University of California
Los Angeles

Algebraic Tori and Essential Dimension

A dissertation submitted in partial satisfaction
of the requirements for the degree
Doctor of Philosophy in Mathematics

by

Anthony Michael Ruozzi

2012
Interest in essential dimension problems has been growing over the past decade. In part, it is because the idea of essential dimension captures quite elegantly the problem of parametrizing a wide range of algebraic objects. But perhaps more, it is because the study of essential dimension requires most of the algebraic arsenal. What began as a problem in Galois cohomology and representation theory now has connections to versal torsors, stacks, motives, birational geometry, and invariant theory. This exposition will focus on just a small bit of this theory: algebraic tori and how they can be used to help us calculate the essential $p$-dimension for PGL$_n$. 
The dissertation of Anthony Michael Ruozzi is approved.

Amit Sahai

Paul Balmer

Richard Elman

Alexander Merkurjev, Committee Chair

University of California, Los Angeles

2012
# Table of Contents

1 Introduction ............................................................................. 1  
1.1 Basic Notations ................................................................. 2

2 Groups and Algebras ............................................................... 3  
2.1 $p$-closed fields ................................................................. 3 
2.2 Central Simple Algebras ...................................................... 4 
  2.2.1 Étale Algebras ............................................................ 5 
  2.2.2 Division Algebras of Degree $p^s$ ................................. 5 
2.3 Algebraic Groups ............................................................... 8 
  2.3.1 Groups of Multiplicative Type ...................................... 9 
  2.3.2 Galois Cohomology ..................................................... 10

3 Essential Dimension ............................................................. 11  
3.1 Definitions ....................................................................... 12 
3.2 Essential $p$-dimension ...................................................... 13 
3.3 Essential Dimension of Algebraic Groups ......................... 14 
  3.3.1 Examples ................................................................. 15 
  3.3.2 Essential Dimension of Groups of Multiplicative Type .................................................. 16 
  3.3.3 Essential Dimension of Algebraic Tori .......................... 17 
  3.3.4 Essential Dimension of Finite Abelian Groups ............... 28

4 Essential Dimension of $\text{PGL}_n$ .......................................... 32  
4.1 The Setup ....................................................................... 33 
4.2 An Upper Bound .............................................................. 34
VITA

2003–2006 Teaching Assistant for MATH 151-153 Calculus at the University of Chicago.

2006 B.S. (Mathematics), University of Chicago.

2007 M.A. (Mathematics), UCLA, Los Angeles, California.

2006–2009 Teaching Assistant, Mathematics Department, UCLA.

Fall 2009 NSF VIGRE instructorship, Mathematics Department, UCLA.

2010 Research Assistant, Mathematics Department, UCLA.

Fall 2011 NSF VIGRE instructorship, Mathematics Department, UCLA.

2011–present Teaching Assistant, Mathematics Department, UCLA.

PUBLICATIONS

CHAPTER 1

Introduction

Essential dimension is a relatively young idea, but its study has generated much interest. This dissertation will explore a small facet of the essential dimension problem and provide a framework for understanding the computation for algebraic tori. Any new-comer to the field would certainly stumble across with the oft-referenced paper by Berhuy and Favi on the subject, and it still contains much of the basic theory. Endeavoring to not repeat that theory here, I present a slightly different outlook that I hope novices and experts alike can appreciate.

The trajectory of this dissertation is as follows. In Chapter 2, I outline the basic knowledge that forms the foundation of all subsequent chapters. For the well-informed reader, this is mostly a refresher. The highlight is a slightly improved version of a theorem of Rowen and Saltman that is useful later for the computation of the essential $p$-dimension of $\text{PGL}_n$.

In Chapter 3, I describe the essential dimension problem. The main focus is on groups of multiplicative type, and I present some new results that give a practical approach to the essential dimension problem for tori. This new method agrees with all previously know results. Indeed, I conjecture that this should be the general solution to the essential dimension problem. However, with no proof in hand, I simply demonstrate how my theory works through many examples: norm one tori, most tori of dimension 2, and small order abelian groups.

In Chapter 4, I show how algebraic tori can be used to give some bounds on the essential $p$-dimension of $\text{PGL}_n$. To date, this is the best known upper bound for the problem. The exposition mostly follows the paper I published on the subject with a notable addition: I show that the upper bound that I find actually agrees with the essential $p$-dimension of a
particular torus. I conclude with some general remarks on the known lower bounds for this problem and what conclusions can be drawn from both bounds together.

1.1 Basic Notations

$k$ will be a fixed base field. The following is a list, in roughly chronological order, of notations that will be used in this text.

- $\overline{k}$: An algebraic closure of $k$.
- $k_{\text{sep}}$: A separable closure of $k$.
- $M_n(R)$: The algebra of $n \times n$ matrices over the ring $R$.
- $A_F$: For a $k$-algebra $A$, $A \otimes_k F$.
- $C_{AB}$: The centralizer of the $A \subset B$.
- $\deg(A)$: The degree of the central simple algebra $A$.
- $\text{ind}(A)$: The index of the central simple algebra $A$.
- $\varphi(x)$: $\varphi(x) = x^p - x$.
- $R^n$: $R \times R \times \ldots \times R$, the product of $n$ copies of $R$.
- $G_m$: The multiplicative group scheme.
- $S_n$: The symmetric group on $n$ elements.
- $Z_n$: The cyclic group on $n$ elements.
- $\mu_n$: The group scheme of $n$-th roots of unity.
- $R_{F/k}(G)$: The Weil restriction of the group scheme $G$.
- $\text{trdeg}_k(F)$: The transcendence degree of the field $F$ over $k$.
- $\text{ed}_k(\mathcal{F})$: The essential dimension of the functor $\mathcal{F}$.
- $\text{ed}_p(\mathcal{F})$: The essential $p$-dimension of the functor $\mathcal{F}$.
- $\text{ed}(\mathcal{F}; p)$: The essential $p$-dimension of the functor $\mathcal{F}$.
- $A(V)$: The affine space associated to the vector space $V$.
- $\Gamma_p$: A Sylow $p$-subgroup of the profinite group $\Gamma$.
- $R^{(1)}_{F/k}(G_m)$: The torus of norm one elements for the field extension $F/k$.
- $\varphi(n)$: The Euler phi function of $n$.  

2
CHAPTER 2

Groups and Algebras

In this chapter, I outline the basic theory of central simple algebras, algebraic groups, and Galois cohomology as it will be used later in this work. Therefore, the reader well-informed of these ideas may skip this chapter with the notable exception of Section 2.2.2 where I prove a new result about the structure of degree $p^r$ division algebras after prime to $p$ extension (Corollary 5). This theorem is the basis for the argument in Chapter 4 which computes some bounds on the essential $p$-dimension of $\text{PGL}_n$.

2.1 $p$-closed fields

I make use of the following simplification employed in [LMMR09]. A field $F/k$ is called $p$-closed if every finite extension of $F$ has degree a power of $p$. After fixing a separable closure $k_{\text{sep}}$ of $k$, a $p$-closure of $k$ can be constructed as follows. Let $\Gamma = \text{Gal}(k_{\text{sep}}/k)$ and choose $\Gamma_p$ to be a Sylow $p$-subgroup. I remark that $\Gamma$ is actually a profinite group, but this notion still makes sense [RZ00]. Then

$$k_p = \{ x \in \overline{k} | x \text{ is purely inseparable over } k_{\text{sep}}^{\Gamma_p} \}$$

is the desired $p$-closure of $k$. For a further discussion of the $p$-closure see [LMMR09].

It will be useful later to have the following notion as well. A natural transformation of functors $F \to G$ will be called $p$-surjective if for any $K/k$, there is a finite extension $L/K$ of degree prime to $p$ such that $F(L) \to G(L)$.
### 2.2 Central Simple Algebras

The following can found in any standard reference on central simple algebras c.f. [KMRT98].

A central simple algebra over $k$ is a finite dimensional $k$-algebra $A \neq 0$ with center $k$ such that there are no non-trivial two sided ideals. A central simple algebra will be called a division algebra if every non-zero element is invertible. The canonical examples of a central simple algebras are the matrix algebras $M_n(k)$ for some $n$. It turns out that all other central simple algebras are “twisted forms” of these:

**Theorem 1.** *(Wedderburn)* The following are all equivalent:

1. $A$ is a central simple algebra over $k$.
2. There is a field extension $L/k$ and an integer $s$ such that $A_L \cong M_s(L)$.
3. $A_{\overline{k}} \cong M_s(\overline{k})$ for $\overline{k}/k$ any algebraic closure of $k$.
4. There is a unique up to isomorphism division $k$-algebra $D$ and an integer $t$ such that $A \cong M_t(D)$.

The fields in (2) will be referred to as splitting fields. A given algebra $A$ can have many splitting fields. For example, any central simple algebra is split by a finite separable extension. Also, the function field of the generic point of the associated Severi-Brauer variety splits $A$ [Ami82]. This is an example of a generic splitting field, the study of which is closely related to the concept of essential dimension.

Because the dimension of an algebra does not change after a field extension, (2) also implies that every central simple algebra has $\dim_k A = s^2$. As a consequence, the integer $s$ will be called the degree of $A$ (denoted $\deg(A)$). The degree of the division algebra $D$ in (4) is called the index of $A$, $\text{ind}(A)$.

The following basic fact about central simple algebras will be used in the sequel, so it is stated here for reference.

**Theorem 2.** *(KMRT98)/[Theorem 1.5]*) Let $A$ be a central simple $k$-algebra and $B \subset A$ a simple subalgebra with center $F/k$. Denote by $C_{AB}$ the set of elements of $A$ which commute
with every element of $B$. It is also a simple subalgebra of $A$ and

$$\dim(A) = \dim(B) \cdot \dim(C_A B).$$

Moreover, if $F = k$, then $C_A B$ is a central simple algebra and $A = B \otimes C_A B$.

Two central simple algebras, $A$ and $B$, will be called Brauer equivalent if $D_A$ and $D_B$, the division algebras from (4), are isomorphic. The set of all central simple algebras under Brauer equivalence forms a group under tensor product. This group is of fundamental importance to the study of the cohomology of algebraic groups as we shall see later.

### 2.2.1 Étale Algebras

Let $E$ be any (commutative, associative) finite dimensional $k$-algebra. $E$ is an étale algebra if it satisfies one of the following equivalent properties:

1. $E \simeq F_1 \times \ldots \times F_n$ where the $F_i$ are finite separable field extensions of $k$.

2. $E_{\text{sep}} = k_{\text{sep}} \times \ldots \times k_{\text{sep}}$.

Étale algebras figure prominently in the theory of central algebras. If $A$ is a central simple algebra/$k$, then by Theorem 1 (3), $A_{\overline{k}} \simeq M_n(\overline{k})$ for some $n$. In particular, there is a subalgebra $E \subset A$ such that $E_{\overline{k}} \simeq \overline{k}^n$ is the subalgebra of diagonal matrices. By (2) above, $E$ is an étale algebra. In fact, $E$ is maximal: if any other étale subalgebra of $A$ contains $E$ then it is equal to $E$. All maximal étale subalgebras of $A$ have dimension $n = \deg(A)$ [Alb39].

