Title
Essential Dimension of Finite Groups

Author
Wong, Wanshun

Publication Date
2012

Peer reviewed|Thesis/dissertation

University of California
Los Angeles

Essential Dimension of Finite Groups

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

by

Wanshun Wong

2012

Abstract of the Dissertation

Essential Dimension of Finite Groups

by

Wanshun Wong

Doctor of Philosophy in Mathematics

University of California, Los Angeles, 2012

Professor Alexander Merkurjev, Chair

In this thesis we study the essential dimension of the first Galois cohomology functors of finite groups. Following the result by N. A. Karpenko and A. S. Merkurjev about the essential dimension of finite p-groups over a field containing a primitive p-th root of unity, we compute the essential dimension of finite cyclic groups and finite abelian groups over a field containing all primitive p-th roots of unity for all prime divisors p of the order of the group. For the computation of the upper bound of the essential dimension we apply the techniques about affine group schemes, and for the lower bound we make use of the tools of canonical dimension and fibered categories. We also compute the essential dimension of small groups over the field of rational numbers to illustrate the behavior of essential dimension when the base field does not contain all relevant primitive roots of unity.

The dissertation of Wanshun Wong is approved.

Amit Sahai

Richard Elman

Paul Balmer

Alexander Merkurjev, Committee Chair

University of California, Los Angeles

2012

Table of Contents

Acknowledgments

I would like to thank my parents, my sister Sowan, and my girlfriend Suetying for their support through all these years. I am deeply grateful to my adviser Professor Alexander Merkurjev, who teaches me not only mathematics but also the way to do mathematics. I also thank the staffs of UCLA Department of Mathematics and everyone in the UCLA Algebra group for making me feel at home at UCLA. Finally, I want to thank my friends, especially Ivan Ip, Bun Chan, Justin Shih, Siwei Zhu and Anthony Ruozzi, for accompanying me through this long journey.

Vita

2003-2006	Bachelor of Science, Double Major in Mathematics and Physics, **University of Hong Kong**, Hong Kong
2007	Master of Arts in Mathematics, **University of California, Los Angeles**, Los Angeles, California, USA
2007-2012	Teaching Assistant, Department of Mathematics, UCLA.

Publications

On the essential dimension of cyclic groups.

Journal of Algebra, Volume 334, Issue 1, May 2011, 285-294.

CHAPTER 1

Introduction

Informally speaking, the essential dimension of an algebraic object is the smallest number of algebraically independent parameters required to define the object, thus it can be viewed as a numerical invariant that measures the complexity of the object. The notion of essential dimension was first introduced by J. Buhler and Z. Reichstein in [4] in studying the reduction of the number of independent coefficients of a general monic polynomial by nondegenerate Tschirnhaus transformations. Since then essential dimension has been studied in broader contexts, and the definition of essential dimension for a general functor was given by A. S. Merkurjev, see [1]. We refer to [21] for a comprehensive survey.

One class of the algebraic objects that we are interested in is the first Galois cohomology functor $H^1(-, G)$ of group schemes G. Since $H^1(K, G)$ is the set of isomorphism classes of G-torsors over $\mathrm{Spec}(K)$ for any field K, the essential dimension of the functor $H^1(-, G)$, which we will simply call the essential dimension of G, measures the complexity of the category of G-torsors over fields. The study of essential dimension of G is connected to many problems in algebra and algebraic geometry via Galois descent: if G is the automorphism group of an algebraic structure, then $H^1(K, G)$ classifies the K-isomorphism classes of twisted forms of that structure. For example, the study of the essential dimension of $\mathbf{PGL}_n$ is connected to central simple algebras of degree n and also to Severi-Brauer varieties of dimension $n - 1$.

In this thesis we focus on studying the essential dimension of finite groups. Making use of the ideas and techniques developed by N. A. Karpenko and A. S. Merkurjev in [15] in computing the essential dimension of finite p-groups over a field containing a primitive p-th root of unity ξ_p, we obtain new results about the essential dimension of finite cyclic groups and finite abelian groups over a field containing all primitive p-th roots of unity ξ_p for all prime divisors p of the order of the group, when certain conjectures about the canonical dimension of central simple algebras hold.

Theorem 10.1. *Let F be a field such that $char(F) \neq p_i$ and $\xi_{p_i} \in F$ for prime numbers $p_1, \ldots, p_r$. If Conjecture 8.7 is valid for algebras of degree $\prod_{i=1}^{r}[F(\xi_{p_i^{n_i}}) : F]$, then*

$$\begin{aligned}\mathrm{ed}(\mathbb{Z}/p_1^{n_1}\cdots p_r^{n_r}\mathbb{Z}) &= \mathrm{ed}(\mathbb{Z}/p_1^{n_1}\mathbb{Z}) + \cdots + \mathrm{ed}(\mathbb{Z}/p_r^{n_r}\mathbb{Z}) - r + 1 \\ &= [F(\xi_{p_1^{n_1}}) : F] + \cdots + [F(\xi_{p_r^{n_r}}) : F] - r + 1.\end{aligned}$$

Theorem 11.4. *Let $G = \prod_{j=1}^{s_1}\mathbb{Z}/p_1^{n_{1,j}}\mathbb{Z} \times \cdots \times \prod_{j=1}^{s_r}\mathbb{Z}/p_r^{n_{r,j}}\mathbb{Z}$ with $s_1 \geq \cdots \geq s_r$. Let F be a field such that $char(F) \neq p_i$ and $\xi_{p_i} \in F$ for every i. If Conjecture 11.3 is valid, then*

$$\begin{aligned}\mathrm{ed}(G) &= \sum_{i=1}^{r}\sum_{j=1}^{s_i} \ \mathrm{ed}(\mathbb{Z}/p_i^{n_{i,j}}\mathbb{Z}) - \sum_{i=2}^{r} s_i \\ &= \sum_{i=1}^{r}\sum_{j=1}^{s_i} \ [F(\xi_{p_i^{n_{i,j}}}) : F] - \sum_{i=2}^{r} s_i.\end{aligned}$$

We also compute the essential dimension of some finite groups of small order over the field of rational numbers to illustrate the behavior of essential dimension when the base field does not contain all relevant primitive roots of unity. In particular, we have the following new result.

Theorem 12.10. *Let G be a finite group. Let F be a field such that $char(F) = 0$, and $\xi_p \notin F$ for $p = 3$ and for any prime p dividing $|Z(G)|$. Then*

$$\mathrm{ed}(G \times \mathbb{Z}/3\mathbb{Z}) = \mathrm{ed}(G) + 1.$$

The layout of this thesis is as follows. Chapters 2 to 6 are about introducing notions and developing tools we need to prove our main theorems, and references for these Chapters are [1] and [19]. In particular, in Chapter 2 we give the definition of essential dimension and then we prove some of the basic properties. In Chapter 3 we define the essential dimension of a group scheme via the first Galois cohomology functor. The standard reference for Galois cohomology is [23]. Then we introduce cohomological invariants in Chapter 4 to give lower bounds of essential dimension. A reference for cohomological invariants is [10]. In Chapter 5 we recall some facts about group scheme actions and torsors, which can be found in [6] and [19] respectively. These are used to give upper bounds of essential dimension. We also show a connection between essential dimension and linear representations, and a reference for the latter is [22]. In Chapter 6 we introduce the notion of generic torsors following [10]. We prove that the essential dimension of a linear algebraic group G is the same as that of a generic G-torsor, and this result allows us to understand essential dimension from various viewpoints.

In Chapter 7 we apply the techniques about affine group schemes to give an upper bound of the essential dimension of finite cyclic groups. This result can be found in the author's publication [25]. References for affine group schemes are [16] and [24]. We remark that this result can also be obtained by a totally different method, see [17].

We introduce the tools needed to find a lower bound of the essential dimension of finite cyclic groups in Chapters 8 and 9. In Chapter 8 we introduce the notion of canonical dimension, and in Chapter 9 we study the canonical and essential dimension of fibered categories. References for these Chapters are [14], [18] and [19]. A comprehensive survey of canonical dimension is [13], and a general reference for fibered categories is [8].

In Chapter 10 we give a lower bound of the essential dimension of finite cyclic groups in terms of the canonical dimension of a central simple algebra. This lower bound coincides with our upper bound in Chapter 7 if a conjecture about canonical dimension of central simple algebras holds. This result can be found in [25], and it is also studied in [3]. A reference for central simple algebras is [11].

In Chapter 11 we generalize our results to the essential dimension of finite abelian groups. Again the lower bound depends on a conjecture about canonical dimension of central simple algebras.

Finally in Chapter 12 we compute the essential dimension of finite groups of small order over $\mathbb{Q}$. Since $\mathbb{Q}$ does not contain any primitive p-th roots of unity for $p \neq 2$, we see that the techniques used in this chapter is vastly different from those used in Chapters 7, 10 and

11. References for this chapter are [1] and [12].

CHAPTER 2

Definition and Basic Properties

Let F be a field. We write Fun_F for the category of all (covariant) functors from $Fields/F$ the category of field extensions of F and field homomorphisms over F to $Sets$ the category of sets. Let $\mathfrak{F}$ be an object in Fun_F. If $K \to L$ is a morphism in $Fields/F$, for every element $a \in \mathfrak{F}(K)$ we denote by a_L the image of a in $\mathfrak{F}(L)$ under the map $\mathfrak{F}(K) \to \mathfrak{F}(L)$.

Definition 2.1. *Let $\mathfrak{F}$ be an object in Fun_F, K/F a field extension, and $a \in \mathfrak{F}(K)$. The essential dimension of a, denoted by* $\mathrm{ed}(a)$*, is defined by*

$$\mathrm{ed}(a) = \min\{tr.deg_F(K_0)\}$$

where the minimum is taken over all subfields K_0 of K over F such that $a = b_K$ for some $b \in \mathfrak{F}(K_0)$.

The essential dimension of $\mathfrak{F}$, denoted by $\mathrm{ed}(\mathfrak{F})$*, is defined by*

$$\mathrm{ed}(\mathfrak{F}) = \sup\{\mathrm{ed}(a)\}$$

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

Intuitively speaking, for any $a \in \mathfrak{F}(K)$, the essential dimension of a is the number of algebraically independent parameters we need to describe a. The essential dimension of $\mathfrak{F}$ is then the number of algebraically independent parameters required to describe any arbitrary element of $\mathfrak{F}$.

Example 2.2. Let F be our fixed base field.

(1) Let S be a singleton set, and $\mathfrak{F}$ be the functor that sends every $K \in Fields/F$ to S. It is clear that $\mathrm{ed}(\mathfrak{F}) = 0$.

(2) Let $\mathfrak{O} : Fields/F \to Sets$ be the forgetful functor. Then it follows from the definition that $\mathrm{ed}(\mathfrak{O}) = 1$.

It is also not hard to see that $\mathrm{ed}(\prod_{i=1}^{n} \mathfrak{O}) = n$ for every positive integer n, and therefore $\mathrm{ed}(\prod_{i\in\mathbb{N}} \mathfrak{O}) = \infty$.

(3) Let Alg_n be the functor that sends every $K \in Fields/F$ to the set of isomorphism classes of n-dimensional K-algebras of the form $K[X]/\langle f(X)\rangle$, where $f(X)$ is a degree n monic polynomial over K.

Let $A = K[X]/\langle f(X)\rangle$ and $B = K[Y]/\langle g(Y)\rangle$ be two such n-dimensional K-algebras, and let x and y be the class of X in A and the class of Y in B respectively. A homomorphism $\phi : A \to B$ is determined by the image of x, which satisfies $f(\phi(x)) = 0$. ϕ is an isomorphism if and only if $\phi(x)$ generates B, and in this case $\phi(x)$ is a nondegenerate Tschirnhaus transformation of f.

Write $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$. Then we see that $A = A'_K \in Alg_n(K)$ where $A' = K_0[X]/\langle f(X)\rangle \in Alg_n(K_0)$ with $K_0 = F(a_0, \ldots, a_{n-1})$. Therefore the smallest number of coefficients appearing in $f(X)$ by applying nondegenerate Tschirnhaus transformations is equal to the essential dimension of the isomorphism class of $K[X]/\langle f(X)\rangle$.

Assume $char(F)$ does not divide n, then we can drop the coefficient a_{n_1} for X^{n-1} by using the substitution $Y = X - \frac{a_{n-1}}{n}$. Therefore $\mathrm{ed}(Alg_n) \leq n - 1$.

For $n = 2$, we know that $\mathrm{ed}(Alg_2) \leq 1$. Let t be an algebraically independent element over F. The algebra $F(t)[X]/\langle X^2 + t\rangle$ is not defined over any algebraic field extension of F, thus $\mathrm{ed}(Alg_2) = 1$.

For $n = 3$, first any monic degree 3 polynomial can be reduced to the form $X^3+a_1X+a_0$. If $a_1 \neq 0$, we can use the substitution $Y = \frac{a_0}{a_1}X$ to make the two coefficients equal, and reduce the polynomial to the form $X^3 + bX + b$. Therefore $\mathrm{ed}(Alg_3) \leq 1$. Similar to the $n = 2$ case, we consider the algebra $F(t)[X]/\langle X^3 + tX + t\rangle$ which is not defined over any algebraic field extension of F. Hence $\mathrm{ed}(Alg_3) = 1$.

Remark 2.3. As we can see from the definition that the notion of essential dimension depends on the base field F. When the base field is fixed, or when it is clear from the context that over what base field we are considering, there is no confusion by writing $\mathrm{ed}(\mathfrak{F})$. However, when the context is not clear, or when we want to emphasize our base field, we will write $\mathrm{ed}_F(\mathfrak{F})$.

Proposition 2.4. *Let $\mathfrak{F}$ be an object in Fun_F, K/F a field extension. By restriction we can view $\mathfrak{F}$ as an object in Fun_K. Then*

$$\mathrm{ed}_K(\mathfrak{F}) \leq \mathrm{ed}_F(\mathfrak{F}).$$

Proof. For every field extension L/K and $a \in \mathfrak{F}(L)$, there is a subextension $F \subseteq K_0 \subseteq L$ such that $tr.deg_F(K_0) \leq \mathrm{ed}_F(\mathfrak{F})$ and $a = b_L$ for some $b \in \mathfrak{F}(K_0)$. The composite field K_0K has $tr.deg_K(K_0K) \leq \mathrm{ed}_F(\mathfrak{F})$, and there exists $b' = b_{K_0K} \in \mathfrak{F}(K_0K)$ such that $a = b'_L$. Therefore $\mathrm{ed}_K(a) \leq \mathrm{ed}_F(\mathfrak{F})$ and $\mathrm{ed}_K(\mathfrak{F}) \leq \mathrm{ed}_F(\mathfrak{F})$. $\square$

Let $\mathfrak{F}$ and $\mathfrak{G}$ be objects in Fun_F. A morphism $f : \mathfrak{F} \to \mathfrak{G}$ is called a surjection if for any field extension K/F, the corresponding map of sets $f_K : \mathfrak{F}(K) \to \mathfrak{G}(K)$ is surjective.

Lemma 2.5. *Let $f : \mathfrak{F} \to \mathfrak{G}$ be a surjection in Fun_F. Then*

$$\mathrm{ed}(\mathfrak{G}) \leq \mathrm{ed}(\mathfrak{F}).$$

Proof. For every field extension K/F and every $b \in \mathfrak{G}(K)$, by assumption there exists $a \in \mathfrak{F}(K)$ such that $f_K(a) = b$. Since $\mathrm{ed}(a) \leq \mathrm{ed}(\mathfrak{F})$, there is a subextension $F \subseteq K_0 \subseteq K$ such that $tr.deg_F(K_0) \leq \mathrm{ed}(\mathfrak{F})$ and $a = a'_K$ for some $a' \in \mathfrak{F}(K_0)$. Hence $\mathrm{ed}(b) \leq \mathrm{ed}(\mathfrak{F})$ as there is $b' = f_{K_0}(a') \in \mathfrak{G}(K_0)$ satisfying $b'_K = f_{K_0}(a')_K = f_K(a'_K) = b$. $\square$

Next we are going to study the behavior of essential dimension under coproducts and products.

Lemma 2.6. *Let $\mathfrak{F}$ and $\mathfrak{G}$ be objects in Fun_F. Then*

$$\mathrm{ed}(\mathfrak{F} \coprod \mathfrak{G}) = \max\{\mathrm{ed}(\mathfrak{F}), \mathrm{ed}(\mathfrak{G})\}.$$

Proof. For every field extension K/F and every $a \in \mathfrak{F}(K) \coprod \mathfrak{G}(K)$, we have $\mathrm{ed}(a) \leq \mathrm{ed}(\mathfrak{F})$ or $\mathrm{ed}(a) \leq \mathrm{ed}(\mathfrak{G})$. Thus $\mathrm{ed}(\mathfrak{F} \coprod \mathfrak{G}) \leq \max\{\mathrm{ed}(\mathfrak{F}), \mathrm{ed}(\mathfrak{G})\}$.

For the opposite inequality, it suffices to note that $(\mathfrak{F} \coprod \mathfrak{G})(K) = \mathfrak{F}(K) \coprod \mathfrak{G}(K)$. □

Lemma 2.7. *Let $\mathfrak{F}$ and $\mathfrak{G}$ be objects in Fun_F. Then*

$$\mathrm{ed}(\mathfrak{F} \times \mathfrak{G}) \leq \mathrm{ed}(\mathfrak{F}) + \mathrm{ed}(\mathfrak{G}).$$

Proof. For every field extension K/F and every $(a, a') \in \mathfrak{F}(K) \times \mathfrak{G}(K)$, there are subextensions $F \subseteq L, L' \subseteq K$ such that $tr.deg_F(L) \leq \mathrm{ed}(\mathfrak{F})$, $tr.deg_F(L') \leq \mathrm{ed}(\mathfrak{G})$ and $a = b_K$ for some $b \in \mathfrak{F}(L)$, $a' = b'_K$ for some $b' \in \mathfrak{G}(L')$. Then the composite field LL' has $tr.deg_F(LL') \leq tr.deg_F(L) + tr.deg_F(L')$, and there exists $c = b_{LL'} \in \mathfrak{F}(LL')$, $c' = b'_{LL'} \in \mathfrak{G}(LL')$ such that $(a, a') = (c, c')_K$. Therefore

$$\mathrm{ed}(a, a') \leq tr.deg_F(LL') \leq tr.deg_F(L) + tr.deg_F(L') \leq \mathrm{ed}(\mathfrak{F}) + \mathrm{ed}(\mathfrak{G})$$

and this completes the proof. □

Remark 2.8. Since there are surjections from $\mathfrak{F} \times \mathfrak{G}$ to $\mathfrak{F}$ and $\mathfrak{G}$, we have

$$\max\{\mathrm{ed}(\mathfrak{F}), \mathrm{ed}(\mathfrak{G})\} \leq \mathrm{ed}(\mathfrak{F} \times \mathfrak{G}) \leq \mathrm{ed}(\mathfrak{F}) + \mathrm{ed}(\mathfrak{G}).$$

Let $\mathfrak{F}$ and $\mathfrak{G}$ be objects in Fun_F, and in addition $\mathfrak{F}$ is a group-valued functor. We say that $\mathfrak{F}$ acts on $\mathfrak{G}$ if, for every field extension K/F, the group $\mathfrak{F}(K)$ acts on the set $\mathfrak{G}(K)$ such that the following compatibility condition holds: for every field extension L/K and every $a \in \mathfrak{F}(K)$, $b \in \mathfrak{G}(K)$, one has $(a \cdot b)_L = a_L \cdot b_L$. We say that the action of $\mathfrak{F}$ on $\mathfrak{G}$ is transitive if, for every field extension K/F, the group $\mathfrak{F}(K)$ acts transitively on the set $\mathfrak{G}(K)$.

Let $\pi : \mathfrak{G} \to \mathfrak{H}$ be a morphism in Fun_F, and let K/F be a field extension of F. Then every element $a \in \mathfrak{H}(K)$ induces a functor $\pi^{-1}(a)$ in Fun_K by setting $\pi^{-1}(a)(L) = \{b \in \mathfrak{G}(L) : \pi_L(b) = a_L\}$ for every extension L/K.

Definition 2.9. *Let $\mathfrak{F}$ be a group-valued functor in Fun_F, and let $\pi : \mathfrak{G} \to \mathfrak{H}$ be a surjection in Fun_F. We say that $\mathfrak{F}$ is in fibration position for π if for every field extension K/F and every element $a \in \mathfrak{H}(K)$, $\mathfrak{F}$ (viewed over Fun_K) acts transitively on $\pi^{-1}(a)$.*

Proposition 2.10. *Let $\mathfrak{F}$ be in fibration position for $\pi : \mathfrak{G} \to \mathfrak{H}$. Then*

$$\mathrm{ed}(\mathfrak{G}) \leq \mathrm{ed}(\mathfrak{F}) + \mathrm{ed}(\mathfrak{H}).$$

Proof. Let K/F be a field extension and $b \in \mathfrak{G}(K)$. Consider $\pi_K(b) \in \mathfrak{H}(K)$. There is a subextension $F \subseteq L \subseteq K$ such that $tr.deg_F(L) \leq \mathrm{ed}(\mathfrak{H})$ and $\pi_K(b) = c_K$ for some $c \in \mathfrak{H}(L)$. As π is surjective, there exists $b' \in \mathfrak{G}(L)$ such that $\pi_L(b') = c$. Note that $\pi_K(b'_K) = c_K = \pi_K(b)$, therefore by assumption there is $a \in \mathfrak{F}(K)$ such that $a \cdot b'_K = b$. Then there exists a subextension $F \subseteq L' \subseteq K$ such that $tr.deg_F(L') \leq \mathrm{ed}(\mathfrak{F})$ and $a = a'_K$ for some $a' \in \mathfrak{F}(L')$. Consider the composite extension LL' and $d = a'_{LL'} \cdot b'_{LL'} \in \mathfrak{G}(LL')$. We have

$$d_K = (a'_{LL'} \cdot b'_{LL'})_K = a'_K \cdot b'_K = a \cdot b'_K = b,$$

and hence

$$\mathrm{ed}(b) \leq tr.deg_F(LL') \leq tr.deg_F(L) + tr.deg_F(L') \leq \mathrm{ed}(\mathfrak{H}) + \mathrm{ed}(\mathfrak{F}).$$ □

Corollary 2.11. *Let $1 \longrightarrow \mathfrak{F} \longrightarrow \mathfrak{G} \longrightarrow \mathfrak{H} \longrightarrow 1$ be a short exact sequence of group-valued functor. Then*

$$\mathrm{ed}(\mathfrak{G}) \leq \mathrm{ed}(\mathfrak{F}) + \mathrm{ed}(\mathfrak{H}).$$

Proof. It follows directly from the fact that $\mathfrak{H}(K) \cong \mathfrak{G}(K)/\mathfrak{F}(K)$ for every field extension K/F, and $\mathfrak{F}(K)$ acts transitively on the fibers by group multiplication. □

Let X be a scheme over F, which we will always mean a scheme of finite type over F. It defines an object in Fun_F, a "functor of points" which is still denoted by X, by setting $X(K) = \mathrm{Hom}(\mathrm{Spec}(K), X)$ the set of all K-rational points of X for every field extension K/F. The following proposition justifies the terminology of essential dimension.

