Essential Dimension of Algebraic Groups

by

Aurel Nathan Meyer

B.Sc., The University of Basel, 2004
M.Sc., The University of British Columbia, 2006

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

in

The Faculty of Graduate Studies

(Mathematics)

THE UNIVERSITY OF BRITISH COLUMBIA

(Vancouver)

August 2010

© Aurel Nathan Meyer 2010
Abstract

We study the essential dimension of linear algebraic groups.

For a group $G$, essential dimension is a measure for the complexity of $G$-torsors or, more generally, the complexity of any algebraic or geometric structure with automorphism group $G$. This makes essential dimension a powerful invariant with many interesting and surprising connections to problems in algebra and geometry.

We show that for various classes of groups, including finite (algebraic) groups and algebraic tori, the essential dimension is related to minimal faithful representations. In many cases this renders the exact value of the essential dimension computable and we explore several of its consequences.

An important open problem is the essential dimension of the projective linear group $\text{PGL}_n$. This topic is closely related to the structure theory of central simple algebras, which may be viewed as twisted forms of the algebra of $n \times n$ matrices. We study central simple algebras with additional structure such as a distinguished Galois subfield. We prove new bounds on the essential dimension of these algebras and, as a corollary, of the group $\text{PGL}_n$. 
Preface

The following results in this thesis were obtained in joint work and are published or submitted for publication. The results are reproduced in this thesis with permission from the coauthors and journals. All work involved in these publications was shared in equal parts between the authors.

From [MR09a], coauthor: Z. Reichstein.
- A variant of Theorem 5.2.
- Most of Chapter 9, in particular the main Theorem 9.1.

From [MR08], coauthor: Z. Reichstein.
- Theorem 5.4.
- Most of Chapter 6, in particular the main results Theorem 6.1 and 6.3.
- Theorem 7.1.

From [MR09b], coauthor: Z. Reichstein.
- Theorems 10.1, 11.2. Sections 10.2, 10.3, 10.4.

From [LMMR09], coauthors: R. Lötscher, M. MacDonald, Z. Reichstein.
- Chapters 4, Sections 5.1 and 5.3.
- Most of Chapter 8, in particular Theorems 8.1, 8.5, 8.6, 8.8 and variants of Theorems 8.3, 8.4.
Table of Contents

Abstract ................................................................. ii
Preface ................................................................. iii
Table of Contents ..................................................... iv
List of Tables ........................................................ vi
List of Symbols ...................................................... vii
Acknowledgements ................................................... ix

1 Introduction ........................................................ 1
  1.1 Essential Dimension - Definitions ............................. 2
  1.2 Overview ......................................................... 5

2 Preliminaries ....................................................... 8
  2.1 Algebraic Groups ............................................... 8
  2.2 Finite Groups .................................................. 8
  2.3 Extensions ...................................................... 9
  2.4 Unipotent Groups, Passage to Reductive Groups .......... 10
  2.5 Algebraic Tori, Characters, Lattices ......................... 11
  2.6 (FT)-Groups .................................................... 13
  2.7 (Semi-)Simple Groups ......................................... 15

3 Actions, Representations, Lattices ............................. 16
  3.1 Faithful and Generically Free Actions ....................... 16
  3.2 Geometric Interpretation of Essential Dimension .......... 19
  3.3 Representations of (FT)-Groups ............................... 21

4 The $p$-Closure of a Field ......................................... 26
5 Group Extensions ................................................................. 30
  5.1 $p$-Isogenies ............................................................... 30
  5.2 Groups of Index Prime to $p$ ............................................ 32
  5.3 Direct Products ........................................................... 35
  5.4 Quotients of Large Essential Dimension ......................... 36

6 Finite Groups ........................................................................ 38
  6.1 Essential Dimension of Finite Constant $p$-Groups ............... 38
  6.2 $p$-Groups of Essential Dimension $\leq p$ ......................... 44

7 GL($\mathbb{Z}$) and SL($\mathbb{Z}$) .................................................. 46
  7.1 Forms of Algebraic Groups .............................................. 46
  7.2 Forms of Algebraic Tori .................................................. 46

8 Algebraic Tori ........................................................................ 51
  8.1 A Lower Bound ............................................................... 51
  8.2 $p$-(FT)-Groups .............................................................. 53
  8.3 The Central Split Group $C(G)$ ......................................... 56
  8.4 Proof of Theorem 8.2 (a) and (b) ........................................ 58
  8.5 Proof of the Additivity Theorem ........................................ 62
  8.6 Proof of Theorem 8.2 (c) ................................................... 64
  8.7 Tori of Essential Dimension $\leq 1$ ..................................... 65
  8.8 Tori Split by Cyclic Extensions of Degree Dividing $p^2$ ...... 68

9 Normalizers of Maximal Tori ................................................... 73
  9.1 First Reductions and Proof of Theorem 9.1 Parts (a) and (b) .. 75
  9.2 Proof of Theorem 9.1 Part (c) ............................................ 77
  9.3 Proof of Theorem 9.1 Part (d) ............................................ 81

10 Central Simple Algebras ........................................................ 84
  10.1 Crossed Products, Splitting Groups and Fields .................... 86
  10.2 $G$-Lattices ................................................................. 89
  10.3 An Upper Bound ............................................................ 91
  10.4 Proofs of Theorems 10.1 and 10.2 ................................. 93

11 The Projective Linear Group $\text{PGL}_n$ .................................... 95

Bibliography .............................................................................. 99
List of Tables

2.1 Dictionary of the anti-equivalence Diag. ......................... 12
8.1 Indecomposable \(\mathbb{Z}C_{p^2}\)-lattices. ............................. 69
8.2 Essential dimension of tori split by \(C_{p^2}\). ....................... 71
8.3 Permutation ranks for lattices \(M_7-M_{12}\). ....................... 72
11.1 Essential dimension of \(\text{PGL}_m\). ............................... 96
11.2 Essential \(p\)-dimension of \(\text{PGL}_m\). ......................... 97
# List of Symbols

- $k$: base field
- $K/k$: field extension of $k$
- $K_{\text{alg}}$: algebraic closure of the field $K$
- $K_{\text{sep}}$: separable closure of the field $K$
- $K^{(p)}$: $p$-closure of the field $K$, for a prime number $p$
- $\text{Fields}/k$: category of field extensions of $k$
- $\text{Algebras}/k$: category of commutative $k$-algebras with identity
- $\text{Sets}$: category of sets
- $\text{Groups}$: category of groups
- $\text{ed}(\ast)$: essential dimension of $\ast$
- $\text{ed}(\ast; p)$: essential $p$-dimension of $\ast$
- $\text{Diag}(M)$: group of multiplicative type corresponding to $M$
- $X(G)$: character module of the group $G$
- $\Gamma = \text{Gal}(K_{\text{sep}}/K)$: absolute Galois group

## Groups:
- $G_a$: additive group
- $G_m$: multiplicative group
- $\text{GL}_n$: split general linear group
- $\text{SL}_n$: split special linear group
- $\text{Sp}_{2n}$: split symplectic linear group
- $O_n$: split orthogonal linear group
- $\text{PGL}_n$: split projective linear group
- $\mu_n$: group of $n$th roots of unity
- $C_n$: cyclic group of order $n$
- $S_n$: symmetric group in $n$ letters
- $P_n$: Sylow-$p$ subgroup of $S_n$
- $G^0$: connected component of the group $G$
- $\pi_0 G$: étale quotient of the group $G$
- $R_u G$: unipotent radical of $G$
\( (\text{FT})\)-group \( \text{extension of a finite group by a torus} \)
\( (\text{FxT})\)-group \( \text{product of a torus and a finite group} \)

**Algebras:**

- \( \text{UD}(n) \) \( \text{universal division algebra of degree } n \)
- \( \text{M}_n \) \( \text{matrix algebra of degree } n \)

**Functors:**

- \( \text{H}^1(\ast, G) \) \( \text{Galois cohomology} \)
- \( \text{Tors}_G \) \( \text{G-torsors} \)
- \( \text{Forms}_G \) \( \text{forms of } G \)
- \( \text{Et}_n \) \( \text{degree } n \text{ étale algebras} \)
- \( \text{Gal}_G \) \( \text{G-Galois algebras} \)
- \( \text{Tori}_n \) \( \text{n-dimensional tori} \)
- \( \text{CSA}_n \) \( \text{central simple algebras of degree } n \)
- \( \text{CP}_{G/H} \) \( \text{G/H-crossed product algebras} \)
- \( \text{Split}_{n,G} \) \( \text{n-dimensional algebras split by the group } G \)
- \( \text{Split}_{n,E/k} \) \( \text{n-dimensional algebras split by the extension } E/k \)
- \( \text{Pairs}_{n,G} \) \( \text{pairs of an algebra and a splitting field with group } G \)
Acknowledgements

First and foremost I would like to thank my advisor Zinovy Reichstein for all he has done for me; for the abundance of ideas he has introduced me to and for his constant support and advice in all academic matters.

I would also like to thank my teachers and committee members Kai Behrend, Patrick Brosnan, Jim Carrell and Kalle Karu, my coauthors Roland L"otscher and Mark MacDonald and fellow graduate student Alex Duncan for all I have learnt from them.

Finally I thank the mathematics community and department at UBC for providing an excellent learning and working environment and making my stay very enjoyable.
1

Introduction

It is a fundamental problem in algebra to understand the complexity of its objects and structures and to classify them according to certain invariants. Natural examples of such invariants include the dimension of a vector space, the order of a finite group, the transcendence degree of a field extension or the exponent of a central simple algebra. In this thesis we study another such invariant and measure of complexity, called essential dimension.

Let $A$ be an algebraic object or structure. The essential dimension of $A$, denoted by $\text{ed}(A)$, is usually explained informally as

$$\text{ed}(A) = \text{minimal number of parameters needed to define } A.$$ 

The algebraic object or structure here could be almost anything in algebra or algebraic geometry. For example,

$A$ = an algebraic group, a torsor, a variety or scheme, a quadratic form, a Galois field extension, an (associative, central simple, étale) algebra, or any set which is associated in a functorial way to a field.

In the next section we will make precise what we mean by “algebraic object or structure” and define essential dimension via certain functors, see Definitions 1.1 and 1.2.

We will also study a variant of essential dimension which is called essential $p$-dimension, where $p$ is a prime number. As essential dimension is a measure of how complex the structure $A$ is, essential $p$-dimension captures this information locally or relatively to the prime $p$. Essential $p$-dimension is denoted by $\text{ed}(A; p)$ and will be defined in Definitions 1.3 and 1.4.

Essential dimension arises in many natural settings, in particular, in connection with some classical open problems, such as Hilbert’s 13th problem (algebraic version), the cyclicity problem for division algebras (Albert’s conjecture) or Serre’s Conjecture II.

The notion of essential dimension was first introduced by J. Buhler and Z. Reichstein for finite groups [BR97] and for algebraic groups by Reichstein [Rei00]. The functorial definition of essential dimension which we will use is due to A. Merkurjev [BF03].
1.1 Essential Dimension - Definitions

In what follows, \( k \) denotes a fixed base field and \( p \) a prime number. All fields will be assumed to be extensions of \( k \). We denote by \( K_{\text{sep}} \) a separable closure and by \( K_{\text{alg}} \) an algebraic closure of the field \( K \).

Let
\[
\mathcal{F}: \text{Fields}/k \to \text{Sets}
\]
be a covariant functor from the category of field extensions \( K/k \) to the category of sets. The functor \( \mathcal{F} \) formalizes what we mean by “algebraic structure” and the objects in \( \mathcal{F}(K) \) what we mean by “algebraic object”. Before we define the essential dimension of \( \mathcal{F} \), let us give some natural examples of such functors (see also the list in [BF03, Example 1.1]).

Examples 1.1.
(a) Let \( X \) be a scheme over \( \text{Spec} k \). It is a functor \( \text{Fields}/k \to \text{Sets} \) defined as
\[
X(K) = \text{Mor} (\text{Spec} K, X) = \{ K\text{-rational points of } X \}.
\]
(b) Let \( G \) be a linear algebraic group. Define a functor
\[
\mathcal{T}_{\text{tors}}_G: \text{Fields}/k \to \text{Sets}
\]
\[
K \mapsto \{ G\text{-torsors over } K \}/\simeq
\]
See Section 3.2 for the definition of a torsor.

(c) Let \( G \) be a group scheme over \( k \). Define \( H^1(K, G) := H^1(\Gamma, G(K_{\text{sep}})) \), where \( \Gamma = \text{Gal}(K_{\text{sep}}/K) \) the absolute Galois group of \( K \) and \( K_{\text{sep}} \) a separable closure. \( H^1(*, G) \) is called the Galois cohomology functor. If \( G \) is a smooth algebraic group, there is a well known equivalence (cf. Section 3.2) of \( \mathcal{T}_{\text{tors}}_G \) and the Galois cohomology functor
\[
\mathcal{T}_{\text{tors}}_G \simeq H^1(*, G).
\]
(d) Define a functor \( \mathcal{CSA}_n : \text{Fields}/k \to \text{Sets} \)
\[
K \mapsto \{ \text{central simple } K\text{-algebras of degree } n \}/\simeq
\]
There are well known equivalences \( \mathcal{CSA}_n \simeq \mathcal{T}_{\text{tors}}_{\text{PGL}_n} \simeq H^1(*, \text{PGL}_n) \), where \( \text{PGL}_n \) is the projective linear group, cf. [KMRT98, VII 29] and Chapter 10.

(e) The functor \( \text{Br} : \text{Fields}/k \to \text{Sets} \) defined by \( \text{Br}(K) = \text{Brauer group of } K \).
Let \( \text{Curves}_g : \text{Fields}/k \to \text{Sets} \) be defined as
\[
\text{Curves}_g(K) = \{\text{isom. classes of smooth curves of genus } g\}.
\]

Let \( \alpha \in \mathfrak{F}(K) \) be an object for some functor \( \mathfrak{F} : \text{Fields}/k \to \text{Sets} \). If \( K_0 \) is a subfield of \( K \) (over \( k \)) and \( \alpha \) is in the image of the functorial map \( \mathfrak{F}(K_0) \to \mathfrak{F}(K) \), we say that \( \alpha \) is defined over \( K_0 \). Essential dimension measures the “smallest” field where \( \alpha \) can be defined over:

**Definition 1.1.**
\[
ed(\alpha) = \min \{\text{trdeg}_k K_0 \mid \alpha \in \operatorname{Im}(\mathfrak{F}(K_0) \to \mathfrak{F}(K))\}
\]

The essential dimension of the functor \( \mathfrak{F} \) is defined to be the maximum of essential dimensions of objects taken over all \( \alpha \in \mathfrak{F}(K) \) and all fields \( K/k \):

**Definition 1.2.**
\[
ed(\mathfrak{F}) = \max \{\text{ed}(\alpha) \mid \alpha \in \mathfrak{F}(K)\}
\]

**Example 1.1.** Suppose \( k \) contains an \( n \)-th root of unity \( \xi_n \) and \( \operatorname{char} k \nmid n \). If \( a, b \in K \) for some \( K/k \), let \( A \in \mathcal{CS} A_n(K) \) be the (isomorphism class of) the cyclic algebra
\[
A = \langle x, y \mid x^n = a, y^n = b, xy = yx \xi_n \rangle
\]
It is clear that \( A \) is defined over \( K_0 = k(a, b) \) and so \( \text{ed}(A) \leq 2 \) (in fact, equality holds if \( a, b \) are algebraically independent over \( k \), cf. [Rei00, 9.2]).

**Example 1.2.** Let \( X \) be the functor of rational points of an integral scheme 1.1 (a). The generic point \( x \) of \( X \) has maximal essential dimension and \( \text{ed}(X) = \text{ed}(x) = \text{trdeg}_k k(x) = \dim X \), [Mer09].

**Remark.** The definition of essential dimension depends on the base field \( k \). Sometimes we write \( \text{ed}_k \) instead of \( \text{ed} \) to emphasize that fact but whenever the context is clear we will omit it. One has the obvious inequality
\[
\text{ed}_k(*) \geq \text{ed}_{k'}(*) \quad \text{if } k \subset k'.
\]

A variant of essential dimension is essential dimension relative to a prime \( p \) (also called essential dimension at \( p \) or essential \( p \)-dimension):

Again, let \( \alpha \in \mathfrak{F}(K) \) be an object. We allow first to pass to a finite field extension \( L/K \) of degree \( [L : K] \) prime to \( p \). Denote by \( \alpha_L \) the image of \( \alpha \) under the natural map \( \mathfrak{F}(K) \to \mathfrak{F}(L) \).
Definition 1.3. The essential $p$-dimension of $\alpha$ is

$$\text{ed}(\alpha; p) = \min \{ \text{ed}(\alpha_L) \mid L/K \text{ finite of degree prime to } p \}$$

In other words, we take the minimum trdeg$_k L_0$ over all finite prime to $p$ extensions $L/K$ for which there exists a diagram

$$\begin{array}{ccc}
\alpha_L & \in & \mathcal{Z}(L) \\
\searrow & \swarrow & \nwarrow \\
\mathcal{Z}(K) \supseteq & \alpha_K & \in \mathcal{Z}(L_0)
\end{array} \quad (1.2)
$$

As before, the essential $p$-dimension of the functor $\mathcal{Z}$ is the maximum of these numbers taken over all $\alpha \in \mathcal{Z}(K)$ and all fields $K/k$:

Definition 1.4.

$$\text{ed}(\mathcal{Z}; p) = \max \text{ed}(\alpha; p).$$

Our main focus will be on (torsors of) algebraic groups. The essential dimension of an algebraic group (or more generally group scheme) $G$ over $k$ is defined to be the essential dimension of the functor $\mathcal{Tors}_G$:

Definition 1.5.

$$\text{ed}(G) := \text{ed}(\mathcal{Tors}_G), \quad \text{ed}_p(G) := \text{ed}_p(\mathcal{Tors}_G).$$

For example, if $k$ is an algebraically closed field of characteristic 0 then groups $G$ of essential dimension 0 are precisely the so-called special groups, i.e., algebraic groups $G/k$ with the property that every $G$-torsor over Spec($K$) is split, for every field $K/k$. These groups were classified by A. Grothendieck [Gro58], see also [Rei00, 5.2].

Remark. In Chapter 3.2 we will give a more geometric interpretation of essential dimension of algebraic groups and torsors. We refer to the following sources: The original papers introducing essential dimension for finite and algebraic groups are [BR97] and [Rei00]. Definitions 1.1 and 1.2 were first used in [BF03]. Essential $p$-dimension appeared first in [RY00]. A good introduction to essential dimension can also be found in [Rei10] or [Mer08].
1.2 Overview

We outline the topic and results of this thesis. Essential dimension was defined in the previous section and some of the relevant notions (such as affine algebraic group, torus, lattice, etc.) will be explained in the preliminary Chapter 2.

In Chapter 4 we define the $p$-closure of a field and discuss its properties with respect to essential dimension. The $p$-closure is an important technical tool which removes some of the difficulties in choosing a prime to $p$ field extension in the definition of essential $p$-dimension.

Ultimately we would like to be able to find the essential dimension of any given affine algebraic group. In this generality the project is far beyond our scope but as usual in mathematics, we divide it into smaller projects which are more manageable.

We study groups with special properties such as finite groups, unipotent groups, algebraic tori or simple groups. From two such groups $G_1, G_2$ a new group $G$ is obtained as an extension, i.e. a short exact sequence

$$1 \to G_1 \to G \to G_2 \to 1$$

Any affine algebraic group is built up this way and one could set the following program:

Determine the essential dimension of

(a) finite groups,

(b) unipotent groups,

(c) algebraic tori,

(d) simple groups.

(e) Determine the behaviour of essential dimension in short exact sequences.

In part (e), a simple general formula relating the essential dimensions of the groups in a short exact sequence seems to be out of reach. However, if one makes additional assumptions on the groups or the extension (such as being a direct product) some partial results can be proved, see Chapter 5.

Regardless of the limitations imposed by the lack of a general formula in part (e), it is natural to try to find the essential dimension of the four given classes of groups. Except in the “modular” case which will not be treated here, the essential dimension of unipotent groups is 0, see page 10.

One of the deepest results in the theory of essential dimension is the following
Theorem 1.1 (Karpenko-Merkurjev [KM08]). Let $G$ be an abstract finite $p$-group and $k$ be a field of characteristic $\neq p$ containing a primitive $p$th root of unity. Then
\[ \text{ed}(G; p) = \text{ed}(G) = \min \dim(V), \]
where the minimum is taken over all faithful $k$-representations $G \hookrightarrow \text{GL}(V)$.

Note that abstract finite groups and constant finite algebraic groups are equivalent. A general finite algebraic group does not have to be constant and is sometimes called twisted, see Section 2.1 for some preliminaries on finite groups.

First, in Chapter 6, we derive some direct consequences of Theorem 1.1. In particular we prove a new formula, Theorem 6.1, for the essential dimension of finite constant $p$-groups in terms of subgroups of fixed index. With this tool at hand we determine the essential dimension of groups of small nilpotency class, classify finite $p$-groups of small essential $p$-dimension, Section 6.2, and we complete the computation of essential dimension of the group schemes $\text{GL}_n(\mathbb{Z})$ and $\text{SL}_n(\mathbb{Z})$ in Chapter 7. This is our first look at algebraic tori, whose automorphism group is exactly $\text{GL}_n(\mathbb{Z})$.

Informally speaking, Theorem 1.1 means that a faithful linear representations of a $p$-group cannot be compressed (to an action on a lower dimensional variety), cf. Section 3.2. We will expand and generalize this result to a much larger class of groups. The context we need to work in is a class of groups which we call here (FT)-groups (for Finite by Tori -group). This class contains all algebraic tori, finite algebraic groups and extensions thereof. Natural examples of (FT)-groups are normalizers of maximal tori in reductive groups. We define (FT)-groups and describe some of their properties in Section 2.6. For many (conjecturally all) groups $G$ of type (FT) the essential dimension is of the form
\[ \text{ed}(G) = \min \dim V - \dim G, \]
where $V$ is a (generically free) linear $G$-representation. One reason for this is that the linear representations of (FT)-groups enjoy special properties and can be nicely interpreted in terms of certain lattices, see Sections 3.3 and 8.2.

The two extreme cases of (FT)-groups, algebraic tori and finite twisted groups, are already very interesting. Algebraic tori have a very rich structure, given through their connection to integral representations of certain Galois groups and, in the words of Voskresenskii [Vos98], their study provides an amount of work sufficient for all future generations of mathematicians. Some of our main results, Theorems 8.3, 8.4 are the complete description of essential $p$-dimension of algebraic tori, the absolute essential dimension of algebraic tori over a $p$-closed field.
and the essential $p$-dimension of an arbitrary finite algebraic group, all in terms of linear representations. Previously there was not much known about the essential dimension of algebraic tori and our results on tori were used by Merkurjev 11.1 to prove a strong new lower bound on the essential dimension of the projective linear group $\text{PGL}_n$. Even in the case of (twisted) cyclic finite groups the results are new and extend and generalize (besides Theorem 1.1) work by Rost [Ros02], Bayarmagnai [Bay07] and Florence [Flo08].

As applications of Theorems 8.3, we classify tori of small essential dimension and calculate the essential dimension of tori with small splitting fields, see Theorems 8.5, 8.6 and 8.8.

In Chapter 9, Theorem 9.1, we completely determine the essential dimension of the normalizer of a maximal torus in the projective linear group $\text{PGL}_n$. This normalizer is an example of an (FT)-group where again the essential dimension is determined via linear representations. Normalizers $N$ of maximal tori in an algebraic group $G$ allow reduction of structure from $G$ to $N$, cf. [Ser97, 4.3.6], which means in many cases one can study the simpler structure of the (FT)-group $N$ to obtain information about the group $G$. In particular, the essential dimension of $G$ is always bounded from above by the essential dimension of $N$.

Chapters 10 and 11 are devoted to the study of central simple algebras and the simple algebraic group $\text{PGL}_n$. The essential dimension of $\text{PGL}_n$ is one of the main open problems of the theory.

In Theorem 10.1 we prove a new upper bound on the essential dimension of a central simple algebra in terms of certain Galois subfields. We study several functors of central simple algebras which carry some additional structure (such as a distinguished Galois subfield or splitting group) and which allow us to interpret them in terms of (FT)-groups. Finally in Theorem 11.2 we apply these results to the so called universal division algebra $\text{UD}(n)$ and obtain a new upper bound on the essential $p$-dimension of $\text{PGL}_n$. 

2

Preliminaries

2.1 Algebraic Groups

By an affine (or linear) group scheme over $k$ we mean a representable functor $G : \text{Algebras}/k \to \text{Groups}$. Denote the $k$-algebra that represents $G$ by $k[G]$. It carries the structure of a Hopf-algebra and many group theoretic statements on $G$ can be translated into algebraic statements on $k[G]$. $G$ is called algebraic if $k[G]$ is finitely generated and it is called smooth if $k[G] \otimes k_{\text{alg}}$ is reduced. There doesn’t seem to be a consensus in the literature whether the definition of “algebraic group” includes smoothness. We will not assume smoothness in general. Good first references on affine algebraic groups are [Wat79] [Mil06]; further we refer to [DG70a], [SGA3I, SGA3II, SGA3III], [Jan03] and [KMRT98].

When we speak about the essential dimension of an affine algebraic group $G$, we mean the essential dimension of the functor $\text{Tors}_G$ (see Definition 1.5 and Section 3.2) and not the essential dimension of the underlying scheme (which would be just the usual dimension of the scheme, cf. [Mer08, 1.2]).

In the sequel all algebraic groups will be affine and we will often omit the word affine. Examples of algebraic groups that are not affine are abelian varieties; as for their essential dimension we refer to [Bro07] and [BS08].

In the rest of this chapter we give a brief overview of some classes of groups and recall some definitions.

2.2 Finite Groups

By a finite group we understand an algebraic group $G$ over $k$ whose algebra $k[G]$ is finite dimensional as a $k$-vector space.

Smooth finite groups are called étale. Equivalently, their algebra $k[G]$ is an étale $k$-algebra, i.e. a product of finite separable field extensions of $k$.

The order of a finite algebraic group $G$ is defined as the dimension $|G| := \dim_k k[G]$. If $G$ is smooth this number coincides with the order of the abstract
group $G(k_{\text{alg}})$.

For every (abstract) finite group $\Gamma$ there is an algebraic group $G$ over $k$ called \textit{constant} such that $G(K) = \Gamma$ for all $K/k$, see for example [KMRT98, VI 20]. The standard example of a non-constant group is $\mu_n$, the $n$-th roots of unity; for example if $n$ is odd and $k = \mathbb{R}$, $\mu_n(\mathbb{R})$ consists only of the identity element \{1\} but $\mu_n(\mathbb{C})$ is a group of order $n$.

A finite group which is not necessarily constant we will sometimes call \textit{twisted}. This notion comes from the fact that all \'{e}tale algebraic groups are obtained from abstract groups by twisting them by an action of the absolute Galois group $\text{Gal}(k_{\text{sep}}/k)$. Finite algebraic groups are studied in the more general context of finite flat group schemes. We refer to [Tat97] and [Sha86].

### 2.3 Extensions

A sequence of group homomorphisms

$$1 \to F \to G \xrightarrow{\phi} H \to 1$$

(2.1)

is \textit{short exact} if $\phi$ is a quotient map with kernel $F$. Here we say a homomorphism $\phi: G \to H$ is a \textit{quotient map} if its associated $k$-algebra map $k[H] \to k[G]$ is injective, see [Wat79, 15]. Note that in general the morphism of $K$-points $G(K) \xrightarrow{\phi} H(K)$ need not be surjective for an arbitrary field $K/k$. If a sequence as above exists, $G$ is called an \textit{extension} of $H$ by $F$.

An \textit{isogeny} of algebraic groups is a quotient map $G \to H$ such that the kernel $F$ is finite. In that situation $G, H$ are called \textit{isogenous}. If the kernel is of order prime to $p$ we say that the isogeny is a $p$-\textit{isogeny}.

For any affine algebraic group $G$ there is a unique connected normal (in fact characteristic) subgroup $G^0$ with a finite \'{e}tale quotient denoted by $\pi_0 G$. Thus in principal we can pass from an arbitrary group to a connected group via an extension

$$1 \to G^0 \to G \xrightarrow{\pi_0} G \to 1,$$

(2.2)

see for example [Wat79, 6.7] or [DG70a, II 5.1].
2 Preliminaries

2.4 Unipotent Groups, Passage to Reductive Groups

An algebraic group $G$ is called unipotent if every linear $G$-representation ($\neq 0$) has non-trivial fixed points. Alternatively, $G$ embeds into a group of upper triangular matrices with 1 on the diagonal, cf. [DG70a, IV 2.2]. In many cases the essential dimension of a unipotent group $G$ is zero:

**Proposition 2.1.** Let $G$ be a unipotent group over $k$.

(a) Suppose $\text{char } k = 0$. Then $\text{ed}(G; p) = \text{ed}(G) = 0$ for all $p$.

(b) Suppose $\text{char } k = q > 0$. Then $\text{ed}(G; p) = 0$ for all $p \neq q$.

**Proof.** $G$ has a central composition series with quotients isomorphic to $G_a$ or a finite $q$-group (if $\text{char } k = q$), see [DG70a, IV 2.2.5]. Now note that $H^1(K, G_a) = \{0\}$, [Ser62b, II 1.2] for any $K$. For part (b) we can assume $K$ is so called $p$-closed (see Definition 4.1 and Lemma 4.1) and thus perfect and the Galois cohomology $H^1(K, F) = Tors_F(K) = \{0\}$ for any finite $q$-group $F$, cf. Lemma 5.2. Part (b) now follows by induction on the length of the composition series. \hfill $\square$

There are however unipotent groups in positive characteristic with non-trivial essential dimension: For example the constant group $\mathbb{Z}/p$ is unipotent over a field of characteristic $p$ and its essential dimension is 1, see [BF03, Ex. 2.3]. Some new results on unipotent groups in positive characteristic can be found in a recent preprint by Tossici and Vistoli [TV10].

A smooth algebraic group $G$ is called reductive, if the unipotent radical $R_u G^0_{kalg}$ is trivial. If $G = G^0$ is smooth and connected over a perfect field $k$, the unipotent radical $R_u G$ is defined over $k$ and one can pass to the reductive quotient via an extension

$$1 \to R_u G \to G \to G/R_u G \to 1,$$

Moreover, in characteristic 0, [San81, Lemma 1.13], $H^1(K, G) = H^1(K, G/R_u G)$ and thus

$$\text{ed}(G) = \text{ed}(G/R_u G).$$
2.5 Algebraic Tori, Characters, Lattices

In this section we collect preliminary facts about groups of multiplicative type, tori, lattices and their interplay. The references are [DG70a, IV 1.], [Vos98, Section 3.4], [Wat79, 7] or [KMRT98] and [Lor05] (for lattices).

An algebraic group $G$ over a field $k$ is said to be diagonalizable if every linear $G$-representation can be diagonalized and $G$ is called of multiplicative type if $G_{k_{\text{sep}}}$ is diagonalizable over the separable closure $k_{\text{sep}}$ of $k$. Here, as usual, $G_{k'} := G \times_{\text{Spec}k} \text{Spec}(k')$ for any field extension $k'/k$.

Let $X(G) := \text{Hom}(G_{k_{\text{sep}}}, \mathbb{G}_m)$ be the character group of $G$ and $\Gamma = \text{Gal}(k_{\text{sep}}/k)$ be the absolute Galois group of the field $k$. It acts continuously on $X(G)$ which is to say the kernel is of finite index and thus $\Gamma$ acts via a finite quotient $\Gamma = \text{Gal}(K/k)$, for $K/k$ some finite extension. We denote the action of $\Gamma$ (or $\overline{\Gamma}$) by superscripts

$$\gamma \cdot \chi(t) := \gamma \cdot \chi(\gamma^{-1} \cdot t)$$

where $\gamma \in \Gamma$, $\chi \in X(T)$ and $t \in T(k_{\text{sep}})$.

Conversely a finitely generated abelian group $A$ with continuous $\Gamma$-action (= a $\mathbb{Z}[\Gamma]$-module) yields a group of multiplicative type represented by the Hopf-algebra $k_{\text{sep}}[A]_{\Gamma}$. We denote this group by $\text{Diag}(A)$.

In fact these two operations determine an anti-equivalence of the categories of groups of multiplicative type over $k$ and finitely generated abelian groups $A$ with continuous $\Gamma$-action. This equivalence is exact, i.e. the sequence of $\mathbb{Z}[\Gamma]$-modules

$$0 \to A_1 \to A_2 \to A_3 \to 0$$

is exact if and only if the following sequence of algebraic groups is exact:

$$1 \to \text{Diag}(A_3) \to \text{Diag}(A_2) \to \text{Diag}(A_1) \to 1.$$

Suppose an algebraic group $F$ over $k$ acts on the group $G$ of multiplicative type on the right. Then we obtain an action of the group $F(k_{\text{sep}})$ on $X(G)$ by setting

$$f \cdot \chi(t) := \chi(tf^{-1})$$

where $f \in F(k_{\text{sep}})$, $\chi \in X(T)$ and $t \in T(k_{\text{sep}})$. This action is compatible with the $\Gamma$-action in the sense that

$$\gamma f \cdot \gamma \chi = \gamma(f \cdot \chi).$$

Moreover, given an algebraic group $F$ and a $\Gamma$-compatible action of $F(k_{\text{sep}})$ on $X(G)$ one recovers the action of $F$ on $G$. 
A smooth connected group of multiplicative type is called *algebraic torus* (we will usually omit the word *algebraic*). A diagonalizable torus is called *split*. A split torus is simply a product of finitely many copies of the multiplicative group $\mathbb{G}_m$. The character group of a torus is a $\mathbb{Z}\Gamma$-lattice by which we mean the following: Let $R$ be a commutative ring and $B$ an $R$-algebra (we will mostly use $R = \mathbb{Z}$ or the localization $R = \mathbb{Z}_{(p)}$). A $B$-module is called a $B$-lattice if it is finitely generated and projective as an $R$-module. For $B = \mathbb{Z}\Gamma$ this is as usual a free abelian group of finite rank with an action of $\Gamma$.

