ESSENTIAL DIMENSION OF CUBICS

Grégory Berhuy & Giordano Favi

March 2003

Abstract. In this paper, we compute the essential dimension of cubics in three variables, when the base field has characteristic different from 2 and 3 and contains a primitive third root of unity. For this, we use canonical pencils of cubics, Galois descent techniques, and the material introduced in[BeF].

§0 Introduction

Let C be a polynomial in n variables with coefficients somewhere, say in a ring or a field. A question one may ask is whether is it possible, by changing linearly the coordinates, to drop some of its coefficients or make it "nicer". For instance, the quadratic polynomial X^2+bX+c can always be brought 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 that in these cases 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. It turns out that this number is not always easy to compute. One has to carry out some tools in order to estimate it. The aim of this paper is to use techniques, previously developed in [BeF], for the computation of the essential dimension of homogenous cubic polynomials in three variables. 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 Fundation, grant No 2100-065128.01/1 (Project leader: E.Bayer-Fluckiger).

§1 Essential dimension of functors: some definition 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 $\mathbf{F} : \mathfrak{C}_k \longrightarrow \mathbf{Sets}$ as introduced in [BeF].

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 $\mathrm{ed}_k(G)$.

Let us recall some results proved in [BeF]:

For any field extension k'/k, any functor $\mathbf{F} : \mathfrak{C}_k \longrightarrow \mathbf{Sets}$ can be considered as an element of $\mathfrak{F}_{k'}$. We denote by $\mathrm{ed}_{k'}(\mathbf{F})$ its essential dimension. It is easily checked that the inequality $\mathrm{ed}_{k'}(\mathbf{F}) \leq \mathrm{ed}_k(\mathbf{F})$ 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.

We shall say that a morphism of functors $f : \mathbf{F} \longrightarrow \mathbf{F}'$ is a **surjection** if, for every L/k, the corresponding map of sets $f_L : \mathbf{F}(L) \longrightarrow \mathbf{F}'(L)$ is a surjection.

Lemma 1.1. *Let* $\mathbf{F} \twoheadrightarrow \mathbf{F}'$ *be a surjection between functors. Then* $\mathrm{ed}_k(\mathbf{F}) \geq \mathrm{ed}_k(\mathbf{F}')$*.*

Proof. See [BeF].

One case of special interest, though not used extensively in these notes, is when one of the functors is a scheme over k. Indeed take X a k-scheme of finite type. One can view it as a functor simply saying $X(L) = \mathrm{Hom}(\mathrm{Spec}(L), X)$ for L/k. Its essential dimension is easily computed as $\mathrm{ed}_k(X) = \dim(X)$. Now we shall say that X is a **classifying scheme** for a functor $\mathbf{F}$ if there is a surjection $X \twoheadrightarrow \mathbf{F}$. In this case the above lemma tells us that $\mathrm{ed}_k(\mathbf{F}) \leq \dim(X)$.

Here is a new result which happens to be very useful for our purpose.

Let $i : k \to k'$ an object of $\mathfrak{C}_k$. We will describe a construction which will give rise to a functor $i^* : \mathfrak{F}_{k'} \longrightarrow \mathfrak{F}_k$.
Let $\mathbf{F}$ be any functor on $\mathfrak{C}_{k'}$. For any object L/k of $\mathfrak{C}_k$ we set

$$(i^*\mathbf{F})(L/k) = \coprod_{\mathrm{Hom}_k(k',L)} \mathbf{F}(L/k').$$

This means, more precisely, that for every k-linear map $f : k'/k \to L/k$ (if there is any) we take a copy of the set $\mathbf{F}(L/k')$ where L is considered as an object of $\mathfrak{C}_{k'}$ via f. In other words elements of $(i^*\mathbf{F})(L/k)$ are elements of $\mathbf{F}(L/k)$ labelled by k-morphisms from k'/k to

L/k. We may write elements in $(i^*\mathbf{F})(L/k)$ as pairs (f,a) where $f : k' \to L$ is a morphism and $a \in \mathbf{F}(L/k')$. If now $\varphi : L/k \to L'/k$ is a morphism in $\mathfrak{C}_k$ we define

$$i^*\varphi : \coprod_{\mathrm{Hom}_k(k',L)} \mathbf{F}(L/k') \longrightarrow \coprod_{\mathrm{Hom}_k(k',L')} \mathbf{F}(L'/k')$$

to be the map which sends an element $a \in \mathbf{F}(L/k')$ (labelled by the morphism $f : k'/k \to L/k$) to the element $\mathbf{F}(\varphi)(a)(L'/L/k')$ (labelled by the morphism $\varphi \circ f : k'/k \to L/k$). That is the pair (f,a) goes to $(\varphi \circ f, a_{L'})$. The functoriality is left to the reader.

Take now the representable functor $\mathbf{h}_i : \mathfrak{C}_k \longrightarrow \mathbf{Sets}$ defined by $\mathbf{h}_i(K/k) = \mathrm{Hom}_k(k'/k, K/k)$. One easily checks that $i^*(\mathbf{1}) = \mathbf{h}_i$ where $\mathbf{1}$ denotes the one-point functor over $\mathfrak{C}_{k'}$ sending each object to a one-point set. Moreover one computes that $\mathrm{ed}_k(\mathbf{h}_i) = \mathrm{trdeg}(k' : k)$. The following lemma generalizes this fact.

