(N_F(T_1, T_2))$, then there exists some $(t_1', t_2') \in T_1 \times T_2$ such that $N_F(t_1', t_2') = (t_1, t_2)$, so $t_i \in \mathrm{Im}(N_F(T_i))$. Again, given $t_i \in N_F(T_i)$, then $(t_1, t_2) \in \mathrm{Im}(N_F)(T_1 \times T_2)$. Therefore there exists canonical isomorphisms $(T_1 \times T_2)^F \cong T_1^F \times T_2^F$, and $\mathrm{Im}(N_F(T_1 \times T_2)) \cong \mathrm{Im}(N_F(T_1)) \times \mathrm{Im}(N_F)(T_2)$, so

$$\begin{aligned} H^2(F; T_1 \times T_2) &= (T_1 \times T_2)^F / \mathrm{Im}(N_F(T_1 \times T_2)) \\ &= T_1^F / \mathrm{Im}(N_F(T_1)) \times T_2^F / \mathrm{Im}(N_F(T_2)), \end{aligned}$$

and each 2 cocycle $c \in H^2(F; T_1 \times T_2)$ equals $c_1 \oplus c_2$, for $c_i \in H^2(F; T_i)$. Therefore any object $(L, c) \in \mathbf{Ext}_F$ decomposes to a sum $\bigoplus (L_i, c_i)$ for indecomposable L_i. $\square$

Given a group F of finite representation type and a list of the indecomposable F-lattices $\mathbb{L}$, then the category $\mathbf{Ext}_F$ of all extensions of F by split tori is characterised by the list $\mathbb{L}$ and the choice of 2-cocycle $c \in H^2(F; \mathrm{Diag}(L))$. Bounds on the essential (p-)dimension can be found using Proposition 5.1.4, and because the lower bound is given by the symmetric p-rank, Remark 4.0.5 asserts that the symmetric p-rank, (and therefore the dimension of a minimally p-faithful representation) is additive with $\oplus_F$. For G an extension of a finite group by a torus, define $\mathrm{gap}(G; p)$ as the difference between the dimensions of a minimally p-faithful and minimally p-generically free representation (as done in [29]).

Proposition 5.2.2. *Let F be a group of finite representation type, and (L, c_1), (L_2, c_2) be two objects in $\mathbf{Ext}_F$, over a field characteristic not p. Let G_i be the algebraic groups given by (L_i, c_i). Then*

$$\mathrm{gap}(G_1 \oplus_F G_2; p) \leq \min\{\mathrm{gap}(G_1; p), \mathrm{gap}(G_2; p)\}.$$

Proof. Suppose V_i, W_i are minimal p-faithful and p-generically free representations of G_i respectively, so $\mathrm{gap}(G_i) = \dim(W_i) - \dim(V_i)$. Then $V_1 \oplus V_2$ is a (minimal) p-faithful representation of $G_1 \oplus_F G_2$ (see previous discussion). Now consider the representation $W_i \oplus V_j$, $i \neq j$. There exists some dense open set $U_i \subset W_i$ such that $|\mathrm{Stab}_{G_i}(U_i)| = q$, for some q prime to p. For U_j dense in V_j, $U := U_i \oplus U_j$ is a dense open subset of $V_i \oplus W_j$ with $|\mathrm{Stab}_G(U)| = q'$ for some q' prime to p. Therefore, $V_i \oplus W_j$ is a p-generically free representation of $G_1 \oplus_F G_2$, the smallest of which has dimension $\min\{\dim(W_i \oplus V_j)\}$, $i \neq j$, so $\mathrm{gap}(G_1 \oplus_F G_2) \leq \min\{\mathrm{gap}(G_1), \mathrm{gap}(G_2)\}$. □

In [27, Theorem 12.3], for all indecomposable $\mathcal{C}_{p^2}$-lattices M_i, the value of $\mathrm{ed}_k(\mathrm{Diag}(M_i); p)$ was calculated, where $T := \mathrm{Diag}(M_i)$ was split by $\mathcal{C}_{p^2}$. By Proposition 3.4.2, this is exactly the value of the symmetric p-rank, and could be extended to any $\mathcal{C}_{p^2}$-lattice, as the symmetric p-rank is additive (see Remark 4.0.5). Considered here are instead groups that are extensions of $\mathcal{C}_{p^2}$ by split tori, along with similar considerations for $\mathcal{C}_2 \times \mathcal{C}_2$ and D_{2p}.

5.3 $\mathcal{C}_p$ and $\mathcal{C}_{p^2}$

An example where a minimal p-faithful representation fails to be p-generically free is when $G = \mathrm{Diag}(A_{p-1}) \rtimes \mathcal{C}_p$ (here, $\mathrm{Diag}(A_{p-1})$ is the torus of root datum of Lie type A_{p-1}). G has a faithful representation of dimension p, that is not generically free (see Example 3.5.8) and the dimension of the minimal p-generically free representation is $p+1$, which leaves $1 \leq \mathrm{ed}_k(\mathrm{Diag}(A_{p-1}) \rtimes \mathcal{C}_p; p) \leq 2$. The true value is 2, because $\mathrm{Diag}(A_{p-1}) \rtimes \mathcal{C}_p$ is the normalizer of the maximal torus of PGL_p, which has essential p-dimension 2, and for any semisimple algebraic group G, $\mathrm{ed}_k(N_T(G); p) \geq \mathrm{ed}_k(G; p)$. By Proposition 3.5.2, given any (p)-faithful representation V of G, then $V \times W$ is (p)-generically free, where W is the faithful 1 dimensional representation of $\mathcal{C}_{p^2}$. It is shown by the following proposition that the gap between the dimensions of the p-faithful and p-generically free representations only exists for the split extensions.

Proposition 5.3.1. *If G is a non-split extension of $F := \mathcal{C}_{p^2}$ by a split torus, over a field containing a $(p^2)^{th}$ root of unity, then a p-faithful representation is p-generically free.*

Proof. If a representation V is p-faithful, then the restriction to T is p-generically free (see [28, Lemma 2.5]), so for any dense open set $U \subset V$, $|\mathrm{Stab}_T(U)| = q$ for some q prime to p. Take some $g = r^i t$, of order p^2 modulo T as in Proposition 5.1.3, then $g^{p^2} \in T$ but $g^{p^2} \neq 1$ as the extension is not split. Suppose for a contradiction that $|\mathrm{Stab}_G(U)|$ is either infinite or divides p. So g fixes u then g^{p^2} fixes u, so $|\mathrm{Stab}_T(U)|$ divides p, a contradiction. Therefore $|\mathrm{Stab}_G(U)| = q'$ for some q' prime to p. □

Corollary 5.3.2. *Let G satisfy 2.31, where $F = \mathcal{C}_{p^2}$ and $\mathrm{char}(k) \neq p$. Let $(G^\circ)^* = \bigoplus_i L_i$, where L_i are indecomposable F-lattices. If G is non-split then*

$$\mathrm{ed}_k(G;p) = \max\{\sum \mathrm{SymRank}(L_i;p) - \dim(G), 1\}. \tag{5.5}$$

Else

$$\begin{aligned} \max\{\sum_i \mathrm{SymRank}(L_i;p) - \dim(G), 1\} &\leq \mathrm{ed}_k(G;p) \\ &\leq \sum_i \mathrm{SymRank}(L_i;p) - \dim(G) + 1. \end{aligned} \tag{5.6}$$

Proof. Propositions 5.1.4 along with Remark 4.0.5 give the upper and lower bounds in (5.6). As the group G is disconnected, $\mathrm{ed}_k(G) \geq 1$. If G is a non split extension, then from Proposition 5.3.1, this is also the dimension of a minimal p-generically free representation, so the bounds meet, resulting in (5.5).

Remark 5.3.3. Each $\mathcal{C}_{p^2}$-invariant p-generating set found in Table 5.1 is also generating, the p-generically free representations are in fact generically free, and as $\mathrm{ed}_k(G;p) \leq \mathrm{ed}_k(G)$, these bounds are also true for the essential dimension.

□

To calculate the symmetric p-ranks of the indecomposable $\mathcal{C}_{p^2}$-lattices, an exhaustive list can be found in [12, 34.35], where they are given as certain extensions of other lattices. In [27, pp. 27], this list was translated into quotients of various permutation lattices. The group, $\mathcal{G} := \langle g \rangle = \mathcal{C}_{p^2}$, and $\mathcal{H} := \langle h \rangle = \mathcal{C}_p$, The permutation lattice $\mathbb{Z}\mathcal{H}$ can be considered as a $\mathcal{G}$ lattice by the action $g \cdot h^i = h^{i+1}$, $g \in \mathcal{G}$, $h \in \mathcal{H}$. In the following list, $\delta_{\mathcal{G}} := \sum_i g^i$, and $\epsilon := \sum_i g^{pi}$ for $i \in [0, \ldots, p-1]$.

$$M_1 = \mathbb{Z}, \qquad M_2 = \mathbb{Z}\mathcal{H}, \qquad M_3 = \mathbb{Z}\mathcal{H}/\langle \delta_{\mathcal{H}} \rangle, \quad M_4 = \mathbb{Z}\mathcal{G},$$
$$M_5 = \mathbb{Z}\mathcal{G}/\langle \delta_{\mathcal{G}} \rangle, \quad M_6 = \mathbb{Z}\mathcal{G} \oplus \mathbb{Z}/\langle \delta_{\mathcal{G}} - p \rangle. \quad M_7 = \mathbb{Z}\mathcal{G}/\langle \epsilon \rangle, \qquad M_8 = \mathbb{Z}\mathcal{G}/\langle \epsilon - g\epsilon \rangle \quad ,$$

and the following four families

$$\begin{aligned}
M_{9,r} &= \mathbb{Z}\mathcal{G} \oplus \mathbb{Z}\mathcal{H}/\langle \epsilon - (1-h)^r \rangle, && 1 \le r \le p-1 \\
M_{10,r} &= \mathbb{Z}\mathcal{G} \oplus \mathbb{Z}\mathcal{H}/\langle \epsilon(1-g) - (1-h)^{r+1} \rangle, && 1 \le r \le p-2 \\
M_{11,r} &= \mathbb{Z}\mathcal{G} \oplus \mathbb{Z}\mathcal{H}/\langle \epsilon - (1-h)^r, \delta_{\mathcal{H}} \rangle, && 1 \le r \le p-2 \\
M_{12,r} &= \mathbb{Z}\mathcal{G} \oplus \mathbb{Z}\mathcal{H}/\langle \epsilon(1-g) - (1-h)^{r+1}, \delta_{\mathcal{H}} \rangle. && 1 \le r \le p-2
\end{aligned}$$

Proposition 5.1.2 and the subsequent discussion gives the definition $H^2(F;T) = T^F/\mathrm{Im}(N_F(T))$, where $N_F(T)$ is the norm map $t \mapsto \sum_{g \in G} g \cdot t$. The calculations of $H^2(F;T)$ given by the formula in Proposition 5.1.2, and an invariant generating

set for each M_i are given in Appendix B.1. Each symmetric p-rank is given by the rank of P, so for the corresponding p-presentation $\phi : P \to P/N$, we have $\ker \phi = qN$ for some q prime to p. As N has a faithful action by $\mathcal{H}$, the condition K_F (see Lemma 3.5.3) fails on every one of the lattices in $\mathbb{L}$ because N is a faithful $\mathcal{H}$-module, and this is in the kernel of $P/N \to N$. In Table 5.1, the symmetric p-ranks were already known, but the data in column $H^2(\mathcal{C}_{p^2}; \mathrm{Diag}(L))$ is new.