**Example.** Let $\Gamma_1, \ldots, \Gamma_m \subset \Gamma$ be subgroups of finite index in the absolute Galois group of $k$. Let $M = \mathbb{Z}[\Gamma/\Gamma_1] \oplus \cdots \oplus \mathbb{Z}[\Gamma/\Gamma_m]$. $\Gamma$ acts on $M$ by permuting the cosets. A $\mathbb{Z}\Gamma$-lattice of this form is called *permutation lattice* (it has a basis permuted by $\Gamma$). The torus $\text{Diag}(M)$ is called *quasi split*. An alternate description is as follows: Let $M$ be as above and $E$ the étale algebra $E = L_1 \times \cdots \times L_m$ where $L_i = k_{\text{sep}}\Gamma_i$. Then $\text{Diag}(M)$ is just the Weil restriction $R_{E/k}(\mathbb{G}_m)$.

We summarize the above in Table 2.1.

**Table 2.1: Dictionary of the anti-equivalence Diag.**

<table>
<thead>
<tr>
<th>Algebraic $k$-groups of multiplicative type</th>
<th>$\text{Diag}(\ast)$</th>
<th>Finitely generated abelian $\Gamma$-groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diagonalizable</td>
<td>$\leftrightarrow$</td>
<td>trivial $\Gamma$-action</td>
</tr>
<tr>
<td>Connected</td>
<td>$\leftrightarrow$</td>
<td>torsion free,</td>
</tr>
<tr>
<td>Smooth</td>
<td></td>
<td>except allow $p$-torsion if $\text{char } k = p$</td>
</tr>
<tr>
<td>Torus (=smooth, connected)</td>
<td>$\leftrightarrow$</td>
<td>no $p$-torsion if $\text{char } k = p$</td>
</tr>
<tr>
<td>Split torus $\simeq \mathbb{G}_m^n$</td>
<td>$\leftrightarrow$</td>
<td>free abelian group $\simeq \mathbb{Z}^n$</td>
</tr>
<tr>
<td>Quasisplit torus $\simeq R_{E/k}(\mathbb{G}_m)$</td>
<td>$\leftrightarrow$</td>
<td>permutation lattice</td>
</tr>
<tr>
<td>Anisotropic torus</td>
<td>$\leftrightarrow$</td>
<td>no $\Gamma$ fixed-points other than 0</td>
</tr>
<tr>
<td>$F$-action</td>
<td>$\leftrightarrow$</td>
<td>$\Gamma$-compatible $F(k_{\text{sep}})$-action</td>
</tr>
</tbody>
</table>
We will sometimes pass from $\mathbb{Z}\Gamma$-lattices to $\mathbb{Z}(p)\Gamma$-lattices which corresponds to identifying $p$-isogenous tori. For a $\mathbb{Z}$-module $M$ write $M_{(p)} := \mathbb{Z}(p) \otimes M$.

**Lemma 2.1.** Let $M, L$ be $\mathbb{Z}\Gamma$-lattices. Then the following statements are equivalent:

(a) $L_{(p)} \simeq M_{(p)}$.

(b) There exists an injective map $\phi: L \rightarrow M$ of $\mathbb{Z}\Gamma$-modules with cokernel $Q$ finite of order prime to $p$.

(c) There exists a $p$-isogeny $\text{Diag}(M) \rightarrow \text{Diag}(L)$.

**Proof.** The equivalence (b) $\Leftrightarrow$ (c) is clear from the anti-equivalence of $\text{Diag}$.

The implication (b) $\Rightarrow$ (a) follows from $Q_{(p)} = 0$ and that tensoring with $\mathbb{Z}(p)$ is exact.

For the implication (a) $\Rightarrow$ (b) we use the fact that $L$ and $M$ may be considered as subsets of $L_{(p)}$ (resp. $M_{(p)}$). The image of $L$ under a map $\alpha: L_{(p)} \rightarrow M_{(p)}$ of $\mathbb{Z}(p)\Gamma$-modules lands in $\frac{1}{m}M$ for some $m \in \mathbb{N}$ (prime to $p$) and the index of $\alpha(L)$ in $\frac{1}{m}M$ is finite and prime to $p$ if $\alpha$ is surjective. Since $\frac{1}{m}M \simeq M$ as $\mathbb{Z}\Gamma$-modules the claim follows. \hfill \Box

## 2.6 (FT)-Groups

We will repeatedly encounter groups for which there is a short exact sequence

$$1 \rightarrow T \rightarrow G \rightarrow F \rightarrow 1,$$

where $T$ is a torus and $F$ finite. For convenience we define

**Definition 2.1.** An extensions of a finite group by a torus is called an $(\text{FT})$-group.

Alternatively, $(\text{FT})$-groups are characterized in the following

**Lemma 2.2.**

(a) $G$ is an $(\text{FT})$-group $\iff$ $G$ is an extension of a finite group by a multiplicative group.

(b) A smooth group $G$ is $(\text{FT})$ $\iff$ the connected component $G^0$ is a torus.
(c) The class of (FT)-groups is closed under taking subgroups and quotients.

(d) Let \( \text{char } k = 0 \). Then a group \( G \) is (FT) \( \iff \) every subgroup of \( G \) is reductive.

Proof. (a) If \( G \) is an extension of a finite group by a multiplicative group \( M \), then \([DG70a, IV1.3.9]\) \( M \) has a maximal subtorus \( T = M_{\text{red}}^0 \) which is characteristic in \( M \) and thus normal in \( G \). Then \( G/T \) is finite and \( G \) is (FT).

(b) If \( G \) is (FT), given as an extension of the finite group \( F \) by the torus \( T \) and \( G \) is smooth, then \([KMRT98, 22.4]\) \( F \) is smooth too. It follows that \( G^0/T = F^0 \) is finite, smooth and connected, hence trivial. Thus \( T = G^0 \). The other direction is trivial (and does not require smoothness).

(c) If \( H \subset G \) is a subgroup where \( G \) is an extension of a finite group by the torus \( T \), \( H \cap T \) is multiplicative \([SGA3II, 2.10]\) and \( H/T \cap H \) is finite. Then apply (a). The assertion about quotients is proved in a similar manner.

(d) If \( G \) is (FT), all subgroups of \( G \) are also (FT) by (c) and thus reductive. Conversely, suppose \( G \) is not (FT). Then its connected component \( G^0 \) is not a torus by (b) (since all groups in characteristic 0 are smooth). If \( G^0 \) is not reductive, we are done. Otherwise we may assume \( G^0 \) is semi-simple by replacing it by its derived subgroup. It then contains an almost simple group and in fact must contain a group of type \( A_1 \), i.e. a form of \( \text{SL}_2 \) or \( \text{PGL}_2 \), cf. \([Spr98, 7.2.4]\). But either of these have subgroups which are not reductive.

\[ \square \]

Note that part (b) is not necessarily true if \( G \) is not smooth, for example a finite connected group is (FT) but its connected component is not a torus. In general if \( G \) is (FT), \( G^0 \) is an extension of a connected finite group by a torus.

We will also be interested in certain subclasses of (FT)-groups. We say \( G \) is a \( p-(\text{FT}) \)-group if \( G \) is an extension of a finite \( p \)-group by a torus and we say \( G \) is a split (FT)-group if it is a semidirect product of a finite group and a torus. Note also that abelian (FT)-groups are exactly multiplicative groups, i.e. groups that are diagonalizable over \( k_{\text{alg}} \). In a slightly different context, supersolvable (FT)-groups were studied in \([BS53]\).

The case where the extension is just a direct product will also be of interest. To avoid the ugly name “central split (FT) groups”, define

**Definition 2.2.** A direct product of a finite group and a torus is called an (FxT)-group.

(FT)-groups are groups for which certain representations cannot be compressed, in a sense to be made precise in Chapters 3 and 8.
2.7 (Semi-)Simple Groups

A non-commutative connected smooth algebraic groups is called \textit{simple} if it has no non-trivial normal subgroups and it is called \textit{almost simple} if it has a finite center and the quotient by the center is a simple group. A connected smooth algebraic groups $G$ is called \textit{semi-simple} if there is an isogeny

$$1 \rightarrow F \rightarrow G_1 \times \cdots \times G_r \rightarrow G \rightarrow 1$$

with $G_1, \ldots, G_r$ almost simple (and $F$ finite). If the base field is perfect, one can pass from an arbitrary smooth connected group to a semi-simple group by taking the quotient by its radical $RG$, the largest connected normal solvable subgroup.

Almost simple groups are classified via root systems and Dynkin diagrams into four classical families $A_n, B_n, C_n, D_n$ and the exceptional groups $G_2, F_4, E_6, E_7, E_8$. We usually write in bold face the classical split almost simple groups $\text{SL}_n$, $\text{PGL}_n = \text{GL}_n / \mathbb{G}_m$ (type $A_{n-1}$), $\text{SO}_n$ (type $B_{(n-1)/2}$, $n$ odd, type $D_{n/2}$, $n$ even) and $\text{Sp}_{2n}$ (type $C_n$). “Split” here means that they contain a split maximal torus.

The problem of computing the essential dimension of semi-simple groups is largely open. Known cases include the special linear group $\text{SL}_n$, the symplectic group $\text{Sp}_{2n}$ which are “special” and have essential dimension 0, the special orthogonal group $\text{SO}_n$ which has essential dimension $n - 1$ (for $n > 2$), some of the spin groups, the exceptional group of type $G_2$ and $\text{PGL}_4$.

We refer to [Rei00], [RY00], [Lem04], [Mac08], [BRV10] for these and more results (note that some restrictions on the base field $k$ apply).

The projective linear group $\text{PGL}_n$ will be discussed in detail in chapter 11.
3

Actions, Representations, Lattices

In this chapter we collect some preliminary results on representations and essential
dimension. We will see that (FT)-groups (see Section 2.6) play a special role in
this context. Unless otherwise specified we will assume that the dimensions of all
varieties and ranks of all modules are finite.

3.1 Faithful and Generically Free Actions

Let \( p \) be a prime and \( k \) a field of characteristic different from \( p \). Let \( G \) be an
algebraic group defined over \( k \) and \( \alpha : G \times X \rightarrow X \) an action of \( G \) on an algebraic
variety \( X \) over \( k \). Here, a variety over \( k \) means a (not necessarily connected)
separated scheme over \( \text{Spec} \ k \) of finite type and an action of \( G \) on \( X \) is a (regular)
morphism such that \( \alpha \) defines an action of the abstract group \( G(K) \) on the set
\( X(K) \), for all \( K/k \).

Definition 3.1.

(a) (Cf. [Rei00, 2.7] or [BF03, 4.10])

\( X \) (or \( \alpha \)) is called generically free if the scheme-theoretic stabilizer \( \text{Stab}_G(x) \)
is trivial for all points in general position. This means that there is an open
dense subset \( U \subset X \) such that for all \( K/k \) and \( x \in U(K) \), \( \text{Stab}_G(x) \) is trivial,
where \( \text{Stab}_G(x) \) is a group scheme over \( K \).

(b) \( X \) (or \( \alpha \)) is called \( p \)-faithful if the kernel of the action is finite of order prime
to \( p \).

(c) \( X \) (or \( \alpha \)) is called \( p \)-generically free if the kernel \( N \) of the action is finite of
order prime to \( p \) and \( \alpha \) descends to a generically free action of \( G/N \).

The following simple lemma shows that one can always pass to the algebraic
closure to check generic freeness:
Lemma 3.1. A $G$-variety $X$ is generically free if and only if the $G_{\text{alg}}$-variety $X_{\text{alg}}$ is.

Proof. Let $U \subset X_{\text{alg}}$ be an open dense subvariety on which $G_{\text{alg}}$ acts freely. Let $\Gamma = \text{Gal}(k_{\text{sep}}/k)$ be the absolute Galois group of $k$. Its action on $X(k_{\text{sep}})$ extends to an action on $X(k_{\text{alg}})$. If $U(k_{\text{alg}})$ is not $\Gamma$-invariant, we replace it by the union of its translates by $\gamma \in \Gamma$, on which $G$ still acts freely. Then $U$ is defined over $k$, see [Spr98, 11.2.8]. For any $K$-point $x \in U(K)$, $\text{Stab}_G(x)$ is trivial if and only if it is trivial after base extension to $K_{\text{alg}}$ and the lemma follows. \hfill \Box

Remark. In characteristic 0, $G$ acts freely on $U$ if and only if $G(k_{\text{alg}})$ acts freely on $U(k_{\text{alg}})$. In positive characteristic one needs in addition certain Lie stabilizer to be trivial, see [BF03, 4.2].

Groups $G$ for which

$$\text{Every } p\text{-faithful irreducible } G\text{-variety is } p\text{-generically free} \tag{3.1}$$

will play an important role later. Note that for a group that satisfies (3.1), in particular every faithful $G$-action is generically free. The converse, every $(p)$-generically free action is $(p)$-faithful, is true for any group.

The following lemma is known to the experts, cf. [MR09a, 2.1]; [LMMR09, 7.1]. For completeness we include a proof which does not depend on the base field.

Lemma 3.2. Let $k$ be of characteristic different from $p$.

(a) If $G$ is finite it satisfies (3.1).

(b) If $G$ is a torus it satisfies (3.1).

(c) If $G$ satisfies (3.1) and $H$ is a finite $p$-group then $G \times H$ satisfies (3.1).

Proof. (a) If the kernel of the action is finite of order prime to $p$, we can factor out the kernel and the group is still finite, so it suffices to prove that every faithful action of a finite group is generically free. Recall [SGA3II, VIII 6.5(e)] that for an algebraic group $H$ over $k$ which acts on a $k$-variety $X$, the fixed points $X^H$, defined as $X^H(K) = \{x \in X(K) | hx = x\}$ is a closed subscheme of $X$. Let $Y = \bigcup_H X^H$ where $H$ ranges over all nontrivial subgroups of $G$. If the $G$-action on $X$ is faithful then $Y \neq X$ and $G$ acts freely on the dense open $X \setminus Y$.

(b) As in (a) we can factor out the finite kernel of the action first and the quotient will still be a torus. Thus we can assume the action is faithful and by the
lemma above, $G$ is diagonalizable. If the action is given by a linear representation $V$ then $G$ acts on $V$ via characters $\chi$. Take a basis of $V$ such that each basis element $v$ is in a character space i.e. $t \cdot v = \chi(t)v$ for some character. Then we can remove the elements in $V$ which have some 0 coefficient with respect to this basis. Since the $G$-action is faithful, the remaining elements form a non-empty open $G$-invariant subspace of $V$ and $G$ acts freely on it.

For the general case, after applying an equivariant normalization we may assume first that $X$ is normal. Reducing it further, by [Sum74, Theorem 1, Corollary 2] we may assume that $X$ is affine the action is linear. Then proceed as before.

(c) Assume again that $k$ is algebraically closed and so $H$ is constant and smooth (since char $k \neq p$). Since the kernel of the action has order prime to $p$ it is a subgroup of $G$ and the quotient of $G$ by the kernel acts generically freely on $X$. Let $U$ be a closed subvariety of $X$ such that $G$ acts freely on $X \setminus U$. Replacing it by the translates of $h \in H(k)$, we can assume $U$ is $H$-invariant. The closed subvarieties $U^{(h)}$ for $h \in H(k)$ are $G$-invariant. After removing them, the remaining dense open subvariety is generically free for the $G \times H$-action.

Remark. As a variant of part (c) one can prove that every faithful action of a smooth group of multiplicative type is generically free.

In general, algebraic groups do not satisfy (3.1), even if they are of type (FT), as the following simple example of a split (FT)-group shows.

Example 3.1. Let $G = G_m \ltimes \mathbb{Z}/2 \simeq \mathbb{O}_2$ where $\sigma \in \mathbb{Z}/2$ acts by $\sigma t = t^{-1}$. Let $\rho : G \to \text{GL}_2$ be given by

$$t \mapsto \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}, \quad \sigma \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. $$

Clearly $\rho$ is faithful but for any $v = (x, y)$ in general position, $g = (x/y, \sigma) \in G$ is in the stabilizer (here $g \in G(K), t \in T(K)$ and $v \in K^2$ for some field $K/k$).

We recall the following criterion from [LR00]:

Lemma 3.3. Let $N$ be a normal subgroup of $G$ and $X$ a $G$-variety. Then $X$ is generically free as a $G$-variety if an only if it is generically free as an $N$-variety and $X/N$ is generically free as a $G/N$-variety.

Here $X/N$ denotes the rational quotient. If $N$ acts generically freely on $X$ one can replace $X$ by some open $U \subset X$ on which the action is free and the quotient $U/N$ in the category of schemes exists, [BF03, 4.7].

For future reference we record the following easy corollary.
Corollary 3.1. Let $G$ be an $(FT)$-group given as an extension of a finite group $F$ by a torus $T$. Let $W$ be a faithful representation of $F$ and $V$ be a representation of $G$ whose restriction to $T$ is faithful. Then $V \times W$ is a generically free representation of $G$.

Proof. We view $W$ as a representation of $G$ via the natural projection $G \to G/T = F$. The corollary follows from the lemma in combination with Proposition 3.2. □

3.2 Geometric Interpretation of Essential Dimension

With the notion of a generically free action we are able to give a more geometric definition of essential dimension of an algebraic group, cf. [Rei00]. Historically this approach preceded the functorial definition via the functors $H^1(\ast, G)$ or $\mathcal{T} \text{ors}_G$.

Let us recall first the definition of a $G$-torsor which can be thought of as a principal homogeneous space in the category of schemes over some base.

Let $X$ be a scheme over $Y$ such that the morphism $X \to Y$ is $fppf$ (faithfully flat of finite presentation). If $Y = \text{Spec } K$ the spectrum of a field, faithfully flat is automatic and of finite presentation means that $X$ is of finite type i.e. algebraic [Wat79, 13], [DG70a, I 2.2, I 3]. $X$ is called a pseudo-$G$-torsor over $Y$ if it is endowed with a $G$-action such that $X \to Y$ is $G$-invariant and

$$X \times_Y G \to X \times_Y X$$

$$(x, g) \mapsto (x, x \cdot g)$$

is an isomorphism (here we assume $G$ is a scheme over $Y$, otherwise if $Y$ is defined over $k$ replace $G$ by $G_Y$). A pseudo-$G$-torsor is a torsor if it is locally trivial in the $fppf$-topology, i.e. there is a $fppf$-covering $(Y_i \to Y)$ such that $X_{Y_i} \cong G_{Y_i}$ for each $i$. For details we refer to [SGA3I, Exp. IV 5], [DG70a, III 4] or [BF03, 4.5].

In most of the cases here the base $Y = \text{Spec } K$ will be the spectrum of a field $K/k$. Then locally trivial in the $fppf$-topology simply means that there is a field $K' \subset K_{\text{alg}}$ such that $X_{K'} \cong G_{K'}$ [Wat79, 18.4] or what amounts to the same, $X(K') \neq \emptyset$. Moreover, if $G$ is smooth, $K'$ can be chosen to be separable over $K$ and thus $X$ is a $K_{\text{sep}}/K$-form of $G_K$. These $K_{\text{sep}}/K$-forms are classified by the Galois cohomology $H^1(K, G)$ which explains the equivalence of functors $\mathcal{T} \text{ors}_G = H^1(\ast, G)$. 


Let $X$ be an algebraic variety over $k$ on which $G$ acts generically freely. Then on an open $U \subset X$ the categorical quotient $U/G$ exists and gives rise to a $G$-torsor $U \to U/G$, cf. [BF03, 4.7]. Alternatively we can work with a rational quotient $X/G$, i.e. a model for $k(X)^G$ and a rational map $X \to X/G$. Rosenlicht’s theorem, cf. [Ros56], [Ros63], links these two approaches; see also [Rei00, 2.3]. Without loss of generality assume now that $X/G$ is a categorical quotient and $X \to X/G$ a $G$-torsor, otherwise replace $X$ by $U$.

A compression of a $G$-torsor $X \to X/G$ is a diagram

$$
\begin{array}{ccc}
X & \to & X' \\
\downarrow & & \downarrow \\
X/G & \to & X'/G
\end{array}
$$

where $X' \to X'/G$ is $G$-torsor, the top horizontal map is $G$-equivariant rational and the bottom horizontal map is rational.

**Definition 3.2** ([Rei00, 3.1], [BF03, 6.8]). Let $X$ be as above. The essential dimension of $X$ (or $X \to X/G$) is defined as the minimal dimension of $X'/G$ such that there exists a compression (3.2).

For any $K$-point $\text{Spec } K \to X/G$ we can take the fiber

$$
\begin{array}{ccc}
X' & \to & X \\
\downarrow & & \downarrow \\
\text{Spec } K & \to & X/G
\end{array}
$$

to obtain an element $\alpha = [X' \to \text{Spec } K]$ in $Tors_G(K)$. In particular if $K = k(X/G) = k(X)^G$ is a field, we can take the generic fiber over the generic point and we have $\text{trdeg}_k K = \dim X/G = \dim X - \dim G$. Recall that $X$ is called primitive if $K = k(X/G) = k(X)^G$ is a field or equivalently $G$ transitively permutes the components of $X$, see [Rei00, 2.1].

The following Lemma from [BF03, 6.11] asserts that the two definitions 1.1 and 3.2 of essential dimension of $G$-torsors agree:

**Lemma 3.4.** Let $X$ be a primitive generically free $G$ variety, $K = k(X)^G$ and $\alpha = [X' \to \text{Spec } K]$ the generic fiber. Then

$$
\text{ed}(X) = \text{ed}(\alpha).
$$
Moreover, we have the obvious upper bound
\[ \text{ed}(X) = \text{ed}(\alpha) \leq \text{trdeg}_k K = \dim X - \dim G. \]

The essential dimension of \( G \), \( \text{ed}(G) = \text{ed}(\text{Tors}_G) \), is the maximal essential dimension of a \( G \)-torsor \( \alpha \) or equivalently the maximal essential dimension of a primitive generically free \( G \)-variety. This maximum is attained in the case where \( \alpha \) is a so called \textit{versal} \( G \)-torsor in the sense of [GMS03, Section 1.5]; see also [Dun09, 2.1]. If \( X \) is a primitive generically free \( G \)-variety such that \( X \to X/G \) is versal we obtain
\[ \text{ed}(G) = \text{ed}(X) \leq \dim X - \dim G. \]

This is in particular the case when \( X = V \) is a generically free linear representation \( \rho : G \to \text{GL}(V) \), by [GMS03, 1.5.4]. The following inequality will be used often in the sequel (for part (a) see [Rei00, 3.4] or [BF03, 4.11]):

**Lemma 3.5.**

(a) Let \( \rho : G \to \text{GL}(V) \) be a generically free \( G \)-representation. Then
\[ \text{ed}(G; p) \leq \text{ed}(G) \leq \dim(V) - \dim(G). \]

(b) Let \( \rho : G \to \text{GL}(V) \) be a \( p \)-generically free \( G \)-representation. Then
\[ \text{ed}(G; p) \leq \dim(V) - \dim(G). \]

**Proof.** For part (b), let \( N \) be the kernel of \( \rho \). It is a finite group of order prime to \( p \). In Chapter 5, Theorem 5.1 we will show that the essential \( p \)-dimension does not change by factoring out a finite prime to \( p \) normal subgroup. Then, together with part (a) we have
\[ \text{ed}(G; p) = \text{ed}(G/N; p) \leq \dim(V) - \dim(G). \]

\( \square \)

### 3.3 Representations of (FT)-Groups

In this section we will collect some results about representations of (FT)-groups \( G \). As we saw in Example 3.1 there are faithful representations of (FT)-groups that are not generically free.
Proposition 3.1. Let $\Gamma = \text{Gal}(k_{\text{sep}}/k)$ and $G$ a smooth group of multiplicative type over $k$ with char $k \neq p$. There is a 1:1 correspondence between linear representations $\rho : G \to \text{GL}(V)$ and maps of $\mathbb{Z}\Gamma$-lattices $\phi : L \to X(G)$ with $L$ permutation. Write $L = \mathbb{Z}[\Lambda]$ where $\Lambda$ is a basis permuted by $\Gamma$. Then in the above correspondence,

(a) $\dim V = \text{rk } L = |\Lambda|$. 

(b) $\rho$ is generically free $\iff$ $\rho$ is faithful $\iff$ $\phi$ is surjective. 

(c) Assume $G$ is a torus. Then $\rho$ is $p$-generically free $\iff$ $\rho$ is $p$-faithful $\iff$ $\phi$ has finite cokernel of order prime to $p$ $\iff$ $L(\rho) \to X(G)(\rho)$ is a surjective map of $\mathbb{Z}(\rho)\Gamma$-modules.

Proof. Let $\rho : G \to \text{GL}(V)$ be a representation of $G$. Since $G_{k_{\text{sep}}}$ is diagonalizable, there exist characters $\chi_1, \ldots, \chi_n \in X(G)$ (counted with multiplicities) such that $G$ acts on $V_{k_{\text{sep}}}$ via diagonal matrices with entries $\chi_1(g), \ldots, \chi_n(g)$ (for $g \in G_{k_{\text{sep}}}$) with respect to a suitable basis of $V_{k_{\text{sep}}}$. Moreover $\Gamma$ permutes the set $\Lambda := \{\chi_1, \ldots, \chi_n\}$. Define $L = \mathbb{Z}[\Lambda]$ and a map $\phi : L \to X(G)$ of $\mathbb{Z}\Gamma$-modules by sending the basis element $\chi_j \in \Lambda$ to itself. Clearly $\dim V = |\Lambda| = \text{rk } L$. Conversely, assume we have a map $L \to X(G)$. Using the anti-equivalence $\text{Diag}$ we obtain a homomorphism $G \to \text{Diag}(L)$. We can embed the quasi-split torus $\text{Diag}(L)$ in $\text{GL}_n$, where $n = \text{rk } L$ [Vos98, 6.1]. The kernel of $\rho$ corresponds to the cokernel of $\phi$ by exactness of $\text{Diag}$ and the first two equivalences in (b) and (c) follow from Lemma 3.2.

Now consider the case where $G$ is a torus. Assume we have a surjective map $\alpha : L \to X(G)(\rho)$ of $\mathbb{Z}(\rho)\Gamma$-modules where $L = \mathbb{Z}(\rho)[\Lambda]$ is permutation, $\Lambda$ a $\Gamma$-set. Then $\alpha(\Lambda) \subseteq \frac{1}{m}X(G)$ for some $m \in \mathbb{N}$ prime to $p$ (note that $\frac{1}{m}X(G)$ can be considered as a subset of $X(G)(\rho)$ since $X(G)$ is torsion free). By construction the induced map $\mathbb{Z}[\Lambda] \to \frac{1}{m}X(G) \approx X(G)$ becomes surjective after localization at $\rho$, hence its cokernel is finite of order prime to $p$. 

Suppose now that we have an (FT)-group $G$ which is an extension of the finite group $F$ by $T$. Then, from a linear representation $\rho : G \to \text{GL}(V)$ we can still get the map of $\mathbb{Z}\Gamma$-lattices $\phi : L \to X(T)$ by first restricting the representation to $T$.

The group $F(k_{\text{sep}})$ acts on $X(T)$ compatibly with the $\Gamma$-action, see Section 2.5. Moreover $F(k_{\text{sep}})$ permutes the weight spaces $V_\chi$ of $\rho$ restricted to $T_{k_{\text{sep}}}$, i.e. the subspaces on which $T_{k_{\text{sep}}}$ acts by multiplication of $\chi(*)$. Let $\Lambda$ be the set of weights counted with multiplicities so that $|\Lambda| = \dim V$. Suppose we can find bases of $V_\chi$
for each \( \chi \) which are permuted by the \( F(k_{\text{sep}}) \)-action up to scaling (this is trivially possible if each weight space is 1-dimensional), then we obtain a permutation action of \( F(k_{\text{sep}}) \) on \( \Lambda \) and thus \( L = \mathbb{Z}[\Lambda] \) is an \( F(k_{\text{sep}}) \) permutation lattice. Following [Sal88, sec. 2] we say \( \rho \) has a good basis if in the above correspondence \( L = \mathbb{Z}[\Lambda] \) is an \( F(k_{\text{sep}}) \) permutation lattice.

The group \( F(k_{\text{sep}}) \) acts on the kernel \( M = \ker \phi \) of the map \( \phi : L \to X(T) \). Similarly \( F \) acts on the quasisplit torus \( \text{Diag}(L) \subset \text{GL}(V) \) and the quotient \( \text{Diag}(L)/T = \text{Diag}(M) \). Applying Lemma 3.2 and Proposition 3.1 we obtain:

**Proposition 3.2.** Let \( \rho : G \to \text{GL}(V) \) be a representation of the \((FT)\)-group \( G \) which is an extension of \( F \) by \( T \) and suppose \( \rho \) has a good basis. Let \( \phi : L \to X(T) \) be the associated map of \( F(k_{\text{sep}}) \)-lattices. Then \( \rho \) is generically free if and only if \( \phi \) is surjective and \( F(k_{\text{sep}}) \) acts faithfully on \( \ker \phi \).

**Remark.** For our purposes the assumption that a representation has a good basis is mostly harmless. Indeed, one can show that a faithful or generically free representation of minimal dimension has a good basis because all the weight spaces \( V_\chi \) are 1-dimensional.

**Corollary 3.2.** Let \( G \) be an \((FT)\)-group. Suppose every \( F(k_{\text{sep}}) \)-invariant generating set \( \Lambda \) of \( X(T) \) contains \( \geq d \) elements. If \( G \to \text{GL}(V) \) is a generically free \( k \)-representation of \( G \) then \( \dim(V) \geq d \).

Of course we would like to run this argument in the other direction: For every map of \( \mathbb{Z}\Gamma \)-lattices \( L \to X(T) \) with \( L \) permutation and which is also a map of \( F(k_{\text{sep}}) \)-modules, can we construct a representation \( \rho : G \to \text{GL}(V) \) “inverting” the construction above? In Proposition 3.1 we saw that by embedding \( \text{Diag}(T) \) in some \( \text{GL}(V) \) we obtain a \( T \)-representation, but a priori it is not clear how to define an action of all of \( G \) on \( V \).

In the special case where \( G \) is a split \((FT)\)-group, so that \( G = T \rtimes F \), \( F \) smooth and \( L \) is a permutation \( F(k_{\text{sep}}) \)-lattice, \( F \) permutes the basis in \( V \) and the \( F \)- and \( T \)-actions are compatible, thus give a \( G \)-action on \( V \). Explicitly, let \( L = \mathbb{Z}[\Lambda] \) with \( F(k_{\text{sep}}) \) permuting the finite set \( \Lambda \). Let \( V_\Lambda \) be the vectorspace (defined as a variety over \( k \)) with basis elements \( v_\lambda \) for each \( \lambda \in \Lambda \). The finite group \( F \) acts on \( V_\Lambda \) by permuting these basis elements in the natural way,

\[
\tilde{f} : v_\lambda \mapsto v_{f.\lambda}.
\]

(3.3)

(where \( f \in F(K) \) which we think of as a subgroup of \( F(k_{\text{sep}}) \)).
The torus $T$ acts by the character $\phi(\lambda)$ on each 1-dimensional space $\text{Span}(v_\lambda)$,

$$t: v_\lambda \mapsto \phi(\lambda)(t)v_\lambda \quad (3.4)$$

In $G$ we have $tf = f(f^{-1} \cdot t)$ where the action in the parenthesis defines the semi-direct product $T \rtimes F$. One checks that

$$\rho(t)\rho(f) = \rho(f)\rho(f^{-1} \cdot t)$$

and so these actions extend to a linear action of $G = T \rtimes F$.

**Proposition 3.3.** Let $\Gamma = \text{Gal}(k_{\text{sep}}/k)$ and $G$ a smooth split (FT)-group over $k$. There is a 1:1 correspondence between linear representations $\rho: G \to \text{GL}(V)$ with good bases and maps of lattices $\phi : L \to X(G)$ with compatible $\Gamma$- and $F(k_{\text{sep}})$-actions and such that $L$ is permutation with respect to both of these actions. In the above correspondence,

(a) $\text{dim} V = \text{rk} L$.

(b) $\rho$ is generically free $\iff \phi$ is surjective and $F(k_{\text{sep}})$ acts faithfully on $\ker \phi$.

(c) $\rho$ is $p$-generically free $\iff \phi$ has finite cokernel of order prime to $p$ and $F(k_{\text{sep}})$ acts faithfully on $\ker \phi$.