Lemma 1.2. *Let $i : k \to k'$ be any morphism and $\mathbf{F}$ be an object of $\mathfrak{F}_{k'}$. Then*

$$\mathrm{ed}_k(i^*\mathbf{F}) = \mathrm{ed}_{k'}(\mathbf{F}) + \mathrm{trdeg}(k' : k).$$

Proof. Take an element $(f,a) \in i^*\mathbf{F}(L/k)$ for some extension L/k where $f : k'/k \to L/k$ and $a \in \mathbf{F}(L/k')$. Take now $a' \in \mathbf{F}(L'/k')$ for some $f' = L'/k'$ and some k'-morphism $L' \to L$ such that $a'_L = a$, where $\mathrm{trdeg}(L'/k')$ is minimal. The element (f,a) now comes from the element $(f',a') \in i^*\mathbf{F}(L'/k'/k)$. It follows that

$$\mathrm{ed}(f,a) \leq \mathrm{trdeg}(L' : k) = \mathrm{trdeg}(L' : k') + \mathrm{trdeg}(k' : k) \leq \mathrm{ed}_{k'}(\mathbf{F}) + \mathrm{trdeg}(k' : k).$$

Consequently $\mathrm{ed}_k(i^*\mathbf{F}) \leq \mathrm{ed}_{k'}(\mathbf{F}) + \mathrm{trdeg}(k' : k)$.
For the reverse inequality take $a \in \mathbf{F}(L/k')$ for some extension L/k'. This defines an element $(f,a) \in i^*\mathbf{F}(L/k'/k)$ where f denotes the extension L/k'. Take an extension L'/k, a k-morphism $\varphi : L' \to L$ and an element $(f',a') \in i^*\mathbf{F}(L'/k)$ such that $(f',a')_L = (f,a)$, where $\mathrm{trdeg}(L'/k)$ is minimal. This means that $\varphi \circ f' = f$ hence $\varphi : L'/k' \to L/k'$ is k'-linear. Consequently a is defined over L'/k' and we have

$$\mathrm{ed}(a) \leq \mathrm{trdeg}(L' : k') = \mathrm{trdeg}(L' : k) - \mathrm{trdeg}(k' : k) \leq \mathrm{ed}_k(i^*\mathbf{F}) - \mathrm{trdeg}(k' : k).$$

It follows that $\mathrm{ed}_k(\mathbf{F}) \leq \mathrm{ed}_k(i^*\mathbf{F}) - \mathrm{trdeg}(k' : k)$.

Remark. The previous things are almost trivial. The only real problem is notation. It is an (tedious) exercice left to the reader to show that $i^* : \mathfrak{F}_{k'} \to \mathfrak{F}_k$ is a functor. One could go a step further and prove that the association $k \mapsto \mathfrak{F}_k$ is functorial. We will not use such things and leave it to the courageous reader.

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 1.1. *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 [BeF].

Proposition 1.2. *Let G be an algebraic group over k acting linearly on an affine space $\mathbb{A}(V)$. Assume that there exists a non-empty G-stable open subset U of $\mathbb{A}(V)$ such that:*

1) the quotient U/G exists

2) for every L/k the stabilizer of each element of $U(L_s)$ under $G(L_s)$ is trivial.

Then U/G is a classifying scheme for $H^1(\_, G)$. In particular, we have

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

Proof. See [BeF].

We now give an application of this last proposition which we will use later.

Proposition 1.3. *Let G be a finite constant closed 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 find an open subset of $\mathbb{A}^n$ for which the hypotheses of Proposition 1.2 are fulfilled. Notice first that the quotient $U/\widetilde{G}$ exists when one takes $U = \mathbb{A}^n \setminus \{0\}$. Indeed it is easily seen that this quotient is the same as the quotient of $\mathbb{P}^{n-1}$ by the finite group G. So we only have to worry about the condition of stabilizers. Actually one only has to cut out of $\mathbb{A}^n$ a *bad* closed set those points have non trivial stabilizer. We will now go into all the details.

By definition $\widetilde{G}(K) = \pi_K^{-1}(G(K))$ for any field extension K/k and $\dim \widetilde{G} = 1$. Moreover, the map π_K induces a group isomorphism $\widetilde{G}(K)/K^\times \simeq G(K)$. For any element of $G(k)$, choose a preimage in $\widetilde{G}(k)$. We choose I_n for the preimage of $\overline{I}_n$. Denote by S the set of these preimages. Since G is a constant group scheme we have $G(K) = G(k) = G$ for all field extension K/k. Hence the previous isomorphism shows that

$$\widetilde{G}(K) = \{\mu g \mid \mu \in K^\times, g \in S\}.$$

Take $g \in S - \{I_n\}$ and write it $g = (m_{ij})$. Let I_g be the ideal of $k[X_1, \dots, X_n]$ generated by the polynomials

$$X_i\Big(\sum_j m_{1j}X_j\Big) - X_1\Big(\sum_j m_{ij}X_j\Big) \qquad i = 1, \dots, n.$$

Let $F = \bigcup \mathrm{V}(I_g)$. This is a closed subset of $\mathbb{A}^n$ since $S - \{I_n\}$ is finite. Notice that, by construction, $F(K) = \{v \in K^n \mid \text{there exists } g \in S - \{I_n\} \text{ and } \lambda \in K \text{ such that } gv = \lambda v\}$.
Let $U = \mathbb{A}^n \setminus F$. This is a dense open subset of $\mathbb{A}^n$ which does not contain 0.

We first show that $U(L_s)$ is $\widetilde{G}(L_s)$-stable for every L/k.

