



INSTITUT DE MATHÉMATIQUES

Essential dimension: A functorial point of view

Thèse de doctorat

présentée à la

Faculté des Sciences
de l'Université de Lausanne

par

Giordano Favi

Diplômé en Mathématiques
de l'Université de Lausanne

Jury

M. le Prof. Jean Hernandez, président
M. le Prof. Manuel Ojanguren, directeur de thèse
M. le Prof. Paul Balmer, expert
Mme. la Prof. Parimala Raman, experte
Mme. la Prof. Donna Testerman, experte
M. le Prof. Jacques Thévenaz, expert

LAUSANNE
2003

Essential dimension:
A functorial point of view

Thèse de doctorat

présentée à la

Faculté des Sciences
de l'Université de Lausanne

par

Giordano Favi

Diplômé en Mathématiques
de l'Université de Lausanne

LAUSANNE
2003

Imprimatur

Vu le rapport présenté par le jury d'examen, composé de

| | | |
|--------------------|----------------|------------------|
| Président | Monsieur Prof. | Jean Hernandez |
| Directeur de thèse | Monsieur Prof. | Manuel Ojanguren |
| Rapporteur | | |
| Experts | Madame Prof. | Parimala Raman |
| | Madame Prof. | Donna Testermann |
| | Monsieur Prof. | Jacques Thévenaz |
| | Monsieur Prof. | Paul Balmer |

le Conseil de Faculté autorise l'impression de la thèse de

Monsieur Giordano Favi

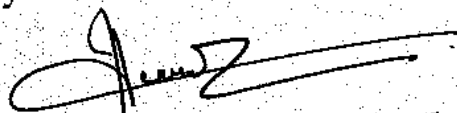
Mathématicien diplômé de l'Université de Lausanne

intitulée

**Essential dimension:
A functorial point of view**

Lausanne, le 8 décembre 2003

Le Doyen de la Faculté des Sciences



Prof. Jean Hernandez

*“Reddite ergo quae sunt Caesaris Caesari
et quae sunt Dei Deo”*

Matthew 22 : 21

*“The Rediscovery of the Scientific Geometric Point
is a Reality for that It Exists, recorded internation-
ally and copyrighted under my name”*

Ion Vulcanescu, Philosopher

CONTENTS

| | |
|--|------|
| Abstract | vii |
| Résumé | ix |
| Riassunto | xi |
| Remerciements | xiii |
| Summary | xv |
| Chapter I. Introduction | 1 |
| 1. Historical survey | 1 |
| 2. Definitions | 5 |
| Chapter II. Cohomological methods | 17 |
| 1. Galois cohomology | 17 |
| 2. Cohomological invariants | 23 |
| Chapter III. Actions, torsors and generic elements | 29 |
| 1. Free actions and torsors | 29 |
| 2. Versal pairs and Rost's definition | 39 |
| 3. Generic torsors and compressions | 42 |
| Chapter IV. Applications | 51 |
| 1. Some finite groups | 51 |
| 2. Homotopy invariance | 61 |
| Chapter V. Cubics | 65 |
| 1. Some considerations on cubics | 65 |
| 2. Galois descent for functors. Applications to cubics | 71 |
| 3. Essential dimension of non-singular cubics | 74 |
| 4. The case of singular cubics. | 79 |
| Bibliography | 85 |

ABSTRACT

In this work we develop a systematic study of the *essential dimension* of functors. This approach is due to A. Merkurjev and can be found in his unpublished notes [17].

The notion of essential dimension was earlier introduced for finite groups by J. Buhler and Z. Reichstein in [7] and for an arbitrary algebraic group over an algebraically closed field by Z. Reichstein in [19]. They also established the connection between essential dimension and Hilbert's 13th problem.

Merkurjev's approach made the study of this notion over an arbitrary field possible. The essential dimension of an algebraic group is a numerical invariant depending on the group G and the field k .

This number is denoted by $\text{ed}_k(G)$. It has many interpretations and reformulates properly the notion of "how many parameters are needed to describe a given structure".

In the present work we insist on the behaviour of the essential dimension under field extension k'/k and try to compute $\text{ed}_k(G)$ for *any* k . This will be done in particular for the group \mathbb{Z}/n when $n \leq 5$ and for the circle group.

Along the way we define the essential dimension of functors with versal pairs, following Rost, and prove that all the different notions of essential dimension agree in the case of algebraic groups.

Applications to finite groups are given. We also give a proof of the so-called *homotopy invariance*, that is $\text{ed}_k(G) = \text{ed}_{k(t)}(G)$, for an algebraic group G over an infinite field k .

Finally a whole chapter is dedicated to the computation of the essential dimension of cubics in three variables which is one of the main results of this work.

RÉSUMÉ

Dans ce mémoire, nous développons de manière systématique la notion de *dimension essentielle* d'un foncteur. Cette approche est due à A. Merkurjev. On peut la trouver dans ses notes non publiées [17] qui sont pratiquement introuvables.

Cette notion a été originellement introduite pour des groupes finis par J. Buhler et Z. Reichstein dans [7]. Ils ont également établi le lien entre la dimension essentielle et le 13ème problème de Hilbert. Quelques temps plus tard, la même notion pour un groupe algébrique quelconque sur un corps algébriquement clos a été étudiée par Z. Reichstein dans [19].

Grâce à Merkurjev, l'étude de cet objet a pu être envisagée sur un corps de base quelconque. La dimension essentielle d'un groupe algébrique est un invariant numérique qui dépend du groupe G et du corps k sur lequel G est défini.

Ce nombre sera noté par $\text{ed}_k(G)$ pour ne pas choquer les anglophones. Cette dimension essentielle possède plusieurs interprétations et a le bon goût de définir correctement la vague notion de "combien de paramètres faut-il pour décrire une structure donnée".

Dans le présent travail une priorité sera donnée à l'étude du comportement de la dimension essentielle par rapport à un changement de base k'/k et on tentera de calculer $\text{ed}_k(G)$ pour k quelconque. Pour des groupes comme \mathbb{Z}/n , avec $n \leq 5$, et pour le cercle S^1 ce but sera atteint.

Tout au long du travail nous définirons plusieurs notions parmi lesquelles la dimension essentielle *à la Rost* inspirée d'un article de ce dernier.

Des applications aux cas des groupes finis seront discutées également. Pour un groupe algébrique G sur un corps infini k on établira aussi l'invariance homotopique, c'est-à-dire $\text{ed}_k(G) = \text{ed}_{k(t)}(G)$.

Finalement un chapitre entier est consacré au calcul de la dimension essentielle des cubiques en trois variables. C'est un des principaux résultats obtenus dans ce travail.

RIASSUNTO

Nel presente lavoro sviluppiamo sistematicamente la nozione di *dimensione essenziale* di un funtore. Questo recente punto di vista è dovuto a A. Merkurjev. Lo si può trovare nei suoi appunti non pubblicati (vedi [17]) che peraltro sembrerebbe siano stati smarriti. Il testo originale è stato ormai dichiarato *testo sacro*.

Questa nozione è stata introdotta per la prima volta, nel caso dei gruppi finiti, da J. Buhler e Z. Reichstein nell'articolo [7]. Nel loro lavoro gli autori hanno collegato la dimensione essenziale al 13esimo problema di Hilbert. Un pò più tardi, Z. Reichstein in [19] estende questa stessa definizione a un gruppo algebrico qualunque, definito su un campo algebricamente chiuso.

Lo studio di questa nozione su un campo qualsiasi è stato possibile grazie a Merkurjev. La dimensione essenziale di un gruppo algebrico è un invariante numerico che dipende dal gruppo G e dal campo k sul quale G è definito.

Questo numero sarà abbreviato con $\text{ed}_k(G)$ per non sconcertare gli inglesi. Questa dimensione essenziale possiede diverse interpretazioni e dà una definizione precisa della nozione di “quanti parametri occorrono per descrivere una struttura data”.

Nel presente lavoro si studierà in modo accurato il comportamento della dimensione essenziale rispetto a un cambiamento di base k'/k e si cercherà di calcolare $\text{ed}_k(G)$ per un campo k qualunque. Per certi gruppi come \mathbb{Z}/n , per $n \leq 5$, e per il cerchio S^1 la risposta sarà completa.

Nel presente testo si tratteranno e si introdurranno diverse definizioni, tra le quali la dimensione essenziale *à la Rost* ispirata da un articolo di quest'ultimo.

Si discuterà a lungo anche di alcune applicazioni nel caso dei gruppi finiti. Un altro risultato ottenuto è la cosiddetta *invarianza omotopica* per un gruppo algebrico G su un campo infinito k , ovvero $\text{ed}_k(G) = \text{ed}_{k(t)}(G)$.

Per finire, un capitolo intero sarà consacrato al calcolo della dimensione essenziale delle cubiche in tre variabili. È uno dei risultati più importanti ottenuti in questo lavoro.

REMERCIEMENTS

Je remercie sincèrement Monsieur le Professeur Manuel Ojanguren de m'avoir savamment dirigé pendant ce travail de thèse. Ses conseils précis et géométriques, son goût raffiné et enfin ses questions pertinentes m'ont agréablement conduit au fil des pages. Ce fut un véritable plaisir que de travailler avec lui. Ces quelques pages lui sont dédiées.

Ma gratitude s'adresse également aux experts Madame le Professeur Donna Testerman et Monsieur le Professeur Jacques Thévenaz. Leurs remarques très pertinentes, leur relecture précise et leurs conseils rédactionnels m'ont été d'une aide précieuse.

I would also thank Professor Parimala for her kindness and her availability. I am honoured that she could read and appreciate my work.

Je tiens également à remercier le plus dithyrambiquement possible Monsieur l'expert Paul Balmer pour son œil acéré et son verbe tranchant. Sans sa présence et son souffle catégorique ce travail aurait été un peu diminué et la ptose maximale n'aurait sans doute jamais atteinte.

Je ne pourrai pas dormir tranquille sans avoir auparavant dûment remercié celui sans lequel ce travail aurait été amputé de son plus bel accomplissement : le calcul des cubiques. Je veux, bien entendu, parler de Grégory Berhuy, Docteur ès Mathématiques de l'Université de Besançon, avec lequel j'ai eu le plaisir d'exercer mes neurones durant près de deux ans de collaboration. Outre ses qualités mathématiques, diamétralement opposées aux miennes et donc complémentaires, sa pugnacité et son dévouement pour les calculs ont rendu possibles des perspectives que je n'aurais pu imaginer seul. Un grand merci donc à Grégory grâce à qui ce travail a aussi vu le jour, après une savante dichotomie, sous la forme d'une double publication.

Je tiens à exprimer également ma profonde gratitude envers l'inoubliable Institut de Mathématique de l'Université de Lausanne. Ses professeurs et ses assistants ont créé, au fil des ans, ce qui désormais restera une légende. Cette thèse est dédiée à Madame IMA.

En dernier lieu, je voudrais exprimer ma gratitude envers Monsieur le Professeur Jean-Pierre Serre pour avoir lu la totalité de ce texte. Sa compétence hors pair et ses remarques précises m'ont été d'une aide inestimable. Les questions pertinentes qu'il a su soulever vont sans nul doute stimuler la recherche dans la dimension essentielle et lui donner encore un souffle de vie pendant de nombreuses années.

SUMMARY

In Chapter I, after a brief account on the history of essential dimension, we introduce the notion of essential dimension of a covariant functor from the category of field extensions over a base field k to the category of sets. This point of view is due to A. Merkurjev and can be found in [17]. We then study the behaviour of this notion under products, coproducts and field extensions. Along the way, we define the notion of fibration of functors. This material will be frequently used in the sequel.

In Chapter II, we first introduce the essential dimension of an algebraic group G defined over an *arbitrary* field k . We then give some examples of computation of this essential dimension, including the case of the circle group.

The second section of Chapter II deals with Merkurjev's notions of n -simple functors and non-constant morphisms (see [17]). We apply it to give lower bounds of essential dimension of some algebraic groups (e.g. symmetric groups) using non-trivial cohomological invariants always following [17].

Chapter III emphasizes the point of view of group scheme actions on schemes and in particular on vector spaces. It also deals with versal elements and generic torsors. In Section 1 the notions of quotient schemes and G -torsors are freely used. We give an upper bound for the essential dimension of an algebraic group which acts linearly and generically freely on a finite-dimensional vector space. Compare this material with [19] where the essential dimension of G is defined taking the point of view of G -actions. Very sketchy proofs of these results can be found in [17]. For the convenience of the reader, we present complete proofs of them using the ideas of [17], filling in technical details. We then apply the previous results to estimate the essential dimension of finite abelian groups and dihedral groups when the base field is sufficiently large.

Section 2 of Chapter III is inspired by Rost's definition of essential dimension for some subfunctors of Milnor's K -theory (see [21]). We define there the notion of versal pair for functors from the category of commutative and unital k -algebras to the category of sets. We then define the (Rost's) essential dimension for functors having a versal pair, and compare it to Merkurjev's essential dimension.

In Section 3 of Chapter III, we introduce the notion of generic torsor, following [13]. We then prove that the essential dimension of an algebraic

group G is the essential dimension of a generic torsor. We also compare the essential dimension of an algebraic group G with that of any closed subgroup. Along the way the notion of compression of torsors is introduced following [19]. The present approach has the advantage that no hypothesis on the ground field is needed.

Chapter IV is concerned with some applications of the techniques previously developed. In Section 1 we focus on the essential dimension of finite constant group schemes. First of all, we prove that the essential dimension of such a group G is the minimum of the $\text{trdeg}(E : k)$ for all the fields $E \subseteq k(V)$ on which G acts faithfully (see [7]). We then apply these results to compute the essential dimension of cyclic and dihedral groups over real numbers, and the essential dimension of cyclic groups of order at most 6 over any base field.

As a second application, in Section 2 of Chapter IV, we give the proof of the homotopy invariance for essential dimension of algebraic groups over an infinite field, that is $\text{ed}_k(G) = \text{ed}_{k(t)}(G)$.

Finally, Chapter V talks about cubics. In this rather long chapter we compute the essential dimension of cubics in two and three variables. For cubics in three variables the computation is performed by reducing the problem to the computation of the essential dimension of some appropriate algebraic groups. This uses in particular canonical pencils of cubics and a Galois Descent Lemma for functors which could be useful for other future purposes.

CHAPTER I

INTRODUCTION

1. HISTORICAL SURVEY

All along the course of human history philosophers, geometers, musicians, pædiatricians, architects, mathematicians, politicians, biologists, psychoanalysts, chemists and others have tried to describe the problems they were facing in terms of *parameters*.

How many *parameters* are needed to describe a geometric object? Which are the *parameters* involved in a chemical reaction? Which *parameters* influence child growth?

One sees that the notion of *parameter* is central in the discussions of researchers whatever the field of research may be. Moreover, the way of “minimizing” the number of parameters occurring in a given situation seems to be of great interest.

Indeed it seems to be part of mathematical, and more generally of human reasonment to reduce a problem to smaller problems which are easily handled. It is maybe the “definition” of “scientific” thinking to reduce the number of parameters that describe a given “structure”. Since essential dimension deals with parameters and the way of minimizing them, it is relatively hard to trace back its history or to put a name on some possible ancestor.

However the birth of essential dimension in its actual form may be found in the obstination of mathematicians for the study of equations of the second, third or greater degree.

Among all the mathematicians and all mathematical schools (whose names I shall omit) that worked during centuries on the solutions of the general equation of order n , one name maybe should be cited in the prehistory of essential dimension: Ehrenfried Walter von Tschirnhaus.

Born in Kieslingswalde (Germany) in 1651, Tschirnhaus studied equations up to transforms which do not change the algebra generated by the solutions. Today these transforms are called Tschirnhaus transforms. He also gave a transformation which, when applied to an equation of

degree $n \geq 5$, gives an equation with no term in X^{n-1} and X^{n-2} . He also experimented making porcelain from clay mixed with fusible rock in the 1680's. There was great competition from governments to obtain his porcelain techniques but Tschirnhaus kept them for himself and ended his life deeply in debt. He died in Dresden on the 11th October 1708.

In order to have a better understanding of “minimizing parameters” we shall shortly explain this classical example of reducing an equation by means of non-degenerate Tschirnhaus transform.

That is, if $X^n + a_1X^{n-1} + \cdots + a_n = 0$ is an equation with coefficients in a field K the aim is to transform it (or to simplify it) with some substitution $X \rightsquigarrow r_{n-1}X^{n-1} + \cdots + r_1X + r_0$, where the r_i 's are rational functions in the coefficients a_i . One finds a new equation $X^n + b_1X^{n-1} + \cdots + b_n = 0$ and the purpose is to have fewer independent coefficients appearing in it. The operation consisting of the substitution $X \rightsquigarrow r_{n-1}X^{n-1} + \cdots + r_1X + r_0$ is called a Tschirnhaus transform. If f is the polynomial of the first equation and g that of the second one we shall say that g is a Tschirnhaus transform of f . Saying that this transform is non-degenerate, is nothing but saying that the K -algebras $K[X]/\langle f \rangle$ and $K[X]/\langle g \rangle$ are isomorphic.

So the problem is to reduce an equation, with the help of these transforms, to some form for which computations are easily performed and solutions are easily found.

For example, over the field \mathbb{Q} , the equation $X^2 + aX + b = 0$ is equivalent to $X^2 + c = 0$ for $c = -\frac{a^2}{4} + b$. This is done by setting $X \rightsquigarrow X - \frac{a}{2}$. This reflects the very well known fact that each quadratic extension of \mathbb{Q} is of the form $\mathbb{Q}(\sqrt{d})$. This is moreover clearly true for any field of characteristic not 2.

Equations of degree 3 like $X^3 + aX^2 + bX + c = 0$ are equivalent to $X^3 + b'X + c' = 0$ by putting $X \rightsquigarrow X - \frac{a}{3}$. The latter, by the scaling $X \rightsquigarrow \frac{c'X}{b'}$ (if $b' \neq 0$ of course), is then equivalent to $\frac{b'^3}{c'^3}X^3 + c'X + c' = 0$ which has the same solutions as $X^3 + dX + d = 0$ for a suitable d . The “degenerate” cases like $X^3 + a = 0$ are not dealt since they are not general enough. All these transform can be performed on some “generic” polynomial which covers almost all cases.

In both cases we see that degree 2 and 3 equations depend on only 1 parameter. The degree 4 case is easily done as well and the generic polynomial can always be brought to the form $X^4 + aX^2 + bX + b$ which depends on 2 parameters. One can show that fewer coefficients are not enough to describe all equations of degree 4.

1. Historical survey

All these cases were well known by the mathematicians of the past centuries. Every time they had to work on some equation they were using its simplified form to avoid unnecessary computations.

The first non-trivial case appears in degree 5. It was first Hermite who showed that the general equation of degree 5 can be brought, by means of a Tschirnhaus transform, to the form $X^5 + aX^3 + bX + c = 0$ which depends on only 2 parameters. Moreover Felix Klein showed that 2 parameters are necessary to describe equations of degree 5. Later Joubert showed that in degree 6 one can bring the generic equation to the form $X^6 + aX^4 + bX^2 + cX + d = 0$. It is possible to prove that 2 parameters are not enough. The question of how many parameters are needed for a degree 7 equation is still open.

In 1900, David Hilbert outlined 23 major mathematical problems to be studied in the coming century. Hilbert's 13th problem discusses some questions about the impossibility of the solvability of the equation of seventh order with the help of continuous functions of only two arguments. This problem is not directly related with the above simplification problem but a later algebraic version of it, which is still unsolved, has to do with Tschirnhaus transforms.

Essential dimension makes precise the notion of “how many parameters are needed to describe a given structure” in some general mathematical context.

This notion was formally introduced by Reichstein and Buhler in [7] only in 1995. They defined the essential dimension of a finite group G , denoted by $\text{ed}(G)$, and showed that $\text{ed}(\mathcal{S}_n)$ is equal to the number of parameters needed to describe the general equation of the n th degree up to Tschirnhaus transform. For a more detailed account on the connections between essential dimension and the algebraic version of Hilbert's 13th problem see [7].

Later Reichstein in [19] extended this notion to algebraic groups defined over an algebraically closed field k of characteristic zero, putting the insight and the techniques of algebraic geometry into the question. Many results concerning the behaviour of essential dimension and other interpretations of it were given in both papers [7] and [19].

Then came Merkurjev who developed a general functorial context for essential dimension. This has the advantage to generalise the notion to algebraic groups over arbitrary fields and makes many results easier to

understand. The present work is based on this approach. One can find this material in [17].

Finally Rost in [21] gave his valuation-versal point of view to the question. In his notes he also proves a deep result on $\text{ed}(\mathbf{PGL}_4)$.

The aim of the present work is to give a complete and clear account of the functorial point of view developed by Merkurjev and to apply his methods to the computation of the essential dimension of certain algebraic objects. Moreover a great part of the work is devoted to give different points of view and definitions for the essential dimension.

This work is the fruit of a collaboration with Grégory Berhuy, Ph.D of the University of Besançon, and will be published in two papers.

Reader Warning.

The reader is supposed to know commutative algebra, field theory and Galois theory for a degree-zero understanding of the paper. If he wants to understand more, good notions in algebraic geometry, algebraic groups and Galois cohomology are highly recommended. Some categorical language (very little) is also used.

Let k be a field. We denote by \mathfrak{C}_k the category of field extensions of k , i.e. the category whose objects are field extensions K over k and whose morphisms are field homomorphisms which fix k . We write \mathfrak{F}_k for the category of all *covariant* functors from \mathfrak{C}_k to the category of sets. For such a functor \mathbf{F} and for a field extension K/k we will write $\mathbf{F}(K)$ instead of $\mathbf{F}(K/k)$. If $K \rightarrow L$ is a morphism in \mathfrak{C}_k , for every element $a \in \mathbf{F}(K)$ we will denote by a_L the image of a under the map $\mathbf{F}(K) \rightarrow \mathbf{F}(L)$. We shall say that a morphism $\mathbf{F} \rightarrow \mathbf{G}$ between functors in \mathfrak{F}_k is a **surjection** if, for any field extension K/k , the corresponding map $\mathbf{F}(K) \rightarrow \mathbf{G}(K)$ is a surjection of sets. By a scheme over k , we mean a k -scheme of finite type.

EXAMPLES 2.1.

- (1) The forgetful functor, denoted by \mathbf{O} , which assigns to each field extension K/k the underlying set of K and to each morphism its underlying map of sets, is an object of \mathfrak{F}_k .
- (2) The stupid functor, denoted by $*$, sending a field K to a one-point set is an object of \mathfrak{F}_k .
- (3) Let X be a scheme over k . It defines a “point functor”, still denoted by X , in this way :

$$K \mapsto X(K) = \text{Hom}(\text{Spec}(K), X).$$

The set $X(K)$ is simply the set of all K -rational points of X .

- (4) For any integer $n \geq 1$, we put $\mathbf{Q}_n(K)$ for the set of isomorphism classes of non-degenerate quadratic forms of dimension n over K . It is clear that \mathbf{Q}_n defines an object of \mathfrak{F}_k .
- (5) A K -algebra is called primitive if it is isomorphic to a quotient of $K[X]$. Every such algebra is thus of the form $K[X]/\langle f \rangle$ for a single polynomial $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$. We denote by $\mathbf{Alg}_n(K)$ the set of isomorphism classes of n -dimensional primitive algebras. This also defines a functor \mathbf{Alg}_n from \mathfrak{C}_k to the category of sets.

(6) Let K be a field. We recall that an étale algebra over K is a finite dimensional commutative K -algebra A which satisfies $\sharp \text{Hom}_K(A, \overline{K}) = \dim_K A$, where \overline{K} denotes an algebraic closure of K . This is equivalent to saying that $A \otimes_K \overline{K}$ is reduced or that A is a product of separable extensions of K . Moreover if K is infinite, A is étale over K if and only if $A \simeq K[X]/\langle f \rangle$ where f has no multiple roots in \overline{K} . If A is étale over K and $K \rightarrow L$ is a field homomorphism then $A \otimes_K L$ is étale over L . For any field extension K/k and any integer $n \geq 1$, let $\mathbf{\acute{E}t}_n(K)$ denote the set of isomorphism classes of n -dimensional étale algebras over K . It also defines an object of the category \mathfrak{F}_k . When the base field k is infinite $\mathbf{\acute{E}t}_n$ is a subfunctor of \mathbf{Alg}_n and these functors are closely related for the essential dimension.

(7) Let G be a finite abstract group of order n and K a field. By a Galois G -algebra over K (or Galois K -algebra with group G) we mean an étale K -algebra L of dimension n such that G acts on L as a group of K -automorphisms and such that $L^G = K$. We denote by $G\text{-}\mathbf{Alg}(K)$ the set of isomorphism classes of Galois G -algebras over K . The assignment $K \mapsto G\text{-}\mathbf{Alg}(K)$ from \mathfrak{C}_k to the category of sets defines an object of \mathfrak{F}_k .

(8) For every integer $d, n \geq 2$, define $\mathbf{F}_{d,n}(K)$ to be the set of all (non-trivial) homogenous forms over K of degree d in n variables modulo the $\mathbf{GL}_n(K)$ -action and modulo the relation $f \sim \lambda f$ for $\lambda \in K^\times$. Once again $\mathbf{F}_{d,n}$ is an object of \mathfrak{F}_k .

(9) Let S be a pointed set with at least two elements and $d \geq 1$ an integer. We shall define the functor \mathbf{F}_S^d in the following way :

$$\mathbf{F}_S^d(K) = \begin{cases} S & \text{if } \text{trdeg}(K : k) \geq d \\ * & \text{otherwise} \end{cases}$$

and, for an extension K'/K , the obvious constant map of pointed sets $\mathbf{F}_S^d(K) \rightarrow \mathbf{F}_S^d(K')$.

(10) Let L/k be an arbitrary field extension. Then, the (covariant) representable functor h_L given by $h_L(K) = \text{Hom}(L, K)$ defines also an object of \mathfrak{F}_k .

2. Definitions

One natural question is to ask how many parameters are needed to describe a given structure. For example, any n -dimensional quadratic form in characteristic not 2, is determined by n parameters since it can be reduced to a diagonal form.

A quadratic algebra will certainly be described by one parameter since it can always be written as $k[X]/\langle X^2 + a \rangle$ when $\frac{1}{2}$ exists. The natural notion of functor shall replace the word “structure” and the following crucial definition, which is due to A. Merkurjev, shall make precise the concept of “how many parameters” are needed to describe it.

DEFINITION 2.2. *Let \mathbf{F} be an object of \mathfrak{F}_k , K/k a field extension and $a \in \mathbf{F}(K)$. For $n \in \mathbb{N}$, we say that the **essential dimension of a** is $\leq n$ (and we write $\text{ed}(a) \leq n$), if there exists a subextension E/k of K/k such that:*

i) $\text{trdeg}(E : k) \leq n$,

ii) the element a is in the image of the map $\mathbf{F}(E) \longrightarrow \mathbf{F}(K)$.

*We say that $\text{ed}(a) = n$ if $\text{ed}(a) \leq n$ and $\text{ed}(a) \not\leq n - 1$. The **essential dimension of \mathbf{F}** is the supremum of $\text{ed}(a)$ for all $a \in \mathbf{F}(K)$ and for all K/k . The essential dimension of \mathbf{F} will be denoted by $\text{ed}_k(\mathbf{F})$.*

EXAMPLES 2.3.

(1) It is clear from the very definition that $\text{ed}(*) = 0$ and $\text{ed}(\mathbf{O}) = 1$. More generally, we may say that a functor \mathbf{F} is **flasque** if, for any field extension K'/K , the map $\mathbf{F}(K) \longrightarrow \mathbf{F}(K')$ is surjective. Clearly every flasque functor \mathbf{F} satisfies $\text{ed}(\mathbf{F}) = 0$ and every constant functor is flasque.

(2) We shall do some very easy computations on polynomials of degree 2,3 and 4 in order to compute the essential dimension of \mathbf{Alg}_2 , \mathbf{Alg}_3 and \mathbf{Alg}_4 . We start with simple considerations on the functor \mathbf{Alg}_n for arbitrary n .