Étale algebras can be classified by Galois cohomology groups as we will see later.

### 2.2.2 Division Algebras of Degree $p^s$

The goal of this section is to prove that any central simple algebra of degree $p^s$ for a prime $p$ has a maximal étale algebra of a special form after a suitable prime to $p$ extension. Because of this, throughout this section, $F/k$ will be a $p$-closure of $k$ see Section 2.1. Let $D/F$ be
a division algebra of degree $n = p^s$. The objective is then to construct a maximal subfield of $D$ whose normal closure has Galois group as small as possible. We begin with a classical result:

**Proposition 3.** If $D$ contains a non-trivial separable subfield $K/F$ then $K$ contains a degree $p$ cyclic Galois extension of $F$.

**Proof.** See [RS92][Prop 1.1].

The following theorem was proven without reference to a fixed subfield $L_1$ in [RS92][Theorem 1.2]. The slight modification of this argument below illuminates the basic strategy for the fundamental construction of this section.

**Theorem 4.** Let $L_1 \subset D$ be a degree $p$ cyclic Galois extension/F. Then there is another degree $p$ cyclic Galois extension $L_2/F$ contained in $D$ such that $L_1L_2 := L_1 \otimes_F L_2 \subset D$ is a bicyclic Galois extension.

**Proof.** Denote $L_1 = F(a)$ and fix a generator $\langle \sigma \rangle = \text{Gal}(L_1/F)$. The Skolem-Noether theorem gives an element $y \in D^\times$ such that $yxy^{-1} = \sigma(x)$ for all $x \in L_1$. Let $A$ be the degree $p$ algebra generated over $F$ by $y$ and $a$ with center $F(y^p)$, and set $B = C_D A$. There are two possibilities:

- $B$ contains a non-trivial separable field extension $K/F$:

  Applying the proposition to $D$ and $K$, there is a degree $p$ cyclic extension $L_2/F$ contained in $K$. $L_1 \cap B = F$ by definition, so $L_1 \cap L_2 = F$. Thus, $L_1L_2$ is the desired bicyclic extension.

- Every subfield of $B$ is purely inseparable/F:

  Since every division algebra has a maximal separable subfield, $\deg B = 1$. It then follows that $A = C_D F(y^p)$ and $\deg A \cdot [F(y^p) : F] = \deg D$. In particular, $\deg A = p$ and so $F(y)$ is a maximal purely inseparable subfield of $D$. This is equivalent to $D$ being a cyclic $p$-algebra [Alb39][VII Theorem 25].

We will show by induction on $s$ that any cyclic $p$-algebra $D$ containing a degree $p$ subfield $L_1/F$ contains a bicyclic extension $L_1L_2/F$. First, suppose $s = 2$. Following the argument
in [Sal77] [Proposition 7], we have the degree \( p \) cyclic sub-algebra \( C = C_D L_1 \). By definition, \( C \supset F(y^p) \), so we can write \( C \simeq [x, y^p] \) for some \( x \in L_1 \). By [Sal77][Lemma6] (choosing \( a' = 0 \)), \( C = [a_0, b_0] \) with \( a_0 \in F \). Let \( \varphi(x_0) = x_0^p - x_0 = a_0 \) for \( x_0 \in C \) and set \( L = L_1(x_0) \). If \( a \) and \( a_0 \) are linearly independent elements of the \( \mathbb{F}_p \)-vector space \( F/\varphi(F) \) then \( L_2 = F(x_0) \) is the desired extension. Otherwise, \( a_0 \in \varphi(F) \) which implies that \( C \) is split. Since degree \( p \) split algebras contain every degree \( p \) extension of \( F \), we can choose for \( L_2 \) any cyclic extension disjoint from \( L_1 \). Such a field always exists if \( \dim_{\mathbb{F}_p} F/\varphi(F) \geq 2 \). Since \( D \) is a division algebra of degree \( \geq 2 \), this condition holds by [Sal77][Theorem 3].

Now assume that we have the result for \( s \geq 3 \) and consider \( A' = C_D F(y^{p^{s-1}}) \). It is a degree \( p^{s-1} \) algebra containing \( F(y) \) and \( L_1 \). Therefore, it is also cyclic and the induction hypothesis implies that there is a cyclic degree \( p \) extension \( L_2/F(y^{p^{s-1}}) \) disjoint from \( L_1(y^{p^{s-1}}) \). Since \( F(y^{p^{s-1}}) \) is purely inseparable, there is a cyclic degree \( p \) field \( L_2/F \) such that \( L_2(y^{p^{s-1}}) = L_2' \) which is still disjoint from \( L_1 \).

**Corollary 5.** For \( A \) any central simple algebra/\( F \) of degree \( p^s \geq p^2 \) and \( K_1 \subset A \) an étale subalgebra of degree \( p \), there is a maximal étale subalgebra \( K \subset A \) that can be written as \( K = K_1 \otimes_F K_2 \) for \( K_2/F \) an étale algebra of dimension \( p^{s-1} \).

**Proof.** First, consider the case where \( A \) is a division algebra. By the theorem, \( A \) contains two distinct degree \( p \) cyclic extensions \( K_1 \) and \( L \) over \( F \). Proceed by induction on \( s \).

If \( s = 2 \), then taking \( K_2 = L \) we are done. Otherwise, assume we have the result for any division algebra of degree \( p^{s-1} \) and any degree \( p \) subfield \( L' \). The centralizer \( C_A L \) is a division algebra over \( L \) of degree \( p^{s-1} \). By definition it contains the degree \( p \) subfield \( K_1 L/L \), so by induction hypothesis, \( C_A L \) has subfield \( K_2/L \) disjoint from \( K_1 L \) of degree \( p^{s-2} \).

Since \( K_2 \cap K_1 L = L \) and \( L \) is disjoint from \( K_1, K_2 \cap K_1 = F \). It follows that \( K_2/F \) is a degree \( p^{s-1} \) extension disjoint from \( K_1 \) and \( K_1 \otimes K_2 \subset A \).

Suppose \( A \) is not a division algebra. If \( A \) is split, the result is immediate. Otherwise, choose a division algebra \( D \sim A \). Then

\[
\deg(D) = p^t \leq p^s = \deg(A).
\]
If \( t = 1 \), then any maximal subfield \( K_1 \subset D \) gives the desired étale algebra \( K_1 \otimes F^{x p^{s-1}} \subset A \), so suppose \( t \geq 2 \). By the above argument, \( D \) has a subfield

\[
L = L_1 L_2 \simeq L_1 \otimes L_2
\]

with \( [L_1 : F] = p \) and \( [L_2 : F] = p^{t-1} \). Set \( K = L^{x p^{s-t}} \) an étale sub-algebra of \( A \). Since \( K \) has dimension \( p^s \), it is maximal. But \( K \simeq L_1 \otimes L_2^{x p^{s-t}} \), so \( L_1 \) and \( L_2^{x p^{s-t}} \) are étale algebras of the desired degree.

\[ \square \]

### 2.3 Algebraic Groups

An affine algebraic group is a functor \( G : \text{CommAlg}_k \to \text{Group} \) that is representable by a Hopf algebra \( /k \). That is, there is a commutative \( k \)-algebra \( A \) equipped with three homomorphisms

\[
c : A \to A \otimes A
\]

\[
i : A \to A
\]

\[
u : A \to F
\]

satisfying the usual commutative diagrams for the co-multiplication, co-inverse, and co-unit such that \( G(R) = \text{Hom}(A, R) \) for any commutative \( k \)-algebra \( R \) see [KMRT98] for more details.

Many of the most familiar groups are actually group schemes: finite (constant) groups, the additive group scheme \( \mathbb{G}_a \), the multiplicative group scheme \( \mathbb{G}_m \), \( \text{GL}_n \), \( \text{PGL}_n \), etc. Moreover, group schemes have all of the usual properties of groups. There are well-defined notions of subgroup, normal subgroup, homomorphism, and quotient group that satisfy the usual properties. One important exception is that a surjective map between two group schemes need not be surjective on every \( R \)!

Group schemes behave quite nicely with respect to field extensions. In fact, given a field extension \( F/k \) and a group scheme \( G \) over \( k \), we can produce the restriction over \( F \) simply by setting \( G_F(R) := \text{Hom}(A_F, R) \) where \( A \) is the Hopf algebra associated to \( G \). Similarly, if \( H \)
is a group scheme over $F$, we define the corestriction (or more frequently Weil restriction) to be the group scheme $R_{F/k}(H)(R) := H(R \otimes_k F)$. Restrictions are obviously group schemes, but the corestriction requires a bit of work to produce the corresponding Hopf algebra c.f. [KMRT98][Lemma 20.6].

2.3.1 Groups of Multiplicative Type

The primary concern of this work will be with algebraic tori, so I will explain this theory in more detail. For any abelian group $H$ (written multiplicatively), the group ring $k\langle H \rangle$ has the structure of a Hopf algebra given by the choices $c(h) = h \otimes h$, $i(h) = h^{-1}$, and $u(h) = 1$. Therefore, the corresponding representable functor is a group scheme. Such groups are called diagonalizable. As an example, $\mathbb{G}_m$ is the diagonalizable group associated to the abelian group $\mathbb{Z}$.

A group of multiplicative type is any group scheme that becomes diagonalizable over a separable closure $k_{sep}$. This family of group schemes includes the algebraic tori: group schemes $T$ such that $T_{k_{sep}} \cong \mathbb{G}_m \times \ldots \times \mathbb{G}_m$ and the roots of unity: $\mu_n$. Part of their value in the theory of algebraic groups is the following equivalence of categories.

**Theorem 6.** [KMRT98][Proposition 20.17] There is an equivalence of categories between the category of group schemes of multiplicative type$/k$ and the category of abelian groups with continuous $\text{Gal}(k_{sep}/k)$-action.

The equivalence is given by sending a group of multiplicative type to its characters, $G^* = \text{Hom}(G_{k_{sep}}, \mathbb{G}_{m,k_{sep}})$. And conversely, sending an abelian group $A$ to the functor $A(R) = \text{Hom}(A, (R \otimes_k k_{sep})^*)$. We will see later how this correspondence can be fruitful in many calculations. As a final notation, a torus will be called quasi-split if the associated $\Gamma$-module is a permutation module.
2.3.2 Galois Cohomology

Again, following [KMRT98], I will give a brief survey of Galois cohomology. Let \( \Gamma \) be a profinite group. A \( \Gamma \)-group is a group \( M \) with \( \Gamma \) acting by group homomorphisms. We can define cohomology (pointed) sets as follows

\[
H^0(\Gamma, M) = \{ m \in M | \gamma m = m \text{ for all } \gamma \in \Gamma \}.
\]

This is simply the subgroup of elements of \( M \) fixed by the \( \Gamma \)-action. The first cohomology groups is defined in two steps. First, we consider 1-cocycles:

\[
Z^1(\Gamma, M) = \{ \text{continuous maps } \alpha : \Gamma \to M | \alpha(\gamma_1 \gamma_2) = \alpha(\gamma_1) \gamma_1 \alpha(\gamma_2) \text{ for } \gamma_i \in \Gamma \}.
\]

Two 1-cocycles \( \alpha \) and \( \beta \) are equivalent if there is an element \( m \in M \) such that \( \beta(\gamma) = m \alpha(\gamma) \gamma m^{-1} \) for all \( \gamma \in \Gamma \). \( H^1(\Gamma, M) \) is defined to be \( Z^1(\Gamma, M) / \sim \).