L	$\mathrm{rank}(L)$	$H^2(\mathcal{C}_{p^2}; \mathrm{Diag}(L))$	$\mathrm{SymRank}(L; p)$
M_1	1	$\{1\}$	1
M_2	p	$\{1\}$	p
M_3	$p-1$	$\mathbb{Z}/p\mathbb{Z}$	p
M_4	p^2	$\{1\}$	p^2
M_5	p^2-1	$\mathbb{Z}/p^2\mathbb{Z}$	p^2
M_6	p^2	$\{1\}$	p^2
M_7	p^2-p	$\mathbb{Z}/p\mathbb{Z}$	p^2
M_8	p^2-p+1	$\{1\}$	p^2
$M_{9,r}$	p^2	$\mathbb{Z}/p\mathbb{Z}$	p^2+p
$M_{10,r}$	p^2+1	$\{1\}$	p^2+p
$M_{11,r}$	p^2-1	$(\mathbb{Z}/p\mathbb{Z})^2$	p^2+p
$M_{12,r}$	p^2	$\mathbb{Z}/p\mathbb{Z}$	p^2+p

Table 5.1: Summary information table for all indecomposable $\mathcal{C}_{p^2}$ lattices.

Example 5.3.4. Take $L := M_{9,r}$. The condition $\epsilon - (1-h)^r = 0$ yields

$$\sum_{i=0}^{p-1} g^{pi} - \sum_{k=0}^{r} (-1)^k \binom{r}{k} h^k = 0$$

Acting by g^j, for $0 \leq j \leq p-1$ gives

$$\begin{aligned} g^j \cdot (\sum_{i=0}^{p-1} g^{pi} - \sum_{k=0}^{r} (-1)^k \binom{r}{k} h^k) = 0 \qquad & 0 \leq j \leq p-1 \\ g^j \cdot (\sum_{i=0}^{p-1} g^{pi}) = g^j \cdot (\sum_{k=0}^{r} (-1)^k \binom{r}{k} h^k) \qquad & 0 \leq j \leq p-1 \\ \Rightarrow \sum_{i=0}^{p-1} g^{pi+j} = \sum_{k=0}^{r} (-1)^k \binom{r}{k} h^{k+j}. \qquad & 0 \leq j \leq p-1. \end{aligned}$$

Translated to the torus case $T := \{t_1, \ldots t_{p^2}, s_1, \ldots s_p)\} = \mathrm{Diag}(M_{9,r})$, the relations become multiplicative,

$$\prod_{i=1}^{p} t_{pi+j} = \prod_{k=1}^{r} s_{k+j}^{(-1)^{k-1}\binom{r}{k-1}} \tag{5.7}$$

To find $H^2(\mathcal{G}; T)$, the formula in Proposition 5.1.2 is used. First note that elements in $T^{\mathcal{G}}$ must be of the form $(t, \ldots, t, s, \ldots, s)$. As the alternating sum of binomial coefficients is 0, the right hand side of (5.7) is 1, so $t^p = 1$, thus t is a p^{th} root of unity. There are no other constraints, so $T^{\mathcal{G}} = (\zeta, \ldots, \zeta, s, \ldots, s)$, where ζ is a p^{th} root of unity. Now consider

$N_{\mathcal{G}}(t_1, \ldots, t_{p^2}, s_1, \ldots, s_p)$. The first p^2 entries are

$$\begin{aligned} \prod_{i=1}^{p^2} t_i &= \prod_{j=0}^{p-1} \prod_{i=1}^{p} t_{ip+j} \\ &= \prod_{j=0}^{p-1} \prod_{k=1}^{r} s_{k+j}^{(-1)^{k-1}\binom{r}{k-1}} \qquad \text{using (5.7)} \\ &= \prod_{j=1}^{p} \prod_{k=1}^{r} s_j^{\sum_{k=1}^{r} (-1)^{k-1}\binom{r}{k-1}} \\ &= 1. \end{aligned}$$

Also, as $N_{\mathcal{G}}(1,\ldots,1,s^{\frac{1}{p^2}},\ldots,s^{\frac{1}{p^2}}) = (1,\ldots,1,s,\ldots,s)$, then

$$H^2(\mathcal{G};T) = T^{\mathcal{G}}/\mathrm{Im}(N_{\mathcal{G}}(T)) = \mathbb{Z}/p\mathbb{Z}.$$

A generating set is just the image of the standard basis of $P = \mathbb{Z}\mathcal{G} \oplus \mathbb{Z}\mathcal{H}$ in L, so this set of characters are just evaluation on the entries of $(t_1,\ldots,t_{p^2},s_1,\ldots,s_p)$.

5.4 $\mathcal{C}_2 \times \mathcal{C}_2$

The following proposition shows how to build representations of extensions of $\mathcal{C}_2 \times \mathcal{C}_2$ by algebraic tori, by slightly adapting the proof of Proposition 5.1.3. Many of the same arguments are used; to avoid too much repetition, the reader is referred back at certain points in this proof.

Proposition 5.4.1. *Let G be an algebraic group over k, $\mathrm{char}(k) \neq 2$, that satisfies (2.31) with $F = \mathcal{C}_2 \times \mathcal{C}_2$, and $T := G^\circ$. For an F-invariant subset $\Delta \subset T^*$, a representation V_Δ of G exists such that,*

1. *If G is split, then $\dim V_\Delta = |\Delta|$.*
2. *If G is non-split, then $\dim V_\Delta = |\Delta| + |\Delta_0|$, where Δ_0 is the subset of Δ that comprises exclusively of all orbits of size 1.*

In addition,

1. *If Δ is 2-generating then V_Δ is 2-faithful.*

2. If Δ satisfies K_F, then V_Δ is 2-generically free.

Proof. Firstly, if G is split, then the representation $V_\Delta := \mathrm{Span}_k\{(v_\lambda) \mid \lambda \in \Delta\}$ (as in the proof of Theorem 4.2.1) gives a representation of G of dimension $|\Delta|$. Now suppose G is non-split. Define $\Delta' = \Delta \setminus \Delta_0$, F_λ the subgroup of F that fixes $\lambda \in \Delta$, and G_λ the preimage of F_λ under the surjection π (G_λ is therefore all the elements of G that fix λ under the natural action of G on Δ). As the distinct orbits $\Delta_i \subset \Delta'$ contain no orbits of size 1, then for all $\lambda \in \Delta_i$, $G_\lambda/T \simeq \mathcal{C}_2$ or $G_\lambda = T$. For each Δ_i, a representation V_{Δ_i} of G of dimension $|\Delta_i|$ can be therefore be constructed using the same argument as Proposition 5.1.3; there exists a character of G_λ, and the induced representation $\mathrm{Ind}_{G_\lambda}^G(\rho)$ gives a representation of G of dimension $|\Delta_i|$. Set $V_{\Delta'} = \bigoplus_i V_{\Delta_i}$.

Now for each $\lambda \in \Delta_0$, find a $G' \leqslant G$ such that $G'/T \simeq \mathcal{C}_2$. As there exists a character of G', define V_λ as the 2 dimensional induced representation $\mathrm{Ind}_{G'}^G$, and set $V_{\Delta_0} = \bigoplus_{\lambda \in \Delta_0} V_\lambda$. Putting these together, there exists a representation $V_\Delta = V_{\Delta'} \oplus V_{\Delta_0}$ with dimension $|\Delta'| + 2|\Delta_0| = |\Delta| + |\Delta_0|$.

For the second set of statements; the first is shown using the exact same argument as Proposition 5.1.3 (which is true for any choice of finite group F), and the second is a application of Lemma 3.5.3. □

Corollary 5.4.2. *Let G be as in Proposition 5.4.1. If G is split, then*

$$\mathrm{SymRank}(\phi_{T^*}; 2) - \dim(T) \leq \mathrm{ed}_k(G; 2) \leq \mathrm{SymRank}(\phi_{T^*}; 2) - \dim(T) + 2. \quad (5.8)$$

Else

$$\mathrm{SymRank}(\phi_{T^*};2) - \dim(T) \leq \mathrm{ed}_k(G;2) \leq \mathrm{SymRank}(\phi_{T^*};2) - \dim(T) + 2 + r,$$

where r equals the number of trivial rank 1 summands in T^*. If K_F is satisfied, then the lower bound is an equality.

Proof. Replacing k by the 2-special closure $k^{(2)}$ (and thus not changing the value of $\mathrm{ed}(G;2)$) means one can apply Theorem 3.5.7 for the bounds on $\mathrm{ed}(G;2)$. As in the proof of Proposition 5.1.4, the lower bound is gained by the virtue that any 2-faithful representation must decompose into weight spaces of which there are at least $\mathrm{SymRank}(\phi_{T^*};p)$. Note that an orbit $\Delta_i \subset \Delta$ has size 1 if and only if $L := T^*$ can be decomposed with trivial rank 1 summands, so applying Proposition 5.4.1 gives upper and lower bounds for G according to whether G is split. If the 2-faithful representation is not 2-generically free, then take the representation $V_\Lambda \times W$, where W is the faithful 2 dimensional representation of $\mathcal{C}_2 \times \mathcal{C}_2$, which is 2-generically free by Proposition 3.5.2. Finally, the last statement is an application of Lemma 3.5.3. □

Remark 5.4.3. As with $\mathcal{C}_{p^2}$, all minimal 2 generating sets are also generating sets, giving generically free representations of G, so the bounds of the essential p-dimension are true for the essential dimension, by Proposition 3.2.1.

There is not a finite set of indecomposable $\mathcal{C}_2 \times \mathcal{C}_2$-lattices, but there are finitely many of a given rank. In fact, indecomposable $\mathcal{C}_2 \times \mathcal{C}_2$-lattices are closely connected to solutions of the "4-subspace problem" over the field $\mathbb{F}_2$ which was solved by Nazarova [38]. A *reduced 4-subspace system* over k comprises a vector space V over k, and a

set of 4 subspaces of V, $\{V, V_1, V_2, V_3, V_4\}$ such that any three of the V_i span V. The 4-subspace problem is classifying all such indecomposable systems over an arbitrary field k.

