ESSENTIAL DIMENSION OF CUBICS

Grégory Berhuy & Giordano Favi

March 2003

Abstract. In this paper, we compute the essential dimension of the functor of cubics in three variables up to linear changes of coordinates when the base field has characteristic different from 2 and 3. For this, we use canonical pencils of cubics, Galois descent techniques, and the basic material on essential dimension developed in [BeF] which is based on Merkurjev's notes [M].

§0 Introduction

Let C be a polynomial in n variables with coefficients in a ring or a field. A question one may ask is whether it is possible, by linearly changing the variables, to drop some of its coefficients or make it "nicer". For instance, the quadratic polynomial X^2+bX+c can always be brought, by a change of variables, to the form X^2+d as soon as one can divide by 2. Similarly the cubic polynomial X^3+aX^2+bX+c can be reduced to X^3+dX+d when $\frac{1}{3}$ makes sense. In both cases one feels that "only one parameter is needed" to describe these polynomials. We shall say in these cases that the *essential dimension* is 1.

Essential dimension makes precise the notion of "how many parameters are needed to describe a given structure" in some general context. This was first introduced by Reichstein and Buhler in [BR] and by Reichstein in [Re]. Later Merkurjev in [M] developed some general functorial context for essential dimension. Since [M] is unpublished, we refer to [BeF] for all the generalities on essential dimension.

The aim of this paper is to use some techniques, which can be found in [BeF], for the computation of the essential dimension of the functor $\mathbf{Cub}_3$ of homogenous cubic polynomials in three variables up to linear changes of coordinates. This functor associates to a field L the set of equivalence classes of cubic curves in $\mathbb{P}^2$ defined over L, where two curves are considered equivalent if they differ by a linear change of coordinates in $\mathbb{P}^2(L)$.

We will show the following result:

Theorem. *Let k be a field of characteristic different from 2 and 3. Then*

$$\mathrm{ed}_k(\mathbf{Cub}_3) = 3.$$

The proof of this result is based on the following geometric idea: informally speaking, defining a non-singular cubic over a field L up to projective equivalence is equivalent to specifying (i) a configuration of nine (unordered) flex points in $\mathbb{P}^2(L_s)$ (where L_s is a separable closure of L) and (ii) a value of the j-invariant. We show that these two choices are independent and that

(i) requires two parameters. For this, we compute the essential dimension of the functor of cubics with prescribed j-invariant and of the functor of cubics with prescribed flex points. The advantage of this approach is that these two functors can be described as Galois cohomology functors of some suitable algebraic groups; we then use crucially generically free representations of these groups to compute their essential dimensions.

In §1, we introduce the basic material on essential dimension which will be needed in the sequel. We then recall in §2 the basic definitions and classical results on cubics in 3 variables. In §3, we state and prove a Galois descent lemma for functors, which generalize a little bit the classical one, and apply it to classify pencils of cubics and cubics with prescribed j-invariant. Along the way, we also compute the essential dimension of cubics in 2 variables. Finally, the two last sections are devoted to the proof of the main result, by separate computations of the essential dimension of the functors of singular and non-singular cubics.

We will assume that the reader is familiar with the theory of affine group schemes, and we will refer to [KMRT] for all the basic material we could use on this topic.

The authors would thank warmly Philippe Chabloz, Manuel Ojanguren, Zinovy Reichstein and Armin Rigo for helpful conversation. The first named author also gratefully acknowledges support from the Swiss National Science Foundation, grant No 2100-065128.01/1. Finally the authors would also thank the referee for his/her careful reading and constructive remarks, which have permitted in particular to shorten considerably the proof of Proposition 4.2.

§1 Essential dimension of functors: some definitions and results

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. If $\mathbf{F}$ is such a functor in $\mathfrak{F}_k$ and $K/k \longrightarrow L/k$ is a morphism in $\mathfrak{C}_k$, for every element $a \in \mathbf{F}(K/k)$ its image under the map $\mathbf{F}(K/k) \longrightarrow \mathbf{F}(L/k)$ will be denoted by a_L. When no confusion is possible, we will write $\mathbf{F}(K)$ instead of $\mathbf{F}(K/k)$.
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.

We recall the definition of the essential dimension of a functor $\mathbf{F} : \mathfrak{C}_k \longrightarrow \mathbf{Sets}$ due to Merkurjev as introduced in [M] and [BeF, Definition 1.2].

Definition 1.1. *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* $\mathrm{ed}(a) \leq n$*), if there exists a subextension E/k of K/k such that :*

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

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

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

For a group scheme G of finite type over k the essential dimension of the Galois cohomology functor $H^1(\_, G)$ will be denoted by $\mathrm{ed}_k(G)$. This is the case of main interest in [BR],[Re],[M] and [BeF] since many functors can be viewed as Galois cohomology functors.

Let us recall some results proved in [BeF]:

For any field extension k'/k, any functor $\mathbf{F} : \mathfrak{C}_k \longrightarrow \mathbf{Sets}$ gives rise to an element of $\mathfrak{F}_{k'}$. We denote by $\mathrm{ed}_{k'}(\mathbf{F})$ its essential dimension. It is easily checked that $\mathrm{ed}_{k'}(\mathbf{F}) \leq \mathrm{ed}_k(\mathbf{F})$ holds. We will often use this fact. For example to give lower bounds of the essential dimension of a functor one can suppose k algebraically closed.

The following result will be useful for our purpose. It relates the essential dimension of an algebraic group to that of a closed subgroup.

Proposition 1.2. *Let G be an algebraic group defined over k, and let H be a closed subgroup. Then*

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

Proof. See [Re],[M] or [BeF, Theorem 6.19].