Let $v \in U(L_s)$, and $\mu g \in \widetilde{G}(L_s)$. Assume that $(\mu g)v \notin U(L_s)$, that is $(\mu g)v \in F(L_s)$. Then there exists $\lambda \in L_s$ and $g' \in S - \{I_n\}$, such that $g'(\mu g v) = \lambda(\mu g v)$. Since $\widetilde{G}(K)$ acts linearly on K^n and $\mu \neq 0$, we get $g' g v = \lambda g v$, hence $(g^{-1}g'g)v = \lambda v$. Let $g'' \in S$ which represents $\pi_k(g^{-1}g'g)$. Then there exists $\gamma \in k^\times$ such that $g^{-1}g'g = \gamma g''$. Then $g''v = \gamma^{-1}\lambda v$. Since $v \in U(L_s)$, this implies that $g'' = I_n$, so $\pi_k(g^{-1}g'g) = \overline{I}_n$. Then we get $\pi_k(g') = \overline{I}_n$. By construction of S, this implies that $g' = I_n$, which is a contradiction.

We now check that the stabilizer of any element of $U(L_s)$ is trivial.

Let $v \in U(L_s)$, and let $\mu g \in \widetilde{G}(L_s)$ such that $\mu g v = v$. We then have $gv = \mu^{-1} v$, hence $g = I_n$ by hypothesis on v. Since $v \in U(L_s)$, we have $v \neq 0$, hence $\mu = 1$. This implies that $\mu g = I_n$.

Thus the action of $\widetilde{G}$ on $\mathbb{A}^n_k$ satisfy the conditions of Proposition 1.2. Hence

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

§2 Degree d curves and specialization

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 curves in n variables**. We will often use the same notation for a curve and for one polynomial which defines it. We also will have to consider non-singular curves in the sequel. Let's denote by $\mathbf{C}^+_{d,n}$ the functor of non-singular degree d curves in n variables.

We want to discuss the following general question. Take C a degree d curve 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 coordinates some of these coefficients may drop or become equal. Hence we would like to know how many parameters are needed to describe the curve 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 coordinates. More precisely, if $C \in \mathbf{C}_{d,n}(L)$ and $\varphi \in \mathrm{GL}_n(L)$, define $\varphi(C)$ to be the curve defined by $C \circ \varphi$. Since scalar matrices do nothing on curves this action induces an action of $\mathbf{PGL}_n$ on $\mathbf{C}_{d,n}$.

We denote by $\mathbf{F}_{d,n}$ the functor of curves 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 $\mathbf{C}^+_{d,n}$. We then denote by $\mathbf{F}^+_{d,n}$ the functor $\mathbf{C}^+_{d,n}/\mathbf{GL}_n$. These are exactely 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 curve up to change of coordinates. In other words we would like to compute its essential dimension.

At this point there is a useful remark to be made. In order to compute the essential dimension of $\mathbf{F}_{d,n}$ one sees that it is sufficient to minimize the number of parameters appearing in the most general polynomial, that is $C_0 = \sum t_I X^I$ where the t_I's are algebraically independent variables over k. This C_0 is called the **generic polynomial** of degree d in n variables. We will show in the detail that $\mathrm{ed}(\mathbf{F}_{d,n}) = \mathrm{ed}([C_0]) = \mathrm{ed}(\mathbf{F}^+_{d,n})$. In the sequel we will often use this fact.

So let $C_0 = \sum t_I X^I$ be the generic homogeneous polynomial of degree d in n variables, where the t_I's are independent indeterminates over k (with obvious notation). Set $\mathbf{t} = (t_I)$ and $K_0 = k(\mathbf{t})$.

We begin by a technical lemma, which says in particular that the generic cubic $[C_0]$ can be specialized in almost any cubic $[C]$.

Technical Lemma. *Let $P \in k[\mathbf{t}]$. Let $\varphi \in \mathbf{GL}_n(K_0)$, L/k be a field extension and C be a homogeneous polynomial of degree d in n variables with coefficients in L. If L is infinite, there exists $\psi \in \mathbf{GL}_n(L)$ and a specialization $\mathbf{t} \to \mathbf{b} = (b_I)$ such that:*

1) $\varphi(\mathbf{b})$ is well-defined and $\varphi(\mathbf{b}) \in \mathbf{GL}_n(L)$,

2) $P(\mathbf{b}) \neq 0$,

3) $C_0(\mathbf{b}) \circ \varphi(\mathbf{b}) = C \circ \psi \circ \varphi(\mathbf{b})$.

Proof. Write $\varphi = (\varphi_{ij}(\mathbf{t})) = \left(\frac{P_{ij}(\mathbf{t})}{Q_{ij}(\mathbf{t})}\right)$ and $C_0 \circ \varphi = \sum_I F_I(\mathbf{t}) X^I$.

Clearly there exists some polynomials with coefficients in K_0 in n^2 variables T_{ij}, say $R_I(T_{ij}, \mathbf{t})$, such that $F_I(\mathbf{t}) = R_I(\varphi_{ij}(\mathbf{t}), \mathbf{t})$. In particular, the set of poles of these F_I's is contained is the set of zeros of the Q_{ij}'s. Hence $F_I(\mathbf{b})$ is well-defined if $Q_{ij}(\mathbf{b}) \neq 0$ for all i, j. Set $\det \varphi = \frac{D_1(\mathbf{t})}{D_2(\mathbf{t})}$. The set of poles of $\det \varphi$ is contained in the set of zeros of the Q_{ij}'s, so $\varphi(\mathbf{b})$ is well-defined and invertible if $D_1(\mathbf{b}) \neq 0$ and $Q_{ij}(\mathbf{b}) \neq 0$ for all i, j.