Remark 5.4.4. The 4 subspace problem is also equivalent to finding the indecomposable representations of the quiver $\widetilde{D}_4$ diagram. In 1972, it was proved by Gabriel ([17]) that the representations of a quiver have finite type if and only if the quiver is a simply laced Dynkin diagram, (appropriately titled *Gabriel's theorem*). Indeed if this was the "3-subspace problem" then the representation theory would be of finite type, as these is equivalent to representations of the quiver D_4. See [42] for an introduction to quivers and their representations.

Figure 5.1: Dynkin diagram D_4 and $\tilde{D}_4$, indecomposable representations of which correspond to the indecomposable solutions of the 3-subspace and 4-subspace problems.

The usual notions of morphisms and decomposability of 4-subspace systems exist; a morphism of systems is a k-linear map $\theta : V \to W$ such that $\theta(V_i) \subset W_i$ for all i, and a system is decomposable if there exists systems $\{W, W_1, W_2, W_3, W_4\}$ and $\{W', W_1', W_2', W_3', W_4'\}$ such that $W_i \oplus W_i' = V_i$ for all i, and $W \oplus W' = V$.
A $\mathcal{G}$-lattice is *reduced* if it non-trivial and contains no $\mathbb{Z}G$-free or rank 1 summands.

Proposition 5.4.5. *There is a bijection between reduced 4-subspace systems over $\mathbb{F}_2$ and reduced $\mathcal{C}_2 \times \mathcal{C}_2$-lattices.*

For a proof, see [7, pp. 200]. Rather than proving the bijection here, it will be illustrated how to construct a $\mathcal{C}_2 \times \mathcal{C}_2$-lattice from a 4-subspace system. Let L_i, $i = 1, \ldots, 4$ be the four non-isomorphic rank 1 $\mathbb{Z}G$-lattices. These are $\mathbb{Z}e_i$, where e_i are the 4 idempotents of $\mathbb{Z}G$, or equivalently 4 different copies of $\mathbb{Z}$ where g and h act as ± 1. If $\{V; V_i\}$ is a reduced 4-subspace system, then set $d_i = \dim V_i$, and define $H_i = L_i^{d_i}$. There is an exact sequence,

$$0 \longrightarrow 2H_i \longrightarrow H_i \xrightarrow{\sigma_i} V_i \longrightarrow 0, \tag{5.9}$$

where the map σ_i takes $(m_1, \ldots m_{d_i}) \in H_i$ to its canonical image in V_i. Setting $H = \bigoplus H_i$, σ_i can be extended to a map $\sigma : H \to V$, where $\sigma|_{H_i} = \sigma_i$. The reduced $\mathcal{C}_2 \times \mathcal{C}_2$-lattice associated to the 4-subspace system $\{V; V_i\}$ is defined as $M = \ker \sigma$.

Example 5.4.6. Take $V := \mathbb{F}_2^3$, $V_1 = \langle e_1 \rangle$, $V_2 = \langle e_2 \rangle$, $V_3 = \langle e_3 \rangle$ and $V_4 = \langle e_1 + e_2 + e_3 \rangle$. Then any choice of three of the V_i's span V. The kernel of the map $\bigoplus V_i \to V$ is $\langle (1, 1, 1, -1) \rangle$, in the basis vectors of the V_i. Set L_i as the rank 1 $\mathcal{C}_2 \times \mathcal{C}_2$-lattices where the following table shows the actions of the two generators g, $h \in \mathcal{C}_2 \times \mathcal{C}_2$.

	L_1	L_2	L_3	L_4
g	1	-1	1	-1
h	1	1	-1	-1

Set $H_i := L_i$, and $H = \bigoplus H_i$. Then $M \subset \mathbb{Z}^4$ is spanned by $(1, 1, 1, -1)$, and $2H$, so

a $\mathbb{Z}$-basis is

$$\begin{pmatrix} 1 & 1 & 1 & -1 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix},$$

where g acts by -1 on entries 2 and 4, h acts by -1 on entries 3 and 4, and gh acts by -1 on entries 2 and 3. Considering the action of g and h on this $\mathbb{Z}$-basis, the integral representation of $\mathcal{C}_2 \times \mathcal{C}_2$ is

$$\rho(g) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & -1 \end{pmatrix}, \ \rho(h) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ -1 & 0 & 0 & -1 \end{pmatrix}.$$

Applying Corollary 5.4.2, if G is an extension of $\mathcal{C}_2 \times \mathcal{C}_2$ by $\mathrm{Diag}(L)$, L a $\mathcal{C}_2 \times \mathcal{C}_2$-lattice, $\mathrm{ed}_k(G;2)$ (and therefore $\mathrm{ed}_k(G)$) is bounded below by $\mathrm{SymRank}(\phi_L;2) - \mathrm{rank}(L)$ and above by $\mathrm{SymRank}(\phi_L;2) - \mathrm{rank}(L) + 2$, using the dimension 2 faithful representation of $\mathcal{C}_2 \times \mathcal{C}_2$. If the subset generates rather than just 2-generates, this is an upper bound for $\mathrm{ed}_k(G)$, and if $\Lambda \subset L$ satisfies K_F, then $\mathrm{SymRank}(\phi_L;2) - \mathrm{rank}(L) = \mathrm{ed}_k(G;2) = \mathrm{ed}_k(G)$.

A list of the indecomposable 4-subspace systems. up to permutation of the $\{V_i\}$ can be found in [32, pp. 22]. This section will use the same notation found there. Different choices of which rank 1 lattice L_i is assigned to which subspace V_i gives non-isomorphic lattices, so each of the 9 types yields up to $\frac{1}{2}\binom{4}{2} = 3$ non-isomorphic lattices for a given rank. This family of these lattices with rank r associated to the

type T subspace system is denoted $L_{T,r}$.

In calculating the symmetric 2-ranks of these lattices, the algorithm featured in Section 4.0.1 will be utilised. An element of a reduced $\mathcal{C}_2 \times \mathcal{C}_2$-lattice L is written as a sublattice of $\bigoplus H_i$, so each element of $x \in L$ is partitioned into 4 blocks of length d_i $x = (\underline{x_1}, \underline{x_2}, \underline{x_3}, \underline{x_4})$, where an element of $\mathcal{C}_2 \times \mathcal{C}_2$ acts by -1 on two of these blocks. For instance, if g acts on the second and fourth blocks, it acts as the matrix $\mathrm{Id}_{d_1} \oplus -\mathrm{Id}_{d_2} \oplus \mathrm{Id}_{d_3} \oplus -\mathrm{Id}_{d_4}$ on x. The element $(g - e)$ thus acts by $\underline{0}_{d_1} \oplus -2\mathrm{Id}_{d_2} \oplus \underline{0}_{d_3} \oplus -2\mathrm{Id}_{d_4}$, and as the augmentation ideal $I = \langle g - e \rangle$, for $g \in G$, the elements in IL have the form $(0, 2\underline{x_2}, 2\underline{x_3}, 2\underline{x_4})$.

The method used to calculate $\mathrm{SymRank}(L; 2)$ is perhaps best illuminated by an example.

Example 5.4.7. Let V be a 2-dimensional vector space, with subspaces $V_1 = \langle e_1 \rangle$, $V_2 = \langle e_1 + e_2 \rangle$, $V_3 = V_4 = \langle e_2 \rangle$. This is an example of a reduced 4-subspace system, and the kernel of the map $\bigoplus V_i \to V$ is spanned by $e_1 - e_2 + e_3$ and $e_3 - e_4$. As in Example 5.4.6, identify the V_i with the rank 1 L_i, thus L is spanned by $(1, -1, 1, 0)$, $(0, 0, 1, -1)$ and the cyclic permutations of $(2, 0, 0, 0)$. The elements of $\mathcal{C}_2 \times \mathcal{C}_2$ act in the canonical way (g acts as -1 on the second and fourth coordinate and so on). A $\mathbb{Z}$-basis of this lattice is $\{(1, -1, 1, 0), (0, 0, 1, -1), (2, 0, 0, 0), (0, 2, 0, 0)\}$, which will be denoted as $\{e_i'\}$. It is claimed that $\overline{L} := L/2L + IL$ is generated by the images of e_1' and e_2'.

As $(g - \mathrm{id}) \cdot (1, -1, 1, 0) = (0, -2, 0, 0)$, and $(h - \mathrm{id}) \cdot (1, -1, 1, 0) = (0, 0, 2, 0)$, then the images of both e_4' and e_3' are 0 in $\overline{L}$. Now consider the point $x = (a_1, -a_1, a_1 + a_2, -a_2) \in \langle e_1', e_2' \rangle$. If $x \in IL$ then $a_1 = 0$, as G acts trivially on the first block. As e_2' contains entries not divisible by 2, it is not in IL either, so $\mathrm{rank}(\overline{L}) = 2$.

Finally, if x was fixed under any element of G,

$$g \cdot x = x \Rightarrow a_1 = a_2 = 0,$$

$$h \cdot x = x \Rightarrow a_1 + a_2 = a_2 = 0,$$

$$gh \cdot x = x \Rightarrow a_1 = a_1 + a_2 = 0.$$

So x is not fixed under any element of G. Therefore, in the language of Theorem 4.0.1, $\text{rank}(V_2) = 2$, $\text{rank}(V_i) = 0$ all other i, so $\text{SymRank}(L; 2) = (2 - 0) \cdot 2^2 = 8$. For an explicit generating invariant set, take the orbits of e_1 and e_2; each have size 4. In [32, p.22], subspace systems are represented by block matrices. This example is a "Type I" subspace system (with $n = 1$). The representation of this example is the following

V_1	V_2	V_3	V_4
1	1	0	0
0	1	1	1

The two rows represent the basis vectors e_1 and e_2 respectively, and the 4 columns, the description of the basis vectors of each V_i. A more detailed guide on interpreting the following tables can be found in Appendix A.

The steps to generalize this to any n are straightforward. The rows still represent the basis vectors e_1 – e_{2n}. The matrix $J_n^+(0)$ is the Jordan block of order n, with

eigenvalue 0. L is then spanned by

$$e_i - e_{n+i} + e_{2n+i},\ 1 \leq i \leq n$$

$$e_{2n+1} - e_{3n+1},$$

$$e_i + e_{2n+i+1} - e_{3n+i+1},\ 1 \leq i \leq n-1,$$

$$2e_i\ 1 \leq i \leq 4n.$$

The subspace system is

V_1	V_2	V_3	V_4
I_n	I_n	0	$J_n^+(0)$
0	I_n	I_n	I_n

Using the exact argument as before, the cyclic permutations of $(2, 0, \ldots, 0)$ lie in the augmentation ideal. A point that lies in the span of the other vectors can be written as $x = (a_1 + b_2, \ldots, a_n + b_{n-1}, a_1 + b_1, \ldots, a_n + b_m, -a_1, \ldots, -a_n, -b_1 - b_2, \ldots, -b_n)$, where a_i, $b_i \in \mathbb{Z}$. Taking each element of $\mathcal{C}_2 \times \mathcal{C}_2$ in turn,

$$g \cdot x = x \Rightarrow a_i + b_i = 0, -b_i - b_{i+1} = 0, b_n = 0,$$

$$h \cdot x = x \Rightarrow a_i = 0, -b_i - b_{i+1} = 0, b_n = 0,$$

$$gh \cdot x = x \Rightarrow a_i = 0, a_i + b_i = 0.$$

All of which mean $x = 0$, so $\mathrm{SymRank}(L; 2) = 8n$. As before, taking the orbits of this spanning set gives a generating invariant set.