**Remark.** It is possible that the proposition can be generalized to all supersolvable (FT)-groups (and thus also $p$-(FT)-groups) $G$. For such groups every representation $\rho: G \to \text{GL}(V)$ is monomial, i.e. $\rho(G)$ is contained in the normalizer $N$ of a maximal torus in $\text{GL}(V)$, and $N$ is a split (FT)-group, cf. [BS53]. However, we haven’t checked the details of this.

For later use we also record two easy corollaries.

**Corollary 3.3.** Let $\Gamma, G$ be as above and suppose there is an exact sequence of $\Gamma$ and $F(k_{\text{sep}})$-lattices (the two actions being compatible)

$$0 \to M \to L \to X(T) \to C \to 0$$

(a) If $C = 0$, $L$ is permutation and $M$ is $F(k_{\text{sep}})$-faithful, then

$$\text{ed}(G) \leq \text{rk} M.$$
(b) If $C$ is finite of order prime to $p$, $L$ is permutation and $M$ is $F(k_{\text{sep}})$-faithful, then
\[ \text{ed}(G; p) \leq \text{rk } M. \]

\[ \square \]

**Corollary 3.4.** Let $T$ be a split torus, $F$ finite and $N = T \rtimes F$. Suppose there is a finite $F$-invariant set $\Lambda \subset X(T)$. Then there is a $N$-representation $V_\Lambda$ of dimension $|\Lambda|$. $V_\Lambda$ is faithful restricted to $T$ $\iff$ $\Lambda$ generates $X(T)$. $V_\Lambda$ is generically free $\iff$ $\Lambda$ generates $X(T)$ and $F$ acts faithfully on $\ker [\mathbb{Z}[\Lambda] \rightarrow X(T)]$. $\square$

Similar statements appeared in [LR00], [LRRS03] and [Lem04].
4

The $p$-Closure of a Field

Throughout this chapter we assume $\text{char} \ k \neq p$. Let $K$ be a field extension of $k$ and $K_{\text{alg}}$ an algebraic closure. We will construct a field $K^{(p)}/K$ in $K_{\text{alg}}$ with all finite subextensions of $K^{(p)}/K$ of degree prime to $p$ and all finite subextensions of $K_{\text{alg}}/K^{(p)}$ of degree a power of $p$. We will call $K^{(p)}$ a $p$-closure of $K$ (to avoid the cumbersome name prime to $p$ closure). We will show some of the advantages in passing from $K$ to a $p$-closure $K^{(p)}$ when working with essential $p$-dimension.

Fix a separable closure $K_{\text{sep}} \subset K_{\text{alg}}$ of $K$ and denote $\Gamma = \text{Gal}(K_{\text{sep}}/K)$. Recall that $\Gamma$ is profinite and has Sylow-$p$ subgroups which enjoy similar properties as in the finite case, see for example [RZ00] or [Wil98]. Let $\Phi$ be a Sylow-$p$ subgroup of $\Gamma$ and $K_{\text{sep}}\Phi$ its fixed field.

Definition 4.1. The field

$$K^{(p)} = \{a \in K_{\text{alg}} | a \text{ is purely inseparable over } K_{\text{sep}}\Phi\}$$

is called a $p$-closure of $K$. A field $K$ is called $p$-closed if $K = K^{(p)}$.

Note that $K^{(p)}$ is unique in $K_{\text{alg}}$ only up to the choice of a Sylow-$p$ subgroup $\Phi$ in $\Gamma$. The notion of being $p$-closed does not depend on this choice.

Proposition 4.1.

(a) $K^{(p)}$ is a direct limit of finite extensions $K_i/K$ of degree prime to $p$.

(b) Every finite extension of $K^{(p)}$ is separable of degree a power of $p$; in particular, $K^{(p)}$ is perfect.

(c) The cohomological dimension of $\Psi = \text{Gal}(K_{\text{alg}}/K^{(p)})$ is $\text{cd}_q(\Psi) = 0$ for any prime $q \neq p$.

Proof. (a) First note that $K_{\text{sep}}$ is the direct limit of the directed set $\{K_{\text{sep}}N\}$ over all normal subgroups $N \subset \Gamma$ of finite index. Let

$$\mathcal{L} = \{K_{\text{sep}}^N\Phi | N \text{ normal with finite index in } \Gamma\}.$$
This is a directed set, and since \( \Phi \) is Sylow, the index of \( N\Phi \) in \( \Gamma \) is prime to \( p \). Therefore \( \mathcal{L} \) consists of finite separable extensions of \( K \) of degree prime to \( p \). Moreover, \( K_{\text{sep}}^\Phi \) is the direct limit of fields \( L \) in \( \mathcal{L} \).

If \( \text{char} \ k = 0 \), \( K^{(p)} = K_{\text{sep}}^\Phi \) and we are done. Otherwise suppose \( \text{char} \ k = q \neq p \). Let

\[
\mathcal{E} = \{ E \subset K_{\text{alg}} | E/L \text{ finite and purely inseparable for some } L \in \mathcal{L} \}.
\]

\( \mathcal{E} \) consists of finite extensions of \( K \) of degree prime to \( p \), because a purely inseparable extension has degree a power of \( q \). One can check that \( \mathcal{E} \) forms a directed set.

Finally note that if \( a \) is purely inseparable over \( K_{\text{sep}}^\Phi \) with minimal polynomial \( x^{q^n} - l \) (so that \( l \in K_{\text{sep}}^\Phi \)), then \( l \) is already in some \( L \in \mathcal{L} \) since \( K_{\text{sep}}^\Phi \) is the direct limit of \( \mathcal{L} \). Thus \( a \in E = L(a) \) which is in \( \mathcal{E} \) and we conclude that \( K^{(p)} \) is the direct limit of \( \mathcal{E} \).

(b) \( K^{(p)} \) is the purely inseparable closure of \( K_{\text{sep}}^\Phi \) in \( K_{\text{alg}} \) and \( K_{\text{alg}}/K^{(p)} \) is separable, see [Win74, 2.2.20]. Moreover, \( \text{Gal}(K_{\text{alg}}/K^{(p)}) \simeq \text{Gal}(K_{\text{sep}}/K_{\text{sep}}^\Phi) = \Phi \) is a pro-\( p \) group and so every finite extension of \( K^{(p)} \) is separable of degree a power of \( p \).

(c) See [Ser97, Cor. 2, I. 3]. \( \square \)

**Remark.** Given an arbitrary algebraic extension \( L/K \) there may not exist an intermediate subfield \( K \subset K^{(p)} \subset L \) such that the degree of every finite subextension of \( K^{(p)}/K \) is prime to \( p \) and the degree of every finite subextension of \( L/K^{(p)} \) is a power of \( p \). An intermediate subfield with these properties exists if and only if \( L = K_{s}K_{is} \), where \( K_{s} \) (respectively, \( K_{is} \)) denotes the separable (purely inseparable) closure of \( K \) in \( L \). Such fields are sometimes called balanced [Lip66].

We call a covariant functor \( \mathfrak{F} : \text{Fields}_k \rightarrow \text{Sets} \) colimit-preserving if for any directed system of fields \( \{ K_i \} \), \( \mathfrak{F}(\lim_i K_i) = \lim_i \mathfrak{F}(K_i) \). For example if \( G \) is an algebraic group, the \( fppf \)-cohomology functor \( H^1_{fppf}(\ast, G) = \mathfrak{F} \text{rs}_G \) is colimit-preserving; see [Mar07, 2.1].

**Lemma 4.1.** Let \( \mathfrak{F} \) be colimit-preserving and \( \alpha \in \mathfrak{F}(K) \) an object. Denote the image of \( \alpha \) in \( \mathfrak{F}(K^{(p)}) \) by \( \alpha_{K^{(p)}} \).

(a) \( \text{ed}_k(\alpha; p) = \text{ed}_k(\alpha_{K^{(p)}}; p) = \text{ed}_k(\alpha_{K^{(p)}}) \).

(b) \( \text{ed}_k(\mathfrak{F}; p) = \text{ed}_k(\mathfrak{F}; p) \).
Proof. (a) The inequalities \( \text{ed}(\alpha; p) \geq \text{ed}(K(p); p) = \text{ed}(K(p)) \) are clear from the definition and Proposition 4.1(b) since \( K(p) \) has no finite extensions of degree prime to \( p \). It remains to prove \( \text{ed}(\alpha; p) \leq \text{ed}(K(p)) \). If \( L/K \) is finite of degree prime to \( p \),

\[
\text{ed}(\alpha; p) = \text{ed}(\alpha_L; p),
\]

(4.1)

cf. [Mer08, Proposition 1.5] and its proof. For the \( p \)-closure \( K(p) \) this is similar and uses (4.1) repeatedly:

Suppose there is a subfield \( K_0 \subset K(p) \) and \( \alpha_{K(p)} \) comes from an element \( \beta \in \mathfrak{F}(K_0) \), so that \( \beta_{K(p)} = \alpha_{K(p)} \). Write \( K(p) = \lim L \), where \( L \) is a direct system of finite prime to \( p \) extensions of \( K \). Then \( K_0 = \lim L_0 \) with \( L_0 = \{ L \cap K_0 \mid L \in L \} \) and by assumption on \( \mathfrak{F} \), \( \mathfrak{F}(K_0) = \lim L \in L_0 \). Thus there is a field \( L' = L \cap K_0 \) (\( L \in L \)) and \( \gamma \in \mathfrak{F}(L') \) such that \( \gamma_{K_0} = \beta \). Since \( \alpha_L \) and \( \gamma_L \) become equal over \( K(p) \), after possibly passing to a finite extension, we may assume they are equal over \( L \) which is finite of degree prime to \( p \) over \( K \). Combining these constructions with (4.1) we see that

\[
\text{ed}(\alpha; p) = \text{ed}(\alpha_L; p) = \text{ed}(\gamma_L; p) \leq \text{ed}(\gamma_L) \leq \text{ed}(\alpha_{K(p)}).
\]

(b) This follows immediately from (a), taking \( \alpha \) of maximal essential \( p \)-dimension.

\( \square \)

Remark 4.1. The Lemma shows that we can always assume that the base field is \( p \)-closed when we are computing the essential \( p \)-dimension. In particular, we may assume that \( k \) contains a primitive \( p \)th root of unity, since adjoining it results in an extension of degree prime to \( p \) (however we can’t assume that \( k \) contains primitive roots of higher powers of \( p \) in general).

Proposition 4.2. Let \( \mathfrak{F}, \mathfrak{G} : \text{Fields}/k \rightarrow \text{Sets} \) be colimit-preserving functors and \( \mathfrak{F} \rightarrow \mathfrak{G} \) a natural transformation. If the map

\[
\mathfrak{F}(K) \rightarrow \mathfrak{G}(K)
\]

is bijective (resp. surjective) for any \( p \)-closed field extension \( K/k \) then

\[
\text{ed}(\mathfrak{F}; p) = \text{ed}(\mathfrak{G}; p) \quad (\text{resp. } \text{ed}(\mathfrak{F}; p) \geq \text{ed}(\mathfrak{G}; p)).
\]

Proof. Assume the maps are surjective. By Proposition 4.1(a), the natural transformation is \( p \)-surjective, in the terminology of [Mer08], so we can apply [Mer08, Prop. 1.5] to conclude \( \text{ed}(\mathfrak{F}; p) \geq \text{ed}(\mathfrak{G}; p) \).
Now assume the maps are bijective. Let $\alpha$ be in $\mathcal{F}(K)$ for some $K/k$ and $\beta$ its image in $\mathcal{G}(K)$. We claim that $\text{ed}(\alpha; p) = \text{ed}(\beta; p)$. First, by Lemma 4.1 we can assume that $K$ is $p$-closed and it is enough to prove that $\text{ed}(\alpha) = \text{ed}(\beta)$.

Assume that $\beta$ comes from $\beta_0 \in \mathcal{G}(K_0)$ for some field $K_0 \subset K$. Any finite prime to $p$ extension of $K_0$ is isomorphic to a subfield of $K$ (cf. [Mer08, Lemma 6.1]) and so also any $p$-closure of $K_0$ (which has the same transcendence degree over $k$). We may therefore assume that $K_0$ is $p$-closed. By assumption $\mathcal{F}(K_0) \to \mathcal{G}(K_0)$ and $\mathcal{F}(K) \to \mathcal{G}(K)$ are bijective. The unique element $\alpha_0 \in \mathcal{F}(K_0)$ which maps to $\beta_0$ must therefore map to $\alpha$ under the natural restriction map. This shows that $\text{ed}(\alpha) \leq \text{ed}(\beta)$. The other inequality always holds and the claim follows.

Taking $\alpha$ maximal with respect to its essential dimension, we obtain $\text{ed}(\mathcal{F}; p) = \text{ed}(\alpha; p) = \text{ed}(\beta; p) \leq \text{ed}(\mathcal{G}; p)$. \qed
5

Group Extensions

In this chapter we consider extensions of algebraic groups, i.e. short exact sequences
\[ 1 \to G_1 \to G_2 \to G_3 \to 1, \]  
and investigate in some special cases how the essential dimensions of two of the groups are related to the essential dimension of the third group. We assume again \( \text{char } k \neq p \) throughout this chapter.

5.1 \( p \)-Isogenies

We will prove that \( p \)-isogenous groups have the same essential \( p \)-dimension. This result will play a key role in the proof of Theorem 8.2 where we need to remove finite prime to \( p \) kernels of linear representations.

**Theorem 5.1.** Suppose \( G \to Q \) is a \( p \)-isogeny of algebraic groups over \( k \). Then

(a) For any \( p \)-closed field \( K \) containing \( k \) the natural map \( H^1(K, G) \to H^1(K, Q) \) is bijective.

(b) \( ed_k(G; p) = ed_k(Q; p) \).

**Remark.** Since the \( p \)-closed field \( K \) is perfect (Proposition 4.1) we have \( H^1(K, G) = H^1_{\text{fppf}}(K, G) \), cf. Section 3.2, and the following does not depend on whether \( G \) is smooth or not.

**Example.** (cf. [GR09, Remark 9.7]) Let \( E_6^{sc}, E_7^{sc} \) be simply connected simple groups of type \( E_6, E_7 \) respectively. In [GR09, 9.4, 9.6] it is shown that if \( k \) is an algebraically closed field of characteristic \( \neq 2 \) and \( 3 \) respectively, then
\[ ed_k(E_6^{sc}; 2) = 3 \text{ and } ed_k(E_7^{sc}; 3) = 3. \]

These results can also be deduced from [Gar09, (11.2), Lemma 13.1]. For the adjoint groups \( E_6^{ad} = E_6^{sc} / \mu_3, E_7^{ad} = E_7^{sc} / \mu_2 \) Theorem 5.1 tells us that
\[ ed_k(E_6^{ad}; 2) = 3 \text{ and } ed_k(E_7^{ad}; 3) = 3. \]
We will need two lemmas.

**Lemma 5.1.** Let $N$ be a finite algebraic group over $k$. The following are equivalent:

(a) $p$ does not divide the order of $N$.

(b) $p$ does not divide the order of $N_{\text{alg}}$.

If $N$ is also assumed to be abelian, denote by $N[p]$ the $p$-torsion subgroup of $N$. The following are equivalent to the above conditions.

(c) $N[p](k_{\text{alg}}) = \{1\}$.

(d) $N[p](k^{(p)}) = \{1\}$.

**Proof.** (a) $\iff$ (b): Let $N^\circ$ be the connected component of $N$ and $N^{\text{et}} = N/N^\circ$ the étale quotient. Recall that the order of a finite algebraic group $N$ over $k$ is defined as $|N| = \dim_k k[N]$ and $|N| = |N^\circ||N^{\text{et}}|$, see for example [Tat97]. If $\text{char } k = 0$, $N^\circ$ is trivial, if $\text{char } k = q \neq p$ is positive, $|N^\circ|$ is a power of $q$. Hence $N$ is of order prime to $p$ if and only if the étale algebraic group $N^{\text{et}}$ is. Since $N^\circ$ is connected and finite, $N^\circ(k_{\text{alg}}) = \{1\}$ and so $N(k_{\text{alg}})$ is of order prime to $p$ if and only if the group $N^{\text{et}}(k_{\text{alg}})$ is. Then $|N^{\text{et}}| = \dim_k k[N^{\text{et}}] = |N^{\text{et}}(k_{\text{alg}})|$, cf. [Bou03, V.29 Corollary].

(b) $\iff$ (c) $\Rightarrow$ (d) are clear.

(c) $\Leftarrow$ (d): Suppose $N[p](k_{\text{alg}})$ is nontrivial. The Galois group $\Gamma = \text{Gal}(k_{\text{alg}}/k(p))$ is a pro-$p$ group and acts on the $p$-group $N[p](k_{\text{alg}})$. The image of $\Gamma$ in $\text{Aut}(N[p](k_{\text{alg}}))$ is again a (finite) $p$-group and the size of every $\Gamma$-orbit in $N[p](k_{\text{alg}})$ is a power of $p$. Since $\Gamma$ fixes the identity in $N[p](k_{\text{alg}})$, this is only possible if it also fixes at least $p - 1$ more elements. It follows that $N[p](k(p))$ contains at least $p$ elements, a contradiction. \hfill $\square$

**Remark.** Part (d) could be replaced by the slightly stronger statement that $N[p](k(p) \cap k_{\text{sep}}) = \{1\}$, but we won’t need this in the sequel.

**Lemma 5.2.** Let $\Gamma$ be a profinite group, $G$ an (abstract) finite $\Gamma$-group and $|\Gamma|, |G|$ coprime. Then $H^1(\Gamma, G) = \{1\}$.

The case where $\Gamma$ is finite and $G$ abelian is classical. In the generality we stated, this lemma is also known, [Ser97, I.5, ex. 2]. Since we haven’t found a proof in the literature, we outline it here.
Proof. First, it is easy to reduce to the case when $\Gamma$ is finite since $\Gamma$ is the inverse limit of finite groups. Then consider the semidirect product $G \rtimes \Gamma$. Each cocycle $c : \gamma \mapsto g_\gamma$ defines a section $\phi_c : \Gamma \to G \rtimes \Gamma$, $\gamma \mapsto (g_\gamma, \gamma)$. Cohomologous cocycles define $G$-conjugate sections and there is a bijection between $H^1(\Gamma, G)$ and sections $\{\phi : \Gamma \to G \rtimes \Gamma\}/G$-conjugation.

One of the groups has odd order and by the Feit-Thompson theorem is solvable. Then, a theorem by Zassenhaus ([Zas58, IV. 7]) asserts that any two sections are conjugate.

Proof of Theorem 5.1. (a) Let $N$ be the kernel of $G \to Q$ and $K = K^{(p)}$ be a $p$-closed field over $k$. Since $K_{\text{sep}} = K_{\text{alg}}$, the sequence of $K_{\text{sep}}$-points $1 \to N(K_{\text{sep}}) \to G(K_{\text{sep}}) \to Q(K_{\text{sep}}) \to 1$ is exact. By Lemma 5.1, the order of $N(K_{\text{sep}})$ is not divisible by $p$ and therefore coprime to the order of $\Psi = \text{Gal}(K_{\text{sep}}/K)$. Thus $H^1(K, N) = \{1\}$ by Lemma 5.2. Similarly, if $cN$ is the group $N$ twisted by a cocycle $c : \Psi \to G$, $cN(K_{\text{sep}}) = N(K_{\text{sep}})$ is of order prime to $p$ and $H^1(K, cN) = \{1\}$. It follows that $H^1(K, G) \to H^1(K, Q)$ is injective, cf. [Ser97, I.5.5].

Surjectivity is a consequence of [Ser97, I. Proposition 46] and the fact that the $q$-cohomological dimension of $\Psi$ is 0 for any divisor $q$ of $|N(K_{\text{sep}})|$, by Proposition 4.1).

This concludes the proof of part (a). Part (b) immediately follows from (a) and Proposition 4.2. □

5.2 Groups of Index Prime to $p$

Let $H$ be a closed subgroup of an algebraic group $G$ defined over $k$. The homogeneous space $G/H$ of left cosets is an algebraic scheme (i.e. of finite type) over $k$, see [DG70a, III 3.5.4]). If $G/H$ is finite over $k$, i.e. the algebra $A$ of any affine open is a finite dimensional $k$-algebra, then this dimension does not depend on the choice of affine open, and one defines the index $[G : H] = \dim_k A$. The index can be defined in more generality for schemes over an arbitrary base scheme, see [Tat97].

Theorem 5.2. Let $H$ be a closed subgroup of an algebraic group $G$ defined over $k$. Assume that the index $[G : H]$ is finite and prime to $p$. Then $\text{ed}(G;p) = \text{ed}(H;p)$.

In the case where $G$ is finite constant, this is proved in [Mer08, Proposition 4.10].
Proof. Recall that if $G$ is a linear algebraic group and $H$ is a closed subgroup then
\begin{equation}
\text{ed}(G; p) \geq \text{ed}(H; p) + \dim(H) - \dim(G);
\end{equation}
for any prime $p$; see, [BRV10, Lemma 2.2] or [Mer08, 4.3]. Since $\dim H = \dim G$, this yields $\text{ed}(G; p) \geq \text{ed}(H; p)$.

To prove the opposite inequality, by Proposition 4.2 it suffices to show that for any $p$-closed field $K = K^{(p)}$ over $k$ the map $H^1(K, H) \to H^1(K, G)$ induced by the inclusion $H \subset G$ is surjective.

Let $X$ be a $G$-torsor over $K$ and $X/H$ be the natural quotient of $X$ by the action of $H$. Recall that $X/H$ is a $K$-form of $G/H$, constructed by descent or Galois twisting of $G/H$ by $X$ with respect to the natural $G$-action on $G/H$; see [Ser62a, 1.3.2] or [Mil80, p. 134].

For a field $L/K$ and an $L$-point $\text{Spec}(L) \to X/H$ we construct an $H$-torsor $Y$ as the pullback
\[
\begin{array}{ccc}
Y & \longrightarrow & X \\
\downarrow & & \downarrow \\
\text{Spec}(L) & \longrightarrow & X/H \\
& \downarrow & \\
& \text{Spec}(K) & 
\end{array}
\]
In this situation the homogeneous fiber product $Y \times^H G$ is isomorphic to the restriction $X_L$ as $G$-torsors. Thus we have the natural diagram
\[
\begin{array}{ccc}
H^1(L, H) & \longrightarrow & H^1(L, G) \\
[Y] & \mapsto & [X]_L \\
\downarrow & & \downarrow \\
[X] & \mapsto & H^1(K, G)
\end{array}
\]
where $[X]$ and $[Y]$ denote the classes of $X$ and $Y$ in $H^1(K, G)$ and $H^1(L, H)$, respectively. It remains to show the existence of a $K$-point of $X/H$.

Let $A$ be the $K$-algebra of an affine open of $X/H$. By assumption, $A$ has finite dimension. Let $N$ be the nilradical of $A$. Since $K$ is $p$-closed, it is perfect and thus $A/N$ is étale, in other words a direct product of field extensions $L_i/K$:
\[
A/N \cong L_1 \times \cdots \times L_r;
\]
see, e.g., [Mil06, 2,19] and [Bou03, V, Theorem 4]. Note that \( \dim_K A/N \) divides \( \dim_K A \) (cf. [Tat97, Prop. 3.1]) and

\[
\dim_K A/N = \sum_{j=1}^r [L_j : K].
\]

As \( \dim_K A = [G : H] \) is prime to \( p \), at least one of the \( [L_j : K] \) has to be prime to \( p \) as well but that is only possible if \( L_j = K \) because \( K \) is \( p \)-closed. Then the projection \( A \to A/N \to L_j = K \) gives the required \( K \)-point \( \text{Spec} K \to \text{Spec}A \to X/H \).

\begin{corollary}
Suppose \( k \) is a field of characteristic \( \neq p \). Let \( \mathcal{S}_n \) be the symmetric group in \( n \) letters. Then \( \text{ed}(\mathcal{S}_n; p) = [n/p] \).
\end{corollary}

\begin{proof}
Let \( m = [n/p] \) and let \( D \cong (\mathbb{Z}/p\mathbb{Z})^m \) be the subgroup generated by the disjoint \( p \)-cycles

\[
\sigma_1 = (1,\ldots,p), \ldots, \sigma_m = ((m-1)p+1,\ldots,mp).
\]

The inequality \( \text{ed}(\mathcal{S}_n; p) \geq \text{ed}(D; p) \geq [n/p] \) is well known; see, [BR97, 6], [BR99, 7], or [BF03, 3.7].

The opposite inequality was first noticed by J.-P. Serre and independently R. L"otscher worked out a proof (both unpublished).

The semi-direct product \( D \rtimes \mathcal{S}_m \), where \( \mathcal{S}_m \) permutes \( \sigma_1, \ldots, \sigma_m \), embeds in \( \mathcal{S}_n \) with index prime to \( p \). By Theorem 5.2, \( \text{ed}(D \rtimes \mathcal{S}_m; p) = \text{ed}(\mathcal{S}_n; p) \) and it suffices to show that \( \text{ed}(D \rtimes \mathcal{S}_m) \leq [n/p] \). By Lemma 3.5 it is enough to construct a generically free \( m \)-dimensional representation of \( D \rtimes \mathcal{S}_m \) defined over \( k \). Moreover, by Remark 4.1 we may assume that \( \zeta_p \in k \), where \( \zeta_p \) denotes a primitive \( p \)th root of unity.

Let \( \sigma_1^*, \ldots, \sigma_m^* \subset X(D) \) be the “basis” of \( D \) dual to \( \sigma_1, \ldots, \sigma_m \). That is,

\[
\sigma_i^*(\sigma_j) = \begin{cases} 
\zeta_p, & \text{if } i = j \\
1, & \text{otherwise}.
\end{cases}
\]

The \( \mathcal{S}_m \)-invariant subset \( \Lambda = \{ \sigma_1^*, \ldots, \sigma_m^* \} \) of \( X(D) \) gives rise to the \( m \)-dimensional \( k \)-representation \( V_\Lambda \) of \( D \rtimes \mathcal{S}_m \), similarly as in Corollary 3.4 and it is easily checked that this representation is generically free.

Another application of Theorem 5.2 is the following: Consider the group \( \text{SL}_{nm}/\mu_m \) where we identify \( \mu_m \) with \( \langle \zeta_m \rangle \) and assume that the \( m \)th root of unity \( \zeta_m \) is in the ground field. \( \text{SL}_{nm}/\mu_m \) sits between \( \text{SL}_{nm} \) and \( \text{PGL}_{nm} \).
Corollary 5.2. Let $p^r$ and $p^s$ be the highest power of $p$ in $n$ and $m$ respectively. Then
\[
ed(\text{SL}_{nm}/\mu_m;p) = \ned(\text{SL}_{p^r+p^s}/\mu_{p^r};p)
\]
In particular,
\[
ed(\text{SL}_{nm}/\mu_m;p) = 0 \text{ if } p \nmid m,
\]
\[
ed(\text{SL}_{nm}/\mu_m;p) = \ned(\text{PGL}_m;p) \text{ if } p \nmid n.
\]

Proof. Apply Theorem 5.2 to
\[
1 \to \mu_m/p^r \to \text{SL}_{nm}/\mu_{p^r} \to \text{SL}_{nm}/\mu_m \to 1
\]
and show that $H^1(K,\text{SL}_{nm}/\mu_{p^r}) = H^1(K,\text{SL}_{p^r+p^s}/\mu_{p^r})$ for any $p$-closed field $K$.

5.3 Direct Products

Recall that for algebraic groups $G,H$ the following inequalities hold:
\[
\max\{\ned(G),\ned(H)\} \leq \ned(G \times H) \leq \ned(G) + \ned(H),
\]
see [Rei00, 3.8] and [BF03, 1.16. b)]. The same also holds for essential $p$-dimension. Additivity (equality on the right) was proved for constant $p$-groups in [KM08]. We will extend this to (FXT)-group i.e. direct products of a torus and a (twisted) finite group, see Section 2.6. We say a group is $p$-(FXT) if it is a direct product of a torus and a (twisted) finite $p$-group.

Theorem 5.3.

(a) Let $G$ and $H$ be (FXT)-groups over $k$. Then
\[
ed(G \times H;p) = \ned(G;p) + \ned(H;p).
\]

(b)

Let $G,H$ be $p$-(FXT)-groups over $k$ and suppose $k = k^{(p)}$ is $p$-closed. Then
\[
ed(G \times H) = \ned(G) + \ned(H).
\]

The proof of this theorem will be deferred until Section 8.5 and after Theorem 8.2 which determines the essential dimension of (FXT)-groups in terms of representations.
5.4 Quotients of Large Essential Dimension

C. U. Jensen, A. Ledet and N. Yui asked if \( \text{ed}(G) \geq \text{ed}(G/N) \) for every finite group \( G \) and normal subgroup \( N \triangleleft G \); see [JLY02, p. 204]. The following theorem shows that this inequality is false in general.

**Theorem 5.4.** Assume \( k \) contains a primitive \( p \)-th root of unity. For every real number \( \lambda > 0 \) there exists a \( p \)-group \( G \) and a central subgroup \( H \) of \( G \) such that \( \text{ed}(G/H) > \lambda \text{ed}(G) \).

**Proof.** Let \( \Gamma \) be the non-abelian (constant) group of order \( p^3 \) given by generators \( x, y, z \) and relations \( x^p = y^p = z^p = [x, z] = [y, z] = 1, [x, y] = z \). Choose a multiplicative character \( \chi : H \to k^* \) of the subgroup \( A = \langle x, z \rangle \simeq (\mathbb{Z}/p\mathbb{Z})^2 \) which is non-trivial on the center \( \langle z \rangle \) of \( \Gamma \) and consider the \( p \)-dimensional induced representation \( \text{Ind}_{A}^{\Gamma}(\chi) \). Since the center \( \langle z \rangle \) of \( \Gamma \) does not lie in the kernel of \( \text{Ind}_{A}^{\Gamma}(\chi) \), we conclude that \( \text{Ind}_{A}^{\Gamma}(\chi) \) is faithful. Thus we have constructed a faithful \( p \)-dimensional representation of \( \Gamma \) defined over \( k \). Consequently, by Lemma 3.5,

\[
\text{ed} (\Gamma) \leq p. 
\]  

(5.4)

Taking the direct sum of \( n \) copies of this representation, we obtain a faithful representation of \( \Gamma^n \) of dimension \( np \). Thus with (5.3) we have for any \( n \geq 1 \)

\[
\text{ed} \Gamma^n \leq np. 
\]  

(5.5)

(We remark that both (5.4) and (5.5) are in fact equalities. Indeed, if \( \zeta_{p^2} \) is a primitive root of unity of degree \( p^2 \) then

\[
\text{ed} (\Gamma) \geq \text{ed}_{k(\zeta_{p^2})}(\Gamma) = \sqrt{p^2 + 1} - 1 = p, 
\]

where the middle equality will follow from Theorem 6.2(b). Hence, we have \( \text{ed}(\Gamma) = p \). Moreover, by the additivity theorem 5.3, \( \text{ed} \Gamma^n = n \cdot \text{ed}(\Gamma) = np \). However, we will only need the upper bound (5.5) in the sequel.)

The center of \( \Gamma \) is \( \langle z \rangle \); denote it by \( C \). The center of \( \Gamma^n \) is then isomorphic to \( C^n \). Let \( H_n \) be the subgroup of \( C^n \) consisting of \( n \)-tuples \( (c_1, \ldots, c_n) \) such that \( c_1 \cdots c_n = 1 \). The center \( C(\Gamma^n/H_n) \) of \( \Gamma^n/H_n \) is clearly cyclic of order \( p \) (it is generated by the class of the element \( (z, 1, \ldots, 1) \) modulo \( H_n \)), and the commutator \( [\Gamma^n/H_n, \Gamma^n/H_n] \) is central. Hence,

\[
\text{ed}(\Gamma^n/H_n) \geq \text{ed}_{k(\zeta_{p^2})}(\Gamma^n/H_n) = \sqrt{p^2n + 1} - 1 = p^n, 
\]  

(5.6)
where the middle equality follows from a theorem by Brosnan, Reichstein and Vistoli, cf. Theorem 6.2(b). Setting $G = \Gamma^n$ and $H = H_n$, and comparing (5.5) with (5.6), we see that the desired inequality $\text{ed}(G/H) > \lambda \text{ed}(G)$ holds for suitably large $n$. \qed
6

Finite Groups

6.1 Essential Dimension of Finite Constant $p$-Groups

An important result in the theory of essential dimension was Karpenko and Merkurjev’s Theorem 1.1 on constant finite $p$-groups. In this chapter we will explore some of the consequences of this theorem.

First we will give a new explicit formula for $\text{ed}(G; p)$ in terms of certain subgroups.

For the rest of this chapter we assume that the base field $k$ satisfies

$$\text{char}(k) \neq p \text{ and } k \text{ contains } \zeta,$$

(6.1)

where $\zeta$ is a primitive $p$th root of unity if $p \geq 3$ and a primitive 4th root of unity if $p = 2$. Note that for $p = 2$, Theorem 1.1 is true over fields containing only a primitive second root of unity. However, the properties of $p$-groups we need in the sequel (all representations are monomial, cf. Lemma 6.1) require the stronger assumption. We don’t know if Theorem 6.1 below is true if $k$ contains no primitive 4th root of unity.