Let $\psi = (\psi_{ij}) \in M_n(L)$, where ψ_{ij} have to be determined, and write $C \circ \psi = \sum b_I X^I$.
Clearly $C \circ \psi \circ \varphi = \sum R_I(\varphi_{ij}(\mathbf{t}), \mathbf{b}) X^I$. Since the b_I's are polynomials in ψ_{ij} (and in coefficients of C), we can write $b_I = S_I(\psi_{ij})$ for some polynomials $S_I(T_{ij}) \in L[T_{ij}]$.
Set $\mathbf{S} = (S_I)$ and let $U(T_{ij})$ be the product of the polynomials $Q_{ij}(\mathbf{S}), D_1(\mathbf{S}), P(\mathbf{S})$ and $\det(T_{ij})$. The polynomial U with coefficients in L is non zero, hence there exist an element $(\psi_{11}, \cdots, \psi_{nn})$ of L^{n^2} such that $U(\psi_{ij}) \neq 0$, since L is infinite. The specialization $t_I \mapsto b_I = S_I(\psi_{ij})$ then satisfies the required conditions.

Definition 2.1. *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 depends on the choice of C.*

Corollary 2.1. *Using the above notation the following holds:*

1) The class of the cubic $[C_0]$ is anisotropic, hence non singular.

2) One has $\mathrm{ed}_k(\mathbf{F}_{d,n}) = \mathrm{ed}_k([C_0])$ and $\mathrm{ed}_k(\mathbf{F}^+_{d,n}) = \mathrm{ed}^+_k([C_0])$, where $\mathrm{ed}^+_k([C_0])$ denotes the essential dimension of $[C_0]$ viewed as an element of $\mathbf{F}^+_{d,n}$.

Proof. 1) Assume that $[C_0]$ is isotropic, and let $(P_1(\mathbf{t}), \cdots, P_n(\mathbf{t}))$ be a nontrivial solution of the equation $C_0 = 0$. Let P the product of all P_i's which are non zero, let $L = k(s_1, \cdots, s_n)$, where the s_i's are independent indeterminates over k and let $C = s_1 X_1^d + \cdots + s_n X_n^d$. By the Technical Lemma, there is a specialization of the t_I's such that $[C_0]$ maps to $[C]$, and such that the specialization of P is non zero. Consequently, the non zero P_i's map to non zero elements of L and $[C]$ is then isotropic over L. This is not the case, by [Re], Theorem 3.2, hence we get a contradiction.

2) We only show the first equality. The proof of the second one is similar. The inequality $\mathrm{ed}([C_0]) \leq \mathrm{ed}_k(\mathbf{F}_{d,n})$ follows from the definition. Let L/k be a field extension, and take $[C] \in \mathbf{F}_{d,n}(L)$. We have to show that $\mathrm{ed}([C]) \leq \mathrm{ed}([C_0])$.
If L is finite, then L/k is algebraic, hence $\mathrm{ed}([C]) = 0 \leq \mathrm{ed}([C_0])$.
Now assume that L is infinite. Let $K \subset K_0$ be a field extension such that $[C_0] = [C'_0]_{K_0}$ for some $[C'_0] \in \mathbf{F}_{d,n}(K)$ with $\mathrm{trdeg}(K : k) = \mathrm{ed}([C_0])$. By definition, there exists $\lambda \in K_0^\times$ and

$\varphi \in \mathbf{GL}_n(K_0)$ such that $\lambda C_0 \circ \varphi = C_0'$. Write $C_0' = \sum F_I(\mathbf{t}) X^I$. Notice that C_0' is defined over $k(F_I(\mathbf{t}))$. By minimality of the transcendence degree of K, we have

$$\mathrm{ed}_k([C_0]) = \mathrm{trdeg}(K:k) = \mathrm{trdeg}(k(F_I(\mathbf{t})):k).$$

Write $\lambda = \frac{P_1}{P_2}$. By the Technical Lemma, there exists a specialization $\mathbf{t} \to \mathbf{b}$ such that $C_0 \circ \varphi$ maps to to a polynomial C' equivalent to C and $P_1 P_2$ maps to a non zero element of L. It follows that λ maps to a non zero element μ of L, hence C_0' maps to $\mu C'$. In particular, $\mu C' = \sum F(\mathbf{b}) X^I$, so $[\mu C'] = [C]$ is defined over $k(F_I(\mathbf{b}))$. Since

$$\mathrm{ed}([C]) \leq \mathrm{trdeg}(k(F_I(\mathbf{b})):k) \leq \mathrm{trdeg}(k(F_I(\mathbf{t})):k) = \mathrm{ed}([C_0])$$

we then get the result.

Corollary 2.2. *We have* $\mathrm{ed}_k(\mathbf{F}_{d,n}) = \mathrm{ed}_k(\mathbf{F}^+_{d,n})$.

Proof. This follows from part 2) of the above corollary and the easy fact (left to the reader) that the essential dimension of C_0 in $\mathbf{F}_{d,n}$ is the same that its essential dimension in $\mathbf{F}^+_{d,n}$.

§3 Some considerations on cubics

0. Warm-up

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. $\mathbf{F}^+_{d,n}$) is simply denoted by $\mathbf{Cub}_n$ (resp. by $\mathbf{Cub}^+_n$).

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

Proposition 3.1. *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_0 be the generic cubic polynomial in 2 variables. Write $C_0 = t_1 X^3 + t_2 X^2 Y + t_3 XY^2 + t_4 Y^3$
We have to show that, up to a linear change of coordinates and to a scalar, C_0 is defined over an extension of k of transcendence degree at most 1.