Let $A = K[X]/\langle f \rangle$ and $B = K[Y]/\langle g \rangle$ two n -dimensional primitive algebras. We denote by x and y the classes of X and Y respectively. A homomorphism $\varphi : A \longrightarrow B$ is determined by the image of x , say

$$\varphi(x) = c_{n-1}y^{n-1} + c_{n-2}y^{n-2} + \cdots + c_1y + c_0,$$

satisfying $f(\varphi(x)) = 0$. Saying that φ is an isomorphism is nothing but saying that $\varphi(x)$ generates B . In this case we say that $\varphi(x)$ is a nondegenerate **Tschirnhaus transformation** of f . Clearly a polynomial $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ is defined over $k(a_0, \dots, a_{n-1})$ and thus computing the essential dimension of (the isomorphism class of) $K[X]/\langle f \rangle$ is the same as reducing the number of coefficients appearing in f by means of nondegenerate Tschirnhaus transformations. (This is the starting point of the paper [7]). It clearly suffices to do this on the “generic element” $X^n + t_{n-1}X^{n-1} + \cdots + t_1X + t_0$ (where the t_i ’s are algebraically independent over k) since every other polynomial is a specialization of this one.

Now, when the characteristic of the ground field k does not divide n , the substitution $X \rightsquigarrow X - \frac{t_{n-1}}{n}$ drops the coefficient t_{n-1} and hence

$$\text{ed}(\mathbf{Alg}_n) \leq n - 1.$$

For the polynomial $X^2 + aX + b$ this says that one can reduce it to the form $X^2 + c$. Now the algebra $k(t)[X]/\langle X^2 + t \rangle$ is clearly not defined over an algebraic extension of k and hence

$$\text{ed}(\mathbf{Alg}_2) = 1.$$

Now $X^3 + aX^2 + bX + c$ can be reduced to $X^3 + b'X + c'$ and, setting $Y = \frac{c'}{b'}X$, one makes the second and the third coefficient equal.

Thus one can reduce it to the form $X^3 + dX + d$. As before the algebra $k(t)[X]/\langle X^3 + tX + t \rangle$ is not defined over an algebraic extension of k and so

$$\text{ed}(\mathbf{Alg}_3) = 1.$$

Similarly the generic polynomial of degree 4 can be reduced to the form $X^4 + sX^2 + tX + t$ and hence $\text{ed}(\mathbf{Alg}_4) \leq 2$. We will see that it cannot be reduced, thus $\text{ed}(\mathbf{Alg}_4) = 2$.

REMARK 2.4. The notion of essential dimension depends on the ground field k . However, when the field k is fixed, there is no confusion by writing $\text{ed}(\mathbf{F})$. When the context is not clear, or when we want to insist on some hypotheses made on the field, we shall write $\text{ed}_k(\mathbf{F})$. In general, if k'/k is a field extension, every object \mathbf{F} of \mathfrak{F}_k , can be viewed (by restriction) as an object of $\mathfrak{F}_{k'}$. The following proposition shows the behaviour of essential dimension under field extension.

2. Definitions

PROPOSITION 2.5. *Let k'/k a field extension and \mathbf{F} an object of \mathfrak{F}_k . Then*

$$\text{ed}_{k'}(\mathbf{F}) \leq \text{ed}_k(\mathbf{F}).$$

Proof. If $\text{ed}_k(\mathbf{F}) = \infty$, the result is obvious. Let $\text{ed}_k(\mathbf{F}) = n$. Take K/k' a field extension and $a \in \mathbf{F}(K)$. There exists a field extension $k \subseteq E \subseteq K$ with $\text{trdeg}(E : k) \leq n$ such that a is in the image of the map $\mathbf{F}(E) \rightarrow \mathbf{F}(K)$. The composite extension $E' = Ek'$ then satisfies $\text{trdeg}(E' : k') \leq n$ and clearly a is in the image of the map $\mathbf{F}(E') \rightarrow \mathbf{F}(K)$. Thus $\text{ed}(a) \leq n$ and $\text{ed}_{k'}(\mathbf{F}) \leq n$.

REMARKS 2.6.

- (1) The above proposition says that, for a fixed functor $\mathbf{F} \in \mathfrak{F}_k$, the map

$$\text{ed}_-(\mathbf{F}) : \mathfrak{C}_k \longrightarrow \mathbb{N} \cup \{\infty\}$$

is a contravariant functor where $\mathbb{N} \cup \{\infty\}$ is considered as a category by saying that there is a morphism $n \rightarrow m$ exactly when $n \leq m$. This implies that, if \mathbf{F} is a functor defined over the category of *all* fields, to give an upper bound of $\text{ed}_k(\mathbf{F})$ it is sufficient to give an upper bound on each prime field \mathbb{F}_p when $\text{char}(k) > 0$, and to give an upper bound on \mathbb{Q} when $\text{char}(k) = 0$.

- (2) In general one does not have $\text{ed}_k(\mathbf{F}) = \text{ed}_{k'}(\mathbf{F})$ for any field extension k'/k . Example (9) above shows that the essential dimension can decrease considerably: one sees immediately that $\text{ed}_{k'}(\mathbf{F}_S^d) = 0$ if $\text{trdeg}(k' : k) \geq d$. This is due to the fact that the functor becomes constant over k' and hence its essential dimension is zero. On the other hand it is clear that $\text{ed}_k(\mathbf{F}_S^d) = d$.
- (3) Let L/k be an extension and \mathbf{h}_L the corresponding representable functor of Example (10). Then one has $\text{ed}_{k'}(\mathbf{h}_L) = \text{trdeg}(L : k')$ if $k \subseteq k' \subseteq L$ and $\text{ed}_{k'}(\mathbf{h}_L) = 0$ otherwise. This is an easy exercise for the reader.

We shall see later on (Corollary 1.7 in Chapter II) examples of functors for which the inequality of Proposition 2.5 is strict even if the extension k'/k is algebraic.

The behaviour of essential dimension with respect to subobjects is not very clear. For example take for \mathbf{G} the constant functor $\mathbf{G}(K) = S$ where S is a set with at least two elements. Then \mathbf{F}_S^d is a subfunctor of \mathbf{G} and

the dimension of the former is d (which is arbitrarily large) whereas the dimension of \mathbf{G} is zero. However there is a large class of subfunctors for which the essential dimension has a nice behaviour.

DEFINITION 2.7. *Let \mathbf{G} be an object of \mathfrak{F}_k . A subfunctor $\mathbf{F} \subseteq \mathbf{G}$ is called **saturated** if for any field extension L/K over k and any element $a \in \mathbf{G}(K)$ such that $a_L \in \mathbf{F}(L)$ there is an algebraic subextension K'/K such that $a_{K'} \in \mathbf{F}(K')$.*

PROPOSITION 2.8. *Let $\mathbf{F} \subseteq \mathbf{G}$ a saturated subfunctor. Then*

$$\text{ed}(\mathbf{F}) \leq \text{ed}(\mathbf{G}).$$

Proof. Let K/k be a field extension and $a \in \mathbf{F}(K)$. Assume that $\text{ed}(\mathbf{G}) = n$. Then there is a subextension L/k and an element $b \in \mathbf{G}(L)$ such that $\text{trdeg}(L : k) \leq n$ and $a = b_K$. Since \mathbf{F} is saturated, there is an algebraic subextension E/L in K/L such that $b_E \in \mathbf{F}(E)$. Thus $a \in \text{im}(\mathbf{F}(E) \rightarrow \mathbf{F}(K))$ and since $\text{trdeg}(E : k) \leq n$ this shows that $\text{ed}(\mathbf{F}) \leq n$.

We continue our investigation with some very simple lemmas concerning the functorial properties of $\text{ed} : \mathfrak{F}_k \rightarrow \mathbb{N} \cup \{\infty\}$.

LEMMA 2.9. *Let $f : \mathbf{F} \twoheadrightarrow \mathbf{G}$ be a surjection in \mathfrak{F}_k . Then*

$$\text{ed}(\mathbf{G}) \leq \text{ed}(\mathbf{F}).$$

Proof. Let K/k be an extension and $b \in \mathbf{G}(K)$. By assumption, there is an element $a \in \mathbf{F}(K)$ such that $f_K(a) = b$. Suppose that $\text{ed}(\mathbf{F}) = n$. Take a subextension $k \subseteq E \subseteq K$ such that $\text{trdeg}(E : k) \leq n$ and such that $a \in \text{im}(\mathbf{F}(E) \rightarrow \mathbf{F}(K))$. The lemma now follows from the commutativity of the diagram

$$\begin{array}{ccc} \mathbf{F}(K) & \xrightarrow{f_K} & \mathbf{G}(K) \\ \uparrow & & \uparrow \\ \mathbf{F}(E) & \xrightarrow{f_E} & \mathbf{G}(E) \end{array}$$

Thus essential dimension is functorial (in a contravariant way) over the category of functors in \mathfrak{F}_k with *surjections* as morphisms. Nevertheless we will not restrict ourselves to that category, since this would not be very

2. Definitions

natural. For instance, we will always consider products and coproducts in the category of functors with *all* morphisms. The next lemma shows that the essential dimension preserves coproducts.

LEMMA 2.10. *Let \mathbf{F} and \mathbf{G} be two objects of \mathfrak{F}_k . Then*

$$\text{ed}(\mathbf{F} \amalg \mathbf{G}) = \max\{\text{ed}(\mathbf{F}), \text{ed}(\mathbf{G})\}.$$

Proof. Let K/k be an extension and $a \in \mathbf{F}(K) \amalg \mathbf{G}(K)$. Clearly one has $\text{ed}(a) \leq \text{ed}(\mathbf{F})$ or $\text{ed}(a) \leq \text{ed}(\mathbf{G})$. Thus $\text{ed}(\mathbf{F} \amalg \mathbf{G}) \leq \max\{\text{ed}(\mathbf{F}), \text{ed}(\mathbf{G})\}$. The opposite inequality is clear since \mathbf{F} and \mathbf{G} are both saturated subfunctors of $\mathbf{F} \amalg \mathbf{G}$.

LEMMA 2.11. *Let \mathbf{F} and \mathbf{G} be two objects of \mathfrak{F}_k . Then*

$$\text{ed}(\mathbf{F} \times \mathbf{G}) \leq \text{ed}(\mathbf{F}) + \text{ed}(\mathbf{G}).$$

Proof. Take K/k a field extension and $(a, a') \in \mathbf{F}(K) \times \mathbf{G}(K)$. Take two extensions $k \subseteq E, E' \subseteq K$ with

$$\text{trdeg}(E : k) \leq \text{ed}(\mathbf{F}), \text{trdeg}(E' : k) \leq \text{ed}(\mathbf{G})$$

and such that a (respectively a') belongs to the image of $\mathbf{F}(E) \rightarrow \mathbf{F}(K)$ (respectively $\mathbf{G}(E') \rightarrow \mathbf{G}(K)$). So there exist $b \in \mathbf{F}(E)$ and $b' \in \mathbf{G}(E')$ such that $b_K = a$ and $b'_K = a'$. If we consider $L = EE'$ and denote by c (respectively c') the image of b in $\mathbf{F}(L)$ (respectively the image of b' in $\mathbf{G}(L)$) it is easily seen that (c, c') maps to (a, a') . Hence

$$\text{ed}(a, a') \leq \text{trdeg}(L : k) \leq \text{trdeg}(E : k) + \text{trdeg}(E' : k) \leq \text{ed}(\mathbf{F}) + \text{ed}(\mathbf{G}).$$

Thus $\text{ed}(\mathbf{F} \times \mathbf{G}) \leq \text{ed}(\mathbf{F}) + \text{ed}(\mathbf{G})$.

A slight generalization of the previous inequality can be performed for functors which are in some kind of “fibration position”.

First recall that an **action** of a set Y over a set X is nothing but a map $Y \times X \rightarrow X$. If $y \in Y$ and $x \in X$ we shall write $y \cdot x$ for the image of (y, x) under this map. We say that a functor $\mathbf{F} : \mathfrak{C}_k \rightarrow \mathbf{Sets}$ acts over a functor $\mathbf{G} : \mathfrak{C}_k \rightarrow \mathbf{Sets}$ if, for every extension K/k , the set $\mathbf{F}(K)$ acts over $\mathbf{G}(K)$ and if the obvious compatibility condition holds: for each morphism $K \rightarrow L$ and for all elements $y \in \mathbf{F}(K)$ and $x \in \mathbf{G}(K)$, one has $(y \cdot x)_L = y_L \cdot x_L$. We shall say that the action of the functor \mathbf{F} over the functor \mathbf{G} is **transitive** if for every K/k the action of the set $\mathbf{F}(K)$ is transitive over $\mathbf{G}(K)$ (that is there is only one orbit).

Recall also that, if $\pi : \mathbf{G} \longrightarrow \mathbf{H}$ is a morphism of functors in \mathfrak{F}_k and K/k is an extension, each element $a \in \mathbf{H}(K)$ gives rise to a functor $\pi^{-1}(a)$, defined over \mathfrak{C}_K , by setting $\pi_L^{-1}(a) = \{x \in \mathbf{G}(L) \mid \pi_L(x) = a_L\}$ for every extension L/K .

DEFINITION 2.12. *Let $\pi : \mathbf{G} \twoheadrightarrow \mathbf{H}$ be a surjection in \mathfrak{F}_k . We say that a functor \mathbf{F} is in **fibration position** for π if \mathbf{F} acts transitively on each fiber of π . More precisely, for every extension K/k and every $a \in \mathbf{H}(K)$, we require that $\mathbf{F}(K)$ acts transitively on $\pi_K^{-1}(a)$ in a functorial way. When \mathbf{F} is in fibration position for π we simply write $\mathbf{F} \rightsquigarrow \mathbf{G} \twoheadrightarrow \mathbf{H}$ and call this a **fibration of functors**.*

In the following proposition we insist on the fact that all the functors involved *do not necessarily* take values in the category of groups.

PROPOSITION 2.13. *Let $\mathbf{F} \rightsquigarrow \mathbf{G} \twoheadrightarrow \mathbf{H}$ be a fibration of functors. Then*

$$\text{ed}(\mathbf{G}) \leq \text{ed}(\mathbf{F}) + \text{ed}(\mathbf{H}).$$

Proof. Let K/k a field extension and $a \in \mathbf{G}(K)$. By definition there is a field extension E with $k \subseteq E \subseteq K$, satisfying $\text{trdeg}(E : k) \leq \text{ed}(\mathbf{H})$, and an element $b' \in \mathbf{H}(E)$ such that $b'_K = \pi_K(a)$. Since π_E is surjective there exists $a' \in \mathbf{G}(E)$ such that $\pi_E(a') = b'$. Now clearly $\pi_K(a'_K) = \pi_K(a)$ and thus a'_K and a are in the same fiber. By assumption there exists an element $c \in \mathbf{F}(K)$ such that $a'_K \cdot c = a$. Now there exists an extension E' with $k \subseteq E' \subseteq K$ and $\text{trdeg}(E' : k) \leq \text{ed}(\mathbf{F})$ such that c is in the image of the map $\mathbf{F}(E') \longrightarrow \mathbf{F}(K)$. We take $c' \in \mathbf{F}(E')$ such that $c'_K = c$. Considering now the composite extension $E'' = EE'$ and setting $d = a'_{E''} \cdot c'_{E''} \in \mathbf{G}(E'')$ we have, since the action is functorial,

$$d_K = (a'_{E''} \cdot c'_{E''})_K = a'_K \cdot c'_K = a'_K \cdot c = a$$

and thus

$$\text{ed}(a) \leq \text{trdeg}(E'' : k) \leq \text{trdeg}(E : k) + \text{trdeg}(E' : k) \leq \text{ed}(\mathbf{H}) + \text{ed}(\mathbf{F}).$$

Since this is true for an arbitrary element a the desired inequality follows.

REMARK 2.14. The inequality $\text{ed}(\mathbf{F} \times \mathbf{G}) \leq \text{ed}(\mathbf{F}) + \text{ed}(\mathbf{G})$ is a consequence of this proposition. Indeed for $a \in \mathbf{G}(K)$ the fiber of the projection is $\mathbf{F}(K) \times \{a\}$ and the set $\mathbf{F}(K)$ acts transitively by simply setting $x \cdot (y, a) = (x, a)$.

2. Definitions

COROLLARY 2.15. *Let $1 \longrightarrow \mathbf{F} \longrightarrow \mathbf{G} \longrightarrow \mathbf{H} \longrightarrow 1$ be a short exact sequence of group-valued functors. Then*

$$\text{ed}(\mathbf{G}) \leq \text{ed}(\mathbf{F}) + \text{ed}(\mathbf{H}).$$

Proof. This is clear since $\mathbf{H}(K) \cong \mathbf{G}(K)/\mathbf{F}(K)$ and the set $\mathbf{F}(K)$ acts transitively on equivalence classes by group multiplication.

REMARKS 2.16.

a) One can have $\text{ed}(\mathbf{G}) < \text{ed}(\mathbf{F}) + \text{ed}(\mathbf{H})$ as is shown by the following example: For every field extension K let $\mathbf{F}(K) = K^{\times 2}$ be the subgroup of $\mathbf{G}(K) = K^{\times}$ consisting of all the squares and $\mathbf{H}(K) = K^{\times}/K^{\times 2}$ the corresponding quotient (as groups). It is not difficult to see that $\text{ed}(\mathbf{F}) = \text{ed}(\mathbf{G}) = \text{ed}(\mathbf{H}) = 1$, and thus $1 = \text{ed}(\mathbf{G}) < \text{ed}(\mathbf{F}) + \text{ed}(\mathbf{H}) = 2$ (but note that $\mathbf{G} \not\cong \mathbf{F} \times \mathbf{H}$ as functors).

b) For a product of functors, since $\mathbf{F} \times \mathbf{G}$ maps onto both \mathbf{F} and \mathbf{G} , we have

$$\max\{\text{ed}(\mathbf{F}), \text{ed}(\mathbf{G})\} \leq \text{ed}(\mathbf{F} \times \mathbf{G}) \leq \text{ed}(\mathbf{F}) + \text{ed}(\mathbf{G}).$$

However, even the behaviour of products with respect to essential dimension is not clear. Consider for instance the following two examples :

- Consider the functor \mathbf{F}_S^d of example (9) above. Clearly $\mathbf{F}_S^d \times \mathbf{F}_S^d = \mathbf{F}_{S \times S}^d$ and hence

$$\text{ed}(\mathbf{F}_S^d \times \mathbf{F}_S^d) = \text{ed}(\mathbf{F}_{S \times S}^d) = d = \text{ed}(\mathbf{F}_S^d).$$

Thus it is possible to have $\text{ed}(\mathbf{F} \times \cdots \times \mathbf{F}) = \text{ed}(\mathbf{F})$.

- In contrast with the previous example consider \mathbf{O} the forgetful functor. Then

$$\text{ed}(\underbrace{\mathbf{O} \times \cdots \times \mathbf{O}}_{n \text{ times}}) = n$$

and hence $\text{ed}(\prod_{n \in \mathbb{N}} \mathbf{O}) = \infty$.

The geometric class of functors introduced in example (3) has an easy essential-dimensional behaviour. This is treated in the following

PROPOSITION 2.17. *Let X be a scheme over k . Then*

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

Proof. Let K/k and $a \in X(K) = \text{Hom}(\text{Spec}(K), X)$. If x denotes the corresponding point, we have an inclusion $k(x) \hookrightarrow K$, where $k(x)$ is the residue field at x . But

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

hence $\dim(X) = \text{ed}(X)$.

DEFINITION 2.18. *Let \mathbf{F} be an object of \mathfrak{F}_k . A **classifying scheme of \mathbf{F}** is a k -scheme X such that there is a surjection $X \twoheadrightarrow \mathbf{F}$.*

COROLLARY 2.19. *If X is a classifying scheme of \mathbf{F} then*

$$\text{ed}(\mathbf{F}) \leq \dim(X).$$

Proof. This is clear from the definition and the previous considerations.

EXAMPLES 2.20.

- Consider \mathbb{G}_m the multiplicative group scheme over k . If $\text{char}(k) \neq 2$, then every quadratic form is diagonalizable, thus there is a surjective morphism of functors $\mathbb{G}_m^n \twoheadrightarrow \mathbf{Q}_n$ given by

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

Hence \mathbb{G}_m^n is a classifying scheme of \mathbf{Q}_n . This shows that $\text{ed}_k(\mathbf{Q}_n) \leq n$ when $\text{char}(k) \neq 2$.

- For example (6) above, when k is infinite, there is also a classifying scheme X . Take $A = k[t_1, \dots, t_n, \frac{1}{d(f)}]$ where $f = x^n + t_1x^{n-1} + \dots + t_n$ and $d(f)$ is the discriminant of f . It now suffices to take $X = \text{Spec}(A)$. Hence $\text{ed}_k(\hat{\mathbf{E}}\mathbf{t}_n) \leq n$.

- In example (8) we easily see that every homogenous form of degree d with n variables can be written with at most $m = \binom{d+n-1}{n-1}$ coefficients. So one has a very rough classifying scheme \mathbb{P}^{m-1} and thus

$$\text{ed}(\mathbf{F}_{d,n}) \leq m - 1.$$

2. Definitions

Moreover there is a fibration of functors

$$X_n \rightsquigarrow \mathbb{P}^{m-1} \twoheadrightarrow \mathbf{F}_{d,n}$$

where X_n is \mathbf{PGL}_n viewed as a scheme over k . Thus, by Proposition 2.13, we have $\text{ed}(\mathbb{P}^{m-1}) \leq \text{ed}(X_n) + \text{ed}(\mathbf{F}_{d,n})$. Since $\text{ed}(\mathbb{P}^{m-1}) = m - 1$ and $\text{ed}(X_n) = n^2 - 1$ it follows that

$$\text{ed}(\mathbf{F}_{d,n}) \geq m - n^2.$$

In the case $n = 2$ one can easily show that $\text{ed}(\mathbf{F}_{d,2}) \leq d - 2$ and the above inequality tells us that $\text{ed}(\mathbf{F}_{d,2}) \geq d - 3$. Hence

$$d - 3 \leq \text{ed}(\mathbf{F}_{d,2}) \leq d - 2.$$

For a discussion of the essential dimension of cubics in few variables, see Chapter V.

- In example (8) one could have preferred considering homogenous forms only up to \mathbf{GL}_n and not up to a scalar. Denote by $\mathbf{G}_{d,n}$ this new functor. There is a simple relationship between $\text{ed}(\mathbf{F}_{d,n})$ and $\text{ed}(\mathbf{G}_{d,n})$. Indeed there is an obvious surjection of functors

$$\mathbf{G}_{d,n} \twoheadrightarrow \mathbf{F}_{d,n}$$

sending a class modulo \mathbf{GL}_n to its class in $\mathbf{F}_{d,n}$. But the fiber of a form $[f] \in \mathbf{F}_{d,n}(K)$ is clearly the subset $\{[\lambda f] \in \mathbf{G}_{d,n}(K) \mid \lambda \in K^\times\}$ and thus K^\times acts transitively on each fiber. We hence obtain a fibration of functors

$$X \rightsquigarrow \mathbf{G}_{d,n} \twoheadrightarrow \mathbf{F}_{d,n}$$

where X is the scheme $\mathbb{A}^1 \setminus \{0\}$ viewed as a functor. This gives the inequality

$$\text{ed}(\mathbf{G}_{d,n}) \leq \text{ed}(\mathbf{F}_{d,n}) + \text{ed}(X) = \text{ed}(\mathbf{F}_{d,n}) + 1.$$

REMARK 2.21. In this section all the basic concepts are introduced by Merkurjev in [17] with complete proofs. We have completed these results with Lemma 2.10, Definition 2.12, Corollary 2.15 and some trivial results. The discussion on $\mathbf{F}_{d,n}$ is also a new element.

CHAPTER II

COHOMOLOGICAL METHODS

1. GALOIS COHOMOLOGY

We introduce an important class of functors using Galois cohomology. These functors will be the center of our considerations. Their essential dimension was first introduced by Reichstein, over an algebraically closed field, in terms of compressions. See [19] for details. The standard reference for Galois cohomology is [23].

Let G be a k -group scheme (always of finite type). Take K/k a field extension and K_s a separable closure. The group $\Gamma_K = \text{Gal}(K_s/K)$ acts on $G(K_s)$ compatibly with the G -action. The **Galois cohomology set** $H^1(\Gamma_K, G(K_s)) =: H^1(K, G)$ is then well defined, i.e. does not depend on the choice of the separable closure. This set may be defined either using cocycles either principal homogenous spaces (see [23]). We will freely use both representations in the sequel without mentioning it. Moreover $H^1(-, G)$ is a functor in the first variable and thus is an object of \mathfrak{F}_k (see [23] page 83). This allow us to set the following definition.

DEFINITION 1.1. *Let G be a k -group scheme. The **essential dimension of G** is defined as*

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

A big portion of the present work is dedicated to the study of the essential dimension of certain group schemes. A certain number of techniques are developed in order to estimate it. In the sequel all group schemes are assumed for simplicity to be affine. We will mostly restrict ourselves to algebraic groups over k , that is smooth affine group schemes over k whose Hopf algebra is finitely generated.

We briefly recall the following interpretation of Galois cohomology which will be useful in the sequel (cf [23] pages 128-129).

PROPOSITION 1.2. *Let (V_0, x_0) be an algebraic structure over k in the sense of [23]. For any field extension K/k let $G(K) = \text{Aut}_K(V_0 \otimes_k K)$ be the group of K -automorphisms which preserve the structure. Then the set $H^1(k, G)$ classifies the k -isomorphism classes of algebraic structures over k which become isomorphic to (V_0, x_0) over a separable closure.*

First examples. It is well known that $H^1(K, \mathbf{GL}_n) = 1$ for every field K . This is the so-called *Hilbert 90 Theorem*. Thus $\text{ed}_k(\mathbf{GL}_n) = 0$ for every field k . Moreover the short exact sequence

$$1 \rightarrow \mathbf{SL}_n \rightarrow \mathbf{GL}_n \rightarrow \mathbb{G}_m \rightarrow 1$$

induces an exact sequence in cohomology showing that $H^1(K, \mathbf{SL}_n) = 1$ for every field K . Thus one also has $\text{ed}_k(\mathbf{SL}_n) = 0$ for every field k .

Example of $H^1(k, \mathcal{S}_n)$. We consider the symmetric group $G = \mathcal{S}_n$ as a constant group scheme over k .

Take $V_0 = k \times \cdots \times k = k^n$ with its product k -algebra structure. It is easily computed that $\mathcal{S}_n = \text{Aut}_{K\text{-alg}}(V_0 \otimes_k K)$. Thus, by the preceding proposition, we have that $H^1(k, \mathcal{S}_n)$ is the set of isomorphism classes of k -algebras A such that there exists a separable extension L/k with $A \otimes_k L \cong L^n$. It is then easily checked that $H^1(-, \mathcal{S}_n) \cong \hat{\mathbf{E}t}_n$ as functors and thus

$$\text{ed}_k(\mathcal{S}_n) = \text{ed}_k(\hat{\mathbf{E}t}_n).$$

Galois algebras. Let G any arbitrary finite constant group scheme over k . For any field extension K/k there is a bijection from $G\text{-Alg}(K)$ to $H^1(K, G)$ given as follows: let L be a Galois G -algebra over K . The set E_L of K -algebra homomorphisms $L \rightarrow K_s$ is finite with $\dim_K L$ elements. One shows easily that E_L is a principal homogenous space under Γ_K and G . Sending $[L]$ to $[E_L]$ yields a well defined map from $G\text{-Alg}(K)$ to $H^1(K, G)$ which one can show to be a bijection (see [15] for details). Thus $G\text{-Alg} \cong H^1(-, G)$.

1. Galois cohomology

EXAMPLES 1.3.

• **The group μ_n .**

Let k be a field and consider $\mu_n = \text{Spec}(k[X]/\langle X^n - 1 \rangle)$ the k -group scheme of the n -th roots of unity.

– Suppose that n is prime to the characteristic of k . Then it is well known that for any field extension L/k one has a functorial isomorphism $H^1(L, \mu_n) \cong L^\times / L^{\times n}$. It thus follows that $\text{ed}_k(\mu_n) = 1$.