For a finite group $H$, we will denote the intersection of the kernels of all multiplicative characters $\chi : H \to k^*$ by $H'$. In particular, if $k$ contains an $e$th root of unity, where $e$ is the exponent of $H$, then $H' = [H, H]$, the commutator subgroup.

Given a $p$-group $G$, we set $Z(G)$ to be the center of $G$ and

$$C(G) := \{ g \in Z(G) \mid g^p = 1 \}$$

(6.2)

to be the $p$-torsion subgroup of $Z(G)$. We will view $C(G)$ and its subgroups as $\mathbb{F}_p$-vector spaces, and write “$\text{dim}_{\mathbb{F}_p}$” for their dimensions. We further set

$$K_i := \bigcap_{[G:H]=p^i} H' \quad \text{and} \quad C_i := K_i \cap C(G).$$

(6.3)

for every $i \geq 0$, $K_{-1} := G$ and $C_{-1} := K_{-1} \cap C(G) = C(G)$. 

Theorem 6.1. Let $G$ be a $p$-group, $k$ be a base field satisfying (6.1) and $\rho : G \hookrightarrow \text{GL}(V)$ be a faithful linear $k$-representation of $G$. Then

(a) $\rho$ has minimal dimension among the faithful linear representations of $G$ defined over $k$ if and only if for every $i \geq 0$ the irreducible decomposition of $\rho$ has exactly

$$\dim_{F_p} C_{i-1} - \dim_{F_p} C_i$$

irreducible components of dimension $p^i$, each with multiplicity 1.

(b) $\text{ed}(G;p) = \text{ed}(G) = \sum_{i=0}^{\infty} (\dim_{F_p} C_{i-1} - \dim_{F_p} C_i) p^i$.

Note that $K_i = C_i = \{1\}$ for large $i$ (say, if $p^i \geq |G|$), so only finitely many terms in the above infinite sum are non-zero.

Remark. In [Mer09, 4.3] Merkurjev proves a similar formula for tori derived from our result Theorem 8.3. Theorem 8.3 in turn is based on Karpenko and Merkurjev’s Theorem 1.1.

Theorem 6.1 will be needed in the classification of $p$-groups of essential dimension $\leq p$ (Theorem 6.3), Theorem 5.4, as well as the calculation of essential dimension of $\text{SL}(\mathbb{Z})$ (Theorem 7.1). First we write down an easy but useful corollary.

Corollary 6.1. Let $G$ be a $p$-group, and $k$ as in (6.1).

(a) If $C(G) \subset K_i$ then $\text{ed}(G)$ is divisible by $p^{i+1}$.

(b) If $C(G) \subset G'$ then $\text{ed}(G)$ is divisible by $p$.

(c) If $C(G) \subset G^{(i)}$, where $G^{(i)}$ denotes the $i$th derived subgroup of $G$, then $\text{ed}(G)$ is divisible by $p^i$.

Proof. (a) $C(G) \subset K_i$ implies $C_{i-1} = C_0 = \cdots = C_i$. Hence, in the formula of Theorem 6.1(b) the $p^0, p^1, \ldots, p^i$ terms appear with coefficient 0. All other terms are divisible by $p^{i+1}$, and part (a) follows.

(b) is an immediate consequence of (a), since $K_0 = G'$.

(c) By [Hup67, Theorem V.18.6] $G^{(i)}$ is contained in the kernel of every $p^{i-1}$-dimensional representation of $G$. Lemma 6.1 below now tells us that $G^{(i)} \subset K_{i-1}$ and part (c) follows from part (a).
To make notation easier we write $C = C(G)$ for the $p$-torsion subgroup $C(G)$ of the center of $G$. An important role in the proof Theorem 6.1 will be played by $C$ and by the descending sequences

$$K_{-1} = G \supset K_0 \supset K_1 \supset K_2 \supset \ldots$$
$$C_{-1} = C \supset C_0 \supset C_1 \supset C_2 \supset \ldots$$

of characteristic subgroups of $G$ defined in (6.3).

We will repeatedly use the well-known fact that a normal subgroup $N$ of $G$ is trivial if and only if $N \cap C$ is trivial. (6.4)

We begin with three elementary lemmas.

**Lemma 6.1.** $K_i = \bigcap_{\dim(\rho) \leq p^i} \ker(\rho)$, where the intersection is taken over all irreducible representations $\rho$ of $G$ of dimension $\leq p^i$.

**Proof.** Let $j \leq i$. Recall that every irreducible representation $\rho$ of $G$ of dimension $p^j$ is induced from a 1-dimensional representation $\chi$ of a subgroup $H \subset G$ of index $p^j$; see [LGP86, (II.4)] for $p \geq 3$ (cf. also [Vol63]) and [LGP86, (IV.2)] for $p = 2$. (Note that our assumption (6.1) on the base field $k$ is crucial here. In the case where $k = \mathbb{C}$ a more direct proof can be found in [Ser77, Section 8.5]).

Thus $\ker(\rho) = \ker(\text{Ind}_H^G \chi) = \bigcap_{g \in G} g \ker(\chi) g^{-1}$, and since each $g \ker(\chi) g^{-1}$ contains $(g H g^{-1})'$, we see that $\ker(\rho) \supset K_j \supset K_i$. The opposite inclusion is proved in a similar manner. $\square$

**Lemma 6.2.** Let $G$ be a finite group, $C$ be a central subgroup of exponent $p$ and $\rho : G \to \text{GL}(V)$ an irreducible representation of $G$. Then

(a) $\rho(C)$ consists of scalar matrices. In other words, the restriction of $\rho$ to $C$ decomposes as $\chi \oplus \ldots \oplus \chi$ (dim($V$) times), for some multiplicative character $\chi : C \to \mathbb{G}_m$. We will refer to $\chi$ as the character associated to $\rho$.

(b) $C_i = \bigcap_{\dim(\rho) \leq p^i} \ker(\chi_{\rho})$, where the intersection is taken over all irreducible $G$-representations $\rho$ of dimension $\leq p^i$ and $\chi_{\rho} : C \to \mathbb{G}_m$ denotes the character associated to $\rho$. In particular, if $\dim(\rho) \leq p^i$ then $\chi_{\rho}$ vanishes on $C_i$. 

Proof. (a) follows from Schur’s lemma. (b) By Lemma 6.1

\[ C_i = C \cap \bigcap_{\dim(\rho) \leq p^i} \ker(\rho) = \bigcap_{\dim(\rho) \leq p^i} (C \cap \ker(\rho)) = \bigcap_{\dim(\rho) \leq p^i} \ker(\chi_{\rho}). \]

Lemma 6.3. Let \( G \) be a \( p \)-group and \( \rho = \rho_1 \oplus \ldots \oplus \rho_m \) be the direct sum of the irreducible representations \( \rho_i : G \to \text{GL}(V_i) \). Let \( \chi_i := \chi_{\rho_i} : C \to \mathbb{G}_m \) be the character associated to \( \rho_i \).

(a) \( \rho \) is faithful if and only if \( \chi_1, \ldots, \chi_m \) span \( C^* \) as an \( \mathbb{F}_p \)-vector space.

(b) Moreover, if \( \rho \) is of minimal dimension among the faithful representations of \( G \) then \( \chi_1, \ldots, \chi_m \) form an \( \mathbb{F}_p \)-basis of \( C^* \).

Proof. (a) By (6.4), \( \ker(\rho) \) is trivial if and only if \( \ker(\rho) \cap C = \bigcap_{i=1}^m \ker(\chi_i) \) is trivial. On the other hand, \( \bigcap_{i=1}^m \ker(\chi_i) \) is trivial if and only if \( \chi_1, \ldots, \chi_m \) span \( C^* \).

(b) Assume the contrary, say \( \chi_m \) is a linear combination of \( \chi_1, \ldots, \chi_{m-1} \). Then part (a) tells us that \( \rho_1 \oplus \ldots \oplus \rho_{m-1} \) is a faithful representation of \( G \), contradicting the minimality of \( \dim(\rho) \).

We are now ready to proceed with the proof of Theorem 6.1. To simplify the notation, we will write \( C \) for \( C_{-1} = C(G) \) for the rest of this section. Part (b) of Theorem 6.1 is an immediate consequence of part (a) and Theorem 1.1. We will thus focus on proving part (a). In the sequel for each \( i \geq 0 \) we will set

\[ \delta_i := \dim_{\mathbb{F}_p} C_{i-1} - \dim_{\mathbb{F}_p} C_i \]

and

\[ \Delta_i := \delta_0 + \delta_1 + \cdots + \delta_i = \dim_{\mathbb{F}_p} C - \dim_{\mathbb{F}_p} C_i, \]

where the last equality follows from \( C_{-1} = C \).

Our proof will proceed in two steps. In Step 1 we will construct a faithful representation \( \mu \) of \( G \) such that for every \( i \geq 0 \) exactly \( \delta_i \) irreducible components of \( \mu \) have dimension \( p^i \). In Step 2 we will show that \( \dim(\rho) \geq \dim(\mu) \) for any other faithful representation \( \rho \) of \( G \), and moreover equality holds if and only if for every \( i \geq 0 \) \( \rho \) has exactly \( \delta_i \) irreducible components of dimension \( p^i \).
Proof of Theorem 6.1 (a).

Step 1: We begin by constructing \( \mu \). By definition,

\[
C = C_{-1} \supset C_0 \supset C_1 \supset \ldots ,
\]

where the inclusions are not necessarily strict. Dualizing this flag of \( \mathbb{F}_p \)-vector spaces, we obtain a flag

\[
(0) = (C^*)_{-1} \subset (C^*)_0 \subset (C^*)_1 \subset \ldots
\]
of \( \mathbb{F}_p \)-subspaces of \( C^* \), where

\[
(C^*)_i := \{ \chi \in C^* | \chi \text{ is trivial on } C_i \} \cong (C/C_i)^*.
\]

Let \( \text{Ass}(C) \subset C^* \) be the set of characters of \( C \) associated to irreducible representations of \( G \), and let \( \text{Ass}_i(C) \) be the set of characters associated to irreducible representations of dimension \( p^i \). Lemma 6.2(b) tells us that

\[
\text{Ass}_0(C) \cup \text{Ass}_1(C) \cup \cdots \cup \text{Ass}_i(C) \text{ spans } (C^*)_i
\]

for every \( i \geq 0 \). Hence, we can choose a basis \( \chi_1, \ldots, \chi_{\Delta_i} \) of \( (C^*)_0 \) from \( \text{Ass}_0(C) \), then complete it to a basis \( \chi_1, \ldots, \chi_{\Delta_i} \) of \( (C^*)_1 \) by choosing the last \( \Delta_1 - \Delta_0 \) characters from \( \text{Ass}_1(C) \), then complete this basis of \( (C^*)_1 \) to a basis of \( (C^*)_2 \) by choosing \( \Delta_2 - \Delta_1 \) additional characters from \( \text{Ass}_2(C) \), etc. We stop when \( C_i = (0) \), i.e., \( \Delta_i = \dim_{\mathbb{F}_p} C \).

By the definition of \( \text{Ass}_i(C) \), each \( \chi_j \) is the associated character of some irreducible representation \( \mu_j \) of \( G \). By our construction

\[
\mu = \mu_1 \oplus \cdots \oplus \mu_{\dim_{\mathbb{F}_p}(C)},
\]

has the desired properties. Indeed, since \( \chi_1, \ldots, \chi_{\dim_{\mathbb{F}_p}(C)} \) form a basis of \( C^* \), Lemma 6.3 tells us that \( \mu \) is faithful. On the other hand, by our construction exactly

\[
\delta_i - \delta_{i-1} = \dim_{\mathbb{F}_p} C_i - \dim_{\mathbb{F}_p} C_{i-1} = \dim_{\mathbb{F}_p} C_i - \dim_{\mathbb{F}_p} C_i
\]
of the characters \( \chi_1, \ldots, \chi_c \) come from \( \text{Ass}_i(C) \). Equivalently, exactly

\[
\dim_{\mathbb{F}_p} C_{i-1} - \dim_{\mathbb{F}_p} C
\]
of the irreducible representations \( \mu_1, \ldots, \mu_c \) are of dimension \( p^i \).
Step 2: Let $\rho: G \to \text{GL}(V)$ be a faithful linear representation of $G$ of the smallest possible dimension,

$$\rho = \rho_1 \oplus \ldots \oplus \rho_c$$

be its irreducible decomposition, and $\chi_i: C \to \mathbb{G}_m$ be the character associated to $\rho_i$. By Lemma 6.3(b), $\chi_1, \ldots, \chi_c$ form a basis of $C^n$. In particular, $c = \dim_{\mathbb{F}_p} C$ and at most $\dim_{\mathbb{F}_p} C - \dim_{\mathbb{F}_p} C_i$ of the characters $\chi_1, \ldots, \chi_c$ can vanish on $C_i$. On the other hand, by Lemma 6.2(b) every representation of dimension $\leq p^i$ vanishes on $C_i$. Thus if exactly $d_i$ of the irreducible representations $\rho_1, \ldots, \rho_c$ have dimension $p^i$ then

$$d_0 + d_1 + d_2 + \ldots + d_i \leq \dim_{\mathbb{F}_p} C - \dim_{\mathbb{F}_p} C_i$$

for every $i \geq 0$. For $i \geq 0$, set $D_i := d_0 + \cdots + d_i = \text{number of representations of dimension } \leq p^i \text{ among } \rho_1, \ldots, \rho_c$. We can now write the above inequality as

$$D_i \leq \Delta_i \text{ for every } i \geq 0. \quad (6.5)$$

Our goal is to show that $\dim(\rho) \geq \dim(\mu)$ and that equality holds if and only if exactly $\delta_i$ of the irreducible representations $\rho_1, \ldots, \rho_{\dim_{\mathbb{F}_p}(C)}$ have dimension $p^i$. The last condition translates into $d_i = \delta_i$ for every $i \geq 0$, which is, in turn equivalent to $D_i = \Delta_i$ for every $i \geq 0$.

Indeed, setting $D_{-1} := 0$ and $\Delta_{-1} := 0$, we have,

$$\dim(\rho) - \dim(\mu) = \sum_{i=0}^{\infty} (d_i - \delta_i)p^i = \sum_{i=0}^{\infty} (D_i - \Delta_i)p^i - \sum_{i=0}^{\infty} (D_{i-1} - \Delta_{i-1})p^i$$

$$= \sum_{i=0}^{\infty} (D_i - \Delta_i)(p^i - p^{i+1}) \geq 0,$$

where the last inequality follows from (6.5). Moreover, equality holds if and only if $D_i = \Delta_i$ for every $i \geq 0$, as claimed. This completes the proof of Step 2 and thus of Theorem 6.1.

Another application of Theorem 6.1 is the following result on $p$-groups of nilpotency class 2 due to Brosnan, Reichstein and Vistoli [BRV07]. For a proof via Theorem 6.1 see [MR08].

**Theorem 6.2.** Let $G$ be a $p$-group of exponent $e$ and $k$ be a field of characteristic $\neq p$ containing a primitive $e$-th root of unity. Suppose the commutator subgroup $(G, G)$ is central in $G$. Then
(a) \( \text{ed}(G; p) = \text{ed}(G) \leq \text{rk } Z(G) + \text{rk } (G, G)(p^{\lfloor m/2 \rfloor} - 1) \), where \( p^m \) is the order of \( G/Z(G) \).

(b) Moreover, if \( (G, G) \) is cyclic then \( |G/Z(G)| \) is a complete square and equality holds in (a). That is, in this case

\[
\text{ed}(G; p) = \text{ed}(G) = \sqrt{|G/Z(G)|} + \text{rk } Z(G) - 1.
\]

Example. Recall that a \( p \)-group \( G \) is called *extra-special* if its center \( Z \) is cyclic of order \( p \), and the quotient \( G/Z \) is elementary abelian. The order of an extra special \( p \)-group \( G \) is an odd power of \( p \); the exponent of \( G \) is either \( p \) or \( p^2 \); cf. [Hup67, III. 13]. Note that every non-abelian group of order \( p^3 \) is extra-special. For extraspecial \( p \)-groups Theorem 6.2(b) reduces to the following.

*Let \( G \) be an extra-special \( p \)-group of order \( p^{2m+1} \). Assume that the characteristic of \( k \) is different from \( p \), that \( \zeta_p \in k \), and \( \zeta_{p^2} \in k \) if the exponent of \( G \) is \( p^2 \). Then \( \text{ed}(G) = p^m \).*

### 6.2 \( p \)-Groups of Essential Dimension \( \leq p \)

It is a formidable task to classify finite groups of a given essential dimension. Finite groups of essential dimension 1 were described in [BR97, 6.2], [Led07] and [CHKZ08]; finite groups of essential dimension 2 over \( \mathbb{C} \) in [Dun09]. We content ourselves here with the case where \( G \) is a \( p \)-group.

**Theorem 6.3.** Let \( p \) be a prime, \( k \) be as in (6.1) and \( G \) be a \( p \)-group such that \( G' \neq \{1\} \). Then the following conditions are equivalent.

\( (a) \) \( \text{ed}(G) \leq p \),

\( (b) \) \( \text{ed}(G) = p \),

\( (c) \) The center \( Z(G) \) is cyclic and \( G \) has a subgroup \( A \) of index \( p \) such that \( A' = \{1\} \).

\( (d) \) \( G \) is isomorphic to a subgroup of \( \mathbb{Z}/p^\alpha \rtimes \mathbb{Z}/p = (\mathbb{Z}/p^\alpha)^p \rtimes \mathbb{Z}/p \), where \( \alpha \geq 1 \) is an integer such that \( k \) contains a primitive \( p^\alpha \)th root of unity.
Note that the assumption that $G' \neq \{1\}$ is harmless. Indeed, if $G' = \{1\}$ then by Theorem 6.1(b) $\text{ed}(G) = \text{rk}(G)$; cf. also [BR97, Theorem 6.1] or [BF03, section 3].

Proof. Since $K_0 = G'$ is a non-trivial normal subgroup of $G$, we see that $K_0 \cap Z(G)$ and thus $C_0 = K_0 \cap C(G)$ is non-trivial. This means that in the summation formula of Theorem 6.1(b) at least one of the terms

$$(\dim_{\mathbb{F}_p} C_{i-1} - \dim_{\mathbb{F}_p} C_i) p^i$$

with $i \geq 1$ will be non-zero. Hence, $\text{ed}(G) \geq p$; this shows that (a) and (b) are equivalent. Moreover, equality holds if and only if (i) $\dim_{\mathbb{F}_p} C_{-1} = 1$, (ii) $\dim_{\mathbb{F}_p} C_0 = 1$ and (iii) $C_1$ is trivial. We show that (i), (ii) and (iii) are equivalent to (c):

Since $C_{-1} = C(G)$, (i) is equivalent to $Z(G)$ being cyclic.

Now recall that we are assuming $K_0 = G' \neq \{1\}$. By (6.4) this is equivalent to $C_0 = K_0 \cap C(G) \neq \{1\}$. Since $C_0 \subset C_{-1}$, $C_0$ has dimension at most 1, and (ii) follows from (i).

Finally, (iii) means that

$$K_1 = \bigcap_{[G:H]=p} H'$$

(6.6)

intersects $C(G)$ trivially. Since $K_1$ is a normal subgroup of $G$, (6.4) tells us that (iii) holds if and only if $K_1 = \{1\}$.

We claim that $K_1 = \{1\}$ if and only if $H' = \{1\}$ for some subgroup $H$ of $G$ of index $p$. One direction is obvious: if $H' = \{1\}$ for some $H$ of index $p$ then the intersection (6.6) is trivial. To prove the converse, assume the contrary: the intersection (6.6) is trivial but $H' \neq \{1\}$ for every subgroup $H$ of index $p$. Since every such $H$ is normal in $G$ (and so is $H'$), (6.4) tells us that that $H' \neq \{1\}$ if and only if $H' \cap Z(G) \neq \{1\}$. Since $Z(G)$ is cyclic, the latter condition is equivalent to $C(G) \subset H'$. Thus

$$C(G) \subset K_1 = \bigcap_{[G:H]=p} H',$$

contradicting our assumption that $K_1 = \{1\}$. This proves (c) is equivalent to (a) and (b).

$p$-groups that have a faithful representation of degree $p$ over a field $k$, satisfying (6.1) are described in [LGP86, II.4, III.4, IV.2]; see also [Vol63]. They are exactly the subgroups of $\mathbb{Z}/p^\alpha \cap \mathbb{Z}/p$, where $k$ contains a primitive root of unity of degree $p^\alpha$. Part (d) follows. \qed
7

\textbf{GL}(\mathbb{Z}) \text{ and } \text{SL}(\mathbb{Z})

\subsection*{7.1 \textbf{Forms of Algebraic Groups}}

The notion of \textit{forms} of an algebraic object is variation of the same principle we already encountered which relates an algebraic structure with cohomology. We use the notion of forms here since we want to work with automorphism groups of algebraic groups. The automorphism groups themselves need not be algebraic, i.e. they are not necessarily of finite type over the base field. This however is not a problem and one defines the essential dimension of an affine group scheme in the same way as we defined it for affine algebraic groups.

Let $G$ be an algebraic group over $k$ and $K/k$ a field. We say an algebraic $K$-group $G'$ is a $L/K$-\textit{form} of $G$ if $G'_L \simeq G_L$, or simply a $K$-\textit{form} of $G$ if $G'_K \text{sep} \simeq G_K \text{sep}$. We can define a functor

\[ \text{Forms}_G : \text{Fields}/k \to \text{Sets} \]

\[ K \mapsto \{K\text{-forms of } G \}/ \simeq \]

Now let $\text{Aut}(G)$ be the automorphism group of $G$. Then there is an equivalence of functors

\[ \text{Forms}_G \simeq H^1(\ast, \text{Aut}(G)), \]

see [Ser62b, III 1.3].

\subsection*{7.2 \textbf{Forms of Algebraic Tori}}

Define a functor $\text{Fields}/k \to \text{Sets}$ by

\[ \mathcal{Tori}_n(K) = \{n\text{-dimensional } K\text{-tori}\}/ \simeq \]

Since every $n$-dimensional $K$-torus is split over $K_{\text{sep}}$, i.e. isomorphic to $\mathbb{G}_m^n$ and $\text{Aut}(\mathbb{G}_m^n) = \text{GL}_n(\mathbb{Z})$ we have equivalences

\[ \mathcal{Tori}_n \simeq \text{Forms}(\mathbb{G}_m^n) \simeq H^1(\ast, \text{GL}_n(\mathbb{Z})). \]
As a variant of this we define
\[ \mathfrak{T}_n^1(K) = \{ \text{n-dimensional } K\text{-tori } T \mid \phi_T \subset SL_n(\mathbb{Z}) \} / \cong \]
where \( K/k \) is a field extension and \( \phi_T : \text{Gal}(K) \to GL_n(\mathbb{Z}) \) is the natural representation of the Galois group of \( K \) on the character lattice of the torus \( T \). A slightly different description of \( \mathfrak{T}_n^1 \) is given in [FF08, 5] as the functor of pairs \((T, t)\) where \( T \) is an \( n \)-dimensional torus and \( t : \wedge^n T \to \mathbb{G}_m \) an isomorphism. There is an equivalence
\[ \mathfrak{T}_n^1 \simeq H^1(\ast, SL_n(\mathbb{Z})). \]

Both \( GL_n(\mathbb{Z}) \) and \( SL_n(\mathbb{Z}) \) are not algebraic, but we define their essential dimension as in the algebraic case as the essential dimension of the functors \( H^1(\ast, GL_n(\mathbb{Z})) \) and \( H^1(\ast, SL_n(\mathbb{Z})) \) respectively.

The essential dimension of \( GL_n(\mathbb{Z}) \) and \( SL_n(\mathbb{Z}) \) was first studied by G. Favi and M. Florence [FF08], who showed that \( ed(GL_n(\mathbb{Z})) = n \) for every \( n \geq 1 \) and \( ed(SL_n(\mathbb{Z})) = n - 1 \) for every odd \( n \). For even \( n \) Favi and Florence showed that \( ed(SL_n(\mathbb{Z})) = n - 1 \) or \( n \) and left the exact value of \( ed(SL_n(\mathbb{Z})) \) for \( n \geq 4 \) as an open question. We answer this question and also compute the essential \( p \)-dimension of \( GL_n(\mathbb{Z}) \) and \( SL_n(\mathbb{Z}) \) for every prime \( p \).

**Theorem 7.1.** Suppose \( k \) is a field of characteristic \( \neq 2 \). Then

(a) \( ed(GL_n(\mathbb{Z}); 2) = ed(GL_n(\mathbb{Z})) = n. \)

(b) \( ed(SL_n(\mathbb{Z}); 2) = ed(SL_n(\mathbb{Z})) = \begin{cases} n - 1, & \text{if } n \text{ is odd,} \\ n, & \text{if } n \text{ is even} \end{cases} \) for any \( n \geq 3. \)

**Remark.** For completeness we also record that \( ed(SL_2(\mathbb{Z})) = 1 \) if \( k \) contains a 12th root of unity, see [FF08, Remark 5.5(2)]. It is interesting to note that while the value of \( ed(SL_2(\mathbb{Z})) \) depends on the base field \( k \), for \( n \geq 3 \), the value of \( ed(SL_n(\mathbb{Z})) \) does not (as long as \( \text{char}(k) \neq 2 \)).

**Theorem 7.2.** Let \( p \) be an odd prime, \( \text{char} k \neq p \) and \( k \) contains a primitive \( p \)-th root of unity.

\[ ed(SL_n(\mathbb{Z}); p) = ed(GL_n(\mathbb{Z}); p) = \left\lfloor \frac{n}{p-1} \right\rfloor. \]

G. Favi and M. Florence [FF08] showed that for \( \Gamma = GL_n(\mathbb{Z}) \) or \( SL_n(\mathbb{Z}) \),

\[ ed(\Gamma) = \max \{ ed(F) \mid F \text{ finite subgroup of } \Gamma \}. \quad (7.1) \]
A minor modification of the arguments in [FF08] shows that (7.1) holds also for essential dimension at a prime $p$:

$$\text{ed}(\Gamma; p) = \max\{\text{ed}(F; p) | F \text{ a finite subgroup of } \Gamma\}, \quad (7.2)$$

or, by Theorem 5.2 equivalently

$$\text{ed}(\Gamma; p) = \max\{\text{ed}(F; p) | F \text{ a finite } p\text{-subgroup of } \Gamma\}, \quad (7.3)$$

The finite groups $F$ that Florence and Favi used to find the essential dimension of $\text{GL}_n(\mathbb{Z})$ and $\text{SL}_n(\mathbb{Z})$ ($n$ odd) are $(\mathbb{Z}/2\mathbb{Z})^n$ and $(\mathbb{Z}/2\mathbb{Z})^{n-1}$ respectively. Thus $\text{ed}(\text{GL}_n(\mathbb{Z}); 2) = \text{ed}(\text{GL}_n(\mathbb{Z})) = n$ for every $n \geq 1$ and $\text{ed}(\text{SL}_n(\mathbb{Z}); 2) = \text{ed}(\text{SL}_n(\mathbb{Z})) = n - 1$ if $n$ is odd.

Our proof of Theorem 7.1 will rely on Corollary 6.1. 

**Proof of Theorem 7.1.** We assume that $n = 2d \geq 4$ is even. To prove Theorem 7.1 it suffices to find a 2-subgroup $F$ of $\text{SL}_n(\mathbb{Z})$ of essential dimension $n$.

Diagonal matrices and permutation matrices generate a subgroup of $\text{GL}_n(\mathbb{Z})$ isomorphic to $\mu_2^n \rtimes S_n$. The determinant function restricts to a homomorphism $\text{det}: \mu_2^n \rtimes S_n \to \mu_2$ sending $((\varepsilon_1, \ldots, \varepsilon_n), \tau) \in \mu_2^n \rtimes S_n$ to the product $\varepsilon_1 \varepsilon_2 \cdots \varepsilon_n \cdot \text{sign}(\tau)$. Let $P_n$ be a Sylow 2-subgroup of $S_n$ and $F_n$ be the kernel of

$$\text{det}: \mu_2^n \rtimes P_n \to \mu_2.$$

By construction $F_n$ is a finite 2-group contained in $\text{SL}_n(\mathbb{Z})$. Theorem 7.1 is now a consequence of the following proposition.

**Proposition 7.1.** If $\text{char}(k) \neq 2$ then $\text{ed}(F_{2d}) = 2d$ for any $d \geq 2$.

To prove the proposition, let

$$D_{2d} = \{\text{diag}(\varepsilon_1, \ldots, \varepsilon_{2d}) | \text{ each } \varepsilon_i = \pm 1 \text{ and } \varepsilon_1 \varepsilon_2 \cdots \varepsilon_{2d} = 1\}$$

be the subgroup of “diagonal” matrices contained in $F_{2d}$.

Since $D_{2d} \simeq \mu_2^{2d-1}$ has essential dimension $\geq 2d - 1$, we see that $\text{ed}(F_{2d}) \geq \text{ed}(D_{2d}) = 2d - 1$. On the other hand the inclusion $F_{2d} \subset \text{SL}_{2d}(\mathbb{Z})$ gives rise to a $2d$-dimensional representation of $F_{2d}$, which remains faithful over any field $k$ of characteristic $\neq 2$. Hence, $\text{ed}(F_{2d}) \leq 2d$. We thus conclude that

$$\text{ed}(F_{2d}) = 2d - 1 \text{ or } 2d. \quad (7.4)$$
Using elementary group theory, one easily checks that
\[ C(F_{2d}) \subset [F_{2d}, F_{2d}] \subset F_{2d}' . \]  
(7.5)
Thus, if \( k' \supset k \) is a field as in (6.1), \( ed_k'(F_{2d}) \) is even by Corollary 6.1; since \( ed(F_{2d}) \geq ed_k'(F_{2d}) \), (7.4) now tells us that \( ed(F_{2d}) = 2d \). This completes the proof of Proposition 7.1 and thus of Theorem 7.1.

**Remark.** (a) The assumption that \( d \geq 2 \) is essential in the proof of the inclusion (7.5). In fact, \( F_2 \cong \mathbb{Z}/4\mathbb{Z} \), so (7.5) fails for \( d = 1 \).

(b) Note that for any integers \( m, n \geq 2 \), \( F_{m+n} \) contains the direct product \( F_m \times F_n \). Thus
\[
ed(F_{m+n}) \geq ed(F_m \times F_n) = ed(F_m) + ed(F_n),
\]
where the last equality follows from Theorem 1.1. Thus Proposition 7.1 only needs to be proved for \( d = 2 \) and 3 (or equivalently, \( n = 4 \) and 6); all other cases are easily deduced from these by applying the above inequality recursively, with \( m = 4 \). In particular, the group-theoretic inclusion (7.5) only needs to be checked for \( d = 2 \) and 3. Somewhat to our surprise, this reduction does not appear to simplify the proof of Proposition 7.1 presented above to any significant degree.

**Proof of Theorem 7.2.** First we let \( \Gamma = \text{GL}_n(\mathbb{Z}) \). Maximal \( p \)-subgroups of \( \text{GL}_n(\mathbb{Z}) \) were described by Abold and Plesken [AP78]. Let \( m = [n/(p-1)] \) and denote by \( \mathcal{C}_p \) the cyclic group of order \( p \) and \( \mathcal{P}_m \) a Sylow-\( p \) subgroup of the symmetric group \( \mathcal{S}_m \). By [AP78, Satz], every \( p \)-subgroup \( H \) of \( \Gamma \) is \( \mathbb{Q} \)-conjugate to a subgroup of the wreath product
\[
G = \mathcal{C}_p \wr \mathcal{P}_m = \mathcal{C}_p^m \rtimes \mathcal{P}_m.
\]
Since \( ed(H; p) \leq ed(G; p) = ed(G) \), with (7.3) we have \( ed(\Gamma; p) = ed(G) \). It remains to show that \( ed(G) = m = [n/(p-1)] \).

Write \( m \) in the \( p \)-adic expansion (omitting 0 terms):
\[
m = a_r p^r + a_{r-1} p^{r-1} + \ldots + a_1 p + a_0
\]
with \( 0 < a_i < p \) for all \( i \). Then \( \mathcal{P}_m \) splits up into a direct product of \( \mathcal{P}_{p^i} \) and using that \( \mathcal{C}_p \wr \mathcal{P}_{p^i} \cong \mathcal{P}_{p^{i+1}} \),
\[
G \cong (\mathcal{P}_{p^r})^{a_r} \times (\mathcal{P}_{p^r})^{a_{r-1}} \times \ldots \times (\mathcal{P}_{p^1})^{a_1} \times (\mathcal{P}_{p})^{a_0}
\]
The essential dimension of $P_{p+1}$ is $\text{ed}(P_{p+1}; p) = \text{ed}(P_{p+1}; p) = p^i$, see Corollary 5.1. Since $G$ is a $p$-group, by additivity Theorem 5.3, the essential dimension of $G$ is the sum

$$\text{ed}_p(G) = a_r \text{ed}_p(P_{p+1}) + \ldots + a_1 \text{ed}_p(P_2) + a_0 \text{ed}_p(P) = m$$

This shows that $\text{ed}(\text{GL}_n(\mathbb{Z}); p) = \text{ed}(G; p) = m$. To conclude the same for $\text{ed}(\text{SL}_n(\mathbb{Z}); p)$ we need only note that $G$ is a subgroup of $\text{SL}_n(\mathbb{Z})$, which is clear since every element of $G$ has finite, odd order and therefore its determinant is equal to 1. □
8

Algebraic Tori

It was noted in Lemma 3.5 that if $G$ is an algebraic group, every generically free linear representation $\rho : G \to \text{GL}(V)$ gives rise to a versal $G$-torsor and we obtain the inequality

$$\text{ed}(G; p) \leq \text{ed}(G) \leq \dim(V) - \dim(G).$$

(8.1)

We are interested in groups for which this inequality is sharp.