We now recall some facts on free actions.

Let G be an algebraic group defined over k acting on a k-scheme X of finite type. We say that G *acts freely on* X if for any k-algebra R the group $G(R)$ acts freely on $X(R)$, that is the stabilizer of any element $x \in X(R)$ under the action of $G(R)$ is trivial.

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

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

Now consider the two following conditions:

(i) The group $G(\bar{k})$ acts freely on $X(\bar{k})$

(i') The group $G(\bar{k})$ acts freely on $X(\bar{k})$, and for any closed point $x \in X$, the Lie algebra $\mathrm{Lie}(G_x)$ is trivial, where G_x denotes of the scheme-theoretic stabilizer of x.

By [DG], III, §2 Corollary 2.5 and Corollary 2.8, G acts freely on X if and only if (i) (resp. (i')) holds if $\mathrm{char}(k) = 0$ (resp. $\mathrm{char}(k) \neq 0$).

The second part of condition (i') can be checked easily using the following description of $\mathrm{Lie}(G_x)$ (see [DeGa], III, §2, proof of Prop. 2.6.): let $k(x)$ be the residue field of x. Then we have

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

We say that G *acts generically freely on* X if there exists a dense G-stable open subset of X on which G acts freely.

Proposition 1.3. *Let G be an algebraic group over k acting linearly an generically freely on an affine space $\mathbb{A}(V)$. Then there exists a non-empty G-stable open subset U of $\mathbb{A}(V)$ such that the geometric quotient U/G exists and is a classifying scheme for $H^1(\_, G)$. In particular, we have*

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

Proof. See [BeF, Proposition 4.10] or [M].

Notice that, if k is an algebraically closed field of characteristic zero, the above proposition is the original definition of Reichstein (see [Re, Definition 3.5]) and that Proposition 1.2 is a direct consequence of that definition.

We now give an application of Proposition 1.3. Recall that a group scheme G is called étale if G is finite and smooth.

Proposition 1.4. *Let G be an étale subgroup of $\mathbf{PGL}_n$ defined over k, and let $\widetilde{G}$ be the inverse image of G under the canonical projection $\pi : \mathbf{GL}_n \longrightarrow \mathbf{PGL}_n$. Then*

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

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

By [BeF, Proposition 4.13], 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 $\widetilde{U}$ be the inverse image of U under the quotient map $\mathbb{A}^n - \{0\} \longrightarrow \mathbb{P}^{n-1}$. Clearly this is a $\widetilde{G}$-dense open subset of $\mathbb{A}^n$. We now show that $\widetilde{G}$ acts freely on $\widetilde{U}$.

Let $\widetilde{u} \in \widetilde{U}(k_s)$ and $\widetilde{g} \in \widetilde{G}(k_s)$ such that $\widetilde{g} \cdot \widetilde{u} = \widetilde{u}$. Now let $g = \pi(\widetilde{g}) \in G(k_s)$ 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 $\widetilde{g} \cdot \widetilde{u} = \widetilde{u}$, so $\widetilde{G}(k_s)$ acts freely on $\widetilde{U}(k_s)$.

We now have to check the condition on the Lie algebra. Recall that the Lie algebra of $\widetilde{G}$ is the Lie algebra of its connected component, which is $\mathbb{G}_m$, so $\mathrm{Lie}(\widetilde{G}) = k$, where k is identified with the subgroup of scalar matrices. It readily follows that condition (i') above is satisfied.
Thus the action of $\widetilde{G}$ on $\mathbb{A}^n_k$ satisfy the conditions of Proposition 1.3. Hence

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

§2 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 its defining polynomial. 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 down $C = \sum a_{i_1,\dots,i_n} X_1^{i_1} \cdots X_n^{i_n}$ (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 become algebraically dependent. 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 $C \in \mathbf{C}_{d,n}(L)$ and $\varphi \in \mathbf{GL}_n(L)$, 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 sometimes by $[C]$ the class of $C \in \mathbf{C}_{d,n}(L)$. 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 a linear change of variables. In other words we would like to compute its essential dimension. It is shown in [BeF, Examples 1.20] that the following inequalities hold

$$m - n^2 \leq \mathrm{ed}(\mathbf{F}_{d,n}) \leq m - 1$$

where m is the binomial coefficient $\binom{d+n-1}{n-1}$.

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

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

since the equality $\mathrm{ed}_k(\mathbf{F} \coprod \mathbf{G}) = \max\{\mathrm{ed}_k(\mathbf{F}), \mathrm{ed}_k(\mathbf{G})\}$ holds for two objects $\mathbf{F}, \mathbf{G}$ of $\mathfrak{F}_k$ (see [BeF, Lemma 1.10]). We will thus treat singular hypersurfaces and non-singular ones separetely.

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 $\mathbf{Cub}^+_n$, $\mathbf{Cub}^-_n$). Our aim is to compute $\mathrm{ed}_k(\mathbf{Cub}_3)$.

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 $\mathrm{char}(k) \neq 3$.

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

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

We also define $C_\infty = X_1 X_2 X_3$. 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, which can be easily found in the literature.

We begin with the following classical result:

Lemma 2.0. *Assume that $k = k_s$. Then every non-singular cubic C over k is equivalent to some C_λ for some $\lambda \in k$.*

For a non-singular cubic C with coefficients in a field L the j-invariant is well defined. We denote it by $j(C)$. This is a rational expression with coefficients in L of the coefficients of C. It depends only on the equivalence class of the cubic and it is a non-constant invariant. One possible way to define it is the following: let C be a non-singular cubic over L. By the previous lemma, C is equivalent over L_s to some C_λ. Then we set $j(C) = \frac{\lambda^3(\lambda^3+8)^3}{(\lambda^3-1)^3}$. One can show that this is in fact an element of L, which is well-defined and which only depends on $[C]$.