Proposition 2.12. *Let X be a scheme over F. Then*

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

Proof. Let $a : \mathrm{Spec}(K) \to X$ be an element in $X(K)$ for some field extension K/F, and let $\{x\}$ be the image of a. Then we have an inclusion of fields $F(x) \hookrightarrow K$, where $F(x)$ is the residue field at x. Therefore $\mathrm{ed}(a) = tr.deg_F(F(x))$, and

$$\mathrm{ed}(X) = \sup\{\mathrm{ed}(a)\} = \sup\{tr.deg_F(F(x))\} = \dim(X),$$

where the second supremum is taken over all $x \in X$. $\square$

Definition 2.13. *Let $\mathfrak{F}$ be an object in Fun_F, and let X be a scheme over F. We say that X is a classifying scheme of $\mathfrak{F}$ if there is a surjection $X \to \mathfrak{F}$ in Fun_F.*

Proposition 2.14. *If X is a classifying scheme of $\mathfrak{F}$, then*

$$\mathrm{ed}(\mathfrak{F}) \leq \dim(X).$$

Proof. It follows directly from the definition of classifying schemes, Lemma 2.5 and Proposition 2.12. $\square$

Proposition 2.14 is one of the important tools in computing essential dimension as it allows us to apply various techniques in algebraic geometry.

Example 2.15. Let n be any positive integer. We define Q_n to be the functor that sends every $K \in Fields/F$ to the set of isomorphism classes of non-degenerate n-dimensional quadratic forms over K.

Suppose $char(F) \neq 2$, then every quadratic form is diagonalizable. Hence there is a surjection $\mathbb{G}_m^n \to Q_n$ in Fun_F, where G_m is the multiplicative group scheme over F, given by

$$\begin{aligned} \mathbb{G}_m^n(K) &\longrightarrow Q_n(K) \\ (a_1, \dots, a_n) &\longmapsto \langle a_1, \dots, a_n \rangle \, . \end{aligned}$$

Therefore $\mathbb{G}_m^n$ is a classifying scheme of Q_n, and $\mathrm{ed}(Q_n) \leq \dim(\mathbb{G}_m^n) = n$.

CHAPTER 3

Essential Dimension of Group Schemes

Let G be a group scheme (of finite type) over F. The Galois cohomology functor $H^1(-, G)$ is an object in Fun_F, and we have the following definition.

Definition 3.1. *Let G be a group scheme over F. The essential dimension of G is defined as*

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

Thus the essential dimension of G measures the complexity of the category of G-torsors (principal homogeneous space). If G is a finite abstract group, we view G as a constant group scheme over F.

We are interested in the essential dimension of group schemes because many objects in Fun_F can be viewed as Galois cohomology functors.

Proposition 3.2. *Let (V, x) be an algebraic structure over a field F in the sense of [23, Chapter III.1]. For every field extension K/F, let $G(K) = \mathrm{Aut}_K(V \otimes_F K)$ be the group of K-automorphisms which preserve the structure. Then $H^1(F, G)$ classifies the F-isomorphism classes of twisted forms of (V, x), i.e. the algebraic structures over F which become isomorphic to (V, x) over F_{sep}.*

Example 3.3.

(1) Let $\acute{E}t_n$ be the functor that sends every $K \in Fields/F$ to the set of isomorphism classes of n-dimensional étale algebras over K. Then we consider the F-algebra $A = F \times \cdots \times F$ (n copies). It is known that $\mathrm{Aut}_K(A \otimes_F K) = S_n$ the symmetric group, and the twisted

forms of A are exactly the n-dimensional étale F-algebras. Therefore $\acute{E}t_n \cong H^1(-, S_n)$ as functors, and $\mathrm{ed}(\acute{E}t_n) = \mathrm{ed}(S_n)$.

(2) Let CSA_n be the functor that sends every $K \in \mathit{Fields}/F$ to the set of isomorphism classes of central simple algebras of degree n over K. Similar to the previous example we consider $A = M_n(F)$ the matrix algebra of degree n. By Skolem-Noether Theorem $\mathrm{Aut}_K(A \otimes_F K) = \mathbf{PGL}_n$ the projective linear group. Since the twisted forms of A are central simple algebras of degree n, we have $CSA_n \cong H^1(-, \mathbf{PGL}_n)$ as functors, and $\mathrm{ed}(CSA_n) = \mathrm{ed}(\mathbf{PGL}_n)$. Note that $\mathbf{PGL}_n$ is also the automorphism group of the projective space $\mathbb{P}^{n-1}$, and the twisted forms of $\mathbb{P}^{n-1}$ are Severi-Brauer varieties of dimension $n-1$. Therefore $\mathrm{ed}(\mathbf{PGL}_n)$ is also equal to $\mathrm{ed}(SB_{n-1})$ where SB_{n-1} is the functor that sends every $K \in \mathit{Fields}/F$ to the set of isomorphism classes of Severi-Brauer varieties of dimension $n-1$.

(3) Let G be a finite abstract group. Recall that a Galois G-algebra over F is an étale F-algebra A endowed with an action by G of F-automorphisms, such that $\dim_F(A) = |G|$ the order of G, and $A^G = F$. Let G-Alg be the functor that sends every $K \in \mathit{Fields}/F$ to the set of G-isomorphism classes of Galois G-algebras over K. By [16, Theorem 18.19] $G\text{-}Alg \cong H^1(-, G)$, thus $\mathrm{ed}(G\text{-}Alg) = \mathrm{ed}(G)$.

Next we are going to do some computations on essential dimension.

Example 3.4.

(1) Let n be any positive integer. By Hilbert's Theorem 90 $H^1(K, \mathbf{GL}_n) = 0$ for every $K \in \mathit{Fields}/F$. Hence $\mathrm{ed}(\mathbf{GL}_n) = 0$. It is also well-known that $H^1(K, \mathbf{SL}_n) = 0$ and $H^1(K, \mathbb{G}_a) = 0$ for every $K \in \mathit{Fields}/F$, thus $\mathrm{ed}(\mathbf{SL}_n) = \mathrm{ed}(\mathbb{G}_a) = 0$.

(2) Let n be a positive integer such that $\mathit{char}(F)$ does not divide n. Consider μ_n the group scheme of n-th roots of unity. Then for every $K \in \mathit{Fields}/F$, $H^1(K, \mu_n) = K^\times / K^{\times n}$ by Kummer theory. It follows that $\mathrm{ed}(\mu_n) = 1$.

On the other hand, if $char(F) = p > 0$, we know that $H^1(K, \mu_p) = 0$. Thus $\mathrm{ed}(\mu_p) = 0$.

(3) Let p be a prime number. We want to compute the essential dimension of the constant group scheme $\mathbb{Z}/p\mathbb{Z}$.

If $char(F) = p$, then by Artin-Schreier theory $H^1(K, \mathbb{Z}/p\mathbb{Z}) = K/\wp(K)$ for every $K \in Fields/F$, where $\wp(x) = x^p - x$ for every $x \in K$. It is then easy to see that $\mathrm{ed}(\mathbb{Z}/p\mathbb{Z}) = 1$.

If $char(F) \neq p$ and F contains all the p-th roots of unity, we can identify (non-canonically) $\mathbb{Z}/p\mathbb{Z}$ with μ_p by choosing a primitive p-th root of unity. In this case we know from the previous example that $\mathrm{ed}(\mathbb{Z}/p\mathbb{Z}) = 1$. When F does not contain all the p-th roots of unity, the computation of $\mathrm{ed}(\mathbb{Z}/p\mathbb{Z})$ is still an open problem.

Remark 3.5. Let F be an algebraically closed field. Recall that a linear algebraic group G over F is called special if $H^1(K, G) = 0$ for every field extension K/F. Thus linear algebraic groups of essential dimension zero are precisely the special groups.

CHAPTER 4

Cohomological Invariants

In general, the essential dimension of functors is very hard to compute. Usually we break down the computation into two parts: finding lower bounds, and finding upper bounds for the essential dimension. One way of giving lower bounds of essential dimension is to make use of cohomological invariants, which we are going to introduce in the following.

Definition 4.1. *Let $\mathfrak{F}$ be an object in Fun_F, and let n be a positive integer. We say that $\mathfrak{F}$ is n-simple if there exists a field extension K/F such that, for any extensions L/K with $tr.deg_K(L) < n$ the set $\mathfrak{F}(L)$ consists of one element.*

Definition 4.2. *Let $f : \mathfrak{F} \to \mathfrak{G}$ be a morphism in Fun_F. We say that f is non-constant if for any field extension K/F, there exists an extension L/K and $a \in \mathfrak{F}(K), b \in \mathfrak{F}(L)$ such that $f_L(a_L) \neq f_L(b)$.*

Proposition 4.3. *Let $f : \mathfrak{F} \to \mathfrak{G}$ be a non-constant morphism in Fun_F. If $\mathfrak{G}$ is n-simple, then*

$$\mathrm{ed}(\mathfrak{F}) \geq n.$$

Proof. Let K/F be a field extension such that $\mathfrak{G}(K')$ is a singleton set for every extensions K'/K satisfying $tr.deg_K(K') < n$. Suppose on contrary $\mathrm{ed}_F(\mathfrak{F}) < n$. By Proposition 2.4 $\mathrm{ed}_K(\mathfrak{F}) \leq \mathrm{ed}_F(\mathfrak{F}) < n$. As f is a non-constant morphism, there is a field extension L/K and $a \in \mathfrak{F}(K), b \in \mathfrak{F}(L)$ such that $f_L(a_L) \neq f_L(b)$. Since $\mathrm{ed}_K(\mathfrak{F}) < n$, there exists a subextension $K \subseteq L_0 \subseteq L$ such that $tr.deg_K(L_0) < n$ and $b = c_L$ for some $c \in \mathfrak{F}(L_0)$. Consider the following commutative diagram

$$\begin{array}{ccc}
\mathfrak{F}(L) & \xrightarrow{f_L} & \mathfrak{G}(L) \\
\uparrow & & \uparrow \\
\mathfrak{F}(L_0) & \xrightarrow{f_{L_0}} & \mathfrak{G}(L_0) \\
\uparrow & & \uparrow \\
\mathfrak{F}(K) & \xrightarrow{f_K} & \mathfrak{G}(K).
\end{array}$$

Then $f_{L_0}(a_{L_0}) \neq f_{L_0}(c)$ because $f_L(a_L) \neq f_L(b) = f_L(c_L)$. Therefore we get a contradiction as $tr.deg_K(L_0) < n$ implies $\mathfrak{G}(L_0)$ is a singleton set. □

Let M be a torsion discrete Galois module over F, i.e. a torsion discrete module over the absolute Galois group $\Gamma_F = Gal(F_{sep}/F)$. For any field extension K/F, M can be endowed with the structure of a Galois module over K and the cohomology group $H^n(K, M)$ is defined for any non-negative integer n. Therefore we have a functor $H^n(-, M)$ from $Fields/F$ to $PtSets$ the category of pointed sets, where $H^n(K, M)$ is pointed by 0 the class of the trivial cocycle.

Definition 4.4. *Let $\mathfrak{F}$ be a functor from $Fields/F$ to $PtSets$. A cohomological invariant of degree n of $\mathfrak{F}$ is a morphism of pointed functors $\phi : \mathfrak{F} \to H^n(-, M)$, where M is a torsion discrete Galois module over F. We say that it is non-trivial if for any field extension K/F, there exists an extension L/K and $a \in \mathfrak{F}(L)$ such that $\phi_L(a) \neq 0 \in H^n(L, M)$.*

Proposition 4.5. *Let $\mathfrak{F}$ be a functor from $Fields/F$ to $PtSets$. If $\mathfrak{F}$ has a non-trivial cohomological invariant of degree n, then*

$$\mathrm{ed}(\mathfrak{F}) \geq n.$$

Proof. It is known that for any torsion discrete Galois module M, $H^n(L, M) = 0$ if L contains an algebraically closed field K and $tr.deg_K(L) < n$ (see [23]). It follows that the functor $H^n(-, M)$ is n-simple by taking K to be $\overline{F}$ an algebraic closure of F. Since any non-trivial cohomological invariant is clearly a non-constant morphism, by applying Proposition 4.3 we immediately see that $\mathrm{ed}(\mathfrak{F}) \geq n$. □

Let G be an abstract finite abelian group. Let $G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$, with $1 \neq n_1 \mid \cdots \mid n_r$, be the invariant factor decomposition of G. The number r is called the rank of G and is denoted by $rank(G)$.

Proposition 4.6. *Let G be an abstract finite abelian group such that $char(F)$ does not divide $exp(G)$ the exponent of G. Then*

$$\mathrm{ed}(G) \geq rank(G).$$

Proof. Our goal is to define a non-trivial cohomological invariant ϕ of degree n for $H^1(-, G)$ so that we can apply Proposition 4.5. First by Proposition 2.4 we may assume F is algebraically closed. From the invariant factor decomposition of G, we have the following isomorphism for every field extension K/F

$$\begin{aligned} H^1(K, G) &\cong H^1(K, \mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times H^1(K, \mathbb{Z}/n_r\mathbb{Z}). \\ a &\mapsto (a_1, \ldots, a_r) \end{aligned}$$

Composing this isomorphism with the cup product

$$\begin{aligned} H^1(K, \mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times H^1(K, \mathbb{Z}/n_r\mathbb{Z}) &\to H^r(K, \mathbb{Z}/n_1\mathbb{Z}) \\ (a_1, \ldots, a_r) &\mapsto a_1 \cup \cdots \cup a_r \end{aligned}$$

gives us a cohomological invariant of degree r

$$\phi : H^1(-, G) \longrightarrow H^r(K, \mathbb{Z}/n_1\mathbb{Z}) \ ,$$

where in the cup product we use the fact that $\mathbb{Z}/n_1\mathbb{Z} \otimes \cdots \otimes \mathbb{Z}/n_r\mathbb{Z} = \mathbb{Z}/n_1\mathbb{Z}$. Then it remains to prove that ϕ is non-trivial.

Let K/F be a field extension. Consider $L = K(t_1, \ldots, t_r)$ where $t_1, \ldots, t_r$ are indeterminates. Since F is algebraically closed and $char(F)$ does not divide $exp(G)$, $H^1(L, \mathbb{Z}/n_i\mathbb{Z}) = L^\times / L^{\times n_i}$ for every i. Denote the class of t_i in $H^1(L, \mathbb{Z}/n_i\mathbb{Z})$ by $\overline{t_i}$, and let $a = (\overline{t_1}, \ldots, \overline{t_r}) \in H^1(L, G)$. Then

$$\phi(a) = \overline{t_1} \cup \cdots \cup \overline{t_r} \in H^r(L, \mathbb{Z}/n_1\mathbb{Z})$$

and we are going to show that it is non-zero by induction on r.

For $r = 1$, $\overline{t_1} \in K(t_1)^\times / K(t_1)^{\times n_1}$ is clearly non-zero. For $r > 1$, let v be the t_r-adic valuation on L. Then the residue field of v is just $K(t_1, \dots, t_{r-1})$, and there is an associated residue homomorphism

$$\partial_v : H^r(L, \mathbb{Z}/n_1\mathbb{Z}) \longrightarrow H^{r-1}(K(t_1, \dots, t_{r-1}), \mathbb{Z}/n_1\mathbb{Z}).$$

We have $\partial_v(\overline{t_1} \cup \cdots \cup \overline{t_r}) = \overline{t_1} \cup \cdots \cup \overline{t_{r-1}}$ which is non-zero by induction hypothesis. Therefore ϕ is non-trivial, and this completes the proof. □

Remark 4.7. The assumption that $char(F) \nmid exp(G)$ cannot be dropped. Suppose $char(F) = p > 0$ and F contains $\mathbb{F}_{p^r}$ the finite field of p^r elements. Consider the group $G = \mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z}$ (r copies). We have the following short exact sequence

$$0 \longrightarrow G \longrightarrow \mathbb{G}_a \xrightarrow{\wp} \mathbb{G}_a \longrightarrow 0$$

where $\wp(x) = x^p - x$. Passing to cohomology yields the exact sequence

$$\mathbb{G}_a(K) \longrightarrow H^1(K, G) \longrightarrow H^1(K, \mathbb{G}_a).$$

for every field extension K/F. Since $H^1(K, \mathbb{G}_a) = 0$, we see that $\mathbb{G}_a$ is a classifying scheme for $H^1(-, G)$. Therefore by Proposition 2.14 (and Remark 2.8) $\mathrm{ed}(G) = 1$, while clearly $rank(G) = r$.

Corollary 4.8. *Let G be the group $\mu_{n_1} \times \cdots \times \mu_{n_r}$, where $1 \neq n_1 \mid \cdots \mid n_r$, and $char(F)$ does not divide n_r. Then*

$$\mathrm{ed}(G) = r.$$

Proof. Since $H^1(K, G) = H^1(K, \mu_{n_1}) \times \cdots \times H^1(K, \mu_{n_r}) = K^\times / K^{\times n_1} \times \cdots \times K^\times / K^{\times n_r}$, we see that there is a surjection of functors $\mathbb{G}_m^r \to H^1(-, G)$. Hence $\mathbb{G}_m^r$ is classifying scheme for $H^1(-, G)$, and $\mathrm{ed}(G) \leq r$.

For the other inequality, first note that $\mathrm{ed}_{\overline{F}}(G) \leq \mathrm{ed}_F(G)$, where $\overline{F}$ is an algebraic closure of F. Since over $\overline{F}$ we have G isomorphic to $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$, by Proposition 4.6 $\mathrm{ed}_{\overline{F}}(G) \geq r$. □

Remark 4.9. We have seen in Remark 2.8 that

$$\max\{\mathrm{ed}(\mathfrak{F}), \mathrm{ed}(\mathfrak{G})\} \leq \mathrm{ed}(\mathfrak{F} \times \mathfrak{G}) \leq \mathrm{ed}(\mathfrak{F}) + \mathrm{ed}(\mathfrak{G}).$$

Let n and m be two positive integers such that $char(F)$ does not divide nm, and n, m are coprime. Then $\mu_n \times \mu_m \cong \mu_{nm}$, and hence

$$\max\{\mathrm{ed}(\mu_n), \mathrm{ed}(\mu_m)\} = 1 = \mathrm{ed}(\mu_n \times \mu_m).$$

Thus it is possible that $\max\{\mathrm{ed}(\mathfrak{F}), \mathrm{ed}(\mathfrak{G})\} = \mathrm{ed}(\mathfrak{F} \times \mathfrak{G})$.

On the other hand, by Corollary 4.8

$$\mathrm{ed}(\mu_n \times \mu_n) = 2 = \mathrm{ed}(\mu_n) + \mathrm{ed}(\mu_n).$$

Therefore it is also possible that $\mathrm{ed}(\mathfrak{F} \times \mathfrak{G}) = \mathrm{ed}(\mathfrak{F}) + \mathrm{ed}(\mathfrak{G})$.

Next we are going to apply the cohomological invariant technique to quadratic forms. The following theorem confirms our intuition that in general we need exactly n parameters to describe an n-dimensional quadratic form over a field of characteristic not equal to 2.

Theorem 4.10. *Let n be any positive integer. Suppose that $char(F) \neq 2$. Then*

$$\mathrm{ed}(Q_n) = n.$$

Proof. By Example 2.15 we have $\mathrm{ed}(Q_n) \leq n$. To show that $\mathrm{ed}(Q_n) \geq n$, consider Delzant's Stiefel-Whitney class denoted by ω_n (see [10]).

Let K/F be a field extension. Take $L = K(t_1, \ldots, t_n)$ where $t_1, \ldots, t_n$ are indeterminates. Let $q = \langle t_1, \ldots, t_n \rangle \in Q_n(L)$. Then we have

$$\omega_n(q) = \overline{t_1} \cup \cdots \cup \overline{t_n} \in H^n(L, \mathbb{Z}/2\mathbb{Z})$$

which is non-zero from the proof of Proposition 4.6. Therefore ω_n is a non-trivial cohomological invariant of degree n, and the result follows from Proposition 4.5. $\square$

CHAPTER 5

Group Scheme Actions

We first recall here some facts about group scheme actions and torsors that we need later.

Let G be a group scheme over a base scheme S and let X be an S-scheme. An action of G on X is a morphism of S-schemes

$$\begin{aligned} G \times_S X &\longrightarrow X \\ (g, x) &\longmapsto x \cdot g \end{aligned}$$

which satisfy the categorical condition of a usual group action. For any S-scheme T, an action of G on X induces an action (in the usual sense) of the group $G(T)$ on the set $X(T)$.

We say that G acts freely on X if for every S-scheme T, the group $G(T)$ acts freely on the set $X(T)$. We also say that the action of G on X is generically free if there exists a G-invariant dense open subset U of X such that G acts freely on U.

Definition 5.1. *Let G be a group scheme over a scheme Y which is flat and locally of finite type over Y. We say that a morphism of schemes $X \to Y$ is a G-torsor over Y if G acts on X, the morphism $X \to Y$ is flat and locally of finite type, and the morphism*

$$\begin{aligned} G \times_Y X &\longrightarrow X \times_Y X \\ (g, x) &\longmapsto (x, x \cdot g) \end{aligned}$$

is an isomorphism.

By [20, Chapter III Proposition 4.1], this condition is equivalent to the existence of a covering $(U_i \to Y)$ for the flat topology on Y such that $G \times_Y U_i$ is isomorphic to $X \times_Y U_i$ for every i. This can be interpreted as saying that X is locally isomorphic to G for the flat topology on Y. Note that if G is smooth, respectively étale, ..., over Y, then so is X by faithfully flat descent.