Karpenko and Merkurjev’s Theorem 1.1 says that finite constant $p$-groups have this property. In this chapter we will prove similar formulas for a broader class of groups. The main result is Theorem 8.2. As consequences of this theorem we obtain the exact value of $\text{ed}(G; p)$ in terms of representations or lattices, where $G$ is an algebraic torus or a finite (twisted) group, as stated in Section 2.1.

The last two sections are intended to illustrate our results by computing essential dimensions of specific algebraic tori. In Section 8.7 we classify algebraic tori $T$ of essential $p$-dimension 0 and 1 and in Section 8.8 we compute the essential $p$-dimension of all tori $T$ over a $p$-closed field $k$, which are split by a cyclic extension $l/k$ of degree dividing $p^2$.

In this chapter we will often write ”$\text{ed}_k$” instead of ”$\text{ed}$” since the base field will be changed sometimes and it is good to keep track of it.

8.1 A Lower Bound

Let

$$1 \to C \to G \to Q \to 1$$

(8.2)

be an exact sequence of algebraic groups over $k$ such that $C$ is central in $G$ and isomorphic to $\mu_p^r$ for some $r \geq 0$. Given a character $\chi : C \to \mu_p$, we will, following [KM08], denote by $\text{Rep}^\chi$ the set of irreducible representations $\phi : G \to \text{GL}(V)$, defined over $k$, such that $\phi(c) = \chi(c) \text{Id}_V$ for every $c \in C$.

**Theorem 8.1.** Assume that $k$ is a field of characteristic $\neq p$ containing a primitive $p$th root of unity. Suppose a sequence of the form (8.2) satisfies the following
condition:
\[ \gcd\{\dim(\phi) \mid \phi \in \text{Rep}^X \} = \min\{\dim(\phi) \mid \phi \in \text{Rep}^X \} \]
for every character \( \chi : C \to \mu_p \). Then
\[ \text{ed}(G; p) \geq \min \dim(\rho) - \dim G, \]
where the minimum is taken over all finite-dimensional \( k \)-representations \( \rho \) of \( G \) such that \( \rho|_C \) is faithful.

**Proof.** Denote by \( C^* := \text{Hom}(C, \mu_p) \) the character group of \( C \). Let \( E \to \text{Spec} K \) be a versal \( Q \)-torsor \cite[Example 5.4]{GMS03}, where \( K/k \) is some field extension, and let \( \beta : C^* \to \text{Br}_p(K) \) denote the homomorphism that sends \( \chi \in C^* \) to the image of \( E \in H^1(K, Q) \) in \( \text{Br}_p(K) \) under the map \( H^1(K, Q) \to H^2(K, C) \xrightarrow{\chi_*} H^2(K, \mu_p) = \text{Br}_p(K) \)
given by composing the connecting map with \( \chi_* \). Then there exists a basis \( \chi_1, \ldots, \chi_r \) of \( C^* \) such that
\[ \text{ed}_k(G; p) \geq \sum_{i=1}^r \text{Ind} \beta(\chi_i) - \dim G, \quad (8.3) \]
see \cite[Theorem 4.8, Example 3.7]{Mer08}. Moreover, by \cite[Theorem 4.4, Remark 4.5]{KM08}
\[ \text{Ind} \beta(\chi_i) = \gcd \dim(\rho) , \]
where the greatest common divisor is taken over all (finite-dimensional) representations \( \rho \) of \( G \) such that \( \rho|_C \) is scalar multiplication by \( \chi_i \). By our assumption, \( \gcd \) can be replaced by \( \min \). Hence, for each \( i \in \{1, \ldots, r\} \) we can choose a representation \( \rho_i \) of \( G \) with
\[ \text{Ind} \beta(\chi_i) = \dim(\rho_i) \]
such that \( (\rho_i)|_C \) is scalar multiplication by \( \chi_i \).

Set \( \rho := \rho_1 \oplus \cdots \oplus \rho_r \). The inequality (8.3) can be written as
\[ \text{ed}_k(G; p) \geq \dim(\rho) - \dim G, \quad (8.4) \]
Since \( \chi_1, \ldots, \chi_r \) forms a basis of \( C^* \) the restriction of \( \rho \) to \( C \) is faithful. This proves the theorem. \( \Box \)
8.2 \( p \)-(FT)-Groups

Of particular interest to us will be \( p \)-(FT)-groups, i.e group \( G \) which fit into an exact sequence of the form

\[
1 \rightarrow T \rightarrow G \rightarrow F \rightarrow 1,
\]

where \( F \) is a finite \( p \)-group and \( T \) is a torus over \( k \), see also section 2.1.

For the sake of computing \( \text{ed}(G; p) \) we may assume that \( k \) is a \( p \)-closed field, see Lemma 4.1. The proofs of the following theorems will be provided in the next sections.

**Theorem 8.2.** Suppose \( \text{char} k \neq p \) and \( k^{(p)} \) denotes a \( p \)-closure of \( k \). Let \( G \) be a \( k \)-group of type \( p \)-(FT). Then

(a) \( \text{ed}_{k}(G; p) \geq \min \dim \rho - \dim G \), where the minimum is taken over all \( p \)-faithful linear representations \( \rho \) of \( G_{k^{(p)}} \) over \( k^{(p)} \).

Now let \( G \) be a \( k \)-group of type \( p \)-(FxT). Then

(b) equality holds in (a), and

(c) over \( k^{(p)} \) the absolute essential dimension of \( G \) and the essential \( p \)-dimension coincide:

\[
\text{ed}_{k^{(p)}}(G) = \text{ed}_{k^{(p)}}(G; p) = \text{ed}_{k}(G; p).
\]

If \( G \) is a \( p \)-group, a representation \( \rho \) is \( p \)-faithful if and only if it is faithful. However, for an algebraic torus, “\( p \)-faithful” cannot be replaced by “faithful”; see Remark [LMMR09, 10.3].

If \( G \) is multiplicative, the value of \( \text{ed}_{k}(G; p) \) given by Theorem 8.2 can be rewritten in terms of the character module \( X(T) \) using Proposition 3.1.

**Corollary 8.1.** Let \( G \) be a direct product of a torus and an abelian \( p \)-group over the \( p \)-closed field \( k \) and \( \Gamma := \text{Gal}(k^{\text{sep}}/k) \) be the absolute Galois group of \( k = k^{(p)} \). Let \( \Gamma \) act through a finite quotient \( \hat{\Gamma} \) on \( X(G) \). Then

\[
\text{ed}_{k}(G) = \text{ed}_{k}(G; p) = \min \text{rk } L - \dim G,
\]

where the minimum is taken over all permutation \( \mathbb{Z}\Gamma \)-lattices \( L \) which admit a map of \( \mathbb{Z}\Gamma \)-modules to \( X(G) \) with cokernel finite of order prime to \( p \). \( \square \)
Let us rephrase the main result first for the most important case, algebraic tori. It is easy to show that if \( T \) is a torus over \( k \) such that its minimal splitting field \( L/k \) is of degree a power of \( p \), then any \( T \)-representation over a \( p \)-closure \( k^{(p)} \) can already be defined over \( k \).

Following [Mer09] we call a homomorphism \( P \to X(T) \) of \( \Gamma \)-lattices a \( p \)-

**presentation** if it has finite cokernel of order prime to \( p \) and \( P \) is permutation. It is called **minimal** if the rank of \( P \) is minimal among all \( p \)-presentations.

**Theorem 8.3.** Let \( T \) be a \( k \)-torus with minimal splitting field \( L/k \). Assume \([L:k]\) is a power of \( p \) and let \( \Gamma = \text{Gal}(L/k) \). The following numbers are equal:

(a) \( \text{ed}_k(T) \)

(b) \( \text{ed}_k(T; p) \)

(c) \( \min\{\dim \rho | p \text{-faithful } T \text{-representation} / k\} - \dim T \)

(d) \( \min\{\text{rk ker } \phi | \phi : P \to X(T) \text{ a } p \text{-presentation} \} \).

(e) \( \min\{\text{rk } L\} \), where the minimum is taken over all exact sequences of \( \mathbb{Z}(p)\Gamma \)-

**lattices of the form**

\[
(0) \to L \to P \to X(T)_{(p)} \to (0),
\]

with \( P \) permutation.

\( \square \)

For the equality of (d) and (e) we use Proposition 3.1, the other equalities are clear from the previous results. In many cases Theorem 8.3 renders the value of \( \text{ed}_k(T) \) computable by known representation-theoretic methods, e.g., from [CR90]. We will give several examples of such computations in Sections 8.7 and 8.8. Another application was recently given by Merkurjev [Mer09], see also Theorem 11.1.

Theorem 8.2 appears to be new even in the other extreme case where \( G \) is a twisted cyclic \( p \)-group. It extends earlier work of Rost [Ros02] (cyclic groups of order 4), Bayarmagnai [Bay07] (cyclic groups of order 8) and Florence [Flo08] (constant cyclic groups).

**Theorem 8.4.** Let \( G \) be a finite algebraic group over a \( p \)-closed field \( k = k^{(p)} \) of characteristic \( \neq p \). Then \( G \) has a Sylow-\( p \) subgroup \( G_p \) defined over \( k \) and

\[ \text{ed}_k(G; p) = \text{ed}_k(G_p; p) = \text{ed}_k(G_p) = \min \dim(\rho) \]

where the minimum is taken over all faithful representations of \( G_p \) over \( k \).
Proof. By assumption, \( \Gamma = \text{Gal}(k_{\text{sep}}/k) \) is a pro-\( p \) group. It acts on the set of Sylow-\( p \) subgroups of \( G(k_{\text{sep}}) \). Since the number of such subgroups is prime to \( p \), \( \Gamma \) fixes at least one of them and by Galois descent one obtains a subgroup \( G_p \) of \( G \). By Lemma 5.1, \( G_p \) is a Sylow-\( p \) subgroup of \( G \). The first equality \( \text{ed}_k(G; p) = \text{ed}_k(G_p; p) \) is proved in Theorem 5.2. The minimal \( G_p \)-representation \( \rho \) from Theorem 8.2(b) is faithful and thus \( \text{ed}_k(G_p) \leq \dim(\rho) \), see for example [BF03, Prop. 4.11]. \( \square \)

Remark. Two Sylow-\( p \) subgroups of \( G \) defined over \( k = k^{(p)} \) do not need to be isomorphic over \( k \).

Corollary 8.2. Let \( A \) be a finite (twisted) cyclic \( p \)-group over \( k \). Let \( l/k \) be a minimal Galois splitting field of \( A \). Then

\[
\text{ed}(A; p) = |\text{Gal}(l/k)|_p = |\text{Gal}(l^{(p)}/k^{(p)})|, 
\]

where \( |\text{Gal}(l/k)|_p \) denotes the \( p \)-primary part of \( |\text{Gal}(l/k)| \).

Note that for \( p = 2 \) we have \( |\text{Gal}(l/k)|_p = |\text{Gal}(l/k)| \) above since the automorphism group of \( X(A) \cong \mathbb{Z}/2^n\mathbb{Z} \) is a 2-group.

Proof. The second equality follows from the properties of the \( p \)-closure. Moreover \( l^{(p)} \) is a minimal Galois splitting field of \( A_{k^{(p)}} \). Since the essential \( p \)-dimension of \( A \) does not change when passing to the \( p \)-closure, we can assume \( k = k^{(p)} \). Set \( \Gamma = \text{Gal}(l/k) \) which is now automatically a \( p \)-group. By Corollary 8.1 \( \text{ed}(A; p) \) is equal to the least cardinality of a \( \Gamma \)-set \( \Lambda \) such that there exists a map \( \phi : \mathbb{Z}[\Lambda] \to X(A) \) of \( \mathbb{Z}[\Gamma] \)-modules with cokernel finite of order prime to \( p \). The group \( X(A) \) is a (cyclic) \( p \)-group, hence \( \phi \) must be surjective. Moreover \( \Gamma \) acts faithfully on \( X(A) \). Surjectivity of \( \phi \) implies that some element \( \lambda \in \Lambda \) maps to a generator \( a \) of \( X(A) \). Hence \( |\Lambda| \geq |\Gamma \lambda| \geq |\Gamma a| = |\Gamma| \). Conversely we have a surjective homomorphism \( \mathbb{Z}[\Gamma] \to X(A) \) that sends \( a \) to itself. \( \square \)

It is natural to try to extend the formula of Theorem 8.2(b) to all groups \( G \) of type \( p \)-(FT) or all (FT) for that matter, by Theorem 5.2. Suppose that \( k \) is \( p \)-closed. Then by Theorem 8.2(a) and Lemma 3.5,

\[
\min \dim \mu - \dim(G) \leq \text{ed}(G; p) \leq \min \dim \rho - \dim(G), \tag{8.6}
\]

where the two minima are taken over all \( p \)-faithful representations \( \mu \), and \( p \)-generically free representations \( \rho \), respectively. If \( G \) is a direct product of a
torus and a \( p \)-group, then every \( p \)-generically free representation is \( p \)-faithful, see Lemma 3.2, so in this case the lower and upper bounds coincide, yielding the exact value of \( \text{ed}_k(G; p) \) of Theorem 8.2(b). However, if we only assume \( G \) is a \( p \)-group extended by a torus, then faithful \( G \)-representations no longer need to be generically free, see example 3.1. We put forward the following conjecture.

**Conjecture.** Let \( G \) be of type \((\text{FT})\) and \( k \) of characteristic \( \neq p \). Then

\[
\text{ed}(G; p) = \min \dim \rho - \dim G,
\]

where the minimum is taken over all \( p \)-generically free representations \( \rho \) of \( G_{k[p]} \) over \( k^{(p)} \).

### 8.3 The Central Split Group \( C(G) \)

Let \( A \) be a group of multiplicative type and \( A[p] \) the \( p \)-torsion subgroup \( \{ a \in A \mid a^p = 1 \} \) of \( A \). Clearly \( A[p] \) is defined over \( k \).

If \( T \) is a torus it is well known how to construct a maximal split subtorus of \( T \), see for example [Bor61, 8.15] or [Wat79, 7.4]. The following definition is a variant of this.

**Definition 8.1.** Let \( A \) be an algebraic group of multiplicative type over \( k \). Let \( \Delta(A) \) be the \( \Gamma \)-invariant subgroup of \( X(A) \) generated by elements of the form \( x - \gamma(x) \), as \( x \) ranges over \( X(A) \) and \( \gamma \) ranges over \( \Gamma \). Alternatively, \( \Delta(A) = IX(A) \) where \( I \) is the augmentation ideal in \( \mathbb{Z}\Gamma \). Define

\[
\text{Split}_k(A) = \text{Diag}(X(A)/\Delta(A)).
\]

**Definition 8.2.** Let \( G \) be a \( p \)-(\text{FT})-group as in (8.5).

\[
C(G) := \text{Split}_k(Z(G)[p]),
\]

where \( Z(G) \) denotes the centre of \( G \).

If \( X = X(Z(G)) \), we have \( C(G) = \text{Diag}(X/(pX + IX)) \) where again \( I \) is the augmentation ideal of \( X \) in \( \mathbb{Z}\Gamma \), see [Mer09, Section 4].

**Lemma 8.1.** Let \( A \) be an algebraic group of multiplicative type over \( k \).

(a) \( \text{Split}_k(A) \) is split over \( k \),
(b) \( \text{Split}_k(A) = A \) if and only if \( A \) is split over \( k \).

(c) If \( B \) is a \( k \)-subgroup of \( A \) then \( \text{Split}_k(B) \subset \text{Split}_k(A) \).

(d) For \( A = A_1 \times A_2 \), \( \text{Split}_k(A_1 \times A_2) = \text{Split}_k(A_1) \times \text{Split}_k(A_2) \).

(e) If \( A[p] \neq \{1\} \) and \( A \) is split over a Galois extension \( l/k \), such that \( \Gamma = \text{Gal}(l/k) \) is a p-group, then \( \text{Split}_k(A) \neq \{1\} \).

**Proof.** Parts (a), (b), (c) and (d) easily follow from the definition.

Proof of (e): By part (c), it suffices to show that \( \text{Split}_k(A[p]) \neq \{1\} \). Hence, we may assume that \( A = A[p] \) or equivalently, that \( X(A) \) is a finite-dimensional \( \mathbb{F}_p \)-vector space on which the \( p \)-group \( \Gamma \) acts. Any such action is upper-triangular, relative to some \( \mathbb{F}_p \)-basis \( e_1, \ldots, e_n \) of \( X(A) \); see, e.g., [Ser77, Proposition 26]. That is,

\[ \gamma(e_i) = e_i + (\mathbb{F}_p \text{-linear combination of } e_{i+1}, \ldots, e_n) \]

for every \( i = 1, \ldots, n \) and every \( \gamma \in \Gamma \). Our goal is to show that \( \Delta(A) \neq X(A) \). Indeed, every element of the form \( x - \gamma(x) \) is contained in the \( \Gamma \)-invariant submodule \( \text{Span}(e_2, \ldots, e_n) \). Hence, these elements cannot generate all of \( X(A) \).

**Proposition 8.1.** Suppose \( G \) is a \( p \)-(FT) group over a \( p \)-closed field \( k \). Suppose \( N \) is a normal subgroup of \( G \). Then the following conditions are equivalent:

(a) \( N \) is finite of order prime to \( p \),

(b) \( N \cap C(G) = \{1\} \),

(c) \( N \cap Z(G)[p] = \{1\} \)

In particular, taking \( N = G \), we see that \( C(G) \neq \{1\} \) if \( G \neq \{1\} \).

**Proof.** (i) \( \Rightarrow \) (ii) is obvious, since \( C(G) \) is a \( p \)-group.

(ii) \( \Rightarrow \) (iii). Assume the contrary: \( A := N \cap Z(G)[p] \neq \{1\} \). By Lemma 8.1

\[ \{1\} \neq C(A) \subset N \cap C(Z(G)[p]) = N \cap C(G), \]

contradicting (ii).

Our proof of the implication (iii) \( \Rightarrow \) (i), will rely on the following

Claim: Let \( M \) be a non-trivial normal finite \( p \)-subgroup of \( G \) such that the commutator \( (G^0, M) = \{1\} \). Then \( M \cap Z(G)[p] \neq \{1\} \).
To prove the claim, note that $M(k_{\text{sep}})$ is non-trivial and the conjugation action of $G(k_{\text{sep}})$ on $M(k_{\text{sep}})$ factors through an action of the $p$-group $(G/G^0)(k_{\text{sep}})$. Thus each orbit has $p^n$ elements for some $n \geq 0$; consequently, the number of fixed points is divisible by $p$. The intersection $(M \cap Z(G))(k_{\text{sep}})$ is precisely the fixed point set for this action; hence, $M \cap Z(G)[p] \neq \{1\}$. This proves the claim.

We now continue with the proof of the implication (iii) $\implies$ (i). For notational convenience, set $T := G^0$. Assume that $N \trianglelefteq G$ and $N \cap Z(G)[p] = \{1\}$. Applying the claim to the normal subgroup $M := (N \cap T)[p]$ of $G$, we see that $(N \cap T)[p] = \{1\}$, i.e., $N \cap T$ is a finite group of order prime to $p$. The exact sequence

$$1 \to N \cap T \to N \to \overline{N} \to 1,$$  \hspace{1cm} (8.7)

where $\overline{N}$ is the image of $N$ in $G/T$, shows that $N$ is finite. Now observe that for every $r \geq 1$, the commutator $(N,T[p^r])$ is a $p$-subgroup of $N \cap T$. Thus $(N,T[p^r]) = \{1\}$ for every $r \geq 1$. We claim that this implies $(N,T) = \{1\}$ by Zariski density. If $N$ is smooth, this is straightforward; see [Bor61, Proposition 2.4, p. 59]. If $N$ is not smooth, note that the map $c: N \times T \to G$ sending $(n,t)$ to the commutator $ntn^{-1}t^{-1}$ descends to $\overline{c}: \overline{N} \times T \to G$ (indeed, $N \cap T$ clearly commutes with $T$). Since $|\overline{N}|$ is a power of $p$ and $\text{char}(k) \neq p$, $\overline{N}$ is smooth over $k$, and we can pass to the separable closure $k_{\text{sep}}$ and apply the usual Zariski density argument to show that the image of $\overline{c}$ is trivial.

We thus conclude that $N \cap T$ is central in $N$. Since $\gcd(|N \cap T|, \overline{N}) = 1$, by [Sch80a, Corollary 5.4] the extension (8.7) splits, i.e., $N \simeq (N \cap T) \times \overline{N}$. This turns $\overline{N}$ into a subgroup of $G$ satisfying the conditions of the claim. Therefore $\overline{N}$ is trivial and $N = N \cap T$ is a finite group of order prime to $p$, as claimed. \hfill \Box

For future reference, we record the following obvious consequence of the equivalence of conditions (i) and (ii) in Proposition 8.1.

**Corollary 8.3.** Let $k = k^{(p)}$ be a $p$-closed field and $G$ be a $p$-(FT) group over $k$, as in (8.5). A finite-dimensional representation $\rho$ of $G$ defined over $k$ is $p$-faithful if and only if $\rho|_{C(G)}$ is faithful. \hfill \Box

### 8.4 Proof of Theorem 8.2 (a) and (b)

The key step in our proof will be the following proposition.

**Proposition 8.2.** Let $k$ be a $p$-closed field, and $G$ be a $p$-(FT) group, as in (8.5). Then the dimension of every irreducible representation of $G$ over $k$ is a power of $p$. 


Assuming Proposition 8.2 we can easily complete the proof of Theorem 8.2(a) and (b). The proof of part (c) will be postponed until section 8.6. Indeed, by Proposition 4.2 we may assume that \( k = k^{(p)} \) is \( p \)-closed. In particular, since we are assuming that \( \text{char}(k) \neq p \), this implies that \( k \) contains a primitive \( p \)th root of unity, see Remark 4.1. Proposition 8.2 tells us that Theorem 8.1 can be applied to the exact sequence

\[
1 \to C(G) \to G \to \mathbb{Q} \to 1.
\]

(8.8)

This yields

\[
ed(G; p) \geq \min \dim(\rho) - \dim(G),
\]

(8.9)

where the minimum is taken over all representations \( \rho : G \to \text{GL}(V) \) such that \( \rho|_{C(G)} \) is faithful. By Corollary 8.3, \( \rho|_{C(G)} \) is faithful if and only if \( \rho \) is \( p \)-faithful, and Theorem 8.2(a) follows. Part (b) follows from our preparations in Chapter 3; Lemma 3.1 and 11.1.

The rest of this section will be devoted to the proof of Proposition 8.2. We begin by settling it in the case where \( G \) is a finite \( p \)-group.

**Lemma 8.2.** Proposition 8.2 holds if \( G \) is a finite \( p \)-group.

*Proof.* Choose a finite Galois field extension \( l/k \) such that (i) \( G \) is constant over \( l \) and (ii) every irreducible linear representation of \( G \) over \( l \) is absolutely irreducible. Since \( k \) is assumed to be \( p \)-closed, \( [l : k] \) is a power of \( p \).

Let \( A := k[G]^* \) be the dual Hopf algebra of the coordinate algebra of \( G \). By [Jan03, Section 8.6] a \( G \)-module structure on a \( k \)-vector space \( V \) is equivalent to an \( A \)-module structure on \( V \). Now assume that \( V \) is an irreducible \( A \)-module and let \( W \subseteq V \otimes_k l \) be an irreducible \( A \otimes_k l \)-submodule. Then by [Kar89, Theorem 5.22] there exists a divisor \( e \) of \( [l : k] \) such that

\[
V \otimes l \simeq e \left( \bigoplus_{i=1}^{r} \sigma_i W \right),
\]

where \( \sigma_i \in \text{Gal}(l/k) \) and \( \{\sigma_i W \mid 1 \leq i \leq r\} \) are the pairwise non-isomorphic Galois conjugates of \( W \). By our assumption on \( k, e \) and \( r \) are powers of \( p \) and by our choice of \( l, \dim_l W = \dim_l(\sigma_1 W) = \ldots = \dim_l(\sigma_r W) \) is also a power of \( p \), since it divides the order of \( G_\ell \). Hence, so is \( \dim_k(V) = \dim_l V \otimes l = e(\dim_l \sigma_1 W + \ldots + \dim_l \sigma_r W) \).

Our proof of Proposition 8.2 in full generality will based on leveraging Lemma 8.2 as follows.
Lemma 8.3. Let $G$ be an algebraic group defined over a field $k$ and

$$F_1 \subseteq F_2 \subseteq \cdots \subseteq G$$

be an ascending sequence of finite $k$-subgroups whose union $\bigcup_{n \geq 1} F_n$ is Zariski dense in $G$. If $\rho : G \to \text{GL}(V)$ is an irreducible representation of $G$ defined over $k$ then $\rho|_{F_i}$ is irreducible for sufficiently large integers $i$.

Proof. For each $d = 1, \ldots, \dim(V) - 1$ consider the $G$-action on the Grassmannian $\text{Gr}(d, V)$ of $d$-dimensional subspaces of $V$. Let $X^{(d)} = \text{Gr}(d, V)^G$ and $X_i^{(d)} = \text{Gr}(d, V)^{F_i}$ be the subvariety of $d$-dimensional $G$- (resp. $F_i$-)invariant subspaces of $V$. Then $X_1^{(d)} \supseteq X_2^{(d)} \supseteq \cdots$ and since the union of the groups $F_i$ is dense in $G$,

$$X^{(d)} = \bigcap_{i \geq 0} X_i^{(d)}.$$  

By the Noetherian property of $\text{Gr}(d, V)$, we have $X^{(d)} = X_{m_d}^{(d)}$ for some $m_d \geq 0$.

Since $V$ does not have any $G$-invariant $d$-dimensional $k$-subspaces, we know that $X^{(d)}(k) = \emptyset$. Thus, $X_{m_d}^{(d)}(k) = \emptyset$, i.e., $V$ does not have any $F_{m_d}$-invariant $d$-dimensional $k$-subspaces. Setting $m := \max\{m_1, \ldots, m_{\dim(V) - 1}\}$, we see that $\rho|_{F_m}$ is irreducible. \hfill $\square$

We now proceed with the proof of Proposition 8.2. By Lemmas 8.2 and 8.3, it suffices to construct a sequence of finite $p$-subgroups

$$F_1 \subseteq F_2 \subseteq \cdots \subseteq G$$

defined over $k$ whose union $\bigcup_{n \geq 1} F_n$ is Zariski dense in $G$.

In fact, it suffices to construct one $p$-subgroup $F' \subseteq G$, defined over $k$ such that $F'$ surjects onto $F$. Indeed, once $F'$ is constructed, we can define $F_i \subseteq G$ as the subgroup generated by $F'$ and $T[p^i]$, for every $i \geq 0$. Since $\bigcup_{n \geq 1} F_n$ contains both $F'$ and $T[p^i]$, for every $i \geq 0$ it is Zariski dense in $G$, as desired.

The following lemma, which establishes the existence of $F'$, is thus the final step in our proof of Proposition 8.2 (and hence, of Theorem 8.2(a)).

Lemma 8.4. Let $1 \to T \to G \xrightarrow{\pi} F \to 1$ be an extension of a $p$-group $F$ by a torus $T$ over $k$. Then $G$ has a finite $p$-subgroup $F'$ with $\pi(F') = F$.

In the case where $F$ is split and $k$ is algebraically closed this is proved in [CGR06, p. 564]; cf. also the proof of [BS64, 5.11].
Proof. Denote by $\tilde{\text{Ex}}^1(F,T)$ the group of equivalence classes of extensions of $F$ by $T$. We claim that $\tilde{\text{Ex}}^1(F,T)$ is torsion. Let $\text{Ex}^1(F,T) \subset \tilde{\text{Ex}}^1(F,T)$ be the classes of extensions which have a scheme-theoretic section (i.e. $G(K) \rightarrow F(K)$ is surjective for all $K/k$). There is a natural isomorphism $\text{Ex}^1(F,T) \simeq H^2(F,T)$, where the latter one denotes Hochschild cohomology, see [DG70a, III. 6.2, Proposition]. By [Sch81] the usual restriction-corestriction arguments can be applied in Hochschild cohomology and in particular, $m \cdot H^2(F,T) = 0$ where $m$ is the order of $F$. Now recall that $M \mapsto \tilde{\text{Ex}}^i(F,M)$ and $M \mapsto \text{Ex}^i(F,M)$ are both derived functors of the crossed homomorphisms $M \mapsto \text{Ex}^0(F,M)$, where in the first case $M$ is in the category of $F$-module sheaves and in the second, $F$-module functors, cf. [DG70a, III. 6.2]. Since $F$ is finite and $T$ an affine scheme, by [Sch80b, Satz 1.2 & Satz 3.3] there is an exact sequence of $F$-module schemes $1 \rightarrow T \rightarrow M_1 \rightarrow M_2 \rightarrow 1$ and an exact sequence $\text{Ex}^0(F,M_1) \rightarrow \text{Ex}^0(F,M_2) \rightarrow \tilde{\text{Ex}}^1(F,T) \rightarrow H^2(F,M_1) \simeq \text{Ex}^1(F,M_1)$. The $F$-module sequence also induces a long exact sequence on $\text{Ex}(F,\ast)$ and we have a diagram

\[ \begin{array}{c}
\tilde{\text{Ex}}^1(F,T) \\
\downarrow \\
\text{Ex}^0(F,M_1) \rightarrow \text{Ex}^0(F,M_2) \rightarrow \text{Ex}^1(F,M_1) \\
\downarrow \\
\text{Ex}^1(F,T)
\end{array} \]

An element in $\tilde{\text{Ex}}^1(F,T)$ can thus be killed first in $\text{Ex}^1(F,M_1)$ so it comes from $\text{Ex}^0(F,M_2)$. Then kill its image in $\text{Ex}^1(F,T) \simeq H^2(F,T)$, so it comes from $\text{Ex}^0(F,M_1)$, hence is $0$ in $\tilde{\text{Ex}}^1(F,T)$. In particular we see that multiplying twice by the order $m$ of $F$, $m^2 \cdot \tilde{\text{Ex}}^1(F,T) = 0$. This proves the claim.

Now let us consider the exact sequence $1 \rightarrow N \rightarrow T \xrightarrow{\times m^2} T \rightarrow 1$, where $N$ is the kernel of multiplication by $m^2$. Clearly $N$ is finite and we have an induced exact sequence

$\tilde{\text{Ex}}^1(F,N) \rightarrow \tilde{\text{Ex}}^1(F,T) \xrightarrow{\times m^2} \tilde{\text{Ex}}^1(F,T)$

which shows that the given extension $G$ comes from an extension $F'$ of $F$ by $N$. Then $G$ is the pushout of $F'$ by $N \rightarrow T$ and we can identify $F'$ with a subgroup of $G$. \[\square\]
8.5 Proof of the Additivity Theorem

Recall the earlier stated

**Theorem 5.3.** Let $k$ be of characteristic $\neq p$.

(a) Let $G$ and $H$ be $(\text{F}x\text{T})$-groups over $k$. Then

$$\text{ed}(G \times H; p) = \text{ed}(G; p) + \text{ed}(H; p).$$

(b)

Let $G, H$ be $p$-$(\text{F}x\text{T})$-groups over $k$ and suppose $k = k^{(p)}$ is $p$-closed. Then

$$\text{ed}(G \times H) = \text{ed}(G) + \text{ed}(H).$$

First we need a lemma. Let $G$ be an algebraic group over $k$ and $C$ be a subgroup of $G$. Denote the minimal dimension of a representation $\rho$ of $G$ (defined over $k$) such that $\rho|_C$ is faithful by $f(G, C)$.

**Lemma 8.5.** For $i = 1, 2$ let $G_i$ be an algebraic group and $C_i$ be a central subgroup of $G_i$. Assume that $C_i$ is isomorphic to $\mu^r_{p^i}$ over $k$ for some $r_1, r_2 \geq 0$. Then

$$f(G_1 \times G_1; C_1 \times C_2) = f(G_1; C_1) + f(G_2; C_2).$$

Our argument is a variant of the proof of [KM08, 5.1], where $G$ is assumed to be a (constant) finite $p$-group and $C$ is the socle of $G$.

**Proof.** For $i = 1, 2$ let $\pi_i : G_1 \times G_2 \to G_i$ be the natural projection and $\varepsilon_i : G_i \to G_1 \times G_2$ be the natural inclusion.