Since $t_1 \neq 0$ one can divide by t_1 and obtain $X^3 + s_2 X^2 Y + s_3 XY^2 + s_4 Y^3$ where $s_i = \frac{t_i}{t_1}$.
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 some $u, v \in k(s_2, s_3, s_4)$ which are easily computed to be non zero. Let now $\varphi' = \begin{pmatrix} \frac{v}{u} & 0 \\ 0 & 1 \end{pmatrix}$. 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 $\mathrm{ed}_k(\mathbf{Cub}_2) \geq 1$. 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 $\mathrm{ed}([C]) = 0$. This means that $[C]$ is defined over k, since $k(t)/k$ is purely transcendental. Hence there exists

$\lambda \in k(t)^\times, \varphi \in \mathrm{GL}(k(t))$ 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 $\mathrm{ed}_k(\mathbf{Cub}_2) \geq \mathrm{ed}([C]) = 1$. This concludes the proof of the statement.

1. 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 $C_\lambda = X_1^3 + X_2^3 + X_3^3 - 3\lambda X_1X_2X_3$. 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 3rd 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 [BK].

The Hessian group G_{216} is 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 $\mathrm{SL}_2(\mathbb{F}_3)$. One can view this group as a subgroup of $\mathrm{PGL}_3(k_s)$ as follows:

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

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

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

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

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 $\overline{M}_g \in \mathrm{PGL}_3(k_s)$ 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 G_{216} 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 $B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$, has order 2.

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

When talking about cubics in three variables it's hard not to mention the so called j**-invariant**. For our purpose we will need only few things about it. First of all we have to know that it exists. That is for a non-singular cubic $C = \sum_{i_1+i_2+i_3=3} a_{i_1,i_2,i_3} X_1^{i_1} X^{i_2} X_3^{i_3}$ with coefficients in a field K there is a rational expression of the coefficients, denoted by $j(C)$, which lies in the ground field K and which does not depend on the class of the cubic. 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 [BK] p.301-302).

We now recall some results proved in [BK], p.292-298:

Lemma 3.1. *Assume that $k = k_s$. Then:*

1) *Every non-singular cubic C can be mapped 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 $\overline{\varphi} \in \mathrm{PGL}_3(k)$, $\overline{\varphi}$ maps C_λ to some C_μ if and only if $\overline{\varphi} \in G_{216}$.*

3) *Let $\lambda \in k \cup \{\infty\}$. For any $\overline{\varphi} \in \mathrm{PGL}_3(k)$, $\overline{\varphi}$ maps the cubic C_λ to itself if and only if $\overline{\varphi}$ belongs to the subgroup $H = \langle \overline{A}, \overline{B}, \overline{C} \rangle$.*

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 mentionned without proof, but can be obtained by easy computation. Notice that in the two last statements, C_λ is not supposed to be non-singular.

2. Canonical pencils of cubics

If C is a cubic polynomial in 3 variables with coefficients in L, let $H_C = \det\left(\frac{\partial^2 C}{\partial X_i \partial X_j}\right)$, and let $\mathcal{F}_C$ be the set of cubics of the form $\alpha C + \beta H_C$, for some $\alpha, \beta \in L$. 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 a cubic C over a field L and 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 $\mathbf{C}_{3,3} \twoheadrightarrow \mathfrak{P}$. Let now act the group $\mathbf{GL}_3$ naturally on $\mathfrak{P}$ as follows: for $\varphi \in \mathrm{GL}_3(L)$ and $C \in \mathbf{C}_{3,3}(L)$ we set $\varphi(\mathcal{F}_C) = \mathcal{F}_{\varphi(C)}$.

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.

Lemma 3.2. *Let C be a cubic in three variables with coefficients in L. Then sending the class of C to the class of its pencil $\mathcal{F}_C$ induces a well defined morphism of functors $\mathbf{Cub}_3 \longrightarrow \mathbf{Pen}_3$.*

Proof. The statement follows from the formula $H_{C\circ\varphi} = (\det\varphi)^2 H_C \circ \varphi$. The proof of this formula is left to the reader.

Lemma 3.1 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 3.3. *Assume that $\mathrm{char} k \neq 2, 3$ and let L/k be a field extension. For any $\lambda \in L, \lambda^3 \neq 1$, we have*

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

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

Proof. It is easy to see 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

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

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 $72(1-\lambda^3) = 1$. Since $\mathrm{char}(k) \neq 2, 3$, this implies that $\lambda^3 \neq 1$, 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 3.1. 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 of non-singular cubics.

We will denote by $\mathfrak{P}^+$ and $\mathbf{Pen}_3^+$ the corresponding functors. This little restriction does not matter for the computation of essential dimension for we have seen that $\mathrm{ed}(\mathbf{Cub}_3) = \mathrm{ed}(\mathbf{Cub}_3^+)$.

Lemma 3.4. *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 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, 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 $n + 1$.

§4 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 $\mathbf{F}$ 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-valuated functor and $\rho : G \longrightarrow \mathrm{Aut}(\mathbf{F})$ be a morphism of group-valuated functors which is Γ-equivariant. For each E/k we define an equivalence relation on $F(E)$ saying that $b, b' \in F(E)$ 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 valuated 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:

Galois Descent Lemma. *Let $\rho : G \longrightarrow \mathrm{Aut}(\mathbf{F})$ as above. Assume that for any $L \in \mathfrak{C}_k$, the following conditions hold:*
1) $H^1(L, G(L_s)) = 1$
2) $\mathbf{F}(L_s)^{\Gamma_L} = \mathbf{F}(L)$ and $G(L_s)^{\Gamma_L} = G(L)$.
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' 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 $X(L)$. 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 4.1. Assume that 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 3.3 tells us that $\mathbf{F}_a(L) = \mathbf{Pen}_3^+(L)$ for any extension L/k.