We recall now the definition of a flex point. 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. This is again a cubic polynomial with coefficients in L. A **flex point** of a given cubic C is a point $P \in \mathbb{P}^2(L_s)$ which satisfies $C(P) = H_C(P) = 0$.

Any non-singular cubic of the form C_λ (and hence any non-singular cubic) has exactly nine flex points.

We denote the flex points of C_λ by $x_{00}, \ldots, x_{22}$. We then have

$$x_{00} = (0 : -1 : 1),\ x_{01} = (0 : -\varepsilon : 1),\ x_{02} = (0 : -\varepsilon^2 : 1),$$

$$x_{10} = (1 : 0 : -1),\ x_{11} = (1 : 0 : -\varepsilon),\ x_{12} = (1 : 0 : -\varepsilon^2),$$

$$x_{20} = (-1 : 1 : 0),\ x_{21} = (-\varepsilon : 1 : 0),\ x_{22} = (-\varepsilon^2 : 1 : 0),$$

where ε denotes a primitive cubic root of unity.

If $C = C_1, C_\varepsilon, C_{\varepsilon^2}$ or C_∞, then C consists in three distincts lines in $\mathbb{P}^2(k_s)$. We then get a configuration of 9 points and 12 lines, each line passing exactly through 3 of these points.

We recall the definition of the Hessian group, which plays a crucial rule in our work.

The Hessian group, that is denoted by G_{216} in [BK], and that we will denote here by $\mathfrak{G}$ is the group of elements of $\mathbf{PGL}_3(k_s)$ which preserves the configuration above. This group is isomorphic to the group of special affinities $\mathrm{SA}_2(\mathbb{F}_3)$, which is generated by the translations of the plane $\mathbb{F}_3^2$ and the elements of $\mathrm{SL}_2(\mathbb{F}_3)$. It has 216 elements and is isomorphic to the semidirect product $\mathbb{F}_3^2 \ltimes \mathrm{SL}_2(\mathbb{F}_3)$. The isomorphism in one direction is given as follows:

If $g \in \mathrm{SA}_2(\mathbb{F}_3)$, 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 exists a unique element $\overline{M}_g \in \mathbf{PGL}_3(k_s)$ 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 $\overline{A}$ and $\overline{C}$, where

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \text{ and } C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \varepsilon & 0 \\ 0 & 0 & \varepsilon^2 \end{pmatrix}.$$

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 $\overline{D}, \overline{E}$ and $\overline{E'}$, where

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \varepsilon & 0 \\ 0 & 0 & \varepsilon \end{pmatrix}, E = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \varepsilon & \varepsilon^2 \\ 1 & \varepsilon^2 & \varepsilon \end{pmatrix} \text{ and } E' = \begin{pmatrix} \varepsilon^2 & 1 & 1 \\ \varepsilon & 1 & \varepsilon \\ \varepsilon & \varepsilon & 1 \end{pmatrix}.$$

Notice that the set of generators for $\mathrm{SA}_2(\mathbb{F}_3)$ in [BK] is not completely correct. Indeed, the 2-Sylow subgroup of $\mathfrak{G}$ is the quaternion group, so it is generated by 2 elements of order 4, but the element $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$, which corresponds to the class of $B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ given in [BK] p. 297, has order 2. Notice also that $\mathfrak{G}$ is in fact a subgroup of $\mathbf{PGL}_3(k(\varepsilon))$.

Let us recall some results proved in [BK], p. 292–298:

Lemma 2.1. *Assume that $k = k_s$. Then:*

1) *Two cubics are equivalent if and only if they have same j-invariant.*
2) *Let $\lambda \in k \cup \{\infty\}$. For any $\overline{\varphi} \in \mathbf{PGL}_3(k)$, $\overline{\varphi}$ maps C_λ to some C_μ if and only if $\overline{\varphi} \in \mathfrak{G}$.*
3) *Let $\lambda \in k \cup \{\infty\}$. For any $\overline{\varphi} \in \mathbf{PGL}_3(k)$, $\overline{\varphi}$ maps the cubic C_λ to itself if and only if $\overline{\varphi}$ belongs to the subgroup $H = \langle \overline{A}, \overline{B}, \overline{C} \rangle$.*

Lemma 2.0 and the two first statements of Lemma 2.1 are proved in [BK], 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 mentionned in [BK] 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

As we have pointed out in the introduction, we would like to show that the choice of flex points and of the j-invariant is sufficient to describe a cubic up to equivalence. In particular, we have to study cubics with prescribed flex points. This can be done using pencils.

If C is a cubic polynomial in 3 variables with coefficients in L, let $\mathcal{F}_C$ be the set of cubic hypersurfaces of the form $\alpha C + \beta H_C \in \mathbf{C}_{3,3}(L)$, 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.

If $P \in \mathbb{P}^2(L_s)$ is a flex point of the cubic C, then it is also a point of any cubic belonging to the pencil $\mathcal{F}_C$. In particular, if C is non-singular, any non-singular cubic $C' \in \mathcal{F}_C$ has the same flex points as C. In fact $\mathcal{F}_C$ is, in this case, the set of all cubics (singular or not) which pass through the nine flex points of C.