If $\rho_i$ is a $d_i$-dimensional $k$-representation of $G_i$ whose restriction to $C_i$ is faithful, then clearly $\rho_1 \circ \pi_1 \oplus \rho_2 \circ \pi_2$ is a $d_1 + d_2$-dimensional representation of $G_1 \times G_2$ whose restriction to $C_1 \times C_2$ is faithful. This shows that

$$f(G_1 \times G_1; C_1 \times C_2) \leq f(G_1; C_1) + f(G_2; C_2).$$

To prove the opposite inequality, let $\rho : G_1 \times G_2 \to \text{GL}(V)$ be a $k$-representation such that $\rho|_{C_1 \times C_2}$ is faithful, and of minimal dimension

$$d = f(G_1 \times G_1; C_1 \times C_2)$$
with this property. Let $\rho_1, \rho_2, \ldots, \rho_n$ denote the irreducible decomposition factors in a decomposition series of $\rho$. Since $C_1 \times C_2$ is central in $G_1 \times G_2$, each $\rho_i$ restricts to a multiplicative character of $C_1 \times C_2$ which we will denote by $\chi_i$. Moreover since $C_1 \times C_2 \simeq \mu_p^{\alpha_1 + \alpha_2}$ is linearly reductive $\rho|_{C_1 \times C_2}$ is a direct sum $\chi_1^{\oplus d_1} \oplus \cdots \oplus \chi_n^{\oplus d_n}$ where $d_i = \dim V_i$. It is easy to see that the following conditions are equivalent:

(i) $\rho|_{C_1 \times C_2}$ is faithful,

(ii) $\chi_1, \ldots, \chi_n$ generate $(C_1 \times C_2)^*$ as an abelian group.

In particular we may assume that $\rho = \rho_1 \oplus \cdots \oplus \rho_n$. Since $C_i$ is isomorphic to $\mu_p^{\alpha_i}$, we will think of $(C_1 \times C_2)^*$ as a $\mathbb{F}_p$-vector space of dimension $r_1 + r_2$. Since $\rho$ is faithful, so is $\rho_i$, and in particular $\chi_i \mid \rho$.

We claim that it is always possible to replace each $\rho_j$ by $\rho'_j$, where $\rho'_j$ is either $\rho_j \circ \varepsilon_1 \circ \pi_1$ or $\rho_j \circ \varepsilon_2 \circ \pi_2$ such that the restriction of the resulting representation $\rho' = \rho'_1 \oplus \cdots \oplus \rho'_n$ to $C_1 \times C_2$ remains faithful. Since $\dim(\rho) = \dim(\rho')$, we see that $\dim(\rho') = \dim(\rho)$. Moreover, $\rho'$ will then be of the form $\alpha_1 \circ \pi_1 \oplus \alpha_2 \circ \pi_2$, where $\alpha_1$ is a representation of $G_i$ whose restriction to $C_i$ is faithful. Thus, if we can prove the above claim, we will have

$$f(G_1 \times G_1; C_1 \times C_2) = \dim(\rho) = \dim(\rho') = \dim(\alpha_1) + \dim(\alpha_2)$$

as desired.

To prove the claim, we will define $\rho'_j$ recursively for $j = 1, \ldots, n$. Suppose $\rho'_1, \ldots, \rho'_{j-1}$ have already been defined, so that the restriction of

$$\rho'_1 \oplus \cdots \oplus \rho'_{j-1} \oplus \rho_j \cdots \oplus \rho_n$$

to $C_1 \times C_2$ is faithful. For notational simplicity, we will assume that $\rho_1 = \rho'_1, \ldots, \rho_{j-1} = \rho'_{j-1}$. Note that

$$\chi_j = (\chi_j \circ \varepsilon_1 \circ \pi_1) + (\chi_j \circ \varepsilon_2 \circ \pi_2).$$

Since $\chi_1, \ldots, \chi_n$ form a basis $(C_1 \times C_2)^*$ as an $\mathbb{F}_p$-vector space, we see that (a) $\chi_j \circ \varepsilon_1 \circ \pi_1$ or (b) $\chi_j \circ \varepsilon_2 \circ \pi_2$ does not lie in $\text{Span}_{\mathbb{F}_p}(\chi_1, \ldots, \chi_{j-1}, \chi_{j+1}, \ldots, \chi_n)$. Set

$$\rho'_j := \begin{cases} \rho_j \circ \varepsilon_1 \circ \pi_1 & \text{in case (a),} \\ \rho_j \circ \varepsilon_2 \circ \pi_2 & \text{otherwise.} \end{cases}$$
Using the equivalence of (i) and (ii) above, we see that the restriction of
\[ \rho_1 \oplus \cdots \oplus \rho_{j-1} \oplus \rho_j' \oplus \rho_{j+1} \oplus \cdots \oplus \rho_n \]
to C is faithful. This completes the proof of the claim and thus of Lemma 8.5. \( \square \)

**Proof of Theorem 5.3.** Part (a) follows from (b) with Lemma 4.1 and Theorem 5.2. For part (b), let \( C(G) \) be as in Definition 8.2. By Theorem 8.2(b)
\[ \text{ed}(G; p) = f(G, C(G)) - \dim G; \]
cf. Corollary 8.3. Furthermore, we have \( C(G_1 \times G_2) = C(G_1) \times C(G_2) \); cf. Lemma 8.1(d). Applying Lemma 8.5 finishes the proof. \( \square \)

### 8.6 Proof of Theorem 8.2 (c)

We will prove Theorem 8.2(c) by using the lattice point of view and the additivity theorem from Section 8.5.

Let \( \Gamma \) be a finite group. Two \( \mathbb{Z} \Gamma \)-lattices \( M, N \) are said to be in the same *genus* if \( M(p) \cong N(p) \) for all primes \( p \), cf. [CR90, 31A]. It is sufficient to check this condition for divisors \( p \) of the order of \( \Gamma \). By a theorem of A.V. Roiter [CR90, Theorem 31.28] \( M \) and \( N \) are in the same genus if and only if there exists a \( \mathbb{Z} \Gamma \)-lattice \( L \) in the genus of the free \( \mathbb{Z} \Gamma \)-lattice of rank one such that \( M \oplus \mathbb{Z} \Gamma \cong N \oplus L \).

This has the following consequence for essential dimension:

**Proposition 8.3.** Let \( T, T' \) be \( k \)-tori. If the lattices \( X(T), X(T') \) belong to the same genus then \( H^1(K, T) = H^1(K, T') \) for all field extensions of \( K/k \). In particular
\[ \text{ed}_k(T) = \text{ed}_k(T') \quad \text{and} \quad \text{ed}_k(T; \ell) = \text{ed}_k(T'; \ell) \]
for all primes \( \ell \).

**Proof.** Let \( \text{Gal}(k_{\text{sep}}/k) \) act through a finite quotient \( \hat{\Gamma} \) on \( X(T) \) and \( X(T') \). By assumption there exists a \( \mathbb{Z} \hat{\Gamma} \)-lattice \( L \) in the genus of \( \mathbb{Z} \hat{\Gamma} \) such that \( X(T) \oplus \mathbb{Z} \hat{\Gamma} \cong X(T') \oplus L \). The torus \( S = \text{Diag}(\mathbb{Z} \hat{\Gamma}) \) has \( H^1(K, S) = \{1\} \) for all field extensions \( K/k \). The same applies to the torus \( S' = \text{Diag}(L) \) since \( L \) is a direct summand of \( \mathbb{Z} \hat{\Gamma} \). Therefore \( H^1(K, T) = H^1(K, T \times S) = H^1(K, T' \times S') = H^1(K, T') \) for all \( K/k \). This concludes the proof. \( \square \)

**Corollary 8.4.** Let \( k = k^{(p)} \) be a \( p \)-closed field and \( T \) a \( k \)-torus. Then
\[ \text{ed}_k(T) = \text{ed}_k(T; p). \]
Proof. The inequality $\text{ed}_k(T; p) \leq \text{ed}_k(T)$ is clear. By Theorem 8.2(a) there is a $p$-faithful representation $\rho : T \to \text{GL}(V)$ of minimal dimension so that $\text{ed}_k(T; p) = \dim \rho - \dim T$. The representation $\rho$ can be considered as a faithful representation of the torus $T' = T/N$ where $N := \ker \rho$ is finite of order prime to $p$. By construction the character lattices $X(T)$ and $X(T')$ are isomorphic after localization at $p$. Since $\text{Gal}(k_{\text{sep}}/k)$ is a (profinite) $p$-group it follows that $X(T)$ and $X(T')$ belong to the same genus. Hence by Proposition 8.3 we have $\text{ed}_k(T') = \text{ed}_k(T')$. Moreover $\text{ed}_k(T') \leq \dim \rho - \dim T'$, since $\rho$ is a generically free representation of $T'$.

Proof of Theorem 8.2(c). The equality $\text{ed}_{k(p)}(G_{k(p)}; p) = \text{ed}_k(G; p)$ is Lemma 4.1. Now we are assuming $G = T \times F$ for a torus $T$ and a $p$-group $F$ over $k$, which is $p$-closed. Notice that a minimal $p$-faithful representation of $F$ from Theorem 8.2(a) is also faithful, and therefore $\text{ed}_k(F; p) = \text{ed}_k(F)$. Combining this with Corollary 8.4 and the additivity Theorem 5.3, we see

$$\text{ed}(T \times F) \leq \text{ed}(T) + \text{ed}(F) = \text{ed}(T; p) + \text{ed}(F; p) = \text{ed}(T \times F; p) \leq \text{ed}(T \times F).$$

8.7 Tori of Essential Dimension $\leq 1$

Theorem 8.5. Let $k = k^{(p)}$ be a $p$-closed field, $\Gamma = \text{Gal}(k_{\text{alg}}/k)$ be the absolute Galois group of $k$ and $T$ be a torus over $k$. Then the following conditions are equivalent:

(a) $\text{ed}_k(T) = 0$.

(b) $\text{ed}_k(T; p) = 0$.

(c) $X(T)_{(p)}$ is a $\mathbb{Z}(p)\Gamma$-permutation module.

(d) $X(T)$ is an invertible $\mathbb{Z}\Gamma$-lattice (i.e. a direct summand of a permutation lattice).

(e) There is a torus $S$ over $k$ and an isomorphism

$$T \times S \simeq R_{E/k}(\mathbb{G}_m),$$

for some étale algebra $E$ over $k$.

(f) $H^1(K, T) = \{1\}$ for any field $K$ containing $k$. 

8. Algebraic Tori

65
Remark. A prime \( p \) for which any of these statements fails is called a torsion prime of \( T \).

Proof. (a) \( \Leftrightarrow \) (b) by Theorem 8.2(c).

(b) \( \Rightarrow \) (c) follows from Corollary 8.1. Indeed, \( \text{ed}_k(T;p) = 0 \) implies the existence of a \( \mathbb{Z}_p \Gamma \)-permutation lattice \( L \) together with a surjective homomorphism \( \alpha : L \rightarrow X(T)(p) \) such that \( \text{rk} \ L = \text{rk} \ X(T)(p) \). It follows that \( \alpha \) is injective and \( X(T)(p) \cong L \).

(c) \( \Rightarrow \) (d): Let \( L \) be a \( \mathbb{Z} \Gamma \)-permutation lattice such that \( L(p) \cong X(T)(p) \). Then by [CR90, Corollary 31.7] there is a \( \mathbb{Z} \Gamma \)-lattice \( L' \) such that \( L \oplus L' \cong X(T) \oplus L' \).

(d) \( \Leftrightarrow \) (e): A permutation lattice \( P \) can be written as

\[
P = \bigoplus_{i+1} \mathbb{Z}[\Gamma / \Gamma_{L_i}],
\]

for some (separable) extensions \( L_i/k \) and \( \Gamma_{L_i} = \text{Gal}(k_{\text{alg}}/L_i) \). Set \( E = L_1 \times \cdots \times L_m \). The torus corresponding to \( P \) is exactly \( R_{E/k}(\mathbb{G}_m) \), cf. [Vos98, 3. Example 19].

(e) \( \Rightarrow \) (f) because \( H^1(K, R_{E/k}(\mathbb{G}_m)) = \{1\} \).

(f) \( \Rightarrow \) (a) is obvious from the definition of \( \text{ed}_k(T) \).

Example. Let \( T \) be a torus over \( k \) of rank \( < p - 1 \). Then \( \text{ed}_k(T;p) = 0 \). This follows from the fact that there is no non-trivial integral representation of dimension \( < p - 1 \) of any \( p \)-group, see for example [AP78, Satz]. Thus any finite quotient of \( \Gamma = \text{Gal}(k_{\text{alg}}/k) \) acts trivially on \( X(T) \) and so does \( \Gamma \).

Remark. The equivalence of parts (d) and (f) can also be deduced from [CTS77, Proposition 7.4].

Theorem 8.6. Let \( p \) be an odd prime, \( T \) an algebraic torus over \( k \), and \( \Gamma = \text{Gal}(k_{\text{alg}}/k(p)) \).

(a) \( \text{ed}(T;p) \leq 1 \) iff there exists a \( \Gamma \)-set \( \Lambda \) and an \( m \in \mathbb{Z}[\Lambda] \) fixed by \( \Gamma \) such that \( X(T)(p) \cong \mathbb{Z}(p)[\Lambda]/\langle m \rangle \) as \( \mathbb{Z}(p) \Gamma \)-lattices.

(b) \( \text{ed}(T;p) = 1 \) iff \( m = \sum a_{\lambda} \lambda \) from part (a) is not 0 and for any \( \lambda \in \Lambda \) fixed by \( \Gamma \), \( a_{\lambda} = 0 \) mod \( p \).

(c) If \( \text{ed}(T;p) = 1 \) then \( T_k(p) \cong T' \times S \) where \( \text{ed}_k(S;p) = 0 \) and \( X(T') \cong \text{an indecomposable } \mathbb{Z}(p) \Gamma \)-lattice, and \( \text{ed}_k(T';p) = 1 \).
Proof. (a) If \( \text{ed}(T; p) = 1 \), then by Corollary 8.1 there is a map of \( \mathbb{Z} \Gamma \)-lattices from \( \mathbb{Z}[\Lambda] \) to \( X(T) \) which becomes surjective after localization at \( p \) and whose kernel is generated by one element. Since the kernel is stable under \( \Gamma \), any element of \( \Gamma \) sends a generator \( m \) to either itself or its negative. Since \( p \) is odd, \( m \) must be fixed by \( \Gamma \).

The \( \text{ed}(T; p) = 0 \) case and the converse follows from Theorem 8.3 or Corollary 8.1.

(b) Assume we are in the situation of (a), and say \( \lambda_0 \in \Lambda \) is fixed by \( \Gamma \) and \( a_{\lambda_0} \) is not \( 0 \mod p \). Then \( X(T)(p) \cong \mathbb{Z}(p)[\Lambda - \{\lambda_0\}] \), so by Theorem 8.5 we have \( \text{ed}(T; p) = 0 \).

Conversely, assume \( \text{ed}(T; p) = 0 \). Then by Theorem 8.5, we have an exact sequence \( 0 \to \langle m \rangle \to \mathbb{Z}(p)[\Lambda] \to \mathbb{Z}(p)[\Lambda'] \to 0 \) for some \( \Gamma \)-set \( \Lambda' \) with one fewer element than \( \Lambda \). We have

\[
\text{Ext}^1_\Gamma(\mathbb{Z}(p)[\Lambda'], \mathbb{Z}(p)) = (0)
\]

by [CTS77, Key Lemma 2.1(i)] together with the Change of Rings Theorem [CR90, 8.16]; therefore this sequence splits. In other words, there exists a \( \mathbb{Z}(p) \Gamma \)-module homomorphism \( f: \mathbb{Z}(p)[\Lambda] \to \mathbb{Z}(p)[\Lambda] \) such that the image of \( f \) is \( \langle m \rangle \) and \( f(m) = m \). Then we can define \( c_\lambda \in \mathbb{Z}(p) \) by \( f(\lambda) = c_\lambda m \). Note that \( f(\gamma(\lambda)) = f(\lambda) \) and thus

\[
c_{\gamma(\lambda)} = c_\lambda \quad (8.10)
\]

for every \( \lambda \in \Lambda \) and \( \gamma \in \Gamma \). If \( m = \sum_{\lambda \in \Lambda} a_\lambda \lambda \), as in the statement of the theorem, then \( f(m) = m \) translates into

\[
\sum_{\lambda \in \Lambda} c_\lambda a_\lambda = 1.
\]

Since every \( \Gamma \)-orbit in \( \Lambda \) has a power of \( p \) elements, reducing modulo \( p \), we obtain

\[
\sum_{\lambda \in \Lambda^\Gamma} c_\lambda a_\lambda = 1 \pmod{p}.
\]

This shows that \( a_\lambda \neq 0 \mod p \), for some \( \lambda \in \Lambda^\Gamma \), as claimed.

(c) Decompose \( X(T)(p) \) uniquely into a direct sum of indecomposable \( \mathbb{Z}(p) \Gamma \)-lattices by the Krull-Schmidt theorem [CR90, Theorem 36.1]. Since \( \text{ed}(T; p) = 1 \), and the essential \( p \)-dimension of tori is additive (Theorem 5.3), all but one of these summands are permutation \( \mathbb{Z}(p) \Gamma \)-lattices. Now by [CR90, 31.12], we can lift this decomposition to \( X(T) \cong X(T') \oplus X(S) \), where \( \text{ed}(T'; p) = 1 \) and \( \text{ed}(S; p) = 0 \). \( \Box \)
Example. Let $E$ be an étale algebra over $k$. It can be written as $E = L_1 \times \cdots \times L_m$ with some separable field extensions $L_i/k$. The kernel of the norm $R_{E/k}(\mathbb{G}_m) \to \mathbb{G}_m$ is denoted by $R_{E/k}^{(1)}(\mathbb{G}_m)$. It is a torus with lattice

$$\bigoplus_{i=1}^m \mathbb{Z}[\Gamma/\Gamma_{L_i}] / \langle 1, \cdots, 1 \rangle,$$

where $\Gamma = \text{Gal}(k_{\text{sep}}/k)$ and $\Gamma_{L_i} = \text{Gal}(k_{\text{sep}}/L_i)$. Let $\Lambda$ be the disjoint union of the cosets $\Gamma/\Gamma_{L_i}$. Passing to a $p$-closure $k^{(p)}$ of $k$, $\Gamma_{k^{(p)}}$ fixes a $\lambda$ in $\Lambda$ iff $[L_i : k]$ is prime to $p$ for some $i$. We thus have

$$\text{ed}_k(R_{E/k}^{(1)}(\mathbb{G}_m); p) = \begin{cases} 1, & [L_i : k] \text{ is divisible by } p \text{ for all } i = 1,\ldots,m \\ 0, & [L_i : k] \text{ is prime to } p \text{ for some } i. \end{cases}$$

8.8 Tori Split by Cyclic Extensions of Degree Dividing $p^2$

In this section we assume $k = k^{(p)}$ is $p$-closed. Over $k = k^{(p)}$ every torus is split by a Galois extension of $p$-power order. We wish to compute the essential dimension of all tori split by a Galois extension with a (small) fixed Galois group $G$. The following theorem tells us for which $G$ this is feasible:

**Theorem 8.7** (A. Jones [Joh71]). For a $p$-group $G$ there are only finitely many genera of indecomposable $\mathbb{Z}G$-lattices if and only if $G$ is cyclic of order dividing $p^2$.

**Remark.** For $G = C_2 \times C_2$ a classification of the (infinitely many) different genera of $\mathbb{Z}G$-lattices has been worked out by [Naz61]. In contrast for $G = C_p \times C_p$ and $p$ odd (in the latter case) no classification is known.

We fix

$$G = C_{p^2} = \langle g | g^{p^2} = 1 \rangle.$$

We consider tori $T$ whose character lattice $X(T)$ is a $\mathbb{Z}G$-lattice or equivalently whose minimal splitting field is cyclic of degree dividing $p^2$.

Heller and Reiner [HR62], (see also [CR90, 34.32]) classified all indecomposable $\mathbb{Z}G$-lattices. Our goal consists in computing the essential dimension of $T$. By Corollary 8.4 we have $\text{ed}_k(T) = \text{ed}_k(T; p)$, hence by the additivity Theorem 5.3 it will be enough to find the essential $p$-dimension of the tori corresponding to
indecomposable \( \mathbb{Z}G \)-lattices. Recall that two lattices are in the same genus if their \( p \)-localization (or equivalently \( p \)-adic completion) are isomorphic. By Proposition 8.3 tori with character lattices in the same genus have the same essential \( p \)-dimension, which reduces the task to calculating the essential \( p \)-dimension of tori corresponding to the \( 4p + 1 \) cases in the list [CR90, 34.32].

Denote

\[ H = \langle \mathfrak{C} \rangle = \langle h | h^p = 1 \rangle. \]

We can consider \( \mathbb{Z}H \) as a \( G \)-lattice with the action \( g \cdot h^i = h^{i+1} \). Let

\[ \delta_G = 1 + g + \ldots + g^{p^2-1} \]
\[ \delta_H = 1 + h + \ldots + h^{p^2-1} \]

be the “diagonals” in \( \mathbb{Z}G \) and \( \mathbb{Z}H \) and

\[ \varepsilon = 1 + g^p + \ldots + g^{p^2-p}. \]

In table 8.1 representatives of all genera of indecomposable \( \mathbb{Z}G \)-lattices are listed (by \( \langle \ast \rangle \) we mean the \( \mathbb{Z}G \)-sublattice generated by \( \ast \)).

<table>
<thead>
<tr>
<th>( M_i )</th>
<th>( \mathbb{Z} )-lattices</th>
</tr>
</thead>
<tbody>
<tr>
<td>( M_1 )</td>
<td>( \mathbb{Z} )</td>
</tr>
<tr>
<td>( M_2 )</td>
<td>( \mathbb{Z}H )</td>
</tr>
<tr>
<td>( M_3 )</td>
<td>( \mathbb{Z}H / \langle \delta_H \rangle )</td>
</tr>
<tr>
<td>( M_4 )</td>
<td>( \mathbb{Z}G )</td>
</tr>
<tr>
<td>( M_5 )</td>
<td>( \mathbb{Z}G / \langle \delta_G \rangle )</td>
</tr>
<tr>
<td>( M_6 )</td>
<td>( \mathbb{Z}G \oplus \mathbb{Z} / \langle \delta_G - p \rangle )</td>
</tr>
<tr>
<td>( M_7 )</td>
<td>( \mathbb{Z}G / \langle \varepsilon \rangle )</td>
</tr>
<tr>
<td>( M_8 )</td>
<td>( \mathbb{Z}G / \langle \varepsilon - g\varepsilon \rangle )</td>
</tr>
<tr>
<td>( M_{9,r} )</td>
<td>( \mathbb{Z}G \oplus \mathbb{Z}H / \langle \varepsilon - (1-h)^r \rangle )</td>
</tr>
<tr>
<td>( M_{10,r} )</td>
<td>( \mathbb{Z}G \oplus \mathbb{Z}H / \langle \varepsilon(1-g) - (1-h)^{r+1} \rangle )</td>
</tr>
<tr>
<td>( M_{11,r} )</td>
<td>( \mathbb{Z}G \oplus \mathbb{Z}H / \langle \varepsilon - (1-h)^r, \delta_H \rangle )</td>
</tr>
<tr>
<td>( M_{12,r} )</td>
<td>( \mathbb{Z}G \oplus \mathbb{Z}H / \langle \varepsilon(1-g) - (1-h)^{r+1}, \delta_H \rangle )</td>
</tr>
</tbody>
</table>

In table 8.1 we describe \( \mathbb{Z}G \)-lattices as quotients of permutation lattices of minimal possible rank, whereas [CR90, 34.32] describes these lattices as certain extensions \( 1 \rightarrow L \rightarrow M \rightarrow N \rightarrow 1 \) of \( \mathbb{Z}[\zeta_{p^2}] \)-lattices by \( \mathbb{Z}H \)-lattices. Therefore these two lists look differently. Nevertheless they represent the same \( \mathbb{Z}G \)-lattices.
We show in the example of the lattice $M_{10,r}$ how one can translate from one list to the other.

Let $\mathbb{Z}x$ be a $\mathbb{Z}G$-module of rank 1 with trivial $G$-action. We have an isomorphism

$$M_{10,r} = \mathbb{Z}G \oplus \mathbb{Z}h / \langle \epsilon(1-g) - (1-h)^r \rangle \simeq \mathbb{Z}G \oplus \mathbb{Z}H \oplus \mathbb{Z}x / \langle \epsilon - (1-h)^r - x \rangle$$

induced by the inclusion $\mathbb{Z}G \oplus \mathbb{Z}H \hookrightarrow \mathbb{Z}G \oplus \mathbb{Z}H \oplus \mathbb{Z}x$.

This allows us to write $M_{10,r}$ as the pushout

$$\begin{array}{ccc}
\mathbb{Z}H & \xrightarrow{h \mapsto \epsilon} & \mathbb{Z}G \\
\downarrow & & \downarrow \\
\mathbb{Z}H \oplus \mathbb{Z}x & \longrightarrow & M_{10,r}
\end{array}$$

Completing both lines on the right we see that $M_{10,r}$ is an extension

$$0 \to \mathbb{Z}H \oplus \mathbb{Z}x \to M_{10,r} \to \mathbb{Z}G/\mathbb{Z}H \to 0$$

with extension class determined by the vertical map $h \mapsto (1-h)^r + x$ cf. [CR90, 8.12] and we identify (the $p$-adic completion of) $M_{10,r}$ with one of the indecomposable lattices in the list [CR90, 34.32].

Similarly, $M_1, \ldots, M_{12,r}$ are representatives of the genera of indecomposable $\mathbb{Z}G$-lattices.

**Theorem 8.8.** Every indecomposable torus $T$ over $k$ split by $G$ has character lattice isomorphic to one of the $\mathbb{Z}G$-lattices $M$ in table 8.1 after $p$-localization and $\text{ed}(T) = \text{ed}(T; p) = \text{ed}((\text{Diag}(M); p))$. Their essential dimensions are given in the tables `ta.editori`.

**Proof of Proposition 8.8.** We will assume $p > 2$ in the sequel. For $p = 2$ the Theorem is still true but some easy additional arguments are needed which we leave out here.

The essential $p$-dimension of tori corresponding to $M_1, \ldots, M_6$ easily follows from the discussion in section 8.7. Let $M$ be one of the lattices $M_7, \ldots, M_{12,r}$ and $T = \text{Diag} M$ the corresponding torus. We will determine the minimal rank of a permutation $\mathbb{Z}G$-lattice $P$ admitting a homomorphism $P \to M$ which becomes surjective after localization at $p$. Then we conclude $\text{ed}(T; p) = \text{rk } P - \text{rk } M$ with Corollary 8.1.
Table 8.2: Essential dimension of tori split by $\mathcal{C}_{p^2}$.

<table>
<thead>
<tr>
<th>$M$</th>
<th>$\text{rk} M$</th>
<th>$\text{ed}(T)$</th>
<th>$M$</th>
<th>$\text{rk} M$</th>
<th>$\text{ed}(T)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$M_1$</td>
<td>1</td>
<td>0</td>
<td>$M_7$</td>
<td>$p^2 - p$</td>
<td>$p$</td>
</tr>
<tr>
<td>$M_2$</td>
<td>$p$</td>
<td>0</td>
<td>$M_8$</td>
<td>$p^2 - p + 1$</td>
<td>$p - 1$</td>
</tr>
<tr>
<td>$M_3$</td>
<td>$p - 1$</td>
<td>1</td>
<td>$M_{9,r}$</td>
<td>$p^2$</td>
<td>$p$</td>
</tr>
<tr>
<td>$M_4$</td>
<td>$p^2$</td>
<td>0</td>
<td>$M_{10,r}$</td>
<td>$p^2 + 1$</td>
<td>$p - 1$</td>
</tr>
<tr>
<td>$M_5$</td>
<td>$p^2 - 1$</td>
<td>1</td>
<td>$M_{11,r}$</td>
<td>$p^2 - 1$</td>
<td>$p + 1$</td>
</tr>
<tr>
<td>$M_6$</td>
<td>$p^2$</td>
<td>1</td>
<td>$M_{12,r}$</td>
<td>$p^2$</td>
<td>$p$</td>
</tr>
</tbody>
</table>

We have the bounds

$$\text{rk} M \leq \text{rk} P \leq p^2 \ (\text{or } p^2 + p), \quad (8.11)$$

where the upper bound holds since every $M$ is given as a quotient of $\mathbb{Z}G$ (or $\mathbb{Z}G \oplus \mathbb{Z}H$). Let $C = \text{Split}_k(T[p])$ the finite constant group used in the proof of Theorem 8.2. The rank of $C$ determines exactly the number of direct summands into which $P$ decomposes. Moreover each indecomposable summand has rank a power of $p$.

As an example, we show how to find $C$ for $M = M_{11,r}$: The relations $g^i \cdot (\varepsilon - (1 - h)^r); \delta_h$ are written out as

$$\sum_{i=0}^{p-1} g^{pi+j} - \sum_{\ell=0}^{r} \binom{r}{\ell} (-1)^{j} h^{\ell+j}, \quad 0 \leq j \leq p - 1; \quad \sum_{i=0}^{p-1} h^{i}$$

and the $k_{\text{sep}}$-point of the torus are

$$T(k_{\text{sep}}) = \left\{ (t_0, \ldots, t_{p^2-1}, s_0, \ldots, s_{p-1}) \mid \prod_{i=0}^{p-1} t_{pi+j} = \prod_{\ell=0}^{r} s_{\ell+j}^{(-1)^{j}(-1)^{j}}, \quad 0 \leq j \leq p - 1; \quad \prod_{i=0}^{p-1} s_i = 1 \right\}$$

and $C$ is the constant group of fixed points of the $p$-torsion $T[p]$:

$$C(k) = \left\{ (\zeta_i, \ldots, \zeta_{ip}, \zeta_j, \ldots, \zeta_{jp}) \mid 0 \leq i, j \leq p - 1 \right\} \simeq \mu_p^s.$$  

(Note that the primitive $p$th root of unity $\zeta_p$ is in $k$ by our assumption that $k$ is $p$-closed). For other lattices this is similar: $C$ is equal to $\text{Split}_k(\text{Diag}(P)[p]) \simeq \mu_p^s$.  

Table 8.3: Permutation ranks for lattices $M_7$-$M_{12}$.

<table>
<thead>
<tr>
<th>$M$</th>
<th>rk $C$</th>
<th>rk $M$</th>
<th>possible rk $P$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$M_7$</td>
<td>1</td>
<td>$p^2 - p$</td>
<td>$p^2$</td>
</tr>
<tr>
<td>$M_8$</td>
<td>1</td>
<td>$p^2 - p + 1$</td>
<td>$p^2$</td>
</tr>
<tr>
<td>$M_{9,r}$</td>
<td>2</td>
<td>$p^2$</td>
<td>$p^2 + 1$ or $p^2 + p$</td>
</tr>
<tr>
<td>$M_{10,r}$</td>
<td>2</td>
<td>$p^2 + 1$</td>
<td>$p^2 + 1$ or $p^2 + p$</td>
</tr>
<tr>
<td>$M_{11,r}$</td>
<td>2</td>
<td>$p^2 - 1$</td>
<td>$p^2 + 1$ or $p^2 + p$</td>
</tr>
<tr>
<td>$M_{12,r}$</td>
<td>2</td>
<td>$p^2$</td>
<td>$p^2 + 1$ or $p^2 + p$</td>
</tr>
</tbody>
</table>

where $M$ is presented as a quotient $P/N$ of a permutation lattice $P$ (of minimal rank) as in table 8.3 and where $s$ denotes the number of summands in a decomposition of $P$. We need to exclude the possibility $\text{rk } P = p^2 + 1$ for the lattices $M = M_{9,r}, \ldots, M_{12,r}$. We can only have the value $p^2 + 1$ if there exists a character in $M$ which is fixed under the Galois group and nontrivial on $C$. The following Lemma 8.6 tells us, that such characters do not exist in either case. Hence the minimal dimension of a $p$-faithful representation of all these tori is $p^2 + p$.

**Lemma 8.6.** For $i = 9, \ldots, 12$ and $r \geq 1$ every character $\chi \in M_{i,r}$ fixed under $G$ has trivial restriction to $C$.

**Proof.** By [Hil85] the cohomology group $H^0(G, M_{i,r}) = M^G_{i,r}$ of $G$-fixed points in $M_{i,r}$ is trivial for $i = 11$, has rank 1 for $i = 9, 12$ and rank 2 for $i = 10$, respectively. They are represented by $\mathbb{Z}\delta_H$ in $M_{9,r}$, by $\mathbb{Z}(\varepsilon - (1 - h)^r)$ in $M_{12,r}$ and by $\mathbb{Z}(\varepsilon - (1 - h)^r) \oplus \mathbb{Z}\delta_H$ in $M_{10,r}$, respectively. Since all these characters are trivial on

$$C = \text{Split}_k(\text{Diag}(\mathbb{Z}G \oplus \mathbb{Z}H)[p]),$$

the claim follows.
Normalizers of Maximal Tori

The normalizer of a torus in a reductive group is a (FT)-group, thus we can apply some of the techniques from the previous chapters to obtain information on its essential dimension. Besides being of independent interest, normalizers $N$ of maximal tori in a group $G$ are a good source to obtain upper bounds on the essential dimension of $G$, in fact many of the best known upper bounds on the essential dimension of semisimple groups were obtained this way; cf. [Rei00], [LR00] or [Lem04]. Indeed, if $G$ is smooth and reductive, for any field $K/k$ the natural map

$$H^1(K, N) \to H^1(K, G)$$

is surjective, cf. [Ser97, III Lemma 6] or [CGR08, Cor. 5.3] for full generality. Via Propositions 4.1 and 4.2 we obtain

$$\text{ed}(N; p) \geq \text{ed}(G; p) \quad \text{ed}(N) \geq \text{ed}(G),$$

where $p$ is a prime different from the characteristic of $k$ and the second inequality follows from [BF03, 1.9].