A morphism between two G-torsors $f : X \to Y$ and $f' : X' \to Y$ defined over the same base scheme is a G-equivariant morphism $\varphi : X \to X'$ satisfying $f' \circ \varphi = f$. It follows from faithfully flat descent that any morphism between G-torsors is an isomorphism. If $X \to Y$ is a G-torsor over Y, then for every morphism $Y' \to Y$ the pullback of the diagram

$$\begin{tikzcd} & X \arrow[d] \\ Y' \arrow[r] & Y \end{tikzcd}$$

is a G-torsor over Y'.

Remark 5.2. Note that if $X \to Y$ is a G-torsor, then G acts freely on X: For any $x \in X$, the stabilizer G_x of x is defined by the following pullback diagram

$$\begin{tikzcd} G_x \arrow[r] \arrow[d] & G \times_Y \{x\} \arrow[d] \\ \mathrm{Spec}(F(x)) \arrow[r, "x"] & X \end{tikzcd}$$

where $F(x)$ is the residue field at x, and the morphism $G \times_Y \{x\} \to X$ is the composition of the inclusion morphism with the group action morphism

$$G \times_Y \{x\} \hookrightarrow G \times_Y X \longrightarrow X \ .$$

Then the fiber of the point $(x, x) \in X \times_Y X$ under the morphism $\phi : G \times_Y X \to X \times_Y X$ is isomorphic to the stabilizer G_x. Since ϕ is an isomorphism, G_x is trivial for every $x \in X$. The result then follows from [6, Chapter III.2 Corollary 2.3].

Let G acts on an S-scheme X. A morphism $\pi : X \to Y$ is called a categorical quotient of X by G if π is (isomorphic to) the pushout of the diagram

$$\begin{tikzcd} G \times_S X \arrow[r] \arrow[d, "pr_2"] & X \\ X & \end{tikzcd}$$

where the horizontal morphism is the action of G on X, and the vertical morphism is the second projection. If a categorical quotient exists the scheme Y is denoted by X/G. In general such a quotient does not exist in the category of schemes. However the following theorem by P. Gabriel (see [7]) asserts the existence of a generic quotient, i.e. a G-invariant dense open subscheme U of X for which the quotient $U \to U/G$ exists.

Theorem 5.3. *Let G act freely on a S-scheme of finite type X such that the second projection $pr_2 : G \times_S X \to X$ is flat and of finite type. Then there exists a G-invariant dense open subscheme U of X satisfying the following properties:*

(i) There exists a quotient $\pi : U \to U/G$ in the category of schemes.

(ii) π is surjective and open, and U/G is of finite type over S.

(iii) $\pi : U \to U/G$ is a G-torsor.

Definition 5.4. *A G-invariant dense open subscheme U which satisfies the properties of the above theorem will be called a friendly open subscheme of X.*

Note that if G acts generically freely on X, then there exists a friendly open subscheme U of X on which G acts freely.

From now on we take $S = \mathrm{Spec}(F)$ where F is our base field, and take G to be a (linear) algebraic group over F, i.e. G is affine, smooth and of finite type over F. All morphisms between schemes will be of finite type. Let G_Y be the group scheme obtained from G by applying base change $Y \to \mathrm{Spec}(F)$. Then when $X \to Y$ is a G_Y-torsor, by abuse of language we will say that $X \to Y$ is a G-torsor.

Definition 5.5. *Let $f : X \to Y$ be a G-torsor. For any field extension K/F we define a map*

$$\partial : Y(K) \longrightarrow H^1(K, G)$$

as follows: For any $y \in Y(K)$, the fiber X_y of $f : X \to Y$ at y is a twisted form of G and is locally isomorphic to G for the flat topology. Hence X_y is smooth over K and it has a K_{sep}-rational point x. So $X_y(K_{sep})$ is non-empty and is a principal homogeneous space under $G(K_{sep})$. We then define $\partial(y)$ to be the isomorphism class of $X_y(K_{sep})$ in $H^1(K, G)$.

$\partial : Y(K) \to H^1(K,G)$ can also defined in terms of cocycles. Fix a point $y \in Y(K)$. For every $\gamma \in \Gamma_K = Gal(K_{sep}/K)$, and for every $x \in X_y(K_{sep})$,

$$f(\gamma \cdot x) = \gamma \cdot f(x) = \gamma \cdot y = y.$$

Therefore $\gamma \cdot x$ is also in $X_y(K_{sep})$. Since $f : X \to Y$ is a G-torsor, there exists a unique $g(\gamma) \in G(K_{sep})$ such that $\gamma \cdot x = x \cdot g(\gamma)$. The map $\gamma \to g(\gamma)$ is a 1-cocycle, and $\partial(y)$ is the class of this 1-cocycle in $H^1(K,G)$.

Proposition 5.6. *Let G be an algebraic group over F acting linearly and generically freely on an affine space $\mathbb{A}(V)$, where V is a finite dimensional vector space over F. Let U be a friendly open subscheme of $\mathbb{A}(V)$ on which G acts freely. Then U/G is a classifying scheme for $H^1(-,G)$, thus*

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

Proof. Let K/F be a field extension, and let $g \in Z^1(K,G)$ be a 1-cocycle. We twist the action of Γ_K on $V(K_{sep})$ by setting

$$\gamma * x = \gamma \cdot x \cdot g(\gamma)^{-1}$$

for every $\gamma \in \Gamma_K$ and $x \in V(K_{sep})$. Since G acts linearly on $\mathbb{A}(V)$, we see that $\gamma * (\lambda x) = \gamma(\lambda)(\gamma * x)$, thus our new action is Γ_K-semilinear. Thus $V(K_{sep})^{(\Gamma_K,*)}$ is Zariski-dense in $V(K_{sep})$, and this implies that $V(K_{sep})^{(\Gamma_K,*)}$ has a non-empty intersection with our friendly open subscheme U. Let $v \in U(K_{sep})$ be a $(\Gamma_K,*)$-invariant point. Then

$$v = \gamma * v = \gamma \cdot v \cdot g(\gamma)^{-1},$$

which implies $v \cdot g(\gamma) = \gamma \cdot v$. Let $\pi : U \to U/G$ be the morphism given by Theorem 5.3. It follows that

$$\gamma \cdot \pi(v) = \pi(\gamma \cdot v) = \pi(v \cdot g(\gamma)) = \pi(v),$$

and hence $\pi(v) \in U/G(K)$. By the discussion after Definition 5.5, $\partial(\pi(v))$ is just the class of g in $H^1(K,G)$. Therefore $\partial : U/G(K) \to H^1(K,G)$ is surjective for any field extension K/F. □

Remark 5.7. It is known that any algebraic group G acts linearly and generically freely on some finite dimensional vector space: First G is isomorphic to a closed subgroup of $\mathbf{GL}_n$ for some integer n, so we may assume $G \subseteq \mathbf{GL}_n$. Let $V = M_{n\times n}(F)$. Then G acts linearly on $\mathbb{A}(V)$ by right matrix multiplication. Let $U = \mathbf{GL}_n$ viewed as a G-invariant non-empty open subscheme of $\mathbb{A}(V)$. It can be checked that the action of G on U is free, hence G acts generically freely on $\mathbb{A}(V)$. By the previous proposition the essential dimension of G is finite.

Recall that an (affine) group scheme over F is called étale if its Hopf algebra is an étale F-algebra. For example, constant group schemes are étale. Note that by Cartier's Theorem, if $char(F) = 0$ then every finite group scheme is étale.

Proposition 5.8. *Let G be an étale group scheme over F, and let V be a finite dimensional F-vector space. Then*

(i) G acts linearly and generically freely on $\mathbb{A}(V)$ if and only if G is isomorphic to a closed subgroup of $\boldsymbol{GL}(V)$.

(ii) G acts linearly and generically freely on $\mathbb{P}(V)$ if and only if G is isomorphic to a closed subgroup of $\boldsymbol{PGL}(V)$.

Proof. We will only prove (ii) as (i) is similar. The "only if" part is easy to see, so it suffices to prove the "if" part. Suppose G is isomorphic to a closed subgroup of $\mathbf{PGL}(V)$, then clearly G acts linearly on $\mathbb{P}(V)$. So we only need to find an open subscheme U of $\mathbb{P}(V)$ on which G acts freely. First consider the action of $G(F_{sep})$ on $\mathbb{P}(V)(F_{sep})$. For every $g \in G(F_{sep})$, let S_g to be the linear subspace $\{x \in \mathbb{P}(V)(F_{sep}) : g \cdot x = x\}$. Then consider $S = \bigcup S_g \subseteq \mathbb{P}(V)(F_{sep})$, where the union is taken over all $g \in G(F_{sep})$. Since S is invariant under the action of the absolute Galois group Γ_F, by descent theory there exists a closed subscheme X of $\mathbb{P}(V)$ defined over F such that $X(F_{sep}) = S$. Note that G acts on X as $G(F_{sep})$ acts on $X(F_{sep}) = S$. Let $U = \mathbb{P}(V)\backslash X$. Then for every $x \in U$, by construction $G_x(F_{sep}) = 1$ where G_x is the stabilizer at x. As G is étale, G_x is also étale. Hence the fact that $G_x(F_{sep}) = 1$ implies G_x is trivial (this can be seen, for example, from the antiequivalence between the category of étale group schemes over F and the category of finite groups with continuous Γ_F-action). Since G_x is trivial for every $x \in U$, by [6, Chapter III.2 Corollary 2.3] G acts freely on U. $\square$

Proposition 5.9. *Let G be a finite abstract group, and let V be a finite dimensional F-vector space. Then G acts linearly and generically freely on $\mathbb{A}(V)$ if and only if G is isomorphic to a subgroup of $\boldsymbol{GL}(V)(F)$. In this case, we have*

$$\mathrm{ed}(G) \leq \dim(V).$$

Proof. Again the "only if" part is clear, so we only need to prove the "if" part. Suppose G is isomorphic to a subgroup of $\mathbf{GL}(V)(F)$, there exists an injective group homomorphism $\phi : G(F) \hookrightarrow \mathbf{GL}(V)(F)$, viewing G as a constant group scheme over F. Then it is known that ϕ can be extended uniquely into an injective group scheme morphism $\varphi : G \hookrightarrow \mathbf{GL}(V)$. Then the result follows immediately from Proposition 5.8 (i).

For the inequality $\mathrm{ed}(G) \leq \dim(V)$, we just need to apply Proposition 5.6 and note that $\dim(G) = 0$. $\square$

Let G be a finite abstract group, and let V be a finite dimensional F-vector space. Recall that a faithful (linear) representation of G on V is an injective homomorphism from G into $\mathbf{GL}(V)(F) = \mathrm{GL}(V)$. Therefore Proposition 5.9 shows that linear generically free actions of G on V corresponds to faithful representations of G on V.

Note that by applying Proposition 5.8 (ii) and the same proof for Proposition 5.9, we obtain the following result.

Proposition 5.10. *Let G be a finite abstract group, and let V be a finite dimensional F-vector space. Then G acts linearly and generically freely on $\mathbb{P}(V)$ if and only if G is isomorphic to a subgroup of $\boldsymbol{PGL}(V)(F)$.*

With Proposition 5.9 we are now able to compute the essential dimension of finite abelian groups over sufficiently large fields.

Corollary 5.11. *Let G be an abstract finite abelian group such that $char(F)$ does not divide $exp(G)$ the exponent of G. If F contains all the $exp(G)$-th roots of unity, then*

$$\mathrm{ed}(G) = rank(G).$$

Proof. By applying Proposition 4.6 it remains to prove that $\mathrm{ed}(G) \leq rank(G)$. Let $G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$, with $1 \neq n_1 \mid \cdots \mid n_r$, be the invariant factor decomposition of G. Let $\xi_{n_i} \in F$ be a primitive n_i-th root of unity. Then the following

$$\begin{aligned} \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z} &\longrightarrow \mathbf{GL}_r(F) \\ (\overline{m_1}, \ldots, \overline{m_r}) &\longmapsto \mathrm{Diag}(\xi_{n_1}^{m_1}, \ldots, \xi_{n_r}^{m_r}) \end{aligned}$$

is an injective group homomorphism, where $\mathrm{Diag}(a_1, \ldots, a_r)$ is the diagonal matrix with entries $a_1, \ldots, a_r$. Then the result follows from Proposition 5.9. $\square$

CHAPTER 6

Generic Torsors

Let G be an algebraic group over F. Recall that if G acts linearly and generically freely on a finite dimensional F-vector space V, then there exists a open subscheme U of $\mathbb{A}(V)$ such that $\pi : U \to U/G$ is a G-torsor. Let K/F be a field extension. In the proof of Proposition 5.6, we show that for every torsor $P \in H^1(K, G)$, there exists a non-empty subset S of U/G such that the isomorphism class of $\pi^{-1}(x)$ is equal to P for every $x \in S(K)$. If K is infinite then S is a Zariski-dense subset of Y.

Definition 6.1. *Let $f : X \to Y$ be a G-torsor with Y irreducible. We say that it is classifying for G if, for any field extension K/F with K infinite, and for any G-torsor $P \in H^1(K, G)$, the set of points $y \in Y(K)$ such that P is isomorphic to the fiber $f^{-1}(y)$ is dense in Y.*

Remark 6.2.

(1) If $f : X \to Y$ is a classifying G-torsor, then we have a surjection of functors $Y \to H^1(-, G)$. Hence Y is a classifying scheme for G, and $\mathrm{ed}(G) \leq \dim(Y)$.

(2) Let G be an algebraic group. Since G acts linearly and generically freely on some finite dimensional vector space, a classifying G-torsor $f : X \to Y$ always exists. Moreover we may assume that X and Y are reduced: Let $\phi : Y_{red} \to Y$ be the reduced scheme of Y with its canonical morphism. Then pulling back f along ϕ gives a torsor isomorphic to $X_{red} \to Y_{red}$ which is also classifying.

(3) The existence of a classifying G-torsor can also be proved as follows. First embed G into $\mathbf{GL}_n$ for some positive integer n, and we get an exact sequence of group schemes

$$1 \longrightarrow G \longrightarrow \mathbf{GL}_n \longrightarrow \mathbf{GL}_n/G \longrightarrow 1\ .$$

Then for every field extension K/F, there is an exact sequence of pointed sets

$$G(K) \longrightarrow \mathbf{GL}_n(K) \longrightarrow (\mathbf{GL}_n/G)(K) \xrightarrow{\partial} H^1(K,G) \longrightarrow 0$$

where we use the fact that $H^1(K, \mathbf{GL}_n) = 0$ by Hilbert's Theorem 90. The map $\partial : (\mathbf{GL}_n/G)(K) \to H^1(K,G)$ is given by taking the fiber of $\mathbf{GL}_n \to \mathbf{GL}_n/G$ at a K-rational point of $\mathbf{GL}_n/G$. We claim that $\mathbf{GL}_n \to \mathbf{GL}_n/G$ is a classifying G-torsor. Indeed the above exact sequence shows that any G-torsor $P \in H^1(K,G)$ is isomorphic to the fiber of a point $y \in (\mathbf{GL}_n/G)(K)$. Moreover, $y, y' \in (\mathbf{GL}_n/G)(K)$ are in the same $\mathbf{GL}_n(K)$-orbit if and only if $\partial(y) = \partial(y')$. If K is infinite, then $\mathbf{GL}_n(K)$ is dense in $\mathbf{GL}_n$ and hence the $\mathbf{GL}_n(K)$-orbit of y is also dense in $\mathbf{GL}_n/G$.

Definition 6.3. *Let $f : X \to Y$ be a classifying G-torsor. The generic fiber of f is called a generic torsor for G. If $P \to \mathrm{Spec}(F(Y))$ is a generic torsor for G, where $F(Y)$ is the function field of Y, then it can be viewed as an element of $H^1(F(Y), G)$.*

If $f : X \to Y$ is a classifying G-torsor, then for any non-empty open subset V of Y, $f : f^{-1}(V) \to V$ is also a classifying G-torsor. Therefore generic torsors for G correspond to the birational classes of classifying torsors for G.

Definition 6.4. *Let $f : X \to Y$ and $f' : X' \to Y'$ be G-torsors. We say that f' is a compression of f if there exists a diagram*

$$\begin{tikzcd} X \arrow[r, dashed, "g"] \arrow[d, "f"] & X' \arrow[d, "f'"] \\ Y \arrow[r, dashed, "h"] & Y' \end{tikzcd}$$

where g is a G-equivariant dominant rational morphism and h is a dominant rational morphism. The essential dimension of a G-torsor f, denoted by $\mathrm{ed}'(f)$, is the smallest dimension of Y' in a compression f' of f.

Remark 6.5. Take as above a compression of $f : X \to Y$. Let $U \subseteq Y$ be the largest domain of definition for h. Taking the pullback of $f' : X' \to Y'$ along $h : U \to Y'$ gives us a G-torsor which fits into the follow diagram

$$\begin{tikzcd} X \arrow[r, dashed] \arrow[d, "f"] & P \arrow[r] \arrow[d, "f''"] & X' \arrow[d, "f'"] \\ Y \arrow[r, dashed] & U \arrow[r] & Y', \end{tikzcd}$$

and we see that f'' is also a compression of f.

Next we are going to prove several results about compressions that we need in the sequel.

Lemma 6.6. *Let $f' : X' \to Y'$ be a compression of a classifying torsor $f : X \to Y$. Then f' is also a classifying torsor.*

Proof. Let

$$\begin{tikzcd} X \arrow[r, dashed, "g"] \arrow[d, "f"] & X' \arrow[d, "f'"] \\ Y \arrow[r, dashed, "h"] & Y' \end{tikzcd}$$

be such a compression. Let K/F be a field extension with K infinite, and $P \in H^1(K, G)$. Let $U \subseteq Y$ be the largest domain of definition for h. As f is classifying, the set $S = \{y \in Y(K) : P \cong f^{-1}(y)\}$ is dense in Y. The fact that h is dominant implies that $h(U \cap S)$ is dense in Y'. For every $y' \in h(U \cap S)$, it is clear that $f'^{-1}(y')$ is isomorphic to P. Therefore f' is also classifying. □

Lemma 6.7. *Let X and X' be schemes on which G acts generically freely, and let $g : X \dashrightarrow X'$ be a G-equivariant dominant rational morphism. Then there exists friendly open subschemes $U \subseteq X$ and $U' \subseteq X'$ such that g induces a compression of G-torsors*

$$\begin{tikzcd} U \arrow[r, dashed, "g"] \arrow[d] & U' \arrow[d] \\ U/G \arrow[r, dashed, "h"] & U'/G. \end{tikzcd}$$

Proof. Let V be a friendly open subscheme of X. By definition V is dense in X. Since g is dominant there is a non-empty open subscheme V' of X' lying inside $g(V)$. By intersecting V' with a friendly open subscheme of X' we obtain U' which is a friendly open subscheme inside $g(V)$. Take $U = g^{-1}(U')$. The following diagram

$$\begin{tikzcd}
& G \times U \arrow[rr] \arrow[dl, "(id_G{,}g)"'] \arrow[dd, "pr_2"] & & U \arrow[dl, "g"'] \arrow[dd] \\
G \times U' \arrow[rr, crossing over] \arrow[dd, "pr_2"] & & U' & \\
& U \arrow[rr] \arrow[dl, "g"] & & U/G \\
U' \arrow[rr] & & U'/G \arrow[from=uu, crossing over] &
\end{tikzcd}$$

is commutative, where the commutativity of the top square follows from the fact that g is G-equivariant. This diagram then induces the desired morphism h by the universal property of pushout. $\square$

Lemma 6.8. *Let $f : X \to Y$ be a G-torsor with Y integral. Let $P \to \mathrm{Spec}(F(Y))$ be the generic fiber of f, with P viewed as element of $H^1(F(Y), G)$. Then*

$$\mathrm{ed}'(f) = \mathrm{ed}(P).$$

Proof. Let $f' : X' \to Y'$ be a compression of f such that Y' is integral and $\dim(Y') = \mathrm{ed}'(f)$, and let $P' \to \mathrm{Spec}(F(Y'))$ be its generic fiber. Consider the G-torsor f'' in Remark 6.5. Since the generic fiber of f is isomorphic to the generic fiber of f'', and f' is a compression of f'', by replacing f with f'' we may assume the compression is a pullback. The diagram

$$\begin{tikzcd}
& P \arrow[rr] \arrow[dl] \arrow[dd] & & X \arrow[dl] \arrow[dd] \\
P' \arrow[rr, crossing over] \arrow[dd] & & X' & \\
& \mathrm{Spec}(F(Y)) \arrow[rr] \arrow[dl] & & Y \arrow[dl] \\
\mathrm{Spec}(F(Y')) \arrow[rr] & & Y' \arrow[from=uu, crossing over] &
\end{tikzcd}$$

then shows that P' maps to P under $H^1(F(Y'), G) \to H^1(F(Y), G)$. Therefore

$$\mathrm{ed}(P) \leq tr.deg_F(F(Y')) = \dim(Y') = \mathrm{ed}'(f).$$

For the other inequality, suppose there is a subextension $F \subseteq K \subseteq F(Y)$ such that P is the image of some P' under $H^1(K, G) \to H^1(F(Y), G)$. Our goal is to find a G-torsor $f' : X' \to Y'$ such that f' is a compression of f, and the generic fiber of f' is isomorphic to $P' \to \mathrm{Spec}(K)$.

First we may assume that all the schemes are affine: Note that the generic point of Y lies in some open affine subscheme U of Y, and $P \to \mathrm{Spec}(K)$ is also the generic fiber of $f^{-1}(U) \to U$. Then let $Y = \mathrm{Spec}(A), X = \mathrm{Spec}(B), P = \mathrm{Spec}(R)$ and $P' = \mathrm{Spec}(R')$. Then A is an integral domain, $F(Y)$ is the quotient field of A, $R = B \otimes_A F(Y)$ and $R \cong R' \otimes_K F(Y)$. Since $F(Y)$ is of finite type over F, $F(Y) = F(a_1, \ldots, a_n)$ for some elements $a_1, \ldots, a_n$, and we will just use the shorthand notation $F(a)$. Similarly, R is of finite type over $F(Y)$ and we write $R = F(Y)[b]$. In the same way we have $K = F(a')$ and $R' = K[b']$.