– If $n = \text{char}(k)$, then μ_n has trivial cohomology and thus $\text{ed}_k(\mu_n) = 0$.

• **The group \mathbb{Z}/p .**

Let k be a field, p a prime number and denote by \mathbb{Z}/p the constant k -group scheme represented by $\text{Spec}(k^{\mathbb{Z}/p})$.

– If $\text{char}(k) \neq p$ and k contains all the p -th roots of unity we can identify the group scheme \mathbb{Z}/p with μ_p by choosing a primitive root of unity. In this case one finds $\text{ed}_k(\mathbb{Z}/p) = 1$. When the field does not contain all the p -th roots of unity, the computation of $\text{ed}_k(\mathbb{Z}/p)$ is much harder as we shall see later.

– When $\text{char}(k) = p$ the situation is easier. The long exact sequence in cohomology induced by the short exact sequence

$$0 \longrightarrow \mathbb{Z}/p \longrightarrow \mathbb{G}_a \longrightarrow \mathbb{G}_a \longrightarrow 0$$

gives a functorial isomorphism $H^1(L, \mathbb{Z}/p) \cong L/\wp(L)$ where $\wp(x) = x^p - x$ for $x \in L$. It now clearly follows that $\text{ed}_k(\mathbb{Z}/p) = 1$.

REMARK 1.4. When $\text{char}(k) = p$, the group \mathbb{Z}/p^n fits into a short exact sequence of k -group schemes analogous to the previous one, but using Witt vectors:

$$0 \longrightarrow \mathbb{Z}/p^n \longrightarrow W_n \longrightarrow W_n \longrightarrow 0$$

where $W_n(k)$ is the additive group of Witt vectors of length n (see [24]). Applying again cohomology and using the fact that $H^1(k, W_n) = 0$, one finds that W_n is a classifying scheme for \mathbb{Z}/p^n and hence

$$\text{ed}_k(\mathbb{Z}/p^n) \leq n.$$

Another proof of the inequality $\text{ed}_k(\mathbb{Z}/p^n) \leq n$ is performed by looking at the exact sequence

$$0 \longrightarrow \mathbb{Z}/p \longrightarrow \mathbb{Z}/p^n \longrightarrow \mathbb{Z}/p^{n-1} \longrightarrow 0.$$

It induces a long exact sequence in Galois cohomology but, when the base field k is of characteristic p one has $H^2(K, \mathbb{Z}/p) = 0$ for every extension K/k (see [23] page 86), and thus it reduces to a short exact sequence of group-valued functors

$$0 \longrightarrow H^1(-, \mathbb{Z}/p) \longrightarrow H^1(-, \mathbb{Z}/p^n) \longrightarrow H^1(-, \mathbb{Z}/p^{n-1}) \longrightarrow 0.$$

Then, by Corollary 2.15 of Chapter I, one has

$$\text{ed}_k(\mathbb{Z}/p^n) \leq \text{ed}_k(\mathbb{Z}/p^{n-1}) + \text{ed}_k(\mathbb{Z}/p)$$

and, since $\text{ed}_k(\mathbb{Z}/p) = 1$, we are done by induction.

• **The circle.**

We are interested in the group $S^1 = \text{Spec}(k[X, Y]/\langle X^2 + Y^2 - 1 \rangle)$ with its usual group structure. We first notice that when -1 is a square and $\text{char}(k) \neq 2$, the rings $k[X, Y]/\langle X^2 + Y^2 - 1 \rangle$ and $k[t, t^{-1}]$ are isomorphic. In that case it follows that the algebraic groups S^1 and \mathbb{G}_m are isomorphic and hence $\text{ed}_k(S^1) = 0$. When -1 is not a square we will see that the essential dimension increases.

Actually we will solve the problem for a wider class of algebraic groups.

Let k be a field and L an étale algebra over k . One defines the group scheme $\mathbb{G}_{m,L}^1$ by the exact sequence

$$1 \longrightarrow \mathbb{G}_{m,L}^1 \longrightarrow \mathbf{R}_{L/k}(\mathbb{G}_{m,L}) \xrightarrow{N_{L/k}} \mathbb{G}_m \longrightarrow 1,$$

where $\mathbf{R}_{L/k}$ denotes the Weil restriction (see [15] p.329 where it is called corestriction).

In the sequel, we will prove the following result:

THEOREM 1.5. *Let L/k be an étale algebra of dimension $n \geq 1$. Then*

$$\text{ed}_k(\mathbb{G}_{m,L}^1) = \begin{cases} 0 & \text{if } L \text{ is isomorphic to a product of field} \\ & \text{extensions of relatively prime degrees} \\ 1 & \text{otherwise.} \end{cases}$$

1. Galois cohomology

The above sequence induces, for any extension K/k , the exact sequence in cohomology

$$(L \otimes K)^\times \xrightarrow{N_K} K^\times \longrightarrow H^1(K, \mathbb{G}_{m,L}^1) \longrightarrow 1$$

where N_K is a short notation for $N_{L \otimes K/K}$. This gives an isomorphism

$$H^1(K, \mathbb{G}_{m,L}^1) \simeq K^\times / N_{L \otimes K/K}(L \otimes K)^\times.$$

In particular one has $\text{ed}_k(\mathbb{G}_{m,L}^1) \leq 1$ for every field k .

Since the case $n = 1$ is trivial, we may assume until the end of this section that $n \geq 2$.

We start with the following lemma:

LEMMA 1.6. *Let k be a field, let L be a finite dimensional étale k -algebra of dimension $n \geq 2$, and let t be a transcendental element over k . Then t belongs to the norm group of $L \otimes k(t)/k$ if and only if L is isomorphic to a product of some finite separable field extensions of k those degrees are relatively prime.*

Proof. Assume that there exists $\alpha \in L \otimes k(t)$ with $N_{L \otimes k(t)/k(t)}(\alpha) = t$. In the sequel, we will write $L(t)$ instead of $L \otimes k(t)$ in order to simplify

notation. Write $\alpha = \frac{1}{Q(t)} \cdot \sum_{i=0}^m \lambda_i t^i$, for some $\lambda_i \in L$, with $\lambda_m \neq 0$ and

some nonzero polynomial $Q(t) \in k[t]$ of degree $d \geq 0$. Assume first that L is a field. Then $L(t)/k(t)$ is again a separable field extension, and we have

$$Q(t)^n t = N_{L(t)/k(t)}(Q(t) \cdot \alpha) = \prod_{\sigma} \left(\sum_{i=0}^m \sigma(\lambda_i) \otimes t^i \right),$$

where σ describes $\text{Hom}_k(L, k_s)$. Since L is a field and $\lambda_m \neq 0$, the leading coefficient of the right hand side term is equal to $N_{L/k}(\lambda_m) t^{mn}$. Since $Q(t)^n t$ is a polynomial of degree $nd + 1$ and $n \geq 2$, we get a contradiction.

Hence $L \simeq L_1 \times \cdots \times L_r$ for $r \geq 2$, where L_i/k is a finite separable field extension of degree n_i . We then have

$$t = N_{L_1(t)/k(t)}(\alpha_1) \cdots N_{L_r(t)/k(t)}(\alpha_r)$$

for some $\alpha_i \in L_i(t)^\times$. As above write $\alpha_i = \frac{1}{Q_i(t)} \cdot \sum_{j=0}^{m_i} \lambda_j^{(i)} \otimes t^j$, where

$\lambda_{m_i}^{(i)} \neq 0$. Since L_i is a field, the computation above shows that the

leading coefficient of $Q_1(t)^{n_1} \cdots Q_r(t)^{n_r} t$ is

$$N_{L_1/k}(\lambda_{m_1}^{(1)})t^{m_1 n_1} \cdots N_{L_r/k}(\lambda_{m_r}^{(r)})t^{m_r n_r},$$

which has degree $m_1 n_1 + \cdots + m_r n_r$. By assumption, this degree is equal to $1 + n_1 d_1 + \cdots + n_r d_r$. It follows immediately that the n_i 's are relatively prime. The converse is clear.

We now prove Theorem 1.5. Assume first that $\text{ed}(\mathbb{G}_{m,L}^1) = 0$. Then the class of t in $H^1(k(t), \mathbb{G}_{m,L}^1)$ is defined over k . That is there exists an element $a \in k$ such that $t = a N_{k(t)}(\alpha)$ for some $\alpha \in L \otimes k(t)$. Then $u = \frac{t}{a}$ is a transcendental element over k which belongs to the norm group of $L \otimes k(u)$. Applying the previous lemma shows that L is isomorphic to a product of some finite separable field extensions of k those degrees are relatively prime. Conversely, if L is isomorphic to a product of some finite separable field extensions of k those degrees are relatively prime, then one can easily see that N_K is surjective for any field extension K/k , so $\text{ed}(\mathbb{G}_{m,L}^1) = 0$.

COROLLARY 1.7. *Let k be a field. Then*

$$\text{ed}_k(S^1) = \begin{cases} 1 & \text{if } \text{char}(k) \neq 2 \text{ and } -1 \notin k^{\times 2} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. If $\text{char}(k) \neq 2$, apply the previous theorem to the étale algebra $L = k[X]/(X^2 - 1)$. If $\text{char}(k) = 2$, it is easy to see that for any field extension K/k , we have $S^1(K_s) = \{(x, x+1) \mid x \in K_s\}$. In particular $S^1(K_s) \simeq K_s$ as Galois modules and $H^1(-, S^1) = 0$, showing that $\text{ed}_k(S^1) = 0$.

REMARK 1.8. In this section new results are Remark 1.4, Theorem 1.5 and Corollary 1.7.

2. COHOMOLOGICAL INVARIANTS

One way of giving lower bounds of essential dimension of functors is to use cohomological invariants. This idea can be found in [19]. The advantage of Merkurjev's functorial point of view is that the definitions are natural and that one could in theory apply these methods to a broader class of invariants.

DEFINITION 2.1. *Let \mathbf{F} be an object of \mathfrak{F}_k and $n \geq 1$ an integer. We say that \mathbf{F} is **n -simple** if there exists a field extension \tilde{k}/k such that for any extension K/\tilde{k} with $\text{trdeg}(K : \tilde{k}) < n$ the set $\mathbf{F}(K)$ consists of one element.*

EXAMPLE 2.2. Let M be a discrete torsion Γ_k -module and $n \geq 1$ an integer. Then it is known that $H^n(K, M) = 0$ if K contains an algebraically closed field and is of transcendence degree $< n$ over this field (see [23], Proposition 11, page 93). Taking for \tilde{k} an algebraic closure of k one sees that $H^n(-, M)$ is n -simple.

DEFINITION 2.3. *A morphism of functors $f : \mathbf{F} \rightarrow \mathbf{G}$ is called **non-constant** if for any field extension K/k there exists an extension L/K and elements $a \in \mathbf{F}(K)$, $a' \in \mathbf{F}(L)$ such that $f_L(a_L) \neq f_L(a')$.*

PROPOSITION 2.4. *Let $f : \mathbf{F} \rightarrow \mathbf{G}$ be a non-constant morphism and suppose that \mathbf{G} is n -simple. Then $\text{ed}_k(\mathbf{F}) \geq n$.*

Proof. Let \tilde{k} be the field in the definition of n -simplicity of \mathbf{G} . Suppose that $\text{ed}_k(\mathbf{F}) < n$. Since $\text{ed}_{\tilde{k}}(\mathbf{F}) \leq \text{ed}_k(\mathbf{F})$ one has $\text{ed}_{\tilde{k}}(\mathbf{F}) < n$ too. Since f is non-constant there exists an extension L/\tilde{k} and elements $a \in \mathbf{F}(\tilde{k})$, $a' \in \mathbf{F}(L)$ such that $f_L(a_L) \neq f_L(a')$. Since $\text{ed}_{\tilde{k}}(\mathbf{F}) < n$ there exists a subextension $\tilde{k} \subseteq E \subseteq L$ of transcendence degree $< n$ over \tilde{k} such that $a' \in \text{im}(\mathbf{F}(E) \rightarrow \mathbf{F}(L))$ that is $a' = a'_L$ for some $a'' \in \mathbf{F}(E)$.

Since the diagram

$$\begin{array}{ccc}
 \mathbf{F}(L) & \xrightarrow{f_L} & \mathbf{G}(L) \\
 \uparrow & & \uparrow \\
 \mathbf{F}(E) & \xrightarrow{f_E} & \mathbf{G}(E) \\
 \uparrow & & \uparrow \\
 \mathbf{F}(\tilde{k}) & \xrightarrow{f_{\tilde{k}}} & \mathbf{G}(\tilde{k})
 \end{array}$$

is commutative, and since $f_L(a_L) \neq f_L(a')$, one has $f_E(a_E) \neq f_E(a'')$. This contradicts the fact that $\mathbf{G}(E)$ consists of one element.

DEFINITION 2.5. *Let k be a field and \mathbf{F} a functor from \mathfrak{C}_k to the category of pointed sets. A **cohomological invariant of degree n of \mathbf{F}** is a morphism of pointed functors $\varphi : \mathbf{F} \rightarrow H^n(-, M)$, where M is a discrete torsion Γ_k -module. (Here $H^n(-, M)$ is pointed by 0, the class of the trivial cocycle.) We say that it is **non-trivial** if for any extension K/k there exists $L \supseteq K$ and $a \in \mathbf{F}(L)$ such that $\varphi_L(a) \neq 0$ in $H^n(L, M)$.*

COROLLARY 2.6. *Let k be an arbitrary field and \mathbf{F} a functor from \mathfrak{C}_k to the category of pointed sets. If \mathbf{F} has a non-trivial cohomological invariant φ of degree n , then $\text{ed}_k(\mathbf{F}) \geq n$.*

Proof. Clearly any non-trivial cohomological invariant is a non-constant morphism.

We will apply the above corollary to a special class of algebraic groups: finite constant abelian groups. Recall that such a group G can always be written as $G \cong \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_n$ where $d_1 \mid d_2 \mid \cdots \mid d_n$. The number n is called the **rank of G** and is denoted by $\text{rank}(G)$.

PROPOSITION 2.7. *Let G be a finite abelian group and k a field such that $\text{char}(k) \nmid \exp(G)$. Then $\text{ed}_k(G) \geq \text{rank}(G)$.*

Proof. For the proof one can suppose that k is algebraically closed. We will define a cohomological invariant φ of degree n for $H^1(-, G)$. There is an isomorphism

$$H^1(K, G) \cong H^1(K, \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_n) \cong H^1(K, \mathbb{Z}/d_1) \times \cdots \times H^1(K, \mathbb{Z}/d_n),$$

$$c \longmapsto (c_1, \dots, c_n)$$

which, composed with the cup product

$$H^1(K, \mathbb{Z}/d_1) \times \cdots \times H^1(K, \mathbb{Z}/d_n) \rightarrow H^n(K, \mathbb{Z}/d_1 \otimes \cdots \otimes \mathbb{Z}/d_n)$$

$$(c_1, \dots, c_n) \longmapsto c_1 \cup \cdots \cup c_n$$

defines a cohomological invariant

$$\varphi : H^1(-, G) \longrightarrow H^n(-, \mathbb{Z}/d_1)$$

since $\mathbb{Z}/d_1 \otimes \cdots \otimes \mathbb{Z}/d_n \cong \mathbb{Z}/d_1$. It suffices to show that it is non-trivial. We have to show that, for a field extension K/k , there exists $L \supseteq K$ and $a \in H^1(L, G)$ such that $\varphi_L(a) \neq 0$. We take $L = K(t_1, \dots, t_n)$ and set

2. Cohomological invariants

(t_i) = class of t_i in $L^\times/L^{\times d_i} \cong H^1(L, \mathbb{Z}/d_i)$ (this isomorphism holds since k is algebraically closed). Then, the image of

$$a = ((t_1), \dots, (t_n)) \in H^1(L, \mathbb{Z}/d_1) \times \cdots \times H^1(L, \mathbb{Z}/d_n) \cong H^1(L, G)$$

is the element $\varphi(a) = (t_1) \cup \cdots \cup (t_n) \in H^n(L, \mathbb{Z}/d_1)$. We show that this element is $\neq 0$ by induction on n :

– For $n = 1$, $(t_1) \in K(t_1)^\times/K(t_1)^{\times d_1}$ is clearly non-zero.

– Suppose that $n > 1$:

We use a more general fact (see [1]). If K is a field equipped with a discrete valuation $v : K^\times \rightarrow \mathbb{Z}$, then there is the so-called residue homomorphism

$$\partial_v : H^n(K, \mathbb{Z}/d) \rightarrow H^{n-1}(\kappa(v), \mathbb{Z}/d)$$

where $\kappa(v)$ denotes the residue field of v . This homomorphism has the following property :

If $v(a_1) = \cdots = v(a_{n-1}) = 0$ and $v(a_n) = 1$ (i.e. $a_i \in \mathcal{O}_v^\times$ for $i < n$) then

$$\partial_v((a_1) \cup \cdots \cup (a_{n-1}) \cup (a_n)) = (\bar{a}_1) \cup \cdots \cup (\bar{a}_{n-1}) \in H^{n-1}(\kappa(v), \mathbb{Z}/d)$$

where \bar{a}_i is the class of a_i in $\mathcal{O}_v/\mathfrak{m}_v = \kappa(v)$.

In our case, we take for v the t_n -adic valuation on L . We thus have

$$\partial_v((t_1) \cup \cdots \cup (t_n)) = (t_1) \cup \cdots \cup (t_{n-1}) \in H^{n-1}(K(t_1, \dots, t_{n-1}), \mathbb{Z}/d_1).$$

By induction hypothesis this element is non-zero, hence $(t_1) \cup \cdots \cup (t_n) \neq 0$ and $\text{ed}(G) = n$.

REMARK 2.8. In fact this shows that $\text{ed}_k(G) \geq \text{rank}_p(G)$ for any field k with $\text{char}(k) \neq p$. Here $\text{rank}_p(G)$ denotes the rank of the largest p -elementary subgroup of G .

If $\text{char}(k) = p$ this result is no longer true. Indeed, consider the group $\mathbb{Z}/p \times \cdots \times \mathbb{Z}/p$ (n copies). If one takes for k a field containing \mathbb{F}_{p^n} there is a short exact sequence

$$0 \rightarrow \mathbb{Z}/p \times \cdots \times \mathbb{Z}/p \rightarrow \mathbb{G}_a \rightarrow \mathbb{G}_a \rightarrow 0$$

where the map $\mathbb{G}_a \rightarrow \mathbb{G}_a$ is given by $x \mapsto x^p - x$. This gives in cohomology an exact sequence

$$\mathbb{G}_a(K) \rightarrow H^1(K, \mathbb{Z}/p \times \cdots \times \mathbb{Z}/p) \rightarrow \underbrace{H^1(K, \mathbb{G}_a)}_{=0} \rightarrow \cdots$$

Thus \mathbb{G}_a is a classifying scheme for $\mathbb{Z}/p \times \cdots \times \mathbb{Z}/p$, when the field k contains \mathbb{F}_{p^n} , and it follows that $\text{ed}_k(\mathbb{Z}/p \times \cdots \times \mathbb{Z}/p) = 1$.

COROLLARY 2.9. *Let n be an integer and k a field with $\text{char}(k) \nmid n$. Then*

$$\text{ed}_k(\underbrace{\mu_n \times \cdots \times \mu_n}_{r \text{ times}}) = r.$$

Proof. Since $H^1(K, \mu_n \times \cdots \times \mu_n) = K^\times/K^{\times n} \times \cdots \times K^\times/K^{\times n}$, one has a surjection of functors

$$\mathbb{G}_m \times \cdots \times \mathbb{G}_m \longrightarrow H^1(-, \mu_n \times \cdots \times \mu_n)$$

and thus $\text{ed}_k(\mu_n \times \cdots \times \mu_n) \leq r$. For the opposite inequality it suffices to remark that over an algebraic closure the group $\mu_n \times \cdots \times \mu_n$ is isomorphic to the constant group $\mathbb{Z}/n \times \cdots \times \mathbb{Z}/n$ and apply Proposition 2.7.

Applying the same cohomological-invariant techniques to quadratic forms one can prove the following result which can be found in [19].

THEOREM 2.10. *Assume that $\text{char}(k) \neq 2$. Then $\text{ed}_k(\mathbf{Q}_n) = n$.*

Proof. In Chapter I we have already shown that $\text{ed}(\mathbf{Q}_n) \leq n$ using a classifying scheme. We prove that $\text{ed}(\mathbf{Q}_n) = n$ using a non-trivial cohomological invariant: the Delzant's Stiefel-Whitney class (see [9]) denoted by ω_n .

For any field extension K/k take $L = K(t_1, \dots, t_n)$ and let $q = \langle t_1, \dots, t_n \rangle$. One has $\omega_n(q) = (t_1) \cup \cdots \cup (t_n) \in H^n(L, \mathbb{Z}/2)$ which is non-zero, as it was checked before. Hence ω_n is a non-trivial cohomological invariant of degree n . It follows that $\text{ed}(\mathbf{Q}_n) = n$.

One of the most interesting features of the use of cohomological invariants is the following application to the symmetric group. This was originally found in [7].

COROLLARY 2.11. *If $\text{char}(k) \neq 2$ one has $\text{ed}(\mathcal{S}_n) \geq \lfloor \frac{n}{2} \rfloor$.*

Proof. We have already seen that $H^1(K, \mathcal{S}_n) = \mathbf{Ét}_n(K)$. By Proposition 2.5 of Chapter I, one can assume that k is algebraically closed.

Consider now the functorial morphism

$$\begin{aligned} \mathbf{Ét}_n(K) &\longrightarrow \mathbf{Q}_n(K) \\ A &\longmapsto (\mathcal{T}_{A/K} : x \mapsto \text{Tr}_{A/K}(x^2)) \end{aligned}$$

and $\omega_m : \mathbf{Q}_n(K) \longrightarrow H^m(K, \mathbb{Z}/2)$ with $m = \lfloor \frac{n}{2} \rfloor$. We show that the composite

$$\mathbf{Ét}_n(K) \longrightarrow H^m(K, \mathbb{Z}/2)$$

2. Cohomological invariants

is a non-trivial cohomological invariant. For any field extension K/k take $L = K(t_1, \dots, t_m)$ and let

$$A \cong \begin{cases} L(\sqrt{t_1}) \times \cdots \times L(\sqrt{t_m}) & \text{if } n = 2m \\ L(\sqrt{t_1}) \times \cdots \times L(\sqrt{t_m}) \times L & \text{if } n = 2m + 1. \end{cases}$$

Clearly the matrix of the trace form expressed in the basis $\{1, \sqrt{t_i}\}$ is $\begin{pmatrix} 2 & 0 \\ 0 & 2t_i \end{pmatrix}$. Hence

$$\begin{aligned} \mathcal{T}_{A/L} &\simeq \begin{cases} \langle 2, 2t_1, \dots, 2, 2t_m \rangle & \text{if } n = 2m \\ \langle 2, 2t_1, \dots, 2, 2t_m, 1 \rangle & \text{if } n = 2m + 1 \end{cases} \\ &\simeq \langle t_1, \dots, t_m \rangle \perp \langle 1, \dots, 1 \rangle, \end{aligned}$$

since k is algebraically closed.

Thus $\omega_m(\mathcal{T}_{A/L}) = \omega_m(\langle t_1, \dots, t_m, 1, \dots, 1 \rangle) = (t_1) \cup \cdots \cup (t_m) \neq 0$.

REMARK 2.12. All the present section is due to Merkurjev except Remark 2.8 and Corollary 2.9. The proofs are a little bit more complete than the original ones.

CHAPTER III

ACTIONS, TORSORS AND GENERIC ELEMENTS

1. FREE ACTIONS AND TORSORS

We recall here some facts about actions of group schemes and torsors in order to estimate $\text{ed}(G)$. The main reference is the book of Demazure-Gabriel [10].

Let G be a group scheme over a scheme S and X an S -scheme. We say that G **acts on** X if there 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 conditions of a usual group (right) action. It follows in particular that for any morphism $T \rightarrow S$ there is an action of the group $G(T)$ on the set $X(T)$.

Recall that a group G acts freely on a set X if the stabilizer of any point of X is trivial. One can mimic this and say that a group scheme G acts **freely** on a scheme X if for any S -scheme $T \rightarrow S$ the group $G(T)$ acts freely on the set $X(T)$. One can also define the stabilizer of a point of X in the following way:

Let $x \in X$ be any point. The **scheme-theoretic stabilizer of x** is the pull-back of the diagram

$$\begin{array}{ccc} & G \times_S \{x\} & \\ & \downarrow & \\ \text{Spec}(k(x)) & \xrightarrow{x} & X \end{array}$$

where the vertical map is the composite $G \times_S \{x\} \rightarrow G \times_S X \rightarrow X$. We denote it by G_x . One shows that it is a group scheme over $\text{Spec}(k(x))$ and that it is a closed group subscheme of $G \times_S \{x\}$.

Once the vocabulary is established one has the following lemma.

LEMMA 1.1. *Let X and G be as above, everything being of finite type over $S = \text{Spec}(k)$. Then the following are equivalent*

- (i) G acts freely,
- (ii) $G_x = \{1\}$ for all points $x \in X$.

Proof. See [10], III §2 Corollary 2.3.

One can also check these conditions on \bar{k} -points, where \bar{k} denotes an algebraic closure of k .

Recall first that, for an algebraic group G over k , the Lie algebra can be defined as the kernel of the map $G(k[\tau]) \rightarrow G(k)$ where $k[\tau]$ is the algebra $k[t]/t^2$ and the map $k[\tau] \rightarrow k$ is given by $\tau \mapsto 0$. See [15] 21. A.

Let x be a point of a scheme X and denote by K its residue field. The point x is then viewed as an element of $X(K) = \text{Hom}(\text{Spec}(K), X)$ and thus also as an element of $X(K[\tau])$ which we will denote by $x_{K[\tau]}$.

LEMMA 1.2. *Let G be a group scheme of finite type over k acting on a k -scheme X of finite type.*

- (i) *Suppose $\text{char}(k) = 0$. Then G acts freely on X if and only if the group $G(\bar{k})$ acts freely on $X(\bar{k})$.*
- (i') *Suppose $\text{char}(k) > 0$. Then G acts freely on X if and only if the group $G(\bar{k})$ acts freely on $X(\bar{k})$, and for any closed point $x \in X$ the Lie algebra $\text{Lie}(G_x)$ is trivial.*

Proof. See [10], III, §2 Corollary 2.5 and Corollary 2.8. The Lie algebra $\text{Lie}(G_x)$ is called the Lie stabilizer of x .

REMARK 1.3. The second part of condition (i') can be checked easily using the following description of $\text{Lie}(G_x)$ (see [10], III, §2, proof of Proposition 2.6.). Let K be the residue field of x . Then we have

$$\text{Lie}(G_x) = \{g \in \text{Lie}(G) \otimes K[\tau] \mid g \cdot x_{K[\tau]} = x_{K[\tau]}\}.$$

REMARK 1.4. Let G act on X as above. For every scheme T consider the quotient map of sets $\pi : X(T) \rightarrow Y(T) := X(T)/G(T)$. Sending a pair $(g, x) \in G(T) \times X(T)$ to $(x, x \cdot g)$ gives a mapping

$$G(T) \times X(T) \rightarrow X(T) \times_{Y(T)} X(T).$$

If G acts freely this map is easily seen to be an isomorphism. It also says that the fibers of π are principal homogenous spaces under $G(T)$

1. Free actions and torsors

(at least when they are non-empty). The notion of G -torsor generalizes this remark in the category of schemes and is the suitable definition for defining “parametrized” principal homogenous spaces.

DEFINITION 1.5. Let G be a group scheme over Y which is flat and locally of finite type over Y . We say that a morphism of schemes $X \rightarrow Y$ is a **(flat) G -torsor over Y** if G acts on X , the morphism $X \rightarrow Y$ is flat and locally of finite type, and the map $\varphi : G \times_Y X \rightarrow X \times_Y X$ defined by

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

is an isomorphism.