L	$\mathrm{SymRank}(L, 2)$
$L_{0,2n}$	$8n$
$L_{\mathrm{I},2n}$	$8n - 2r,\ r = 0, 1, 2$
$L_{\mathrm{II},2n+1}$	$8n + 2r,\ r = 1, 2$
$L_{\mathrm{III},2n}$	$8n$
$L_{\mathrm{III}^*,2n+2}$	$8n + 2r + 4,\ r = 0, 1, 2$
$L_{\mathrm{IV},2n+1}$	$8n + 4$
$L_{\mathrm{IV}^*,2n+3}$	$8n + 2r + 6,\ r = 0, 2, 3$
$L_{\mathrm{V},2n-1}$	$8n - 2r - 2,\ r = 1, 2$
$L_{\mathrm{V}^*,2n+3}$	$8n + 4r + 2,\ r = 1, 2$

Table 5.2: Symmetric p-ranks of the reduced $\mathcal{C}_2 \times \mathcal{C}_2$-lattices.

Remark 5.4.8. The identification of the H_i lattices to the V_i subspaces (permutation of the columns of the subspace system) is crucial; a different choice gives non-isomorphic $\mathcal{C}_2 \times \mathcal{C}_2$-lattices, and therefore potentially different symmetric 2-ranks. The table of symmetric 2-ranks in 5.2 reflects this by the different values for each type, corresponding to different choices of $V_i \mapsto H_i$.

The values of the symmetric 2-rank of each lattice is given in Table 5.2 below, and the techniques used were identical to the example. A list of the indecomposable 4-subspaces systems can be found in Table A.2 (from [32]) in the appendix. The classification is complete upon adding $\mathrm{SymRank}(\mathrm{Diag}(\mathbb{Z}G), 2) = 4$, $\mathrm{SymRank}(\mathrm{Diag}(\mathbb{Z}), 2) = 1$ for the trivial lattice, and $\mathrm{SymRank}(\mathrm{Diag}(L_i), 2) = 2$ for the non-trivial rank 1 lattices.

Corollary 5.4.9. *For an algebraic group G over k, $\mathrm{char}(k) \neq 2$, satisfying (2.31) and where $F = \mathcal{C}_2 \times \mathcal{C}_2$, and $(G^\circ)^*$ containing no trivial rank 1 summands,*

$$\mathrm{ed}_k(G; 2) \leq 3 \cdot \dim\,(G) + 2. \tag{5.10}$$

Proof. Inspecting Table 5.2 shows that for all reduced lattices, $\mathrm{SymRank}(L;2) \leq 4 \cdot \mathrm{rank}(L)$. Together with $\mathrm{SymRank}(A_1;2) = 2$ for all the non-trivial rank 1 lattices, then

$$\begin{aligned}\mathrm{ed}_k(G;2) &\leq \mathrm{SymRank}(L;2) - \mathrm{rank}(L) + 2 \\ &\leq 4 \cdot \mathrm{rank}(L) - \mathrm{rank}(L) + 2 \\ &= 3 \cdot \mathrm{rank}(L) + 2.\end{aligned}$$

□

5.5 D_{2p}

Lastly our attention turns to the dihedral group D_{2p}, for p an odd prime. They have Sylow p-subgroups of $\mathcal{C}_2$ and $\mathcal{C}_p$, so have finite representation type, which is described in [21], which this section will be using. The essential p-dimension of extensions of D_{2p} by a torus has already been covered in Section 5.3 thanks to Proposition 5.1.3, as its Sylow p-subgroup is $\mathcal{C}_p$. However there is something more to say about the essential dimension. As D_{2p} is a subgroup of PGL_2, it acts faithfully on $\mathbb{P}^1$. Recall the definition of a versal variety from the discussion after Proposition 3.2.5.

Lemma 5.5.1. *Let G be an extension of an algebraic torus T by D_{2p} over a field k, $\mathrm{char}(k) \neq 2$ or p, and let V be a representation of G that is faithful on T. Then there exists a versal generically free G-variety of dimension* $\dim(V) + 1$.

Proof. Let W be the faithful 2 dimensional representation of D_{2p}. Proposition 3.5.2

says that $V \times W$ is a generically free representation of G. Now D_{2p} acts faithfully on $\mathbb{P}(W) = \mathbb{P}^1$, by virtue of D_{2p} being a subgroup of $PGL_2(k)$. As projectivisation is a G-compression, $V \times \mathbb{P}^1$ is a versal generically-free G-variety. $\square$

Table 5.3 contains the relevant information on the indecomposable D_{2p}-lattices. The description of each lattice L are from [21], can be found in Appendix B.2, along with all the calculations of $H^2(G; \mathrm{Diag}(L))$, and the symmetric rank $\mathrm{SymRank}(\phi)$, for $\phi : D_{2p} \to \mathrm{GL}(L)$.

L	$\mathrm{rank}(L)$	$H^2(G; \mathrm{Diag}(L))$	$\mathrm{ed}_k(G; p)$	$\mathrm{SymRank}(\phi_L)$	K_F
$\mathbb{Z}$	1	$\{1\}$	1	1	$\times$
$\mathbb{Z}_-$	1	$\mathbb{Z}/2\mathbb{Z}$	2	2	$\times$
N_+	$p-1$	$\{1\}$	2	p	$\times$
N_-	$p-1$	$\mathbb{Z}/p\mathbb{Z}$	2	$2p$	✓
M_+	p	$\{1\}$	1	p	$\times$
M_-	p	$\mathbb{Z}/2\mathbb{Z}$	1	$2p$	✓
$\widetilde{M}_+$	$p+1$	$\{1\}$	1	$p+3$	$\times$
$\widetilde{M}_-$	$p+1$	$\{1\}$	1	$2p$	✓

Table 5.3: Summary table for all indecomposable D_{2p}-lattices.

For a field k, $\mathrm{char}(k) \neq 2, p$, then bounds on $\mathrm{ed}_k(G)$ for $G \in \mathbf{Ext}_{D_{2p}}$ can be calculated by the information in Table 5.3. Firstly decompose the character lattice $L := T^*$, into indecomposable D_{2p}-lattices $L = \bigoplus L_i$. For a lower bound, $\mathrm{ed}_k(G; p) = \mathrm{ed}_k(G'; p)$, where G' is an extension of $\mathcal{C}_p$ by a split torus, so can be found using the results in Section 5.3. For an upper bound, note that for two lattices L, M, $\mathrm{SymRank}(\phi_L \oplus \phi_M) \leq$

$\mathrm{SymRank}(\phi_L) + \mathrm{SymRank}(\phi_M)$, so $\sum_i \mathrm{SymRank}(\phi_{L_i}) - \mathrm{rank}(L_i)$ is the dimension of a faithful representation, generically free if K_F is satisfied. If K_F is not satisfied, then Lemma 5.5.1 states the $\mathrm{ed}_k(G) \leq \mathrm{SymRank}(\phi_L) - \mathrm{rank}(L) + 1$.

As an illustration, take $L := \widetilde{M_+}$. It has trivial H^2 group ,so the only extension G is the semidirect product, $D_{2p} \rtimes \mathrm{Diag}(\widetilde{M_+})$. As a $\mathcal{C}_p$-lattice, it decomposes as $\mathbb{Z}\mathcal{C}_p \oplus \mathbb{Z}$, thus $\mathrm{SymRank}(\phi_{\widetilde{M_+}}) = \mathrm{rank}(\widetilde{M_+})$, so $\mathrm{ed}_k(G;p) = 1$. As $\mathrm{SymRank}(\phi_{\widetilde{M_+}}) = p+3$, but K_F isn't satisfied, there exists a generically free representation of G of dimension $p+3$, so $\mathrm{ed}_k(G) \leq (p+3) - (p+1) = 2$. Thus $1 \leq \mathrm{ed}_k(G) \leq 2$.

For each indecomposable D_{2p}-lattice L, the following is a list of the bounds of $\mathrm{ed}(G;p)$, for G an extension of D_{2p} by $\mathrm{Diag}(L)$.

L	$\mathrm{ed}(G)$
$\mathbb{Z}$	1
$\mathbb{Z}_-$	2
N_+	2
N_-	$2 - 2p + 1$

L	$\mathrm{ed}(G)$
M_+	1
M_-	$1 - p$
$\widetilde{M_+}$	$1 - 2$
$\widetilde{M_-}$	$1 - p - 1$

Table 5.4: Bounds on the essential dimension of extensions of $\mathrm{Diag}(L)$ by D_{2p}, where L is an indecomposable D_{2p} lattice.

Note that the difference in bounds are wildly different depending on the integral representation chosen. Each lattice comes in a "$\pm$" pair, for the "+" lattice the gap in the bounds is significantly smaller.

In particular, note this gives exact values of $\mathrm{ed}_k(G)$ for any G that is an extension of D_{2p} by $\mathrm{Diag}(L)$, where $L = \mathbb{Z}^{r_1} \oplus \mathbb{Z}_-^{r_2} \oplus (N_+)^{r_3} \oplus (M_+)^{r_4}$.

Appendix A

Reference Tables

G_i	Root system	$\mathrm{ed}_k(G_i;p)$			
		$p=2$	$p=3$	$p=5$	$p=7$
G_{23}	$\mathcal{H}_3$	3	1	1	0
G_{24}	$\mathcal{J}_3^{(4)}$	3	1	0	1
G_{25}	$\mathcal{L}_3$	2	3	0	0
G_{26}	$\mathcal{M}_3$	3	3	0	0
G_{27}	$\mathcal{J}_3^{(5)}$	3	3	1	0
G_{28}	$\mathcal{F}_4$	4	2	0	0
G_{29}	$\mathcal{N}_4$	4	1	1	0
G_{30}	$\mathcal{H}_4$	4	2	2	0
G_{31}	$\mathcal{O}_4$	4	2	1	0
G_{32}	$\mathcal{L}_4$	4	4	1	0
G_{33}	$\mathcal{K}_5$	5	3	1	0
G_{34}	$\mathcal{K}_6$	6	3	1	1
G_{35}	$\mathcal{E}_6$	5	3	1	0
G_{36}	$\mathcal{E}_7$	7	3	1	1
G_{37}	$\mathcal{E}_8$	8	4	2	1

Table A.1: $\mathrm{ed}_k(G_i;p)$ for each complex reflection group in Table 4.2, the first two columns of which are taken from [25].