Let $F[G]$ be the algebra of G. Since $P' \to \mathrm{Spec}(K)$ is a G-torsor, we have the following isomorphisms

$$P' \times_{\mathrm{Spec}(K)} P' \cong G_{\mathrm{Spec}(K)} \times_{\mathrm{Spec}(K)} P' \cong G \times_{\mathrm{Spec}(F)} P',$$

which corresponds to $R' \otimes_K R' \cong F[G] \otimes_F R'$. Note that since $R' \otimes_K R'$ and $F[G] \otimes_F R'$ are finitely generated algebra over $K = F(a')$, there is a polynomial ρ in the a'_i such that $(F[a']_\rho)[b'] \otimes_{F[a']_\rho} (F[a']_\rho)[b'] \cong F[G] \otimes_F (F[a']_\rho)[b']$. Such an ρ exists because there are only finitely many elements we need to invert in order to define the isomorphism. Let $A' = F[a']_\rho$ and $B' = (F[a']_\rho)[b']$. Then by construction $f' : \mathrm{Spec}(B') \to \mathrm{Spec}(A')$ is a G-torsor. We also note that $R' = K[b'] \cong B' \otimes_{A'} K$, and hence the generic fiber of f' is isomorphic to $P' \to \mathrm{Spec}(K)$.

It remains to show that f' is a compression of f. Consider the image of A' under the composition $A' \hookrightarrow K \hookrightarrow F(Y)$. We see that the image of A' lies inside a subring of the form $F[a]_\phi$ for some polynomial ϕ in the a_i, as we only need to invert the polynomials appearing in the image of a_i which are finitely many. Since $A = F[a]_\psi$ for some ψ, there is a natural homomorphism

$$A' \longrightarrow F[a]_\phi \longrightarrow (F[a]_\phi)_\psi = A_\phi,$$

which corresponds to a rational morphism $\mathrm{Spec}(A) \dashrightarrow \mathrm{Spec}(A')$. By the same argument there is a rational morphism $\mathrm{Spec}(B) \dashrightarrow \mathrm{Spec}(B')$ compatible with the previous one, and it gives the desired compression. As a result we have $\mathrm{ed}'(f) \leq \mathrm{ed}(P)$. $\square$

Remark 6.9. The hypothesis that Y is reduced can be dropped by replacing A with $A/nil(A)$ in the proof. We do not need this result in full generality because reduced classifying torsors always exist by Remark 6.2.

Corollary 6.10. *Let $P \to \mathrm{Spec}(K)$ be a generic G-torsor. Let $K_0 \subseteq K$ be a subextension, and $T \to \mathrm{Spec}(K_0)$ be a G-torsor such that $T_K = P$. Then $T \to \mathrm{Spec}(K_0)$ is also a generic G-torsor.*

Proof. Let $f : X \to Y$ be a classifying G-torsor such that its generic fiber is $P \to \mathrm{Spec}(K)$. By the proof of Lemma 6.8, there exists a G-torsor $f' : X' \to Y'$ such that f' is a compression of f, and the generic fiber of f' is isomorphic to $T \to \mathrm{Spec}(K_0)$. Note that f' is a classifying G-torsor by Lemma 6.6, thus $T \to \mathrm{Spec}(K_0)$ is generic. $\square$

Theorem 6.11. *Let G be an algebraic group over F, and let $P \to \mathrm{Spec}(K)$ be a generic G-torsor. Then*

$$\mathrm{ed}(G) = \mathrm{ed}(P).$$

Proof. It is clear from definition that $\mathrm{ed}(G) \geq \mathrm{ed}(P)$, so it remains to prove the other inequality. First, there is a subextension $F \subseteq K_0 \subseteq K$ such that $tr.deg_F(K_0) = \mathrm{ed}(P)$ and $P = Q_K$ for some $Q \in H^1(K_0, G)$. By Corollary 6.10 $Q \to \mathrm{Spec}(K_0)$ is also a generic torsor. Hence by replacing $P \to \mathrm{Spec}(K)$ with $Q \to \mathrm{Spec}(K_0)$ we may assume $\mathrm{ed}(P) = tr.deg_F(K)$.

Let L/F be a field extension and $T \in H^1(L, G)$. Let $f : X \to Y$ be a classifying G-torsor such that its generic fiber is $P \to \mathrm{Spec}(K)$. Then by the definition of a classifying torsor, there exists a L-rational point $y : \mathrm{Spec}(L) \to Y$ such that $T \to \mathrm{Spec}(L)$ fits into a pullback diagram

$$\begin{tikzcd} T \arrow[r] \arrow[d] & X \arrow[d, "f"] \\ \mathrm{Spec}(L) \arrow[r] & Y. \end{tikzcd}$$

Let $F(y)$ be the residue field at the point $y \in Y$. Then $y : \mathrm{Spec}(L) \to Y$ factors through $\mathrm{Spec}(F(y))$. If we denote by $T' \to \mathrm{Spec}(F(y))$ the G-torsor obtained by pulling back f along the canonical morphism $\mathrm{Spec}(F(y)) \to Y$, we get the following diagram

$$\begin{tikzcd}
T \arrow[r] \arrow[d] & T' \arrow[r] \arrow[d] & X \arrow[d, "f"] \\
\mathrm{Spec}(L) \arrow[r] & \mathrm{Spec}(F(y)) \arrow[r] & Y.
\end{tikzcd}$$

Therefore $T = T'_L$ and this implies

$$\mathrm{ed}(T) \leq tr.deg_F(F(y)) \leq tr.deg_F(K) = \mathrm{ed}(P).$$

Since $\mathrm{ed}(T) \leq \mathrm{ed}(P)$ for every $T \in H^1(L, G)$ and every field extensions L/F, we have $\mathrm{ed}(G) \leq \mathrm{ed}(P)$. □

Remark 6.12.

(1) Recall that $\mathrm{ed}(G) = \max\{\mathrm{ed}(T)\}$ where the maximum is taken over all $T \in H^1(L, G)$ and all field extensions L/F. Theorem 6.11 then says that the maximum is attained at any generic G-torsor.

(2) Theorem 6.11 also allows us to understand the essential dimension of an algebraic group G from a geometric point of view. By Lemma 6.8 and Theorem 6.11 we have $\mathrm{ed}(G) = \mathrm{ed}'(f)$ for any classifying G-torsor $f : X \to Y$. Since a compression of a classifying torsor is also a classifying torsor by Lemma 6.6, we obtain

$$\mathrm{ed}(G) = \min\{\dim(Y)\}$$

where the minimum is taken over all classifying G-torsors $X \to Y$.

(3) Let $f : X \to Y$ be a classifying G-torsor. If $f' : X' \to Y'$ is a compression of f, then it is clear that $X \dashrightarrow X'$ is a G-equivariant dominant rational morphism between generically free G-schemes, i.e. schemes on which G acts generically freely. Conversely, any such morphism between generically free G-schemes induces a compression by Lemma 6.7.

Let $d = \min\{\dim(X')\}$ where the minimum is taken over all generically free G-scheme X' such that there exists a G-equivariant dominant rational morphism $X \dashrightarrow X'$. Then

$$\mathrm{ed}(G) = \mathrm{ed}'(f) = d - \dim(G).$$

Proposition 6.13. *Let G be an algebraic group over F acting linearly and generically freely on $\mathbb{A}(V)$, where V is a finite dimensional vector space over F. Supposed the induced G-action on $\mathbb{P}(V)$ is also generically free. Then*

$$\mathrm{ed}(G) \leq \dim(V) - \dim(G) - 1.$$

Proof. The canonical morphism $\mathbb{A}(V)\backslash\{0\} \to \mathbb{P}(V)$ gives a G-equivariant dominant rational morphism $\mathbb{A}(V) \dashrightarrow \mathbb{P}(V)$. The result then follows from the above remark. $\square$

Corollary 6.14. *Let G be a finite abstract group, and let $n \geq 2$ be an integer. Suppose there exists an injective homomorphism $\phi : G \to \boldsymbol{GL}_n(F)$ such that $\pi \circ \phi$ remains injective, where $\phi : \boldsymbol{GL}_n(F) \to \boldsymbol{PGL}_n(F)$ is the canonical projection. Then*

$$\mathrm{ed}(G) \leq n - 1.$$

Proof. By Proposition 5.9 and 5.10, G acts linearly and generically freely on both $\mathbb{A}^n$ and $\mathbb{P}^{n-1}$. Therefore $\mathrm{ed}(G) \leq n-1$ from the above result. $\square$

We can study the behavior of the essential dimension of G with respect to closed subgroups by means of compressions of torsors.

Theorem 6.15. *Let G be an algebraic group and H a closed algebraic subgroup of G. Then*

$$\mathrm{ed}(H) + \dim(H) \leq \mathrm{ed}(G) + \dim(G).$$

In particular, if G is finite, then

$$\mathrm{ed}(H) \leq \mathrm{ed}(G).$$

Proof. Let $\mathbb{A}(V)$ be an affine space on which G (and hence H also) acts linearly and generically freely. Let $U_G, U_H \subseteq \mathbb{A}(V)$ be friendly open subschemes for the actions of G and H

respectively. Take $U = U_G \cap U_H$, then $\pi_G : U \to U/G$ and $\pi_H : U \to U/H$ are classifying torsors. Let

$$\begin{tikzcd} U \arrow[r, dashed, "g"] \arrow[d, "\pi_G"'] & X \arrow[d] \\ U/G \arrow[r, dashed] & Y \end{tikzcd}$$

be a compression of G-torsors such that $\dim(Y) = \mathrm{ed}'(\pi_G) = \mathrm{ed}(G)$. Note that H acts generically freely on both U and X, and g is H-invariant. Hence by Lemma 6.7, g induces a compression of H-torsors of π_H. Therefore

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

□

Remark 6.16. Notice that if G is not finite, then $\mathrm{ed}(H) \leq \mathrm{ed}(G)$ does not necessarily hold. For example, consider $G = \mathbb{G}_m$ and $H = \mu_n$ for some n coprime to $char(F)$. We have

$$1 = \mathrm{ed}(\mu_n) > \mathrm{ed}(\mathbb{G}_m) = 0.$$

Corollary 6.17. *If $char(F) \neq 2$, then*

$$\mathrm{ed}(S_n) \geq \lfloor \frac{n}{2} \rfloor$$

where $\lfloor - \rfloor$ is the greatest integer function.

Proof. Let $H = \mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}$ ($\lfloor \frac{n}{2} \rfloor$ copies). Then H is a subgroup of S_n. By Theorem 6.15 and Corollary 5.11 it follows that

$$\mathrm{ed}(S_n) \geq \mathrm{ed}(H) = \lfloor \frac{n}{2} \rfloor.$$

□

CHAPTER 7

Essential Dimension of Cyclic Groups

In this chapter G will always be a finite abstract group.

Let p be a prime number, and let F be a field such that $char(F) \neq p$, and F contains a primitive p-th root of unity ξ_p. The essential dimension of cyclic p-groups over F is computed by M. Florence in [9], and by N. A. Karpenko and A. S. Merkurjev in [15]. In fact, the result in [15] computes the essential dimension of arbitrary p-groups, not just cyclic ones:

Theorem 7.1. *Let G be a p-group, and F be a field containing a primitive p-th root of unity. Then*

$$\mathrm{ed}(G) = \min\{\dim(\phi)\}$$

where the minimum is taken over all faithful representations ϕ of G over F.

Corollary 7.2. *Let F be a field containing a primitive p-th root of unity. Then*

$$\mathrm{ed}(\mathbb{Z}/p^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n_r}\mathbb{Z}) = [F(\xi_{p^{n_1}}) : F] + \cdots + [F(\xi_{p^{n_r}}) : F].$$

Our goal is to study the essential dimension of cyclic groups G of arbitrary order $|G|$, over a field F containing a primitive p-th root of unity for every prime divisor p of $|G|$.

First we are going to fix the notations.

Fix a prime number p. Let F be a field that $char(F) \neq p$ and F contains a primitive p-th root of unity ξ_p. As before we denote the absolute Galois group $Gal(F_{sep}/F)$ of F by $\Gamma_F = \Gamma$.

For any non-negative integer r, let $G_r = \mathbb{Z}/p^r\mathbb{Z}$ viewed as a constant group scheme over F, F_r be the field extension $F(\xi_{p^r})$ of F and Γ_r be the corresponding Galois group

$Gal(F_r/F)$. The corestriction $R_{F_r/F}(\mathbb{G}_m)$ of $\mathbb{G}_m$ from F_r to F will be denoted by T_r. Notice that G_r is a group scheme of multiplicative type since $G_{r,sep}$ $(= (G_r)_{F_{sep}})$ is isomorphic to μ_{p^r}, and T_r is a quasi-split torus with dimension $\dim(T_r) = [F_r : F]$.

For any $\gamma \in \Gamma_r$, it is clear that $\gamma(\xi_{p^r})$ has the same order as ξ_{p^r}, hence $\gamma(\xi_{p^r})$ is also a primitive p^r-th root of unity and $\gamma(\xi_{p^r}) = \xi_{p^r}^{\chi_r(\gamma)}$ for some $\chi_r(\gamma) \in (\mathbb{Z}/p^r\mathbb{Z})^\times$. Then we get a homomorphism $\chi_r : \Gamma_r \to (\mathbb{Z}/p^r\mathbb{Z})^\times$. By extending χ_r linearly we obtain a surjective Γ-homomorphism $f_r : (T_{r,sep})^* = \mathbb{Z}[\Gamma_r] \to \mathbb{Z}/p^r\mathbb{Z} = (G_{r,sep})^*$,

$$f_r(\sum a_\gamma \gamma) = \sum \overline{a_\gamma}\chi_r(\gamma).$$

Now fix a positive integer n, and let $s = \min\{n,\ \sup\{m \in \mathbb{N} | \ \xi_{p^m} \in F\}\}$. It follows from the definition of s that G_s is the largest subgroup of G_n such that G_s is isomorphic to μ_{p^s}. Define a surjective Γ-homomorphism $g : \mathbb{Z}[\Gamma_{n-s}] \oplus \mathbb{Z}[\Gamma_n] \to \mathbb{Z}/p^n\mathbb{Z}$ by

$$g(x, y) = (\iota \circ f_{n-s})(x) + f_n(y)$$

for every $(x, y) \in \mathbb{Z}[\Gamma_{n-s}] \oplus \mathbb{Z}[\Gamma_n]$, where $\iota : \mathbb{Z}/p^{n-s}\mathbb{Z} \hookrightarrow \mathbb{Z}/p^n\mathbb{Z}$ is the canonical inclusion taking $\overline{1}$ to $\overline{p^s}$. Then g corresponds to an injective homomorphism from G_n to $T_{n-s} \times T_n$. We have the following short exact sequence

$$1 \longrightarrow G_n \longrightarrow T_{n-s} \times T_n \longrightarrow V \longrightarrow 1$$

where $V = (T_{n-s} \times T_n)/G_n$ is the factor torus with $(V_{sep})^* = \ker(g)$. Let K/F be a field extension. By passing to cohomology we get

$$V(K) \xrightarrow{\partial_K} H^1(K, G_n) \longrightarrow 0$$

where the last term follows from $H^1(K, T_{n-s} \times T_n) = 0$ by Shapiro's Lemma and Hilbert's Theorem 90. Let $\pi_K : H^1(K, G_n) \to H^1(K, G_{n-s})$ be the canonical homomorphism induced by the exact sequence

$$1 \longrightarrow G_s \longrightarrow G_n \longrightarrow G_{n-s} \longrightarrow 1\ .$$

By setting $\mathfrak{F}(K) = (\pi_K \circ \partial_K)(V(K))$ we obtain a subfunctor $\mathfrak{F}$ of $H^1(-, G_{n-s})$. Notice that $\mathfrak{F}(K) = \pi_K(H^1(K, G_n))$ because ∂_K is surjective.

Proposition 7.3. *There exists a closed subscheme $Y \subseteq V$ of dimension $[F_n : F] - 1$ such that for every infinite $K \in Fields/F$, the image $(\pi_K \circ \partial_K)(Y(K))$ of $Y(K)$ in $H^1(K, G_{n-s})$ is equal to $\mathfrak{F}(K)$.*

Proof. If $n = s$, the result follows immediately from the fact that $H^1(K, G_{n-s}) = 0$ and $[F_n : F] = 1$. For the case $n > s$, we first consider the following commutative diagram of Γ-modules

$$\begin{tikzcd}
\mathbb{Z}/p^s\mathbb{Z} & \mathbb{Z}/p^n\mathbb{Z} \arrow[l, "\rho"'] & \mathbb{Z}/p^{n-s}\mathbb{Z} \arrow[l, "\iota"'] \\
\mathbb{Z}[\Gamma_n] \arrow[u, "\rho\circ f_n"] & \mathbb{Z}[\Gamma_{n-s}] \oplus \mathbb{Z}[\Gamma_n] \arrow[l, "pr_2"'] \arrow[u, "g"] & \mathbb{Z}[\Gamma_{n-s}] \arrow[l, "i_1"'] \arrow[u, "f_{n-s}"] \\
\ker(\rho \circ f_n) \arrow[u] & \ker(g) \arrow[l, "pr_2"'] \arrow[u] & \ker(f_{n-s}) \arrow[l, "i_1"'] \arrow[u]
\end{tikzcd} \tag{7.1}$$

where ρ is the canonical projection, i_1 is the inclusion into the first component, and pr_2 is the projection onto the second component. Note the all the rows and columns in (7.1) are short exact sequences. Then by setting $U = T_n/G_s$ and $S = T_{n-s}/G_{n-s}$, with $(U_{sep})^* = \ker(\rho \circ f_n)$ and $(S_{sep})^* = \ker(f_{n-s})$, we have the following commutative diagram of group schemes dual to (7.1)

$$\begin{tikzcd}
G_s \arrow[r] \arrow[d] & G_n \arrow[r] \arrow[d] & G_{n-s} \arrow[d] \\
T_n \arrow[r] \arrow[d] & T_{n-s} \times T_n \arrow[r] \arrow[d] & T_{n-s} \arrow[d] \\
U \arrow[r] & V \arrow[r] & S.
\end{tikzcd}$$

Therefore for every field extension K/F,

$$\begin{tikzcd}
T_{n-s}(K) \times T_n(K) \arrow[r] \arrow[d] & T_{n-s}(K) \arrow[d] \\
V(K) \arrow[r] \arrow[d, two heads, "\partial_K"'] & S(K) \arrow[d, two heads] \\
H^1(K, G_n) \arrow[r, "\pi_K"] & H^1(K, G_{n-s})
\end{tikzcd} \tag{7.2}$$

is commutative.

In order to construct Y, we consider one more diagram

$$\begin{tikzcd} \mathbb{Z}[\Gamma_{n-s}] \oplus \mathbb{Z} & \mathbb{Z}[\Gamma_{n-s}] \arrow[l, hook', "i_1"'] \\ \ker(g) \arrow[u, "\varphi"] & \ker(f_{n-s}) \arrow[l, hook', "i_1"] \arrow[u] \end{tikzcd} \tag{7.3}$$

where φ is defined by $\varphi(x,y) = (x, \epsilon(y)/p^s)$ for every $(x,y) \in \ker(g) \subseteq \mathbb{Z}[\Gamma_{n-s}] \oplus \mathbb{Z}[\Gamma_n]$, with ϵ being the augmentation homomorphism of a group ring.

Lemma 7.4. *$\varphi : \ker(g) \to \mathbb{Z}[\Gamma_{n-s}] \oplus \mathbb{Z}$ is well-defined and surjective.*

Proof. Let (x,y) be any element in $\ker(g)$. To prove that φ is well-defined it suffices to show that $\epsilon(y)$ is a multiple of p^s.

1. For $p \neq 2$, and for $p = 2$ and $s \geq 2$, Γ_n is a cyclic group. Let σ be the generator of Γ_n such that $\sigma(\xi_{p^n}) = \xi_{p^n}^{p^s+1}$. Then we can write $y = \sum a_m \sigma^m$, and it follows that $f_n(y) = \sum a_m (p^s+1)^m \pmod{p^n}$. Notice that $(x,y) \in \ker(g)$ implies

$$g(x,y) = p^s \cdot f_{n-s}(x) + \sum a_m (p^s+1)^m = 0 \pmod{p^n}.$$

   Therefore p^s divides $\sum a_m = \epsilon(y)$.

2. For $p = 2$ and $s = 1$, write $y = \sum a_\gamma \gamma$. Just like the previous case, we have

$$g(x,y) = 2f_{n-1}(x) + \sum a_\gamma \chi_n(\gamma) = 0 \pmod 2$$

   as $(x,y) \in \ker(g)$. Note that $\chi_n(\gamma) \in (\mathbb{Z}/2^n\mathbb{Z})^\times$ for every γ, in particular $\chi_n(\gamma)$ is odd. Then it is clear that $\sum a_\gamma = \epsilon(y)$ is even.

Therefore φ is well-defined.

Claim: If $\epsilon/p^s : \ker(f_n) \to \mathbb{Z}$ is surjective, then φ is surjective.

First notice that for every $y \in \ker(f_n)$, $(0,y) \in \ker(g)$. Therefore $\epsilon/p^s : \ker(f_n) \to \mathbb{Z}$ is well-defined by the proof above.

To prove the claim let (x,m) be an arbitrary element in $\mathbb{Z}[\Gamma_{n-s}] \oplus \mathbb{Z}$. Recall that $f_n : \mathbb{Z}[\Gamma_n] \to \mathbb{Z}/p^n\mathbb{Z}$ is surjective. Then there is an element $y \in \mathbb{Z}[\Gamma_n]$ such that

$f_n(y) = -(\iota \circ f_{n-s})(x)$, which implies $(x,y) \in \ker(g)$. Let $m' = \epsilon(y)/p^s \in \mathbb{Z}$. Suppose $\epsilon/p^s : \ker(f_n) \to \mathbb{Z}$ is surjective. There exists $y' \in \ker(f_n)$ such that $\epsilon(y')/p^s = 1$. Then $(x, y+(m-m')y') = (x,y) + (0,(m-m')y') \in \ker(g)$ as both (x,y) and $(0,(m-m')y')$ are in $\ker(g)$. It is easy to see that $\varphi(x, y+(m-m')y') = (x,m)$, proving the claim.

Now we are going to show that $\epsilon/p^s : \ker(f_n) \to \mathbb{Z}$ is surjective.

1. For $p \neq 2$, and for $p = 2$ and $s \geq 2$, simply note that $\sigma - p^s - 1 \in \ker(f_n)$, which we recall that σ is the generator of Γ_n satisfying $\sigma(\xi_{p^n}) = \xi_{p^n}^{p^s+1}$.