Let $\mathfrak{P}(L)$ denote the set $\{\mathcal{F}_C \mid C \in \mathbf{C}_{3,3}(L)\}$. For any k-morphism $L \to L'$ we define a map $\mathfrak{P}(L) \longrightarrow \mathfrak{P}(L')$ by sending the pencil $\mathcal{F}_C$ to the pencil $\mathcal{F}_{C_{L'}}$. We then obtain a functor $\mathfrak{P} : \mathfrak{C}_k \longrightarrow \mathbf{Sets}$. The association $C \mapsto \mathcal{F}_C$ gives rise to a surjective map of functors $\mathbf{C}_{3,3} \twoheadrightarrow \mathfrak{P}$. Consider the natural action of $\mathbf{GL}_3$ on $\mathfrak{P}$: 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 2.2. *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* $\mathbf{Cub}_3 \longrightarrow \mathbf{Pen}_3$.

A L-isomorphism f between $\mathcal{F}_C$ and $\mathcal{F}_{C'}$ maps the flex points of C to the flex points of C'. Hence $\mathcal{F}_{[C]}$ can be thought roughly speaking as the set of isomorphism classes of cubics $[C']$ such that the flex points of C can be mapped to those of C' via an element of $\mathbf{GL}_3(L)$.

Lemma 2.0 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 infinitely many cubics defined over L which are not equivalent over L_s. Hence one cannot classify cubics using Galois cohomology like in the quadratic form case. However the next lemma shows that pencils of cubics can, indeed, be classified in this manner, as we will see in the next section.

Lemma 2.3. *Assume that* $\mathrm{char}(k) \neq 2, 3$ *and let L/k be a field extension. For any $\lambda \in L$ with $\lambda^3 \neq 1$, 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 $\alpha = \dfrac{72 - 54\lambda^2\mu - 18\lambda^3}{\lambda - \mu}$.
We claim that $\alpha - 54\lambda^2 \neq 0$. Indeed, assume the contrary. Then we easily get that $72(1-\lambda^3) = 0$. Since $\mathrm{char}(k) \neq 2, 3$, 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 $\alpha = -\dfrac{\lambda^2}{4(\lambda^3 - 1)}$ and $\beta = -\dfrac{1}{216(\lambda^3 - 1)}$.

Remark 2.4. 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.

Roughly speaking, Lemma 2.3 suggests that an element of $\mathcal{F}_C$ can have any prescribed value for its j-invariant since, after scalar extension, one obtains all the cubics C_μ. The next lemma shows that at most only one more parameter is needed to define $[C]$ once the flex points are prescribed:

Lemma 2.5. *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 $\mathrm{trdeg}(K:k) = \mathrm{ed}_k([C])$. 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, and $[C'] \in \mathbf{C}_{3,3}(E)$ such that $[\mathcal{F}_C] = [\mathcal{F}_{C'_K}]$. 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 $n+1$.

§3 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 set. 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 [BOI], Proposition (29.1). This lemma will apply to our situation.

Let k be any field, and let $\mathbf{F} : \mathfrak{C}_k \to \mathbf{Sets}$ be a functor. 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 defined 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

$$\mathbf{Stab}_G(a)(R) = \{g \in G(R) \mid \rho_R(g)(a_R) = a_R\}$$

for any k'-algebra R. This is a closed group subscheme of $G_{k'}$ (not necessarily affine).

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:

Galois Descent Lemma. *Let $\rho : G \longrightarrow \mathrm{Aut}(\mathbf{F})$ as above. Assume that for any extension L/k, the following conditions hold:*

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

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

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 [BOI], Corollary 28.2 for example).

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 is a natural a 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.

Example 3.0. (**Cubics in 2 variables**). Let k be a field of characteristic not equal to 3. Denote by $\mathbf{F}$ the functor $\mathbf{C}_{3,2}$ and let G be the group $\mathbf{GL}_2$. A cubic in 2 variables with coefficients in k determines a set of three (non necessarily distinct) points in $\mathbb{P}^1(k_s)$. Since $\mathbf{PGL}_2(k_s)$ acts transitively on triples of distinct points in $\mathbb{P}^1(k_s)$ it follows that all non-singular cubics in 2 variables are equivalent over k_s. Thus if $a \in \mathbf{C}^+_{3,2}(k)$ is a fixed non-singular cubic then $\mathbf{F}_a(L) = \mathbf{Cub}^+_2(L)$ for every L/k. We then get an isomorphism of functors

$$\mathbf{Cub}_2^+ \simeq H^1(\_, \mathbf{Stab}_G(a))$$

for every non-singular cubic a defined over k.

Notice that in this case, $\mathbf{Stab}_G(a)$ is affine. Moreover, an easy computation shows that the Lie algebra of $\pi(\mathbf{Stab}_G(a)) \subset \mathbf{PGL_2}$ is trivial, hence this last group scheme is finite and smooth.

Consequently, $\mathbf{Stab}_G(a)$ is the inverse image of an étale subgroup of $\mathbf{PGL_2}$. To determine this étale subgroup, it suffices to determine its k_s-points. For example, if $a = XY(X+Y)$, it is easy to see that $\pi(\mathbf{Stab}_G(a))(k_s)$ is the subgroup of $\mathbf{PGL}_2(k_s)$ isomorphic to S_3 (as an abstract group) generated by the classes of $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Notice that Γ_k acts trivially on this group, so $\pi(\mathbf{Stab}(a))$ is isomorphic to the constant group scheme S_3. Thus

$$\mathbf{Cub}_2^+ \simeq H^1(\_, \widetilde{S}_3).$$

In particular, $\mathrm{ed}_k(\mathbf{Cub}_2^+) = \mathrm{ed}_k(\widetilde{S}_3)$. Applying Proposition 1.4 we get that $\mathrm{ed}_k(\widetilde{S}_3) \leq 1$. Now $\widetilde{S}_3$ contains a subgroup isomorphic to $\mathbb{G}_m \times \mathbb{Z}/2$, which has essential dimension 1. Proposition 1.2 then shows the $\mathrm{ed}_k(\widetilde{S}_3) \geq 1$, so $\mathrm{ed}_k(\mathbf{Cub}_2^+) = 1$.