The most important case for our purposes will be when \( \Gamma = \text{Gal}(k_{\text{sep}}) \) and \( M = G(k_{\text{sep}}) \) for some algebraic group \( G \). In this case, we will abbreviate \( H^1(\Gamma, M) = H^1(k, G) \). If \( N \) is smooth then an exact sequence of algebraic groups

\[
1 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 1
\]

induces an exact sequence of pointed sets

\[
1 \rightarrow N(k_{\text{sep}})^{\Gamma} \rightarrow G(k_{\text{sep}})^{\Gamma} \rightarrow H^{1}(k_{\text{sep}})^{\Gamma} \rightarrow H^1(k, N) \rightarrow H^1(k, G) \rightarrow H^1(k, H).
\]

If \( N \) is abelian, then this sequence may be continued to the right. Moreover, \( H^1(k, G) \) is functorial in both \( k \) and \( G \).

For many algebraic groups, the first Galois cohomology group classifies algebras [KMRT98][Section 29.B]. That is, the elements of the pointed set \( H^1(k, G) \) are in bijective correspondence with isomorphism classes of a certain type of algebra/\( k \). Some important examples are for \( S_n, \text{PGL}_n, \) and \( O_n \) which classify, \( n \)-dimensional étale algebras, central simple algebras of degree \( n \), and \( n \)-dimensional quadratic forms respectively. This fact will be quite important for us in later chapters.
CHAPTER 3

Essential Dimension

The essential dimension of an algebraic group $G$ is a measure of the “least number of parameters” needed to define a generic $G$-torsor. Since $G$-torsors classify special classes of algebras, as shown in Chapter 2, this allows us to study the essential dimension via our knowledge of algebras. Theoretically, one would like to go the other way as well: can we use the essential dimension to study the structure of algebras? So far, we have no results in this direction.

The study of essential dimension began in 1997 with J. Buhler and Z. Reichstein’s study of Galois $G$-algebras [BR97] for a finite group $G$. In the most familiar case, this is just a choice of Galois extension over a field $F$ with Galois group $G$. Let $\alpha$ be a generator of this extension over $F$. It has a minimal polynomial with coefficients in $F$. The number of algebraically independent coefficients in this equation gives a measure of the complexity of this field extension. Of course, this choice of generator is not canonical, so perhaps with a different choice of generator $\beta$, we can get a minimal polynomial with a smaller number of coefficients. The least number of algebraically independent coefficients in a minimal polynomial of a field generator is exactly the essential dimension of this Galois extension.

Later, A. Merkurjev reformulated the essential dimension problem functorially, c.f. [BF03]. In this way, essential dimension is a general notion that encompasses the usual dimensions for schemes and vector spaces as well as the “dimension” of Galois cohomology functors. This latter case is perhaps the most studied example with applications to inverse Galois theory and the theory of central simple algebras.

The essential dimension problem is also inherently geometric. P. Brosnan, Z. Reichstein, and A. Vistoli [BRV07] have discussed a generalization to algebraic stacks, and because Galois cohomology groups classify the torsors of a algebraic group, the essential dimension
problem also admits an interpretation in terms of versal torsors c.f. [Rei10, Section 2].

In this chapter, I will introduce the theory of essential dimension and survey some of the known results. My focus is on the essential dimension of algebraic tori (or more generally groups of multiplicative type) because they play a central role in most of our bounds. In fact, most of the known results for abelian groups can be summarized by a single idea which I call a permutation representation. Even for non-abelian groups, though, tori are crucial to most of our constructions but you will have to wait until Chapter 4 for more on this.

3.1 Definitions

We wish to extend the idea of dimension to a broader class of algebraic objects. This can be accomplished using the following observation. Let $\text{Fields}/k$ be the category of field extensions of $k$ with inclusion maps. Any scheme $X$ over $k$ can be considered as functor

$$X : \text{Fields}/k \to \text{Set}$$

defined as $X(F) = \text{Hom}(\text{Spec } k, X)$. The dimension of this scheme can be computed as

$$\dim(X) = \sup_{x \in X} \text{trdeg}_k k(x)$$

where $k(x)$ is the residue field at $x$.

This definition extends to an arbitrary functor $\mathcal{F} : \text{Fields}/k \to \text{Set}$. An element $a \in \mathcal{F}(K)$ is said to be defined over $k \subset K_0 \subset K$ (and that $K_0$ is a field of definition of $a$) if it is in the image of the map $\mathcal{F}(K_0) \to \mathcal{F}(K)$. The essential dimension of $a$, denoted $\text{ed}_k(a)$, is the least transcendence degree $/k$ of a field of definition for $a$. The essential dimension of $\mathcal{F}$ is defined as the possibly infinite value

$$\text{ed}_k(\mathcal{F}) = \sup \{ \text{ed}_k(a) \}$$

where the supremum is taken over all $a \in \mathcal{F}(K)$ and all field extensions $K/k$.

**Proposition 7.** Let $\mathcal{F}$ and $\mathcal{G}$ be functors as above. Then we have the following useful properties:
(1) For any field extension $L/k$, $\text{ed}_k(\mathcal{F}) \geq \text{ed}_L(\mathcal{F})$.

(2) Given a surjective natural transformation $\phi : \mathcal{F} \to \mathcal{G}$ then $\text{ed}_k(\mathcal{F}) \geq \text{ed}_k(\mathcal{G})$.

Proof. (1) Choose a field extension $K/L$ and an element $a \in \mathcal{F}(K)$. By definition, there is a field $K_0$ and an element $b \in \mathcal{F}(K_0)$ mapping to $a$ such that $\text{ed}_k(a) = \text{trdeg}_k(K_0) \leq \text{ed}_k(\mathcal{F})$. Consider the composite field extension $K_0L$. By construction, $\text{trdeg}_L(K_0L) \leq \text{ed}_k(\mathcal{F})$ and $b$ maps to $a$ under the composite $\mathcal{F}(K_0) \to \mathcal{F}(K_0L) \to \mathcal{F}(L)$. Therefore $a$ is defined over $K_0L$ and

$$\text{ed}_{L}(a) \leq \text{trdeg}_{L}(K_0L) \leq \text{ed}_{k}(\mathcal{F}).$$

(2) Choose a field extension $K/k$ and an element $a \in \mathcal{G}(K)$ such that $\text{ed}_k(a) = \text{ed}_k(\mathcal{G}) = \text{trdeg}_k(K)$. Since $\phi$ is surjective, choose an element $c \in \mathcal{F}(K)$ mapping to $a$. By definition, there is a subfield $k \subset K_0 \subset K$ such that $c$ is defined over $K_0$ and $\text{ed}_k(c) = \text{trdeg}_k(K_0) \leq \text{ed}_k(\mathcal{F})$. By commutativity of the diagram

$$\begin{array}{ccc}
\mathcal{F}(K) & \to & \mathcal{G}(K) \\
\downarrow & & \downarrow \\
\mathcal{F}(K_0) & \to & \mathcal{G}(K_0)
\end{array}$$

it follows that $a$ is also defined over $K_0$, and so

$$\text{ed}_k(\mathcal{F}) \geq \text{ed}_k(c) = \text{trdeg}_k(K_0) \geq \text{ed}_k(a) = \text{ed}_k(\mathcal{G}).$$

\[\square\]

Remark 8. If $\mathcal{F} \hookrightarrow \mathcal{G}$ it does not follow that $\text{ed}_k(\mathcal{F}) \leq \text{ed}_k(\mathcal{G})$. In general, we need stronger conditions to make this true c.f. [BF03][Prop 1.8].

3.2 Essential $p$-dimension

The computation of the essential dimension of a functor can in general be quite challenging. It is often useful in the computation of lower bounds to replace it with a weaker notion: essential $p$-dimension. The basic idea is to allow a bit more flexibility in our fields of definition.
Let $\mathcal{F}$ be a functor as in the previous section. An element $a \in \mathcal{F}(K)$ is $p$-defined over $K_0/k$ if there is a finite prime to $p$ extension $K' \supset K_0$ such that the image of $a$ in $K'$ is in the image of an element from $K_0$. Again, define $ed_p(a) = \mintrdeg_k(K_0)$ where the minimum is taken over all fields of $p$-definition. Similarly, set $ed_p(\mathcal{F}) = \sup\{ed_p(a)\}$.

It is clear that $ed_p$ satisfies the same properties as listed in the previous section. Moreover, $ed_p(\mathcal{F}) \leq ed(\mathcal{F})$ for any prime $p$. Sometimes, in order to avoid a preponderance of indices, I will use the notation $ed_k(\_; p)$ for the essential $p$-dimension, especially when the base field is not understood.

The language of $p$-closures can help us to simplify the discussion of essential $p$-dimension (see Section 2.1). For limit-preserving functors, the essential $p$-dimension of any element can be computed over a $p$-closure [LMMR09][Lemma 3.3], so we can always assume that our field $F$ is $p$-closed when doing such a computation. Moreover, if $F/k$ is $p$-closed and $\mathcal{F}(F) \twoheadrightarrow \mathcal{G}(F)$ for two functors $\mathcal{F}$ and $\mathcal{G}$, then the map is $p$-surjective and $ed_k(\mathcal{F}; p) \geq ed_k(\mathcal{G}; p)$ [LMMR09][Prop 3.4].

### 3.3 Essential Dimension of Algebraic Groups

For algebraic groups, we have the Galois cohomology functors as defined in Section 2.3.2. It is standard to abbreviate $ed(H^1(\_; G))$ by $ed(G)$. Since these functors classify algebras (or more generally torsors), computing the essential dimension of algebraic groups is a very interesting problem. Before computing some examples, I would like to first give some connections of this theory with representations.

Let $G$ be an algebraic group. $G$ is said to act generically freely on a scheme $X$ if there is a $G$-stable open subscheme $U \subset X$ on which $G$ acts freely. A generically free representation is a $G$-generically free action on the affine space $A(V)$ where $V$ is a finite dimensional vector space. Such representations give convenient upper bounds for the essential dimension problem.
Theorem 9. [BF03][Proposition 4.11] If \( V \) is a generically free representation of \( G \) then
\[
ed(G) \leq \dim(V) - \dim(G).
\]

This follows by finding a \( G \)-stable open \( U \subset \mathbb{A}(V) \) for which the quotient \( U/G \) exists (in the category of schemes) and then constructing a surjective morphism from \( U/G(-) \) to \( \mathbb{H}^1(-, G) \). Of course, in many cases, this bound will not be tight, but \( U \to U/G \) is always a versal \( G \)-torsor. Therefore, we can study compressions of this to compute the essential dimension c.f. [BF03][Chapter 6] or [DR11].

3.3.1 Examples

Computing the essential dimension is a difficult problem even for finite abelian groups as we will see later in Section 3.3.4. Below are some known results to contrast between essential dimension and essential \( p \)-dimension.