The case where $G = \text{PGL}_n$ the projective linear group, is of particular interest to us. In that case, as a maximal split torus we have the diagonal in $\text{GL}_n$ mod out by the center $\Delta = \text{G}_m$ (of $\text{GL}_n$).

$$T = \text{G}_m^n / \Delta.$$

The normalizer

$$N = N_{\text{PGL}_n}(T) = T \rtimes \mathcal{S}_n$$

is the semidirect product of $T$ with the Weyl group $\mathcal{S}_n$ (the latter we can think of the subgroup of permutation matrices in $\text{GL}_n$). We can interpret the functor $H^1(\ast, N) = \text{Tors}_N$ in a different way. Define a functor $\text{Fields}/k \to \text{Sets}$ by

$$\mathfrak{N}(K) = \left\{ (A, E) \mid A \text{ a central simple of degree } n \text{ over } K, E \subset A \text{ a maximal étale subalgebra} \right\} / \simeq$$

(9.4)
One checks that the automorphism group of a pair \((A,E)\) is exactly \(N = T \rtimes \mathcal{S}_n\) and we have
\[
ed(N) = \ed(\mathcal{N}) = \ed(H^1(*,N)) = \ed(\mathfrak{T}_{\text{tors}}N).
\]

The functor \(\mathcal{N}\) is often more accessible than \(H^1(*,\text{PGL}_n) = \mathcal{C}\mathcal{S}_A\) because many of the standard constructions in the theory of central simple algebras depend on the choice of a maximal subfield \(L\) in a given central simple algebra \(A/K\). Projecting a pair \((A,L)\) to the first component, we obtain a surjective morphism of functors \(H^1(*,N) \to H^1(*,\text{PGL}_n)\), which gives another interpretation of (9.1).

In this section we compute the essential \(p\)-dimension of \(N\).

**Theorem 9.1.** Let \(N\) the normalizer of a maximal split torus in the projective linear group \(\text{PGL}_n\) defined over a field \(k\) with \(\text{char}(k) \neq p\). Then

(a) \(\ed(N; p) = [n/p]\), if \(n\) is not divisible by \(p\).

(b) \(\ed(N; p) = 2\), if \(n = p\).

(c) \(\ed(N; p) = n^2/p - n + 1\), if \(n = p^r\) for some \(r \geq 2\).

(d) \(\ed(N; p) = p^r(n - p^r) - n + 1\), in all other cases.

Here \([n/p]\) denotes the integer part of \(n/p\) and \(p^r\) denotes the highest power of \(p\) dividing \(n\).

We remark that our proof of the upper bounds on \(\ed(N; p)\) in part (c) and (d) does not use the assumption that \(\text{char}(k) \neq p\). These bounds are valid for every base field \(k\).

As explained above Theorem 9.1 yields an upper bound on the essential \(p\)-dimension of \(\text{PGL}_n\), in particular, since the computation of \(\ed(\text{PGL}_n; p)\) reduces to the case where \(n\) is a power of \(p\) (see Chapter 11),
\[
ed(\text{PGL}_{p^r}; p) \leq p^{2r-1} - p^r + 1
\]
for any field \(k\) and any \(r \geq 2\). In Chapter 11 this bound will be improved.

**Remark.** It would be of interest to prove an analogue of Theorem 9.1 in the more general setting, where \(N\) is the normalizer of a split maximal torus in an arbitrary simple (or semisimple) linear algebraic group \(G\). The new technical difficulty one encounters in this more general setting is that the natural sequence
\[
1 \to T \to N \to W \to 1,
\]
may not split. Here $T$ is a split maximal torus and $W = N/T$ is the Weyl group of $G$. The fact that this sequence splits for $G = \text{PGL}_n$ is an important ingredient in our proof of the upper bound on $\text{ed}(N; p)$.

9.1 First Reductions and Proof of Theorem 9.1

Parts (a) and (b)

Let $P_n$ be a Sylow $p$-subgroup of $S_n$. Theorem 5.2 tells us that $\text{ed}(N; p) = \text{ed}(T \rtimes P_n; p)$.

Note that $T \rtimes P_n$ is a $p$-(FT)-group so that we have upper and lower bounds on $\text{ed}(T \rtimes P_n; p)$ given by (8.6). In all cases (a)-(d) we will construct a generically free $T \rtimes P_n$-representation $V$ and prove that in fact

$$\text{ed}(T \rtimes P_n) = \text{ed}(T \rtimes P_n; p) = \dim V - \dim N,$$

so the upper bound in (8.6) is sharp and the statement of Conjecture 8.2 is satisfied for this group. In the general cases (c) and (d) we will show that the generically free representation we construct is minimal among all faithful representations, thus our lower bound follows from Theorem 8.2.

Note that $\dim N = \dim T \rtimes P_n = \dim N = n - 1$. Also, by Remark 4.1 we may assume without loss of generality that $k$ contains a primitive $p$th root of unity. We recall that the character lattice $X(T)$ is naturally isomorphic to

$$\{(a_1, \ldots, a_n) \in \mathbb{Z}^n \mid a_1 + \cdots + a_n = 0\},$$

where we identify the character

$$(t_1, \ldots, t_n) \rightarrow t_1^{a_1} \cdots t_n^{a_n}$$

of $T = \mathbb{G}_m^n / \Delta$ with $(a_1, \ldots, a_n) \in \mathbb{Z}^n$. Note that $(t_1, \ldots, t_n)$ is viewed as an element of $\mathbb{G}_m^n$ modulo the diagonal subgroup $\Delta$, so the above character is well defined if and only if $a_1 + \cdots + a_n = 0$. An element $\sigma$ of $S_n$ (and in particular, of $P_n \subset S_n$) acts on $a = (a_1, \ldots, a_n) \in X(T)$ by naturally permuting $a_1, \ldots, a_n$.

For notational convenience, we will denote by $a_{i,j}$ the element $(a_1, \ldots, a_n) \in X(T)$ such that $a_i = 1$, $a_j = -1$ and $a_h = 0$ for every $h \neq i, j$. 
We also recall that for $n = p^r$ the Sylow $p$-subgroup $\mathcal{P}_n$ of $\mathcal{I}_n$ can be described inductively as the wreath product

$$\mathcal{P}_{p^r} \cong \mathcal{P}_{p^{r-1}} \wr \mathbb{Z}/p \cong (\mathcal{P}_{p^{r-1}})^p \rtimes \mathbb{Z}/p.$$ 

For general $n$, $\mathcal{P}_n$ is the direct product of certain $\mathcal{P}_{p^r}$, see section 9.3.

**Proof of Theorem 9.1(a).** Since $n$ is not divisible by $p$, we may assume that $\mathcal{P}_n$ is contained in $\mathcal{I}_n - 1$, where we identify $\mathcal{I}_n - 1$ with the subgroup of $\mathcal{I}_n$ consisting of permutations $\sigma \in \mathcal{I}_n$ such that $\sigma(1) = 1$.

For the upper bound we construct a generically free linear representation $V$ of $T \rtimes \mathcal{P}_n$ of dimension $n - 1 + \lceil n/p \rceil$.

Let $\Lambda = \{a_i^i | i = 2, \ldots, n\}$ and $V_\Lambda$ be as in Corollary 3.4. We have $\dim V_\Lambda = |\Lambda| = n - 1$ and the representation is faithful on $T$ since $\Lambda$ generates $X(T)$. Let $W$ be a $[n/p]$-dimensional faithful linear representation of $\mathcal{P}_n$ constructed in the proof of Corollary 5.1 Applying Corollary 3.1, we see that $V = V_\Lambda \times W$ is generically free. This proves the upper bound.

For the lower bound, note that since the natural projection $p : T \rtimes \mathcal{P}_n \to \mathcal{P}_n$ has a section, so does the map $p^* : H^1(K, T \rtimes \mathcal{P}_n) \to H^1(K, \mathcal{P}_n)$ of Galois cohomology sets. Hence, $p^*$ is surjective for every field $K/k$. This implies that

$$\text{ed}(T \rtimes \mathcal{P}_n) \geq \text{ed}(\mathcal{P}_n; p) = \text{ed}(\mathcal{I}_n; p) = \lceil n/p \rceil.$$ 

by Theorem 5.2 and Corollary 5.1.

**Remark.** We will now outline a different and perhaps more conceptual proof of the upper bound $\text{ed}(\mathcal{N}; p) \leq \lceil n/p \rceil$ of Theorem 9.1(a). As we pointed out in (9.4), $\text{ed}(\mathcal{N}; p)$ is the essential dimension at $p$ of the functor $\mathcal{N}$ of pairs. Similarly, $\text{ed}(\mathcal{I}_n; p)$ is the essential dimension at $p$ of the functor $H^1(\mathcal{I}_n)$ which can be interpreted as the functor

$$\mathcal{E}_t_n(K) = \{\text{Étale } K\text{-algebras of degree } n\} / \simeq \quad (9.6)$$

Let $\alpha : \mathcal{E}_t_n \to \mathcal{N}$ be the map taking an $n$-dimensional étale algebra $L/K$ to $(\text{End}_K(L), L)$. Here we embed $L$ in $\text{End}_K(L) \simeq \mathcal{M}_n(K)$ via the regular action of $L$ on itself. It is easy to see that, over the $p$-closure $K^{(p)}$, $\alpha$ is surjective; indeed, any algebra $A$ of degree $n$ ($n$ not divisible by $p$) is split over $K^{(p)}$.

By Proposition 4.2, we conclude that $\text{ed}(\mathcal{N}; p) \leq \text{ed}(\mathcal{I}_n; p)$. Combining this with Corollary 5.1 yields the desired inequality $\text{ed}(\mathcal{N}; p) \leq \lceil n/p \rceil$. 

$\Box$
Proof of Theorem 9.1(b). Here \( n = p \) and \( \mathcal{P}_n \simeq \mathbb{Z}/p \) is generated by the \( p \)-cycle \((1, 2, \ldots, n)\). Let \( \Lambda = \{a_{1, 2}, \ldots, a_{p-1, p}, a_{p, 1}\} \) and \( V_\Lambda \) be as in Corollary 3.4. Let \( V = V_\Lambda \times L \), where \( L \) is a 1-dimensional faithful representation of \( \mathcal{P}_n \simeq \mathbb{Z}/p \) and \( T \rtimes \mathcal{P}_n \) acts on \( L \) via the natural projection \( T \rtimes \mathcal{P}_n \to \mathcal{P}_n \). Note that \( \dim(V) = |\Lambda| + 1 = n + 1 \). Since \( \Lambda \) generates \( X(T) \), Corollary 3.1 tells us that \( V \) is a generically free representation of \( T \rtimes \mathcal{P}_n \).

The lower bound follows from

\[
\text{ed}(T \rtimes \mathcal{P}_p) = \text{ed}(N; p) \geq \text{ed}(\text{PGL}_p; p) = 2;
\]

see [RY00]. \( \square \)

In order to prove Theorem 9.1(c) and (d) it suffices to establish the following proposition.

**Proposition 9.1.** Assume that \( k \) is of characteristic \( \neq p \) and \( n \neq p \) is divisible by \( p \). There is a generically free representation \( V \) of \( T \rtimes \mathcal{P}_n \) which is minimal among all faithful representations. Its dimension is

1. \( \dim V = n^2/p \), if \( n = p^r \) for some \( r \geq 2 \).
2. \( \dim V = p^e(n - p^e) \), if \( p^e \) is the highest power of \( p \) dividing \( n (n \neq p^e; e \geq 1) \).

This will be proved in the next two sections.

### 9.2 Proof of Theorem 9.1 Part (c)

Assume in this section that \( n = p^r \) for some \( r \geq 2 \).

**Construction of the representation**

For the upper bound we need to construct a generically free representation \( V \) of \( T \rtimes \mathcal{P}_n \) of dimension \( p^{2r-1} \). Our \( V \) will be of the form \( V_\Lambda \) for a particular \( \mathcal{P}_n \)-invariant \( \Lambda \subset X(T) \), again as in Corollary 3.4. This construction (and thus the above inequality) will not require any assumption on the base field \( k \).

For notational convenience, we will subdivide the integers \( 1, 2, \ldots, p^r \) into \( p \) “big blocks” \( B_1, \ldots, B_p \), where each \( B_i \) consists of the \( p^{r-1} \) consecutive integers \((i-1)p^{r-1} + 1, (i-1)p^{r-1} + 2, \ldots, ip^{r-1} \).
We define $\Lambda \subset X(T)$ as the $P_n$-orbit of the element

$$a_{1,p^r-1+1} = (1,0,\ldots,0,-1,0,\ldots,0,0,\ldots,0,0,\ldots,0,0,\ldots,0)$$

in $X(T)$. Thus, $\Lambda$ consists of elements $a_{\alpha,\beta}$, subject to the condition that if $\alpha$ lies in the big block $B_i$ then $\beta$ has to lie in $B_j$, where $j - i \equiv 1$ modulo $p$. There are $p^r$ choices for $\alpha$. Once $\alpha$ is chosen, there are exactly $p^r-1$ further choices for $\beta$. Thus

$$|\Lambda| = p^r \cdot p^{r-1} = p^{2r-1}.$$

The associated linear representation $V_{\Lambda}$ of $T \rtimes P_n$ has the desired dimension

$$\dim(V_{\Lambda}) = |\Lambda| = p^{2r-1}.$$

It remains to prove that $V_{\Lambda}$ is generically free. By Corollary 3.4 it suffices to show that

(i) $\Lambda$ generates $X(T)$ as an abelian group and

(ii) the $P_n$ action on the kernel of the natural morphism $\phi: \mathbb{Z}[\Lambda] \rightarrow X(T)$ is faithful.

The elements $a_{\alpha,\beta}$ clearly generate $X(T)$ as an abelian group, as $\alpha$ and $\beta$ range over $1,2,\ldots,p^r$. Thus in order to prove (i) it suffices to show that $\text{Span}_{\mathbb{Z}}(\Lambda)$ contains every element of this form. Suppose $\alpha$ lies in the big block $B_i$ and $\beta$ in $B_j$. If $j - i \equiv 1 \pmod{p}$, then $a_{\alpha,\beta}$ lies in $\Lambda$ and there is nothing to prove. If $j - i \equiv 2 \pmod{p}$ then choose some $\gamma \in B_{i+1}$ (where the subscript $i+1$ should be viewed modulo $p$) and write

$$a_{\alpha,\beta} = a_{\alpha,\gamma} + a_{\gamma,\beta}.$$

Since both terms on the right are in $\Lambda$, we see that in this case $a_{\alpha,\beta} \in \text{Span}_{\mathbb{Z}}(\Lambda)$. Using this argument recursively, we see that $a_{\alpha,\beta}$ also lies in $\text{Span}_{\mathbb{Z}}(\Lambda)$ if $j - i \equiv 3,\ldots,p \pmod{p}$, i.e., for all possible $i$ and $j$. This proves (i).

To prove (ii), denote the kernel of $\phi$ by $M$. Since $P_n$ is a finite $p$-group, every normal subgroup of $P_n$ intersects the center of $P_n$, which we shall denote by $Z_n$. Thus it suffices to show that $Z_n$ acts faithfully on $M$.

Recall that $Z_n$ is the cyclic subgroup of $P_n$ of order $p$ generated by the product of disjoint $p$-cycles

$$\sigma_1 \cdot \ldots \cdot \sigma_{p^r-1} = (1\ldots p)(p+1\ldots 2p)\ldots(p^r-p+1,\ldots,p^r).$$
Since \(|Z_n| = p\), it either acts faithfully on \(M\) or it acts trivially, so we only need to check that the \(Z_n\)-action on \(M\) is non-trivial. Indeed, \(Z_n\) does not fix the non-zero element
\[
\mathbf{a}_{1,p^{r-1}+1} + \mathbf{a}_{p^{r-1}+1,2p^{r-1}+1} + \cdots + \mathbf{a}_{(p-1)p^{r-1}+1,1} \in \mathbb{Z}[\Lambda]
\]
which lies in \(M\). This gives the existence of the generically free representation in Proposition 9.1(a).

**Minimality**

Let
\[
q := p^e, \text{ where } e \geq 1 \text{ if } p \text{ is odd and } e \geq 2 \text{ if } p = 2.
\]
be a power of \(p\). The specific choice of \(e\) will not be important in the sequel; in particular, the reader may assume that \(q = p\) if \(p\) is odd and \(q = 4\), if \(p = 2\). Whatever \(e\) we choose, \(q = p^e\) will remain unchanged for the rest of this section.

For the purpose of proving a lower bound we may assume that \(k\) contains a primitive \(q\)th root of unity, using the fact that if we adjoin such a root to the base field, the essential dimension can only go down, see 1.1.

Let \(T[q] = \mu_n^q / \mu_q\) be the \(q\)-torsion subgroup of \(T = G_m^n / \Delta\). Suppose \(W\) is a faithful \(G = T \rtimes \mathcal{P}_n\). Restricting to the finite constant group \(T[q] \rtimes \mathcal{P}_n\) we see that the dimension of a faithful \(G\)-representation is bounded from below by the minimal dimension of a faithful \(T[q] \rtimes \mathcal{P}_n\) (which, by Theorem 1.1 is equal to its essential \(p\)-dimension).

Thus it suffices to show that \(T[q] \rtimes \mathcal{P}_n\) does not have a faithful linear representation of dimension \(< p^{2r-1}\). Corollary 3.2 further reduces this representation-theoretic assertion to the combinatorial statement of Proposition 9.2 below.

Before stating Proposition 9.2 we recall that the character lattice of \(T[q] = \mu_n^q / \mu_q\) is
\[
X_n := \{(a_1, \ldots, a_n) \in (\mathbb{Z}/q\mathbb{Z})^n \mid a_1 + \cdots + a_n = 0 \text{ in } \mathbb{Z}/q\mathbb{Z}\},
\]
where we identify the character
\[
(t_1, \ldots, t_n) \mapsto t_1^{a_1} \cdots t_n^{a_n}
\]
of \(T[q]\) with \((a_1, \ldots, a_n) \in (\mathbb{Z}/q\mathbb{Z})^n\). Here \((t_1, \ldots, t_n)\) stands for an element of \(\mu_n^q\), modulo the diagonally embedded \(\mu_q\), so the above character is well defined if and only if \(a_1 + \cdots + a_n = 0\) in \(\mathbb{Z}/q\mathbb{Z}\). (This is completely analogous to our description of the character lattice of \(T\) in the previous section.) Note that \(X_n\) depends on the integer \(q = p^e\), which we assume to be fixed throughout this section.
Proposition 9.2. Let \( n = p^r \) and \( \mathcal{P}_n \) be a Sylow \( p \)-subgroup of \( \mathcal{I}_n \). If \( \Lambda \) is a \( \mathcal{P}_n \)-invariant generating subset of \( X_n \) then \( |\Lambda| \geq p^{2r-1} \) for any \( r \geq 1 \).

Our proof of Proposition 9.2 will rely on the following special case of Nakayama’s Lemma [AM69, Proposition 2.8].

Lemma 9.1. Let \( q = p^r \) be a prime power, \( M = (\mathbb{Z}/q\mathbb{Z})^d \) and \( \Lambda \) be a generating subset of \( M \) (as an abelian group). If we remove from \( \Lambda \) all elements that lie in \( pM \), the remaining set, \( \Lambda \setminus pM \), will still generate \( M \). \( \square \)

Proof of Proposition 9.2. We argue by induction on \( r \). For the base case, set \( r = 1 \). We need to show that \( |\Lambda| \geq p \). Assume the contrary. In this case \( \mathcal{P}_n \) is a cyclic \( p \)-group, and every non-trivial orbit of \( \mathcal{P}_n \) has exactly \( p \) elements. Hence, \( |\Lambda| < p \) is only possible if every element of \( \Lambda \) is fixed by \( \mathcal{P}_n \). Since we are assuming that \( \Lambda \) generates \( X_n \) as an abelian group, we conclude that \( \mathcal{P}_n \) acts trivially on \( X_n \). This can happen only if \( p = q = 2 \). Since these values are ruled out by our definition (9.7) of \( q \), we have proved the proposition for \( r = 1 \).

In the previous section we subdivided the integers \( 1, 2, \ldots, p^r \) into \( p \) “big blocks” \( B_1, \ldots, B_p \) of length \( p^{r-1} \). Now we will now work with “small blocks” \( b_1, \ldots, b_{p^{r-1}} \), where \( b_j \) consists of the \( p \) consecutive integers

\[
(j-1)p + 1, (j-1)p + 2, \ldots, jp.
\]

We can identify \( \mathcal{P}_{p^{r-1}} \) with the subgroup of \( \mathcal{P}_{p^r} \) that permutes the small blocks \( b_1, \ldots, b_{p^{r-1}} \) without changing the order of the elements in each block.

For the induction step, assume \( r \geq 2 \) and consider the homomorphism \( \Sigma: X_{p^r} \rightarrow X_{p^{r-1}} \) given by

\[
a = (a_1, a_2, \ldots, a_{p^r}) \mapsto s = (s_1, \ldots, s_{p^{r-1}}),
\]

where \( s_i = a_{(i-1)p+1} + a_{(i-1)p+2} + \ldots + a_{ip} \) is the sum of the entries of \( a \) in the \( i \)th small block \( b_i \). Thus

(i) if \( \Lambda \) generates \( X_{p^r} \) then \( \Sigma(\Lambda) \) generates \( X_{p^{r-1}} \).

(ii) if \( \Lambda \) is a \( \mathcal{P}_{p^{r-1}} \)-invariant subset of \( X_{p^r} \) then \( \Sigma(\Lambda) \) is a \( \mathcal{P}_{p^{r-1}} \)-invariant subset of \( X_{p^{r-1}} \).

Let us remove from \( \Sigma(\Lambda) \) all elements which lie in \( pX_{p^{r-1}} \). The resulting set, \( \Sigma(\Lambda) \setminus pX_{p^{r-1}} \), is clearly \( \mathcal{P}_{p^{r-1}} \)-invariant. By Lemma 9.1 this set generates \( X_{p^{r-1}} \). Thus by the induction assumption \( |\Sigma(\Lambda) \setminus pX_{p^{r-1}}| \geq p^{2r-3} \).

We claim that the fiber of each element \( s = (s_1, \ldots, s_{p^{r-1}}) \) in \( \Sigma(\Lambda) \setminus pX_{p^{r-1}} \) has at least \( p^2 \) elements in \( \Lambda \). If we can show this, then we will be able to conclude that

\[
|\Lambda| \geq p^2 \cdot |\Sigma(\Lambda) \setminus pX_{p^{r-1}}| \geq p^2 \cdot p^{2r-3} = p^{2r-1},
\]
thus completing the proof of Proposition 9.2.

Let \( \sigma_i \) be the single \( p \)-cycle, cyclically permuting the elements in the small block \( b_i \). To prove the claim, note that the subgroup

\[
\langle \sigma_i | i = 1, \ldots, p^{r-1} \rangle \simeq (\mathbb{Z}/p\mathbb{Z})^{p^{r-1}}
\]

of \( \mathcal{P}_n \) acts on each fiber of \( \Sigma \).

To simplify the exposition in the argument to follow, we introduce the following bit of terminology. Let us say that \( a \in (\mathbb{Z}/q\mathbb{Z})^n \) is scalar in the small block \( b_i \) if all the entries of \( a \) in the block \( b_i \) are the same, i.e., if

\[
a(i-1)p+1 = a(i-1)p+2 = \cdots = a_ip.
\]

We are now ready to prove the claim. Suppose \( a = (a_1, \ldots, a_{p^r}) \in X_{p^r} \) lies in the preimage of \( s = (s_1, \ldots, s_{p^r-1}) \), as in (9.8). If \( a \) is scalar in the small block \( b_i \) then clearly

\[
s_i = a(i-1)p+1 + a(i-1)p+2 + \cdots + a_ip \in p\mathbb{Z}/q\mathbb{Z}.
\]

Since we are assuming that \( s \) lies in

\[
\Sigma(\Lambda) \setminus pX_{p^r-1},
\]

\( s \) must have at least two entries that are not divisible by \( p \), say, \( s_i \) and \( s_j \). (Recall that \( s_1 + \cdots + s_{p^r} = 0 \) in \( \mathbb{Z}/q\mathbb{Z} \), so \( s \) cannot have exactly one entry not divisible by \( p \).) Thus \( a \) is non-scalar in the small blocks \( b_i \) and \( b_j \). Consequently, the elements \( \sigma_i^\alpha \sigma_j^\beta(a) \) are distinct, as \( \alpha \) and \( \beta \) range between 0 and \( p-1 \). All of these elements lie in the fiber of \( s \) under \( \Sigma \). Therefore we conclude that this fiber contains at least \( p^2 \) distinct elements. This completes the proof of the claim and thus of Proposition 9.2, Proposition 9.1(c) and Theorem 9.1 (c). \( \Box \)

### 9.3 Proof of Theorem 9.1 Part (d)

In this section we assume that \( n \) is divisible by \( p \) but is not a power of \( p \). We will modify the arguments of the last section. Throughout, let \( p^e \) be the highest power of \( p \) dividing \( n \). Write out the \( p \)-adic expansion

\[
n = n_1p^{e_1} + n_2p^{e_2} + \cdots + n_up^{e_u},
\]

of \( n \), where \( 1 \leq e = e_1 < e_2 < \cdots < e_u \), and \( 1 \leq n_i < p \) for each \( i \). Subdivide the integers \( 1, \ldots, n \) into \( n_1 + \cdots + n_u \) blocks \( B_j^i \) of length \( p^{e_i} \), for \( j \) ranging over
1, 2, ..., n. By our assumption there are at least two such blocks. The Sylow subgroup \( P_n \) is a direct product
\[
P_n = (P_{p^{e_1}})^{n_1} \times \cdots \times (P_{p^{e_u}})^{n_u}
\]
where each \( P_{p^{e_i}} \) acts on one of the blocks \( B_j \).

**Construction of the representation**

We construct a generically free representation of \( T \rtimes P_n \) of dimension \( p^{e_1}(n - p^{e_1}) \). Again this construction does not require any assumption on the field \( k \).

Let \( \Lambda \subset X(T) \) be the union of the \( P_n \)-orbits of the elements
\[
a_{1,j+1} \text{ where } j = p^{e_1}, \ldots, n_1p^{e_1}, n_1p^{e_1} + p^{e_2}, \ldots, n - p^{e_u}
\]
i.e., the union of the \( P_n \)-orbits of elements of the form \((1, 0 \ldots, 0, -1, 0, \ldots, 0)\), where 1 appears in the first position of the first block and \(-1\) appears in the first position of one of the other blocks. For \( a_{\alpha, \beta} \) in \( \Lambda \) there are \( p^{e_1} \) choices for \( \alpha \) and \( n - p^{e_1} \) choices for \( \beta \). Thus
\[
\dim(V_{\Lambda}) = |\Lambda| = p^{e_1}(n - p^{e_1}),
\]
where \( V_{\Lambda} \) is the associated representation in Corollary 3.4. It is not difficult to see that \( \Lambda \) generates \( X(T) \) as an abelian group. To conclude with Corollary 3.4 that \( V_{\Lambda} \) is a generically free representation of \( T \rtimes P_n \), it remains to show that the \( P_n \)-action on the kernel of the natural morphism \( \phi: \mathbb{Z}[\Lambda] \to X(T) \) is faithful when \( e_1 \geq 1 \). As in the previous section we only need to check that the center \( Z_n \) of \( P_n \) acts faithfully on the kernel. Let \( \sigma \) be a non trivial element of \( Z_n = (Z_{p^{e_1}})^{n_1} \times \cdots \times (Z_{p^{e_u}})^{n_u} \), with each \( Z_{p^{e_i}} \) cyclic of order \( p \). Let \( h, h' \) be in the first block \( B_1 \) and \( l, l' \) in some other block \( B_j \) (there are at least two blocks each of size at least \( p \)). The element
\[
a = a_{h,l} - a_{h,l'} + a_{h',l'} - a_{h',l}
\]
lies in the kernel of \( \phi \). To fix \( a \), \( \sigma \) must either (1) fix all \( h, h', l, l' \) or (2) \( \sigma(h) = h' \), \( \sigma(h') = h \) and \( \sigma(l) = l', \sigma(l') = l \). Since \( \sigma \) is nontrivial we may choose \( B_j \) such that (1) is not possible and if \( p \neq 2 \), (2) is not possible either. If \( p = 2 \), by (14), \( B_j \) is at least of size 4 and we can choose \( l, l' \) within \( B_j \) such that (2) does not hold. Therefore \( \sigma \) does not fix a nonzero element of the kernel of \( \phi \).
Minimality

Arguing as in Section 9.2 (and using the same notation, with \( q = p \)), it suffices to show that every faithful representation of \( T(p) \times P_n \) has dimension \( \geq p^{e_1}(n - p^{e_1}) \), or equivalently

**Lemma 9.2.** Let

\[
X_n := \{(a_1, \ldots, a_n) \in (\mathbb{Z}/p\mathbb{Z})^n \mid a_1 + \cdots + a_n = 0 \text{ in } \mathbb{Z}/p\mathbb{Z}\}.
\]

Then every \( P_n \)-invariant generating subset of \( X_n \) has at least \( p^{e_1}(n - p^{e_1}) \) elements.

In the statement of the lemma we allow \( e = 0 \), to facilitate the induction argument. For the purpose of proving minimality in Proposition 9.1(d) we only need this lemma for \( e \geq 1 \).

**Proof.** Once again, we consider the \( p \)-adic expansion (9.9) of \( n \), with \( 0 \leq e_1 < e_2 < \cdots < e_u \) and \( 1 \leq n_i < p \). We may assume that \( n \) is not a power of \( p \), since otherwise the lemma is vacuous.

We will argue by induction on \( e = e_1 \). For the base case, let \( e_1 = 0 \). Here the lemma is obvious: since \( X_n \) has rank \( n - 1 \), every generating set (\( P_n \)-invariant or not) has to have at least \( n - 1 \) elements.

For the induction step, we may suppose \( e = e_1 \geq 1 \); in particular, \( n \) is divisible by \( p \). Define \( \Sigma : X_n \to X_n/p \) by sending \((a_1, \ldots, a_n)\) to \((s_1, \ldots, s_{n/p})\), where

\[
s_j = a_{(j-1)p+1} + \cdots + a_{jp}
\]

for \( j = 1, \ldots, n/p \). Arguing as before we see that \( \Sigma(\Lambda) \setminus pX_{n/p} \) is a \((P_{p^{e_1-1}})^{n_1} \times \cdots \times (P_{p^{e_u-1}})^{n_u}\)-invariant generating subset of \( X_{n/p} \) and that every

\[
s \in \Sigma(\Lambda) \setminus pX_{n/p}
\]

has at least \( p^2 \) preimages in \( \Lambda \). By the induction assumption,

\[
|\Sigma(\Lambda) \setminus pX_{n/p}| \geq p^{e_1-1}\left(\frac{n}{p} - p^{e_1-1}\right)
\]

and thus

\[
|\Lambda| \geq p^2 \cdot p^{e_1-1}\left(\frac{n}{p} - p^{e_1-1}\right) = p^{e_1}(n - p^{e_1})
\]

This completes the proof of Lemma 9.2 and thus of Proposition 9.1 and of Theorem 9.1. \( \square \)
10

Central Simple Algebras

As noted there is an equivalence of the functors $H^1(\ast, \mathbf{PGL}_n)$ and $\mathcal{C\mathcal{S}\mathcal{A}}_n$. In this chapter we work on the side of central simple algebras. For background material on central simple algebras we refer to [Pie82], [Row80, 3] or [Sal99]. We introduce some new functors which describe classes of simple algebras with additional structure, such as crossed product algebras or algebras split by a distinguished Galois extension. These will help us obtain information on $\text{ed}(\mathcal{C\mathcal{S}\mathcal{A}}_n)$.

The main result of this chapter is the following theorem (and its variants Theorems 10.2, 10.4).

**Theorem 10.1.** Let $A/K$ be a central simple algebra of degree $n$. Suppose $A$ contains a field $F$, Galois over $K$ and $\text{Gal}(F/K)$ can be generated by $r \geq 1$ elements. If $[F : K] = n$ then we further assume that $r \geq 2$. Then

$$\text{ed}(A) \leq r \frac{n^2}{[F : K]} - n + 1.$$ 

Note that we always have $[F : K] \leq n$. In the special case where equality holds, i.e., $A$ is a crossed product in the usual sense, Theorem 10.1 reduces to [LRRS03, Corollary 3.10(a)].

Let us assume for the moment that the central simple algebra $A/K$ in Theorem 10.1 has a separable maximal subfield $L/K$, containing the Galois extension $F/K$.