We now determine the stabilizer of the pencil $\mathcal{F}_{C_\lambda}$. Notice that the functors $\mathbf{Cub}_3, \mathbf{Cub}_3^+, \mathbf{Pen}_3$ and $\mathbf{Pen}_3^+$ can be naturally extended to k-algebras. The functor $\mathbf{Stab}_G(a)$ is then the stabilizer of a point of the Grassmanian, hence is a representable functor. This shows that $\mathbf{Stab}_G(a)$ is an algebraic group scheme defined over k.

We first compute the image of this group scheme by the natural projection $\pi : \mathbf{GL}_3 \to \mathbf{PGL}_3$. We have $\pi(\mathbf{Stab}_G(a))(k_s) = \{\overline{\varphi} \in \mathbf{PGL}_3(k_s) \mid \varphi(\mathcal{F}_{C_\lambda}) = \mathcal{F}_{C_\lambda}\}$.

Since over k_s the pencil $\mathcal{F}_{C_\lambda}$ is equal to $\{C_\mu \mid \mu \in k_s \cup \{\infty\}\}$ it follows that any φ in $\mathbf{Stab}_G(a)(k_s)$ maps C_λ to some C_μ. So the same holds for $\overline{\varphi}$ and hence $\overline{\varphi}$ belongs to $G_{216} \subseteq \mathrm{PGL}_3(k(\varepsilon))$ by Lemma 3.1. Conversely, if $\overline{\varphi} \in G_{216}$, then it is clear that $\overline{\varphi} \in \pi(\mathbf{Stab}_G(a))(k_s)$ by Lemma 3.1 again. Hence $\pi(\mathbf{Stab}_G(a))(k_s) = G_{216}$. Since Γ_k acts continuously on G_{216}, the group $\pi(\mathbf{Stab}_G(a))$ is then the étale group scheme $G_{216,\text{ét}}$ (see [BOI], Proposition 20.16). Thus

$$\mathbf{Stab}_G(\mathcal{F}_{C_\lambda}) = \pi^{-1}(G_{216,\text{ét}}).$$

We denote this last group by $\widetilde{G}_{216}$. Since the hypotheses of the Galois Descent Lemma are clearly fulfilled, we get

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

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

Example 4.2. Assume that char$k \neq 3$. 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 $\lambda \in k'$ with $\lambda^3 \neq 1$. Then $\mathbf{F}_a(L)$ is the set of cubics in L which are equivalent to C_λ over L_s. Arguing as previously, one can see that $\mathbf{Stab}_G(a)$ is the algebraic group k'-scheme $\pi^{-1}(H_{\text{ét}})$, where H is the subgroup of G_{216} described in Lemma 3.1. We will denote it by $\widetilde{H}$. Hence, for any field extension k'/k, for any $\lambda \in k', \lambda^3 \neq 1$, and for any field extension L/k', we have a one-to-one correspondence

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

Hence $\mathrm{ed}_{k'}(\mathbf{F}_a) = \mathrm{ed}_{k'}(\widetilde{H})$. Again we have classified cubics which become isomorphic to a fixed cubic by a Galois cohomology set.

§5 Essential dimension of cubics

We can finally state and prove our main result:

Theorem 5.1. *Let k be a field. Assume that* $\mathrm{char}(k) \neq 2, 3$. *If k contains ε, then*

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

In particular, $\mathrm{ed}_k(\mathbf{Cub}_3) \geq 3$ *for any field k.*

This section is devoted to the proof of the statement. We will prove the first part of the statement, the second one will follow from the fact that $\mathrm{ed}_{k(\varepsilon)}(\mathbf{F}) \leq \mathrm{ed}_k(\mathbf{F})$. We will restrict ourselves to the functor $\mathbf{Cub}_3^+$ since we know by §2 that $\mathrm{ed}(\mathbf{Cub}_3) = \mathrm{ed}(\mathbf{Cub}_3^+)$.

By Example 4.1, we have $\mathrm{ed}_k(\mathbf{Pen}_3^+) = \mathrm{ed}_k(\widetilde{G}_{216})$. Since $\varepsilon \in k$, the group Γ_k acts trivially on $G_{216,\text{ét}}(k_s)$, hence $G_{216,\text{ét}}$ is the constant algebraic group G_{216}. Applying Proposition 1.3 with $G = G_{216}$ and $n = 3$ then gives $\mathrm{ed}_k(\widetilde{G}_{216}) \leq 2$. Lemma 3.4 implies in particular that $\mathrm{ed}_k(\mathbf{Cub}_3^+) \leq \mathrm{ed}_k(\mathbf{Pen}_3^+) + 1$, hence $\mathrm{ed}_k(\mathbf{Cub}_3^+) \leq 3$. Notice that $\widetilde{G}_{216}$ contains the constant subgroup $(\mathbb{Z}/3Z)^3$ generated by $\varepsilon I_3, C$ and D, so using Proposition 1.1, we get $\mathrm{ed}_k(\widetilde{G}_{216}) = \mathrm{ed}_k(\mathbf{Pen}_3^+) = 2$.