This condition is equivalent to the existence of a covering $(U_i \rightarrow Y)$ for the flat topology on Y such that $X \times_Y U_i$ is isomorphic to $G \times_Y U_i$ for each i (see [18] Chapter III, Proposition 4.1). This means that X is “locally” isomorphic to G for the flat topology on Y . When the group G is smooth over Y it follows by faithfully flat descent that X is also smooth.

A morphism between two G -torsors $f : X \rightarrow Y$ and $f' : X' \rightarrow Y$ defined over the same base is simply a G -equivariant morphism $\varphi : X \rightarrow X'$ such that $f' \circ \varphi = f$. Again by faithfully flat descent it follows that any morphism between G -torsors is an isomorphism.

REMARK 1.6. Notice that if $X \rightarrow Y$ is a G -torsor, then G acts freely on X . Indeed, take $x \in X$, then the fiber of the point $(x, x) \in X \times_Y X$ under the map $\varphi : G \times_Y X \rightarrow X \times_Y X$ is isomorphic to G_x . Since φ is an isomorphism it follows that G_x is trivial for every x .

We then consider the *contravariant* functor

$$G\text{-Tors} : \mathbf{Schemes} \longrightarrow \mathbf{Sets},$$

defined by

$$G\text{-Tors}(Y) = \text{isomorphism classes of } G\text{-torsors over } Y.$$

For every morphism $f : Y' \rightarrow Y$ the corresponding map $G\text{-Tors}(f)$ is defined as follows: if $X \rightarrow Y$ a G -torsor over Y , then the image of this

torsor under $G\text{-Tors}(f)$ is the pull-back of the diagram

$$\begin{array}{ccc} & & X \\ & & \downarrow \\ Y' & \xrightarrow{f} & Y \end{array}$$

which is easily checked to be a G -torsor over Y' .

When Y is a point, say $Y = \text{Spec}(K)$, and G is smooth over K then any G -torsor $X \rightarrow \text{Spec}(K)$ gives rise to a principal homogeneous space over K . Indeed X is smooth and thus $X(K_s) \neq \emptyset$ is a principal homogenous space under $G(K_s)$, that is an element of $H^1(K, G)$. We may hence consider $G\text{-Tors}$ as a generalization of the first Galois cohomology functor over the category of fields.

Now that the notion of torsor is well-defined we have to overcome the problem of quotients.

Let G act on a S -scheme X . A morphism $\pi : X \rightarrow Y$ is called a **categorical quotient** of X by G if π is (isomorphic to) the *push-out* of the diagram

$$\begin{array}{ccc} G \times_S X & \longrightarrow & X \\ \text{pr}_2 \downarrow & & \downarrow \\ & & X \end{array}$$

In general such a quotient does not exist in the category of schemes. When it exists the scheme Y is denoted by X/G . We will not give a detailed account on the existence of quotients. We will only need the existence of a *generic quotient*, that is a G -invariant dense open subscheme U of X for which the quotient $U \rightarrow U/G$ exists. Moreover, we will need one non-trivial fact (which can be found in [11]) which asserts the existence of a generic quotient which is also a G -torsor.

THEOREM 1.7. *Let G act freely on a S -scheme of finite type X such that the second projection $G \times_S X \rightarrow X$ is flat and of finite type. Then there exists a (non-empty) G -invariant dense open subscheme U of X satisfying the following properties:*

- i) There exists a quotient map $\pi : U \rightarrow U/G$ in the category of schemes.*
- ii) π is onto, open and U/G is of finite type over S .*
- iii) $\pi : U \rightarrow U/G$ is a flat G -torsor.*

1. *Free actions and torsors*

Proof. This follows from [11], Exposé V, Théorème 8.1, p.281 where the statement is much more general and deals with groupoids. In order to recover it we make a translation: in our context the groupoid is that of §2 Exemple a) p.255 which simply defines the equivalence relation on the scheme X under the G -action. The fact that our action is free implies that the morphism $G \times_S X \rightarrow X \times_S X$ is quasi-finite, which is one of the hypotheses of Théorème 8.1.

I thank Professor Serre for pointing out to me this result and an alternative proof which can be found in a paper of Thomason ([27]).

DEFINITION 1.8. *Let G act on X . An open subscheme U which satisfies the conclusion of the above theorem will be called a **friendly** open subscheme of X .*

From now on take $S = \text{Spec}(k)$ where k is a field and G an algebraic group over k , that is we require G to be *smooth* and of finite type over k , and all the morphisms between schemes will be of finite type. Unless otherwise specified, when we say that $X \rightarrow Y$ is a G -torsor we mean that $X \rightarrow Y$ is a G_Y -torsor where G_Y is the group scheme obtained from G by base change $Y \rightarrow \text{Spec}(k)$. In this case this says that there is an isomorphism $G \times_k X \simeq X \times_Y X$.

DEFINITION 1.9. *Let $\pi : X \rightarrow Y$ be a G -torsor. For any field extension K/k 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 $\pi : X \rightarrow Y$ at y is a twisted form of G (that is locally isomorphic to G for the flat topology) and thus smooth over K . Hence X_y has a K_s -rational point x . We then set $\partial(y) =$ isomorphism class of $X_y(K_s)$.

We can paraphrase the definition in terms of cocycles: for all $\gamma \in \Gamma_K$ we have

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

Hence $\gamma \cdot x$ belongs to $X_y(K_s)$. Since $X \rightarrow Y$ is a G -torsor, there exists a unique $g(\gamma) \in G(K_s)$ such that $\gamma \cdot x = x \cdot g(\gamma)$. The assignment $\gamma \mapsto g(\gamma)$ is then a 1-cocycle and the map ∂ sends y to the class of that cocycle in $H^1(K, G)$.

DEFINITION 1.10. *We say that G acts **generically freely** on X if there exists a non-empty G -stable open subscheme U of X on which G acts freely.*

The previous considerations show in particular that, if G acts generically freely on X , then there exists a friendly open subscheme $U \subset X$ on which G acts freely (take for U the intersection of a dense open subset on which G acts freely and a friendly open subscheme). Hence the statement of the following proposition is consistent.

PROPOSITION 1.11. *Let G be an algebraic group over k acting linearly and generically free on an affine space $\mathbb{A}(V)$, where V is a finite dimensional k -vector space. Let U be a non-empty friendly open subscheme of $\mathbb{A}(V)$ on which G acts freely. Then U/G is a classifying scheme of $H^1(-, G)$. In particular we have*

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

Proof. It is sufficient to show that, for any field extension K/k , the map $\partial : U/G(K) \rightarrow H^1(K, G)$ is surjective. Let $g \in Z^1(K, G)$. We twist the action of Γ_K over V_{K_s} by setting

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

for all $\gamma \in \Gamma_K$ and $v \in V_{K_s}$. Clearly this action is Γ_K -semilinear, i.e. $\gamma * (\lambda v) = \gamma(\lambda)(\gamma * v)$ for all $\lambda \in K_s$. Hence $V_{K_s}^{(\Gamma_K, *)}$ is Zariski-dense in V_{K_s} . Since U is open, there exists an invariant point $v_0 \in U(K_s)$ for the new action $*$. We thus have

$$v_0 = \gamma * v_0 = \gamma \cdot v_0 \cdot g(\gamma)^{-1}$$

and hence $v_0 \cdot g(\gamma) = \gamma \cdot v_0$. In particular, we have for any $\gamma \in \Gamma_K$

$$\gamma \cdot \pi(v_0) = \pi(\gamma \cdot v_0) = \pi(v_0 \cdot g(\gamma)) = \pi(v_0),$$

hence $\pi(v_0) \in U/G(K)$ and maps to g under ∂ .

REMARK 1.12. Any algebraic group G acts linearly and generically freely over some vector space. Indeed, since G is isomorphic to a closed subgroup of some \mathbf{GL}_n , one can assume that $G \subset \mathbf{GL}_n$. Let $V = M_n(k)$. The group G then acts linearly on $\mathbb{A}(V)$ by (right) matrix multiplication. Now let $U = \mathbf{GL}_n$, viewed as an open subscheme of $\mathbb{A}(V)$. Clearly, the stabilizer of any matrix $M \in U(\bar{k})$ is trivial. Moreover, since the action of $\text{Lie}(G)$ is obtained by restriction of the action of $G(k[\tau])$ (where $\tau^2 = 0$), the Lie stabilizer of any closed point of U is also trivial. Hence G

1. *Free actions and torsors*

acts freely on U . The previous proposition then shows that the essential dimension of G is finite.

We now study more carefully the case of finite constant group schemes. The following lemma is probably well-known, but we have not found any reference for it, so we give a proof for the convenience of the reader.

LEMMA 1.13. *Let G be a constant group scheme, and let H be any algebraic group scheme defined over k . Then the map*

$$\mathrm{Hom}(G, H) \rightarrow \mathrm{Hom}(G(k), H(k))$$

sending $\Phi \in \mathrm{Hom}(G, H)$ to Φ_k is a bijection. Moreover, Φ is injective if and only if Φ_k is injective.

Proof. Given a morphism $\varphi : G(k) \rightarrow H(k)$, we have to show that there exists a unique morphism of group schemes $\Phi : G \rightarrow H$ such that $\Phi_k = \varphi$. We thus have to define, in a natural way, a group homomorphism $\Phi_R : G(R) \rightarrow H(R)$ for every k -algebra R . Since $G(\prod R_i) = \prod G(R_i)$ and since every commutative ring is product of connected rings one may assume that R is connected. In this case, since G is constant, one has $G(R) = G = G(k)$ and one then defines Φ_R to be the composite $G(R) = G(k) \rightarrow H(k) \rightarrow H(R)$. This proves the first part of the statement.

Since Φ is a natural map and $G(\bar{k}) = G(k)$, it follows that $\Phi_{\bar{k}}$ is the composite of Φ_k and of the inclusion $H(k) \hookrightarrow H(\bar{k})$. Hence, if Φ_k is injective, then $\Phi_{\bar{k}}$ is also injective. Since the Lie algebra of a constant group scheme is trivial, Proposition 22.2 of [15] implies that Φ is injective.

PROPOSITION 1.14. *Let V be a finite dimensional k -vector space, and let G be a finite constant group scheme over k . Then G acts linearly and generically freely on $\mathbb{A}(V)$ if and only if the abstract group G is isomorphic to a subgroup of \mathbf{GL}_V . In this case, we have*

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

Proof. If G is isomorphic to a subgroup of \mathbf{GL}_V , then there exists a group morphism $\varphi : G(k) \hookrightarrow \mathbf{GL}_V(k)$. Let $\Phi : G \rightarrow \mathbf{GL}_V$ be the injective morphism of group schemes extending φ . It corresponds to a linear (faithful) action of G on V . We now prove that this action is generically free.

For any $g \in G(k)$ with $g \neq 1$ and any k -algebra R , set

$$F_g(R) = \{v \in V_R \mid \varphi(g)_R(v) = v\},$$

where $\varphi(g)_R$ is the composite of $\varphi(g)$ and $\mathbf{GL}_V(k) \hookrightarrow \mathbf{GL}_V(R)$. Then $F = \bigcup_{g \neq 1} F_g$ is a G -stable closed subscheme of $\mathbb{A}(V)$, which is not equal to $\mathbb{A}(V)$ since $G(k) \hookrightarrow \mathbf{GL}_V(k)$ is injective. Consequently, $U = \mathbb{A}(V) - F$ is a non-empty G -stable dense open subset of $\mathbb{A}(V)$. As pointed out previously, we have $G(\bar{k}) = G(k)$ and the map $\Phi_{\bar{k}}$ is just the composite of φ and $\mathbf{GL}_V(k) \hookrightarrow \mathbf{GL}_V(\bar{k})$. Hence, the stabilizer of $v \in V_{\bar{k}}$ is equal to the set $\{g \in G(k) \mid \varphi(g)_{\bar{k}}(v) = v\}$. By choice of U , this stabilizer is trivial for any $v \in U(\bar{k})$. Moreover, the condition on Lie stabilizers is automatically fulfilled, since the Lie algebra of any finite constant group is trivial. Hence G acts freely on U , so G acts generically freely on $\mathbb{A}(V)$. The converse is clear. The last statement is a direct application of the Proposition 1.11.

This proposition helps in the computation of the essential dimension of finite abelian groups over sufficiently big fields.

COROLLARY 1.15. *Let G be a finite abelian group and k a field with $\text{char}(k) \nmid \exp(G)$. If the field k contains all the $\exp(G)$ -th roots of unity, then*

$$\text{ed}_k(G) = \text{rank}(G).$$

In particular, if G is cyclic then $\text{ed}_k(G) = 1$.

Proof. By Proposition 2.7 of Chapter II we only have to prove that $\text{ed}_k(G) \leq \text{rank}(G)$. Let $n = \text{rank}(G)$ and write $G \cong \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_n$ where $d_1 \mid d_2 \mid \cdots \mid d_n$. By hypothesis, we have $k \supset \mu_{d_n} \supset \cdots \supset \mu_{d_1}$. We then have the following injection

$$G \cong \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_n \longrightarrow \mathbf{GL}_n(k)$$

$$([m_1], \dots, [m_n]) \mapsto \begin{pmatrix} \zeta_1^{m_1} & & 0 \\ & \ddots & \\ 0 & & \zeta_n^{m_n} \end{pmatrix}$$

where ζ_i denotes a primitive d_i -th root of unity. Now apply the previous proposition.

We will see later on that the computation is much more complicated when no roots of unity are assumed to be in the base field.

An action of an algebraic group G on a scheme X is called **faithful** if G is isomorphic to a subgroup of $\text{Aut}(X)$ via this action. Proposition 1.14

1. *Free actions and torsors*

above then shows that for a finite constant group G , faithful actions on a vector space V correspond to generically free actions on V .

Here is another application of faithful actions which concerns dihedral groups $D_n = \mathbb{Z}/n \rtimes \mathbb{Z}/2$ for a natural integer n . We will use the classical presentation $D_n = \langle \sigma, \tau \mid \sigma^n = \tau^2 = 1, \tau\sigma\tau^{-1} = \sigma^{-1} \rangle$.

COROLLARY 1.16. *Let k be a field of characteristic $p \geq 0$ and n a natural integer such that $p \nmid n$ and $\mu_n \subset k^\times$. Then $\text{ed}_k(D_n) \leq 2$.*

Proof. Let ζ a n -th primitive root of unity and define an homomorphism $D_n \rightarrow \mathbf{GL}_2(k)$ by sending σ to $\begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}$ and τ to $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. One can easily show that this gives an injective group homomorphism, and then apply Proposition 1.14.

For the groups D_4 and D_6 , one can even drop the assumptions on the field at least when $\text{char}(k) \neq 2$: actually,

$$\begin{aligned} D_4 &\longrightarrow \mathbf{GL}_2(k) \\ \sigma &\longmapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ \tau &\longmapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned}$$

and

$$\begin{aligned} D_6 &\longrightarrow \mathbf{GL}_2(k) \\ \sigma &\longmapsto \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \\ \tau &\longmapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

are both faithful representations. Hence $\text{ed}_k(D_4) \leq 2$ and $\text{ed}_k(D_6) \leq 2$ for any field k of characteristic $\neq 2$.

In the sequel we will not only deal with faithful linear representations but also with projective ones. The following lemma is proven in the same way as the linear case.

LEMMA 1.17. *Let G be a finite constant group scheme over k . Then G acts generically freely on $\mathbb{P}(V)$ if and only if the abstract group G is isomorphic to a subgroup of $\mathbf{PGL}(V)$.*

The following proposition is one of the most important ingredients for the computations of the essential dimension of cubics which will be performed in Chapter V. It is a direct application of Proposition 1.11.

PROPOSITION 1.18. *Let G be a finite constant closed subgroup of \mathbf{PGL}_n defined over k , and let \tilde{G} be the inverse image of G under the canonical projection $\pi : \mathbf{GL}_n \longrightarrow \mathbf{PGL}_n$. Then*

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

Proof. The inclusion $\tilde{G} \subset \mathbf{GL}_n$ induces a natural action of \tilde{G} on \mathbb{A}^n . The idea is to show that this action is generically free using Lemma 1.2. We will now go into the details.

By 1.17 above, the group G acts generically freely on \mathbb{P}^{n-1} . Let U be a G -stable dense open subset of \mathbb{P}^{n-1} on which G acts freely. Let \tilde{U} be the inverse image of U under the quotient map $\mathbb{A}^n - \{0\} \longrightarrow \mathbb{P}^{n-1}$. Clearly this is a \tilde{G} -dense open subset of \mathbb{A}^n . We now show that the group \tilde{G} acts freely on \tilde{U} .

Let $\tilde{u} \in \tilde{U}(k_s)$ and $\tilde{g} \in \tilde{G}(k_s)$ such that $\tilde{g} \cdot \tilde{u} = \tilde{u}$. Let $g = \pi(\tilde{g}) \in G(k_s)$ and let $u \in \mathbb{P}^{n-1}(k_s)$ be the image of \tilde{u} under the quotient map. Then we have $g \cdot u = u$, so $g = 1$ by assumption on U and \tilde{g} is then a scalar matrix, which is easily seen to be the identity using the relation $\tilde{g} \cdot \tilde{u} = \tilde{u}$, so $\tilde{G}(k_s)$ acts freely on $\tilde{U}(k_s)$.

We now have to check the condition on the Lie algebra. Recall that the Lie algebra of G is the Lie algebra of its connected component, which is \mathbb{G}_m , so $\mathrm{Lie}(\tilde{G}) = k$, where k is identified with the subgroup of scalar matrices. It readily follows that condition (i') of Lemma 1.2 above is satisfied.

Thus the action of \tilde{G} on \mathbb{A}_k^n satisfy the conditions of Proposition 1.11. Hence

$$\mathrm{ed}(\tilde{G}) \leq \dim(\mathbb{A}^n) - \dim(\tilde{G}) = n - 1.$$

REMARK 1.19. The present section is directly inspired by the work of Merkurjev. In particular Propositions 1.11, 1.14 and Corollary 1.15 can be found in [17]. However, all the previous presentation takes care of many technical details which were not pointed out in Merkurjev's paper. Proofs are consequently a little bit longer and a great attention is given to working without any assumption on the characteristic of the ground field. Proposition 1.18 above is a new result.

2. Versal pairs and Rost's definition

2. VERSAL PAIRS AND ROST'S DEFINITION

In this section we define another notion of essential dimension and compare it with the one introduced at the beginning. The ideas described below are based on the paper [21] where Rost computes $\text{ed}(\mathbf{PGL}_4)$. We therefore call it Rost's essential dimension.

Let k be a field and \mathfrak{A}_k be the category of *all* (associative and unital) commutative k -algebras with homomorphism of k -algebras (sending 1 to 1) as morphisms. Every functor $\mathbf{F} : \mathfrak{A}_k \rightarrow \mathbf{Sets}$ by restriction defines a functor $\mathfrak{C}_k \rightarrow \mathbf{Sets}$ hence an object of \mathfrak{F}_k . We shall define the notion of essential dimension for a special class of functors $\mathbf{F} : \mathfrak{A}_k \rightarrow \mathbf{Sets}$.

Let K/k be an object of \mathfrak{C}_k . For a local k -subalgebra \mathcal{O} of K , with maximal ideal \mathfrak{m} , we will write $\kappa(\mathcal{O}) = \mathcal{O}/\mathfrak{m}$ for its residue field and $\pi : \mathcal{O} \rightarrow \kappa(\mathcal{O})$ for the quotient map.

DEFINITION 2.1. *Let K, L be two extensions of k . A **pseudo k -place** $f : K \rightsquigarrow L$ is a pair $(\mathcal{O}_f, \alpha_f)$ where \mathcal{O}_f is a local k -subalgebra of K and $\alpha_f : \kappa(\mathcal{O}_f) \rightarrow L$ is a morphism in \mathfrak{C}_k .*

Let $\mathbf{F} : \mathfrak{A}_k \rightarrow \mathbf{Sets}$ be a functor and take $f : K \rightsquigarrow L$ a pseudo k -place. We say that an element $a \in \mathbf{F}(K)$ is **unramified** in f if a belongs to the image of the map $\mathbf{F}(\mathcal{O}_f) \rightarrow \mathbf{F}(K)$. In this case we define the **set of specializations of a** to be

$$f^*(a) = \{ \mathbf{F}(\alpha_f \circ \pi)(c) \mid c \in \mathbf{F}(\mathcal{O}_f) \text{ with } c_K = a \}.$$

We say that a pair (a, K) with $a \in \mathbf{F}(K)$ is a **versal pair for \mathbf{F}** (over k) if for every extension L/k and every element $b \in \mathbf{F}(L)$ there exists a pseudo k -place $f : K \rightsquigarrow L$ such that a is unramified in f and such that $b \in f^*(a)$.

Here is a picture of the situation:

$$\begin{array}{ccc} \mathcal{O} & \longrightarrow & K \\ \pi \downarrow & & \\ \kappa(\mathcal{O}) & \xrightarrow{\alpha_f} & L \end{array} \quad \Rightarrow \quad \begin{array}{ccc} \mathbf{F}(\mathcal{O}) & \longrightarrow & \mathbf{F}(K) \ni a \\ \downarrow & & \\ \mathbf{F}(\kappa(\mathcal{O})) & \longrightarrow & \mathbf{F}(L) \ni b \end{array}$$

EXAMPLE 2.2. Let X be an irreducible k -scheme, $k(X)$ its function field and $\eta : \text{Spec}(k(X)) \rightarrow X$ the unique morphism whose image is the generic point of X . Then $(\eta, k(X))$ is a versal pair for X .

Indeed, take $x : \text{Spec}(L) \rightarrow X$ an element in $X(L)$. Then the local ring $\mathcal{O}_{X,x}$ at the point x is naturally a subring of $k(X)$ and there is a canonical morphism from the residue field $k(x)$ to L giving a pseudo k -place $k(X) \rightsquigarrow L$ with the desired property.

DEFINITION 2.3. Let $\mathbf{F} : \mathfrak{A}_k \rightarrow \mathbf{Sets}$ be a functor which has a versal pair. We define its **(Rost's) essential dimension** (denoted by $\text{ed}'(\mathbf{F})$) to be the minimum of the transcendence degree of the field of definition for versal pairs. More precisely $\text{ed}'(\mathbf{F}) = \min \text{trdeg}(K : k)$ for all K/k such that there exists an element $a \in \mathbf{F}(K)$ making (a, K) into a versal pair for \mathbf{F} .

REMARK 2.4. In the paper of Rost ([21]) the notion is a little bit different. What is called k -place in his context is a pseudo k -place where \mathcal{O} is required to be a valuation ring. Every k -place is then trivially a pseudo k -place. However the converse is not true in general. Indeed for a local ring \mathcal{O} in a field K one can always find a valuation whose local ring \mathcal{O}_v dominates it but there is no control on the residue field.

DEFINITION 2.5. Let $\mathbf{F} : \mathfrak{A}_k \rightarrow \mathbf{Sets}$ be a functor which has a versal pair. We say that a versal pair (a, K) is **nice** if for any $L \subset K$ and $a' \in \mathbf{F}(L)$ such that $a = a'_K$, the pair (a', L) is versal. We say that \mathbf{F} is **nice** if it has a nice versal pair.

PROPOSITION 2.6. Let $\mathbf{F} : \mathfrak{A}_k \rightarrow \mathbf{Sets}$ be a functor which has a versal pair. Then we have

$$\text{ed}_k(\mathbf{F}) \leq \text{ed}'_k(\mathbf{F})$$

where on the left \mathbf{F} is viewed as a functor on \mathfrak{C}_k . Moreover, if \mathbf{F} is nice, then

$$\text{ed}'_k(\mathbf{F}) = \text{ed}_k(\mathbf{F}) = \text{ed}(a),$$

where (a, K) is any nice versal pair.

2. Versal pairs and Rost's definition

Proof. Let L/k be any field extension, and let $b \in \mathbf{F}(L)$. Let (a, K) be a versal pair such that $\text{trdeg}(K : k) = \text{ed}'_k(\mathbf{F})$. Since (a, K) is versal, then b comes from an element of $\mathbf{F}(\kappa(\mathcal{O}))$ for some local ring \mathcal{O} . Then $\text{ed}(b) \leq \text{trdeg}(\kappa(\mathcal{O}) : k) \leq \text{trdeg}(K : k)$. This proves the first assertion.

Let now (a, K) be a nice versal pair (notice that $\text{trdeg}(K : k)$ is not necessarily minimal). Take a subextension $k \subset L \subset K$ with an element $a' \in \mathbf{F}(L)$ such that $a = a'_L$ and $\text{trdeg}(L : k) = \text{ed}(a)$. By assumption, (a', L) is versal, so $\text{ed}'_k(\mathbf{F}) \leq \text{trdeg}(L : k) = \text{ed}(a) \leq \text{ed}_k(\mathbf{F})$. This concludes the proof.

REMARK 2.7. All the present section is inspired by the work of Rost which can be found in [21].

3. GENERIC TORSORS AND COMPRESSIONS

Now that we have seen the notion of versal pairs we want to apply it to $H^1(-, G)$ when viewed as a functor over \mathfrak{A}_k . That is we consider the functor G -**Tors** over the category of affine k -schemes. This section deals with compressions of torsors and is closely related to Reichstein's original discussion. Compare with [19] where everything is done over an algebraically closed field. For the definition of generic torsors we follow [13].

Let G be an algebraic group over k . If G acts linearly and generically freely on a vector space V , there exists an open subscheme $U \subseteq \mathbb{A}(V)$ such that $\pi : U \rightarrow U/G = Y$ is a G -torsor. We have defined a map (see Definition 1.9)

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

and proved that ∂ is surjective (see Proposition 1.11). Actually, we have shown a little more: for every torsor $P \in H^1(K, G)$, there exists a non-empty subset S of Y such that the isomorphism class of $\pi^{-1}(y)$ is equal to P for every $y \in S(K)$. Such an S is a Zariski-dense subset of Y if K is infinite.

This leads naturally to the following definition:

DEFINITION 3.1. *Let $f : X \rightarrow Y$ be a G -torsor with Y irreducible. We say that it is **classifying for G** if, for any field extension k'/k with k' infinite and for any principal homogenous space P' of G over k'/k , the set of points $y \in Y(k')$ such that P' is isomorphic to the fiber $f^{-1}(y)$ is dense in Y . In particular we have a surjection of functors $Y \twoheadrightarrow H^1(-, G)$ showing that Y is a classifying scheme of G .*

REMARK 3.2. Proposition 1.11 and Remark 1.12 show that a classifying G -torsor always exist for any algebraic group G . Moreover one can always find a reduced classifying torsor for G . Indeed take $X \rightarrow Y$ a classifying torsor for G and let $\varphi : Y_{\text{red}} \rightarrow Y$ the reduced scheme of Y with its canonical map. Then pulling back $X \rightarrow Y$ along φ gives a torsor which is isomorphic to $X_{\text{red}} \rightarrow Y_{\text{red}}$ and which is also classifying.

3. Generic torsors and compressions

DEFINITION 3.3. We call **generic torsor over G** the generic fiber of a classifying G -torsor $X \rightarrow Y$, i.e. the pullback of

$$\begin{array}{ccc} & X & \\ & \downarrow & \\ \mathrm{Spec}(k(Y)) & \longrightarrow & Y \end{array}$$

where $\mathrm{Spec}(k(Y)) \rightarrow Y$ is the generic point. If $P \rightarrow \mathrm{Spec}(k(Y))$ is such a generic torsor it can be viewed as an element of $H^1(k(Y), G)$.

More precisely one can restate the definition in the following way. Let G be an algebraic group over k , K a field extension of k and $P \rightarrow \mathrm{Spec}(K)$ a G -torsor. We say that P is **k -versal** or **k -generic** if

i) there exists an irreducible scheme Y (whose generic point is denoted by η) with function field $k(Y) \simeq K$ (such a scheme is called a model of K) and a G -torsor $f : X \rightarrow Y$ whose generic fiber $f^{-1}(\eta) \rightarrow \mathrm{Spec}(K)$ is isomorphic to $P \rightarrow \mathrm{Spec}(K)$. In other words

$$\begin{array}{ccc} P & \longrightarrow & X \\ \downarrow & & \downarrow \\ \mathrm{Spec}(K) & \longrightarrow & Y \end{array}$$

is a pull-back.

ii) For every extension k'/k with k' infinite, for every non-empty open set U of Y and for every G -torsor $P' \rightarrow \mathrm{Spec}(k')$, there exists a k' -rational point $x \in U$ such that $f^{-1}(x) \simeq P'$.