2. For $p = 2$ and $s = 1$, consider $\mathrm{im}(\chi_n) \subseteq (\mathbb{Z}/2^n\mathbb{Z})^\times$. First we recall from group theory that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is a direct product of two cyclic subgroups generated by $\overline{5}$ and $\overline{-1}$ respectively. We claim that $\overline{-5}^r \in \mathrm{im}(\chi_n)$ for some integer r. Suppose not, then all elements of $\mathrm{im}(\chi_n)$ are powers of $\overline{5}$, which implies Γ_n fixes $\xi_4 = \xi_{2^n}^{2^{n-2}}$. This contradicts the fact that $\xi_4 \notin F$ as $s = 1$.

   Let $\gamma \in \Gamma_n$ be an element satisfying $\chi_n(\gamma) = \overline{-5}^r$. Since $\gamma + 5^r$ and $2^n \in \ker(f_n)$, we have $(1+5^r)/2$ and $2^{n-1} \in \mathrm{im}(\epsilon/2)$. As $5^r = 1 \pmod 4$, $(1+5^r)/2$ is odd. Hence $(1+5^r)/2$ and 2^{n-1} are coprime and it follows immediately that $\mathrm{im}(\epsilon/2) = \mathbb{Z}$. $\square$

Back to the proof of the proposition. It is clear that the diagram (7.3) is commutative, so we have the dual commutative digram of group schemes

$$\begin{tikzcd} T_{n-s} \times \mathbb{G}_m \arrow[r] \arrow[d, hook] & T_{n-s} \arrow[d] \\ V \arrow[r] \arrow[d, two heads, "pr"] & S \\ V' & \end{tikzcd} \tag{7.4}$$

where $V' = V/(T_{n-s} \times \mathbb{G}_m)$. Notice that V' is a torus because V is a torus. Let E be the function field $F(V')$ of V'. From the exact sequence of cohomology

$$V(E) \longrightarrow V'(E) \longrightarrow H^1(E, T_{n-s} \times \mathbb{G}_m) = 0$$

we see that the generic point of V', $\mathrm{Spec}(E) \to V'$ factors through V. Therefore there exists a rational map $\alpha : V' \dashrightarrow V$ such that the composition with the projection pr is the identity map on the largest domain of definition $U \subseteq V'$ for α. We define Y to be $\overline{\mathrm{im}(\alpha)}$ the closure of the image of α. Since V' is a torus, it is irreducible and this implies U is a dense open subset of V'. Therefore

$$\begin{aligned}
\dim(Y) = \dim(U) &= \dim(V') \\
&= \dim(V) - \dim(T_{n-s} \times \mathbb{G}_m) \\
&= \dim((T_{n-s} \times T_n)/G_n) - \dim(T_{n-s} \times \mathbb{G}_m) \\
&= [F_n : F] - 1.
\end{aligned}$$

Notice that the first equality follows from the fact that α is injective. Now it remains to verify that for every field extension K/F with K infinite, the images of $Y(K)$ and $V(K)$ under $\pi_K \circ \partial_K$ in $H^1(K, G_{n-s})$ are equal.

Lemma 7.5. *Let K/F be a field extension with K infinite. For every $v \in V(K)$, there exists $u \in Y(K)$ such that $(\pi_K \circ \partial_K)(v) = (\pi_K \circ \partial_K)(u)$.*

Proof. First, since $T_{n-s} \times T_n$ is a torus and K is infinite, the set of K-rational points $T_{n-s}(K) \times T_n(K)$ is a dense subset of $T_{n-s} \times T_n$. Recall that we have a surjective morphism $\psi : T_{n-s} \times T_n \to V$, so the image $\psi_K(T_{n-s}(K) \times T_n(K))$ is dense in V. Let $v \in V(K)$ be an arbitrary K-rational point of V. The orbit $\psi_K(T_{n-s}(K) \times T_n(K)) \cdot v$ of v is also dense in V. Consider the largest domain of definition $U \subseteq V'$ for α. As U is a open subset of V', $pr^{-1}(U)$ is an open subset of V and hence its intersection with $\psi_K(T_{n-s}(K) \times T_n(K)) \cdot v$ is non-empty. This means that there exists $v' \in \psi_K(T_{n-s}(K) \times T_n(K))$ such that $pr(v' \cdot v) \in U(K)$. By diagram (7.2) $\partial_K(v)$ is equal to $\partial_K(v' \cdot v)$, therefore by replacing v by $v' \cdot v$ we may assume $pr(v) \in U(K)$.

Let $u = (\alpha \circ pr)(v) \in Y(K)$. As $pr(u) = pr(v)$, by diagram (7.4) u and v differ by an element in $T_{n-s}(K) \times \mathbb{G}_m(K)$. Then by commutativity of diagram (7.4) the images of u and v in $S(K)$ differ by the image of an element in $T_{n-s}(K)$. It follows directly from diagram (7.2) that $(\pi_K \circ \partial_K)(v) = (\pi_K \circ \partial_K)(u)$ in $H^1(K, G_{n-s})$. □

This completes the proof of the proposition. □

Corollary 7.6. $\mathrm{ed}(\mathfrak{F}) \leq \mathrm{ed}(\mathbb{Z}/p^n\mathbb{Z}) - 1$.

Proof. We first show that $\mathrm{ed}(\mathfrak{F}) \leq \mathrm{ed}(Y)$. Let K/F be a field extension and $a \in \mathfrak{F}(K)$. If K is a finite field, then clearly $tr.deg_F(K) = 0$ and $\mathrm{ed}(a) = 0 \leq \mathrm{ed}(Y)$. If K is infinite, by Proposition 7.3 we have a surjection $Y(K) \to \mathfrak{F}(K)$. Then $\mathrm{ed}(a) \leq \mathrm{ed}(Y)$ by the proof of Lemma 2.5.

It follows from Proposition 2.12 and Corollary 7.2 that

$$\mathrm{ed}(\mathfrak{F}) \leq \mathrm{ed}(Y) = \dim(Y) = [F_n : F] - 1 = \mathrm{ed}(\mathbb{Z}/p^n\mathbb{Z}) - 1. \qquad \square$$

Now we are ready to prove our main theorem.

Theorem 7.7. *Let $p_1, \ldots, p_r$ be distinct prime numbers, $n_1, \ldots, n_r$ be positive integers. Let F be a field such that $char(F) \neq p_i$ and $\xi_{p_i} \in F$ for every i. Then*

$$\begin{aligned}\mathrm{ed}(\mathbb{Z}/p_1^{n_1} \cdots p_r^{n_r}\mathbb{Z}) &\leq \mathrm{ed}(\mathbb{Z}/p_1^{n_1}\mathbb{Z}) + \cdots + \mathrm{ed}(\mathbb{Z}/p_r^{n_r}\mathbb{Z}) - r + 1 \\ &= [F(\xi_{p_1^{n_1}}) : F] + \cdots + [F(\xi_{p_r^{n_r}}) : F] - r + 1.\end{aligned}$$

Proof. Let $s_i = \min\{n_i,\ \sup\{m \in \mathbb{N} |\ \xi_{p_i^m} \in F\}\}$ for every i. For each prime number p_i, let $\mathfrak{F}_i$ be the corresponding $\mathfrak{F}$ defined above. We write $C_N = \mathbb{Z}/p_1^{n_1} \cdots p_r^{n_r}\mathbb{Z}$, $C_S = \mathbb{Z}/p_1^{s_1} \cdots p_r^{s_r}\mathbb{Z}$ and $C_{N-S} = \mathbb{Z}/p_1^{n_1-s_1} \cdots p_r^{n_r-s_r}\mathbb{Z}$. The exact sequence of group schemes

$$1 \longrightarrow C_S \longrightarrow C_N \longrightarrow C_{N-S} \longrightarrow 1$$

induces an exact sequence in cohomology

$$H^1(K, C_S) \longrightarrow H^1(K, C_N) \longrightarrow H^1(K, C_{N-S}) \tag{7.5}$$

for every field extension K/F. Notice that

$$H^1(K, C_N) = H^1(K, \mathbb{Z}/p_1^{n_1}\mathbb{Z}) \times \cdots \times H^1(K, \mathbb{Z}/p_r^{n_r}\mathbb{Z}),$$

and similarly

$$H^1(K, C_{N-S}) = H^1(K, \mathbb{Z}/p_1^{n_1-s_1}\mathbb{Z}) \times \cdots \times H^1(K, \mathbb{Z}/p_r^{n_r-s_r}\mathbb{Z}).$$

Recall from the construction of $\mathfrak{F}_i$ that $\mathfrak{F}_i(K)$ is equal to $\pi_{i,K}(H^1(K, \mathbb{Z}/p_i^{n_i}\mathbb{Z}))$, where $\pi_{i,K} : H^1(K, \mathbb{Z}/p_i^{n_i}\mathbb{Z}) \to H^1(K, \mathbb{Z}/p_i^{n_i - s_i}\mathbb{Z})$ is the canonical homomorphism. Then it follows from the exact sequence (7.5) that $H^1(-, C_S)$ is in fibration position (Definition 2.9) for the surjection of functors $H^1(-, C_N) \to \mathfrak{F}_1 \times \cdots \times \mathfrak{F}_r$. Hence by Proposition 2.10

$$\mathrm{ed}(C_N) \leq \mathrm{ed}(C_S) + \mathrm{ed}(\mathfrak{F}_1 \times \cdots \times \mathfrak{F}_r).$$

Notice that $\xi_{p_i^{s_i}} \in F$ by definition of s_i, therefore C_S (viewed as a constant group scheme over F) is isomorphic to $\mu_{p_1^{s_1} \cdots p_r^{s_r}}$. As a result, $\mathrm{ed}(C_S) = 1$. It follows that

$$\begin{aligned}
\mathrm{ed}(C_N) &\leq \mathrm{ed}(C_S) + \mathrm{ed}(\mathfrak{F}_1 \times \cdots \times \mathfrak{F}_r) \\
&= 1 + \mathrm{ed}(\mathfrak{F}_1 \times \cdots \times \mathfrak{F}_r) \\
&\leq 1 + \mathrm{ed}(\mathfrak{F}_1) + \cdots + \mathrm{ed}(\mathfrak{F}_r) \\
&\leq 1 + (\mathrm{ed}(\mathbb{Z}/p_1^{n_1}\mathbb{Z}) - 1) + \cdots + (\mathrm{ed}(\mathbb{Z}/p_r^{n_r}\mathbb{Z}) - 1) \\
&= \mathrm{ed}(\mathbb{Z}/p_1^{n_1}\mathbb{Z}) + \cdots + \mathrm{ed}(\mathbb{Z}/p_r^{n_r}\mathbb{Z}) - r + 1 \\
&= [F(\xi_{p_1^{n_1}}) : F] + \cdots + [F(\xi_{p_r^{n_r}}) : F] - r + 1
\end{aligned}$$

by Lemma 2.7 and Corollary 7.6. □

Example 7.8. If $s_i = n_i$ for $2 \leq i \leq r$, then $\xi_{p_i^{n_i}} \in F$ for $2 \leq i \leq r$. Theorem 7.7 implies that

$$\begin{aligned}
\mathrm{ed}(\mathbb{Z}/p_1^{n_1} \cdots p_r^{n_r}\mathbb{Z}) &\leq [F(\xi_{p_1^{n_1}}) : F] + \cdots + [F(\xi_{p_r^{n_r}}) : F] - r + 1 \\
&= [F(\xi_{p_1^{n_1}}) : F] \\
&= \mathrm{ed}(\mathbb{Z}/p_1^{n_1}\mathbb{Z}).
\end{aligned}$$

On the other hand,

$$H^1(-, \mathbb{Z}/p_1^{n_1} \cdots p_r^{n_r}\mathbb{Z}) = H^1(-, \mathbb{Z}/p_1^{n_1}\mathbb{Z}) \times \cdots \times H^1(-, \mathbb{Z}/p_r^{n_r}\mathbb{Z}).$$

By Remark 2.8 $\max\{\mathrm{ed}(\mathbb{Z}/p_i^{n_i})\} \leq \mathrm{ed}(\mathbb{Z}/p_1^{n_1} \cdots p_r^{n_r}\mathbb{Z})$ where the maximum is taken over $1 \leq i \leq r$ (Note that this inequality can also be derived from Theorem 6.15). Therefore

$$\mathrm{ed}(\mathbb{Z}/p_1^{n_1} \cdots p_r^{n_r}\mathbb{Z}) = \mathrm{ed}(\mathbb{Z}/p_1^{n_1}\mathbb{Z}).$$

The inequality $\mathrm{ed}(\mathbb{Z}/p_1^{n_1}\cdots p_r^{n_r}\mathbb{Z}) \le \mathrm{ed}(\mathbb{Z}/p_1^{n_1}\mathbb{Z})$ can also be obtained by considering faithful representations. First we denote $\mathrm{ed}(\mathbb{Z}/p_1^{n_1}\mathbb{Z}) = [F(\xi_{p_1^{n_1}}) : F]$ by λ, then there exists a faithful representation $\phi : \mathbb{Z}/p_1^{n_1}\mathbb{Z} \to \mathbf{GL}_\lambda(F)$. Let $M = \phi(\overline{1})$ be the image of $\overline{1} \in \mathbb{Z}/p_1^{n_1}\mathbb{Z}$. We define a representation of $\mathbb{Z}/p_1^{n_1}\cdots p_r^{n_r}\mathbb{Z}$ by

$$\begin{aligned}\varphi : \mathbb{Z}/p_1^{n_1}\cdots p_r^{n_r}\mathbb{Z} &\longrightarrow \mathbf{GL}_\lambda(F)\\ \overline{m} &\longmapsto (\xi_{p_2^{n_2}\cdots p_r^{n_r}} \cdot M)^m.\end{aligned}$$

It is easy to verify that φ is faithful. Therefore our inequality follows from Proposition 5.9.

Remark 7.9. Let $m = p_1^{n_1}\cdots p_r^{n_r}$, and $G = \mathbb{Z}/m\mathbb{Z}$. If V is a faithful representation of G over F then $\mathrm{ed}(G) \le \dim(V)$ by Proposition 5.9. We want to compare the least dimension of a faithful representation of G over F with the upper bound of $\mathrm{ed}(G)$ given by Theorem 7.7.

Let $n_i > s_i$ for $1 \le i \le a$, and $n_i = s_i$ for $a < i \le r$ for some integer $1 \le a \le r$. First we recall that by Maschke's Theorem $F[G]$ is semisimple. Since $F[G]$ is a commutative ring, $F[G] \cong F[t]/\langle t^m - 1\rangle$ is isomorphic to a product of fields $E_1 \times \ldots \times E_k$. For every divisor d of m, there exists a surjection $F[t]/\langle t^m - 1\rangle \to F(\xi_d)$, $t \mapsto \xi_d$. Therefore $F(\xi_d) \cong E_i$ for some i. On the other hand, for every E_j clearly there exists a surjection $F[t]/\langle t^m - 1\rangle \to E_j$. Let ξ be the image of t under this surjection. Then $E_j = F[\xi] = F(\xi)$, with $\xi^m = 1$. Hence $E_j \cong F(\xi_d)$ for some divisor d of m. As a result $F[G]$ is isomorphic to a product of $F(\xi_d)$, where d is divisor of m. Note that there can be more than one copy of a particular $F(\xi_d)$ in the product.

For every divisor d of m, it is easy to see that the kernel of the natural representation $G \to \mathrm{GL}(F(\xi_d))$, $\overline{1} \mapsto \xi_d$, is $\langle \overline{d}\rangle$ the subgroup generated by $\overline{d}$. Then the kernel of the natural representation $G \to \mathrm{GL}(\coprod F(\xi_{d_j}))$ is $\bigcap \langle \overline{d_j}\rangle = \langle \mathrm{lcm}\{\overline{d_j}\}\rangle$, where d_j divides m for every j. By choosing d_j to be $p_1^{n_1}, \ldots, p_{a-1}^{n_{a-1}}, p_a^{n_a}\cdots p_r^{n_r}$, we see that the natural representation of G in the F-vector space $V = F(\xi_{p_1^{n_1}}) \oplus \cdots \oplus F(\xi_{p_a^{n_a}})$ is a faithful representation of the least dimension, as $F(\xi_{p_a^{n_a}}) = F(\xi_{p_a^{n_a}\cdots p_r^{n_r}})$. We have

$$\begin{aligned}\dim V &= [F(\xi_{p_1^{n_1}}) : F] + \cdots + [F(\xi_{p_a^{n_a}}) : F] \\ &\geq [F(\xi_{p_1^{n_1}}) : F] + \cdots + [F(\xi_{p_r^{n_r}}) : F] - r + 1\end{aligned}$$

where equality holds if and only if $a = 1$ (see Example 7.8). In particular, if $a \geq 2$, then $\mathrm{ed}(G) < \dim(V)$. This is different from the case for p-groups, where the essential dimension of a p-group G' is equal to the least dimension of a faithful representation of G' over F by Theorem 7.1.

CHAPTER 8

Canonical Dimension

In order to study the lower bounds for $\mathrm{ed}(\mathbb{Z}/p_1^{n_1}\cdots p_r^{n_r}\mathbb{Z})$ we need some more tools. One of them is canonical dimension.

First recall that given two fields K and L, a place $K \to L$ is a local ring homomorphism $\phi : R \to L$ of a valuation ring $R \subseteq K$. If K and L are both extensions of a field F, an F-place, also called a place over F, is a place $K \to L$ with ϕ defined and identical on F.

Note that places are composable. Suppose we have two places $K \to L$ and $L \to E$, given by local ring homomorphisms $\phi : R \to L$ and $\psi : S \to E$ respectively. The composition is the place $K \to E$ given by $\psi \circ \phi : \phi^{-1}(S) \to E$ defined on the valuation ring $\phi^{-1}(S)$. In particular, since an embedding of fields is a place, any place $L \to E$ can be restricted to any subfield $K \subseteq L$.

Definition 8.1. *Let F be a field and $\mathfrak{C}$ be a class of field extensions of F. A field $E \in \mathfrak{C}$ is called generic if for any $K \in \mathfrak{C}$ there exists an F-place $E \to K$. The canonical dimension of the class $\mathfrak{C}$, denoted by* $\mathrm{cdim}(\mathfrak{C})$*, is defined by*

$$\mathrm{cdim}(\mathfrak{C}) = \min\{tr.deg_F(E)\}$$

where the minimum is taken over all generic fields $E \in \mathfrak{C}$.

Let $\mathfrak{F}$ be an object in Fun_F, and $\mathfrak{C}_{\mathfrak{F}}$ be the class of splitting fields of $\mathfrak{F}$, i.e. the class of field extensions K/F such that $\mathfrak{F}(K) \neq \emptyset$. The canonical dimension of $\mathfrak{F}$, denoted by $\mathrm{cdim}(\mathfrak{F})$*, is the canonical dimension of the class $\mathfrak{C}_{\mathfrak{F}}$.*

We use the word 'variety' to mean an integral separated scheme.

Proposition 8.2. *Let X be a regular variety over F. Then the function field $F(X)$ of X is a generic splitting field of X. In particular,*

$$\operatorname{cdim}(X) \leq \dim(X).$$

Proof. First, it is clear that the function field $F(X)$ is a splitting field of X even in the non-regular case. To show that $F(X)$ is generic, let K/F be an arbitrary splitting field of X. Then we take a finitely generated splitting subfield $L \subseteq K$, and Y a variety over F with function field $F(Y) = L$. Since X has a $F(Y)$-rational point, there exists a rational morphism $Y \dashrightarrow X$. Let $x \in X$ be the image of the generic point of Y. By assumption X is regular at x, hence there is a regular system of local parameters around x. Such a system produces a place $F(X) \to F(x)$ as follows: Let $a_1, \ldots, a_n$ be a regular system of parameters in the regular local ring $R = \mathcal{O}_{X,x}$. Let J_i be the ideal of R generated by $a_1, \ldots, a_i$, $R_i = R/J_i$ and $P_i = J_{i+1}/J_i$. Note that R_i is also a regular local ring, and P_i is a height 1 prime ideal of R_i. Denote by F_i the quotient field of R_i, in particular $F_0 = F(X)$ and $F_n = F(x)$. Then the localization $(R_i)_{P_i}$ is a discrete valuation ring with quotient field F_i and residue field F_{i+1}, hence it gives a place $F_i \to F_{i+1}$. Therefore there exists a place $F(X) \to F(x)$ by composition

$$F(X) = F_0 \to F_1 \to \cdots \to F_n = F(x).$$

By composing this place with the embeddings of fields $F(x) \subseteq F(Y)$ and $F(Y) \subseteq K$, we get a place $F(X) \to K$. $\square$

Remark 8.3. If X has an F-rational point, then clearly $\operatorname{cdim}(X) = 0$. Thus we can view canonical dimension of X as a numerical invariant that measures how far away X is from having an F-rational point.

Suppose X is a regular complete variety over F. Then it is shown in [14, Corollary 4.6] that the canonical dimension of X is the least dimension of a closed subvariety $Z \subseteq X$ such that there is a rational morphism $X \dashrightarrow Z$. Therefore $\operatorname{cdim}(X)$ can also viewed as a numerical invariant that measures the compressibility of X. If $\operatorname{cdim}(X) = \dim(X)$, we say that X is incompressible.

Definition 8.4. *Let $\mathfrak{C}$ be a class of field extensions of F that is closed under extensions, i.e. if $K \in \mathfrak{C}$ and L/K is a field extension, then $L \in \mathfrak{C}$. For any $K \in \mathfrak{C}$, we define*

$$\mathrm{ed}^{\mathfrak{C}}(K) = \min\{tr.deg_F(K_0)\}$$

where the minimum is taken over all subfields K_0 of K such that $K_0 \in \mathfrak{C}$.

Theorem 8.5. *Let X be a regular complete variety over F, and let $\mathfrak{C}$ be the class of splitting fields of of X. Then $\mathfrak{C}$ is closed under extension, and*

$$\mathrm{cdim}(X) = \sup\{\mathrm{ed}^{\mathfrak{C}}(K)\}$$

where the supremum is taken over all $K \in \mathfrak{C}$.