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

Let k'/k be a field extension and $\lambda \in k'$ with $\lambda^3 \neq 1$. We define an object $\mathbf{F}_\lambda$ of $\mathfrak{F}_{k'}$ as follows. If L/k' is a field extension, set

$$\mathbf{F}_\lambda(L/k') = \{[C'] \in \mathbf{Cub}_3^+(L) \mid \text{there exists } E/L \text{ such that } C' \sim_E C_\lambda\}.$$

Notice that $\mathbf{F}_\lambda(L/k') = \{[C'] \in \mathbf{Cub}_3^+(L) \mid C' \sim_{L_s} C_\lambda\}$. Indeed, let $[C'] \in \mathbf{Cub}_3^+(L)$ such that $C' \sim_E C_\lambda$, for some E/L. We then have $j(C'_E) = j(C_{\lambda E})$, hence $j([C']) = j(C_{\lambda L})$. Thus $j(C'_{L_s}) = j(C_{\lambda L_s})$, so $C' \sim_{L_s} C_\lambda$. The reverse inclusion is clear. Example 4.2 then shows that $\mathbf{F}_\lambda \simeq H^1(\_, \widetilde{H})$ and thus

$$\mathrm{ed}_{k'}(\mathbf{F}_\lambda) = \mathrm{ed}_{k'}(\widetilde{H}).$$

This means in particular that the essential dimension of $\mathbf{F}_\lambda$ does not depend on λ.

Our next task is to compute the essential dimension of $\mathbf{F}_\lambda$, that is the essential dimension of $\widetilde{H}$. Precisely, we will show the following result:

Proposition 5.1. *Let k' be a field of characteristic different from 2 and 3 containing μ_3. Then* $\mathrm{ed}_{k'}(\widetilde{H}) = 2$.

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 $\widetilde{S} = \pi^{-1}(S)$.
Clearly, we have the following exact sequence of group schemes:

$$1 \longrightarrow \mathbb{G}_{\mathrm{m}} \longrightarrow \widetilde{S} \longrightarrow S \longrightarrow 1,$$

hence $\dim(\widetilde{S}) = 1$. Similarly, we have $\dim(\widetilde{H}) = 1$. Applying Proposition 1.3 we get $\mathrm{ed}_{k'}(\widetilde{H}) \leq 2$. We now prove the reverse inequality.

By Proposition 1.1. we have $\mathrm{ed}_{k'}(\widetilde{H}) \geq \mathrm{ed}_{k'}(\widetilde{S})$. Since $\mu_3 \in k' \subseteq L$, 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

$$1 \longrightarrow \mathbb{G}_{\mathrm{m}} \longrightarrow \widetilde{S} \longrightarrow \mu_3 \times \mu_3 \longrightarrow 1,$$

where the second map is given by

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

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

$$H^1(L, \widetilde{S}) \longrightarrow H^1(L, \mu_3) \times H^1(L, \mu_3) \longrightarrow H^2(L, \mathbb{G}_{\mathrm{m}}).$$

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 $c_a : \Gamma_L \to \mu_3$ 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 correponding cocycle.

Lemma 5.1. *For any field L, the connecting map*

$$\partial : H^1(L, \mu_3) \times H^1(L, \mu_3) \to H^2(L, \mathbb{G}_{\mathrm{m}})$$

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

Proof. Let $(a)_3, (b)_3 \in H^1(L, \mu_3)$. Let $a, b \in L^\times$. If $\sigma \in \Gamma_L$, write $c_a(\sigma) = \varepsilon^{m_\sigma}$ and $c_b(\sigma) = \varepsilon^{n_\sigma}$ for some $m_\sigma, n_\sigma \in \{0, 1, 2\}$. Since Γ_L acts trivially on $\mu_3 \times \mu_3$, the element $\partial((a)_3, (b)_3)$ is the class of the 2-cocycle

$$\alpha : \sigma, \tau \in \Gamma_L \times \Gamma_L \mapsto \beta_\sigma \sigma\beta_\tau \beta_{\sigma\tau}^{-1},$$

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 $\alpha_{\sigma,\tau} = A^{m_\sigma} C^{n_\sigma} A^{m_\tau} C^{n_\tau} C^{-n_{\sigma\tau}} A^{-m_{\sigma\tau}}$. Since $CA = \varepsilon AC$, we get

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

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

$$\alpha : (\sigma, \tau) \in \Gamma_L \times \Gamma_L \mapsto \varepsilon^{m_\sigma n_\tau} \in \mu_3(L),$$

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

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

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

for any field extension L/k'. Hence, by Lemma 1.1 we get

$$\mathrm{ed}_{k'}(\widetilde{S}) \geq \mathrm{ed}_{k'}(\mathbf{N}).$$

To conclude the proof of Proposition 5.1, it suffices to prove the following:

Lemma 5.2. *We have* $\mathrm{ed}_{k'}(\mathbf{N}) \geq 2$.

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'. Let's 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 $\mathbf{N} \longrightarrow \mathbf{Cub}_4$. 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 inderminates over k', and set $b = t, a = 1 + ts^3 + t^2u^3 - 3stu$. Set $L = k'(s, t, u)$. Then $a = N_{L(\beta)/L}(1 + s\beta + u\beta^2)$, 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.

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

Lemma 5.3. *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 $P_1, \cdots, P_4 \in k'[s, t, u]$ not all zero, such that $P_1^3 + aP_2^3 + bP_3^3 + abP_4^3 = 0$. Consider $P_1, \cdots, P_4$ 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 $t = \dfrac{3su - s^3 \pm \sqrt{\Delta}}{2u^3}$. Then, 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 that S is 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, one can assume that $R_3 = 1$.

We then have the equations

$$64u^3 = (R_1^2 - R_2^2\Delta)^3, 4 = R_2^3\Delta + 3R_1^2R_2, 12su - 4s^3 = R_1^3 + 3R_1R2^2\Delta.$$

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 has same degree in u. This gives a contradiction since these degrees don't have the same parity.