Singular cubics are dealt with similarly. Every singular cubic in 2 variables defined over k is equivalent over k_s to either X^3 or X^2Y. Thus we have an isomorphism of functors

$$\mathbf{Cub}_2^- \simeq H^1(\_, \mathbf{Stab}_G(X^3)) \coprod H^1(\_, \mathbf{Stab}_G(X^2Y)).$$

Now the groups $H = \mathbf{Stab}_G(X^3)$ and $K = \mathbf{Stab}_G(X^2Y)$ are easily computed to be equal respectively to $\begin{pmatrix} * & 0 \\ * & * \end{pmatrix}$ and $\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$. Thus $K = \mathbb{G}_m \times \mathbb{G}_m$ and H fits into an exact sequence

$$0 \to \mathbb{G}_a \to H \to \mathbb{G}_m \times \mathbb{G}_m \to 0.$$

It follows easily that $H^1(\_, H) = H^1(\_, K) = 1$, hence $\mathbf{Cub}_2^-$ is reduced to two points, so $\mathrm{ed}_k(\mathbf{Cub}_2^-) = 0$.

Hence we have proved

Proposition 3.1. *Let k be a field of characteristic different from 3. Then*

$$\mathrm{ed}_k(\mathbf{Cub}_2) = 1.$$

Example 3.2. Assume that $\text{char}(k) \neq 2, 3$. 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 2.3 tells us that $\mathbf{F}_a(L) = \mathbf{Pen}_3^+(L)$ for any extension L/k.

Since $\mathcal{F}_{C_\lambda}$ can be viewed as a point in a suitable grassmanian, its stabilizer is affine. As previously, one can check that this stabilizer is the inverse image of an étale closed subgroup of $\mathbf{PGL}_3$. Since over k_s the pencil $\mathcal{F}_{C_\lambda}$ is equal to $\{C_\mu \mid \mu \in k_s \cup \{\infty\}\}$ it follows easily from Lemma 2.1 that the $\pi\left(\mathbf{Stab}_G(\mathcal{F}_{C_\lambda})\right)(k_s) = \mathfrak{G}$, hence $\mathbf{Stab}_G(\mathcal{F}_{C_\lambda}) \simeq \widetilde{\mathfrak{G}}_{\text{ét}}$, where $\mathfrak{G}_{\text{ét}}$ is the étale group scheme associated to the finite group $\mathfrak{G}$. Since the hypotheses of the Galois Descent Lemma are clearly fullfilled, we get

$$\mathbf{Pen}_3^+ \simeq H^1(\_, \widetilde{\mathfrak{G}}_{\text{ét}}).$$

Example 3.3. Under the same hypotheses, 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 k'-group scheme $\mathbf{Stab}_G(a)$ is isomorphic to $\widetilde{H}_{\text{ét}}$, where H is the subgroup of $\mathfrak{G}$ described in Lemma 2.1. 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

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

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

§4 Essential dimension of non-singular cubics

We can finally state and prove our main result:

Theorem 4.1. *Let k be a field. Assume that* $\text{char}(k) \neq 2, 3$. *Then*

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

We prove first the upper bound. Lemma 2.5 implies in particular that

$$\text{ed}_k(\mathbf{Cub}_3^+) \leq \text{ed}_k(\mathbf{Pen}_3^+) + 1.$$

By Example 3.2, we have $\text{ed}_k(\mathbf{Pen}_3^+) = \text{ed}_k(\widetilde{\mathfrak{G}}_{\text{ét}})$. By Proposition 1.4 we have $\text{ed}_k(\widetilde{\mathfrak{G}}_{\text{ét}}) \leq 2$. Moreover, $\widetilde{\mathfrak{G}}_{\text{ét}}$ contains a subgroup isomorphic to $\mathbb{G}_m \times \mu_3 \times \mu_3$ (the inverse image of the étale subgroup of $\mathbf{PGL}_3$ corresponding to the subgroup generated by the classes of C and D). This group has essential dimension 2 (see [BeF, Corollary 3.9]). Then Proposition 1.2 shows that $\text{ed}_k(\widetilde{\mathfrak{G}}_{\text{ét}}) = 2$. We then get $\text{ed}_k(\mathbf{Pen}_3^+) = 2$ (this tells that one needs two parameters to choose nine flex points). In particular, $\text{ed}_k(\mathbf{Cub}_3^+) \leq 3$.

We now show the opposite inequality.

Let k'/k be a field extension, $\lambda \in k'$ with $\lambda^3 \neq 1$ and consider $\mathbf{F}_\lambda$ the functor defined in Example 3.2.

Our task is to compute the essential dimension of $\mathbf{F}_\lambda$, that is the essential dimension of $\widetilde{H}_{\text{ét}}$.