Proof. Let $E \in \mathfrak{C}$ be a generic field such that $tr.deg_F(E) = \mathrm{cdim}(X)$. The existence of such E is guaranteed by Proposition 8.2. Note that if $K \subseteq E$ is a subfield and $K \in \mathfrak{C}$, then K is also generic and it implies that $tr.deg_F(K) = tr.deg_F(E)$. Therefore $tr.deg_F(E) = \mathrm{ed}^{\mathfrak{C}}(E)$, and

$$\mathrm{cdim}(X) = \mathrm{ed}^{\mathfrak{C}}(E) \leq \sup\{\mathrm{ed}^{\mathfrak{C}}(K)\}.$$

For the other inequality, let $E \in \mathfrak{C}$ be a generic field, and let $K \in \mathfrak{C}$. Let $K_0 \in \mathfrak{C}$ be a subfield of K such that $\mathrm{ed}^{\mathfrak{C}}(K) = tr.deg_F(K_0)$. Then by replacing K with K_0 we may assume $\mathrm{ed}^{\mathfrak{C}}(K) = tr.deg_F(K)$. Since E is generic, there exists an F-place $E \to K$ given by a local ring homomorphism $\phi : R \to K$. Let $K' = \phi(R) \subseteq K$ be the image of the place. Since X is complete, $X(E) \neq \emptyset$ implies that $X(\mathrm{Spec}(R)) \neq \emptyset$, thus $X(K') \neq \emptyset$ also, i.e. $K' \in \mathfrak{C}$. Then it follows from $\mathrm{ed}^{\mathfrak{C}}(K) = tr.deg_F(K)$ that $tr.deg_F(K') = tr.deg_F(K)$. Therefore

$$tr.deg_F(E) \geq tr.deg_F(K') = tr.deg_F(K) = \mathrm{ed}^{\mathfrak{C}}(K),$$

hence we have $tr.deg_F(E) \geq \sup\{\mathrm{ed}^{\mathfrak{C}}(K)\}$. □

The concept of canonical dimension can also be applied to elements and subgroups of $Br(F)$ the Brauer group of F. For every $\theta \in Br(F)$, let $\mathfrak{C}_\theta$ be the class of splitting fields of θ. The canonical dimension of θ, denoted by $\mathrm{cdim}(\theta)$, is the canonical dimension of the class

$\mathfrak{C}_\theta$. Similarly, if D is a finite subgroup of $Br(F)$, let $\mathfrak{C}_D$ be the class of common splitting fields of all elements in D. The canonical dimension of D, denoted by $\mathrm{cdim}(D)$, is defined as the canonical dimension of the class $\mathfrak{C}_D$.

Example 8.6. Let $\theta \in Br(F)$ be represented by a central simple F-algebra A, and let $SB(A)$ be the Severi-Brauer variety of A. Then for every field extensions K/F, K splits θ if and only if K splits A if and only if $SB(A)(K) \neq \emptyset$. Therefore $\mathrm{cdim}(\theta) = \mathrm{cdim}(SB(A))$.

Conjecture 8.7. Let A be a central division F-algebra of degree $n = p_1^{a_1} \cdots p_r^{a_r}$, where p_i are distinct prime numbers, a_i are non-negative integers. We can write A as a tensor product $A_i \otimes \cdots \otimes A_r$ where A_i is a central division F-algebra of degree $p_i^{a_i}$. Let $X = SB(A)$ be the Severi-Brauer variety of A, and let $Y = SB(A_1) \times \cdots \times SB(A_r)$ be the product of the Severi-Brauer varieties of A_i. Then for every field extensions K/F, K splits A if and only if it splits A_i for every i, which implies $X(K) \neq \emptyset$ if and only if $Y(K) \neq \emptyset$. Hence we have

$$\mathrm{cdim}(SB(A)) = \mathrm{cdim}(Y) \leq \dim(Y) = p_1^{a_1} + \cdots + p_r^{a_r} - r. \tag{8.6}$$

by Proposition 8.2. It is conjectured in [5] that the inequality in (8.6) is actually an equality. This is proven in [2] in the case when $r = 1$, i.e. when n is a prime power, and proven in [5] when $n = 6$.

CHAPTER 9

Fibered Categories

Let $\mathcal{A}$ be a category and let ϕ be a functor from $\mathcal{A}$ to Sch/F the category of schemes over F. For every scheme $X \in Sch/F$, we denote by $\mathcal{A}(X)$ the fiber category of all objects $a \in \mathcal{A}$ with $\phi(a) = X$ and morphisms over the identity of X. We will always assume that $\mathcal{A}(X)$ is essentially small for every X, i.e. the isomorphism classes of objects in $\mathcal{A}(X)$ is a set.

Let $\mathcal{A}$ be a fibered category over Sch/F. Then for any morphism $f : X \to Y$ in Sch/F, there is a pullback functor $f^* : \mathcal{A}(Y) \to (A)(X)$ such that for any two morphisms $f : X \to Y$ and $g : Y \to Z$ in Sch/F, the composition $f^* \circ g^*$ is isomorphic $(g \circ f)^*$. Let $K \in Fields/F$ be a field extension. We write $S_{\mathcal{A}}(K)$ for the set of isomorphism classes of objects in the fiber category $\mathcal{A}(\mathrm{Spec}(K))$. Given L/K an extension in $Fields/F$, it is easy to see that the corresponding pullback functor induces a map of sets $S_{\mathcal{A}}(K) \to S_{\mathcal{A}}(L)$. Therefore $S_{\mathcal{A}}$ is an object in Fun_F. The essential dimension of $\mathcal{A}$, denoted by $\mathrm{ed}(\mathcal{A})$, is defined as the essential dimension of the functor $S_{\mathcal{A}}$. Similarly, the canonical dimension of $\mathcal{A}$, $\mathrm{cdim}(\mathcal{A})$, is the canonical dimension of $S_{\mathcal{A}}$.

Example 9.1. Let X be a scheme over F. Then X can be viewed as a fibered category, where the objects are schemes over X and the morphisms are morphisms over X. For any scheme Y over X, the fiber category $X(Y)$ is the set of morphisms $\mathrm{Hom}_F(Y, X)$ considered as a category with identity morphisms only. It is obvious that S_X the functor induced by the fibered category X is the same as the "functor of points" X. In particular, the essential dimension of X with X viewed as a fibered category is the same as that with X viewed as a scheme.

Let G be an algebraic group and X be a G-scheme over F, i.e. a scheme over F together with a G-action on it. We define a fibered category denoted by X/G as follows. An object in X/G over a scheme Z is a diagram

$$\begin{tikzcd} J \arrow[r, "\alpha"] \arrow[d, "q"'] & X \\ Z & \end{tikzcd} \tag{9.7}$$

where Q is a G-torsor, and α is a G-equivariant morphism. Given two objects (J, q, α) and (J', q', α') over Z, a morphism between them is a G-equivariant morphism $\beta : J \to J'$ such that $\alpha' \circ \beta = \alpha$ and $q' \circ \beta = q$. The functor $\phi : X/G \to Sch/F$ maps diagram (9.7) to Z. Then for every morphism $f : Y \to Z$ in Sch/F, the pullback functor $f^* : (X/G)(Z) \to (X/G)(Y)$ is given by taking fiber product.

Example 9.2.

(1) Let $X \to Y$ be a G-torsor. Then X/G is isomorphic to Y as fibered categories.

(2) The fibered category $\mathrm{Spec}(F)/G$ is usually denoted by BG and it is called the classifying space of G. Note that the objects of BG are G-torsors over schemes over F. Therefore the induced functor S_{BG} is the same as the functor $K \mapsto H^1(K, G)$ that sends every $K \in Fields/F$ to the set of isomorphism classes of G-torsors over $\mathrm{Spec}(K)$. In particular, $\mathrm{ed}(BG) = \mathrm{ed}(G)$.

Let G be an algebraic group, and let $H = G/C$ be a factor group of G for some normal subgroup $C \subseteq G$. For every H-torsor E over $\mathrm{Spec}(F)$, the group G acts on E via the natural group homomorphism $G \to H$. Consider the fibered category E/G. Let (J, q, α) be an object in E/G over a scheme Z. Then α induces a morphism $J/C \to E \times Z$ of H-torsors over Z, which is an isomorphism from faithfully flat descent. Therefore the natural morphism $J \to E \times Z$ is a C-torsor, and every object of $(E/G)(Z)$ can be viewed as a "lifting" of the H-torsor $E \times Z \to Z$ to a G-torsor $J \to Z$ together with an isomorphism $J/C \xrightarrow{\cong} E \times Z$.

Theorem 9.3. *Let G be an algebraic group over F. Let $C \subseteq G$ be a normal subgroup and $H = G/C$ be the corresponding factor group. Then for every H-torsor E over* $\mathrm{Spec}(F)$*, we have*

$$\mathrm{ed}(G) \geq \mathrm{ed}(E/G) - \dim(H).$$

Proof. Let K/F be a field extension and let $x = (J, q, \alpha)$ be an object of E/G over $\mathrm{Spec}(K)$. Denote by $\beta : J/C \to E_K$ the isomorphism of H-torsors over $\mathrm{Spec}(K)$ induced by α. There is a subextension $F \subseteq L \subseteq K$ such that $tr.deg_F(L) = \mathrm{ed}(J)$ and $J = I_K$ for some G-torsor I over $\mathrm{Spec}(L)$.

Consider $Z = \mathrm{Iso}_L(I/C, E_L)$ the scheme (as functor of points) of isomorphisms of H-torsors over $\mathrm{Spec}(L)$. Note that Z is a torsor over $\mathrm{Spec}(L)$ for the twisted form $\mathrm{Aut}_L(I/C)$ of H, therefore $\dim_L(Z) = \dim(H)$. By construction $\beta \in Z(K)$, and we denote the image of the corresponding morphism $\mathrm{Spec}(K) \to Z$ by $\{z\}$. Then β and hence x are defined over $L(z)$, and we have

$$\begin{aligned} \mathrm{ed}(G) + \dim(H) &\geq \mathrm{ed}(J) + \dim(H) \\ &= tr.deg_F(L) + \dim_L(Z) \geq tr.deg_F(L(z)) \geq \mathrm{ed}(x). \end{aligned}$$

Since this inequality holds for every $x \in (E/G)(X)$ and every field extension K/F, it follows that

$$\mathrm{ed}(G) + \dim(H) \geq \mathrm{ed}(E/G). \qquad \square$$

Suppose that C is commutative. There is a pairing

$$BC \times BC \longrightarrow BC$$

that maps a pair of C-torsors I and I' over the same scheme Z to $(I \times_Z I')/C$, where an element $c \in C$ acts on $(I \times_Z I')$ by (c, c^{-1}). We will write $(t, t') \mapsto t + t'$ for this operation, and 0 for the trivial C-torsor.

Suppose in addition that $C \subseteq G$ is a central subgroup. Let $E \to \mathrm{Spec}(F)$ be an H-torsor where $H = G/C$, and consider the fibered category E/G. We have the pairing functor

$$E/G \times BC \longrightarrow E/G$$

defined as follows. Given an object (J, q, α) of E/G over a scheme Z, and I a C-torsor over the same scheme Z, the pairing sends $((J, q, \alpha), I)$ to $((J \times_Z I)/C, s, \beta)$ where $s(j, i) = q(j)$ and $\beta(j, i) = \alpha(j)$. We will write $(x, t) \mapsto x + t$ for this operation.

There is also the following pairing

$$E/G \times E/G \longrightarrow BC$$

that takes a pair of objects (J, q, α) and (J', q', α'), both over Z, to $(J \times_{(E\times Z)} J')/G$ with the product taken with respect to α and α' and with diagonal G-action. $(J \times_{(E\times Z)} J')/G$ is viewed as a C-torsor via the action of C on the first factor J. We will write $(x, x') \mapsto x - x'$ for this operation.

These pairings satisfy the following properties, justifying our choice for the notations for the pairings.

$$\begin{aligned} (x+t) - x' \cong (x - x') + t \qquad & x + (t + t') \cong (x+t) + t' \\ (x - x') + x' \cong x \qquad & x - x \cong 0 \\ x + 0 \cong x \qquad & t + 0 \cong 0 \end{aligned}$$

for every $t, t' \in BC(Z)$ and every $x, x' \in (E/G)(Z)$.

Lemma 9.4. *The fibered category E/G has an object over* $\mathrm{Spec}(F)$ *if and only if E/G is isomorphic to BC.*

Proof. The "if" part is easy because BC has an object over $\mathrm{Spec}(F)$. For the "only if" part, suppose there is an object $x' \in (E/G)(\mathrm{Spec}(F))$. Then the maps $E/G \to BC$, $x \mapsto x - x'$, and $BC \to E/G$, $t \mapsto x' + t$ are equivalences inverse to each other by the above properties. □

Remark 9.5. Since every H-torsor $E \to \mathrm{Spec}(F)$ splits over a field extension of F, Lemma 9.4 shows that the fibered category E/G can be viewed as a twisted form of BC. We say that E/G is trivial if E/G is isomorphic to BC, i.e. if E/G has an object over $\mathrm{Spec}(F)$.

Let $C \subseteq G$ be a central subgroup, and let $H = G/C$. Since C is commutative, the second Galois cohomology group $H^2(K, C)$ is defined for every field extension K/F, and we have the connecting homomorphism

$$\partial_K : H^1(K, H) \longrightarrow H^2(K, C)$$

induced by the natural exact sequence of algebraic groups. Let E be an H-torsor over $\mathrm{Spec}(F)$. We denote by $\theta(E/G) = \partial_F([E]) \in H^2(F, C)$ the image of the class of E under ∂_F.

The following proposition will be needed in the sequel.

Proposition 9.6. *Let Z be a scheme over F. Then $(E/G)(Z)$ is not empty if and only if $\theta(E/G)_Z = 0$ in $H^2_{ét}(K, C)$.*

Proof. If follows from the exact sequence

$$H^1_{ét}(Z, G) \longrightarrow H^1_{ét}(Z, H) \longrightarrow H^2_{ét}(Z, C)$$

that $\theta(E/G)_Z = 0$ if and only if $[E \times Z]$ is in the image of $H^1_{ét}(Z, G)$.

If there exists a G-torsor $q : J \to Z$ such that J/C is isomorphic to $E \times Z$, then (J, q, α) is an object in $(E/G)(Z)$ where $\alpha : J \to E$ is the composition $J \to J/C \overset{\cong}{\to} E \times Z \to E$. Conversely, if $(E/G)(Z) \neq \emptyset$, let (J, q, α) be an object in $(E/G)(Z)$. Then we have seen in the discussion above Theorem 9.3 that J/C is isomorphic to $E \times Z$. Therefore $[E \times Z]$ is in the image of $H^1_{ét}(K, G)$ if and only if $(E/G)(Z) \neq \emptyset$. □

Next we are going to study the relationships between the essential dimension and the canonical dimension of E/G.

Let $C \subseteq G$ be a central subgroup. Suppose in addition that C is isomorphic to $\mu_{n_1} \times \cdots \times \mu_{n_s}$, where $1 \neq n_1 \mid \cdots \mid n_s$, and $char(F)$ does not divide n_s. Let $E \to \mathrm{Spec}(F)$ be an H-torsor where $H = G/C$. It gives an element $\theta(E/G) \in H^2(F, C)$. Note that $H^2(F, C) \cong Br_{n_1}(F) \times \cdots \times Br_{n_s}(F)$, therefore $\theta(E/G)$ can be represented by an s-tuple central simple algebras $A_1, \ldots, A_s$ with $[A_i] \in Br_{n_i}(F)$. Let P be the product of the Severi-Brauer varieties $SB(A_i)$. By Proposition 9.6, for any field extension K/F,

$$(E/G)(\mathrm{Spec}(K)) \neq \emptyset \;\Leftrightarrow\; \theta(E/G)_K = 0 \;\Leftrightarrow\; K \text{ splits } A_i \; \forall i \;\Leftrightarrow\; P(K) \neq \emptyset.$$

Therefore the class of splitting fields of E/G is the same as that of P, which we denote by $\mathfrak{C}$. Since P is a regular complete variety, by applying Theorem 8.5 we have

$$\mathrm{cdim}(E/G) = \mathrm{cdim}(P) = \sup\{\mathrm{ed}^{\mathfrak{C}}(K)\}.$$

Proposition 9.7. $\mathrm{ed}(E/G) \le \mathrm{cdim}(E/G) + s$.

Proof. Let K/F be a field extension, and $x \in (E/G)(\mathrm{Spec}(K))$. There is a subextension $F \subseteq L \subseteq K$ such that $(E/G)(\mathrm{Spec}(L)) \neq \emptyset$ and $tr.deg_F(L) = \mathrm{ed}^{\mathfrak{C}}(K)$. Note that since $(E/G)(\mathrm{Spec}(L)) \neq \emptyset$, there exists $y \in (E/G)(\mathrm{Spec}(L))$ and we set $t = x - y_K \in BC(\mathrm{Spec}(K))$. Then there is a subextension $F \subseteq L' \subseteq K$ such that $tr.deg_F(L') = \mathrm{ed}(t)$ and $t = t'_K$ for some $t' \in BC(\mathrm{Spec}(L'))$. It follows that $x \cong y_K + t$ is defined over the composite field LL'. Therefore we obtain

$$\begin{aligned} \mathrm{ed}(x) \le tr.deg_F(LL') &\le tr.deg_F(L) + tr.deg_F(L') \\ &= \mathrm{ed}^{\mathfrak{C}}(K) + \mathrm{ed}(t) \\ &\le \mathrm{cdim}(E/G) + \mathrm{ed}(C) \\ &= \mathrm{cdim}(E/G) + s, \end{aligned}$$

where the last equality follows from Corollary 4.8. □

For every commutative algebra R over F and for every $r_1, \dots, r_s \in R^\times$, the ring $R[t_1, \dots, t_s]/\langle t_1^{n_1} - r_1, \dots, t_s^{n_s} - r_s\rangle$ is a Galois C-algebra. We denote by $(r) = (r_1, \dots, r_s)$ the corresponding C-torsor over $\mathrm{Spec}(R)$, viewing (r) as an object of $BC(\mathrm{Spec}(R))$. Since C is isomorphic to $\mu_{n_1} \times \cdots \times \mu_{n_s}$, there is an exact sequence of algebraic groups

$$1 \longrightarrow C \longrightarrow \mathbb{G}_m^s \xrightarrow{(n)} \mathbb{G}_m^s \longrightarrow 1 \,,$$

where $(n) = (n_1, \dots, n_s)$. Passing to étale cohomology, we get an exact sequence

$$\prod_{i=1}^s R^\times \xrightarrow{(n)} \prod_{i=1}^s R^\times \longrightarrow H^1_{\acute{e}t}(\mathrm{Spec}(R), C) \longrightarrow \prod_{i=1}^s \mathrm{Pic}(R) \,.$$

The C-torsors (r) and (r') are isomorphic if and only if $r_i R^{\times n_i} = r'_i R^{\times n_i}$ for every i. If $\mathrm{Pic}(R) = 0$ (for example when R is a local ring), then every C-torsor over $\mathrm{Spec}(R)$ is isomorphic to (r) for some $r_1, \dots, r_s \in R^\times$.

Theorem 9.8. *Let $C \subseteq G$ be a central subgroup such that C is isomorphic to $\mu_{n_1} \times \cdots \times \mu_{n_s}$, where $1 \neq n_1 \mid \cdots \mid n_s$, and $char(F)$ does not divide n_s. Let $E \to \mathrm{Spec}(F)$ be an H-torsor where $H = G/C$. Then*

$$\mathrm{ed}(E/G) = \mathrm{cdim}(E/G) + s.$$

Proof. By Proposition 9.7, we know that

$$\mathrm{ed}(E/G) \leq \mathrm{cdim}(E/G) + s.$$

Therefore it remains to prove $\mathrm{ed}(E/G) \geq \mathrm{cdim}(E/G) + s$.

Let K/F be a splitting field for E/G, and there exists $x \in (E/G)(\mathrm{Spec}(K)) \neq \emptyset$. Consider the field $L = K(t_1, \ldots, t_s)$ where t_i are indeterminates for every i. We set $x' = x_L + (t) \in (E/G)(\mathrm{Spec}(L))$, where $(t) = (t_1, \ldots, t_s) \in BC(\mathrm{Spec}(L))$. There is a subextension $F \subseteq L' \subseteq L$ such that $tr.deg_F(L') = \mathrm{ed}(x')$ and $x' = y_L$ for some $y \in (E/G)(\mathrm{Spec}(L'))$.

For every $i = 1, \ldots, s$, let $L_i = K(t_i, \ldots, t_s)$ and v_i be the discrete valuation of L_i corresponding to t_i. Then the composition v of the discrete valuations v_i is a valuation of L with residue field K. By choosing prime elements in all the L_i the value group of v can be identified with $\mathbb{Z}^s$. Note that for every i we have

$$v(t_i) = e_i$$

where $\{e_1, \ldots, e_s\}$ is the standard basis of $\mathbb{Z}^s$.

Let v' be the restriction of v on L'.

Claim: $rank(v') = s$.

Let $R' \subseteq L'$ be the valuation ring of v'. Since $(E/G)(\mathrm{Spec}(L')) \neq \emptyset$, we have $P(L') \neq \emptyset$. Then $P(\mathrm{Spec}(R')) \neq \emptyset$ because P is a complete variety. It follows that the algebras A_i split over R', which implies that $(E/G)(\mathrm{Spec}(R')) \neq \emptyset$ by Proposition 9.6. Let $x'' \in (E/G)(\mathrm{Spec}(R'))$. Note that $y - x''_{L'} \cong (z) = (z_1, \ldots, z_s) \in BC(\mathrm{Spec}(L'))$ for some $z_1, \ldots z_s \in L'^{\times}$. Therefore

$$(z)_L \cong y_L - x''_L = x' - x''_L = (x_L + (t)) - x''_L \cong (x_L - x''_L) + (t).$$

Let $R \subseteq L$ be the valuation ring of v. Note that $x_L - x''_L$ is in the image of $BC(\mathrm{Spec}(R)) \to BC(\mathrm{Spec}(L))$. Therefore $x_L - x''_L \cong (z')_L = (z'_1, \ldots, z'_s)_L$ for some $z'_1, \ldots, z'_s \in R^{\times}$ as R is a local ring. It follows that

$$(z)_L \cong (z')_L + (t) \cong (z't)_L,$$

and there exists $w_1, \ldots, w_s \in L^\times$ such that

$$z_i = z_i' t_i w_i^{n_i}$$

for every i. Therefore $v'(z_i) = v(t_i)$ modulo p, where p is a prime divisor of n_1. This implies that $v'(z_1), \ldots, v'(z_s)$ are linearly independent modulo p, and they generate a submodule of rank s in $\mathbb{Z}^s$. Thus $rank(v') = s$, proving the claim.