\( S_n \): This is one of the first groups for which the essential dimension was bounded. However, for \( n > 7 \), the precise computation is unknown. First, \( \text{ed}(S_2) = \text{ed}(S_3) = 1 \) and \( \text{ed}(S_3) = 2 \) [BF03][Chapter 7]. For \( n \geq 5 \),
\[
\left\lfloor \frac{n}{2} \right\rfloor \leq \text{ed}(S_n) \leq n - 3.
\]
This lower bound is not tight since Duncan showed that \( \text{ed}(S_7) = 4 \) [Dun10]. The essential \( p \)-dimension problem is completely solved however [MR09][Corollary 4.2]:
\[
\text{ed}_p(S_n) = \left\lfloor \frac{n}{p} \right\rfloor.
\]

\( p \)-groups: A similar situation occurs for \( \mathbb{Z}_p \). Later we will see that the best known upper bound for \( \text{ed}(\mathbb{Z}_p) \) is \( \phi(p - 1) \). However, after a prime to \( p \) extension the groups \( \mathbb{Z}_p \) and \( \mu_p \) become isomorphic. Therefore, we can compute \( \text{ed}_p(\mathbb{Z}_p) \) by looking at the Kummer sequence
\[
1 \longrightarrow \mu_p \longrightarrow \mathbb{G}_m \longrightarrow \mathbb{G}_m \longrightarrow 1.
\]
Using Hilbert Theorem 90 and the long exact sequence in cohomology shows that \( \mathbb{G}_m(F) \to \mathbb{H}^1(F, \mu_p) \). Therefore, \( \text{ed}_p(\mathbb{Z}_p) = \text{ed}(\mu_p) = 1 \). Clearly, these values are substantially different if the base field is \( k = \mathbb{Q} \). However, if \( k \) contains the \( p \)-th roots of unity, we have the following powerful result.
Theorem 10. [KM08][Theorem 4.1] If \( k \) is a field of char \( \neq p \) containing a primitive \( p \)-th root of unity and \( G \) is a finite \( p \)-group, then \( \text{ed}(G) = \text{ed}_p(G) = \min(\dim(V)) \) where the minimum is taken over all faithful (generically free) representations \( V \) of \( G \).

### 3.3.2 Essential Dimension of Groups of Multiplicative Type

Throughout this section, let \( T \) be any group of multiplicative type and \( p \) a prime different from char(\( k \)). Let \( \Gamma \) be the Galois group Gal(\( L/k \)) for some Galois splitting field \( L \) of \( T \) and \( \Gamma_p \) a Sylow \( p \)-subgroup of \( \Gamma \). A map of \( \Gamma_p \) modules \( M \to P \) will be called a \( p \)-presentation if \( P \) is a permutation module and the cokernel is finite of order prime to \( p \). As an extension of the Karpenko-Merkurjev result [KM08], we have the following general theorem which completely solves the essential \( p \)-dimension problem for groups of multiplicative type.

**Theorem 11** ([LMMR09]Corollary 5.1). If \( T \) is split by a Galois extension of \( p \)-power order, then

\[
\text{ed}_p(T) = \min(\phi) - \dim(T)
\]

where the minimum is taken over all \( p \)-presentations \( \phi \) of \( T^* \) (viewed as \( \Gamma_p \)-module).

In general, the calculation of the essential dimension of groups of multiplicative type is mostly unknown. In the rest of this section, I will give a method for constructing upper bounds and use it to reproduce all known upper bounds for the essential dimension problem. I begin with some notation.

**Definition 12.** A \( G \)-module \( Q \) is a permutation representation of \( T \) if there is a map \( \phi : Q \to T^* \), a permutation module \( P \), and another map \( Q \to P \) such that the following diagram commutes:

\[
\begin{array}{ccc}
Q & \to & P \\
\downarrow & & \downarrow \\
T^* & & \\
\end{array}
\]

Such a representation will be called faithful if \( \phi \) is a surjection.
By definition, a faithful permutation representation of $T$ yields a short exact sequence

$$0 \longrightarrow M \longrightarrow Q \longrightarrow T^* \longrightarrow 0$$

Consider the exact sequence in cohomology for the corresponding tori:

$$1 \longrightarrow T(K) \longrightarrow \hat{Q}(K) \longrightarrow \hat{M}(K) \longrightarrow H^1(K, \hat{X}) \longrightarrow H^1(K, \hat{Q})$$

Because $T \rightarrow \hat{M}$ factors through a quasi-split torus and quasi-trivial tori have no non-trivial $K$-torsors, it follows that $\hat{M}(K) \rightarrow H^1(K, T)$, and so $\text{ed}(T) \leq \text{rank}(M)$.

I will show that this bound is a very good one in the following sections. As a consequence, I propose the following conjecture whose demonstration either positively or negatively would be a good start to understanding the general problem:

**Conjecture 13.** For a group of multiplicative type $T$,

$$\text{ed}(T) = \min(\text{rank}(Q)) - \text{dim}(T)$$

where the minimum is taken over all faithful permutation representations of $T$.

### 3.3.3 Essential Dimension of Algebraic Tori

To begin, I show that Theorem 11 can be re-written in terms of permutation representations.

**Theorem 14.** Let $X = T^*$ be the $\Gamma$-lattice corresponding to the torus $T$ which splits over a Galois extension of degree $p^n$ with Galois group $G$. Then,

$$\text{ed}_p(T) = \min(\text{rank}(Q)) - \text{dim}(T)$$

where the minimum is taken over all faithful permutation representations of $X$.

**Proof.** Following [LMMR09], we know that this essential $p$-dimension is given by $\text{rank}(P) - \text{rank}(X)$ where $P$ is a permutation module of minimal rank with a map $\phi : P \rightarrow X$ such that $\text{coker}(\phi)$ is finite of order prime to $p$. Let $I = \text{Im}(\phi)$ and $M = \ker(\phi)$. We then have an exact sequence:

$$0 \longrightarrow M \longrightarrow P \longrightarrow I \longrightarrow 0$$
By definition, $I_{(p)} := \mathbb{Z}_{(p)} \otimes I = X_{(p)}$, and since $p$ is the only prime dividing the order of $G$, $I$ and $X$ are in the same genus. By an amazing result [CR81][Theorem 31.28], this implies that if we take any faithful $G$-lattice, say $\mathbb{Z}[G]$, there is another $G$-lattice $J$ in the same genus as $\mathbb{Z}[G]$ such that

$$I \oplus \mathbb{Z}[G] \simeq X \oplus J.$$

Consider now the exact sequence

$$0 \longrightarrow M \longrightarrow P \oplus \mathbb{Z}[G] \longrightarrow I \oplus \mathbb{Z}[G] \longrightarrow 0$$

Using the above isomorphism, we have two maps $i : X \hookrightarrow I \oplus \mathbb{Z}[G]$ and $p : I \oplus \mathbb{Z}[G] \twoheadrightarrow X$ where $p \circ i = id_X$. Pulling back the above sequence along $i$ gives a diagram

$$
\begin{array}{ccccccccc}
0 & & 0 \\
& \downarrow & & \downarrow \\
0 & \longrightarrow & M & \longrightarrow & Q & \longrightarrow & X & \longrightarrow & 0 \\
& \parallel & g & \downarrow & i & \downarrow & \\
0 & \longrightarrow & M & \longrightarrow & P \oplus \mathbb{Z}[G] & \longrightarrow & I \oplus \mathbb{Z}[G] & \longrightarrow & 0
\end{array}
$$

Then $f = p \circ h \circ g$ factors through a permutation module, so $Q$ is a faithful permutation representation and the essential $p$-dimension is bounded above by $\text{rank}(M)$. This is the exact value by assumption, so $M$ has minimal rank coinciding with the essential dimension as desired. \hfill \Box

**Corollary 15.** Let $G$ be a group of multiplicative type which splits over a Galois extension of degree $p^n$ with Galois group $H$ that fits into an exact sequence

$$1 \longrightarrow T \longrightarrow G \longrightarrow F \longrightarrow 1$$

where $T$ is a maximal subtorus and $F$ is a $p$-group. Then,

$$\text{ed}_p(T) = \min(\text{rank}(Q)) - \dim(T)$$

where the minimum is taken over all faithful permutation representations of $T^*$. 

18
Proof. Clearly, permutation representations give upper bounds, so we only need prove the lower bound. By Theorem 11, we know that the essential \( p \)-dimension is given by \( \dim(P) - \dim(G) \) where \( P \) is a quasi-split torus of minimal rank with a map \( \phi : G \to P \) such that \( N = \text{Ker}(\phi) \) is finite of order prime to \( p \). Let \( J = \text{Im}(\phi) \) and set \( I \) to be the image of \( T \) in \( J \). We have a diagram:

\[
\begin{array}{ccccccc}
1 & \longrightarrow & T & \longrightarrow & G & \longrightarrow & F & \longrightarrow & 1 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 & & N & & J & & F & & 1 \\
\end{array}
\]

The cokernel of the composition from \( T \) to \( J \) and the cokernel of the composition from \( N \) to \( F \) agree, so since \( N \) and \( F \) are relatively prime, \( N \to F \) is the trivial map. We get the exact sequence

\[
1 \longrightarrow I \longrightarrow J \longrightarrow F \longrightarrow 1.
\]

Similarly, both kernels must be the same, so it follows that \( \text{Ker}(T \to P) = N \) yielding the exact sequence

\[
1 \longrightarrow N \longrightarrow T \longrightarrow I \longrightarrow 1.
\]
The inclusions of $I$ and $J$ into $P$ induce a diagram (1):

\[
\begin{array}{ccccccccc}
1 & & & & & & & & 1 \\
& & & & & & & & \\
1 & & F & & & & & & 1 \\
& & & & & & & & \\
1 & \longrightarrow & I & \longrightarrow & P & \longrightarrow & S & \longrightarrow & 1 \\
& & & & & & & & \\
1 & \longrightarrow & J & \longrightarrow & P & \longrightarrow & R & \longrightarrow & 1 \\
& & & & & & & & \\
& & & & & F & & & 1 \\
& & & & & & & & \\
& & & & & & & & 1 \\
\end{array}
\]

where $F$ is the kernel of $S \rightarrow R$ by the Snake Lemma.