Proposition 4.2. *Let k' be a field with* $\mathrm{char}(k') \neq 2, 3$. *Then*

$$\mathrm{ed}_{k'}(\widetilde{H}_{\text{ét}}) = 2.$$

Proof. We begin with some easy observations on the group $\widetilde{H}_{\text{ét}}$. First of all, we have the following exact sequence of group schemes:

$$1 \longrightarrow \mathbb{G}_m \longrightarrow \widetilde{H}_{\text{ét}} \longrightarrow H_{\text{ét}} \longrightarrow 1,$$

hence $\dim(\widetilde{H}_{\text{ét}}) = 1$. Moreover, the connected component of $\widetilde{H}_{\text{ét}}$ is $\mathbb{G}_m$ and the quotient $\widetilde{H}_{\text{ét}}/\mathbb{G}_m$ is isomorphic to the étale group scheme $H_{\text{ét}} = (\mathbb{Z}/3 \times \mu_3) \ltimes \mathbb{Z}/2$. Finally, notice that $\widetilde{H}_{\text{ét}}$ contains the closed subgroup $\pi^{-1}(\langle B \rangle) \simeq \mathbb{G}_m \times \mathbb{Z}/2$.

We now compute the essential dimension of $\widetilde{H}_{\text{ét}}$. Applying Proposition 1.4 we get $\mathrm{ed}_{k'}(\widetilde{H}_{\text{ét}}) \leq 2$. Moreover, since $\dim(\mathbb{G}_m \times \mathbb{Z}/2) = 1$ and $\mathrm{ed}_{k'}(\mathbb{G}_m \times \mathbb{Z}/2) = \mathrm{ed}_{k'}(\mathbb{Z}/2) = 1$, we get that $\mathrm{ed}_{k'}(\widetilde{H}_{\text{ét}}) \geq 1$ by Proposition 1.2.

We finally prove that $\mathrm{ed}_{k'}(\widetilde{H}_{\text{ét}}) \neq 1$. If $\mathrm{ed}_{k'}(\widetilde{H}_{\text{ét}}) = 1$ then, by [BeF, Proposition 6.21], the quotient $\widetilde{H}_{\text{ét}}/\widetilde{H}^0_{\text{ét}} = \widetilde{H}_{\text{ét}}/\mathbb{G}_m$ will be a subgroup of $\mathbf{PGL}_2$. This would show that $H_{\text{ét}}(\overline{k'})$ is, as an abstract group, isomorphic to a subgroup of $\mathbf{PGL}_2(\overline{k'})$. In particular, $\mathbf{PGL}_2(\overline{k'})$ would contain a subgroup isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$, which is not the case.

This proposition shows that cubics with prescribed j-invariant can be described with two parameters.

We are now able to finish the proof of Theorem 4.1 using Proposition 4.2. The idea is to show that the j-invariant can be choosen independently from the flex points. This is why we consider now the functor of cubics with a transcendental j-invariant.

Let t be an indeterminate over k, let $\overline{k(t)}$ be an algebraic closure of $k(t)$. Let i be the composite $k \to k(t) \to \overline{k(t)}$, where the first map is the natural inclusion, and $k(t) \to \overline{k(t)}$ is a fixed k-linear morphism which maps t to itself.
Let $\lambda \in \overline{k(t)}$ such that $j(C_\lambda) = t$ and consider the functor $\mathbf{F}_\lambda$ of Example 3.2. By Proposition 4.2 we have $\mathrm{ed}_{\overline{k(t)}}(\mathbf{F}_\lambda) = 2$. Thus there exists a field extension $L/\overline{k(t)}$ with $\mathrm{trdeg}(L : \overline{k(t)}) = 2$ and 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 $[C] \in \mathbf{Cub}_3^+(L/k)$ we have $\mathrm{ed}([C]) = 3$ over k.

Assume that there exists a subextension K'/k of L/k with $\mathrm{trdeg}(K' : k) \leq 2$ and $[C'] \in \mathbf{Cub}_3^+(K')$ such that $[C']_L = [C]$.

Since $[C] \in \mathbf{F}_\lambda(L/\overline{k(t)})$, we have $j(C'_L) = j(C) = j((C_\lambda)_L) =$ image of t 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 $k(t) \to K'$ sending t to $j(C')$.

Now the diagram of k-morphisms

$$\begin{array}{ccccc} & & L & & \\ & \nearrow & & \nwarrow & \\ \overline{k(t)} & & & & K' \\ & \nwarrow & & \nearrow & \\ & & k(t) & & \end{array}$$

clearly commutes and hence we can define the compositum E of $\overline{k(t)}$ and K' in L.

Take now the element $[C''] := [C']_E \in \mathbf{Cub}_3^+(E)$. Then clearly $[C'']_L = [C]$ and $[C''] \in \mathbf{F}_\lambda(E)$. But $\mathrm{trdeg}(K' : k) \leq 2$ and $\mathrm{trdeg}(k(t) : k) = 1$ so we have $\mathrm{trdeg}(K' : k(t)) \leq 1$. It follows that $\mathrm{trdeg}(E : \overline{k(t)}) \leq 1$. Consequently, $[C]$ is defined over a subextension of $L/\overline{k(t)}$ of transcendence degree at most 1 which is absurd.

We then get $\mathrm{ed}_k(\mathbf{Cub}_3^+) \geq \mathrm{ed}([C]) = 3$ and this concludes the proof of Theorem 4.1.

§5 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 $\mathrm{ed}(\mathbf{Cub}_3^-)$. That is the purpose of this section. In fact, we have the following result:

Theorem 5.1. *Let k be a field with $\mathrm{char}(k) \neq 2, 3$. Then*

$$\mathrm{ed}_k(\mathbf{Cub}_3^-) = 2.$$

Proof. We first recall the well-known list of the eight geometric types of singular cubics over a separably closed field, and a possible equation for each of them (see [Kr], Chapter I, §7 for example):

1) The triple line: $C_1 = X^3$,

2) The union of a double line and of a tranverse line: $C_2 = X^2Y$,

3) The union of three distincts concurrent lines: $C_3 = XY(X+Y)$,

4) The union of three non concurrent lines: $C_4 = XYZ$,

5) The union of a non-degenerate conic and of a line tangent to it: $C_5 = (Y^2 - XZ)Z$,

6) The union of a non-degenerate conic and of a transverse line: $C_6 = (X^2 - YZ)X$,

7) The cuspidal cubic: $C_7 = Y^2Z - X^3$,

8) The nodal cubic: $C_8 = Y^2Z - X^3 - X^2Z$.