We will denote the Galois closure of $L$ over $K$ by $E$ and the associated Galois groups by $G = \text{Gal}(E/K)$, $H = \text{Gal}(E/L)$ and $N = \text{Gal}(E/F)$, as in the diagram
In the terminology of [LRRS03], $A/K$ is a $G/H$-crossed product; cf. also [FSS94, Appendix]. Note that since $E/K$ is the smallest Galois extension containing $L/K$, we have

$$\text{Core}_G(H) = \bigcap_{g \in G} H^g = \{1\}. \quad (10.1)$$

where $H^g := gHg^{-1}$. We will assume that this condition is satisfied whenever we talk about $G/H$-crossed products.

In general no (strictly) maximal subfield $L$ needs to exist and it is more natural to allow étale algebras, in particular if the property of being a $G/H$-crossed product needs to be preserved under scalar extensions (as in Definition 10.2). However, for our proves we may always assume that $L$ and $E$ are fields as the Lemma 10.1 below shows.

**Lemma 10.1.** In the course of proving Theorem 10.1 we may assume without loss of generality that $F$ is contained in a subfield $L$ of $A$ such that $L/K$ is a separable extension of degree $n = \deg(A)$.

**Proof.** Note that we are free to replace $K$ by $K(t)$, $F$ by $F(t)$ and $A$ by $A(t) = A \otimes_K K(t)$, where $t$ is an independent variable. Indeed, $\text{ed}_K A(t) = \text{ed}_K(A)$; see, e.g., [LRRS03, Lemma 2.7(a)]. Thus if the inequality of Theorem 10.1 is proved for $A(t)$, it will also hold for $A$.

The advantage of passing from $A$ to $A(t)$ is that $K(t)$ if Hilbertian for any infinite field $K$; see, e.g., [FJ08, Proposition 13.2.1]. Thus after adjoining two variables, $t_1$ and $t_2$ as above, we may assume without loss of generality that $K$ is Hilbertian. (Note that a subfield $L \subset A$ of degree $n$ over $K$ may not exist without this assumption).
Let $F \subset F'$ be maximal among separable field extensions of $F$ contained in $A$. We will look for $L$ inside the centralizer $C_A(F')$. By the Double Centralizer Theorem, $C_A(F')$ is a central simple algebra with center $F'$. The maximality of $F'$ tells us that $C_A(F')$ contains no non-trivial field extensions of $F'$. In particular, $C_A(F') = M_r(F')$, where $r[F':K] = n$.

On the other hand, since $K$ is Hilbertian, so is its finite separable extension $F'$; cf. [FJ08, 12.2.3]. Consequently, $F'$ admits a finite separable extension $L/F'$ of degree $r$. To construct $L/F'$, start with the field extension $L = F'(t_1, \ldots, t_r)/F(t_1, \ldots, t_n)$ of degree $r$, where $f(x) = x^r + t_1 x^{r-1} + \ldots + t_{n-1} x + t_n$ is the general polynomial of degree $r$. Then specialize $t_1, \ldots, t_r$ in $F'$, using the Hilbertian property, to obtain a field extension $L/F'$ of degree $r$. Any such $L/F'$ can be embedded into $M_r(F')$ via the regular representation of $L$ on $L \cong M_n(L)$; cf. [Pie82, Lemma 13.1a]. By the maximality of $F'$, we conclude that $L = F'$, i.e., $r = 1$ and $[L : K] = n$, as desired.

Since $[G : H] = [L : K] = \deg(A) = n$, and $\frac{n}{[F : K]} = [L : F] = [N : H]$, we can restate Theorem 10.1 as follows.

**Theorem 10.2.** Let $A$ be a $G/H$-crossed product. Suppose $H$ is contained in a normal subgroup $N$ of $G$ and $G/N$ is generated by $r$ elements. Furthermore, assume that either $H \neq \{1\}$ or $r \geq 2$. Then


### 10.1 Crossed Products, Splitting Groups and Fields

Recall the following definitions, cf. [Pie82, 13.2], [TA85, 6.1]:

**Definition 10.1.** An étale algebra $E/K$ is said to **split** the algebra $A/K$, if $E = L_1 \times \cdots \times L_r$ for some fields $L_i/K$ and $A_{L_i} := A \otimes_K L_i \simeq M_n(L_i)$ is split for each $i = 1, \ldots, r$. Alternatively the Azumaya algebra $A \otimes_K E \simeq M_n(E)$ is split.

A finite group $G$ is called **splitting group** of $A/K$ if there exists a Galois étale algebra $E/K$ with Galois group $\text{Gal}(E/K) \subset G$ such that $E$ splits $A$.

In the diagram above, $L$ and $E$ are splitting fields (see [Pie82, 13.3]) and $G$ a splitting group. This gives rise to the following functors $\text{Fields}/k \to \text{Sets}$:

**Definition 10.2.** Let $K/k$ be a field. Define
(a) Suppose $E/k$ is an étale algebra.

$$\mathcal{\text{Split}}_{n,E/k}(K) = \{ \text{deg. } n \text{ central simple } K\text{-algebras, split by } E_K = E \otimes_k K \} / \simeq$$

(b) Let $G \subset S_n$ a finite group and $H \subset G$ of index $n$.

$$\mathcal{CP}_{G/H}(K) = \{ G/H\text{-crossed product algebras over } K \} / \simeq$$

(c) More generally, let $G$ be any finite group.

$$\mathcal{\text{Split}}_{n,G}(K) = \{ \text{Central simple } K\text{-algebras of degree } n, \text{ split by } G \} / \simeq$$

(d) $G$ as before.

$$\mathcal{\text{Pairs}}_{n,G}(K) = \left\{ (A,E) \mid \begin{array}{c} \text{A central simple of degree } n \text{ over } K \\ \text{E/K } G\text{-Galois algebra, splitting } A \end{array} \right\} / \simeq$$

Remark. Some similar functors are discussed in [Mer09]. If one starts say with a field extension $L/K$ which not necessarily descends to a field extension over $k$, it is sometimes useful to consider the functor $\mathcal{\text{Split}}_{n,L/K} : \text{Fields}/K \to \text{Sets}$ over the larger base field $K$.

In everything that follows we assume that $G \subset S_n, H \subset G$ of index $n$. Let $E/k$ be a $G$-Galois algebra, the functors are related as follows:

$$\mathcal{\text{Pairs}}_{n,G} \rightarrow \mathcal{\text{Split}}_{n,G} = \mathcal{CP}_{G/H} \rightarrow \mathcal{CSA}_n \tag{10.2}$$

Here the first map sends a pair $(A,E)$ to $A$ and the fact that $\mathcal{\text{Split}}_{n,G} = \mathcal{CP}_{G/H}$ is easily checked, using e.g. [Pie82, Cor. 13.3]. By [BF03, 1.9] and Proposition 4.2 we have

Lemma 10.2.

$$\text{ed}(\mathcal{\text{Pairs}}_{n,G}) \geq \text{ed}(\mathcal{\text{Split}}_{n,G}) = \text{ed}(\mathcal{CP}_{G/H})$$

The same inequality holds for essential $p$-dimension. \qed
If $F$ is a subfunctor of $G$ and $\alpha \in F(K) \subset G(K)$, then we can calculate the essential dimension of $\alpha$ with respect to both of these functors (which we will indicate by superscripts) and we have

$$\text{ed}^F(\alpha) \geq \text{ed}^G(\alpha), \quad \text{ed}^F(\alpha; p) \geq \text{ed}^G(\alpha; p). \quad (10.3)$$

Now we can do the following: If we start with an arbitrary central simple $K$-algebra $A \in CSA_n(K)$ of degree $n$, let $L$ be a maximal subfield (or étale algebra) and $E$ a Galois closure and suppose $G$ is the Galois group Gal$(E/K)$. Thus $A \in \text{Split}_{n,G}(K)$ and $(A, E) \in \text{Pairs}_{n,G}(K)$. By the lemma above and the definition of essential dimension we have

$$\text{ed}^{\text{CSA}}(A) \leq \text{ed}^{\text{Split}_{n,G}}(A) \leq \text{ed}(A, E) \leq \text{ed}(\text{Pairs}_{n,G}). \quad (10.4)$$

Let $T = G_m^n / \Delta$ be a maximal split torus in $\text{PGL}_n$, see also Chapter 9. Now $G \subset \mathcal{S}_n$ acts on $G_m^n$ by permuting the elements in the product and this action descends to $T$. We can thus form the semidirect product $T \rtimes G$ which is a subgroup of the normalizer $N = T \rtimes \mathcal{S}_n$ and thus of $\text{PGL}_n$.

**Lemma 10.3.** There is an equivalence of functors

$$\text{Pairs}_{n,G} = H^1(\ast, T \rtimes G).$$

**Proof.** Let $(M_n(K), \mathbb{Z}[G] \otimes K)$ be the split element in $\text{Pairs}_{n,G}(K)$. An automorphism of the pair must preserve $(\mathbb{Z}[G] \otimes K)^H = \mathbb{Z}[G/H] \otimes K$ which is of degree $n$ and we can think of a maximal commutative subalgebra of $M_n(K)$. Ones checks that the automorphism group of this pair is exactly $T \rtimes G$. We conclude with [KMRT98, 29.12]. \qed

**Corollary 10.1.** Assume $A \in CSA_n(K)$ is split by a $G$-Galois algebra $E/K$. Then $\text{ed}(A) \leq \text{ed}(T \rtimes G)$.

**Example.** Let $G = \mathcal{S}_n$ then $T \rtimes \mathcal{S}_n = N$ is the normalizer studied in the previous chapter. We have

$$\text{Pairs}_{n,\mathcal{S}_n} = H^1(\ast, N) = \mathfrak{N},$$

where $\mathfrak{N}$ was defined as the functor of pairs of an algebra with a distinguished maximal étale subalgebra.
Suppose we start again with an arbitrary central simple $K$-algebra $A \in CSA_n(K)$, $L$ is a maximal subfield (or étale algebra) and $E$ a Galois closure. If in addition $E/K$ is defined over $k$, i.e. there exists an étale algebra $E_0/k$ which becomes isomorphic to $E$ over $K$, then $A \in Split_{n,E_0/k}(K)$ and we have $ed_{CSA}(A) \leq ed_{Split_{n,E_0/k}}(A) \leq ed(Split_{n,E_0/k})$. The condition that $E/K$ is defined over $k$ is of course a strong restriction.

The functor $Split_{n,E/k}$ becomes most interesting by the following observation, due to Merkurjev [Mer09], which relates it to a certain torus (for which we have Theorem 8.3 to compute the essential dimension): For any étale algebra $E/k$ the Weil restriction $R_{E/k}(G_m)$ is a torus over $k$. Let $T$ be the torus $R_{E/K}(G_m)/G_m$ where $G_m$ embeds diagonally.

**Lemma 10.4** ([Mer09, (7)]). There is an equivalence of functors

$$\text{Split}_{n,E/k} = H^1(\ast, T).$$

\[ \square \]

### 10.2 $G$-Lattices

In the sequel $H \leq G$ will be finite groups. Given $g \in G$ we will write $\overline{g}$ for the left coset $gH$ of $H$. We will denote the identity element of $G$ by $1$.

Here again we will reduce the task to a lattice theoretic problem. This is achieved directly via the theorem below from [LRRS03].

Any finite set $X$ with a $G$-action gives rise to a permutation $G$-lattice $\mathbb{Z}[X]$. Of particular interest to us will be the $G$-lattice $\omega(G/H)$, which is defined as the kernel of the natural augmentation map $\mathbb{Z}[G/H] \to \mathbb{Z}$, sending $n_1\overline{g_1} + \cdots + n_s\overline{g_s}$ to $n_1 + \cdots + n_s$.

**Theorem 10.3.** [LRRS03, Theorem 3.5] Let $P$ be a permutation $G$-lattice and

$$0 \to M \to P \to \omega(G/H) \to 0$$

be an exact sequence of $G$-lattices. If the $G$-action on $M$ is faithful then

$$ed(A) \leq rk(P) - n + 1$$

for any $G/H$-crossed product $A$. 
The theorem is easy to deduce from the preparations made earlier here and we include a short proof.

**Proof.** Let \( A \in \mathcal{C}P_{G/H}(K) \) be a \( G/H \)-crossed product of degree \( n \) over \( K \) and \( E \) a \( G \)-Galois algebra which is the Galois closure of a maximal étale subalgebra of \( A \). By Corollary 10.1 and Corollary 3.3,

\[
ed(A) \leq \text{ed}(\text{Pairs}_{n,G}) = \text{ed}(T \rtimes G) \leq \text{rk} \ M = \text{rk} \ P - n + 1.
\]

The condition that \( G \) acts faithfully on \( M \) is not automatic. However, the following lemma shows that it is satisfied for many natural choices of \( P \).

**Lemma 10.5.** Let \( G \neq \{1\} \) be a finite group \( H \leq G \) be a subgroup of \( G \), \( H_1, \ldots, H_r \) be subgroups of \( H \) and

\[
0 \to M \to \bigoplus_{i=1}^r \mathbb{Z}[G/H_i] \to \omega(G/H) \to 0 \tag{10.5}
\]

be an exact sequence of \( G \)-lattices. Assume that \( H \) does not contain any nontrivial normal subgroup of \( G \) (i.e., \( H \) satisfies condition (10.1) above). Then the \( G \)-action on \( M \) fails to be faithful if and only if \( s = 1 \) and \( H_1 = H \).

Here we are not specifying the map \( \bigoplus_{i=1}^r \mathbb{Z}[G/H_i] \to \omega(G/H) \); the lemma holds for any exact sequence of the form (10.5). We also note that in the case where \( H_1 = \cdots = H_r = \{1\} \), Lemma 10.5 reduces to [LRRS03, Lemma 2.1].

**Proof.** To determine whether or not the \( G \)-action on \( M \) is faithful, we may replace \( M \) by \( M_{\mathbb{Q}} := M \otimes \mathbb{Q} \). After tensoring with \( \mathbb{Q} \), the sequence (10.5) splits, and we have an isomorphism

\[
\omega(G/H)_{\mathbb{Q}} \oplus M_{\mathbb{Q}} \simeq \bigoplus_{i=1}^r \mathbb{Q}[G/H_i]. \tag{10.6}
\]

Case 1: \( r \geq 2 \). Then \( H_r \) is a subgroup of \( H \), we have a natural surjective map \( \mathbb{Q}[G/H_r] \to \mathbb{Q}[G/H] \). Using complete irreducibility over \( \mathbb{Q} \) once again, we see that \( \mathbb{Q}[G/H] \) (and hence \( \omega(G/H) \)) is a subrepresentation of \( \mathbb{Q}[G/H_r] \). Thus (10.6) tells us that \( \mathbb{Q}[G/H_{r-1}] \) is a subrepresentation of \( M_{\mathbb{Q}} \). The kernel of the \( G \)-representation on \( \mathbb{Q}[G/H_{r-1}] \) is a normal subgroup of \( G \) contained in \( H_{r-1} \) (and hence, in \( H \)); by our assumption on \( H \), any such subgroup is trivial. This shows that \( G \) acts faithfully on \( \mathbb{Q}[G/H_{r-1}] \) and hence, on \( M \).
Case 2: Now assume \( r = 1 \). Our exact sequence now assumes the form
\[
0 \to M \to \mathbb{Q}[G/H_1] \to \omega(G/H)_\mathbb{Q} \to 0.
\]
If \( H = H_1 \) then \( M \simeq \mathbb{Z} \), with trivial (and hence, non-faithful) \( G \)-action.

Our goal is thus to show that if \( H_1 \subsetneq H \) then the \( G \)-action on \( M \mathbb{Q} \) is faithful. Denote by \( \mathbb{Q}[1] \) the trivial representation (it will be clear from the context of which group). Observe that
\[
\mathbb{Q}[G/H_1] \simeq \text{Ind}_{H_1}^G \mathbb{Q}[1] \simeq \text{Ind}_{H_1}^G \text{Ind}_{H}^H \mathbb{Q}[1] \simeq \text{Ind}_{H}^G \mathbb{Q}[H/H_1],
\]
and we obtain
\[
M \mathbb{Q} \simeq \text{Ind}_{H_1}^G \omega(H/H_1)_\mathbb{Q} \oplus \mathbb{Q}[1].
\]
If \( H_1 \subsetneq H \) then the kernel of the \( G \)-representation \( \text{Ind}_{H_1}^G \omega(H/H_1)_\mathbb{Q} \) is a normal subgroup of \( G \) contained in \( H_1 \) (and hence, in \( H \)). By our assumption on \( H \), this kernel is trivial.

\[10.3 \quad \text{An Upper Bound}\]

In this section we will prove the following upper bound on the essential dimension of a \( G/H \)-crossed product.

We will say that \( g_1, \ldots, g_s \in G \) generate \( G \) over \( H \) if \( G = \langle g_1, \ldots, g_s, H \rangle \).

**Theorem 10.4.** Let \( A \) be a \( G/H \)-crossed product. Suppose that

(i) \( g_1, \ldots, g_s \in G \) generate \( G \) over \( H \), and

(ii) if \( G \) is cyclic then \( H \neq \{1\} \).

Then \( \text{ed}(A) \leq \sum_{i=1}^s [G : (H \cap H^{g_i})] - [G : H] + 1 \).

**Remark.** The index \([G : (H \cap H^{g_i})]\) appearing in the above formula can be rewritten as
\[
[G : H] \cdot [H : (H \cap H^{g_i})] = [G : H] \cdot [(H \cdot H^{g_i}) : H];
\]
see, e.g., [Hup67, I 2.12]. Note \( H \cdot H^g := \{hh' \mid h \in H, h' \in H^g\} \) is a subset of \( G \) but may not be a subgroup, and \([(H \cdot H^g) : H]\) is defined as \( \frac{|H \cdot H^g|}{|H|} \).
If $H$ is contained in a normal subgroup $N$ of $G$ then clearly $H \cdot H^{g} \leq [N : H]$ and thus Theorem 10.4 yields


This is a bit weaker than the inequality of Theorem 10.2, even though the two look very similar. The difference is that we have replaced $r$ in the inequality of Theorem 10.2 by $s$, where $G$ is generated by $s$ elements over $H$ and by $r$ elements over $N$. A priori $r$ can be smaller than $s$. Nevertheless in the next section we will deduce Theorem 10.2 from Theorem 10.4 by a more delicate argument along these lines.

Our proof of Theorem 10.4 will rely on the following lemma.

**Lemma 10.6.** Let $V$ be a $\mathbb{Z}[G]$-submodule of $\omega(G/H)$. Then

$$G_{V} := \{ g \in G | \overline{g - T} \in V \}$$

is a subgroup of $G$ containing $H$.

**Proof.** The inclusion $H \subset G_{V}$ is obvious from the definition.

To see that $G_{V}$ is closed under multiplication, suppose $g, g' \in G_{V}$. That is, both $\overline{g - T}$ and $\overline{g' - T}$ lie in $V$. Then

$$\overline{gg' - T} = g \cdot (\overline{g' - T}) + (\overline{g - T})$$

also lies in $V$, i.e., $gg' \in G_{V}$, as desired. \qed

**Proof of Theorem 10.4.** We claim that the elements $\overline{g_{1} - T}, \ldots, \overline{g_{s} - T}$ generate $\omega(G/H)$ as a $\mathbb{Z}[G]$-module.

Indeed, let $V$ be the $\mathbb{Z}[G]$-submodule of $\omega(G/H)$ generated by these elements. Lemma 10.6 and condition (i) tell us that $V$ contains $\overline{g - T}$ for every $g \in G$. Translating these elements by $G$, we see that $V$ contains $\overline{a - b}$ for every $a, b \in G$. Hence, $V = \omega(G/H)$, as claimed.

For $i = 1, \ldots, s$, let

$$S_{i} := \{ g \in G | g \cdot (\overline{g_{i} - T}) = \overline{g_{i} - T} \}$$

be the stabilizer of $\overline{g_{i} - T}$ in $G$. We may assume here that $g_{i}$ is not in $H$, otherwise it could be removed since it is not needed to generate $G$ over $H$. Then clearly
$g \in S_i$ if $gg_i = g_i$ and $g = \overline{1}$. From this one easily sees that $S_i = H \cap H^{g_i}$. Thus we have an exact sequence

$$0 \rightarrow M \rightarrow \bigoplus_{i=1}^{s} \mathbb{Z}[G/S_i] \xrightarrow{\phi} \omega(G/H) \rightarrow 0$$

where $\phi$ sends a generator of $\mathbb{Z}[G/S_i]$ to $g_i - 1 \in \omega(G/H)$. By Theorem 10.3 it remains to show that $G$ acts faithfully on $M$.

By Lemma 10.5 $G$ fails to act faithfully on $M$ if and only if $s = 1$ and $S_1 = H = H^{g_1}$. But this possibility is ruled out by (ii). Indeed, assume that $s = 1$ and $S_1 = H = H^{g_1}$. Then $G = \langle g_1, H \rangle$ and $H = H^{g_1}$. Hence, $H$ is normal in $G$. Condition (10.1) then tells us that $H = \{1\}$. Moreover, in this case $G = \langle g_1, H \rangle = \langle g_1 \rangle$ is cyclic, contradicting (ii).

10.4 Proofs of Theorems 10.1 and 10.2

We will prove Theorem 10.2 which is equivalent to Theorem 10.1.

Let $t_1, \ldots, t_r \in G/N$ be a set of generators for $G/N$. Choose $g_1, \ldots, g_r \in G$ representing $t_1, \ldots, t_r$, and let $H' := \langle H, H^{g_1}, \ldots, H^{g_r} \rangle$. Since $H \leq N$ and $N$ is normal in $G$, $H' \leq N$. The group $H'$ depends on the choice of $g_1, \ldots, g_r \in G$, so that $g_iN = t_i$. Fix $t_1, \ldots, t_r$ and choose $g_1, \ldots, g_r \in G$ representing them, so that $H'$ has the largest possible order or equivalently the smallest possible index in $N$. Denote this minimal possible value of $[N : H']$ by $m$. In particular

$$m = [N : H'] \leq [N : (H^{g_i} \cdot H)] \quad (10.7)$$

for any $i = 1, \ldots, r$ and any $g \in N$. Here $[N : (H^{g_i} \cdot H)] = \frac{|N|}{|H^{g_i} \cdot H|}$, as in Remark 10.3.

Choose a set of representatives $1 = n_1, n_2, \ldots, n_m \in N$ for the distinct left cosets of $H'$ in $N$. We claim that the elements

$$\{g_in_j \mid i = 1, \ldots, r; j = 1, \ldots, m\}$$

generate $G$ over $H$.

Indeed, let $G_0$ be the subgroup of $G$ generated by these elements and $H$. Since $n_1 = 1$, $G_0$ contains $g_1, \ldots, g_r$. Hence, $G_0$ contains $H'$. Moreover, $G_0$ contains $n_j = g_1^{-1}(g_{1}n_j)$ for every $j$; hence, $G_0$ contains all of $N$. Finally, since $t_1 = g_1N, \ldots, t_r = g_rN$ generate $G/N$, we conclude that $G_0$ contains all of $G$. This proves the claim.
We now apply Theorem 10.4 to the elements \( \{g_inj\} \). Substituting \([G : H] \cdot [H : (H \cdot H^{g_inj})] \) for \([G : (H \cap H^{g_inj})] \), as in Remark 10.3, we obtain

\[
ed(A) \leq \sum_{i=1}^{r} \sum_{j=1}^{m} [G : (H \cap H^{g_inj})] - [G : H] + 1
\]

\[
= [G : H] \cdot \sum_{i=1}^{r} \sum_{j=1}^{m} [(H \cdot H^{g_inj}) : H] - [G : H] + 1
\]

\[
= [G : H] \cdot \sum_{i=1}^{r} \sum_{j=1}^{m} \frac{[N : H]}{[N : (H \cdot H^{g_inj})]} - [G : H] + 1
\]

\[
\leq \text{(by (10.7))} \quad [G : H] \cdot \sum_{i=1}^{r} \sum_{j=1}^{m} \frac{[N : H]}{m} - [G : H] + 1
\]

\[
\]

as desired. This completes the proof of Theorem 10.2 and thus of Theorem 10.1. \( \square \)
The Projective Linear Group $\text{PGL}_n$

Recall that the essential dimension of the projective linear group $\text{PGL}_n$ is given as

$$\text{ed}(\text{PGL}_n) = \text{ed}(H^1(\ast, \text{PGL}_n)) = \text{ed}(\mathcal{T}_{\text{PGL}_n}) = \text{ed}(\mathcal{C}\mathcal{S}\mathcal{A}_n)$$

where $\mathcal{T}_{\text{PGL}_n}$ denotes the functor of $\text{PGL}_n$-torsors and $\mathcal{C}\mathcal{S}\mathcal{A}_n$ the functor of central simple algebras of degree $n$, cf. Section 1.1 and Chapter 10. By definition we also have

$$\text{ed}(\text{PGL}_n) = \text{ed}(\mathcal{C}\mathcal{S}\mathcal{A}_n) = \max_{\deg A = n} \text{ed}(A),$$

the maximum essential dimension that a degree $n$ central simple algebra (over any field $K/k$) can have.

The problem of computing $\text{ed}(\text{PGL}_n)$ was first raised by C. Procesi in the 1960s. Procesi and S. Amitsur constructed so-called universal division algebras $\text{UD}(n)$ which have various generic properties among central simple algebras of degree $n$ (see [Pie82, 20.8] or [Row80, 3.2] for the definition of $\text{UD}(n)$). In particular, $\text{UD}(n)$ has the rational specialization property: Let $Z \supset k$ be the center of $\text{UD}(n)$ and $A$ any simple $K$ algebra of degree $n$ with $K \supset k$. Then there exists a field $R$, both containing $Z$ and $K$ such that $R$ is rational (i.e. purely transcendental) over $K$ and

$$\text{UD}(n) \otimes_Z R \simeq A \otimes_K R.$$ 

It follows from this that $\text{ed}(\text{UD}(n)) \geq \text{ed}(A)$, see [LRRS03, 2.4]. Since $A$ is arbitrary, $\text{UD}(n)$ is an instance of an algebra with maximal essential dimension,

$$\text{ed}(\text{PGL}_n) = \text{ed}(\text{UD}(n)).$$

(Alternatively, one shows that the $\text{PGL}_n$-torsor corresponding to $\text{UD}(n)$ is versal). Procesi also showed that the center $Z$ of $\text{UD}(n)$ has transcendence degree $\text{trdeg}_k Z = n^2 + 1$, thus giving the upper bound

$$\text{ed}(\text{PGL}_n) = \text{ed}(\text{UD}(n)) \leq n^2 + 1.$$ 

In fact Procesi himself improved this bound and showed (using different terminology) that $\text{ed}(\text{PGL}_n) \leq n^2$, [Pro67, 2.1]. The problem of computing $\text{ed}(\text{PGL}_n)$
was raised again by B. Kahn in the early 1990s who asked (implicitly in [Kah00, Section 2]) if $\text{ed}(\text{PGL}_n)$ grows sublinearly in $n$, i.e., whether

$$\text{ed}(\text{PGL}_n) \leq an + b$$

for some positive real numbers $a$ and $b$.

There has been much work to improve the bounds on $\text{ed}(\text{PGL}_n)$ but still very little is known about the exact values of $\text{ed}(\text{PGL}_n)$ (assume $\text{char } k \neq n$):

Table 11.1: Essential dimension of $\text{PGL}_n$.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$\text{ed}(\text{PGL}_n)$</th>
<th>reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2, 3, 6$</td>
<td>$2$</td>
<td>[Rei00, 9.4]</td>
</tr>
<tr>
<td>$4$</td>
<td>$5$</td>
<td>[Ros08, 12.4], [Mer10, 1.2]</td>
</tr>
</tbody>
</table>

The best known upper bound,

$$\text{ed}(\text{PGL}_n) \leq \begin{cases} 
\frac{(n-1)(n-2)}{2}, & \text{for every odd } n \geq 5 \\
 n^2 - 3n + 1, & \text{for every } n \geq 4 
\end{cases}$$

(see [LR00], [LRRS03, Theorem 1.1], [Lem04, Proposition 1.6] and [FF08]), is quadratic in $n$. Recently Merkurjev [Mer09] made a substantial improvement on the lower bound for $n = p^r$ a power of a prime:

**Theorem 11.1.**

$$\text{ed}(\text{PGL}_{p^r}) \geq \text{ed}(\text{PGL}_{p^r}; p) \geq (r - 1)p^r + 1.$$  

The proof of this result relies on our Theorem 8.3.

Essential $p$-dimension of $\text{PGL}_n$ is a bit more accessible. One first notes that if $p^r$ is the largest power of $p$ dividing $n$ then, using primary decomposition of central simple algebras, $\text{ed}(\text{PGL}_n; p) = \text{ed}(\text{PGL}_{p^r}; p)$, cf. [RY00, 8.5]. Thus for the purpose of computing $\text{ed}(\text{PGL}_n; p)$ it suffices to consider the case where $n = p^r$. Table 11.2 lists the powers of $p$ for which $\text{ed}(\text{PGL}_{p^r}; p)$ is known (in all cases $\text{char } k \neq p$).

For higher powers, a first new upper bound on $\text{ed}(\text{PGL}_{p^r}; p)$ follows from the computations on the essential dimension of the normalizer of a maximal torus,
Table 11.2: Essential \( p \)-dimension of \( \text{PGL}_n \).

<table>
<thead>
<tr>
<th>( n )</th>
<th>( \text{ed}(\text{PGL}_n; p) )</th>
<th>reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>( p )</td>
<td>2</td>
<td>[RY00, 8.5]</td>
</tr>
<tr>
<td>( p^2 )</td>
<td>( p^2 + 1 )</td>
<td>[Mer10, 1.2], [MR09a, remark; Cor. 1.2]</td>
</tr>
</tbody>
</table>

see (9.5). With a more careful analysis and the results in Chapter 10 we will now establish the following new upper bound \(^1\):

**Theorem 11.2.** Let \( n = p^r \) for some \( r \geq 2 \). Then

\[
\text{ed}(\text{PGL}_n; p) \leq \frac{2n^2}{p^2} - n + 1.
\]

**Proof.** We will deduce Theorem 11.2 from Theorem 10.1. Let \( n = p^r \) and \( A = \text{UD}(n) \). In [RS92, 1.2], L. H. Rowen and D. J. Saltman showed that if \( r \geq 2 \) then there is a finite field extension \( K'/K \) of degree prime to \( p \), such that \( A' := A \otimes_K K' \) contains a field \( F \), Galois over \( K' \) with \( \text{Gal}(F/K') \simeq \mathbb{Z}/p \times \mathbb{Z}/p \). Thus, if \( r \geq 2 \), Theorem 10.1 tells us that

\[
\text{ed}(\text{PGL}_n; p) = \text{ed}(A; p) \leq \text{ed}(A') \leq \frac{2n^2}{p^2} - n + 1.
\]

---

\(^1\)We just learnt that Ruozzi [Ru10] showed that after a prime to \( p \) extension, \( \text{UD}(n) \) has a \( \mathcal{S}_p \times \mathcal{S}_{p-1} \) splitting group. Using our methods he sharpened the bound to \( \text{ed}(\text{PGL}_n; p) \leq \frac{n^2}{p^2} + 1. \)
This follows basically from the rational specialization property. In combination with Lemma 10.2 we obtain

**Corollary 11.1.** Suppose $G$ is a splitting group of $\text{UD}(n)$. Then $\mathcal{SA}_n = \text{Split}_{n,G}$. Thus

$$\text{ed}(\text{PGL}_n) = \text{ed}(\mathcal{SA}_n) = \text{ed}(\text{Split}_{n,G}) \leq \text{ed}(T \rtimes G)$$

*The same holds for essential p-dimension.*

In fact one can show that if $G$ is a splitting group of $\text{UD}(n)$ then the map $H^1(K, T \rtimes G) \to H^1(K, \text{PGL}_n)$ is surjective for any field $K/k$.

We end with the following question:

*Does there exist a splitting group $G$ of $\text{UD}(n)$ such that $\text{ed}(\text{PGL}_n) = \text{ed}(T \rtimes G)$?*

The splitting groups of $\text{UD}(n)$ were studied in [TA85], but they appear to be somewhat mysterious. The symmetric group $\mathcal{S}_n$ for example splits $\text{UD}(n)$ (see [LRRS03, 4]) but the bound obtained in the above corollary with $G = \mathcal{S}_n$ is not sharp at least for essential $p$-dimension. The advantage of the group $T \rtimes G$ over $\text{PGL}_n$, for the computation of essential dimension, is that it is an $(\text{FT})$-group and the representation and lattice theoretic methods explained here can be used.
Bibliography


URL http://arxiv.org/abs/math/0701903


URL http://dx.doi.org/10.1006/jabr.2000.8380


[Mil06] James S. Milne, *Algebraic groups and arithmetic groups*, 2006, Online course notes
URL http://www.jmilne.org/math/

URL http://www.math.uni-bielefeld.de/LAG/man/309.html

URL http://pjm.math.berkeley.edu/ant/2009/3-4/p06.xhtml

URL http://dx.doi.org/10.1016/j.jalgebra.2009.09.019


URL http://www.math.ubc.ca/~reichst/pub.html


URL http://www.math.uni-bielefeld.de/~rost/ed.html

[Ros08] Markus Rost, Computation of some essential dimensions, 1–19, Preprint.
URL http://www.math.uni-bielefeld.de/~rost/ed.html


URL http://www.math.uni-bielefeld.de/LAG/man/385.html


URL http://www.math.uni-bielefeld.de/LAG/man/377.html