Let $\mathbb{Z}[H]^\oplus r \rightarrow N^*$ be a faithful representation of $N$. If we take the exact sequence of characters corresponding to the quotient of $T$ by $I$ above and pullback along $\mathbb{Z}[H]^\oplus r \rightarrow N^*$ we get

\[
\begin{array}{ccccccccc}
0 & & 0 & & & & & & 0 \\
& & & & & & & & \\
M & \longrightarrow & M & & & & & & \\
& & & & & & & & \\
0 & \longrightarrow & I^* & \longrightarrow & X & \longrightarrow & \mathbb{Z}[H]^\oplus r & \longrightarrow & 0 \\
& & & & & & & & \\
0 & \longrightarrow & I^* & \longrightarrow & T^* & \longrightarrow & N^* & \longrightarrow & 0 \\
& & & & & & & & \\
0 & & 0 & & & & & & 0 \\
\end{array}
\]

Since $\mathbb{Z}[H]^\oplus r$ is projective, the middle sequence splits. To see that $X \simeq M \oplus T^*$ as well, it suffices by [CR81][Corollary 31.3(i)] to first localize at $p$. Luckily, $N$ has order prime to $p$, so it vanishes in the localization and the splitting is trivial. Note, however, that if we do the same with the sequence:

\[
\begin{array}{cccccc}
1 & \longrightarrow & N & \longrightarrow & G & \longrightarrow & J & \longrightarrow & 1, \\
\end{array}
\]

20
the fact that $G$ is not a lattice means that we can’t get a splitting in general. However, we can combine these two pullback diagrams to get a commutative diagram (2):

\[
\begin{array}{cccccccccc}
0 & \longrightarrow & F^* & \longrightarrow & J^* \oplus \mathbb{Z}[H]^{\oplus r} & \longrightarrow & I^* \oplus \mathbb{Z}[H]^{\oplus r} & \longrightarrow & 0 \\
& & | & & | & & | & & |
0 & \longrightarrow & F^* & \longrightarrow & G^* & \longrightarrow & T^* & \longrightarrow & 0.
\end{array}
\]

Now, I argue for $T^*$ as in the theorem. By pulling back along the inclusion of $T^*$ into $I^* \oplus \mathbb{Z}[H]^{\oplus r}$ we get

\[
\begin{array}{cccccccccc}
0 & \longrightarrow & S^* & \longrightarrow & Q^* & \longrightarrow & T^* & \longrightarrow & 0 \\
& & | & & | & & | & & |
0 & \longrightarrow & S^* & \longrightarrow & P^* \oplus \mathbb{Z}[H]^{\oplus r} & \longrightarrow & I^* \oplus \mathbb{Z}[H]^{\oplus r} & \longrightarrow & 0
\end{array}
\]

and since $i$ splits, the first row is a permutation representation of $T$ as before. Note that $S$ is the torus given in diagram (1) above. This diagram can be extended to a commutative diagram (with non-exact columns) using (2):

\[
\begin{array}{cccccccccc}
0 & \longrightarrow & S^* & \longrightarrow & Q^* & \longrightarrow & T^* & \longrightarrow & 0 \\
& & | & & | & & i & & |
0 & \longrightarrow & S^* & \longrightarrow & P^* \oplus \mathbb{Z}[H]^{\oplus r} & \longrightarrow & I^* \oplus \mathbb{Z}[H]^{\oplus r} & \longrightarrow & 0 \\
& & | & & | & & j & & |
0 & \longrightarrow & F^* & \longrightarrow & G^* & \longrightarrow & T^* & \longrightarrow & 0.
\end{array}
\]

This defines a map $Q^* \to G^*$ that factors through a permutation module. The left hand map $S^* \to F^*$ is exactly the one that follows from (1) and the Snake Lemma, so it is a surjection. On the right, $j \circ i$ is the identity. Therefore, by the 5-Lemma, the $Q^* \to G^*$ is also surjective.

Finally,

\[
ed_p(G) = \dim(P) - \dim(G) = \dim(S) = \dim(Q) - \dim(T) = \dim(Q) - \dim(G)
\]

as desired.
Corollary 16. A torus $T$ has $ed(T) = 0$ if and only if $T^*$ is an invertible $\Gamma$-module.

Proof. If $T^*$ is invertible then $H^1(K, T) = 0$ for all field extensions $K/F$, so clearly it has essential dimension 0.

Conversely, $ed(T) \geq ed_p(T)$ for all $p$, so if $ed(T) = 0$, then all essential $p$-dimensions are likewise 0. By the theorem, for any $p$ there is a faithful permutation resolution of $\Gamma_p$-modules:

$$
0 \rightarrow M \rightarrow Q \rightarrow T^* \rightarrow 0
$$

where $\text{rank}(M) = 0$. But $Q$ is a free $\mathbb{Z}$-module which implies that $M = 0$. Therefore, there is a $\Gamma_p$-isomorphism of $T^*$ that factors through a permutation module. That is, $T^*$ is an invertible $\Gamma_p$-module. Since this is true for any $p$, $T^*$ is also an invertible $\Gamma$-module as desired. \qed

I remark that this proof can be done without the aid of Theorem 11, but this would take us too far afield. I now want to compute some other more examples to show how difficult the essential dimension problem can be in general.

3.3.3.1 Examples

$R^{(1)}_{L/F}(\mathbb{G}_m)$:

Let $L/F$ be any finite separable extension, then the norm homomorphism gives an exact sequence:

$$
1 \rightarrow R^{(1)}_{L/F}(\mathbb{G}_m) \rightarrow R_{L/F}(\mathbb{G}_m) \rightarrow \mathbb{G}_m \rightarrow 1
$$

Since the middle group has no non-trivial $F$-torsors by Shapiro’s Lemma and Hilbert Theorem 90, there is, for any field extension $K/F$ a surjection

$$
\mathbb{G}_m(K) \rightarrow H^1(K, R^{(1)}_{L/F}(\mathbb{G}_m)).
$$

Therefore, $ed_F(R^{(1)}_{L/F}(\mathbb{G}_m)) \leq 1$. A torus has essential dimension 0 if and only if it is a direct summand of a quasi-split torus by Corollary 16, so this torus must have essential dimension 1.
One Dimensional Tori:

Up to choice of a degree 2 field extension $K/F$, there are only two one dimensional tori: $\mathbb{G}_m$ and $R^{(1)}_{K/F}(\mathbb{G}_m)$. These have essential dimension 0 and 1 respectively.

Two Dimensional Tori:

Two dimensional tori were classified in [Vos65]. Every two dimensional torus is split by a Galois extension whose Galois group is a subgroup of either $D_8$ or $D_{12}$. The essential dimension of the $D_8$-tori can be computed directly with the aid of Theorem 11, so let us consider tori split by Galois extensions with degree divisible by six. There are three possible groups: $Z_6$, $S_3$, and $D_{12}$.

There is only one class of torus for $Z_6$: the norm one tori for a degree six cyclic extension. All such tori have essential dimension 1 by the previous example.

There are two class of tori split by an $S_3$-extension. The first is a norm one torus for a non-normal degree 3 extension, so we can compute its essential dimension as above. Instead, consider its dual, the torus $T$

$$1 \longrightarrow \mathbb{G}_m \longrightarrow R_{F/k}(\mathbb{G}_m) \longrightarrow T \longrightarrow 1$$

where $F/k$ is a non-normal degree 3 extension. Then taking an algebraic closure, it is easy to see that $T$ is split by a field extension $L/k$ with $\text{Gal}(L/k) = S_3$. This induces, in the usual way, a sequence of $S_3$-modules:

$$0 \longrightarrow T^* \longrightarrow Z[S_3/Z_2] \longrightarrow Z \longrightarrow 0$$

To get an upper bound, it suffices to find a good permutation representation. Let $S_3 = Z_3 \rtimes Z_2 = \{\sigma\} \rtimes \{\tau\}$. That is, the group generated by $\sigma$ and $\tau$ with the relation $\sigma \tau = \tau \sigma^2$. It follows that $T^*$ is generated by the element $\bar{\sigma} - \bar{1}$ where the bar denotes the coset in $S_3/\{\tau\}$. This means we have an exact sequence

$$0 \longrightarrow M \longrightarrow Z[S_3] \longrightarrow T^* \longrightarrow 0$$

where the second map sends the generator 1 to $\bar{\sigma} - \bar{1}$. This shows that $\text{ed}(T) \leq 4$, but we can actually do better. It is easy to see that $M = \langle \sigma^2 + \tau, \sigma^2 + \sigma + 1 \rangle$. Therefore the natural
map \( \mathbb{Z}[S_3] \to \mathbb{Z}[S_3/\langle \tau \rangle] \) gives a diagram:

\[
\begin{array}{c}
0 & 0 \\
\downarrow & \downarrow \\
0 & 0 \\
\downarrow & \downarrow \\
0 & \rightarrow N & 
\rightarrow Q & 
\rightarrow T^* & 
\rightarrow 0 \\
\downarrow & \downarrow & \mid \\
0 & 
\rightarrow M & 
\rightarrow \mathbb{Z}[S_3] & 
\rightarrow T^* & 
\rightarrow 0 \\
\downarrow & \downarrow \\
\mathbb{Z}[S_3/\langle \tau \rangle] & 
\rightarrow \mathbb{Z}[S_3/\langle \tau \rangle] \\
\downarrow & \downarrow \\
0 & 0 \\
\end{array}
\]

By commutativity, \( Q \to T^* \) factors via a permutation module, so \( \text{ed}(T) \leq \text{rank}(Q) - \text{rank}(T^*) = 1 \). To get a lower bound, we can compute the essential 3-dimension, but after a degree 2 extension \( T \) becomes isomorphic to a norm 1 torus. Thus, \( \text{ed}_3(T) = 1 \leq \text{ed}(T) \) as desired.

There are also two classes of tori split by a \( D_{12} \)-extension. Let \( T \) be

\[
1 \longrightarrow T \longrightarrow R_{KL/k}(\mathbb{G}_m) \longrightarrow R_{K/k}(\mathbb{G}_m) \times R_{L/k}(\mathbb{G}_m) \longrightarrow \mathbb{G}_m \longrightarrow 1
\]

where \( L/k \) is a degree 3 non-normal extension and \( K/k \) is a degree 2 extension. The other class of \( D_{12} \)-tori is the torus \( S \) dual to this one. Write \( D_{12} = S_3 \times S_2 = \langle \sigma \rangle \times \langle \tau \rangle \times \langle \rho \rangle \). It follows from the above that we get an exact sequence

\[
0 \longrightarrow M \longrightarrow \mathbb{Z}[D_{12}/\langle \tau \rangle] \longrightarrow T^* \longrightarrow 0
\]

where \( M = \langle \sigma^2 + \bar{\sigma} + \bar{1}, \bar{\rho} + \bar{1} \rangle \). Therefore, \( \text{ed}(T) \leq 4 \). Again, we can do better. The
augmentation map $P := \mathbb{Z}[D_{12}/\langle \tau \rangle] \rightarrow \mathbb{Z}$ yields a commutative diagram

$$
\begin{array}{ccccccccc}
0 & 0 & & & & & & & \\
\downarrow & & & & & & & & \\
0 & \rightarrow & N & \rightarrow & Q & \rightarrow & T^\ast & \rightarrow & 0 \\
\downarrow & & & & & & & & \\
0 & \rightarrow & M & \rightarrow & P & \rightarrow & T^\ast & \rightarrow & 0 \\
\downarrow & & & & & & & & \\
\mathbb{Z} & = & \mathbb{Z} & & & & & & \\
\downarrow & & & & & & & & \\
0 & 0 & & & & & & & \\
\end{array}
$$

and which shows, as in the $S_3$ case, that $ed(T) \leq 3$.

Now, we move on to lower bounds. Again, we use the essential $p$-dimension. After a degree 4 extension, $T$ becomes isomorphic to the norm one torus for a degree 3 cyclic extension which implies that $ed_3(T) = 1$. After base extension by $L$, $T_L \simeq R_{K/L}(\mathbb{G}_m)/\mathbb{G}_m \times R_{K/L}(\mathbb{G}_m)/\mathbb{G}_m$, and it is easy to see that such a group has essential dimension 2. Thus, $ed_2(T) = 2 \leq ed(T) \leq 3$. This is the smallest algebraic torus for which the essential dimension cannot be computed. The essential dimension of its dual, $S$, has a similar bounds.