Let K' be the residue field of v'. Note that $P(K') \neq \emptyset$ because $P(\mathrm{Spec}(R')) \neq \emptyset$, hence $(E/G)(\mathrm{Spec}(K')) \neq \emptyset$, i.e. $K' \in \mathfrak{C}$. Since K is the residue field of the valuation v, we have $K' \subseteq K$, and it follows that

$$tr.deg_F(K') \geq \mathrm{ed}^{\mathfrak{C}}(K).$$

By [26, Chapter VI, Theorem 3, Corollary 1], we have

$$\mathrm{ed}(E/G) \geq \mathrm{ed}(x') = tr.deg_F(L') \geq tr.deg_F(K') + rank(v') \geq \mathrm{ed}^{\mathfrak{C}}(K) + s.$$

Since the above inequality holds for every $K \in \mathfrak{C}$, it follows that

$$\mathrm{ed}(E/G) \geq \mathrm{cdim}(E/G) + s. \qquad \square$$

CHAPTER 10

Essential Dimension of Cyclic Groups, II

We now have the tools needed to study the lower bounds for $\mathrm{ed}(\mathbb{Z}/p_1^{n_1}\cdots p_r^{n_r}\mathbb{Z})$.

Theorem 10.1. *Let $p_1,\ldots,p_r$ be distinct prime numbers, $n_1,\ldots,n_r$ be positive integers. Let F be a field such that $char(F)\neq p_i$ and $\xi_{p_i}\in F$ for every i. If Conjecture 8.7 is valid for algebras of degree $\prod_{i=1}^{r}[F(\xi_{p_i^{n_i}}):F]$, then*

$$\begin{aligned}\mathrm{ed}(\mathbb{Z}/p_1^{n_1}\cdots p_r^{n_r}\mathbb{Z}) &= \mathrm{ed}(\mathbb{Z}/p_1^{n_1}\mathbb{Z})+\cdots+\mathrm{ed}(\mathbb{Z}/p_r^{n_r}\mathbb{Z})-r+1\\ &= [F(\xi_{p_1^{n_1}}):F]+\cdots+[F(\xi_{p_r^{n_r}}):F]-r+1.\end{aligned}$$

Proof. By Theorem 7.7 we only need to prove

$$\mathrm{ed}(\mathbb{Z}/p_1^{n_1}\cdots p_r^{n_r}\mathbb{Z})\geq [F(\xi_{p_1^{n_1}}):F]+\cdots+[F(\xi_{p_r^{n_r}}):F]-r+1$$

when Conjecture 8.7 is valid for algebras of degree $\prod_{i=1}^{r}[F(\xi_{p_i^{n_i}}):F]$.

Let $m=p_1^{n_1}\cdots p_r^{n_r}$, $G=\mathbb{Z}/m\mathbb{Z}$, C be the subgroup $\mathbb{Z}/p_1\cdots p_r\mathbb{Z}$ of G, and set $H=G/C$. Let $E\to Spec(L)$ be a generic H-torsor for some field extension L/F. We define a homomorphism $\beta^E: C^*\to Br(L)$ as follows, where $C^*=\mathrm{Hom}(C,\mathbb{G}_m)$ is the character group of C. For every character $\chi: C\to\mathbb{G}_m$, we define $\beta^E(\chi)$ to be the image of $[E]$ under the composition

$$H^1(L,H)\xrightarrow{\partial_L}H^2(L,C)\xrightarrow{\chi_*}H^2(L,\mathbb{G}_m)=Br(L)\,.$$

Consider the fibered category E/G. Since L is a field extension of F, L contains ξ_{p_i} for every i. Therefore C is isomorphic to $\mu_{p_1\cdots p_r}$, and $H^2(L,C)\cong Br_{p_1\cdots p_r}(L)$. It follows that $\theta(E/G)\in H^2(L,C)$ can be represented by a central division L-algebra A with

$[A] \in Br_{p_1 \cdots p_r}(L)$. Notice that $\beta^E(\chi)$ is just $\chi_*(\theta(E/G))$, therefore $\mathrm{im}(\beta^E)$ is generated by $[A]$. It follows that E/G and $\mathrm{im}(\beta^E)$ have the same class of splitting fields, in particular

$$\mathrm{cdim}_L(E/G) = \mathrm{cdim}_L(\mathrm{im}(\beta^E)).$$

By applying Theorem 9.3 and Theorem 9.8, we have

$$\mathrm{ed}(G) \geq \mathrm{ed}_L(G) \geq \mathrm{ed}_L(E/G) = \mathrm{cdim}_L(E/G) + 1 = \mathrm{cdim}_L(\mathrm{im}(\beta^E)) + 1. \tag{10.8}$$

For every character $\chi \in C^*$, we denote by $Rep^{(\chi)}(G)$ the category of all finite dimensional representations ρ of G such that $\rho(c)$ is multiplication of $\chi(c)$ for every $c \in C$. By [15, Theorem 4.4 and Remark 4.5], we have

$$\mathrm{ind}(\beta^E(\chi)) = \gcd \dim(V)$$

over all representations $V \in Rep^{(\chi)}(G)$.

Let $\chi \in C^*$ be a character such that $\beta^E(\chi) = [A]$, and let

$$a = \mathrm{ind}(\beta^E(\chi)) = \gcd \dim(V)$$

over all $V \in Rep^{(\chi)}(G)$. Note that since A is a central division algebra, $\deg(A) = \mathrm{ind}(A) = a$. For every $V \in Rep^{(\chi)}(G)$, by the calculation in Remark 7.9 we have $V = \coprod F(\xi_{d_j})$, where d_j divides m for every j. Since c acts on V by multiplication of $\chi(c)$ for every $c \in C$, we see that $\xi_{d_j}^{p_1^{n_1-1} \cdots p_r^{n_r-1}}$ is a primitive $p_1 \cdots p_r$-th root of unity. Combining with the fact that d_j divides m, we have $d_j = m$ for every j, which implies

$$a = [F(\xi_m) : F] = \prod_{i=1}^{r} [F(\xi_{p_i^{n_i}}) : F],$$

where the second equality follows from the fact that $\xi_{p_i} \in F$, $[F(\xi_{p_i^{n_i}}) : F]$ is a power of p_i for every i.

If Conjecture 8.7 is valid for algebras of degree $\prod_{i=1}^{r} [F(\xi_{p_i^{n_i}}) : F]$, then

$$\begin{aligned} \mathrm{cdim}_L(\mathrm{im}(\beta^E)) = \mathrm{cdim}_L([A]) &= \mathrm{cdim}_L(SB(A)) \\ &= [F(\xi_{p_1^{n_1}}) : F] + \cdots + [F(\xi_{p_r^{n_r}}) : F] - r. \end{aligned}$$

By combining the above inequality with (10.8), we have

$$\mathrm{ed}(G) \geq \mathrm{cdim}_L(\mathrm{im}(\beta^E)) + 1 = [F(\xi_{p_1^{n_1}}) : F] + \cdots + [F(\xi_{p_r^{n_r}}) : F] - r + 1. \qquad \square$$

Example 10.2. Let F be a field such that $\xi_2, \xi_3 \in F$ but $\xi_4, \xi_9 \notin F$. Consider $\mathrm{ed}(\mathbb{Z}/36\mathbb{Z}) = \mathrm{ed}(\mathbb{Z}/2^2 3^2\mathbb{Z})$. The connecting homomorphism

$$\partial_L : L^\times/L^{\times 6} \cong H^1(L, \mathbb{Z}/6\mathbb{Z}) \longrightarrow H^2(L, \mathbb{Z}/6\mathbb{Z})$$

sends $\overline{x} \in L^\times/L^{\times 6}$ to the cyclic algebra $(x, \xi_6)_{\xi_6}$. Take $L = F(t)$ where t is an indeterminate. Then by applying Wedderburn's criterion we see that $(t, \xi_6)_{\xi_6}$ is a division algebra of degree 6, which implies $a = \mathrm{ind}(\beta^E(\chi)) = 6$. Since Conjecture 8.7 is proven when A is of degree 6, we have $\mathrm{ed}(\mathbb{Z}/36\mathbb{Z}) = 4$.

CHAPTER 11

Essential Dimension of Finite Abelian Groups

In this chapter we generalize our results to the essential dimension of arbitrary finite abelian groups, over a field F containing a primitive p-th root of unity for every prime divisor p of the order of the group.

Suppose G is a finite abstract abelian group. Let $G = G_1 \times \cdots \times G_r$ be the elementary divisor decomposition of G, where $G_i = \prod_{j=1}^{s_i} \mathbb{Z}/p_i^{n_{i,j}}\mathbb{Z}$ are the Sylow p_i-subgroups of G, p_i are distinct prime numbers, $n_{i,1} \geq \cdots \geq n_{i,s_i} \geq 1$ for every i, and $s_1 \geq \cdots \geq s_r$. We write $s = s_1$. Then $G = G'_1 \times \cdots \times G'_s$ is the invariant factor decomposition of G, where $G'_j = \mathbb{Z}/p_1^{n_{1,j}} \cdots p_{a_j}^{n_{a_j,j}}\mathbb{Z}$ with $a_j = \max\{i \mid s_i \geq j\}$.

Proposition 11.1. *Let G be a finite abstract abelian group with the above decompositions. Let F be a field such that $char(F) \neq p_i$ and $\xi_{p_i} \in F$ for every i. Then*

$$\begin{aligned}
\operatorname{ed}(G) &\leq \sum_{i=1}^{r} \sum_{j=1}^{s_i} \operatorname{ed}(\mathbb{Z}/p_i^{n_{i,j}}\mathbb{Z}) - \sum_{i=2}^{r} s_i \\
&= \sum_{i=1}^{r} \sum_{j=1}^{s_i} [F(\xi_{p_i^{n_{i,j}}}) : F] - \sum_{i=2}^{r} s_i.
\end{aligned}$$

Proof. Consider $G = G'_1 \times \cdots \times G'_s$ the invariant factor decomposition of G. By Lemma 2.7 and Theorem 7.7, we have

$$\begin{aligned}
\operatorname{ed}(G) \leq \sum_{j=1}^{s} \operatorname{ed}(G'_j) &\leq \sum_{j=1}^{s} \left(\sum_{i=1}^{a_j} \operatorname{ed}(\mathbb{Z}/p_i^{n_{i,j}}\mathbb{Z}) - a_j + 1 \right) \\
&= \sum_{i=1}^{r} \sum_{j=1}^{s_i} \operatorname{ed}(\mathbb{Z}/p_i^{n_{i,j}}\mathbb{Z}) - \sum_{i=1}^{r} s_i + s \\
&= \sum_{i=1}^{r} \sum_{j=1}^{s_i} \operatorname{ed}(\mathbb{Z}/p_i^{n_{i,j}}\mathbb{Z}) - \sum_{i=2}^{r} s_i.
\end{aligned}$$

□

Remark 11.2. The number $\sum_{i=2}^{r} s_i$ is a numerical invariant of G, and it is equal to the number of elementary divisors of G minus the number of invariant factors of G.

For the lower bound of the essential dimension of G, we need a generalized version of Conjecture 8.7.

Conjecture 11.3. Let D be a finite subgroup of $Br(F)$ the Brauer group of F, and let D_{p_i} be the Sylow p_i-subgroup of D for all the prime divisors $p_1, \dots, p_r$ of $|D|$ the order of D. It is conjectured that

$$\operatorname{cdim}(D) = \operatorname{cdim}(D_{p_1}) + \cdots + \operatorname{cdim}(D_{p_r}).$$

Note that this generalizes Conjecture 8.7: Let A be a central division F-algebra of degree $n = p_1^{a_1} \cdots p_r^{a_r}$, where p_i are distinct prime numbers and a_i are non-negative integers. Recall that A can be written as $A_i \otimes \cdots \otimes A_r$ where A_i is a central division F-algebra of degree $p_i^{a_i}$. Then $\langle [A_i] \rangle$, the cyclic subgroup in $Br(F)$ generated by $[A_i]$ the class of A_i, is the Sylow p_i-subgroup of $\langle [A] \rangle$ for every i. This follows from the fact that the period and the index of any central simple algebra have the same prime divisors. Since $\operatorname{cdim}(\langle [A] \rangle) = \operatorname{cdim}(SB(A))$ and $\operatorname{cdim}(\langle [A_i] \rangle) = p_i^{a_i} - 1$ for every i, we recover Conjecture 8.7.

Theorem 11.4. *Let G be a finite abstract abelian group with the above decompositions. Let F be a field such that $char(F) \neq p_i$ and $\xi_{p_i} \in F$ for every i. If Conjecture 11.3 is valid, then*

$$\begin{aligned} \operatorname{ed}(G) &= \sum_{i=1}^{r} \sum_{j=1}^{s_i} \operatorname{ed}(\mathbb{Z}/p_i^{n_{i,j}}\mathbb{Z}) - \sum_{i=2}^{r} s_i \\ &= \sum_{i=1}^{r} \sum_{j=1}^{s_i} [F(\xi_{p_i^{n_{i,j}}}) : F] - \sum_{i=2}^{r} s_i. \end{aligned}$$

Proof. By Proposition 11.1 it suffices to prove that if Conjecture 11.3 is valid. then

$$\operatorname{ed}(G) \geq \sum_{i=1}^{r} \sum_{j=1}^{s_i} \operatorname{ed}(\mathbb{Z}/p_i^{n_{i,j}}\mathbb{Z}) - \sum_{i=2}^{r} s_i.$$

Let $C = \prod_{j=1}^{s_1} \mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \prod_{j=1}^{s_r} \mathbb{Z}/p_r\mathbb{Z}$ be a subgroup of G, and set $H = G/C$. Let $E \to Spec(L)$ be a generic H-torsor for some field extension L/F. Recall that we have a homomorphism $\beta^E : C^* \to Br(L)$, where C^* is the character group of C.

Consider the fibered category E/G. Since $\xi_{p_i} \in F$ for every i, $H^2(L, C)$ can be identified with $Br_{p_1}(L)^{s_1} \times \cdots \times Br_{p_r}(L)^{s_r}$. Then $\theta(E/G) \in H^2(L, C)$ can be represented by central simple L-algebras $A_{i,j}$ with $[A_{i,j}] \in Br_{p_i}(L)$ for $1 \leq i \leq r,\ 1 \leq j \leq s_i$. Note that $\operatorname{im}(\beta^E)$ is generated by all the $[A_{i,j}]$, hence the class of splitting fields of E/G is equal to that of $\operatorname{im}(\beta^E)$, and in particular

$$\operatorname{cdim}_L(E/G) = \operatorname{cdim}_L(\operatorname{im}(\beta^E)).$$

Since C is isomorphic to $\mu_{m_1} \times \cdots \times \mu_{m_s}$, where $m_i = p_1 \cdots p_{a_i}$, by Theorem 9.3 and Theorem 9.8 we get

$$\operatorname{ed}(G) \geq \operatorname{ed}_L(G) \geq \operatorname{ed}_L(E/G) = \operatorname{cdim}_L(E/G) + s = \operatorname{cdim}_L(\operatorname{im}(\beta^E)) + s. \qquad (11.9)$$

Let $C_i = \prod_{j=1}^{s_i} \mathbb{Z}/p_i\mathbb{Z}$ and $H_i = G_i/C_i$ for every i, which we recall that G_i is the Sylow p_i-subgroup of G. Then $H = H_1 \times \cdots \times H_r$. Let $E_i = E/\prod_{j\neq i} H_j$ be the categorical quotient, then $E_i \to \operatorname{Spec} L$ is an H_i-torsor.

Claim: $E_i \to \operatorname{Spec} L$ is a generic H_i-torsor.

Let $E \to \operatorname{Spec} L$ be the generic fiber of a classifying H-torsor $f : X \to Y$. Let $J \to \operatorname{Spec} K$ be any H_i-torsor for some field extension K/F with K infinite. Since the morphism $H^1(K, H) \to H^1(K, H_i)$ is surjective, J is equal to the quotient $I/\prod_{j\neq i} H_j$ for some H-torsor $I \to \operatorname{Spec} K$. Note that $I \to \operatorname{Spec} K$ is the pullback of f with respect to a K-point of Y because f is classifying. It follows that $J \to \operatorname{Spec} K$ is the pullback of $f_i : X/\prod_{j\neq i} H_j \to Y$ with respect to a K-point of Y, hence f_i is a classifying H_i-torsor. Therefore $E_i \to \operatorname{Spec} L$ is a generic H_i-torsor as it is the generic fiber of f_i, proving the claim.

For every $\chi_i \in C_i^*$, χ_i is the restriction of χ to C_i for some $\chi \in C^*$. We have the following commutative diagram

$$\begin{tikzcd}
H^1(L,H) \arrow[r, "\partial_L"] \arrow[d] & H^2(L,C) \arrow[r, "\chi"] \arrow[d] & Br(L) \arrow[d] \\
H^1(L,H_i) \arrow[r, "\partial_L"] & H^2(L,C_i) \arrow[r, "\chi_i"] & Br(L)
\end{tikzcd}$$

where the vertical homomorphisms are the canonical homomorphisms, and $E \mapsto E_i$ under the first vertical homomorphism. Hence $\operatorname{im}\beta^{E_i}$ is generated by $[A_{i,j}]$, $1 \leq j \leq s_i$. It follows that $\operatorname{im}\beta^{E_i}$ is the Sylow p_i-subgroup of $\operatorname{im}\beta^{E}$ for every i, thus by Conjecture 11.3

$$\operatorname{cdim}_L(\operatorname{im}\beta^{E}) = \operatorname{cdim}_L(\operatorname{im}\beta^{E_1}) + \cdots + \operatorname{cdim}_L(\operatorname{im}\beta^{E_r}).$$

We know from the proof of [15, Theorem 4.1] that

$$\operatorname{cdim}_L(\operatorname{im}\beta^{E_i}) = \sum_{j=1}^{s_i} \operatorname{ed}(\mathbb{Z}/p_i^{n_{i,j}}\mathbb{Z}) - s_i$$

for every i. Therefore together with (11.9) we get

$$\begin{aligned}\operatorname{ed}(G) \geq \operatorname{cdim}_L(\operatorname{im}(\beta^{E})) + s &= \sum_{i=1}^{r}\left(\sum_{j=1}^{s_i} \operatorname{ed}(\mathbb{Z}/p_i^{n_{i,j}}\mathbb{Z}) - s_i\right) + s \\ &= \sum_{i=1}^{r}\sum_{j=1}^{s_i} \operatorname{ed}(\mathbb{Z}/p_i^{n_{i,j}}\mathbb{Z}) - \sum_{i=2}^{r} s_i.\end{aligned}$$

□

CHAPTER 12

Essential Dimension of Small Groups over $\mathbb{Q}$

In this chapter we study the essential dimension of finite abstract groups of small order. We are particularly interested in the case when our base field is $\mathbb{Q}$ because the essential dimension of finite abstract groups over $\mathbb{Q}$ is related to the inverse Galois problem via the study of generic polynomials (see [12]).

First we recall from Remark 6.12 (3) that given a classifying G-torsor $X \to Y$, we have

$$\mathrm{ed}(G) = d - \dim(G)$$

where $d = \min\{\dim(X')\}$ over all generically free G-scheme X' with a G-equivariant dominant rational morphism $X \dashrightarrow X'$. Let G be a finite abstract group, so $\dim(G) = 0$. By Proposition 5.6 and Proposition 5.9, any faithful representation of G on a finite dimensional F-vector space V gives a classifying G-torsor $U \to U/G$, where U is a friendly open subscheme of $\mathbb{A}(V)$. Then a G-equivariant dominant rational morphism $U \dashrightarrow X'$ from U to a generically free G-scheme X' corresponds to a subfield $K \subseteq F(V)$ on which G acts faithfully. Therefore we have the following result.

Proposition 12.1. *Let G be a finite abstract group, and let V be a finite dimensional faithful representation of G over F. Then*

$$\mathrm{ed}(G) = \min\{tr.deg_F(K)\}$$

where the minimum is taken over all subfields K of $F(V)$ over F on which G acts faithfully.

By using Proposition 12.1 we are able to provide a simple proof to the following lemma.

Lemma 12.2. *Let G be a finite abstract group. If $\mathrm{ed}(G) = 1$, then G is isomorphic to a subgroup of $\boldsymbol{PGL}_2(F)$.*

Proof. Let V be a finite dimensional faithful representation of G over F. If $\mathrm{ed}(G) = 1$, then there is a subextension $F \subseteq K \subseteq F(V)$ such that $tr.deg_F(K) = 1$ and G acts faithfully on K. Since $F(V)$ is rational, by Lüroth's theorem K is rational. Therefore K is isomorphic to $F(t)$ where t is an indeterminate. As G acts faithfully on $F(t)$, it follows that G is isomorphic to a subgroup of $\mathrm{Aut}(F(t)) = \mathbf{PGL}_2(F)$. □

Our goal is to study the essential dimension of groups of order less than or equal to 15. First, it is obvious that for the trivial group $\{e\}$, $\mathrm{ed}(\{e\}) = 0$ over any field. Next, since $\mathbb{Q}$ contains -1, the essential dimension of 2-groups over $\mathbb{Q}$ is computed by Theorem 7.1. For $\mathbb{Z}/3\mathbb{Z}$, we have the following result.

Proposition 12.3. $\mathrm{ed}(\mathbb{Z}/3\mathbb{Z}) = 1$ *over any field* F.

Proof. If $char(F) = 3$, then $\mathrm{ed}(\mathbb{Z}/3\mathbb{Z})$ is computed in Example 3.4.

If $char(F) \neq 3$, notice that the matrix $M = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \in \mathbf{GL}_2(F)$ has order 3, and the class of M in $\mathbf{PGL}_2(F)$ also has order 3. Therefore $\mathrm{ed}(\mathbb{Z}/3\mathbb{Z}) \leq 1$ by Corollary 6.14. □

Next we study the symmetric groups.