Notice that in [Kr], the equation given for C_5 is not exactly the same, but the one given above is more convenient here. Since all these cubics are defined over k, any singular cubic defined over a field extension L/k is equivalent to one of the C_i's over L_s. Applying the Galois Descent Lemma shows that the equivalence 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 in most of cases the following method:

we compute first $\mathbf{Stab}(C_i)(L_s)$ for any field L containing k. 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.

1) The triple line C_1 in $\mathbb{P}^2(L_s)$ corresponds to the point $(1:0:0)$ in the dual space. Hence, any element of $\mathbf{PGL}_2(L_s)$ which stabilizes C_1 corresponds to an automorphism of the dual space which fixes this point. Dualizing again, we then obtain that $\mathbf{Stab}(C_1)$ coincide on the L_s-points with the group scheme G_1 defined by

$$G_1(R) = \left\{ \begin{pmatrix} a & 0 & 0 \\ b & c & d \\ e & f & g \end{pmatrix} \in \mathbf{GL}_3(R) \right\}$$

for any k-algebra R. Let also H_1 and K_1 be the group schemes defined respectively by

$$H_1(R) = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ b & 1 & 0 \\ e & 0 & 1 \end{pmatrix} \in \mathbf{GL}_3(R) \right\} \text{ and } K_1(R) = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & c & d \\ 0 & f & g \end{pmatrix} \in \mathbf{GL}_3(R) \right\}.$$

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 $\mathrm{ed}_k(G_1) = 0$.

2) Here the cubic C_2 corresponds in the dual space to the union of the double point $(1:0:0)$ and the simple point $(0:1:0)$. Since multiplicities have to be preserved, an automorphism of $\mathbb{P}^2(k_s)$ which stabilizes C_2 corresponds to an automorphism of the dual space which fixes these two points. After dualization, we then obtain that the stabilizer of C_2 (in $\mathbf{GL}_3$) coincides on the L-points with the group scheme G_2 defined by

$$G_2(R) = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ c & d & e \end{pmatrix} \in \mathbf{GL}_3(R) \right\}.$$

We then have

$$1 \longrightarrow \mathbb{G}_a \times \mathbb{G}_a \longrightarrow G_2 \longrightarrow \mathbb{G}_m \times \mathbb{G}_m \times \mathbb{G}_m \longrightarrow 1,$$

which gives again $H^1(\_, G_2) = 1$ and $\mathrm{ed}_k(G_2) = 0$.

3) It is easy to see that an element of $\mathbf{PGL}_3(L_s)$ stabilizing C_3 stabilizes the intersection point $(0:0:1)$ and induces an automorphism of the cubic curve $XY(X+Y)$ viewed in $\mathbb{P}^1(k_s)$. Then, by Example 3.0, one can take for G_3 the group scheme defined by

$$G_3(R)=\left\{\begin{pmatrix} a & b & 0\\ c & d & 0\\ e & g & h\end{pmatrix}\in \mathbf{GL}_3(R), \begin{pmatrix} a & b\\ c & d\end{pmatrix}\in \widetilde{S}_3(R)\right\}.$$

We then have

$$1 \longrightarrow \mathbb{G}_a\times\mathbb{G}_a \longrightarrow G_3 \xrightarrow{f} \mathbb{G}_m\times\widetilde{S}_3 \longrightarrow 1\ ,$$

where f is the obvious map.

Since this sequence is split, the map $f_*: H^1(L,G_3)\to H^1(L,\mathbb{G}_m\times\widetilde{S}_3)\simeq H^1(L,\widetilde{S}_3)$ 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 $C=(\mathbb{G}_m\times\widetilde{S}_3)(L_s)$. 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 [KMRT, Proposition 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 $H^1(L,A_\alpha)=H^1(L,(\mathbb{G}_a\times\mathbb{G}_a)_\alpha(L_s))=1$. Thus the fiber of $[\gamma]=f_*([\beta])$ is $\{[\beta]\}$, for any $[\beta]\in H^1(L,B)$, so f_* is injective.

Consequently, we get

$$H^1(\_,G_3)\simeq H^1(\_,\widetilde{S}_3)$$

which shows that $\mathrm{ed}_k(G_3)=\mathrm{ed}_k(\widetilde{S}_3)=1$.

4) Here C_4 corresponds in the dual space to the union of the points $(1:0:0),(0:1:0)$ and $(0:1:0)$. An element of $\mathbf{PGL}_3(L_s)$ which stabilizes C_4 corresponds to an automorphism of the dual space which permutes these 3 points. Hence, one can easily see an element of $\mathbf{Stab}(C_4)(L_s)$ as a product of a diagonal invertible matrix D and of an element of S_3 (where S_3 is viewed in $\mathbf{GL}_3(K_s)$ via the representation by permutation matrices). This gives an isomorphism $\mathbf{Stab}(C_4)(L_s)\simeq L_s^{\times 3}\ltimes S_3$.

Let $G_4=\mathbb{G}_m^3\ltimes S_3$ (where S_3 is considered as a constant group scheme here). The inclusion $G_4\subset\mathbf{GL}_3$ then gives rise to a linear action of G_4 on $\mathbb{A}_k^3$. Letting $\mathbb{G}_m^3$ act trivially on $\mathbb{A}_k^2$, the natural 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 1.3, we get $\mathrm{ed}_k(G_4)\leq 2$.