REMARK 3.4. If $f : X \rightarrow Y$ is a classifying G -torsor, then, for any non-empty open subset U of Y , the map $f : f^{-1}(U) \rightarrow U$ is also a classifying torsor. This says that generic torsors over G correspond bijectively to birational classes of classifying torsors for G .

LEMMA 3.5. *Let $P \rightarrow \text{Spec}(k(Y))$ a generic torsor. Then $(P, k(Y))$ is a versal pair for G -Tors.*

Proof. Take $T \rightarrow \text{Spec}(L)$ any torsor defined over L/k . Since $X \rightarrow Y$ is a classifying torsor there exists a L -rational point $y : \text{Spec}(L) \rightarrow Y$ such that $T \rightarrow \text{Spec}(L)$ fits into a pull-back

$$\begin{array}{ccc} T & \longrightarrow & X \\ \downarrow & & \downarrow \\ \text{Spec}(L) & \longrightarrow & Y \end{array}$$

Take $\mathcal{O}_{Y,y}$ the local ring at the point y and let $\varphi : \text{Spec}(\mathcal{O}_{Y,y}) \rightarrow Y$ be the canonical morphism. Consider $P' \rightarrow \text{Spec}(\mathcal{O}_{Y,y})$ the torsor obtained by pulling-back $X \rightarrow Y$ along φ . The local ring $\mathcal{O}_{Y,y}$ is naturally a sub- k -algebra of $k(Y)$ and we have a diagram

$$\begin{array}{ccc} P & \xrightarrow{\quad} & X \\ \downarrow & \dashrightarrow & \downarrow \\ \text{Spec}(k(Y)) & \xrightarrow{\quad} & Y \\ & \searrow & \downarrow \varphi \\ & & \text{Spec}(\mathcal{O}_{Y,y}) \end{array}$$

showing that $P \rightarrow \text{Spec}(k(Y))$ comes from a torsor over $\text{Spec}(\mathcal{O}_{Y,y})$. Moreover the morphism $y : \text{Spec}(L) \rightarrow Y$ factorizes through $\text{Spec}(k(y))$ and, if we denote by $P'' \rightarrow \text{Spec}(k(y))$ the torsor obtained by pulling-back $P' \rightarrow \text{Spec}(\mathcal{O}_{Y,y})$ along the morphism $\text{Spec}(k(y)) \rightarrow \text{Spec}(\mathcal{O}_{Y,y})$, one has the following diagram

$$\begin{array}{ccc} & T & \longrightarrow & X \\ & \downarrow & & \downarrow \\ P'' & \xrightarrow{\quad} & P' & \longrightarrow & X \\ \downarrow & & \downarrow & & \downarrow \\ \text{Spec}(k(y)) & \xrightarrow{\quad} & \text{Spec}(L) & \xrightarrow{y} & Y \\ & \searrow & \downarrow & & \downarrow \varphi \\ & & \text{Spec}(\mathcal{O}_{Y,y}) & & \end{array}$$

This shows that $T \rightarrow \text{Spec}(L)$ comes from $P'' \rightarrow \text{Spec}(k(y))$. Thus the local ring $\mathcal{O}_{Y,y}$ together with the morphism $k(y) \rightarrow L$ form the desired pseudo k -place showing that $(P, k(Y))$ is a versal pair.

3. Generic torsors and compressions

REMARK 3.6. In the proof of the preceding lemma the density hypothesis in the definition of a classifying torsor is not used. This hypothesis will be used when talking about compressions.

REMARK 3.7. Notice that when Y is smooth over k , the local ring $\mathcal{O}_{Y,y}$ of any point of Y is dominated by a valuation ring whose residue field is equal to $k(y)$. It follows in this case that any pseudo k -place defines a k -place in the sense of Rost (see [21]). Since we do not have a precise reference for this result we have decided to deal only with pseudo k -places.

Actually we will see that a generic torsor give rise to a nice versal pair. We first need a definition

DEFINITION 3.8. Let $f : X \rightarrow Y$ and $f' : X' \rightarrow Y'$ be two G -torsors. We say that f' is a **compression** of f if there is a diagram

$$\begin{array}{ccc} X & \xrightarrow{g} & X' \\ f \downarrow & & \downarrow f' \\ Y & \xrightarrow{h} & Y' \end{array}$$

where g is a G -equivariant rational dominant morphism and h is a rational morphism too. The **essential dimension** of a G -torsor f is the smallest dimension of Y' in a compression f' of f . We still denote this by $\text{ed}(f)$.

REMARK 3.9. Take as above a compression of $f : X \rightarrow Y$ and let $U \subseteq Y$ the open subscheme on which h is defined. Taking the pull-back of $X' \rightarrow Y'$ along h one obtains a G -torsor $f'' : P \rightarrow U$ which fits into a diagram

$$\begin{array}{ccccc} X & \dashrightarrow & P & \longrightarrow & X' \\ f \downarrow & & \downarrow f'' & & \downarrow f' \\ Y & \dashrightarrow & U & \longrightarrow & Y' \end{array}$$

and f'' is a compression too.

The following simple result will be helpful in the sequel.

LEMMA 3.10. *Let $g : X \dashrightarrow X'$ be a rational dominant G -equivariant morphism between generically free schemes. Then there exists X_0 (resp. X'_0) a friendly open subscheme of X (resp. of X') such that g induces a compression of torsors*

$$\begin{array}{ccc} X_0 & \xrightarrow{-g-} & X'_0 \\ \downarrow & & \downarrow \\ X_0/G & \xrightarrow{-h-} & X'_0/G \end{array}$$

Proof. Take U some friendly open subscheme of X . Since g is dominant one can find U' , open subscheme of X' , which lies in the image of g . Intersecting U' with some friendly open set of X' gives a friendly open set X'_0 in the image of U . Then $X_0 = g^{-1}(X'_0)$ is the desired open set.

LEMMA 3.11. *Let $f : X \rightarrow Y$ be a G -torsor with Y irreducible and reduced. Let $T \rightarrow \text{Spec}(k(Y))$ be its generic fiber. Then $\text{ed}(f) = \text{ed}(T)$.*

Proof. Let f and T be as above. Let $f' : X' \rightarrow Y'$ be a compression of f and $T' \rightarrow \text{Spec}(k(Y'))$ its generic fiber. By Remark 3.9 above, and since the generic fiber of f is isomorphic to the generic fiber of f' , one can suppose that the compression is a pull-back. The cube

$$\begin{array}{ccccc} & & T & \longrightarrow & X \\ & \swarrow & \downarrow & & \downarrow \\ T' & \longrightarrow & X' & & Y \\ & \searrow & \downarrow & \longrightarrow & \downarrow \\ & & \text{Spec}(k(Y)) & \longrightarrow & Y \\ \downarrow & & \swarrow & & \downarrow \\ \text{Spec}(k(Y')) & \longrightarrow & Y' & & \end{array}$$

then shows that T' maps to T under $H^1(k(Y'), G) \rightarrow H^1(k(Y), G)$. Hence $\text{ed}(T) \leq \text{ed}(f)$.

Conversely suppose there is a subextension $k \subseteq K' \subseteq K := k(Y)$ together with a principal homogenous space T' over K' such that T' maps to T under $H^1(K', G) \rightarrow H^1(k(Y), G)$. We have to find a G -torsor $f' : X' \rightarrow Y'$ such that T' is isomorphic to its generic fiber and a compression from f to f' .

First remark that one can suppose everything to be affine. Indeed the generic point of Y lies in some open affine subset U and T is also the generic fiber of the G -torsor $f^{-1}(U) \rightarrow U$.

3. Generic torsors and compressions

We now rewrite the problem in terms of rings:

let $Y = \text{Spec}(A)$, $X = \text{Spec}(B)$, $T = \text{Spec}(P)$, $T' = \text{Spec}(P')$ and let $k[G]$ denote the algebra of G . We know that K is the field of fractions of A (since Y is reduced), that $P \simeq B \otimes_A K$ and $P \simeq P' \otimes_{K'} K$. We have to find a subring A' of K' whose field of fractions is K' , a G -torsor B'/A' such that $P' \simeq B' \otimes_{A'} K'$ and a rational compression from B'/A' to B/A .

Since K is of finite type over k we can write it as $K = k(\alpha)$ where (α) is a short notation for $(\alpha_1, \dots, \alpha_n)$. Similarly, since P is of finite type over K we write it $P = K[\beta]$ for some β_1, \dots, β_m . In the same way we write $K' = k(\alpha')$ and $P' = K'[\beta']$.

We will take for A' a localisation of the ring $k[\alpha']$ for which the isomorphism $P' \otimes_{K'} P \simeq P' \otimes_k k[G]$ is defined. More precisely, since both $P' \otimes_{K'} P$ and $P' \otimes_k k[G]$ are finitely generated algebras over K' one can find a polynomial f in the α'_i such that $B' \otimes_{A'} B \simeq B' \otimes_k k[G]$ where $A' = k[\alpha']_f$ and $B' = A'[\beta']$ (since there is only a finite number of polynomials to invert in order to define the isomorphism).

Now obviously $P' \simeq B' \otimes_{A'} K'$ and we just have to find a rational morphism from A' to A and this will induce a rational compression from B'/A' to B/A . This is easily done since the image of A' under the map $A' \subset K' \subset K$ lies in a subring of the form $k[\alpha]_g$ for some polynomial g in the α_i (again one has only to invert the polynomials that appear in the image of the α'_i which are only finite in number). Now $A = k[\alpha]_h$ for some polynomial h and we have a natural map $A' \rightarrow k[\alpha]_g \rightarrow (k[\alpha]_g)_h = A_g$. In the same way one finds a rational map $B' \rightarrow B_p$ compatible with the previous one.

It follows that $\text{ed}(f) \leq \text{ed}(T)$ and the proof is complete.

REMARK 3.12. The hypothesis “reduced” on Y can be dropped easily arguing with $A/\text{Nil}(A)$ rather than A . Since Remark 3.2 tells that one can always find a reduced classifying torsor this will not be proved.

LEMMA 3.13. *Let $f' : X' \rightarrow Y'$ be a compression of a classifying torsor $f : X \rightarrow Y$. Then f' is also classifying.*

Proof. Let

$$\begin{array}{ccc} X & \xrightarrow{g} & X' \\ f \downarrow & & \downarrow f' \\ Y & \xrightarrow{h} & Y' \end{array}$$

be such a compression. Take k'/k a field extension with k' infinite and $P' \in H^1(k', G)$. Since f is classifying one can find a k' -rational point $y \in Y(k')$ which lies in U , the open set on which h is defined, such that $f^{-1}(y) \simeq P'$. Then the fiber of f' at $h(y)$ clearly gives a torsor isomorphic to P' .

COROLLARY 3.14. *Let $T \rightarrow \text{Spec}(K)$ be a generic G -torsor, $K' \subset K$ and $T' \rightarrow \text{Spec}(K')$ such that $T'_K = T$. Then T' is also a generic torsor.*

Proof. Take a classifying G -torsor $X \rightarrow Y$ which is a model for T . Then, by the proof of Lemma 3.11, defining T over a smaller field means compressing the torsor $X \rightarrow Y$. Since the compression of a classifying torsor is again classifying it follows that T comes from a generic torsor.

COROLLARY 3.15. *The functor $G\text{-Tors}$ is nice.*

Proof. We have to show $G\text{-Tors}$ has a nice versal pair. But a generic torsor defines a versal pair and niceness is ensured by the previous corollary.

COROLLARY 3.16. *Let G be an algebraic group defined over k and let $T \in H^1(K, G)$ be a generic torsor. Then $\text{ed}'_k(G) = \text{ed}_k(G) = \text{ed}(T)$.*

Proof. As pointed out above, any generic torsor gives rise to a nice versal pair and we can apply Proposition 2.6.

PROPOSITION 3.17. *Let G be an algebraic group acting linearly and generically freely on $\mathbb{A}(V)$ where V is some vector space. Suppose that the G -action induced on $\mathbb{P}(V)$ is again generically free. Then*

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

Proof. The map $\mathbb{A}(V) \setminus \{0\} \rightarrow \mathbb{P}(V)$ gives a rational G -equivariant map from $\mathbb{A}(V) \rightarrow \mathbb{P}(V)$ which gives a compression of the corresponding torsors in view of Lemma 3.10 above.

3. Generic torsors and compressions

COROLLARY 3.18. *Let G be a finite constant group scheme over k . Suppose that there is an injective map $\rho : G \hookrightarrow \mathbf{GL}_n(k)$ such that $\pi \circ \rho$ stays injective where $\pi : \mathbf{GL}_n(k) \rightarrow \mathbf{PGL}_n(k)$ is the canonical projection. Then $\text{ed}(G) \leq n - 1$.*

Proof. Indeed G acts generically freely on \mathbb{A}^n and by Lemma 1.17 on \mathbb{P}^n too. We can thus apply the above result.

At this point we are able to explain the behaviour of the essential dimension of G with respect to a closed subgroup.

THEOREM 3.19. *Let G be an algebraic group and H a closed algebraic subgroup of G . Then*

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

In particular, if G is finite, we have

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

Proof. Let $\mathbb{A}(V)$ be an affine space on which G acts generically freely. Take U open in $\mathbb{A}(V)$ such that U/G and U/H both exist and are torsors. Now take

$$\begin{array}{ccc} U & \xrightarrow{g} & X \\ \downarrow & & \downarrow \\ U/G & \xrightarrow{h} & Y \end{array}$$

a G -compression such that $\dim(Y) = \text{ed}(G)$. Since the stabilizer in H of a point x is a subgroup of G_x it follows that H acts generically freely on U and on X too. Now g is also H -equivariant and by the Lemma 3.10 above g gives rise to an H -compression of $U \rightarrow U/H$. It then follows that $\text{ed}(H) \leq \dim(X) - \dim(H) = \dim(Y) + \dim(G) - \dim(H) = \text{ed}(G) + \dim(G) - \dim(H)$.

This provides another proof of the following

COROLLARY 3.20. *If $\text{char}(k) \neq 2$ one has $\text{ed}(\mathcal{S}_n) \geq \lfloor \frac{n}{2} \rfloor$.*

Proof. We have $H = \underbrace{\mathbb{Z}/2 \times \cdots \times \mathbb{Z}/2}_{\lfloor \frac{n}{2} \rfloor \text{ times}} \subset \mathcal{S}_n$. But we have seen that the

essential dimension of a finite 2-torsion elementary abelian group is equal to its rank if $\text{char}(k) \neq 2$. One concludes using the preceding theorem.

We finally give a proposition that may be used for giving lower bounds on $\text{ed}(G)$. The argument of the proof below is due to Z. Reichstein.

PROPOSITION 3.21. *Let G be an algebraic group over k and denote by G^0 its connected component. If $\text{ed}_k(G) = 1$ then G/G^0 is isomorphic to a finite subgroup of \mathbf{PGL}_2*

Proof. The fact that G/G^0 is finite is well known. Let $\mathbb{A}(V)$ be an affine space on which G acts generically freely. Let $U \subseteq \mathbb{A}(V)$ be a friendly open subscheme and let $X \rightarrow Y$ a G -torsor together with a compression of the generic torsor $U \rightarrow U/G$

$$\begin{array}{ccc} U & \dashrightarrow & X \\ \downarrow & & \downarrow \\ U/G & \dashrightarrow & Y \end{array}$$

Now G acts freely on X (by Remark 1.6) and hence G^0 too. Then the quotient X/G^0 exists and G/G^0 acts freely on it. It follows that there is a monomorphism of group schemes $G/G^0 \rightarrow \text{Aut}(X/G^0)$. Now $\mathbb{A}(V)$ is rational and thus X/G^0 is unirational. But

$$\dim(X/G^0) = \dim(X) - \dim(G^0) = \dim(X) - \dim(G) = \dim(Y) = 1$$

and then by a theorem of Lüroth X/G^0 is birationally equivalent to \mathbb{P}^1 . Thus $\text{Aut}(X/G^0) \cong \mathbf{PGL}_2$. It follows that G/G^0 is isomorphic to a subgroup of \mathbf{PGL}_2 .

REMARK 3.22. The above discussion is longer than Merkurjev's one. Many details are given and proofs are completed. However the philosophy introduced here is due to Merkurjev which was himself inspired by Reichstein's work. Proposition 3.21 is a new result which was pointed out to us by Professor Jean-Pierre Serre.

CHAPTER IV

APPLICATIONS

1. SOME FINITE GROUPS

In this section we will compute the essential dimension of some constant group schemes. We first deal with some generalities and an application to the symmetric group (which can originally be found in [7]). Groups of the form \mathbb{Z}/n and dihedral groups are then studied more carefully.

In what follows G will denote a finite constant group scheme over k .

We first recall that if G is such a group, then any linear generically free action on a vector space V is actually a faithful representation (see Chapter III, Proposition 1.14). Since G is finite and acts faithfully on the field of functions $k(V)$, this gives rise to a Galois extension $k(V)/k(V)^G$. This is indeed a generic torsor for G by our previous considerations. Now any subfield $E \subseteq k(V)$ on which G acts faithfully gives rise in the same way to a Galois extension E/E^G . From this remark we have the following proposition which is the definition of essential dimension in [7]

PROPOSITION 1.1. *Let G be a finite constant group scheme over k acting faithfully on a k -vector space V . Then the essential dimension of G is the minimum of the $\text{trdeg}(E : k)$ for all the fields $E \subseteq k(V)$ on which G acts faithfully.*

Application to \mathcal{S}_n .

In this example we suppose that $\text{char}(k) \neq 2$.

With this assumption on the ground field, \mathcal{S}_n acts faithfully on the hyperplane $H = \{ x \in \mathbb{A}_k^n \mid x_1 + \cdots + x_n = 0 \}$ and thus on $k(x_1, \dots, x_{n-1})$. But on $k(x_1, \dots, x_{n-1})$ we have a multiplicative action, i.e. a \mathbb{G}_m -action, given by $\lambda \cdot x_i = \lambda x_i$ for all $\lambda \in \mathbb{G}_m(k)$ and all $i = 1, \dots, n-1$. This action commutes with the action of \mathcal{S}_n . We easily see that

$$k(x_1, \dots, x_{n-1})^{\mathbb{G}_m} = k(x_1/x_{n-1}, \dots, x_{n-2}/x_{n-1}).$$

Now, if $n \geq 3$, the group \mathcal{S}_n acts faithfully on the latter field. The transcendence degree of $k(x_1/x_{n-1}, \dots, x_{n-2}/x_{n-1})$ being equal to $n - 2$, one concludes that $\text{ed}(\mathcal{S}_n) \leq n - 2$ for $n \geq 3$.

In particular we find $\text{ed}(\mathcal{S}_3) = 1$ and $\text{ed}(\mathcal{S}_4) = 2$.

If now we suppose $n \geq 5$, we show that $\text{ed}(\mathcal{S}_n) \leq n - 3$.

The group $\mathbf{PGL}_2(k)$ acts on $k(x_1, \dots, x_n)$ in the following way :

$$\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} \right] \cdot x_i = \frac{ax_i + b}{cx_i + d} \quad \forall i = 1, \dots, n.$$

If now i, j, k, ℓ are distinct, the cross-sections $[x_i, x_j, x_k, x_\ell] = \frac{(x_i - x_k)(x_j - x_\ell)}{(x_j - x_k)(x_i - x_\ell)}$ are \mathbf{PGL}_2 -invariant. Hence we have

$$k([x_i, x_j, x_k, x_\ell]) \subset k(x_1, \dots, x_n)^{\mathbf{PGL}_2(k)}$$

where $k([x_i, x_j, x_k, x_\ell])$ is a short notation for the field generated by the biratios $[x_i, x_j, x_k, x_\ell]$ for i, j, k, l all distinct. But $k([x_i, x_j, x_k, x_\ell])$ is generated by the biratios $[x_1, x_2, x_3, x_i]$ with $i = 4, \dots, n$.

Hence $k([x_i, x_j, x_k, x_\ell]) \cong k(y_1, \dots, y_{n-3})$. But, if $n \geq 5$, every permutation $\sigma \in \mathcal{S}_n \setminus \{1\}$ moves at least one of the $[x_i, x_j, x_k, x_\ell]$'s. Consequently, since the above action commutes with the \mathcal{S}_n -action, \mathcal{S}_n acts faithfully on $k(y_1, \dots, y_{n-3})$.

This shows that $\text{ed}(\mathcal{S}_n) \leq n - 3$ for all $n \geq 5$.

In particular we have $\text{ed}(\mathcal{S}_5) = 2$ and $\text{ed}(\mathcal{S}_6) = 3$.

The question is still open concerning \mathcal{S}_7 . Do we have $\text{ed}(\mathcal{S}_7) = 3$ or 4 ?

The point of view of faithful actions allows us to prove the following

LEMMA 1.2 (Useful Lemma). *Let G be a finite constant group. Suppose that $\text{ed}_k(G) = 1$, then G is isomorphic to a subgroup of $\mathbf{PGL}_2(k)$.*

Proof. Let G act faithfully on a vector space V and let $k(V)/k(V)^G$ be the corresponding Galois extension. Saying that $\text{ed}_k(G) = 1$ means that there is a subextension K/k where $\text{trdeg}(K : k) = 1$ with G acting faithfully on K . Since K is a subextension of $k(V)$, which is rational, and since $\text{trdeg}(K : k) = 1$, by Lüroth's theorem K is also rational. Thus $K \cong k(t)$. Since G acts faithfully on $k(t)$ this means that G is a subgroup of $\text{Aut}(k(t)) \cong \mathbf{PGL}_2(k)$.

We continue this section studying more carefully the constant groups \mathbb{Z}/n and D_n .

1. Some finite groups

We recall first of all that, if the field k contains the n -th roots of unity, one has $\text{ed}_k(\mathbb{Z}/n) = 1$ (see Corollary 1.15 in Chapter III) and that the inequality $\text{ed}_k(\mathbb{Z}/n) \geq 1$ holds for any field. Upper bounds are usually given by actions or representations and these will essentially depend on the ground field. Furthermore lower bounds are generally difficult to find. We begin with some easy considerations in order to understand the problem.

Consider \mathbb{Z}/n as a constant \mathbb{R} -group scheme. Then one has a faithful representation

$$\mathbb{Z}/n \longrightarrow \mathbf{SL}_2(\mathbb{R})$$

given by sending the generator of \mathbb{Z}/n to the matrix

$$\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$$

representing the rotation of angle $\theta = 2\pi/n$. Hence $\text{ed}_{\mathbb{R}}(\mathbb{Z}/n) \leq 2$ for every n . Clearly this holds for an arbitrary field k containing \mathbb{R} . The question becomes particularly interesting when the field is \mathbb{Q} . For an account of essential dimension of cyclic and dihedral groups over \mathbb{Q} see the work of A. Ledet in [14] where $\text{ed}_{\mathbb{Q}}(\mathbb{Z}/7)$ is given.

In fact, linear representations do not always give the best possible upper bounds. Recall that if G is a finite subgroup of $\mathbf{GL}_n(k)$ for some n and if its image in $\mathbf{PGL}_n(k)$ is still isomorphic to G then $\text{ed}_k(G) \leq n - 1$ (see Chapter III, Corollary 3.18).

As we shall see, in the study of cyclic groups there appears a gap between groups of odd and even order.

LEMMA 1.3 (Simple Lemma). *Let n be an integer, k a field such that $\text{char}(k) \nmid n$ and $\zeta \in \bar{k}$ a primitive n -th root of unity. Suppose that $\zeta + \zeta^{-1} \in k$. Let $S = \begin{pmatrix} \zeta + \zeta^{-1} & 1 \\ -1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Then the order of S in $\mathbf{GL}_2(k)$ equals n and the subgroup generated by S and T is isomorphic to the dihedral group D_n . Moreover, if n is odd, the same holds in $\mathbf{PGL}_2(k)$ for the classes of S and T .*

Proof. Let $P = \begin{pmatrix} 1 & \zeta^{-1} \\ 1 & \zeta \end{pmatrix}$. Then $S = P^{-1} \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix} P$ showing that S has order n . Moreover easily $TST^{-1} = S^{-1}$.

Now assume that n is odd. We only have to check that $S^i \neq \lambda I$ for all $\lambda \in k$ and all $i = 1, \dots, n - 1$. Suppose that $S^i = \lambda I$ for some $\lambda \in k$ and

some $i = 1, \dots, n - 1$. This would mean that $\zeta^i = \lambda$ and $\zeta^{-i} = \lambda$. Thus $\zeta^{2i} = 1$. This means that $n \mid 2i$ which is impossible.

This lemma gives us already the exact value of $\text{ed}_k(\mathbb{Z}/n)$, with n odd, when the field contains $\zeta + \zeta^{-1}$.

PROPOSITION 1.4. *Let n be an odd integer, k a field such that $\text{char}(k) \nmid n$ and ζ a primitive n -th root of unity. If $\zeta + \zeta^{-1} \in k$ then*

$$\text{ed}_k(\mathbb{Z}/n) = 1.$$

Proof. We only have to prove that $\text{ed}_k(\mathbb{Z}/n) \leq 1$. But the lemma above shows that \mathbb{Z}/n injects into $\mathbf{GL}_2(k)$ and that this map stays injective when passing to $\mathbf{PGL}_2(k)$. Thus $\text{ed}_k(G) \leq 2 - 1 = 1$ by Corollary 3.18 of Chapter III.

This gives the essential dimension of $\mathbb{Z}/3$:

COROLLARY 1.5. *For any field k one has $\text{ed}_k(\mathbb{Z}/3) = 1$.*

Proof. Clearly every field contains $\zeta + \zeta^{-1} = -1$ and hence, in characteristic $\neq 3$, one can apply the above argument. In characteristic 3 we already know the result (see Examples 1.3 in Chapter II).

The tough problem is to deal with groups of the form $\mathbb{Z}/2n$ where n is even. The following theorem gives an answer for $n = 2$. We postpone its proof until the end of the present section.

THEOREM 1.6. *Let k be a field of characteristic $\neq 2$. Then*

$$\text{ed}_k(\mathbb{Z}/4) = \begin{cases} 1 & \text{if } -1 \text{ is a square in } k \\ 2 & \text{otherwise.} \end{cases}$$

The result was already known by Serre in [25] (see Exercice 1.2) even though the notion of essential dimension was not defined. More recently in [22] Rost computed the essential dimension of a twisted form of $\mathbb{Z}/4$ generalizing the present result.

The above Simple Lemma has a converse statement when n is prime.

1. Some finite groups

LEMMA 1.7. *Let $p > 2$ a prime, k a field of characteristic $\neq p$ and $\zeta \in \bar{k}$ a primitive p -th root of unity. If $\mathbf{PGL}_2(k)$ has an element of order p then $\zeta + \zeta^{-1} \in k$.*

Proof. Let $M \in \mathbf{GL}_2(k)$ of order p in $\mathbf{PGL}_2(k)$. There is a $\lambda \in k^\times$ such that $M^p = \lambda I$, thus the minimal polynomial m_M divides $X^p - \lambda$. But $X^p - \lambda$ is not irreducible (otherwise $p = \deg(m_M) \leq 2$) and therefore $\lambda = \mu^p$ for some $\mu \in k^\times$. Thus we can suppose that $\lambda = 1$. In that case, the eigenvalues of M are of the form ζ^i . Let ζ^i and ζ^j be the two eigenvalues of M . We have $\det(M) = \zeta^{i+j} \in k^\times$. Suppose that $i + j \not\equiv 0 \pmod p$, then $\langle \zeta^{i+j} \rangle = \mu_p \subset k^\times$ and hence $\zeta + \zeta^{-1} \in k^\times$. Suppose that $i + j \equiv 0 \pmod p$, then $j \equiv -i$. If $i \equiv 0$ then $M = I$ which is impossible, hence $i \not\equiv 0$ and the eigenvalues are distinct. Thus

$$M = P^{-1} \begin{pmatrix} \zeta^i & 0 \\ 0 & \zeta^{-i} \end{pmatrix} P \in \mathbf{GL}_2(k)$$

for some invertible matrix P . But since $i \not\equiv 0$, there exists j such that $ij \equiv 1 \pmod p$. Then $M^j = P^{-1} \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix} P$ belongs to $\mathbf{GL}_2(k)$ and hence $\zeta + \zeta^{-1} = \text{Tr}(M^j) \in k$.