We are now able to finish the proof of Theorem 5.1 using Proposition 5.1 and Lemma 1.2.

Let t be an indeterminate over k, let $\overline{k(t)}$ be an algebraic closure of $k(t)$. Let i be the composite $k \to k(t) \to \overline{k(t)}$, 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. In the sequel we set $k' = \overline{k(t)}$. Let $\lambda \in k'$ such that $j(C_\lambda) = t$ and consider the functor $\mathbf{F}_\lambda$. By Lemma 1.2, we have

$$\mathrm{ed}_k(i^*\mathbf{F}_\lambda) = \mathrm{ed}_{k'}(\mathbf{F}_\lambda) + \mathrm{trdeg}(k' : k).$$

By Proposition 5.1, we have $\mathrm{ed}_{k'}(\mathbf{F}_\lambda) = 2$. Moreover we have $\mathrm{trdeg}(k' : k) = 1$, so we get

$$\mathrm{ed}_k(i^*\mathbf{F}_\lambda) = 3.$$

Thus there exists a field extension L/k with $\mathrm{trdeg}(L : k) = 3$ and and an element $x = (f, [C]) \in (i^*\mathbf{F}_\lambda)(L/k)$ which can not be defined over a subextension of L of a smaller transcendence degree. By definition of $i^*\mathbf{F}_\lambda(L/k)$, the extension L/k is the composite $f \circ i$. Since $[C] \in F_\lambda(L/k')$, then in particular $[C] \in \mathbf{Cub}_3^+(L/k')$, so $[C]$ can be viewed as an element of $\mathbf{Cub}_3^+(L/k)$ via i.

We now proceed to show that $\mathrm{ed}([C]) = 3$ in $\mathbf{Cub}_3^+$.

Assume that there exists a subextension K'/k of L/k with $\mathrm{trdeg}(K' : k) \leq 2$ and $[C'] \in \mathbf{Cub}_3^+(L)$ such that $[C']_L = [C]$.
Let $\varphi : k \longrightarrow L, \psi : k \longrightarrow K'$ and $\theta : K' \longrightarrow L$. Since K'/k is a subextension of L/k, we then have $\theta \circ \psi = \varphi$.
Since $[C] \in \mathbf{F}_\lambda(L/k')$, we have $j(C'_L) = j(C) = j(C_{\lambda L}) = f(t)$, hence $j(C'_L)$ is transcendental over k. Consequently, $j(C') \in K'$ is transcendental over k and we can define a morphism of k-extensions $\beta : k(t) \to K'$ by $\beta(t) = j(C')$ and $\beta_{|k} = \psi$.

We now check that the composite maps $\eta_1 : k(t) \longrightarrow k' \longrightarrow L$ and $\eta_2 : k(t) \longrightarrow K' \longrightarrow L$ are the same.
Let $\alpha \in k$. We have $\eta_1(\alpha) = f(\alpha)$ and $\eta_2(\alpha) = \theta(\psi(\alpha)) = \varphi(\alpha)$. By definition of L/k, we have $\varphi = f \circ i$ (since L/k factors through i). Hence $\eta_2(\alpha) = f(i(\alpha)) = f(\alpha)$. Moreover, since we have $\eta_1(t) = f(t)$ and $\eta_2(t) = \psi(j(C')) = j(C'_L)$, the maps η_1 and η_2 coincide.

Hence we can define the compositum $E/k(t)$ of $k'/k(t)$ and $K'/k(t)$ in $L/k(t)$.

By definition of $E/k(t)$, the composite map $K' \longrightarrow E \longrightarrow L$ is equal to θ, so we have $([C']_E)_L = [C']_L = [C]$. Now consider the extension E/k defined by $k \longrightarrow k' \longrightarrow E$. By construction, this extension factors through i. Let $g : k' \longrightarrow E$. We then have $(g, [C']_E) \in (i^*\mathbf{F}_\lambda)(E/k)$. Moreover, by definition of $E/k(t)$ again, the map $k' \longrightarrow E \longrightarrow L$ is precisely f, hence $(g, [C']_E)_L = (f, [C])$.
Since $\mathrm{trdeg}(K' : k) \leq 2$ and $\mathrm{trdeg}(k(t) : k) = 1$, we have $\mathrm{trdeg}(K' : k(t)) \leq 1$. Moreover, $\mathrm{trdeg}(k' : k(t)) = 0$, hence $\mathrm{trdeg}(E : k(t)) \leq 1$, so $\mathrm{trdeg}(E : k) \leq 2$. Consequently, $x = (f, [C])$ is defined over a subextension of L/k of transcendence degree at most 2, which is impossible by choice of x.

We then get $\mathrm{ed}_k(\mathbf{Cub}_3^+) \geq \mathrm{ed}([C]) = 3$, which concludes the proof of Theorem 5.1.

REFERENCES

[BeF]G.Berhuy, G. Favi Essential dimension: a functorial point of view. Preprint (2003) Available on ...

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

[BOI] M.-A. Knus, A.S. Merkurjev, M. Rost, J.-P. Tignol, The Book of Involutions, AMS Coll. Pub. vol. 44 (1998)

[Re] Z. Reichstein, On a Theorem of Hermite and Joubert. Canadian J. of Mathematics, **51**(1), 69-95 (1999)

Grégory Berhuy
Ecole Polytechnique Fédérale de Lausanne
MA-Ecublens
CH-1015 Lausanne SWITZERLAND

Email:gregory.berhuy@epfl.ch

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

Email: giordano.favi@ima.unil.ch