### 3.3.3.2 Norm Tori and Valuation Descent

I want to extend the first example of the previous section to a slightly broader class of algebraic groups. These are the algebraic tori that are Weil restrictions of norm one tori:

$$
1 \rightarrow T \rightarrow R_{L/k}(\mathbb{G}_m) \rightarrow R_{L'/k}(\mathbb{G}_m) \rightarrow 1
$$

where $k \subset L' \subset L$ are both finite separable field extensions and the second map is induced by the norm homomorphism. In the sequel, I fix the following notations

$$
\mathcal{N} : K \mapsto K^\times/(N((L \otimes_k K)^\times))
$$

where $L/k$ is a degree $d$ field extension with norm $N$.

$$
\overline{\mathcal{N}} : K \mapsto (L' \otimes_k K)^\times/(N((L \otimes_k K)^\times))
$$
where \( L/L' \) is degree \( d' \) extension with norm \( N \) and \( L'/k \) is a \( d \) degree extension.

By Hilbert Theorem 90, \( \overline{\mathcal{N}} \cong H^1(-, T) \) where \( T \) is the torus above. Therefore, the essential dimension of this functor is the essential dimension of the group \( T \). Of course, \( \mathcal{N} \) is just the cohomology of a norm one torus, as computed in the examples of the previous section.

**Proposition 17.** \( \text{ed}_k(N^\times n = n) \)

**Proof.**

There is an obvious surjection from the functor \( \mathbb{G}_m^n \) to \( \mathcal{N} \), so the essential dimension is bounded above by \( n \). I will now construct an element that has essential dimension \( n \) to demonstrate the lower bound.

Choose the field extension \( K = k(t_1, ..., t_n) \) where the \( t_i \) are independent variables. Consider the element \( t = (t_1, ..., t_n) \in \mathcal{N}(K) \). This element is defined over a field of transcendence degree \( n \), namely \( K \). Suppose that \( t \) can be defined over a subfield \( k \subset k' \subset K \). That is, there are elements \( s_i \in K' \) such that \( s = (s_1, ...s_n) \) maps to \( t \) under the map \( \mathcal{N}(K') \to \mathcal{N}(K) \).

Write \( s_i = t_iN(x_i) \) for \( x_i \in L(t_1, ..., t_n) \). To show that the essential dimension of \( t \) is \( n \), it then suffices to show that \( \text{trdeg}_k(K') \geq n \). The argument is valuation theoretic.

Let \( \nu_i \) be the discrete valuation corresponding to the indeterminate \( t_i \) and denote by \( \nu : K \to \mathbb{Z}^n \) the composite valuation of all the \( \nu_i \), \( 1 \leq i \leq n \). I claim that the restriction, \( \nu' \), of this valuation to \( K' \) continues to have rank \( n \). For each \( i \), \( \nu'(s_i) = \nu'(t_i) + \nu'(N(x_i)) \).

Because it is the restriction of \( \nu \), \( \nu'(t_i) = e_i \in \mathbb{Z}^n \), the standard generating elements. The argument reduces to computing the valuation of the norm.

Let \( \omega_1, ..., \omega_d \) be a basis for the degree \( d \) extension \( L(t_1, ..., t_n)/k(t_1, ..., t_n) \). In this basis \( N(y_1\omega_1 + ... + y_d\omega_d) \) is a degree \( d \) homogeneous polynomial in the \( y_i \) with coefficients in \( k \). By definition, it is the determinant of the multiplication endomorphism associated to an element of \( L(t_1, ..., t_n)^\times \). This means in particular that the norm is not zero on any unit so that each term \( y_i^d \) appears with non-zero coefficient.

Take \( x = y_1\omega_1 + ... + y_d\omega_d \in L(t_1, ..., t_n)^\times \). Since the norm is multiplicative and any element of \( k(t_1, ..., t_n) \) can be written as a quotient of polynomials, we may assume that
$x \in L[t_1, \ldots, t_n]$. Consequently, $N(x)$ is also of this form. To compute $\nu'(N(x))$, we begin with multiples of $t_1$ thinking of the norm as a polynomial in $t_1$. If $t_1$ divides $N(x)$, then $t_1$ must appear as a term in at least one $y_i$. Write $y_i = a_i t_1 + b_i$ where $a_i \in L[t_1, \ldots, t_n]$ and $b_i \in L[t_2, \ldots, t_n]$. Then substituting into the norm, we see that every term is divisible by $t_1$ except for the term $N(b_1 \omega_1 + \ldots + b_n \omega_n)$. Since $t_1$ divides the entire norm and every term but this one, we must have that $N(b_1 \omega_1 + \ldots + b_n \omega_n) = 0$. This can only be the case if $b_i = 0$ for all $i$. Thus, every $y_i$ must be a multiple of $t_1$, and since the norm is homogeneous of degree $d$, the multiple of $t_1$ dividing the norm must be divisible by $d$.

If the norm is not divisible by $t_1$ then we set $t_1 = 0$ and look at multiples of $t_2$. Considering this as a polynomial in the last $n - 1$ variables, we repeat the process: either it is divisible by $t_2$ or not. In the former case, this power must again be a multiple of $d$ by the same argument as above. Continuing the computation inductively, we see that $\nu'(N(x)) \in d\mathbb{Z}^n$.

Combining with the original computation gives, $\nu'(t_i) = e_i \pmod{d}$. In particular, the rank of $\nu'$ modulo $d$ is $n$ and therefore also generally, as claimed. By [ZS75][VI Theorem 3 Corollary 1], we have $n = \text{rank}(\nu') \leq \text{trdeg}_k(K')$ demonstrating the lower bound of $n$ for the essential dimension.

\[ \square \]

**Remark 18.** Since the argument given in the proposition depended only on the homogeneity of the norm, it remains true even if $K$ is chosen to be $F(t_1, \ldots, t_n)$ for an algebraic extension $F/k$. This will allow us to conclude the same result for base extensions of this functor.

**Proposition 19.** $\text{ed}_k(\mathcal{N}^\times) = nd$

**Proof.**
We again have a surjection $\mathcal{R}_{L'/k}(G_m^\times) \to \mathcal{N}^\times$, which shows that the essential dimension is bounded above by $nd$. Consider the functor $\mathcal{N}$ defined over $L'$ instead of $k$. To avoid confusion we will denote it $\mathcal{F}$. Using Weil restriction, we can study this functor over $k$:

\[
\mathcal{R}_{L'/k}(\mathcal{F})(K) = \mathcal{F}(K \otimes_k L') = (K \otimes_k L')^\times / N((K \otimes_k L' \otimes_{L'} L)^\times) \\
= (K \otimes_k L')^\times / N((K \otimes_k L)^\times) = \mathcal{N}(K)
\]
That is, $\mathcal{N}$ is a Weil restriction of the functor $\mathcal{N}$. We will use this identification and our previous results to give the desired lower bound. By Proposition 7(1), it suffices to check that $\text{ed}_F(\mathcal{N}^\times)$ is at least $nd$ for any $F/k$. Define $\tilde{L}$ to be any finite separable extension of $L'$ that splits $L'$. Then we base extend $\mathcal{N}$ and compute the essential dimension:

$$(\mathcal{N}^\times)_L = (R_{L'/k}(\mathcal{F}^\times))_L \simeq (\mathcal{F}^\times)_L^\times nd.$$ 

Now, we conclude by the variant of the previous proposition mentioned in the remark. □

### 3.3.4 Essential Dimension of Finite Abelian Groups

Consider first the case of a cyclic $q$-group for $q = p^r$ a prime power. Let

$$G = \begin{cases} 
  
  \mathbb{Z}_{p-1} & \text{if } p \text{ is odd} \\
  1 & \text{if } p = 2 \text{ and } r = 1 \\
  \mathbb{Z}_{2^{r-2}} \times \mathbb{Z}_2 & \text{if } p = 2 \text{ and } r \neq 1
\end{cases}$$

be the automorphism group of $\mathbb{Z}_q$. The character module corresponding to the finite constant group scheme $\mathbb{Z}_q$ is $\mathbb{Z}/q\mathbb{Z}$ with $G$ acting by automorphisms. Following [Led02], we can construct a faithful permutation resolution to get the following upper bound.

**Theorem 20.** $\text{ed}_Q(\mathbb{Z}_{p^r}) \leq \phi(p - 1)p^{r-1}$.

**Proof.** First consider the case where $p$ is odd and let $X$ denote the set of $p^r$-th roots of unity and fix a primitive $p^r$-th root $\zeta$. $G = \langle \sigma \rangle$ acts by permutations on this set, so we get an exact sequence

$$0 \longrightarrow N \longrightarrow \mathbb{Z}[X] \xrightarrow{f} \mathbb{Z}/q\mathbb{Z} \longrightarrow 0$$

where $f(\zeta^n) = \bar{\pi}$.

Let

$$g(x) = \prod_{i=0}^{r-1} \Phi_{(p-1)p^i} \text{ and } h(x) = \prod_{i=0}^{r-1} \prod_{m<l(p-1)} \Phi_{mpl}$$

where $\Phi_d(x)$ is the $d$-th cyclotomic polynomial. Construct the $G$-module $Q = \mathbb{Z}[x]/\langle g(x) \rangle$ with $G$ acting via multiplication by $x$. Sending $\phi(x) \in Q$ to $\phi(x)h(x)$ is an inclusion of $Q$ into
\[ Z[x] = Z[x]/(x^{(p-1)p^{r-1}} - 1) \]. This \( G \)-module is in turn a submodule of \( Z[X] \) after identifying \( x^i \) with \( \sigma^i \zeta \). Moreover, the restriction of \( f \) to this sub-module remains a surjection, so this gives the desired faithful permutation representation of rank \( \phi(p - 1)p^{r-1} \).

If \( p = 2 \), it is well-known that \( Z_q \) has a faithful representation of degree \( q/2 = 2^{r-1} \). It is given by the map \( Z[G] \rightarrow Z/qZ \) which sends 1 to \( \mathbb{I} \). Note that for \( r = 1 \) this is just \( Z \) with the trivial action. This completes the proof. \( \square \)

Consider now the group \( Z_n = \mathbb{Z}_{p_1^{n_1} \ldots p_r^{n_r}} \). It follows from the primary decomposition theorem that

\[
\text{ed}_Q(Z_n) \leq \sum_i \text{ed}_Q(Z_{p_i^{n_i}}).
\]

This is the best known bound for a general cyclic group. My conjecture stated at the end of the previous section would imply that this is an equality. More generally, if a field \( F/Q \) contains the \( p_i^{m_i} \)-th roots of unity where \( m_i \leq n_i \). Set \( s_i = n_i - m_i \). There is an obvious exact sequence which gives a permutation representation.

\[
0 \rightarrow M \rightarrow \bigoplus \mathbb{Z}[\mathbb{Z}_{p_i^{s_i}}] \rightarrow Z_n \rightarrow 0
\]

Here \( \text{rank}(M) = \sum [F(\mu_{p_i^{n_i}}) : F] \).