Proposition 12.4. *Let* $char(F) \neq 2$, *then*

$$\mathrm{ed}(S_n) \leq \begin{cases} n-2, & \text{if } n = 3, 4 \\ n-3, & \text{if } n \geq 5. \end{cases}$$

Proof. First we note that the natural action of S_n on the hyperplane

$$H = \{(x_1, \dots, x_n) \in \mathbb{A}^n : x_1 + \cdots + x_n = 0\}$$

is faithful, hence S_n acts faithfully on $F(x_1, \dots, x_{n-1})$. Consider the subfield

$$K = F\left(\frac{x_1}{x_{n-1}}, \dots, \frac{x_{n-2}}{x_{n-1}}\right) \subseteq F(x_1, \dots, x_{n-1}).$$

If $n \geq 3$, the induced action of S_n on K remains faithful. Therefore

$$\mathrm{ed}(S_n) \leq tr.deg_F(K) = n - 2.$$

Suppose $n \geq 5$. Consider the field $F(x_1, \ldots, x_n)$ with the natural S_n-action. Let

$$[x_i, x_j, x_k, x_l] = \frac{(x_i - x_k)(x_j - x_l)}{(x_j - x_k)(x_i - x_l)}$$

for distinct i, j, k, l. Denote by K the subfield generated by all the $[x_i, x_j, x_k, x_l]$ with i, j, k, l all distinct. Since we assume $n \geq 5$, every non-trivial element of S_n moves at least one of the $[x_i, x_j, x_k, x_l]$. Hence the action of S_n on K is faithful. Finally, note that K can be generated by $[x_1, x_2, x_3, x_i]$ with $i = 4, \ldots, n$, so there exists a natural isomorphism $K \xrightarrow{\cong} F(y_4, \ldots, y_n)$ where y_i are indeterminates. It follows that

$$\mathrm{ed}(S_n) \leq tr.deg_F(K) = n - 3. \qquad \square$$

Example 12.5.

(1) Combining the results from Proposition 12.4 and Corollary 6.17, we have

$$\mathrm{ed}(S_3) = 1, \;\; \mathrm{ed}(S_4) = \mathrm{ed}(S_5) = 2, \;\; \mathrm{ed}(S_6) = 3$$

if $char(F) \neq 2$.

(2) Let $F = \mathbb{Q}$. Since $\mathbb{Z}/5\mathbb{Z}$ is a subgroup of S_5, it follows from Theorem 6.15 that $\mathrm{ed}(\mathbb{Z}/5\mathbb{Z}) \leq \mathrm{ed}(S_5) = 2$. By Lemma 12.2 we see that $\mathrm{ed}(\mathbb{Z}/5\mathbb{Z}) \neq 1$, hence $\mathrm{ed}(\mathbb{Z}/5\mathbb{Z}) = 2$.

Similarly, as A_4 is a subgroup of S_4 but not a subgroup of $\mathbf{PGL}_2(\mathbb{Q})$, we have $\mathrm{ed}(A_4) = 2$.

Before continuing the study on essential dimension, we prove two technical lemmas that will be needed shortly.

Lemma 12.6. *Let K/F be a field extension, and let v be a discrete valuation on K with residue field L. Also, let $\sigma \in \mathrm{Aut}_F K$ have finite order not divisible by $char(F)$. Assume that v is trivial on F and invariant under σ. Then σ is the identity on K if and only if it induces the identity on both L and $\mathfrak{m}_v/\mathfrak{m}_v^2$.*

Proof. The "only if" part is clear. For the "if" part, the assumptions mean $\sigma x - x \in \mathfrak{m}_v$ for every x in the valuation ring R of v, and $\sigma x - x \in \mathfrak{m}_v^2$ for every $x \in \mathfrak{m}_v$. By induction $\sigma x - x \in \mathfrak{m}_v^{n+1}$ for every n and every $x \in \mathfrak{m}_v^n$.

Suppose σ is not the identity on K. Then there exists $x \in R$ such that $y = \sigma x - x \neq 0$. Let $n = v(y)$. Then $\sigma y - y \in \mathfrak{m}_v^{n+1}$, and $\sigma^j x = x + jy \pmod{\mathfrak{m}_v^{n+1}}$ for every j. Therefore we get a contradition by taking j to be the order of σ. □

Let K/F be a field extension, $char(F) = 0$, and let v be a discrete valuation on K with residue field L. Let G be a finite subgroup of $\mathrm{Aut}_F K$ such that v is G-invariant. Assume that v is trivial on F. For every $\sigma \in G$, σ defines by passage to the quotient an F-automorphism of L. Therefore we obtain a homomorphism

$$\varphi : G \longrightarrow Aut_F L\ .$$

The kernel of φ is called the inertia group I for v.

Lemma 12.7. *Assume that F is relatively algebraically closed in L. Then I is a central cyclic subgroup of G and is isomorphic to a group of roots of unity in F.*

Proof. Since I acts trivially on L, by the previous lemma an element $\tau \in I$ is determined completely by its action on $\mathfrak{m}_v/\mathfrak{m}_v^2$. As $\mathfrak{m}_v/\mathfrak{m}_v^2$ is a one-dimensional vector space over L, τ acts as multiplication by a root of unity $\xi(\tau) \in F$. Therefore I is cyclic, and for every $\tau \in I$ and every $\sigma \in G$ we have $\xi(\sigma\tau\sigma^{-1}) = \sigma\xi(\tau)$. Note that $\xi(\tau) \in F$ as F is relatively algebraically closed in L. Hence $\xi(\sigma\tau\sigma^{-1}) = \xi(\tau)$, meaning that conjugation with elements from G acts trivially on I. Therefore I is central in G. □

We are ready to prove the following theorem.

Theorem 12.8. *Let p be a prime number, and let G be a finite abstract group. Let F be a field such that $char(F) = 0$, $\xi_p \in F$, and $\xi_q \notin F$ for any prime $q \neq p$ dividing $|Z(G)|$ the order of the center of G. Then*

$$\mathrm{ed}(G \times \mathbb{Z}/p\mathbb{Z}) = \mathrm{ed}(G) + 1.$$

Proof. By Lemma 2.7 and Example 3.4 we have

$$\mathrm{ed}(G \times \mathbb{Z}/p\mathbb{Z}) \leq \mathrm{ed}(G) + \mathrm{ed}(\mathbb{Z}/p\mathbb{Z}) = \mathrm{ed}(G) + 1.$$

For the other inequality, let V be a finite dimensional faithful representation of G over F. It induces a faithful representation of $G \times \mathbb{Z}/p\mathbb{Z}$ on the vector space $V \oplus F$, with $\overline{1} \in \mathbb{Z}/p\mathbb{Z}$ acting on F by $x \mapsto \xi_p x$. The corresponding faithful action on $F(V)(t)$, where t is an indeterminate, is given by $\overline{1} \cdot (t) = \xi_p t$. Let $F \subseteq K \subseteq F(V)(t)$ be a subextension such that $tr.deg_F(K) = \mathrm{ed}(G \times \mathbb{Z}/p\mathbb{Z})$, and $G \times \mathbb{Z}/p\mathbb{Z}$ acts faithfully on K. Let v be the t-adic valuation on $F(V)(t)$, and let R be the corresponding valuation ring. Note that for every $\sigma \in G \times \mathbb{Z}/p\mathbb{Z}$, we have $v = v \circ \sigma$ which implies that the residue homomorphism $R \to F(V)$ respects the $G \times \mathbb{Z}/p\mathbb{Z}$-action.

Let v' be the restriction of v on K.

Claim: v' is non-trivial.

Suppose v' is trivial, then $K \subseteq R$ and there exists a field homomorphism $K \hookrightarrow F(V)$ which respects the $\mathbb{Z}/p\mathbb{Z}$-action. Since $\mathbb{Z}/p\mathbb{Z}$ acts trivially on $F(V)$ but non-trivially on K, we get a contradiction.

Let $L \subseteq F(V)$ be the residue field of v'. Since v' is non-trivial, by [26, Chapter VI, Theorem 3, Corollary 1], we have

$$tr.deg_F(L) \leq tr.deg_F(K) - 1 = \mathrm{ed}(G \times \mathbb{Z}/p\mathbb{Z}) - 1.$$

Finally we claim that G acts faithfully on L. Suppose not. Then the inertia group I for v' contains $\mathbb{Z}/p\mathbb{Z}$ properly, and by Lemma 12.7 I is a central cyclic subgroup of $G \times \mathbb{Z}/p\mathbb{Z}$. This implies that $I \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ for some $m > 1$ where p does not divide m. By Lemma 12.7, I is isomorphic to a group of roots of unity in F, and this contradicts our assumption on F.

As G acts faithfully on $L \subseteq F(V)$, it follows that

$$\mathrm{ed}(G) \leq tr.deg_F(L) \leq \mathrm{ed}(G \times \mathbb{Z}/p\mathbb{Z}) - 1. \qquad \square$$

Corollary 12.9. *Let $F = \mathbb{Q}$, and let G be any finite abstract group. Then*

$$\mathrm{ed}(G \times \mathbb{Z}/2\mathbb{Z}) = \mathrm{ed}(G) + 1.$$

By using the same technique in the proof of Theorem 12.8, we have the following result.

Theorem 12.10. *Let G be a finite abstract group. Let F be a field such that $char(F) = 0$, and $\xi_p \notin F$ for $p = 3$ and for any prime p dividing $|Z(G)|$. Then*

$$\mathrm{ed}(G \times \mathbb{Z}/3\mathbb{Z}) = \mathrm{ed}(G) + 1.$$

Proof. Again we only need to prove $\mathrm{ed}(G\times\mathbb{Z}/3\mathbb{Z}) \geq \mathrm{ed}(G)+1$. Let V be a finite dimensional faithful representation of G over F. Consider the faithful $G \times \mathbb{Z}/3\mathbb{Z}$-action on $F(V)(t)$ with $\overline{1} \in \mathbb{Z}/3\mathbb{Z}$ acting by $\overline{1} \cdot t = \frac{t-1}{t}$. Note that this action does not come from a linear representation, instead it is induced by a linear generically free action on $\mathbb{A}(V) \oplus \mathbb{P}^1$. Since it also gives a classifying torsor, the argument for Proposition 12.1 can be applied here.

Let $F \subseteq K \subseteq F(V)(t)$ be a subextension such that $tr.deg_F(K) = \mathrm{ed}(G \times \mathbb{Z}/3\mathbb{Z})$, and $G \times \mathbb{Z}/3\mathbb{Z}$ acts faithfully on K. Let v be the t-adic valuation on $F(V)(t)$, and let v' be the restriction of v on K.

Claim: v' is non-trivial.

Since $\mathbb{Z}/3\mathbb{Z}$ acts faithfully on K, there exists $\frac{f(t)}{g(t)} \in K \subseteq F(V)(t)$ such that $f(t), g(t) \in F(V)[t]$ are coprime, and $\frac{f(t)}{g(t)} \notin F(V)$. Let $f(t) = a_n t^n + \ldots + a_0$ and $g(t) = b_m t^m + \ldots + b_0$ where $a_n, b_m \neq 0$.

(i) If $a_0 = 0$ or $b_0 = 0$, then clearly $v(\frac{f(t)}{g(t)}) \neq 0$.

(ii) If $a_0, b_0 \neq 0$, consider

$$\overline{1} \cdot (\frac{f(t)}{g(t)}) = f(\frac{t-1}{t})/g(\frac{t-1}{t}) = \frac{t^m(a_n(t-1)^n + \ldots + a_0 t^n)}{t^n(b_m(t-1)^m + \ldots + b_0 t^m)}.$$

(a) If $\deg f(t) = n \neq m = \deg g(t)$, then $v(\overline{1} \cdot (\frac{f(t)}{g(t)})) \neq 0$.

(b) If $n = m$, by multiplying $\frac{b_n}{a_n}$ to $\frac{f(t)}{g(t)}$ we may assume $a_n = b_n$. Then $1 - \frac{f(t)}{g(t)} = \frac{g(t)-f(t)}{g(t)} \in K$, $g(t) - f(t) \neq 0$ and $\deg(g(t) - f(t)) < \deg g(t)$. Therefore we can apply the previous cases, and this proves the claim.

Let $L \subseteq F(V)$ be the residue field of v'. Since v' is non-trivial, by [26, Chapter VI, Theorem 3, Corollary 1], we get

$$tr.deg_F(L) \leq tr.deg_F(K) - 1 = \mathrm{ed}(G \times \mathbb{Z}/3\mathbb{Z}) - 1.$$

The last step again is to show that G acts faithfully on L. Suppose not. Since v' is G-invariant, the inertia group $I \subseteq G$ for v' is non-trivial. By Lemma 12.7 I is a central cyclic subgroup of G and is isomorphic to a group of roots of unity in F. Therefore our assumption on F gives a contradiction. As a result,

$$\mathrm{ed}(G) \leq tr.deg_F(L) \leq \mathrm{ed}(G \times \mathbb{Z}/3\mathbb{Z}) - 1. \qquad \square$$

Remark 12.11.

(1) Let G be a finite abstract group. Let F be a field such that $char(F) = 0$, and $\xi_p \notin F$ for any prime p dividing $|Z(G)|$. By the same proof of Theorem 12.10, we have

$$\mathrm{ed}(G \times S_3) = \mathrm{ed}(G) + 1.$$

To prove this we just need to note that S_3 has a faithful action on $F(t)$, where t is an indeterminate, given by $(12) \cdot t = \frac{1}{t}, (13) \cdot t = -t - 1, (23) \cdot t = -\frac{t}{t+1}$.

(2) The condition in Theorem 12.10 about $\xi_p \notin F$ for any prime p dividing $|Z(G)|$ is necessary. For example, over $\mathbb{Q}(\sqrt{3})$ which clearly contains -1,

$$\mathrm{ed}(\mathbb{Z}/12\mathbb{Z}) = 2 \neq \mathrm{ed}(\mathbb{Z}/4\mathbb{Z}) + \mathrm{ed}(\mathbb{Z}/3\mathbb{Z}) = 3.$$

This can be proved by observing that $\begin{pmatrix} \sqrt{3} & 1 \\ -1 & 0 \end{pmatrix}$ has order 12 in $\mathbf{GL}_2(\mathbb{Q}(\sqrt{3}))$.

For semidirect products, there is the following upper bound given by C. U. Jensen, A. Ledet and N. Yui in [12].

Theorem 12.12. *Let $F = \mathbb{Q}$, $q = p^n$ a prime power, and let φ be the Euler's totient function. Then*

$$\mathrm{ed}(\mathbb{Z}/q\mathbb{Z} \rtimes (\mathbb{Z}/q\mathbb{Z})^{\times}) \leq \varphi(p-1)p^{n-1}.$$

Example 12.13. Let $F = \mathbb{Q}$.

(1) Note that both $\mathbb{Z}/7\mathbb{Z}$ and the dihedral group D_7 are subgroups of $\mathbb{Z}/7\mathbb{Z} \rtimes (\mathbb{Z}/7\mathbb{Z})^\times$, where $\mathrm{ed}(\mathbb{Z}/7\mathbb{Z} \rtimes (\mathbb{Z}/7\mathbb{Z})^\times) \leq \varphi(6) = 2$. It follows from Theorem 6.15 and Lemma 12.2 that

$$\mathrm{ed}(\mathbb{Z}/7\mathbb{Z}) = \mathrm{ed}(D_7) = 2.$$

Similarly, by taking $q = 5$ we have $\mathrm{ed}(D_5) = 2$.

(2) By taking $q = 9$ we see that $\mathrm{ed}(\mathbb{Z}/9\mathbb{Z}) \leq \mathrm{ed}(\mathbb{Z}/9\mathbb{Z} \rtimes (\mathbb{Z}/9\mathbb{Z})^\times) \leq 3$. For the lower bound, we apply Proposition 2.4 and Corollary 7.2:

$$\mathrm{ed}_{\mathbb{Q}}(\mathbb{Z}/9\mathbb{Z}) \geq \mathrm{ed}_{\mathbb{Q}(\xi_3)}(\mathbb{Z}/9\mathbb{Z}) = 3.$$

We gather here the remaining known cases.

Example 12.14. Let $F = \mathbb{Q}$.

(1) By Lemma 2.7 and Proposition 12.3,

$$\mathrm{ed}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \leq \mathrm{ed}(\mathbb{Z}/3\mathbb{Z}) + \mathrm{ed}(\mathbb{Z}/3\mathbb{Z}) = 2.$$

To show that $\mathrm{ed}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) = 2$, we can apply Lemma 12.2.

(2) Consider the dihedral group $D_6 = \langle r, s : r^6 = s^2 = e, s^{-1}rs = r^{-1}\rangle$. Then

$$\begin{aligned} D_6 &\longrightarrow \mathbf{GL}_2(\mathbb{Q}) \\ r &\longmapsto \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \\ s &\longmapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

is a faithful representation of D_6. Hence $\mathrm{ed}(D_6) = 2$.

The following table summarizes our results.

$\|G\|$	G	$\mathrm{ed}_{\mathbb{Q}}(G)$	Reference
1	$\{e\}$	0	
2	$\mathbb{Z}/2$	1	
3	$\mathbb{Z}/3$	1	Proposition 12.3
4	$\mathbb{Z}/4$	2	Corollary 7.2
	$\mathbb{Z}/2 \times \mathbb{Z}/2$	2	
5	$\mathbb{Z}/5$	2	Example 12.5
6	$\mathbb{Z}/6$	2	Theorem 12.8
	S_3	1	Example 12.5
7	$\mathbb{Z}/7$	2	Example 12.13
8	$\mathbb{Z}/8$	4	Corollary 7.2
	$\mathbb{Z}/4 \times \mathbb{Z}/2$	3	
	$\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$	3	
	D_4	2	Theorem 7.1
	Q_8	4	
9	$\mathbb{Z}/9$	3	Example 12.13
	$\mathbb{Z}/3 \times \mathbb{Z}/3$	2	Example 12.14
10	$\mathbb{Z}/10$	3	Theorem 12.8
	D_5	2	Example 12.13
11	$\mathbb{Z}/11$		
12	$\mathbb{Z}/12$		
	$\mathbb{Z}/6 \times \mathbb{Z}/2$	3	Theorem 12.8
	A_4	2	Example 12.5
	D_6	2	Example 12.14
	$\mathbb{Z}/3 \rtimes \mathbb{Z}/4$		
13	$\mathbb{Z}/13$		
14	$\mathbb{Z}/14$	3	Theorem 12.8
	D_7	2	Example 12.13
15	$\mathbb{Z}/15$	3	Theorem 12.10

Bibliography

[1] G. Berhuy and G. Favi. Essential dimension: a functorial point of view (after A. Merkurjev). *Documenta Math.*, 8:279–330, 2003.

[2] G. Berhuy and Z. Reichstein. On the notion of canonical dimension for algebraic groups. *Advances in Mathematics*, 198(1):128–171, 2005.

[3] P. Brosnan, Z. Reichstein, and A. Vistoli. Essential dimension and algebraic stacks. arXiv:math/0701903v1 [math.AG], 2007.

[4] J. Buhler and Z. Reichstein. On the essential dimension of a finite group. *Compositio Mathematica*, 106(2):159–179, 1997.

[5] J.-L. Colliot-Thélène, N. A. Karpenko, and A. S. Merkurjev. Rational surfaces and canonical dimension of pgl6. *Algebra i Analiz*, 19(5):159–178, 2007. Translation in St. Petersburg Math. J. 19 (2008), no. 5, 793-804.

[6] M. Demazure and P. Gabriel. *Groupes algébriques, Tome I.* Ed. Masson & Cie, Paris, 1970.

[7] M. Demazure and A. Grothendieck. *Schémas en Groupes I, Propriétés générales des schémas en groupes SGA 3*, volume 151 of *Lecture Notes in Mathematics*. Springer-Verlag, New York, 1970.

[8] B. Fantechi, L. Göttsche, L. Illusie, S. L. Kleiman, N. Nitsure, and A. Vistoli. *Fundamental Algebraic Geometry: Grothendieck's FGA Explained*, volume 123 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2005.

[9] M. Florence. On the essential dimension of cyclic p-groups. *Inventiones Mathematicae*, 171:175–189, 2008.

[10] S. Garibaldi, A. S. Merkurjev, and J.-P. Serre. *Cohomological Invariants in Galois Cohomology*, volume 28 of *University Lecture Series*. American Mathematical Society, Providence, RI, 2003.

[11] P. Gille and T. Szamuely. *Central Simple Algebras and Galois Cohomology*, volume 101 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, New York, 2006.

[12] C. U. Jensen, A. Ledet, and N. Yui. *Generic Polynomials*, volume 45 of *Mathematical Sciences Research Institute Publications*. Cambridge University Press, Cambridge, 2002.

[13] N. A. Karpenko. Canonical dimension. In *Proceedings of The International Congress of Mathematicians 2010 (ICM 2010)*, volume 2, pages 146–161. World Scientific, New Jersey, 2011.

[14] N. A. Karpenko and A. S. Merkurjev. Canonical p-dimension of algebraic groups. *Advances in Mathematics*, 205(2):410–433, 2006.

[15] N. A. Karpenko and A. S. Merkurjev. Essential dimension of finite p-groups. *Inventiones Mathematicae*, 172(3):491–508, 2008.

[16] M.-A. Knus, A. S. Merkurjev, M. Rost, and J.-P. Tignol. *The Book of Involutions*, volume 44 of *Colloquium Publications*. American Mathematical Society, Providence, RI, 1998.

[17] R. Lötscher. Application of multihomogeneous covariants to the essential dimension of finite groups. *Transformation Groups*, 15(3):611–623, 2010.

[18] A. S. Merkurjev. Essential p-dimension of finite groups. http://www.math.ucla.edu/~merkurev/papers/lens08.dvi, 2008. Notes of mini-course in Lens.

[19] A. S. Merkurjev. Essential dimension. In *Quadratic Forms - Algebra, Arithmetic, and Geometry*, volume 493 of *Contemporary Mathematics*, pages 299–325. American Mathematical Society, Providence, RI, 2009.

[20] J. S. Milne. *Etale Cohomology*, volume 33 of *Princeton Mathematical Series*. Princeton University Press, New Jersey, 1980.

[21] Z. Reichstein. Essential dimension. In *Proceedings of The International Congress of Mathematicians 2010 (ICM 2010)*, volume 2, pages 162–188. World Scientific, New Jersey, 2011.

[22] J.-P. Serre. *Linear Representations of Finite Groups*, volume 42 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1977.

[23] J.-P. Serre. *Galois Cohomology*. Springer Monographs in Mathematics. Springer-Verlag, New York, corrected 2nd edition, 2002. Translated by Patrick Ion.

[24] W. C. Waterhouse. *Introduction to Affine Group Schemes*, volume 66 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979.

[25] W. Wong. On the essential dimension of cyclic groups. *Journal of Algebra*, 334(1):285–294, 2022.

[26] O. Zariski and P. Samuel. *Commutative Algebra Volume II*, volume 29 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1976.