COROLLARY 1.8. *Let p be a prime, k a field such that $\text{char}(k) \neq p$ and $\zeta + \zeta^{-1} \notin k$. Then*

$$\text{ed}_k(\mathbb{Z}/p) \geq 2.$$

Proof. Suppose that $\text{ed}(\mathbb{Z}/p) = 1$, then by the Useful Lemma we would have an injection $\mathbb{Z}/p \rightarrow \mathbf{PGL}_2(k)$ which is impossible by the above lemma.

We now have the exact value of the essential dimension of $\mathbb{Z}/5$.

COROLLARY 1.9. *Let k a field such that $\text{char}(k) \neq 5$ and ζ a primitive 5-th root of unity. Then*

$$\text{ed}_k(\mathbb{Z}/5) = \begin{cases} 1 & \text{if } \zeta + \zeta^{-1} \in k \\ 2 & \text{otherwise.} \end{cases}$$

Proof. If $\zeta + \zeta^{-1} \in k$ the conclusion follows from Proposition 1.4. If $\zeta + \zeta^{-1} \notin k$ then by the above corollary we have $\text{ed}_k(\mathbb{Z}/5) \geq 2$. It then suffices to show that $\text{ed}_k(\mathcal{S}_5) \leq 2$ since $\mathbb{Z}/5$ is a subgroup of \mathcal{S}_5 and thus $\text{ed}_k(\mathbb{Z}/5) \leq \text{ed}_k(\mathcal{S}_5) = 2$.

If $\text{char}(k) \neq 2$ this has been proven at the beginning of this section.

Assume now that $\text{char}(k) = 2$. It suffices to show that the generic torsor for \mathcal{S}_5 is defined over a field of transcendence degree at most 2. By [2] Proposition 4.4, the degree 5 generic polynomial defining the generic torsor can be reduced to the form $X^5 + aX^2 + bX + c$. If $b = 0$ we are done. If $b \neq 0$ replacing X by $\frac{c}{b}X$ gives the conclusion.

Another application of the Useful Lemma concerns \mathbb{Z}/p^2 in characteristic p . Recall that we already know that $\text{ed}_k(\mathbb{Z}/p^2) \leq 2$ in that case as it was shown in Chapter II, Section 1.

PROPOSITION 1.10. *If $\text{char}(k) = p$ then $\text{ed}_k(\mathbb{Z}/p^2) = 2$.*

Proof. By the Useful Lemma we know that if $\text{ed}_k(G) = 1$ then G is isomorphic to a subgroup of $\mathbf{PGL}_2(k)$. Thus it suffices to show that, if $\text{char}(k) = p$, there are no elements of order p^2 in $\mathbf{PGL}_2(k)$. This is an easy computation.

One can handle in a similar way the computation of some essential dimensions for the dihedral groups D_n .

COROLLARY 1.11. *Let n be odd, k a field such that $\text{char}(k) \nmid n$ and ζ a primitive n -th root of unity. If $\zeta + \zeta^{-1} \in k$ then $\text{ed}_k(D_n) = 1$.*

Proof. It readily follows from Simple Lemma above and Corollary 3.18 of Chapter III.

COROLLARY 1.12. *Let n be an integer. Then*

$$\text{ed}_{\mathbb{R}}(D_n) = \begin{cases} 1 & \text{if } n \text{ is odd,} \\ 2 & \text{if } n \text{ is even.} \end{cases}$$

Proof. By the Simple Lemma, there is a real 2-dimensional faithful representation of D_n for every n . Hence $\text{ed}_{\mathbb{R}}(D_n) \leq 2$. Moreover, when n is even D_n contains $\mathbb{Z}/4$ or $\mathbb{Z}/2 \times \mathbb{Z}/2$ as a subgroup, according that n is congruent to 0 or 2 modulo 4. Thus the statement is a consequence of Proposition 2.7 of Chapter II and of Theorem 1.6 above together with Theorem 3.19 of Chapter III.

One very interesting result for finite groups can be found in [14] and concerns the essential dimension of $G \times \mathbb{Z}/2$. We give here this result without proof.

1. Some finite groups

THEOREM 1.13. *Let k be a field of characteristic 0 containing the primitive p -th roots of unity, for a prime p , and let G be a finite group. Assume that k does not contain the primitive r -th root of unity for any prime $r \neq p$ dividing $|Z(G)|$. Then*

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

This result gives for example $\text{ed}_{\mathbb{Q}}(G \times \mathbb{Z}/2) = \text{ed}_{\mathbb{Q}}(G) + 1$ for any finite group G . The same holds for \mathbb{R} .

COROLLARY 1.14. *Let n be an odd integer. Then*

$$\text{ed}_{\mathbb{Q}}(\mathbb{Z}/2n) = \text{ed}_{\mathbb{Q}}(\mathbb{Z}/n) + 1.$$

The same holds for \mathbb{R} .

Using this result and Theorem 1.6 the computation over the real numbers for cyclic groups is complete:

COROLLARY 1.15. *Let $n \neq 2$ be an integer. Then*

$$\text{ed}_{\mathbb{R}}(\mathbb{Z}/n) = \begin{cases} 1 & \text{if } n \text{ is odd} \\ 2 & \text{if } n \text{ is even} \end{cases}$$

Proof. We already know that $\text{ed}_{\mathbb{R}}(\mathbb{Z}/n) \leq 2$. If n is odd, Proposition 1.4 tells that $\text{ed}_{\mathbb{R}}(\mathbb{Z}/n) = 1$. If n is even, two cases arise: either $n = 2m$ with m odd and one applies the above corollary, or $n = 4m$ and in this case \mathbb{Z}/n contains $\mathbb{Z}/4$ as a subgroup. Then Theorem 1.6 shows that $\text{ed}_{\mathbb{R}}(\mathbb{Z}/n) \geq 2$.

As promised, we finish the section with a proof of Theorem 1.6 which gives the essential dimension of $\mathbb{Z}/4$.

Notice first that we only have to prove the result in the case where $\text{char}(k) \neq 2$ and $-1 \notin k^{\times 2}$, since we have already dealt with the other ones.

Our proof is based on the following parametrization of cyclic extensions of degree 4 (see [12]).

PROPOSITION 1.16. *Let K be a field with $\text{char}(k) \neq 2$. Let $D \in K^\times \setminus K^{\times 2}$. Then $K(\sqrt{D})/K$ is contained in a cyclic field extension of degree 4 if and only if D is a sum of two squares in K . Let $D = a^2 + b^2, a, b \in K$. Then $K(\sqrt{q(D + a\sqrt{D})})$, $q \in K^\times$ is a parametrization of all cyclic extensions of degree 4 with discriminant D . The trace form of $K(\sqrt{q(D + a\sqrt{D})})$ over K is $\langle 1, D, q, q \rangle$.*

This result tells us that the trace form essentially “depends on two parameters”. One is tempted to consider the invariants (which we will still denote by ω_i for $i = 1, 2, 3$)

$$H^1(-, \mathbb{Z}/4) \xrightarrow{\text{Tr}} H^1(-, O_4) \longrightarrow \text{WG}(-) \xrightarrow{\omega_i} H^i(-, \mu_2)$$

where the first arrow maps a $\mathbb{Z}/4$ -Galois algebra L over K to its trace-form (viewed as a quadratic form of rank 4 over K) and the last arrow is the i^{th} Delzant’s Stiefel-Whitney class. In the case where L_0 is the algebra $K(\sqrt{q(D + a\sqrt{D})})$ as above one has

$$\omega_1(L_0) = (D), \omega_2(L_0) = (q, q) \text{ and } \omega_3(L_0) = (D, q, q).$$

Unfortunately (or fortunately) the second invariant is trivial (indeed $\omega_2(L_0) = (q, q) = (q, -1)$ which is zero over an algebraically closed field) and the third invariant is zero (in fact $(D, q, q) = (D, -1, q)$ and $(D, -1) = 0$ since D is a sum of two squares). Thus the only non trivial invariant is ω_1 which does not give the expected result since it depends on only one parameter.

Let $K = k(s, t)$ the function field in two variables and set $D = s^2 + 1, q = t$ (here $a = s, b = 1$ in the notation of the proposition). Now the algebra L_0 can be viewed as an element of $H^1(k(s, t), \mathbb{Z}/4)$. To prove $\text{ed}(L_0) = 2$ it is sufficient to show that the form $q = \langle 1, s^2 + 1, t, t \rangle$ is not defined over a subfield $K \subset k(s, t)$ of transcendence degree 1. We will show that this is the case when k is a field in which -1 is not a square using an idea of Rost.

We begin by making some easy observations on the first residue map of quadratic forms. For convenience we recall its definition following [26].

Let (F, v) be a field of characteristic different from 2 equipped with a discrete valuation, and let π denotes a prime element (i.e. an element

1. *Some finite groups*

such that $v(\pi) = 1$). We denote by \mathcal{O}_v the valuation ring of v and by $\kappa(v)$ the residue field.

Any quadratic form q defined over F can be diagonalized as

$$q \simeq \langle a_1, \dots, a_m, \pi a_{m+1}, \dots, \pi a_n \rangle,$$

for some $a_i \in \mathcal{O}_v^\times$. The map $\partial_v : W(F) \rightarrow W(\kappa(v))$ defined by $\partial_v(q) := \langle \bar{a}_1, \dots, \bar{a}_m \rangle$ is a well-defined group homomorphism which is independent of the choice of π , called the **first residue map**.

Now let $K \subset F$ be any subfield, and let $\omega = v|_K$. If ω is trivial over K , then $K \subset \kappa(v)$ and it follows from the definition that for any $q \in W(K)$ we have $\partial_v(q_F) = q_{\kappa(v)}$.

If ω is non-trivial over K , then any prime element π' of (K, ω) can be written as $\pi' = u\pi^e$ for some $u \in \mathcal{O}_v^\times$ and some non-negative integer e . The integer e is well-defined and called **the ramification index of (K, ω) in (F, v)** . If $e = 1$, we say that the extension $(F, v)/(K, \omega)$ is **unramified**. Moreover in this case, we have an inclusion $\kappa(\omega) \subset \kappa(v)$.

If e is odd, then for any $q \in W(K)$, one easily checks that in $W(\kappa(v))$ the equality $\partial_v(q_F) = \partial_v(q)_{\kappa(v)}$ holds.

Let now k a field in which -1 is not a square. We consider v the t -adic valuation on the field $F = k(s, t)$ and v' the $(s^2 + 1)$ -adic valuation on $\kappa(v) \cong k(s)$ (note that since -1 is not a square we can consider this valuation).

Suppose now that q is defined over a subfield $K \subset k(s, t)$ such that $\text{trdeg}(K : k) = 1$, and write $q = q'_F$ for some quadratic form q' defined over K . Notice that, since $\text{trdeg}(K : k) = 1$, then $\text{trdeg}(F : K) = 1$, and it follows that F/K is a purely transcendental extension.

If the valuation $\omega = v|_K$ is trivial we have

$$\partial_v(q) = \partial_v(q'_F) = q'_{\kappa(v)}.$$

Since $\kappa(v) = k(s) \subset F$, by scalar extension we obtain the following equality in $W(F)$

$$\partial_v(q)_F = q.$$

It follows that $\langle 1, 1+s^2 \rangle = \langle 1, 1+s^2, t, t \rangle$, showing that $\langle t, t \rangle$ is hyperbolic over F . Then, comparing discriminants, one finds that -1 is a square in $F = k(s, t)$, hence in k , which is a contradiction. Thus the valuation ω is non-trivial over K .

Notice now that $\kappa(\omega)$ is a finite extension of k , since any discrete k -valuation over a field extension of transcendence degree 1 over k is associated to some irreducible polynomial with coefficients in k . Since $\kappa(\omega) \subset k(s)$, this implies that $\kappa(\omega) = k$. It follows, by [8], Prop. 2, p. 327, that ω and v has same value group, that is $(F, v)/(K, \omega)$ is unramified. In particular, we have $\partial_v(q) = \partial_v(q'_F) = \partial_\omega(q')_{\kappa(v)}$. Since $\partial_\omega(q') \in W(\kappa(\omega)) = W(k)$, we then get $\partial_{v'}(\partial_v(q)) = \partial_\omega(q')$, so we finally obtain the equality

$$\partial_{v'}(\partial_v(q))_{\kappa(v)} = \partial_v(q),$$

that is $\langle 1 \rangle = \langle 1, 1 + s^2 \rangle$ in $W(k(s))$, which is a contradiction.

This shows that $\text{ed}(\langle 1, s^2 + 1, t, t \rangle) = 2$ when -1 is not a square and consequently that $\text{ed}_k(\mathbb{Z}/4) \geq 2$ in that case.

Now, to have a complete computation of the essential dimension of $\mathbb{Z}/4$ we only need to give the upper bound. This will be given by a faithful action as follows:

Let k be a field of characteristic $\neq 2$ and let $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Since A is of order 4, there is a faithful representation on \mathbb{A}_k^2 given by $1 \mapsto A$, where 1 is the generator of $\mathbb{Z}/4$. This shows that $\text{ed}_k(\mathbb{Z}/4) \leq 2$.

This completes the proof of Theorem 1.6.

REMARK 1.17. Most of the results of the present section were known to Buhler and Reichstein over an algebraically closed field of characteristic 0. Emphasis is given here to the computation of essential dimension over arbitrary fields.

2. Homotopy invariance

2. HOMOTOPY INVARIANCE

In this section we shall prove the so-called *homotopy invariance* (that is $\text{ed}_k(G) = \text{ed}_{k(t)}(G)$) for algebraic groups defined over infinite fields. We first begin with some considerations on places of the form $k(t) \rightsquigarrow k$. Unadorned tensor product will always mean \otimes_k .

Let k be any field, $a(t) \in k(t)$ and $\tau \in k$. We say that $a(t)$ is **unramified** at τ if $a(t) \in k[t]_{\mathfrak{m}_\tau}$ where \mathfrak{m}_τ denotes the maximal ideal $\langle t - \tau \rangle$ of $k[t]$. When $a(t)$ is unramified at τ one can evaluate or specialize it at τ by simply replacing t by τ . Actually every $\tau \in k$ defines a pseudo k -place $k(t) \rightsquigarrow k$ denoted by $(\mathcal{O}_\tau, \alpha_\tau)$ where the local ring \mathcal{O}_τ is $k[t]_{\mathfrak{m}_\tau}$ and the morphism α_τ is the isomorphism $k[t]/\mathfrak{m}_\tau \simeq k$. Saying that $a(t)$ is unramified at τ is then the same as saying that $a(t)$ (viewed as an element of $\mathbf{F}(k(t))$ where \mathbf{F} is the forgetful functor) is unramified in the place $(\mathcal{O}_\tau, \alpha_\tau)$ and $a(\tau)$ the specialization of $a(t)$ at τ is nothing but the image of $a(t)$ under the map $s_\tau : k[t]_{\mathfrak{m}_\tau} \rightarrow k[t]_{\mathfrak{m}_\tau}/\mathfrak{m}_\tau \simeq k[t]/\mathfrak{m}_\tau \simeq k$. These considerations extend naturally to vector spaces as follows:

DEFINITION 2.1. *Let A be a k -vector space (not necessarily finite dimensional). Let t be an indeterminate over k , and let $\tau \in k$. We say that an element $a(t) \in A \otimes k(t)$ is **unramified** at τ if $a \in A \otimes k[t]_{\mathfrak{m}_\tau}$. Let $s_\tau : k[t]_{\mathfrak{m}_\tau} \rightarrow k$ be the above morphism. The **specialization** of $a(t)$ at τ , denoted by $a(\tau)$, is the image of $a(t)$ under the induced map $\text{Id}_A \otimes s_\tau : A \otimes k[t]_{\mathfrak{m}_\tau} \rightarrow A \otimes k \simeq A$. This is an element of A .*

Let $B \subset A$ be a k -subspace. Recall that the maps $B \otimes k(t) \rightarrow A \otimes k(t)$, $B \otimes k[t]_{\mathfrak{m}_\tau} \rightarrow A \otimes k[t]_{\mathfrak{m}_\tau}$ etc are injective.

We now prove the following result:

PROPOSITION 2.2. *Let $b(t) \in B \otimes k(t)$. Assume that $b(t)$, viewed as an element of $A \otimes k(t)$ is unramified at τ . Then $b(t)$, viewed as an element of $B \otimes k(t)$, is unramified at τ , and the two corresponding specializations coincide. In particular $b(\tau)$ is in B .*

Proof. It suffices to prove that $b(t) \in B \otimes k[t]_{\mathfrak{m}_\tau}$. By assumption, one can write $b(t) = \sum_{i=1}^n b_i \otimes f_i$ where $b_i \in B, f_i \in k(t)$ and also

$b(t) = \sum_{j=1}^m a_j \otimes g_j$ for some $a_i \in A$ and $g_i \in k[t]_{\mathfrak{m}_r}$. Changing suitably the f_i 's, one can assume that the b_i 's are linearly independent over k . Then there exists some a_i 's, say a_1, \dots, a_r , such that $\{b_1, \dots, b_n, a_1, \dots, a_r\}$ form a k -basis of the vector space generated by the b_i 's and the a_j 's. Hence, we get $b(t) = \sum_{i=1}^n b_i \otimes f_i = \sum_{i=1}^n b_i \otimes g'_i + \sum_{j=1}^r a_j \otimes g''_j$ for some $g'_i, g''_j \in k[t]_{\mathfrak{m}_r}$. Since $b_1, \dots, b_n, a_1, \dots, a_r$ are linearly independent, we get that $g''_j = 0$ for all j and $f_i = g'_i$. The desired conclusion follows immediately.

We continue with some considerations on torsors. Let $X \rightarrow Y$ be a G -torsor over k and let E/k be any field extension. Pulling back everything along $\text{Spec}(E) \rightarrow \text{Spec}(k)$ one obtains $X_E \rightarrow Y_E$ a G -torsor over E :

$$\begin{array}{ccc} X_E & \longrightarrow & X \\ \downarrow & & \downarrow \\ Y_E & \longrightarrow & Y \\ \downarrow & & \downarrow \\ \text{Spec}(E) & \longrightarrow & \text{Spec}(k) \end{array}$$

Now, for any field extension L/E and any G -torsor $T \rightarrow \text{Spec}(L)$ there is a one-to-one correspondence between the set of L -rational points of Y having T as a fiber and the set of L -rational points of Y_E having T as a fiber. Indeed if $y : \text{Spec}(L) \rightarrow Y$ is such a point, we have a diagram

$$\begin{array}{ccccc} & & T & & \\ & & \downarrow & \searrow & \\ \text{Spec}(L) & & & & X \\ & \searrow & & \searrow & \downarrow \\ & & X_E & \longrightarrow & X \\ & & \downarrow y & & \\ & & Y_E & \longrightarrow & Y \\ & & \downarrow & & \downarrow \\ & & \text{Spec}(E) & \longrightarrow & \text{Spec}(k) \end{array}$$

by the universal property of the pull-backs involved.

2. Homotopy invariance

From now on we will deal with $E = k(t)$ and we shall write $X(t) \longrightarrow Y(t)$ instead of $X_{k(t)} \longrightarrow Y_{k(t)}$.

LEMMA 2.3. *Let $X \rightarrow Y$ be a classifying torsor over an infinite field k . Then the torsor $X(t) \rightarrow Y(t)$ is a classifying torsor over $k(t)$.*

Proof. First notice that one can suppose Y to be affine. Let now $L/k(t)$ be a field extension and $T \rightarrow \text{Spec}(L)$ be any G -torsor. Let $Z \subset Y$ be the dense subset of Y such that for every $y : \text{Spec}(L) \rightarrow Z$ the fiber of $X \rightarrow Y$ at y is T . Denote by $Z(t)$ the corresponding subset of $Y(t)$. We have to show that $Z(t)$ is dense. Write $Y = \text{Spec}(A)$ for some k -algebra A . We have that $Y(t) = \text{Spec}(A \otimes k(t))$ and the bijection between the sets Z and $Z(t)$ says that every point $\mathfrak{p}(t) \in Z(t)$ is of the form $\mathfrak{p} \otimes k(t)$ for exactly one $\mathfrak{p} \in Z$. Saying that $Z \subset Y$ is dense means that for every non-zero element f of A there exists $\mathfrak{p} \in Z$ such that $f \notin \mathfrak{p}$. Take $f(t) \in A \otimes k(t)$ a non-zero element and suppose that $Z(t)$ is not dense, that is $f(t) \in \mathfrak{p}(t)$ for all $\mathfrak{p}(t) \in Z(t)$. Since k is infinite one can find $\tau \in k$ such that $f(t)$ is unramified at τ and $f(\tau) \neq 0$. Now Proposition 2.2 tells that $f(\tau) \in \mathfrak{p}$ for all $\mathfrak{p} \in Z$ contradicting the fact that Z is dense in Y .

THEOREM 2.4 (Homotopy invariance).

Let G be an algebraic group over an infinite field k . Then

$$\text{ed}_k(G) = \text{ed}_{k(t)}(G).$$

Proof. We only have to prove $\text{ed}_k(G) \leq \text{ed}_{k(t)}(G)$. Let $X \longrightarrow Y$ a classifying G -torsor over k with Y minimal for the dimension (that is $\dim(Y) = \text{ed}_k(G)$). Pulling back everything along $\text{Spec}(k(t))$ one obtains $X(t) \longrightarrow Y(t)$ which is again a classifying torsor in view of the preceding lemma.

Suppose now that $\text{ed}_{k(t)}(G) < \text{ed}_k(G)$. This means that the torsor $X(t) \longrightarrow Y(t)$ can be further compressed over $k(t)$. That means that there exists a G -torsor $X' \longrightarrow Y'$ with $\dim Y' < \dim Y(t) = \dim Y$ fitting into a pull-back

$$\begin{array}{ccc} X(t) & \longrightarrow & X' \\ \downarrow & & \downarrow \\ Y(t) & \longrightarrow & Y' \end{array}$$

But now, one can find $\varphi \in k[t]$ such that the above pull-back is defined over $\text{Spec}(k[t, \frac{1}{\varphi}])$. Now take $\xi : \text{Spec}(k) \rightarrow \text{Spec}(k[t, \frac{1}{\varphi}])$ a k -rational

point. Such a point exists because k is infinite. Since $Y' \rightarrow \text{Spec}(k[t, \frac{1}{\varphi}])$ is flat, Y'_ξ , the fiber of Y' over ξ , satisfies $\dim Y'_\xi \leq \dim Y'$. Pulling back the above square along ξ one has

$$\begin{array}{ccc} X(t)_\xi & \longrightarrow & X'_\xi \\ \downarrow & & \downarrow \\ Y(t)_\xi & \longrightarrow & Y'_\xi \end{array}$$

But $X(t)_\xi \simeq X$, so the torsor $X \rightarrow Y$ can be compressed into a torsor $X'_\xi \rightarrow Y'_\xi$ with $\dim Y'_\xi \leq \dim Y' < \dim Y$ contradicting the minimality of Y .

For the moment we do not know if homotopy invariance holds for finite fields.

REMARK 2.5. To our knowledge the homotopy invariance was not known before.

CHAPTER V

CUBICS

The aim of this chapter is to use some of the techniques previously developed, for the computation of the essential dimension of homogenous cubic polynomials in three variables.

By k_s we will always mean a separable closure of k . If k has characteristic different from 3, we will denote by $\varepsilon \in k_s$ a primitive third root of unity. An algebraic closure of k will be denoted by \bar{k} .

1. SOME CONSIDERATIONS ON CUBICS

Warm up

Let k be a field and let $d \geq 2, n \geq 1$ be two integers. We consider $\mathbf{C}_{d,n}$ the functor of nonzero homogeneous polynomials of degree d in n variables up to a scalar. Elements of $\mathbf{C}_{d,n}$ are called **degree d hypersurfaces in n variables**. We will often use the same notation for a hypersurface and for one polynomial which defines it. We also will have to consider non-singular hypersurfaces in the sequel. Let's denote by $\mathbf{C}_{d,n}^+$ (resp. $\mathbf{C}_{d,n}^-$) the functor of non-singular (resp. singular) degree d hypersurfaces in n variables.

We want to discuss the following general question. Take C a degree d polynomial in n variables and write it as $C = \sum a_{i_1, \dots, i_n} X_1^{i_1} \cdots X_n^{i_n}$ (where $i_1 + \cdots + i_n = d$) for some coefficients a_{i_1, \dots, i_n} in a field extension of k . In general it has $\binom{d+n-1}{n-1}$ coefficients. But as soon as one makes a linear change of variables some of these coefficients may drop or become equal. Hence we would like to know how many parameters are needed to describe the hypersurface C as soon as we allow ourselves to change a little the equation defining it.

The group \mathbf{GL}_n acts on $\mathbf{C}_{d,n}$ as described above by linear change of variables. More precisely, if $C \in \mathbf{C}_{d,n}(K)$ and $\varphi \in \mathbf{GL}_n(K)$, define $\varphi(C)$

to be the hypersurface defined by $C \circ \varphi$. Since scalar matrices do nothing on hypersurfaces this action induces an action of \mathbf{PGL}_n on $\mathbf{C}_{d,n}$. We shall say that two hypersurfaces are **equivalent** if they are in the same orbit under this action.

We denote by $\mathbf{F}_{d,n}$ the functor of hypersurfaces up to this action, and by $[C]$ the class of $C \in \mathbf{C}_{d,n}(K)$. The action of \mathbf{GL}_n clearly restricts to $\mathbf{C}_{d,n}^+$ and $\mathbf{C}_{d,n}^-$. We then denote by $\mathbf{F}_{d,n}^+$ the functor $\mathbf{C}_{d,n}^+/\mathbf{GL}_n$, and by $\mathbf{F}_{d,n}^-$ the functor $\mathbf{C}_{d,n}^-/\mathbf{GL}_n$. These are exactly the functors we are interested in (at least for small values of d and n) since we would like to count the minimal number of parameters needed to describe a degree d hypersurface up to change of variables. In other words we would like to compute their essential dimension.

First of all remark that we have $\mathbf{F}_{d,n} = \mathbf{F}_{d,n}^+ \coprod \mathbf{F}_{d,n}^-$ and hence

$$\mathrm{ed}_k(\mathbf{F}_{d,n}) = \max\{\mathrm{ed}(\mathbf{F}_{d,n}^+), \mathrm{ed}_k(\mathbf{F}_{d,n}^-)\}$$

by Lemma 2.10 in Chapter I. We will thus treat singular hypersurfaces and non-singular ones separately.

We will also need the following definition:

DEFINITION 1.1. *Let $[C] \in \mathbf{F}_{d,n}(L)$. We say that $[C]$ is **isotropic** if the equation $C = 0$ has a non-trivial solution in L^n . Clearly, this does not depend on the choice of C in its class.*

Let us come back to our problem. For $d = 3$, elements of $\mathbf{C}_{d,n}$ are called **cubics**, and the functor $\mathbf{F}_{d,n}$ (resp. $\mathbf{F}_{d,n}^+$, $\mathbf{F}_{d,n}^-$) is simply denoted by \mathbf{Cub}_n (resp. by \mathbf{Cub}_n^+ , \mathbf{Cub}_n^-).

We begin with the two variables case which can be handled without any extra tool.

PROPOSITION 1.2. *Let k be a field. If $\mathrm{char}(k) \neq 3$, then $\mathrm{ed}_k(\mathbf{Cub}_2) = 1$*

Proof. We first show that $\mathrm{ed}_k(\mathbf{Cub}_2) \leq 1$. Let L/k be a field extension, and let C be a cubic polynomial in 2 variables with coefficients in L . Write $C = a_1X^3 + a_2X^2Y + a_3XY^2 + a_4Y^3$

We have to show that, up to a linear change of variables and to a scalar, C is defined over an extension of k of transcendence degree at most 1.