Type	V_1	V_2	V_3	V_4
0	I_n	0	I_n	X
	0	I_n	I_n	I_n
I	I_n	I_n	0	$J_n^+(0)$
	0	I_n	I_n	I_n
II	I_{n+1}	I_{n+1}	$I_n^{\downarrow}$	0
	0	$I_n^{\leftarrow}$	I_n	I_n
III	I_{n+1}	0	$I_n^{\uparrow}$	$I_n^{\downarrow}$
	0	I_n	I_n	I_n
III*	I_n	0	$I_n^{\leftarrow}$	$I_n^{\rightarrow}$
	0	I_{n+1}	I_{n+1}	I_{n+1}

Type	V_1	V_2	V_3	V_4
IV	I_{n+1}	0	I_{n+1}	$I_n^{\uparrow}$
	0	I_{n+1}	I_{n+1}	$I_n^{\downarrow}$
IV*	I_{n+1}	0	I_{n+1}	$I_{n+1}^{\leftarrow}$
	0	I_{n+1}	I_{n+1}	$I_{n+1}^{\rightarrow}$
V	I_n	0	$J_n^+(0)$	I_n
	0	I_n	I_n	$J_n^+(0)$
	0	0	e_1	e_1
V*	$I_n^{\leftarrow}$	$I_n^{\leftarrow}$	$I_n^{\rightarrow}$	0
	0	$I_n^{\rightarrow}$	$I_n^{\leftarrow}$	$I_n^{\leftarrow}$
	e_1	e_1	e_1	e_1

Table A.2: The indecomposable 4 subspace systems, used to calculate the symmetric 2-ranks of the indecomposable reduced $\mathcal{C}_2 \times \mathcal{C}_2$-lattices.

Table A.2 shows the indecomposable 4 subspace systems. $J_n^+(0)$ is the Jordan block of order n with eigenvalue 0, e_i to the standard basis vector, the directional arrow in the I_n matrices refers to a zero column or row added to the matrix from that direction, e.g.

$$I_2^{\rightarrow} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

and finally

$$X = \begin{pmatrix} 1 & 0 & \dots & 0 & 1 \\ 0 & 1 & \dots & 0 & 1 \\ \vdots & & \ddots & & \vdots \\ 0 & & \dots & 1 & 1 \end{pmatrix}.$$

Appendix B

Calculations

B.1 $\mathcal{C}_{p^2}$-lattices

Throughout, W is the dimension 1 faithful representation of $\mathcal{C}_{p^2}$. Only the split case is considered, as the non-split case is dealt with by Proposition 5.3.1. K_F fails on every one as $\mathcal{H}$ acts trivially on the quotient N. A generating set in each case is simply the image of the standard permutation lattice P in $L = P/N$.

B.1.1 M_1

M_1 is the trivial lattice $\mathbb{Z}$, and $T := \mathrm{Diag}(\mathbb{Z}) = k^\times$, with trivial $\mathcal{G}$-action, so $T^{\mathcal{G}} = T$. As $\mathrm{Im}(N_{\mathcal{G}}(t^{\frac{1}{p^2}})) = t$, $H^2(\mathcal{G}; T) = \{1\}$. Clearly $\mathrm{SymRank}(\mathbb{Z}; p) = \mathrm{SymRank}(\mathbb{Z}) = 1$, so $V_\Lambda \times W$ is generically free and has dimension 2, so $1 \leq \mathrm{ed}_k(G; p) = \mathrm{ed}_k(G) \leq 2-1 = 1$.

B.1.2 M_2

$M_2 = \mathbb{Z}\mathcal{H}$, $T := \mathrm{Diag}(\mathbb{Z}\mathcal{H})$. Then $T^{\mathcal{G}} = (t, \ldots, t) = \mathrm{Im}(N_{\mathcal{G}}(t^{\frac{1}{p^2}}))$, so $H^2(\mathcal{G}; T) = \{1\}$. Then $\mathrm{SymRank}(\mathbb{Z}\mathcal{H}; p) = \mathrm{SymRank}(\mathbb{Z}\mathcal{H}) = \mathrm{rank}(\mathbb{Z}\mathcal{H})$, so from the same argument as the trivial module $\mathbb{Z}$, $\mathrm{ed}_k(G; p) = \mathrm{ed}_k(G) = 1$.

B.1.3 M_3

$M_3 = \mathbb{Z}\mathcal{H}/\delta_{\mathcal{H}} = A_{p-1}$. An element of $\mathrm{Diag}(M_3)$ has the form $(t_1, \ldots, t_{p-1}, t_1^{-1} \ldots t_{p-1}^{-1})$, so $t \in T^{\mathcal{G}}$ has $t_i = t_j = \zeta$, where ζ is a p^{th} root of unity. As $N_{\mathcal{G}}(t) = \prod_{i=1}^{p-1} t_i \cdot \prod_{i=1}^{p-1} {t_i}^{-1} = 1$, $H^2(\mathcal{G}; T) = \mathbb{Z}/p\mathbb{Z}$. $K_{\mathcal{G}}$ fails, as $\mathcal{G}$ acts trivially on $(1, \ldots, 1)$, but $\mathrm{ed}_k(G; p) = \mathrm{ed}_k(G) = 2$ (see discussion at the start of Section 5).

B.1.4 M_4

See B.1.2, the same arguments apply.

B.1.5 M_5

An element $(t_1, \ldots, t_{p^2})$ of $\mathrm{Diag}(M_5)$ is of the form has $\prod_0^{p^2} t_i = 1$, so $T^{\mathcal{G}} = \mu_{p^2}$. As $\mathrm{Im}(N_{\mathcal{G}}(T)) = 1$, then $H^2(\mathcal{G}; T) = \mathbb{Z}/p^2\mathbb{Z}$. M_5 is not a permutation lattice, so the image of the basis of $\mathbb{Z}\mathcal{G}$ is a generating invariant set, so $\mathrm{SymRank}(M_5) = p^2$. K_F is not satisfied, as $\mathcal{G}$ acts trivially on $\ker \phi = \langle (1, \ldots, 1) \rangle$, so $1 \leq \mathrm{ed}_k(\mathrm{Diag}(M_5) \rtimes \mathcal{C}_{p^2}) \leq 2$. M_5 decomposes as $(\mathbb{Z}\mathcal{H})^{p-1} \oplus A_{p-1}$ as a $\mathcal{H}$- lattice.

B.1.6 M_6

Elements of $\mathrm{Diag}(M_6)$ satisfy $\prod_i^{p^2} t_i \cdot t_{p^2+1}^p = 1$. $\mathrm{Diag}(T)^{\mathcal{G}} := (t, \ldots, t, t^{-p}) = N_{\mathcal{G}}((t^{\frac{1}{p^2}}, \ldots, t^{\frac{1}{p^2}}, t^{-\frac{1}{p}}))$, so $H^2(\mathcal{G}; T) = 1$. $\mathrm{SymRank}(M_6) = p^2+1$, and $\ker \phi = \langle \delta_{\mathcal{G}} - p \rangle$ which has trivial $\mathcal{G}$-action so K_F fails. As a $\mathcal{H}$-lattice decomposes as $\mathbb{Z} \oplus A_{p-1} \oplus \mathbb{Z}\mathcal{H}^{p-1}$.

B.1.7 M_7

The relations in $\mathrm{Diag}(M_7)$ are $\prod_i^p t_{pi+j} = 1$ for $1 \leq j \leq p$. So $T^{\mathcal{G}} = (t, \ldots t)$, where $t^p = 1$. As $\mathrm{Im}(N_{\mathcal{G}}(T)) = 1$, then $H^2(\mathcal{G}; T) = \mathbb{Z}/p\mathbb{Z}$. $\mathrm{SymRank}(M_7) = p^2$, so $\mathrm{ed}_k(G) \geq p$. As a $\mathcal{H}$-lattice, M_7 decomposes to A_{p-1}^p.

B.1.8 M_8

$\mathrm{Diag}(M_8)^{\mathcal{G}} = (t, \ldots, t) = \mathrm{Im}(N_{\mathcal{G}}(t^{\frac{1}{p^2}}, \ldots, t^{\frac{1}{p^2}})$, so $H^2(\mathcal{G}; \mathrm{Diag}(M_8)) = 1$.
$\mathrm{SymRank}(M_8) = p^2$, and M_8 decomposes as a $\mathcal{H}$-lattice as $A_{p-1}^{p-1} \oplus \mathbb{Z}\mathcal{H}$.

B.1.9 $M_{9,r}$

The points $t = (t_1, \ldots, t_{p^2}, s_1, \ldots, s_p)$ of $\mathrm{Diag}(M_{9,r})$ satisfy
$\prod_{i=1}^p t_{pi+j} = \prod_{k=1}^r s_{k+j}^{(-1)^{k-1}\binom{r}{k-1}}$, for $0 \leq j \leq p-1$. The fixed points of T under $\mathcal{G}$ have the form $(t, \ldots, t, s, \ldots, s)$, and as the alternating sum of binomial coefficients is 0, the relation forces $t^p = 1$. As $\prod_{i=1}^{p^2} t_i = \prod_{j=0}^{p-1} \prod_{k=1}^r s_{k+j}^{(-1)^{k-1}\binom{r}{k-1}} =$

$\prod_{j=1}^{p}\prod_{k=1}^{r} s_j^{\sum_{k=1}^{r}(-1)^{k-1}\binom{r}{k-1}} = 1$, then $N_{\mathcal{G}}(T) = (1,\ldots,1,s,\ldots,s)$, so $H^2(\mathcal{G};T) = \mathbb{Z}/p\mathbb{Z}$.

B.1.10 $M_{10,r}$

The points $(t,\ldots,t,s,\ldots,s) \in T := \mathrm{Diag}(M_{10,r})$ satisfy the condition $\prod_{i=0}^{p-1} t_{ip+j}t_{ip+j+1}^{-1} = \prod_{k=0}^{r+1} s_{k+j}^{(-1)^{k-1}\binom{r}{k-1}}$, $(0 \le j \le p-1)$ because substituting $t_i = t_j$ and $s_i = s_j$ yields 1 on both sides of the equation (alternating sum of binomial coefficients on the right hand side, and $t_{ip+j}t_{ip+j+1}^{-1} = 1$). So the $\mathcal{G}$ fixed points of $T := \mathrm{Diag}(M_{10,r})$ are of the form $(t,\ldots,t,s,\ldots,s)$, however this the image of $(t^{\frac{1}{p^2}},\ldots,t^{\frac{1}{p^2}},s^{\frac{1}{p^2}},\ldots,s^{\frac{1}{p^2}})$ under $N_{\mathcal{G}}$, so $H^2(\mathcal{G};T) = \{1\}$.