For any pair of distinct primes \( p \) and \( q \), the sum of the augmentation maps gives a map \( P = \mathbb{Z}[\mathbb{Z}_{p^a}] \oplus \mathbb{Z}[\mathbb{Z}_{p^b}] \rightarrow \mathbb{Z} \) such that the following diagram commutes:

\[
\begin{array}{ccccccccc}
0 & \rightarrow & M & \rightarrow & \bigoplus \mathbb{Z}[\mathbb{Z}_{p_i^{s_i}}] & \rightarrow & Z_n & \rightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \rightarrow & N & \rightarrow & Q & \rightarrow & \mathbb{Z}_{p^aq^b} & \rightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \parallel & & \downarrow \\
0 & \rightarrow & M & \rightarrow & P & \rightarrow & \mathbb{Z}_{p^aq^b} & \rightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
\mathbb{Z} & \rightarrow & \mathbb{Z} & \rightarrow & \mathbb{Z} & \rightarrow & \mathbb{Z} & \rightarrow & \mathbb{Z} \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \rightarrow & 0 & \rightarrow & 0 & \rightarrow & 0 & \rightarrow & 0
\end{array}
\]

where the equality in the last rows follows since \( p \) and \( q \) are relatively prime.
Applying this same idea \( r - 1 \) times to our original exact sequence produces a resolution

\[
0 \rightarrow N \rightarrow Q \rightarrow \mathbb{Z}_n \rightarrow 0
\]

where \( Q \rightarrow \mathbb{Z}_n \) factors through a permutation module and \( \text{rank}(N) = \sum [F(\mu_{p_i^{n_i}}) : F] - (r-1) \)

which is exactly the result computed in [WW11]:

**Theorem 21.** If \( n = p_i^{n_i} \) and \( F \) is a field containing the \( p_i^{n_i} \)-th roots of unity then

\[
\text{ed}_F(\mathbb{Z}_n) \leq \sum_i [F(\mu_{p_i^{n_i}}) : F] - (r-1)
\]

I want to conclude this section by computing the known values of the essential dimension for small abelian groups.

### 3.3.4.1 Examples

**\( \mathbb{Z}_2, \mathbb{Z}_3 \):**

By Theorem 20, \( \text{ed}_\mathbb{Q}(\mathbb{Z}_2), \text{ed}_\mathbb{Q}(\mathbb{Z}_3) \leq \phi(1) = 1 \). Since the only finite group with essential dimension 0 is 1, \( \text{ed}_\mathbb{Q}(\mathbb{Z}_2) = \text{ed}_\mathbb{Q}(\mathbb{Z}_3) = 1 \).

**\( \mathbb{Z}_4 \):**

Let \( k/\mathbb{Q} \) be any field extension. Again by Theorem 20, \( \text{ed}_k(\mathbb{Z}_4) \leq 2 \). A finite group can have essential dimension 1 over \( k \) only if it is a subgroup of \( \text{PGL}_2(k) \) [BF03][Lemma 7.2]. For \( \mathbb{Z}_4 \), this happens precisely when \(-1\) is a square in \( k \). Therefore,

\[
\text{ed}_k(\mathbb{Z}_4) = \begin{cases} 1 & \text{if } -1 \text{ is a square in } k. \\ 2 & \text{otherwise.} \end{cases}
\]

**\( \mathbb{Z}_5 \):**

\( \text{ed}_\mathbb{Q}(\mathbb{Z}_5) \leq \phi(4) = 2 \), so again by [BF03][Lemma 7.2], it suffices to check whether or not \( \mathbb{Z}_5 \) is a subgroup of \( \text{PGL}_2(\mathbb{Q}) \). It is not which implies that \( \text{ed}_\mathbb{Q}(\mathbb{Z}_5) = 2 \).

**\( \mathbb{Z}_6 \):**

\( \text{ed}_\mathbb{Q}(\mathbb{Z}_6) = \text{ed}_\mathbb{Q}(\mathbb{Z}_2 \times \mathbb{Z}_3) \leq \text{ed}_\mathbb{Q}(\mathbb{Z}_2) + \text{ed}_\mathbb{Q}(\mathbb{Z}_3) = 2 \). Moreover, the essential dimension of an abelian group is always bounded below by its rank [BF03][Proposition 3.7]. Therefore \( \text{ed}_\mathbb{Q}(\mathbb{Z}_6) = 2 \).
$\mathbb{Z}_7$:

$\text{ed}_Q(\mathbb{Z}_7) \leq \phi(6) = 2$, and as in the $\mathbb{Z}_5$ case, $\text{ed}_Q(\mathbb{Z}_7) = 2$.

$\mathbb{Z}_8$:

$\text{ed}_Q(\mathbb{Z}_8) \leq \phi(2)2^2 = 4$. We compute the essential 2-dimension to get a lower bound. By Theorem 11, it suffices to produce a 2-faithful presentation $P \twoheadrightarrow \mathbb{Z}_8$ of minimal rank. If $\text{rank}(P) < 4$, then since $P$ cannot be fixed by the automorphism group, $P = \mathbb{Z} \oplus \mathbb{Z}[\text{Aut}(\mathbb{Z}_8)/\mathbb{Z}_2]$ or $P = \mathbb{Z}[\text{Aut}(\mathbb{Z}_8)/\mathbb{Z}_2]$, but it is easy to see that a generator of $\mathbb{Z}_8$ is not fixed by any subgroup of $\text{Aut}(\mathbb{Z}_8) = \mathbb{Z}_2 \times \mathbb{Z}_2$. Therefore, $\text{rank}(P) \geq 4$, and so $\text{ed}_Q(\mathbb{Z}_8) = 4$.

$\mathbb{Z}_9$:

$\text{ed}_Q(\mathbb{Z}_9) \leq \phi(2)3 = 3$. Again, using Theorem 11 the essential 3-dimension can be computed. After a degree 2 extension, $\text{Aut}(\mathbb{Z}_9) = \mathbb{Z}_3$, and it is clear that no generator of $\mathbb{Z}_9$ is fixed by the $\mathbb{Z}_3$-action. Thus, arguing as in the $\mathbb{Z}_8$ case, the rank of any 3-faithful presentation must be at least 3 which implies that $\text{ed}_Q(\mathbb{Z}_9) = 3$.

$\mathbb{Z}_{10}, \mathbb{Z}_{14}$:

By the above remarks, $\text{ed}_Q(\mathbb{Z}_{10}), \text{ed}_Q(\mathbb{Z}_{14}) \leq \phi(2) + \phi(4) = \phi(2) + \phi(7) = 3$. This is actually equal to the precise value as computed in [JLY02][Theorem 8.2.11].

$\mathbb{Z}_{11}$:

This is the first unknown prime power case. By Theorem 20, $\text{ed}_Q(\mathbb{Z}_{11}) \leq \phi(10) = 4$. I am not aware of any non-trivial lower bound for this problem.

$\mathbb{Z}_{12}$:

This is the first unknown composite case. It has bounds

$$2 \leq \text{ed}_Q(\mathbb{Z}_{12}) \leq 3$$

given by $\text{ed}(\mathbb{Z}_4)$ from below and by $\text{ed}(\mathbb{Z}_4) + \text{ed}(\mathbb{Z}_3)$ from above.
CHAPTER 4

Essential Dimension of $\text{PGL}_n$

In this chapter, I will compute some bounds on the essential $p$-dimension of $\text{PGL}_n$. Throughout, I will use the following notation

$$\text{Alg}_n(F) := \{\text{iso classes of CSAs over } F \text{ of degree } n\} = H^1(F, \text{PGL}_n)$$

General upper bounds for the essential dimension of $\text{Alg}_n$ have been computed

$$\text{ed}_F(\text{Alg}_n) \leq \begin{cases} 
\frac{(n-1)(n-2)}{2} & \text{if } n \geq 5 \text{ odd.} \\
n^2 - 3n + 1 & n \geq 4, F = F_{\text{sep}}, \text{char}(F) = 0.
\end{cases}$$

For references to the above results as well as an overview of what is known see [AAV10]. Unfortunately, these upper bounds differ substantially from the best known lower bounds given by the essential $p$-dimension. Moreover, even computing the essential $p$-dimension is a difficult and mostly unsolved problem. There is one nice break however. Because we can apply primary decomposition to central simple algebras, the computation of $\text{ed}(\text{Alg}_n(-); p)$ reduces to a computation of $\text{ed}(\text{Alg}_{p^s}(-); p)$ where $p^s$ is the largest power of $p$ dividing $n$.

For $s = 1$, over a prime to $p$ extension, every non-trivial degree $p$ central simple algebra is isomorphic to a cyclic algebra (see Proposition 3). Since such an algebra is described by a field element and a cyclic extension, $\text{ed}(\text{Alg}_p; p) \leq 1 + \text{ed}_p(Z_p) = 2$. In fact, this is the precise value since, after base extending to $F' = F_{\text{alg}}$, there can be no non-trivial division algebras over $F'(x)$ by Tsen’s theorem. For $s = 2$, Merkurjev [Mer10a] showed that $\text{ed}(\text{Alg}_{p^2}; p) = p^2 + 1$, but the proof is far more involved (see the discussion at the end of this chapter).

In 2009, Meyer and Reichstein gave an upper bound for the case $s \geq 2$ [MR11][Theorem
1.1]:

\[ \text{ed}(\text{Alg}_{p^s}; p) \leq 2p^{2s-2} - p^s + 1 \]

The goal of this chapter is to show that even though this bound agrees with the actual value in the case \( s = 2 \), it can be improved for larger values of \( s \):

**Theorem 22.**\([Ruo11]\) \( \text{ed}(\text{Alg}_{p^s}; p) \leq p^{2s-2} + 1 \) for \( s \geq 2 \).

### 4.1 The Setup

Let \( \phi : S \to T \) be a map of split algebraic tori defined over \( F \), and suppose that we have a finite group \( G \) acting on \( S \) and \( T \) by automorphisms so that \( \phi \) is \( G \)-equivariant. Then by the usual anti-equivalence of categories (Theorem 6), there is an induced map of \( G \)-modules \( T^* \to S^* \) where \( T^* \) denotes the character group of the torus \( T \).

Let \( T \) be a split maximal torus in \( \text{PGL}_n(F) \). \( T \) can be viewed a quotient of \( S = G^*_m \) by the diagonal elements. If we are given a \( G \) as above, then letting \( I \) denote the character module of \( T \) with \( G \)-action, we obtain an exact sequence of \( G \)-modules:

\[
0 \to I \to \mathbb{Z}[X] \to \mathbb{Z} \to 0
\]

where \( X \) is a \( G \)-set of \( n \) elements.

Construct any \( G \)-module resolution of \( I \)

\[
0 \to M \to P \to I \to 0
\]

where \( P \) is a permutation module.

Now, fixing bases and using the anti-equivalence of categories, this sequence corresponds to an exact sequence of split algebraic tori/\( F \) with \( G \) acting by automorphisms

\[
1 \to T \to U \to S \to 1
\]

Let \( B \) be a basis of \( P \) permuted by \( G \) and let \( V \) be the vector space \( k^{|B|} \) with the corresponding action by \( G \). Then \( U = \text{Spec} \ k \otimes P \) embeds as the diagonal in \( GL(V) \). Thus we have a faithful representation \( T \hookrightarrow GL(V) \).
Since $T$ acts on $V$ via this representation, $G$ acts on $V$ by automorphisms, and the above representation is $G$-equivariant, this extends to a representation $T \rtimes G \to \text{GL}(V)$. I will construct an upper bound for the essential dimension using the following useful result:

**Theorem 23.** If $G$ acts faithfully on $M$ in the resolution of $I$ constructed above, then $\text{ed}(T \rtimes G) \leq \text{rank}(P) - \text{rank}(I) = \text{rank}(M)$.