If $a_1 = a_4 = 0$, we have $C = a_2X^2Y + a_3XY^2$. Since $C \neq 0$, $a_2 \neq 0$ or $a_3 \neq 0$. One can assume that $a_2 \neq 0$, eventually after exchanging X

1. *Some considerations on cubics*

and Y . Then dividing by a_2 shows that $[C]$ is defined over $k(\frac{a_3}{a_2})$, which has transcendence degree at most 1 over k .

Assume now that $a_1 \neq 0$ or $a_4 \neq 0$. As previously, one can assume that $a_1 \neq 0$. Then one can divide by a_1 and obtain $X^3 + s_2X^2Y + s_3XY^2 + s_4Y^3$ where $s_i = \frac{a_i}{a_1}$.

Let $\varphi = \begin{pmatrix} 1 & -\frac{1}{3}s_2 \\ 0 & 1 \end{pmatrix}$. Then $C \circ \varphi = X^3 + uXY^2 + vY^3$ for some $u, v \in L$.

If $uv = 0$, we are done. If $uv \neq 0$, let $\varphi' = \begin{pmatrix} \frac{v}{u} & 0 \\ 0 & 1 \end{pmatrix}$. Then

$$\frac{u^3}{v^3}C \circ \varphi' = X^3 + \frac{u^3}{v^2}XY^2 + \frac{u^3}{v^2}Y^3,$$

so $[C]$ is defined over $k(\frac{u^3}{v^2})$, which has transcendence degree at most 1 over k .

It remains to show that $\text{ed}_k(\mathbf{Cub}_2) \geq 1$. One can assume that k is algebraically closed. Let $L = k(t)$, where t is an indeterminate over k and $C = X^3 - tY^3$. Assume that $\text{ed}([C]) = 0$. This means that $[C]$ is defined over k , since $k(t)/k$ is purely transcendental. Hence there exists $\lambda \in k(t)^\times, \varphi \in \mathbf{GL}(k(t))$ and a polynomial C' with coefficients in k , such that $C = \lambda C' \circ \varphi$. In this case, C' would be isotropic over k (since k is algebraically closed), hence over $k(t)$. Consequently, C is also isotropic over $k(t)$. But this is clearly not the case, since $t \notin k(t)^{\times 3}$. Hence $\text{ed}_k(\mathbf{Cub}_2) \geq \text{ed}([C]) = 1$. This concludes the proof of the statement.

Basic facts about cubics in three variables

From now on we will consider the case $n = 3$. Assume until the end of this section that $\text{char}(k) \neq 3$.

For any field extension L/k and any $\lambda \in L$, let

$$C_\lambda = X_1^3 + X_2^3 + X_3^3 - 3\lambda X_1X_2X_3.$$

We also define $C_\infty = X_1X_2X_3$. It is easy to see that C_λ for $\lambda \in L$ is non-singular if and only if λ is not a third root of unity.

We recall some well-known facts about cubics in 3 variables.

We first begin with the Hessian group G_{216} . It plays a crucial role in our work. We follow [6] p. 293–299.

The Hessian group G_{216} is isomorphic to the group of special affinities $\mathbf{SA}_2(\mathbb{F}_3)$, which is generated by the translations of the plane \mathbb{F}_3^2 and the

elements of $\mathbf{SL}_2(\mathbb{F}_3)$. One can view this group as a subgroup of $\mathbf{PGL}_3(k_s)$ as follows:

Let x_{00}, \dots, x_{22} the nine points of $\mathbb{P}_{k(\varepsilon)}^2$ defined by:

$$\begin{aligned} x_{00} &= (0, -1, 1), & x_{01} &= (0, -\varepsilon, 1), & x_{02} &= (0, -\varepsilon^2, 1) \\ x_{10} &= (1, 0, -1), & x_{11} &= (1, 0, -\varepsilon), & x_{12} &= (1, 0, -\varepsilon^2) \\ x_{20} &= (-1, 1, 0), & x_{21} &= (-\varepsilon, 1, 0), & x_{22} &= (-\varepsilon^2, 1, 0). \end{aligned}$$

If $g \in \mathbf{SA}_2(\mathbb{F}_3)$, then g induces a permutation σ_g of these nine points as follows:

If $g(\bar{a}, \bar{b}) = (\bar{c}, \bar{d})$ (where $a, b, c, d \in \{0, 1, 2\}$), then set $\sigma_g(x_{ab}) = x_{cd}$.

Computation then shows that there is a unique element \bar{M}_g of $\mathbf{PGL}_3(k_s)$ which induces the permutation σ_g on the points x_{ab} (the image of the point x_{ab} is computed by left multiplication by x_{ab} , since we use the row convention).

The two translations $T_{(20)}$ and $T_{(02)}$ then correspond respectively to \bar{A} and \bar{C} , where $A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ and $C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \varepsilon & 0 \\ 0 & 0 & \varepsilon^2 \end{pmatrix}$.

The three generators $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ correspond to \bar{D} , \bar{E} and \bar{E}' , where $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \varepsilon & 0 \\ 0 & 0 & \varepsilon \end{pmatrix}$, $E = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \varepsilon & \varepsilon^2 \\ 1 & \varepsilon^2 & \varepsilon \end{pmatrix}$ and $E' = \begin{pmatrix} \varepsilon^2 & 1 & 1 \\ \varepsilon & 1 & \varepsilon \\ \varepsilon & \varepsilon & 1 \end{pmatrix}$.

Notice that the set of generators for $\mathbf{SA}_2(\mathbb{F}_3)$ in [6] is not completely correct. Indeed, the 2-Sylow subgroup of G_{216} is the quaternion group, so it is generated by two elements of order 4, but the element $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$,

which corresponds to $B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ given in [6] p. 297, has order 2.

Notice that G_{216} is in fact a subgroup of $\mathbf{PGL}_3(k(\varepsilon))$.

For a non-singular cubic C with coefficients in a field K the **j -invariant** is well defined. We denote it by $j(C)$. It depends only on the equivalence class of the cubic and it is a non-constant invariant. For a non-singular cubic of the form C_λ one has $j(C_\lambda) = \frac{\lambda^3(\lambda^3+8)^3}{(\lambda^3-1)^3}$ (see [6] p. 301–302).

1. *Some considerations on cubics*

We now recall some results proved in [6], p. 292–298:

LEMMA 1.3. *Assume that $k = k_s$. Then:*

- (1) *Every non-singular cubic C is equivalent to some C_λ for some $\lambda \in k$. Moreover non-singular cubics are classified by their j -invariant, that is two non-singular cubics are equivalent if and only if they have same j -invariant.*
- (2) *Let $\lambda \in k \cup \{\infty\}$. For any $\bar{\varphi} \in \mathbf{PGL}_3(k)$, $\bar{\varphi}$ maps C_λ to some C_μ if and only if $\bar{\varphi} \in G_{216}$.*
- (3) *Let $\lambda \in k \cup \{\infty\}$. For any $\bar{\varphi} \in \mathbf{PGL}_3(k)$, $\bar{\varphi}$ maps the cubic C_λ to itself if and only if $\bar{\varphi}$ belongs to the subgroup $H = \langle \overline{A}, \overline{B}, \overline{C} \rangle$.*

The two first statements are proved in the case where k is the field of complex numbers, but it is easy to check that they are still true when k is a separably closed field of characteristic different from 3. The third one is only mentioned in [6] without proof, but can be obtained by easy computation. Notice that in the two last statements, C_λ is not assumed to be non-singular.

Canonical pencils of cubics

If C is a cubic polynomial in 3 variables with coefficients in L , let $H_C = \det \left(\frac{\partial^2 C}{\partial X_i \partial X_j} \right)$, the Hessian of C , and let \mathcal{F}_C be the set of cubics of the form $\alpha C + \beta H_C$, for some $\alpha, \beta \in L$ not both zero. The set \mathcal{F}_C is called **the canonical pencil associated to C** . Since $H_{\alpha C} = \alpha^3 H_C$ for any $\alpha \in L^\times$, this set does only depend on the cubic defined by C .

Let $\mathfrak{P}(L)$ denote the set $\{\mathcal{F}_C \mid C \in \mathbf{C}_{3,3}(L)\}$. For any k -morphism $L \rightarrow L'$ we define a map $\mathfrak{P}(L) \rightarrow \mathfrak{P}(L')$ by sending the pencil \mathcal{F}_C to the pencil $\mathcal{F}_{C_{L'}}$. We then obtain a functor $\mathfrak{P} : \mathfrak{C}_k \rightarrow \mathbf{Sets}$. The association $C \mapsto \mathcal{F}_C$ gives rise to a surjective map of functors $\mathbf{C}_{3,3} \twoheadrightarrow \mathfrak{P}$. Let now the group \mathbf{GL}_3 act naturally on \mathfrak{P} as follows: for $\varphi \in \mathbf{GL}_3(L)$ and $C \in \mathbf{C}_{3,3}(L)$ we set $\varphi(\mathcal{F}_C) = \mathcal{F}_{\varphi(C)}$. One checks that this does not depend on the choice of C (that is if C' is such that $\mathcal{F}_{C'} = \mathcal{F}_C$ then $\mathcal{F}_{\varphi(C')} = \mathcal{F}_{\varphi(C)}$) using the formula $H_{C \circ \varphi} = (\det \varphi)^2 H_C \circ \varphi$. The proof of this formula is left to the reader.

We say that \mathcal{F}_C and $\mathcal{F}_{C'}$ are **isomorphic over L** if they are in the same orbit under this action. We denote by $[\mathcal{F}_C]$ the isomorphism class of

\mathcal{F}_C and we denote by \mathbf{Pen}_3 the functor of isomorphism classes of such pencils.

COROLLARY 1.4. *Sending the class of a cubic in three variables C to the class of its pencil \mathcal{F}_C induces a well defined morphism of functors $\mathbf{Cub}_3 \rightarrow \mathbf{Pen}_3$.*

Lemma 1.3 tells us that, over a separably closed field, one can bring every non-singular cubic to some canonical form depending on one parameter. However, unlike quadratic forms, there are several cubics defined over L which are not isomorphic over L_s . Hence one cannot classify cubics using Galois cohomology like in the quadratic form case. However the next lemma shows that one can do something for pencils of cubics.

LEMMA 1.5. *Assume that $\text{char}(k) \neq 2, 3$ and let L/k be a field extension. For any $\lambda \in L, \lambda^3 \neq 1$, we have*

$$\mathcal{F}_{C_\lambda} = \{C_\mu \mid \mu \in L \cup \{\infty\}\}.$$

In particular, for all $[C], [C'] \in \mathbf{Cub}_3^+(L_s)$, the pencils \mathcal{F}_C and $\mathcal{F}_{C'}$ are isomorphic.

Proof. Computation shows that

$$H_{C_\lambda} = -54\lambda^2(X_1^3 + X_2^3 + X_3^3) - 3(18\lambda^3 - 72)X_1X_2X_3,$$

hence we get

$$\alpha C_\lambda + \beta H_{C_\lambda} = (\alpha - 54\lambda^2\beta)(X_1^3 + X_2^3 + X_3^3) - 3(\alpha\lambda + 18\lambda^3\beta - 72\beta)X_1X_2X_3.$$

Let $\mu \in L$. If $\mu = \lambda$, take $\alpha = 1$ and $\beta = 0$.

Assume now that $\mu \neq \lambda$. Take $\beta = 1$ and $\alpha = \frac{72 - 54\lambda^2\mu - 18\lambda^3}{\lambda - \mu}$.

We claim that $\alpha - 54\lambda^2 \neq 0$. Indeed, assume the contrary. Then we easily get that $72(1 - \lambda^3) = 0$. Since $\text{char}(k) \neq 2, 3$, this implies that $\lambda^3 = 1$, which is not the case.

Thus, with these choices of α and β , we get $\alpha C_\lambda + \beta H_{C_\lambda} = (\alpha - 54\lambda^2)C_\mu$, hence the polynomials $\alpha C_\lambda + \beta H_{C_\lambda}$ and C_μ belong to the same class.

If $\mu = \infty$, take $\alpha = -\frac{\lambda^2}{4(\lambda^3 - 1)}$ and $\beta = -\frac{1}{216(\lambda^3 - 1)}$.

2. Galois descent for functors. Applications to cubics

REMARK 1.6. If $\lambda^3 = 1$, the lemma is not true. Indeed, it is easy to see that in this case $\mathcal{F}_{C_\lambda} = \{C_\lambda\}$. Since we want to apply Galois descent to pencils of cubics, we have to restrict ourselves to pencils generated by non-singular cubics.

We will denote by \mathfrak{P}^+ and \mathbf{Pen}_3^+ the corresponding functors.

LEMMA 1.7. *Let L/k be a field extension and let $[C] \in \mathbf{Cub}_3^+(L)$. Then*

$$\mathrm{ed}([\mathcal{F}_C]) \leq \mathrm{ed}([C]) \leq \mathrm{ed}([\mathcal{F}_C]) + 1.$$

Proof. Let K/k be such that $[C]$ is defined over K and such that $\mathrm{trdeg}(K : k) = \mathrm{ed}_k([C])$. Then clearly \mathcal{F}_C is defined over K , hence $\mathrm{ed}([\mathcal{F}_C]) \leq \mathrm{ed}([C])$. Assume now that $\mathrm{ed}([\mathcal{F}_C]) = n$. Then there exists a field extension E/k of transcendence degree equal to n , with $E \subseteq K$, and a cubic $[C'] \in \mathbf{C}_{3,3}(E)$ such that $[\mathcal{F}_C] = [\mathcal{F}_{C'}]$. By definition, there exists $\varphi \in \mathbf{GL}_3(K)$ such that $\mathcal{F}_{\varphi(C)} = \mathcal{F}_{C'_k}$. In particular, there exists $\alpha, \beta \in K$ such that the polynomials $C \circ \varphi$ and $\alpha C' + \beta H_{C'}$ are proportional. Hence $[C] = [\alpha C' + \beta H_{C'}]$. Since α or β is non-zero, $[C]$ is then defined over $E(\frac{\alpha}{\beta})$ or $E(\frac{\beta}{\alpha})$. Thus $[C]$ is defined over a field of transcendence degree at most $n + 1$.

2. GALOIS DESCENT FOR FUNCTORS. APPLICATIONS TO CUBICS

We just dealt with pencils of cubics and saw how all pencils become isomorphic over a separably closed field. A natural idea is then to classify them using Galois cohomology. The problem is that the objects we want to classify are not standard “algebraic structures”. In this section, we prove a Galois Descent Lemma for reasonable functors which is a slight generalization of [15], Proposition (29.1). This lemma will apply to our situation.

Let k be any field, and let \mathbf{F} be an object of \mathfrak{F}_k . We denote by $\mathrm{Aut}(\mathbf{F})$ the functor defined by

$$\mathrm{Aut}(\mathbf{F})(L) = \{\eta : \mathbf{F}_L \longrightarrow \mathbf{F}_L \mid \eta \text{ is an isomorphism of functors}\}$$

for any L/k . Notice that for any extension L/k , the action of the absolute Galois group Γ_L on L_s induces an action on $\mathbf{F}(L_s)$ by functoriality.

Let G be a group scheme of finite type over k and $\rho : G \longrightarrow \mathrm{Aut}(\mathbf{F})$ be a morphism of group-valued functors which is Γ -equivariant. For each

E/k we define an equivalence relation on $\mathbf{F}(E)$ saying that $b, b' \in \mathbf{F}(E)$ are equivalent if there exists $g \in G(E)$ such that $\rho_E(g)(b) = b'$. We note this by $b \sim_E b'$.

Let k'/k be a field extension, and $a \in \mathbf{F}(k')$. For every extension L/k' set

$$X(L) = \{b \in \mathbf{F}(L) \mid b \sim_{L_s} a\}.$$

Denote by $\mathbf{Stab}_G(a)$ the subfunctor of G defined by

$$\mathbf{Stab}_G(a)(L) = \{g \in G(L) \mid \rho_L(g)(a_L) = a_L\}$$

for any extension L/k' . This is a group-valued subfunctor of $G_{k'}$.

Finally, we denote by $\mathbf{F}_a(L)$ the set of equivalence classes of elements of $X(L)$ under the relation $b \sim_L b'$. This defines an object of $\mathfrak{F}_{k'}$, denoted by \mathbf{F}_a .

We now state the Galois Descent Lemma:

LEMMA 2.1 (Galois Descent Lemma). *Let $\rho : G \longrightarrow \text{Aut}(\mathbf{F})$ as above. Assume that for any $L \in \mathfrak{C}_k$, the following conditions hold:*

(i) $H^1(L, G(L_s)) = 1$,

(ii) $\mathbf{F}(L_s)^{\Gamma_L} = \mathbf{F}(L)$.

Then for any k'/k and for any $a \in \mathbf{F}(k')$, there is a natural isomorphism of functors of $\mathfrak{F}_{k'}$

$$\mathbf{F}_a \xrightarrow{\sim} H^1(-, \mathbf{Stab}_G(a)).$$

Moreover, this isomorphism maps the class of a_L to the base point of $H^1(L, \mathbf{Stab}_G(a)(L_s))$.

Proof. We fix once for all an extension k'/k and an element $a \in \mathbf{F}(k')$. Let L/k' be an extension of k' . For the proof we will denote by Γ instead of Γ_L the Galois group of L . We set $A = \mathbf{Stab}_G(a)(L_s)$ and $B = G(L_s)$. It is well-known that there is a natural bijection between

$$\ker(H^1(L, A) \longrightarrow H^1(L, B))$$

and the orbit set of the group B^Γ in $(B/A)^\Gamma$ (see [15], Corollary 28.2). Since the group $G(L_s)$ acts transitively on $X(L_s)$, the Γ -set $X(L_s)$ can be identified with the set of left cosets of $G(L_s)$ modulo $\mathbf{Stab}_G(a)(L_s)$, hence $B/A \simeq X(L_s)$. By assumption on \mathbf{F} , the set $(B/A)^\Gamma$ is then equal to $X(L)$. Moreover, $B^\Gamma = G(L_s)^\Gamma = G(L)$. It follows that the orbit set of B^Γ in $(B/A)^\Gamma$ is precisely $\mathbf{F}_a(L)$. Since $H^1(L, G(L_s))$ is trivial, we then obtain a natural bijection of pointed sets between $H^1(L, \mathbf{Stab}_G(a)(L_s))$ and $\mathbf{F}_a(L)$. The functoriality is left to the reader.

2. Galois descent for functors. Applications to cubics

EXAMPLE 2.2. Assume that $\text{char}(k) \neq 2, 3$ and $\varepsilon \in k$. Take $\mathbf{F} = \mathfrak{P}^+$ and let the group $G = \mathbf{GL}_3$ act on \mathfrak{P}^+ . Take $\lambda \in k$ with $\lambda^3 \neq 1$ and set $a = \mathcal{F}_{C_\lambda}$. Then Lemma 1.5 tells us that $\mathbf{F}_a(L) = \mathbf{Pen}_3^+(L)$ for any extension L/k .

We now determine the L_s -points of the stabilizer of the pencil \mathcal{F}_{C_λ} for any field L containing k . Since $\varepsilon \in k$, the constant group scheme G_{216} is a closed subgroup of \mathbf{PGL}_3 . Let $\pi : \mathbf{GL}_3 \rightarrow \mathbf{PGL}_3$ be the natural projection and denote by \tilde{G}_{216} the group scheme $\pi^{-1}(G_{216})$.

We now proceed to show that $\mathbf{Stab}_G(a)(L_s) = \tilde{G}_{216}(L_s)$ as Γ_L -groups. Let $\varphi \in \mathbf{Stab}_G(a)(L_s)$ and denote by $\bar{\varphi}$ its image in $\mathbf{PGL}_3(L_s)$. Since over L_s the pencil \mathcal{F}_{C_λ} is equal to $\{C_\mu \mid \mu \in L_s \cup \{\infty\}\}$ it follows that any φ in $\mathbf{Stab}_G(a)(L_s)$ maps C_λ to some C_μ . So the same holds for $\bar{\varphi}$ and hence $\bar{\varphi}$ belongs to $G_{216} = G_{216}(L_s)$ by Lemma 1.3. Now let $S \subseteq \mathbf{GL}_3(k)$ be a set of representatives of the elements of $G_{216} \subseteq \mathbf{PGL}_3(k)$.

We then have

$$\tilde{G}_{216}(L_s) = \{\lambda g \mid \lambda \in L_s^\times, g \in S\}.$$

This easily implies that $\tilde{G}_{216}(L_s) \subseteq \mathbf{Stab}_G(a)(L_s)$.

Since the Γ_L -action on $\mathbf{Stab}_G(a)(L_s)$ and $\tilde{G}_{216}(L_s)$ is the same (the restriction of the natural action on $\mathbf{GL}_3(L_s)$), then $\mathbf{Stab}_G(a)(L_s)$ and $\tilde{G}_{216}(L_s)$ are the same Γ_L -groups. We then have

$$H^1(-, \mathbf{Stab}_G(a)) = H^1(-, \tilde{G}_{216}).$$

Since the hypotheses of the Galois Descent Lemma are clearly fulfilled, we get

$$\mathbf{Pen}_3^+ \simeq H^1(-, \tilde{G}_{216}).$$

In particular, $\text{ed}_k(\mathbf{Pen}_3^+) = \text{ed}_k(\tilde{G}_{216})$.

EXAMPLE 2.3. Under the same hypotheses on k , take $\mathbf{F} = \mathbf{C}_{3,3}^+$ and let $G = \mathbf{GL}_3$ act on it as usual. Let k'/k be a field extension and take $a = C_\lambda$ for some $\lambda \in k' \cup \{\infty\}$. Then $\mathbf{F}_a(L)$ is the set of cubics in L which are equivalent to C_λ over L_s for any field extension L/k' . Arguing as previously, one can see that the Γ_L -group $\mathbf{Stab}_G(a)(L_s)$ coincides with the L_s -points of the algebraic group k' -scheme \tilde{H} , where H is the subgroup of G_{216} described in Lemma 1.3. Hence, for any field extension k'/k , for any $\lambda \in k' \cup \{\infty\}$, and for any field extension L/k' , we have a one-to-one correspondence

$$\mathbf{F}_a(L) = \{[C] \in \mathbf{Cub}_3^+(L) \mid C \sim_{L_s} C_\lambda\} \simeq H^1(L, \tilde{H}).$$

The functor \mathbf{F}_a with $a = C_\lambda$ will be denoted by \mathbf{F}_λ . Hence we have $\text{ed}_{k'}(\mathbf{F}_\lambda) = \text{ed}_{k'}(\tilde{H})$. This means in particular that the essential dimension of \mathbf{F}_λ does not depend on λ . Again we have classified cubics which become isomorphic to a fixed cubic by a Galois cohomology set.

3. ESSENTIAL DIMENSION OF NON-SINGULAR CUBICS

We can finally state and prove our main result:

THEOREM 3.1. *Let k be a field. Assume that $\text{char}(k) \neq 2, 3$. If k contains a primitive third root of unity ε , then*

$$\text{ed}_k(\mathbf{Cub}_3^+) = 3.$$

In particular, $\text{ed}_k(\mathbf{Cub}_3^+) \geq 3$ for any field k of characteristic $\neq 2, 3$.

We will prove the first part of the statement, the second one will follow from the fact that $\text{ed}_{k(\varepsilon)}(\mathbf{F}) \leq \text{ed}_k(\mathbf{F})$.

By Example 2.2, we have $\text{ed}_k(\mathbf{Pen}_3^+) = \text{ed}_k(\tilde{G}_{216})$. Since $\varepsilon \in k$, the group Γ_k acts trivially on $G_{216, \acute{e}t}(k_s)$, hence $G_{216, \acute{e}t}$ is the constant algebraic group G_{216} . Applying Theorem 1.18 of Chapter III with $G = G_{216}$ and $n = 3$ then gives $\text{ed}_k(\tilde{G}_{216}) \leq 2$. (Notice that \tilde{G}_{216} contains the constant subgroup $(\mathbb{Z}/3\mathbb{Z})^3$ generated by $\varepsilon I_3, C$ and D , so using Theorem 3.19 in Chapter III, we get $\text{ed}_k(\tilde{G}_{216}) = \text{ed}_k(\mathbf{Pen}_3^+) = 2$.) Lemma 1.7 implies in particular that $\text{ed}_k(\mathbf{Cub}_3^+) \leq \text{ed}_k(\mathbf{Pen}_3^+) + 1$, hence $\text{ed}_k(\mathbf{Cub}_3^+) \leq 3$.

The hard part is to show the converse inequality. We will proceed in several steps.

Let k'/k be a field extension, $\lambda \in k'$ with $\lambda^3 \neq 1$ and consider \mathbf{F}_λ the object of $\mathfrak{F}_{k'}$ defined in Example 2.3.

Our task is to compute the essential dimension of \mathbf{F}_λ , that is the essential dimension of \tilde{H} . Precisely, we will show the following result:

PROPOSITION 3.2. *Let k' be a field with $\text{char}(k') \neq 2, 3$ containing μ_3 . Then*

$$\text{ed}_{k'}(\tilde{H}) = 2.$$

3. Essential dimension of non-singular cubics

Let S be the constant subgroup of \mathbf{PGL}_3 isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$ generated by \overline{A} and \overline{C} , and let $\tilde{S} = \pi^{-1}(S)$. Clearly, we have the following exact sequence of group schemes:

$$1 \longrightarrow \mathbb{G}_m \longrightarrow \tilde{S} \longrightarrow S \longrightarrow 1,$$

hence $\dim(\tilde{S}) = 1$. Similarly, we have $\dim(\tilde{H}) = 1$. Applying Proposition 1.18 of Chapter III we get $\text{ed}_{k'}(\tilde{H}) \leq 2$. We now prove the reverse inequality.

By Chapter III, Proposition 3.19 we have $\text{ed}_{k'}(\tilde{H}) \geq \text{ed}_{k'}(\tilde{S})$. Since $\mu_3 \subseteq k' \subseteq L$, we can identify the algebraic group S with $\mu_3 \times \mu_3$, where the identification is given on the L -points by mapping $\overline{A}^m \overline{C}^n \in S(L)$ to $(\varepsilon^m, \varepsilon^n) \in \mu_3(L) \times \mu_3(L)$. We then have an exact sequence

$$1 \longrightarrow \mathbb{G}_m \longrightarrow \tilde{S} \longrightarrow \mu_3 \times \mu_3 \longrightarrow 1,$$

where the second map is given by

$$\begin{aligned} \tilde{S}(L) &\longrightarrow \mu_3(L) \times \mu_3(L) \\ \lambda A^m C^n &\longmapsto (\varepsilon^n, \varepsilon^m). \end{aligned}$$

Moreover, for any field extension L/k' , the above exact sequence induces the following exact sequence in cohomology:

$$H^1(L, \tilde{S}) \longrightarrow H^1(L, \mu_3) \times H^1(L, \mu_3) \longrightarrow H^2(L, \mathbb{G}_m).$$

Recall that $H^1(L, \mu_3)$ is in one-to-one correspondence with $L^\times/L^{\times 3}$ as follows:

For $aL^{\times 3} \in L^\times/L^{\times 3}$, let $\alpha \in L_s$ such that $\alpha^3 = a$. Then the map $c_a : \Gamma_L \rightarrow \mu_3$ defined by $\sigma \mapsto \frac{\sigma(\alpha)}{\alpha}$ is a 1-cocycle, and its cohomology class does not depend on the choice of α and a . We will write $(a)_3$ the class of the corresponding cocycle.

LEMMA 3.3. *For any field L , the connecting map*

$$\partial : H^1(L, \mu_3) \times H^1(L, \mu_3) \rightarrow H^2(L, \mathbb{G}_m)$$

is given by $\partial((a)_3, (b)_3) = -(a)_3 \cup (b)_3$, where \cup is the cup-product associated to the pairing $\mu_3(L) \times \mu_3(L) \rightarrow \mu_3(L)$ mapping $(\varepsilon^m, \varepsilon^n)$ to ε^{mn} .