B.1.11 $M_{11,r}$

The conditions on $T := \mathrm{Diag}(M_{11,r})$ are $\prod_{i=0}^{p-1} t_{pi+j} = \prod_{k=0}^{r} s_{k+j}^{(-1)^k\binom{r}{k}}$ $(0 \le j \le p-1)$, and $\prod_{i=0}^{p-1} s_i = 1$. For a point $(t,\ldots,t,s,\ldots,s) \in T^{\mathcal{G}}$, the second condition forces $s^p = 1$, and the first forces $\prod_{i=0}^{p-1} t_{pi+j} = 1$, so $t^p = 1$, so $T^{\mathcal{G}} = (\zeta_1,\ldots,\zeta_1,\zeta_2,\ldots,\zeta_2)$, where the ζ_i are p-th roots of unity. As $\mathrm{Im}(N_{\mathcal{G}}(T)) = 1$, then $H^2(\mathcal{G};T) = (\mathbb{Z}/p\mathbb{Z})^2$.

B.1.12 $M_{12,r}$

The conditions on $T := \mathrm{Diag}(M_{12,r})$ are $\prod_{i=0}^{p-1} t_{pi+j}t_{pi+j+1}^{-1} = \prod_{k=0}^{r+1} s_{k+j}^{(-1)^k\binom{r+1}{k}}$ $(0 \le j \le p-1)$, and $\prod_{i=0}^{p-1} s_i = 1$. For a point $(t,\ldots,t,s,\ldots,s) \in T^{\mathcal{G}}$, the second condition forces $s^p = 1$, but the first is consistent with the conditions $t_i = t_j$, so

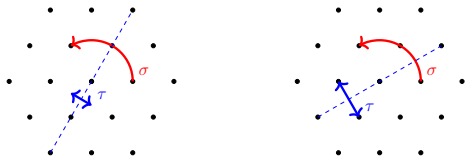


Figure B.1: N_+ and N_- symmetry when $p = 3$.

$T^{\mathcal{G}} = (t, \dots, t, \zeta, \dots, \zeta)$, where ζ is a p-th roots of unity.

As $\mathrm{Im}(N_{\mathcal{G}}(t^{\frac{1}{p^2}}, \dots, t^{\frac{1}{p^2}}, s_1, \dots, s_p)) = (t, \dots, t, 1, \dots, 1)$, then $H^2(\mathcal{G}; T) = \mathbb{Z}/p\mathbb{Z}$.

B.2 D_{2p}-lattices

$H^2(D_{2p}; T)$ can be calculated using the same technique for cyclic groups.

B.2.1 $N_\pm$

These are both lattices of rank $p-1$, that are symmetries of the A_{p-1} root lattice.

N_+ is generated by the following two matrices

$$\rho_1(\sigma) = A := \begin{pmatrix} 0 & & & -1 \\ 1 & & & -1 \\ & \ddots & & -1 \\ & & 1 & -1 \end{pmatrix}, \quad \rho_1(\tau) = B := \begin{pmatrix} & & & 1 \\ & & \iddots & \\ & 1 & & \\ 1 & & & \end{pmatrix},$$

where N_- is generated by A and $-B$.

Example B.2.1. When $p = 3$, $N_\pm$ are the following automorphisms of A_2.

As neither lattice are permutation, $\mathrm{SymRank}(N_\pm) > p-1$. For N_+, an orbit of size p generates, as the standard basis vectors $\{e_i\}$ are contained in the orbit of e_1 so $\mathrm{SymRank}(N_+) = p$. For N_-, note that for $\sum_i \sigma^i x = 0$ for any $x \in N_-$, so $\{\sigma_i x\}_i$ generates a lattice of rank at most $p-1$. Also, any $x \in \mathrm{Fix}(\tau)$ has the form $(a_1, \dots a_{\frac{p-1}{2}}, -a_{\frac{p-1}{2}}, \dots, a_1)$, and for each $\sigma^i x$, the sum of the coordinates is either 0 or a multiple of p, so modulo p, $\{\sigma^i x\}$ does not generate a rank $p-1$ lattice. So $\mathrm{SymRank}(N_-) \geq 2p$. Again, taking the orbit of e_1 gives a generating set of size $2p$. A simple calculation also shows $H^2(F; \mathrm{Diag}(N_+)) = 1$, $H^2(F; \mathrm{Diag}(N_-)) = \mathbb{Z}/p\mathbb{Z}$. The representation of dimension p of $F \rtimes \mathrm{Diag}(N_+)$ is not generically free, using the same argument in M_3 in Section 5.3. So using Lemma 5.5.1, there exists a generically free G-variety of dimension $p+1$, which is the true value as $H := \mathcal{C}_p \rtimes \mathrm{Diag}(A_{p-1}) \leqslant G$, where $\mathrm{ed}_k(H) = 2$ and $\dim(H) = \dim(G)$, so by Proposition 3.2.8 and the previous discussion, $\mathrm{ed}_k(G) = 2$. For N_-, K_F is satisfied, as F acts faithfully on $e_1 + (-e_1)$. Also, T acts faithfully on $\mathbb{P}(V)$, as the equations $\chi(t) = \chi'(t)$ for all χ, $\chi' \in T^*$ imply $t_i^p = t_i^2 = 1$ for all i, so there exists a generically free G- variety of dimension $2p-1$.

B.2.2 $M_{\pm}$

These have rank p, and arise as symmetries of the I_p root lattice. M_+ is generated by the following two matrices

$$\rho_2(\sigma) = A := \begin{pmatrix} 0 & & & 1 \\ 1 & & & 0 \\ & \ddots & & \vdots \\ & & 1 & 0 \end{pmatrix}, \ \rho_2(\tau) = B := \left(\begin{array}{ccc|c} & & 1 & 0 \\ & \iddots & & \vdots \\ 1 & & & 0 \\ \hline 0 & \dots & 0 & 1 \end{array}\right),$$

where M_- is generated by A and $-B$. Clearly, M_+ is a permutation lattice. Any point $l \in M_-$ fixed under $-B$ has that its coordinates sum to 0, so $\sum_{f\in F} f \cdot x = 0$ and thus its orbit generates a sublattice of rank less than p. Also, $\mathrm{Fix}\sigma = \langle(1, \dots, 1)\rangle$, so any τ-fixed point lies in the sublattice generated by $\{f \cdot x\}$ when taken modulo p. Thus any combination of this fixed points fails to generate M_-. As before, the orbit of e_1 of size $2p$, generates the lattice, so $\mathrm{SymRank}(M_-) = 2p$.

Any element in $\mathrm{Diag}(M_+)^F := (t, \dots, t)$ is the image of $(t^{\frac{1}{p}}, \dots)$ under the map N_F, so H^2 is trivial. For M_-, $\mathrm{Im}(N_F)$ is trivial, and $\mathrm{Diag}(M_+)^F = \pm(1, \dots, 1)$, so $H^2 = \mathbb{Z}/2\mathbb{Z}$.

Finally, as M_+ is permutation, $\mathrm{ed}_k(G) = 1$, and for M_-, F acts faithfully on $e_1 + (-e_1)$, so the representation of dimension $2p$ is generically free. Note that $\mathrm{diag}(-1, \dots, -1)$ acts trivially on $\mathbb{P}(V)$.

B.2.3 $\widetilde{M_{\pm}}$

These have rank $p+1$, $\widetilde{M_+}$ being generated by the following two matrices

$$\rho_3(\sigma) = A := \left(\begin{array}{cccc|c} 0 & & & 1 & 0 \\ 1 & & & 0 & 0 \\ & \ddots & & \vdots & \vdots \\ & & 1 & & 0 \\ \hline 0 & \dots & 0 & 0 & 1 \end{array}\right), \quad \rho_3(\tau) = B := \left(\begin{array}{cccc|c} & & 1 & & 1 \\ & \iddots & & & \vdots \\ 1 & & & & 1 \\ & & & 1 & 1 \\ \hline 0 & \dots & 0 & 0 & -1 \end{array}\right),$$

and $\widetilde{M_-}$ is generated by A and $-B$. Both are found in the D^*_{p+1} lattice.

Proposition B.2.2. [21, Thm. 3.4] $\widetilde{M_+} \oplus \mathbb{Z} \simeq \mathbb{Z}[G/\langle\sigma\rangle] \oplus \mathbb{Z}[G/\langle\tau\rangle]$

This means $\widetilde{M_+}$ is a stably permutation lattice, and $\mathrm{SymRank}(\widetilde{M_+}) = p+2$. For $\widetilde{M_-}$, note that $\mathrm{Fix}(\tau)$ has rank $\frac{p-1}{2}+1$, and $\mathrm{Fix}(\sigma)$ has rank 2, so $\mathrm{Fix}(\tau)\cup\mathrm{Fix}(\sigma)$ cannot generate a full rank sublattice if $p > 3$. If $p = 3$, then $\mathrm{Fix}(\tau)\cup\mathrm{Fix}(\sigma) = \langle e_1 - e_2, -2e_1 - e_3 + 2e_4, e_1 + e_2 + e_3, e_4\rangle$, which doesn't contain e_2. Therefore $\mathrm{SymRank}(\widetilde{M_-}) \geq 2p$, which is achieved by the size $2p$ orbit of $x := \sum_{i=\frac{p+1}{2}}^{p} e_i - e_{p+1}$. To see this, note that $x - \tau x = e_{\frac{p+1}{2}}$, so $e_i = \sigma^j(x - \tau x)$ for $i \in [1, \dots, p]$, given a suitable choice of j, and finally from the definition of x, $e_{p+1} = -x + \sum_{i=\frac{p+1}{2}}^{p} e_i$.

H^2 is trivial for both. For $\widetilde{M_+}$, $\mathrm{Diag}(\widetilde{M_+})^F = (t, \dots, t, 1) = \mathrm{Im}N_F(t^{\frac{1}{2}}, 1, \dots, 1)$. In the case of $\widetilde{M_-}$, $\mathrm{Diag}(\widetilde{M_-})^F = (t, \dots, t, t^{-2}) = \mathrm{Im}N_F(1, \dots, 1, t^{-\frac{1}{p}})$.

The representation of size $p+2$ given by the invariant generating set of $\widetilde{M_+}$ is not generically free, Proposition 3.5.2 tells us there exists a generically free representation of dimension $p+3$. When $p = 3$, T acts faithfully on $\mathbb{P}(V)$, so there exists a versal

generically free G-variety of dimension $p+2$, though this isn't the case for $p > 3$, as $\mathrm{diag}(\zeta, \ldots, \zeta)$ acts trivially on $\mathbb{P}(V)$, where ζ is a $(p-2)^{\text{th}}$ root of unity. For $\widetilde{M_-}$, the condition K_F is satisfied, as F acts faithfully on (for instance) $\sum_{i=\frac{p+1}{2}}^{p-1} \sigma^i(x - \tau x) - \tau x$. Thus there exists a generically free representation of size $2p$. Lastly, as the element $\mathrm{diag}(1, \ldots, 1, t) \in T$ acts trivially on $\mathbb{P}(V)$, $2p$ is the best lower bound known.