5) An element $f\in\mathbf{Stab}(C_5)(L_s)$ has to preserve the affine plane $Z=0$ and the quadric $q:=Y^2-XZ$. In particular f is a similitude of q. Since the image of f in $\mathbf{PGL}_3(L_s)$ has to fix the point of tangency $(1:0:0)$, it follows that f is an upper triangular matrix. Easy computations then show that $\mathbf{Stab}(C_5)(L_s)$ coincide on the L_s-points with the group scheme defined by

$$G_5(R)=\left\{\begin{pmatrix} \frac{u^2}{v} & \frac{2uw}{v} & \frac{w^2}{v}\\ 0 & u & w\\ 0 & 0 & v\end{pmatrix}\ \middle|\ u,v\in R^\times, w\in R\right\}.$$

Let H and K be the group schemes defined by

$$H(R) = \left\{ \begin{pmatrix} 1 & 2w & w^2 \\ 0 & 1 & w \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; w \in R \right\}, \text{ and } K(R) = \left\{ \begin{pmatrix} \frac{u^2}{v} & 0 & 0 \\ 0 & u & 0 \\ 0 & 0 & v \end{pmatrix} \;\middle|\; u, v \in R^{\times} \right\}.$$

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

$$1 \longrightarrow \mathbb{G}_a \longrightarrow G_5 \longrightarrow \mathbb{G}_m^2 \longrightarrow 1.$$

Applying Galois cohomology then shows that $H^1(\_, G_5) = 1$, so $\mathrm{ed}_k(G_5) = 0$.

6) An element $f \in \mathbf{Stab}(C_6)(L_s)$ has to preserve the hyperplane $\mathcal{H}$ of L_s^3 given by the equation $X = 0$ and the quadric $q := X^2 - YZ$. In particular, f is a similitude of q. It is easy to see that the decomposition $L_s^3 = \mathcal{H} \oplus Fe_1$ is orthogonal, so f preserves the line Fe_1 and $f' = f_{|\mathcal{H}}$ is a similitude of $q' = q_{|\mathcal{H}}$ (where e_1 denotes the first vector of the canonical basis of L_s^3). Easy computations show that if $f(e_1) = \lambda e_1$ then $\lambda^{-1} f'$ belongs to the orthogonal group $\mathbf{O}(q')(L_s)$, hence $\mathbf{Stab}(C_6)(L_s) = (\mathbb{G}_m \times \mathbf{O}(q'))(L_s)$.
Thus if one takes $G_6 = \mathbb{G}_m \times \mathbf{O}(q')$, one has $H^1(\_, \mathbf{Stab}(C_6)) = H^1(\_, G_6) \simeq H^1(\_, \mathbf{O}(q'))$. Hence we get $\mathrm{ed}_k(G_6) = \mathrm{ed}_k(\mathbf{O}(q')) = 2$ (see [BeF, Theorem 3.10] or [Re] for example).

7) and 8) One can easily check that $\pi(\mathbf{Stab}(C_i))$ for $i = 7, 8$ is an étale group scheme (showing that the Lie algebra is trivial). Then we get $\mathrm{ed}(\mathbf{Stab}(C_i)) \leq 2$ using Proposition 1.4.

This concludes the proof.

Theorem 5.1 proves also that $\mathrm{ed}_k(\mathbf{Cub}_3) = \mathrm{ed}_k(\mathbf{Cub}_3^+)$ and that $\mathrm{ed}(\mathbf{Cub}_3^-) < \mathrm{ed}_k(\mathbf{Cub}_3^+)$. As we have seen in a previous section it is also true for cubics in two variables.

It seems reasonable to expect that $\mathrm{ed}_k(\mathbf{F}_{d,n}) = \mathrm{ed}_k(\mathbf{F}_{d,n}^+)$ and $\mathrm{ed}(\mathbf{F}_{d,n}^-) < \mathrm{ed}(\mathbf{F}_{d,n}^+)$, since singular hypersurfaces are not "general enough" to maximize essential dimension. However, we are not able to prove it at this moment.

REFERENCES

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

[BK] E. Brieskorn, H. Knörrer, *Plane Algebraic Curves.* Birkhaüser Verlag, Basel, Boston, Stuttgart (1986)

[BR] J. Buhler, Z. Reichstein, *On the essential dimension of a finite group.* Comp. Math. **106** (1997), 159–179

[DeGa] M. Demazure, P. Gabriel, *Groupes algébriques, vol. 1,* Ed. Masson & Cie (1970)

[KMRT] M.-A. Knus, A. Merkurjev, M. Rost, J.-P. Tignol, *The book of involutions.* AMS Coll. Pub. **44** (1998)

[Kr] H. Kraft, *Geometrische Methoden in der Invarientheorie.* Aspects of Mathematics, D1. Friedr. Vieweg & Sohn, Braunschweig (1984)

[Me] A. Merkurjev, *Essential dimension.* Private notes (1999)

[Re] Z. Reichstein, *On the notion of essential dimension for algebraic groups.* Transformation Groups **5**, no. 3 (2000), 265–304

Grégory Berhuy
University of British Columbia
Department of Mathematics
1984 Mathematics road
Vancouver BC, V6T 1Z2 CANADA

Email: berhuy@math.ubc.ca

Giordano Favi
Institut de Mathématiques
Université de Lausanne
Dorigny
CH-1015 Lausanne SWITZERLAND

Email: giordano.favi@ima.unil.ch
giordano.favi@epfl.ch