Proof. Let $(a)_3, (b)_3 \in H^1(L, \mu_3)$ with $a, b \in L^\times$. If $\sigma \in \Gamma_L$, write $c_a(\sigma) = \varepsilon^{m_\sigma}$ and $c_b(\sigma) = \varepsilon^{n_\sigma}$ for some $m_\sigma, n_\sigma \in \{0, 1, 2\}$. It is well-known (see [23]) that the element $\partial((a)_3, (b)_3)$ is the class of the 2-cocycle

$$\begin{aligned} \alpha : \Gamma_L \times \Gamma_L &\rightarrow \mu_3(L) \\ (\sigma, \tau) &\mapsto \beta_\sigma \sigma \beta_\tau \beta_{\sigma\tau}^{-1} \end{aligned}$$

where β_σ is any preimage of $(c_a(\sigma), c_b(\sigma))$.

If $(c_a(\sigma), c_b(\sigma)) = (\varepsilon^{m_\sigma}, \varepsilon^{n_\sigma})$, we choose $\beta_\sigma = A^{m_\sigma} C^{n_\sigma}$. Notice that we have $\sigma\beta_\tau = \beta_\tau$ for any $\sigma, \tau \in \Gamma_L$. We then have

$$\alpha_{\sigma,\tau} = A^{m_\sigma} C^{m_\sigma} A^{m_\tau} C^{n_\tau} C^{-n_{\sigma\tau}} A^{-m_{\sigma\tau}}.$$

Since $CA = \varepsilon AC$, we get

$$\alpha(\sigma, \tau) = \varepsilon^{n_\sigma m_\tau} A^{m_\sigma + m_\tau} C^{m_\sigma + n_\tau - n_{\sigma\tau}} A^{-m_{\sigma\tau}}.$$

The fact that c_a and c_b are cocycles and that Γ_L acts trivially on $\mu_3(L_s)$ implies that $m_\sigma + m_\tau - m_{\sigma\tau}$ and $n_\sigma + n_\tau - n_{\sigma\tau}$ are divisible by 3. Hence we get

$$\begin{aligned} \alpha : \Gamma_L \times \Gamma_L &\rightarrow \mu_3(L) \\ (\sigma, \tau) &\mapsto \varepsilon^{m_\sigma n_\tau} \end{aligned}$$

which is precisely a cocycle representing $(b)_3 \cup (a)_3$ since Γ_L acts trivially on $\mu_3(L_s)$. Since $(b)_3 \cup (a)_3 = -(a)_3 \cup (b)_3$ the desired conclusion follows.

We then have a surjection of functors $\partial : H^1(-, \tilde{S}) \rightarrow \mathbf{N}$, where \mathbf{N} is the object of $\mathfrak{F}_{k'}$ defined by

$$\mathbf{N}(L) = \{((a)_3, (b)_3) \in H^1(L, \mu_3) \times H^1(L, \mu_3) \mid (a)_3 \cup (b)_3 = 0\}$$

for any field extension L/k' . Hence, by Lemma 2.9 of Chapter I we get

$$\text{ed}_{k'}(\tilde{S}) \geq \text{ed}_{k'}(\mathbf{N}).$$

To conclude the proof of Proposition 3.2 it suffices to show the following:

LEMMA 3.4. *We have $\text{ed}_{k'}(\mathbf{N}) \geq 2$.*

Proof. It suffices to show the inequality when k' is algebraically closed.

Let $((a)_3, (b)_3) \in \mathbf{N}(L)$ for some L/k' . Consider the cubic in 4 variables

$$C_{a,b} = X^3 + aY^3 + bZ^3 + abT^3.$$

The equivalence class of the cubic $C_{a,b}$ does not depend on the choice of representatives of $(a)_3$ and $(b)_3$. Moreover, this assignment is functorial in L . Hence we have a morphism of functors $\mathbf{N} \rightarrow \mathbf{Cub}_4$. Notice that $((a)_3, (b)_3) \in \mathbf{N}(L)$ if and only if a is a norm of the extension $L(\beta)/L$, where $\beta^3 = b$. Now let s, t, u be independent indeterminates over k' , and set $b = t, a = 1 + ts^3 + t^2u^3 - 3stu$. Set $L = k'(s, t, u)$. We have that $a = N_{L(\beta)/L}(1 + s\beta + u\beta^2)$, hence $((a)_3, (b)_3) \in \mathbf{N}(L)$.

Now assume that $((a)_3, (b)_3)$ is defined over a field L'/k' of transcendence degree at most 1 over k' , then so is $[C_{a,b}]$. Then L' is a C_1 field (since k' is algebraically closed), hence $[C_{a,b}]$ is isotropic over L' , hence over L .

3. Essential dimension of non-singular cubics

To get a contradiction, it remains to show that the polynomial $C_{a,b}$ is anisotropic over L .

LEMMA 3.5. *The polynomial $C_{a,b}$, with $a = 1 + ts^3 + t^2u^3 - 3stu$ and $b = t$ is anisotropic over $k'(s, t, u)$.*

Proof. Assume the contrary. Then there exists $P_1, \dots, P_4 \in k'[s, t, u]$ not all zero, such that $P_1^3 + aP_2^3 + bP_3^3 + abP_4^3 = 0$. Consider P_1, \dots, P_4 and a as elements of $k'(s, u)[t]$, and write $P_i = a^{n_i}Q_i$ where Q_i is not divisible by a as soon as $Q_i \neq 0$. If $n_1 \leq n_2, n_3, n_4$, then one gets

$$Q_1^3 + a^{3(n_2-n_1)+1}Q_2^3 + ta^{3(n_3-n_1)}Q_3^3 + ta^{3(n_4-n_1)+1}Q_4^3 = 0.$$

Hence $Q_1^3 + ta^{3(n_3-n_1)}Q_3^3 = 0$ in $E = k'(s, u)[T]/(a)$.

Assume first that $Q_3 = 0$. Then the previous equation shows that Q_1 is divisible by a , which implies that $Q_1 = 0$ by choice of the Q_i 's. Hence $Q_1 = Q_3 = 0$, so Q_2 and Q_4 are both non-zero, and $a^{3(n_2-n_1)+1}Q_2^3 + ta^{3(n_4-n_1)+1}Q_4^3 = 0$. If $n_2 - n_1 \neq n_4 - n_1$, it would imply that Q_1 or Q_3 is divisible by a , which gives a contradiction since Q_1 and Q_2 are non-zero polynomials. Hence $n_2 - n_1 = n_4 - n_1$, and t is then a cube in E . Assume now Q_3 is non-zero. In this case Q_3 is not divisible by a , so t is a cube in E . The remaining cases also give that t is a cube in E .

By definition, we have $E = k'(s, u)(\sqrt{\Delta})$, where $\Delta = (s^3 - 3su)^2 - 4u^3$, and $t = \frac{3su - s^3 \pm \sqrt{\Delta}}{2u^3}$. If t is a cube in E then $12su - 4s^3 \pm 4\sqrt{\Delta}$ is a cube in E . Let denote by τ the unique non-trivial $k'(s, u)$ -automorphism of E . An element $\lambda \in E$ is a cube if and only if $\tau(\lambda)$ is a cube. So $\lambda = 12su - 4s^3 + 4\sqrt{\Delta}$ is a cube.

Write $\lambda = \mu^3$, with $\mu = \frac{R_1 + R_2\sqrt{\Delta}}{R_3}$, where $R_1, R_2, R_3 \in k'[s, u]$. One can assume that R_1, R_2, R_3 are relatively prime. We have $N_{E/k'(s, u)}(\lambda) = 16(3su - s^3)^2 - 16\Delta = 64u^3$, hence

$$64R_3^6u^3 = (R_1^2 - R_2^2\Delta)^3.$$

We also have $(12su - 4s^3 + 4\sqrt{\Delta})R_3^3 = R_1^3 + 3R_1R_2^2\Delta + (R_2^3\Delta + 3R_1^2R_2)\sqrt{\Delta}$, hence

$$4R_3^3 = R_2^3\Delta + 3R_1^2R_2 \text{ and } (12su - 4s^3)R_3^3 = R_1^3 + 3R_1R_2^2\Delta.$$

We now show that R_3 is a constant. Assume the contrary and let S be an irreducible divisor of R_3 . Then S divides $R_1^2 - R_2^2\Delta$ by the first equation, hence S divides $3R_1^3 - 3R_1R_2^2\Delta$. The third equation implies that S divides $R_1^3 + 3R_1R_2^2\Delta$, hence S divides R_1^3 , so S divides R_1 . Hence

S^3 divides $(12su - 4s^2)R_3^3 - R_1^3$, so S^2 divides $3R_2^2\Delta$. Consequently, S divides R_2^2 (even if $S = \Delta$), so S divides R_2 . This is impossible since R_1, R_2, R_3 are relatively prime. Hence, R_3 is a constant and one can assume that $R_3 = 1$.

We then have the equations

$$64u^3 = (R_1^2 - R_2^2\Delta)^3, 4 = R_2^3\Delta + 3R_1^2R_2, 12su - 4s^3 = R_1^3 + 3R_1R_2^2\Delta.$$

The second equation then implies that R_2 and $R_2^2\Delta + 3R_1^2$ are non-zero constant polynomials. In particular R_1^2 and Δ have the same degree in u . This gives a contradiction since these degrees don't have the same parity.

We can now finish the proof of Theorem 3.1 using Proposition 3.2.

Let t be an indeterminate over k , let $\overline{k(t)}$ be an algebraic closure of $k(t)$. Let i be the composite $k \rightarrow k(t) \rightarrow \overline{k(t)}$, where the first map is the natural inclusion, and $k(t) \rightarrow \overline{k(t)}$ is also the inclusion which maps t to itself.

Let $\lambda \in \overline{k(t)}$ such that $j(C_\lambda) = t$ and consider the functor \mathbf{F}_λ of Example 2.3. By Proposition 3.2 we have $\text{ed}_{\overline{k(t)}}(\mathbf{F}_\lambda) = 2$. Thus there exists a field extension $L/\overline{k(t)}$ with $\text{trdeg}(L : \overline{k(t)}) = 2$ and an element $[C] \in \mathbf{F}_\lambda(L)$ which cannot be defined over a subextension of L of a smaller transcendence degree over $\overline{k(t)}$.

We will show that indeed for the element $[C] \in \mathbf{Cub}_3^+(L/k)$, that is when L is viewed as an extension of k , we have $\text{ed}([C]) = 3$ over k .

Assume that there is a subextension K'/k of L/k with $\text{trdeg}(K' : k) \leq 2$ and $[C'] \in \mathbf{Cub}_3^+(K')$ such that $[C']_L = [C]$. Since $[C] \in \mathbf{F}_\lambda(L/k')$, we have $j(C'_L) = j(C) = j((C_\lambda)_L) = \text{image of } t \text{ in } L$. Hence $j(C'_L)$ is transcendental over k . Consequently, $j(C') \in K'$ is transcendental over k and we can define a k -morphism $k(t) \rightarrow K'$ sending t to $j(C')$.

Now the diagram of k -morphisms

$$\begin{array}{ccc} & L & \\ & \swarrow & \searrow \\ \overline{k(t)} & & K' \\ & \swarrow & \searrow \\ & k(t) & \end{array}$$

clearly commutes and hence we can define the compositum E of $\overline{k(t)}$ and K' in L .

4. *The case of singular cubics.*

Take now $[C''] := [C']_E \in \mathbf{Cub}_3^+(E)$. Then clearly $[C'']_L = [C]$ and $[C''] \in \mathbf{F}_\lambda(E)$. But $\text{trdeg}(K' : k) \leq 2$ and $\text{trdeg}(\overline{k(t)} : k) = 1$ so we have $\text{trdeg}(K' : \overline{k(t)}) \leq 1$. It follows that $\text{trdeg}(E : \overline{k(t)}) \leq 1$. Consequently, $[C]$ is defined over a subextension of $L/\overline{k(t)}$ of transcendence degree at most 1 which is absurd.

We then get $\text{ed}_k(\mathbf{Cub}_3^+) \geq \text{ed}([C]) = 3$ and this concludes the proof of Theorem 3.1.

4. THE CASE OF SINGULAR CUBICS.

In the previous section, we have computed the essential dimension of the functor of non-singular cubics. In order to give the essential dimension of \mathbf{Cub}_3 , it remains to compute $\text{ed}(\mathbf{Cub}_3^-)$. That is the purpose of this section. In fact, we have the following result:

THEOREM 4.1. *Let k be a field with $\text{char}(k) \neq 2, 3$. Assume that k contains a primitive third root of unity ε . Then*

$$\text{ed}_k(\mathbf{Cub}_3^-) = 2.$$

We first recall the list of the eight distinct isomorphism classes of singular cubics over a separably closed field (see [16], Chapter I, §7 for example).

$$C_1 = X^3$$

$$C_2 = X^2Y$$

$$C_3 = XY(X + Y)$$

$$C_4 = XYZ$$

$$C_5 = (X^2 - YZ)Y$$

$$C_6 = (X^2 - YZ)X$$

$$C_7 = Y^2Z - X^3$$

$$C_8 = Y^2Z - X^3 - X^2Z$$

Notice that all these cubics are defined over k , so any singular cubic defined over a field extension L/k is isomorphic to one of the C_i 's over L_s . Applying the Galois Descent Lemma shows that the isomorphism classes of L -forms of C_i are classified by $H^1(L, \mathbf{Stab}(C_i))$, where $\mathbf{Stab}(C_i)$ is the stabilizer of the cubic C_i under the action of \mathbf{GL}_3 .

We then get

$$\mathbf{Cub}_3^- \simeq \coprod_{1 \leq i \leq 8} H^1(-, \mathbf{Stab}(C_i)).$$

In particular, we have

$$\mathrm{ed}_k(\mathbf{Cub}_3^-) = \max_{1 \leq i \leq 8} \mathrm{ed}_k(\mathbf{Stab}(C_i)).$$

We now estimate the essential dimension of each stabilizer. To do this, we will apply the following method, already used in Section 3: First compute $\mathbf{Stab}(C_i)(L_s)$ for any field L containing k (using Maple \mathbb{R} for example). We then find an algebraic group scheme G_i such that $G_i(L_s) = \mathbf{Stab}(C_i)(L_s)$ for any field extension L/k . The functors $H^1(-, G_i)$ and $H^1(-, \mathbf{Stab}(C_i))$ are then equal, so they have same essential dimension.

• If $i = 1$, the stabilizer coincide on the L_s -points with the group scheme G_1 defined by

$$G_1(R) = \left\{ \begin{pmatrix} a & 0 & 0 \\ b & c & d \\ e & f & g \end{pmatrix} \in \mathrm{GL}_3(R) \right\}$$

for any k -algebra R . Let also H_1 and K_1 be the group schemes defined respectively by

$$H_1(R) = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ b & 1 & 0 \\ e & 0 & 1 \end{pmatrix} \in \mathrm{GL}_3(R) \right\}$$

and

$$K_1(R) = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & c & d \\ 0 & f & g \end{pmatrix} \in \mathrm{GL}_3(R) \right\}.$$

We easily have $H_1 \simeq \mathbb{G}_a \times \mathbb{G}_a$ and $K_1 \simeq \mathbb{G}_m \times \mathbf{GL}_2$. We then get the following exact sequence

$$1 \longrightarrow \mathbb{G}_a \times \mathbb{G}_a \longrightarrow G_1 \longrightarrow \mathbb{G}_m \times \mathbf{GL}_2 \longrightarrow 1,$$

hence the exact sequence in cohomology then gives $H^1(-, G_1) = 1$, so $\mathrm{ed}_k(G_1) = 0$.

• If $i = 2$, the stabilizer coincides on the L -points with the group scheme G_2 defined by

$$G_2(R) = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ c & d & e \end{pmatrix} \in \mathrm{GL}_3(R) \right\}.$$

We then have

$$1 \longrightarrow \mathbb{G}_a \times \mathbb{G}_a \longrightarrow G_2 \longrightarrow \mathbb{G}_m \times \mathbb{G}_m \times \mathbb{G}_m \longrightarrow 1,$$

so we have again $H^1(-, G_2) = 1$ and $\mathrm{ed}_k(G_2) = 0$.

4. *The case of singular cubics.*

- If $i = 3$, one can take for G_3 the group scheme defined by

$$G_3(R) = \left\{ \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ e & g & h \end{pmatrix} \in \mathrm{GL}_3(R), \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \tilde{K}(R) \right\},$$

where K is a suitable constant subgroup of \mathbf{PGL}_2 (in fact isomorphic to the Klein group). We then have

$$1 \longrightarrow \mathbb{G}_a \times \mathbb{G}_a \longrightarrow G_4 \xrightarrow{f} \mathbb{G}_m \times \tilde{K} \longrightarrow 1,$$

where f is the obvious map. Since this sequence is split, the map

$$f_* : H^1(L, G_3) \rightarrow H^1(L, \mathbb{G}_m \times \tilde{K}) \simeq H^1(L, \tilde{K})$$

is surjective for any L/k . We now proceed to show that f_* is injective.

Let $A = (\mathbb{G}_a \times \mathbb{G}_a)(L_s)$, $B = G_3(L_s)$ and $C = (\mathbb{G}_m \times \tilde{K})(L_s)$. Let β be a cocycle with values in $G_3(L_s)$, and $\gamma = f_*(\beta)$. They induce respectively cocycles with values in $\mathrm{Aut}(B)$ and $\mathrm{Aut}(C)$. Let α be the cocycle with values in $\mathrm{Aut}(A)$ induced by conjugation by β . By [15, (28.11)], the fiber of $[\gamma]$ under f_* is in one-to-one correspondence with the orbit set of the group $(C_\gamma)^{\Gamma_L}$ in $H^1(L, A_\alpha)$. Since the group scheme $(\mathbb{G}_a \times \mathbb{G}_a)_\alpha$, defined over L , is isomorphic to $\mathbb{G}_a \times \mathbb{G}_a$ over L_s , it is smooth connected and unipotent.

Hence $H^1(L, A_\alpha) = H^1(L, (\mathbb{G}_a \times \mathbb{G}_a)_\alpha(L_s)) = 1$. It follows that the fiber of $[\gamma] = f_*([\beta])$ is $\{[\beta]\}$, for any $[\beta] \in H^1(L, B)$, so f_* is injective.

Consequently, we get

$$H^1(-, G_3) \simeq H^1(-, \tilde{K}).$$

Using Proposition 1.18 of Chapter III we find that $\mathrm{ed}_k(\tilde{K}) \leq 1$.

- If $i = 4$, one can take for G_4 the semidirect product of \mathbb{G}_m^3 by S_3 , the latter group acting on the former by conjugation. The inclusion $G_4 \subset \mathbf{GL}_3$ then gives rise to a linear action of G_4 on \mathbb{A}_k^3 .

Now let $\rho : S_3 \rightarrow \mathbf{GL}_2$ be the faithful representation which sends the permutation (123) to $\begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}$ and (12) to $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Letting \mathbb{G}_m^3 act trivially on \mathbb{A}_k^2 , the corresponding action of S_3 on \mathbb{A}_k^2 then extends to a linear action of G_4 on \mathbb{A}_k^2 .

We then obtain naturally a linear action of G_4 on \mathbb{A}_k^5 , which is generically free (details are left to the reader). By Proposition 1.11 of Chapter III, we get $\mathrm{ed}_k(G_4) \leq 2$.

- If $i = 5$, let G_5 defined by

$$G_5(R) = \left\{ \left(\begin{array}{ccc} u & \frac{vw}{2u} & 0 \\ 0 & v & 0 \\ w & \frac{vw^2}{4u^2} & \frac{u^2}{v} \end{array} \right) \mid u, v \in R^\times, w \in R \right\}.$$

Let H and K be the group schemes defined by

$$H(R) = \left\{ \left(\begin{array}{ccc} 1 & \frac{w}{2} & 0 \\ 0 & 1 & 0 \\ w & \frac{w^2}{4} & 1 \end{array} \right) \mid w \in R \right\},$$

and

$$K(R) = \left\{ \left(\begin{array}{ccc} u & 0 & 0 \\ 0 & v & 0 \\ 0 & 0 & \frac{u^2}{v} \end{array} \right) \mid u, v \in R^\times \right\}.$$

Then one can easily check that H and K are respectively isomorphic to \mathbb{G}_a and \mathbb{G}_m^2 , and that we have an exact sequence

$$1 \rightarrow \mathbb{G}_a \rightarrow G_5 \rightarrow \mathbb{G}_m^2 \rightarrow 1.$$

Applying Galois cohomology to it then shows that $H^1(-, G_5) = 1$, so $\text{ed}_k(G_5) = 0$.

- If $i = 6$, let G_6 defined by

$$G_6(R) = \left\{ u \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & v & 0 \\ 0 & 0 & v^{-1} \end{array} \right), u \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 0 & v \\ 0 & v^{-1} & 0 \end{array} \right) \mid u, v \in R^\times \right\}.$$

Let H be the group scheme defined by

$$H(R) = \left\{ \left(\begin{array}{cc} v & 0 \\ 0 & v^{-1} \end{array} \right), \left(\begin{array}{cc} 0 & v \\ v^{-1} & 0 \end{array} \right) \mid v \in R^\times \right\}.$$

One can easily check that H is the stabilizer of the quadratic form $q_0 : (x, y) \mapsto xy$, namely $\mathbf{O}(q_0)$. We then have $G_6 \simeq \mathbb{G}_m \times \mathbf{O}(q_0)$, so $H^1(-, G_6) \simeq H^1(-, \mathbf{O}(q_0))$. Hence we get $\text{ed}_k(G_6) = \text{ed}_k(\mathbf{O}(q_0)) = 2$ (last equality holds by Theorem 2.10 of Chapter II).

- If $i = 7$, let G_7 defined by

$$G_7(R) = \left\{ \left(\begin{array}{ccc} u & 0 & 0 \\ 0 & \frac{u^3}{v^2} & 0 \\ 0 & 0 & v \end{array} \right), u, v \in R^\times \right\}.$$

Clearly we have $G_7 \simeq \mathbb{G}_m \times \mathbb{G}_m$ and $\text{ed}_k(G_7) = 0$.

4. *The case of singular cubics.*

- If $i = 8$, one can take G_8 of the form \tilde{K} , where K is a constant subgroup of \mathbf{PGL}_3 , so $\text{ed}_k(G_8) \leq 2$ by Proposition 1.18 of Chapter III.

This concludes the proof.

COROLLARY 4.2. *Let k be a field of characteristic different from 2 and 3 containing ε . Then*

$$\text{ed}_k(\mathbf{Cub}_3) = 3.$$

Theorem 4.1 proves also that $\text{ed}_k(\mathbf{Cub}_3) = \text{ed}_k(\mathbf{Cub}_3^+)$ and that

$$\text{ed}(\mathbf{Cub}_3^-) < \text{ed}_k(\mathbf{Cub}_3^+).$$

This is also true for cubics in two variables. Indeed, it is easy to see that any singular cubic in two variables defined over a field L is isomorphic to X^3 or X^2Y over L_s . Arguing as in the proof of Theorem 4.1 shows that the stabilizers of these two cubics have a trivial H^1 . Hence \mathbf{Cub}_2^- is reduced to two points, so $\text{ed}_k(\mathbf{Cub}_2^-) = 0$.

In general it seems reasonable to expect that $\text{ed}_k(\mathbf{F}_{d,n}) = \text{ed}_k(\mathbf{F}_{d,n}^+)$ and that $\text{ed}(\mathbf{F}_{d,n}^-) < \text{ed}(\mathbf{F}_{d,n}^+)$, since singular hypersurfaces are not “general enough” to maximize essential dimension.

REMARK 4.3. All the discussion on cubics is new and the results obtained were not known before. Recently we found a proof of Corollary 4.2 for every field k of characteristic $\neq 2, 3$ thus dropping the hypothesis $\varepsilon \in k$. Moreover Proposition 3.2 is avoided in this new proof thus simplifying considerably the present section. One may find this new argument in [4] which uses a new result in [3].

BIBLIOGRAPHY

- [1] J. Arason, *Cohomologische Invarianten quadratischer Formen*. J. of Algebra **36** (1975), 446–491
- [2] A.–M. Bergé, J. Martinet, *Formes quadratiques et extensions en caractéristique 2*. Ann. Inst. Fourier (2), **35** (1985) 57–77
- [3] G. Berhuy, G. Favi, *Essential dimension: A functorial point of view (After A. Merkurjev)*. Doc. Math., **8** (2003) 277–324
- [4] G. Berhuy, G. Favi, *Essential dimension of cubics*. To appear in Journal of Algebra
- [5] J. Bochnak, M. Coste, M.-F. Roy, *Real algebraic geometry*. Results in Mathematics and Related Areas (3), **36**, Springer-Verlag, Berlin (1998)
- [6] E. Brieskorn, H. Knörrer, *Plane Algebraic Curves*. Birkhäuser Verlag, Basel, Boston, Stuttgart (1986)
- [7] J. Buhler, Z. Reichstein, *On the essential dimension of a finite group*. Comp. Math. **106** (1997), 159–179
- [8] P.M. Cohn, *Algebra, vol. 2*. John Wiley & Sons Ed., London (1977)
- [9] A. Delzant, *Définition des classes de Stiefel-Whitney d’un module quadratique sur un corps de caractéristique différente de 2*. C.R Acad. Sci. Paris **255** (1962), 1366–1368
- [10] M. Demazure, P. Gabriel, *Groupes algébriques, vol. 1*. Ed. Masson & Cie (1970)
- [11] M. Demazure, A. Grothendieck, *Schémas en groupes, vol. 1*. SGA 3, Springer-Verlag (1970)
- [12] C. Drees, M. Epkenhans, M. Krüskemper, *Computation of the trace form of Galois extensions*. J. of Algebra **192** (1997), 209–234
- [13] R. Garibaldi, A. Merkurjev, J.-P. Serre, *Cohomological invariants in Galois cohomology*. AMS University Lecture Series **28** (2003)
- [14] C Jensen, A Ledet, N Yui, *Generic Polynomials* MSRI Publ. **45**, Cambridge University Press (2002)
- [15] M.-A. Knus, A. Merkurjev, M. Rost, J.-P. Tignol, *The book of involutions*. AMS Coll. Pub. **44** (1998)
- [16] H. Kraft, *Geometrische Methoden in der Invariantentheorie*. Aspects of Mathematics, D1. Friedr. Vieweg & Sohn, Braunschweig (1984)
- [17] A. Merkurjev, *Essential dimension*. Private notes (1999), Lecture notes (2000)

- [18] J.S. Milne, *Étale Cohomology*. Princeton Math. Series **33**, Princeton University Press, Princeton, N.J. (1980)
- [19] Z. Reichstein, *On the notion of essential dimension for algebraic groups*. Transformation Groups **5**, no. 3 (2000), 265–304
- [20] M. Rosenlicht, *Some basic theorems on algebraic groups*. American J. of Math. **78** (1963), 401–443
- [21] M. Rost, *Computation of some essential dimensions*. Preprint (2000). Available on <http://www.math.ohio-state.edu/~rost/ed.html>
- [22] M. Rost, *Essential dimension of twisted C_4* . Preprint (2000). Available on <http://www.math.ohio-state.edu/~rost/ed.html>
- [23] J.-P. Serre, *Cohomologie Galoisienne*. Cinquième éd. Lecture Notes **5**, Springer-Verlag (1997)
- [24] J.-P. Serre, *Corps locaux*. Hermann, Paris (1962)
- [25] J.-P. Serre, *Topics in Galois Theory*. Research notes in Math. **1**, Jones and Bartlett Pib., Boston, MA (1992)
- [26] W. Scharlau, *Quadratic and hermitian forms*. Grund. Math. Wiss. **270**, Springer-Verlag, Berlin-Heidelberg (1985)
- [27] R. W. Thomason, *Comparison of equivariant algebraic and topological K - theory*. Duke Math. J. **53**, No 3, (1986), 795–825

Favi Giordano
Institut de Mathématiques (Défunt)
Université de Lausanne
giordano.favi@ima.unil.ch, giordano.favi@epfl.ch