Appendix C

Code

C.1 Magma

C.1.1 Merkurjev's algorithm

```
SeqVkranks:= function(L,p) #Outputs the ranks of the V_k's as a
 sequence of integers.
 G:=AutomorphismGroup(L);
 H:=SylowSubgroup(G,p);
 k:=Divisors(Order(H));
 Seq:=[];
  for r in k do
   h:= [Matrix(g) - Matrix(Identity(H)) : g in Generators(H)];
   #Generators  of the augmentation ideal.
```

```
P:=p*Matrix(Identity(H)); #Generates the pL.
Q,f:=quo<L|h,P>; #Quotient module L/(p+I)L.
M:=&cat[[k: k in Conjugates(H,K)]: K in LowIndexSubgroups(H,r)];
#Gives a list of subgroups upto index r by calling the list of
conjugacy reps, and taking all the conjugate subgroups.
C:= [];
 for m in M do #For all groups of index less than r
 A:= Nullspace(Matrix(Identity(H))-Matrix(Identity(H))); #A is the
 fixed spaces of a particular group.
  for g in Generators(m) do
  A:= Nullspace(Identity(H)-Matrix(g)) meet A; #Recursively find
  the intersection of all fixed spaces of all elements.
  end for;
 n:=Rank(A);
  if n ne 0 then
   for i in [1..Rank(A)] do;
   C:=Append(C,Matrix(A.i));
   end for;
  end if;
 end for;
if C ne [] then
 Sublattice:=sub<L | Matrix(C)>;
 SublatticeRank:=Rank(Sublattice);
 Images:=[];
  for l in [1..SublatticeRank] do
  Images:= Append(Images,f(Sublattice.l));
```

```
     end for;
    Qsub:= sub<Q|Images>;
    Seq:=Append(Seq, #Generators(Qsub)); #Adds the number of
    distinct images to the list Seq.
    else Seq:=Append(Seq,0);
    end if;
   end for;
 return Seq;
end function;

Summation:=function(Seq,p) #Function that takes the sequence outputted
in SeqVkranks and calculates the sum (rank V_k- rankV_{k-1})*p^k.
 n:=#Seq;
 Sum:=p^(n-1)*Seq[n];
 for i in [1..n-1] do
  Sum:= Sum + (p^(i-2)-p^(i-1))*Seq[i];
 end for;
 return Sum;
end function;

SympRank:=function(L) #Outputs the symmetric p ranks for all primes
dividing the order of the aut group.
G:=AutomorphismGroup(L);
rank:=Rank(L);
n:=Order(G);
for p in PrimeDivisors(n) do
```

```
 Seq:=SeqVkranks(L,p);
 print "Symmetric ", p, " rank is ", Summation(Seq,p);
 end for;
return 0;
end function;
```

C.2 GAP

C.2.1 Functions for symmetric p-rank

The following function calculates the fixed points of the integral matrix group G.

```
fixed_points := function(G)
 local gens, nullspaces, fixedpoints, i;
 gens:= GeneratorsOfGroup(G);
 nullspaces:= List(gens, g->NullspaceIntMat(g-
 IdentityMat(DimensionOfMatrixGroup(G),Rationals)));
 fixedpoints:=nullspaces[1];
  if Size(nullspaces) > 1 then
   for i in [1..Size(nullspaces)] do
    fixedpoints:=BaseIntersectionIntMats(fixedpoints,
    nullspaces[i]); od; fi;
 return(fixedpoints);
end;
```

This function outputs the determinant of the Smith Normal Form of an integral

matrix. If $\{v\} \in \mathbb{Z}^n$ form the rows of this matrix, then it is the index of the sublattice generated by $\{v\}$ in $\mathbb{Z}^n$.

```
SNFdet:=function(v)
 local n;
  if Size(v)=0
  then return 0; fi;
 n:=Size(v[1]);
  if Size(v)<n
  then return 0; fi;
 return Determinant(SmithNormalFormIntegerMat(v){[1..n]});
end;
```

A function that returns the value 1 if n is prime to p.

```
index := function(n,p)
if n=0 then return 0;
fi;
if GcdInt(n,p)=1 then return 1;
else return 0;
fi;
end;
```

Given a set of $\{v\}$, $v \in \mathbb{Z}^n$, this function outputs the smallest invariant p-generating sets amongst all orbits of the elements in $\{v\}$.

```
p_generating_set := function(G,p,V) #function to calculate the minimum
```

```
 p-generating invariant set of the orbits of a subset V of the lattice.
 local i, sylow_subgroup, orbit, orbit_collection, index_of_sublattices,
 p_1, p_2;
 sylow_subgroup:=SylowSubgroup(G,p);
 orbit:=Orbit(sylow_subgroup,V[1],OnPoints);
 orbit_collection:=List([O]); #List of orbits of points in V
 for i in [1..Size(V)] do
  if V[i] in O then
   orbit := orbit;
  else
   orbit:=Union(orbit,Orbit(sylow_subgroup,V[i],OnPoints));
   Add(orbit_collection,Orbit(sylow_subgroup,V[i],OnPoints));fi;od;
 orbit_collection:=Combinations(orbit_collection);
 orbit_collection:=orbit_collection{[2..Size(orbit_collection)]};
 index_of_sublattices:=List(orbit_collection,o->index(SNFdet(Union(o)),p));
 p_1:=Positions(M,1); #All invariant subsets that p-generate.
 orbit_collection:=orbit_collection{p_1};
 orbit_collection:=List(orbit_collection,o->Size(Union(o)));
 p_2:=Positions(index_of_sublattices,Minimum(index_of_sublattices));
 orbit_collection:=orbit_collection{p_2};
return(orbit_collection[1]);
end;
```

For a subset $\Delta \subset \mathbb{Z}^n$ and integral matrix group $G < \mathrm{GL}_n(\mathbb{Z})$, this function returns 1 if G acts faithfully on the kernel $\mathbb{Z}[\Delta] \to \mathbb{Z}^n$, known as condition K_F.

```
Kernel_faithful:=function(G,V)  #returns 1 if condition K_F
is satisfied for the action of G on the subset V
local i, dim, linear_rels, is_faithful, linear_rel, List_V,
g_action, elements, sols;
dim:=DimensionOfMatrixGroup(G);
linear_rels:=[];
for i in [1..Size(V)] do
 List_V:=List(V);
 Remove(List_V,i);
 sols:=SolutionIntMat(List_V,V[i]); #Linear relations in the set.
  if sols = fail then
  linear_rels:=linear_rels;
 else
  Add(sols,-1,i);   #Each element ker(phi) in the original basis.
  Add(linear_rels,sols);fi;od;
  linear_rels:=BaseIntMat(linear_rels); #Span(ker(phi))
  in original basis.
  g_action:=[];
  elements:=List(Elements(G));
  for i in [1..Size(elements)] do
   Add(g_action,PermListList(V,V*elements[i]));od; #G action on ker(phi).
   g_action:=List(g_action,l->List(linear_rels,m->Permuted(m,l)));
   #Orbit of ker(phi) under G.
  linear_rels:=DuplicateFreeList(linear_rels);
  if Size(linear_rels)=Size(G) then  #If true then action is faithful.
   is_faithful:=true;
```

```
  else
   is_faithful:=false;fi;
 return(is_faithful);  # Returns whether action is faithful or not.
end;
```

C.2.2 Verification calculations

This section contains the GAP code necessary to calculate the symmetric p-ranks in Section 4.3.

$W(\mathcal{J}_3^{(4)})$

A description of the automorphism group of the lattice $Q_6(1)$, see the description in 4.3.2. The calculation below shows the Sylow 7-subgroup fixes no non-trivial points in the lattice.

```
gap> DisplayImfInvariants(6,5,1);
#I Z-class 6.5.1:  Size = 2^5*3*7
#I   isomorphism type = C2 x PGL(2,7)
#I   elementary divisors = 1^3*7^3
#I   orbit size = 42, minimal norm = 4

gap> G:=ImfMatrixGroup(6,5,1);;
gap> sylow7sbgp:=SylowSubgroup(G,7);;
gap> fixed_points(sylow7sbgp);
[ ]
```

```
gap> Id_6:=IdentityMat(6,Rationals);;
gap> 7genset:=Orbit(sylow7sbgp,Id_6[1],OnPoints);;
gap> Size(7genset);SNFdet(7genset);
7
1
```

$W(\mathcal{J}_3^{(5)})$

The description of the rank 12 lattice $\Lambda_{\text{real}}(\mathcal{J}_3^{(5)})$, described in 4.3.4. The algorithm in C.1.1 is implemented to find the symmetric p-ranks of the automorphism group.

```
L:=Lattice(D, 12, 2);
LatticeName(D,12,2);
SympRank(L);

(C2 x C3.Alt6).(C2 x C2).d12 12
Symmetric  2  rank is  32
Symmetric  3  rank is  54
Symmetric  5  rank is  12
0
```

$W(\mathcal{H}_4)$

The following contains a description of the lattice $Q_8(1) = \Lambda_{\text{real}}(\mathcal{H}_4)$ (see 4.3.5), along with examples of a 2- and 3-generating set.

```
gap> DisplayImfInvariants(8,7,1);
#I Z-class 8.7.1:  Size = 2^7*3^2*5^2
#I   isomorphism type = (SL(2,5) Y SL(2,5)):(C2 x C2)
#I   elementary divisors = 1^4*5^4
#I   orbit size = 120, minimal norm = 4

gap> G:=ImfMatrixGroup(8,7,1);;
gap> sylow2sbgp:=SylowSubgroup(G,2);;
gap> Id_8:=IdentityMat(8,Rationals);;
gap> 2genset:=Orbit(sylow2sbgp,Id_8[1],OnPoints);;
gap> Size(2genset);SNFdet(2genset);
64
1

gap> sylow3sbgp:=SylowSubgroup(G,3);;
gap> orbit_1:=Orbit(sylow3sbgp,Id_8[5],OnPoints);;
gap> orbit_2:=Orbit(sylow3sbgp,Id_8[7],OnPoints);;
gap> 3genset:=Union(orbit_1,orbit_2);;
gap> Size(3genset);SNFdet(3genset);
18
1
```

$W(\mathcal{O}_4)$

Showing that every group isomorphic to $\mathcal{C}_5$ in $W(E_8)$ has symmetric 5-rank of 10 or lower, by finding invariant 5-generating sets, as described in Proposition 4.3.28.

```
gap> DisplayImfInvariants(8,3,1);
#I Z-class 8.3.1:  Size = 2^14*3^5*5^2*7
#I   isomorphism type = W(E8)
#I   elementary divisors = 1^8
#I   orbit size = 240, minimal norm = 2
gap> G:=ImfMatrixGroup(8,3,1);;
gap> sylow5sbgp:=SylowSubgroup(G,5);;
gap> J:=ConjugacyClassesSubgroups(sylow5sbgp);;
gap> List_of_gen_sets:=List(J,j->Size(Union(p_generating_set(j[1],5, Union
(W,fixed_points(j[1])))))); #for each group finds a small 5-generating set
#These give invariant 5-generating sets
[ 8, 8, 10, 10, 10, 10, 8, 25 ]
```

Note the last set of size 25 is that of the Sylow 5-subgroup of $W(E_8)$, which is $\mathcal{C}_5 \times \mathcal{C}_5$.