**Proof.** [MR09][Lemma 3.3] It suffices by Section 3.3 to exhibit a generically free $T \rtimes G$-representation of dimension $\text{rank}(M)$. I claim that $V$ is the desired representation. First, $U$ is a dense open subvariety in $V$. In particular, $T \rtimes G$ acts generically freely on $V$ if and only if it does so on $U$. Moreover, $T \hookrightarrow U$, so $T$ acts faithfully (and thus generically freely) on $U$ by definition. For the $T \rtimes G$ action to be generically free, it suffices to show now that $G$ acts faithfully on $U/T$, but this is exactly the torus corresponding to $M$.

Thus, $V$ is a generically free representation and

$$\text{ed}(T \rtimes G) \leq \dim(V) - \dim(T) = \text{rank}(P) - \text{rank}(I) = \text{rank}(M).$$

One final result about the essential $p$-dimension of algebraic groups will be useful in the next section:

**Proposition 24.** Let $H = \text{Syl}_p(G)$. Then $\text{ed}(T \rtimes G; p) = \text{ed}(T \rtimes H; p)$.

**Proof.** This is just a special case of [MR09][Lemma 4.1].

### 4.2 An Upper Bound

Let $A$ be a central simple algebra over $F$ of degree $p^s$ with $s \geq 2$. By Corollary 2.5, there exists a maximal étale subalgebra $K = K_1 \otimes K_2$ where $K_1$ is étale of degree $p$ and $K_2$ is étale of degree $p^{s-1}$.

The main idea is to consider the functor $H^1(\_, S_n)$ which classifies $n$-dimensional étale algebras up to isomorphism [KMRT98][Section 29.9]. Let $G = S_p \times S_{p-1}$. We have the usual
isomorphism

\[ H^1(F, S_p) \times H^1(F, S_{p^{s-1}}) \to H^1(F, G). \]

Converting this to the language of algebras, \( H^1(F, G) \) can be identified as pairs \((L_1, L_2)\) of étale algebras of dimensions \( p \) and \( p^{s-1} \), respectively. If \( S_p \) acts on a set \( Y \) of \( p \) elements and \( S_{p^{s-1}} \) acts on a set \( Z \) of \( p^{s-1} \) elements, then \( G \) acts on the product \( Y \times Z \), where \( S_p \) permutes the first factor and \( S_{p^{s-1}} \) permutes the second. This yields an inclusion

\[ H^1(F, G) \to H^1(F, S_{p^s}) \]

which sends the pair \((L_1, L_2)\) to the étale algebra \( L_1 \otimes L_2 \). Using these identifications, the maximal étale algebra \( K \subset A \) can be viewed as an element of \( H^1(F, G) \).

Consider the split torus \( T \) for \( G \) as above and \( X \) a \( G \)-set of \( p^s \) elements. For its cohomology group, we have a disjoint union of fibers

\[ H^1(F, T \rtimes G) = \bigsqcup_{\gamma \in H^1(F, G)} H^1(F, T_{\gamma})/G_{\gamma}^\Gamma \]

where \( T_{\gamma} \) denotes \( T \) with action twisted by the cocycle \( \gamma \) and \( \Gamma = \text{Gal}(F_{\text{sep}}/F) \) [KMRT 28.C]. \( T_{\gamma} \) is also a torus with character module \( I \). In particular, if \( X \) corresponds to a \( p^s \)-dimensional étale algebra \( N \) represented by \( \gamma \) then the usual anti-equivalence of categories gives an exact sequence

\[ 1 \to \mathbb{G}_m \to R_{N/F}(\mathbb{G}_{m,N}) \to T_{\gamma} \to 1. \]

Passing to cohomology and applying Hilbert theorem 90 gives

\[ 1 \to H^1(F, T_{\gamma}) \to H^2(F, \mathbb{G}_m) \to H^2(F, R_{N/F}(\mathbb{G}_m)) \]

showing that \( H^1(F, T_{\gamma}) \simeq \text{Br}(N/F) \). Now, \( G_{\gamma}^\Gamma \) acts on \( \mathbb{G}_m \) trivially, so given \( g \in G_{\gamma}^\Gamma \), we get a diagram:

\[
\begin{array}{ccc}
1 & \longrightarrow & H^1(F, T_{\gamma}) & \longrightarrow & H^2(F, \mathbb{G}_m) \\
& & \downarrow g & & \parallel \\
1 & \longrightarrow & H^1(F, T_{\gamma}) & \longrightarrow & H^2(F, \mathbb{G}_m)
\end{array}
\]
and the commutativity implies that the action of \( g \) must be trivial for all \( g \in G \). Combining these observations with the above,

\[
H^1(F, T \rtimes G) = \prod_N \text{Br}(N/F),
\]

and thus we can define a map \( \phi_G(F) : H^1(F, T \rtimes G) \to \text{Alg}_{p^s}(F) \) which sends \([B] \in \text{Br}(N/F)\) to the unique (up to isomorphism) \( C \sim B \) with degree \( C = p^s \). Since any \( A \in \text{Alg}_{p^s} \) is split over \( L = L_1 \otimes L_2 \), it is in the image of this map. I have proven:

**Proposition 25.** \( \phi_G \) is \( p \)-surjective.

Let \( G_s = \text{Syl}_p(S_p \times S_{p^{s-1}}) = \text{Syl}_p(S_p) \times \text{Syl}_p(S_{p^{s-1}}) =: \Sigma_1 \times \Sigma_{s-1} \). Using Proposition 24 and the property of \( p \)-surjective maps (see Section 2.1),

\[
\text{ed}_k(T \rtimes G_s; p) = \text{ed}_k(T \rtimes (S_p \times S_{p^{s-1}}); p) \geq \text{ed}_k(\text{Alg}_{p^s}(-); p).
\]

4.2.0.2 The Computation

The computation of the upper bound is now reduced to that of the essential dimension of \( T \rtimes G_s \). By the above remarks, this requires finding a faithful \( G_s \)-module, \( M \), in a resolution of \( I \) of smallest rank. In what follows, we denote \( G_s = \Sigma_{s-1} \times \mathbb{Z}/p = \Sigma_{s-1} \times \langle \sigma \rangle \), where as above \( \Sigma_s = \text{Syl}_p(S_{p^s}) \).

First observe that \( G_s \) acts by permutation on a set \( X_s \) of \( p^s \) elements. Rewriting \( X_s = Y_s \times Z_s \) for \( Y_s \) a set of \( p \) elements and \( Z_s \) a set of \( p^{s-1} \) elements, this action can be described as an action of \( \mathbb{Z}/p \) on \( Y_s \) and an action of \( \Sigma_{s-1} \) on \( Z_s \). In particular, the action is transitive, so if \( H_s = \text{Stab}(y, z) \) for some \( (y, z) \in X_s \), then \( X_s \simeq G_s/H_s \) as \( G_s \)-sets.

Let \( \tau \in \Sigma_{s-1} \) be any \( p^{s-1} \) cycle. Then \( G_s \) is generated by \( \sigma, \tau \), and the elements of \( H_s \). \( I \) is then generated by \( \sigma x - x \) and \( \tau x - x \); [MR11][proof of Theorem 4.1]. Set \( H'_s = \tau H \tau^{-1} \). It is the subgroup of \( G_s \) that acts trivially on the element \( \tau x - x \). This allows us to define a surjective morphism

\[
\mathbb{Z}[G_s/H_s] \oplus \mathbb{Z}[G_s/H'_s] \to I
\]
by sending a generator of the first summand to $\sigma x - x$ and a generator of the second to $\tau x - x$. Because

$$[G_s : H'_s] = [G_s : H_s][H_s : H'_s] = p^s \cdot p^{s-2}$$

this map has kernel $M$ with

$$\text{rank}(M) = \text{rank}(\mathbb{Z}[G_s/H_s]) + \text{rank}(\mathbb{Z}[G_s/H'_s]) - \text{rank}(I)$$

$$= p^s + p^{s+(s-2)} - (p^s - 1)$$

$$= p^{2s-2} + 1.$$

To use Theorem 23, it remains to show that the $G_s$-action on $M$ is faithful (cf. [MR Lemma 3.2] for a more general argument). Faithfulness can be checked over $\mathbb{Q}$, so we have the split exact sequences:

$$0 \to I \otimes \mathbb{Q} \to \mathbb{Q}[G_s/H_s] \to \mathbb{Q} \to 0$$

$$0 \to N \to \mathbb{Q}[G_s/H'_s] \to \mathbb{Q}[G_s/H_s] \to 0$$

$$0 \to M \otimes \mathbb{Q} \to \mathbb{Q}[G_s/H_s] \oplus \mathbb{Q}[G_s/H'_s] \to I \otimes \mathbb{Q} \to 0$$

Combining these together,

$$(M \otimes \mathbb{Q}) \oplus (I \otimes \mathbb{Q}) \simeq \mathbb{Q}[G_s/H_s] \oplus \mathbb{Q}[G_s/H'_s]$$

$$\simeq \mathbb{Q}[G_s/H_s] \oplus N \oplus \mathbb{Q}[G_s/H_s]$$

$$\simeq \mathbb{Q}[G_s/H_s] \oplus N \oplus \mathbb{Q} \oplus (I \otimes \mathbb{Q}).$$

Therefore, $\mathbb{Q}[G_s/H_s]$ is a direct summand of $M \otimes \mathbb{Q}$, so it suffices to check that the $G_s$ action on $\mathbb{Q}[G_s/H_s]$ is faithful. However, if the coset $gH_s$ is fixed by every element in $G_s$, then $g \in \bigcap_{g_s \in G_s} g_sH_sg_s^{-1}$. A quick induction argument shows that for all $s \geq 2$ this group is trivial.
4.3 A Lower Bound and Some Consequences

Merkurjev [Mer10b] has given a lower bound for the essential $p$-dimension problem:

$$ed_p(\text{Alg}_{p^s}) \geq (s - 1)p^s + 1 \text{ for } s \geq 2.$$ 

Taken together with the upper bound of the previous section, it follows that $ed_p(\text{Alg}_{p^2}) = p^2 + 1$. However, for larger values of $s$ the bounds are quite different. I also remark that the argument used in Merkurjev’s paper is a valuation descent argument which reduces the problem inductively to the computation of the essential $p$-dimension of a torus.

One other interesting consequence of these bounds is that for $s = 3$ and $p = 2$ they also coincide to give $ed_2(\text{Alg}_8) = 17$. In this case, Merkurjev’s lower bound is based on a calculation for $(\mathbb{Z}/2\mathbb{Z})^3$ crossed product algebras, so the equality implies that the essential dimension can be calculated using crossed products. However, Amitsur showed that there are non-crossed product algebras of degree 8 [Ami72].
References