$W(\mathcal{K}_5)$

The next two sections contain the descriptions in GAP of the lattices $\Lambda_{\text{real}}(\mathcal{K}_5)$ and $\Lambda_{\text{real}}(\mathcal{K}_6) = K_{12}$ (see Section 4.3.8). An example of a p-generating set of minimal size is also given, for $p = 2$, 3, 5 and 7. These conclude the proofs of Propositions 4.3.33, 4.3.31, 4.3.34 and 4.3.35 respectively.

```
gap> DisplayImfInvariants(10,4,1);
#I Z-class 10.4.1:  Size = 2^8*3^5*5
#I   isomorphism type = (C6 x SU(4,2)):C2
#I   elementary divisors = 1^5*3^3*6^2
```

```
#I   orbit size = 270, minimal norm = 4

gap> sylow2sbgp:=SylowSubgroup(G,2);;
gap> 2genset:=Orbit(sylow2sbgp,W[1],OnPoints);;
gap> Size(2genset);SNFdet(2genset);
128
1



gap> G:=ImfMatrixGroup(10,4,1);;
gap> sylow3sbgp:=SylowSubgroup(G,3);;
gap> Id_10:=IdentityMat(10,Rationals);;
gap> 3genset:=Orbit(sylow3sbgp,Id_10[3],OnPoints);;
gap> Size(3genset);SNFdet(3genset);
81
1

gap> sylow5sbgp:=SylowSubgroup(G,5);;
gap> orbit_1:=Orbit(sylow5sbgp,Id_10[9],OnPoints);;
gap> orbit_2:=Orbit(sylow5sbgp,Id_10[10],OnPoints);;
gap> 5genset:=Union(orbit_1,orbit_2);;
gap> Size(5genset);SNFdet(5genset);
10
1
```

$W(\mathcal{K}_6)$

```
gap> DisplayImfInvariants(12,5);
#I Q-class 12.5:  Size = 2^10*3^7*5*7
#I   isomorphism type = C6.PSU(4,3).(C2 x C2)
#I   elementary divisors = 1^6*3^6
#I   orbit size = 756, minimal norm = 4

gap> G:=ImfMatrixGroup(12,5);;
gap> sylow2sbgp:=SylowSubgroup(G,2);;
gap> Id_12:=IdentityMat(12,Rationals);;
gap> 2genset:=Orbit(sylow2sbgp,Id_12[6],OnPoints);;
gap> Size(2genset);SNFdet(2genset);
128
1

gap> sylow3sbgp:=SylowSubgroup(G,3);;
gap> 3genset:=Orbit(sylow3sbgp,Id_12[1],OnPoints);;
gap> Size(3genset);SNFdet(3genset);
243
1

gap> sylow5sbgp:=SylowSubgroup(G,5);;
gap> fixedpoints:=fixed_points(sylow5sbgp){[1,2]};;
gap> orbit_1:=Orbit(sylow5sbgp,Id_12[1],OnPoints);;
gap> orbit_2:=Orbit(sylow5sbgp,Id_12[12],OnPoints);;
```

```
gap> 5genset:=Union(fixedpoints,Union(orbit_1,orbit_2));;
gap> Size(5genset);SNFdet(5genset);
12
3

gap> sylow7sbgp:=SylowSubgroup(G,7);;
gap> orbit_1:=Orbit(sylow7sbgp,Id_12[1],OnPoints);;
gap> orbit_2:=Orbit(sylow7sbgp,Id_12[3],OnPoints);;
gap> 7genset:=Union(orbit_1,orbit_2);;
gap> Size(7genset);SNFdet(7genset);
14
1
```

Bibliography

[1] Grégory Berhuy and Giordano Favi. Essential dimension: a functorial point of view (after A. Merkurjev). *Doc. Math*, 8:279–330, 2003.

[2] Michel Brion. On extensions of algebraic groups with finite quotient. *Pacific Journal of Mathematics*, 279(1):135–153, 2015.

[3] Michel Broué, Gunter Malle, and Jean Michel. Towards spetses i. *Transformation groups*, 4(2-3):157–218, 1999.

[4] Michel Broué, Gunter Malle, and Raphaël Rouquier. Complex reflection groups, braid groups, hecke algebras. 1997.

[5] Kenneth S Brown. *Cohomology of groups*, volume 87. Springer-Verlag New York, 2012.

[6] Joe Buhler and Zinovy Reichstein. On the essential dimension of a finite group. *Compositio Mathematica*, 106(2):159–179, 1997.

[7] MCR Butler. The 2-adic representations of klein's four group. In *Proceedings of the Second International Conference on the Theory of Groups*, pages 197–203. Springer, 1974.

[8] John H Conway and Neil J A Sloane. *Sphere packings, lattices and groups*, volume 290. Springer-Verlag New York, 1999.

[9] John H Conway and Neil JA Sloane. The Coxeter–Todd lattice, the Mitchell group, and related sphere packings. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 93, pages 421–440. Cambridge University Press, 1983.

[10] John H Conway and NJA Sloane. Low-dimensional lattices. I. quadratic forms of small determinant. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 418(1854):17–41, 1988.

[11] John H Conway and NJA Sloane. Low-dimensional lattices. II. subgroups of $\mathrm{GL}(n, \mathbf{Z})$. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 419(1856):29–68, 1988.

[12] Charles W Curtis and Irving Reiner. *Methods of Representation Theory: With Applications to Finite Groups and Orders. Vol. I.* Wiley-Interscience, 1990.

[13] Michel Demazure and Alexander Grothendieck. *Schémas en groupes (SGA3)*. Séminaire de Géométrie Algébrique du l'Institut Bois Marie. Springer-Verlag, New York, 1970; Documents mathématiques 7, 8, Soc. Math. France, Paris, 2011.

[14] David S Dummit and Richard M Foote. *Abstract algebra*, volume 3. Wiley Hoboken, 2004.

[15] Alexander Duncan and Zinovy Reichstein. Pseudo-reflection groups and essential dimension. *Journal of the London Mathematical Society*, 90(3):879–902, 2014.

[16] Lei Fu. *Étale cohomology theory*, volume 13. World Scientific, 2011.

[17] Peter Gabriel. Unzerlegbare darstellungen I. *Manuscripta mathematica*, 6(1):71–103, 1972.

[18] Skip Garibaldi and Robert M Guralnick. Essential dimension of algebraic groups, including bad characteristic. *Archiv der Mathematik*, 107(2):101–119, 2016.

[19] Skip Garibaldi, Alexander S Merkurjev, and Jean-Pierre Serre. *Cohomological invariants in Galois cohomology*. Number 28. American Mathematical Soc., 2003.

[20] Robin Hartshorne. *Algebraic geometry*, volume 52. Springer-Verlag New York, 1977.

[21] Akinari Hoshi, Ming-chang Kang, and Aiichi Yamasaki. Class numbers and algebraic tori. *arXiv preprint arXiv:1312.6738*, 2013.

[22] Alfredo Jones. Groups with a finite number of indecomposable integral representations. *The Michigan Mathematical Journal*, 10(3):257–261, 1963.

[23] Camille Jordan. Mémoire sur l'équivalence des formes. *J. Ecole Polytech*, 48:112–150, 1880.

[24] Nikita A Karpenko and Alexander S Merkurjev. Essential dimension of finite p-groups. *Inventiones mathematicae*, 172(3):491–508, 2008.

[25] Gustav I Lehrer and Donald E Taylor. *Unitary reflection groups*, volume 20. Cambridge University Press, 2009.

[26] Martin Lorenz. *Multiplicative invariant theory*, volume 135. Springer-Verlag Berlin Heidelber, 2006.

[27] R. Lötscher, M. MacDonald, A. Meyer, and Z. Reichstein. Essential p-dimension of algebraic tori. *ArXiv e-prints*, October 2009.

[28] Roland Lötscher, Mark MacDonald, Aurel Meyer, and Zinovy Reichstein. Essential dimension of algebraic tori. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 2013(677):1–13, 2013.

[29] Roland Lötscher, Mark MacDonald, Aurel Meyer, and Zinovy Reichstein. Essential p-dimension of algebraic groups whose connected component is a torus. *Algebra & Number Theory*, 7(8):1817–1840, 2013.

[30] Mark L MacDonald. Essential p-dimension of the normalizer of a maximal torus. *Transformation Groups*, 16(4):1143–1171, 2011.

[31] Saunders MacLane. *Categories for the working mathematician*, volume 5. Springer-Verlag New York, 2013.

[32] Gonzalo Medina and Alexander Zavadskij. The four subspace problem: An elementary solution. *Linear algebra and its applications*, 392:11–23, 2004.

[33] Alexander S Merkurjev. A lower bound on the essential dimension of simple algebras. *Algebra & Number Theory*, 4(8):1055–1076, 2011.

[34] Alexander S Merkurjev. Essential dimension: a survey. *Transformation groups*, 18(2):415–481, 2013.

[35] Aurel Meyer and Zinovy Reichstein. The essential dimension of the normalizer of a maximal torus in the projective linear group. *Algebra & Number Theory*, 3(4):467–487, 2009.

[36] James S Milne. Algebraic geometry, 2016.

[37] James S Milne. *Algebraic groups: The theory of group schemes of finite type over a field*, volume 170. Cambridge University Press, 2017.

[38] Lyudmila Aleksandrovna Nazarova. Representation of a tetrad. *Mathematics of the USSR-Izvestiya*, 1(6):1305–1321, 1967.

[39] Gabriele Nebe and Wilhelm Plesken. *Finite rational matrix groups*, volume 556. American Mathematical Soc., 1995.

[40] Zinovy Reichstein. On the notion of essential dimension for algebraic groups. *Transformation Groups*, 5(3):265–304, 2000.

[41] Maxwell Rosenlicht. Some basic theorems on algebraic groups. *American Journal of Mathematics*, 78(2):401–443, 1956.

[42] Ralf Schiffler. *Quiver representations*. Springer, 2014.

[43] Jean-Pierre Serre. *Galois cohomology*. Springer-Verlag Berlin Heidelberg, 2013.

[44] Bernd Souvignier. Irreducible finite integral matrix groups of degree 8 and 10. *Mathematics of Computation*, 63(207):335–350, 1994.