ACTA ARITHMETICA
C.2 (2001)

Orbits under algebraic groups and logarithms of algebraic numbers

by

Stéphane Fischler (Paris)

1. Introduction. Let K be either the field $\mathbb{C}$ of complex numbers, or its p-adic analog $\mathbb{C}_p$, which is the completion of an algebraic closure of $\mathbb{Q}_p$. Then K is an algebraically closed field of characteristic zero. We fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ in K.

In the complex case, let $L = \{\lambda \in \mathbb{C} : \exp(\lambda) \in \overline{\mathbb{Q}}^*\}$ be the $\mathbb{Q}$-vector space of logarithms of algebraic numbers. In the p-adic case, we define $\log(1+x)$ by its power series expansion if $x \in \mathbb{C}_p$ has positive valuation, and we extend the logarithm function into a morphism of $\mathbb{C}_p^*$ to $\mathbb{C}_p$ such that $\log(p) = 0$. Then we denote by L the set of logarithms of nonzero elements of $\overline{\mathbb{Q}} \subset \mathbb{C}_p$; this set is a $\mathbb{Q}$-vector subspace of $\mathbb{C}_p$.

In what follows (unless otherwise specified), we consider the complex and the p-adic cases simultaneously. We denote by $\mathcal{L}$ the $\overline{\mathbb{Q}}$-vector subspace of K spanned by 1 and L. The Algebraic Independence Conjecture (see [6], Historical Notes of Chapter III) asserts that elements $\lambda_1, \dots, \lambda_q$ of $\mathcal{L}$ are algebraically independent over $\overline{\mathbb{Q}}$ if, and only if, $1, \lambda_1, \dots, \lambda_q$ are linearly independent over $\overline{\mathbb{Q}}$.

A new approach to the Algebraic Independence Conjecture has been suggested by Damien Roy. Instead of fixing elements $\lambda_1, \dots, \lambda_q$ of $\mathcal{L}$ and studying polynomial relations between them, he proceeds in the opposite direction: first fix a system of polynomial relations with coefficients in $\overline{\mathbb{Q}}$, in q variables, then focus on the q-tuples of elements of $\mathcal{L}$ which satisfy these relations. In geometric terms, this means that we are given a closed algebraic subset X of K^q, defined over $\overline{\mathbb{Q}}$ (that is, defined as the zero locus of a collection of polynomials with coefficients in $\overline{\mathbb{Q}}$), and we study the set $X(\mathcal{L}) = X \cap \mathcal{L}^q$ of points of X with coordinates in $\mathcal{L}$.

In this situation, Damien Roy states the following conjecture, which is equivalent [10] to that of algebraic independence:

2000 *Mathematics Subject Classification*: Primary 11J85; Secondary 11J81, 33B10, 14R20, 14L35.

CONJECTURE 1. *Let q be a positive integer, and X be a closed algebraic subset of K^q, defined over $\overline{\mathbb{Q}}$. Then*

$$X(\mathcal{L}) = \bigcup_{E \subset X} E(\mathcal{L})$$

where E runs through the linear affine subspaces of K^q contained in X and defined over $\overline{\mathbb{Q}}$.

Conjecture 1 is a very precise description of $X(\mathcal{L})$. The following conjecture is less precise, therefore easier to prove for a given closed algebraic subset X; nevertheless, it is equivalent to Conjecture 1, since both are equivalent to the Algebraic Independence Conjecture:

CONJECTURE 2. *Let q be a positive integer, and X be a closed algebraic subset of K^q, different from K^q, defined over $\overline{\mathbb{Q}}$. Let $x \in X(\mathcal{L}) = X \cap \mathcal{L}^q$. Then x belongs to some affine hyperplane of K^q defined over $\overline{\mathbb{Q}}$.*

These conjectures are very far from being proved; actually, there are only a few closed algebraic subsets X for which anything is known about $X(\mathcal{L})$:

• Let X be a linear affine subspace of K^q, defined over $\overline{\mathbb{Q}}$. Then Conjectures 1 and 2 hold trivially for X.

• Let d, l and r be positive integers such that $r < dl/(d+l)$. Identify K^{dl} with the space of matrices with d rows and l columns, with entries in K. Let X be the subset of K^{dl} consisting of those matrices of rank at most r. Then Conjecture 2 holds for X: this is a straightforward consequence of Theorem 2.1 stated below, which is due to Damien Roy [9].

• Let k and m be integers such that $2 \leq k \leq m-2$, and denote by $G(k,m)$ the affine cone over the Grassmannian which parametrizes the subspaces of dimension k of K^m. Assume $(k,m) \neq (2,4)$. Then Conjecture 2 holds for $G(k,m)$: this follows both from Theorem 2.1 of [10] and from the results in the present paper (see Section 5.1). Further, if Conjecture 1 holds for $G(2,4)$ then it holds for any $G(k,m)$ ([10], Proposition 2.5).

• Finally, if $K = \mathbb{C}$ and X is an algebraic curve, there are a few results ([11], Theorem 0.2 and Corollary 7.2), but they concern only the points $x \in X(L)$.

In this paper, we prove new results about these sets $X(\mathcal{L})$. On the one hand, we prove Conjecture 1 for some algebraic subsets X, including the affine cone $\mathcal{V}(k,m) \subset \mathrm{Sym}^k(K^m)$ over the Veronese variety if $k \geq 3$ (see Section 6). This yields the following result:

THEOREM 1.1. *Let k and m be integers, with $k \geq 3$. Let P be a homogeneous polynomial of degree k, in m variables, with coefficients in $\mathcal{L}$. Assume that P is the kth power of a linear form Λ with coefficients in K. Then there*

exist a linear form ϕ, with coefficients in $\overline{\mathbb{Q}}$, and an element a of $\mathcal{L}$ such that $P = a\phi^k$.

On the other hand, we prove Conjecture 2 for some orbits of algebraic group actions. In more precise terms, we consider an affine algebraic group G defined over $\overline{\mathbb{Q}}$ acting on a vector space W equipped with a $\overline{\mathbb{Q}}$-structure (see Section 2.1). We assume the representation $\varrho : G \to \mathrm{GL}(W)$ to be a morphism of algebraic varieties defined over $\overline{\mathbb{Q}}$. Let X be an orbit of this action; then X is a locally closed subset of W ([5], Proposition 8.3). The following conjecture may be stated:

Conjecture 3. *Assume X is not of maximal dimension among ϱ-orbits. Then every $x \in X(\mathcal{L})$ belongs to some affine hyperplane of W defined over $\overline{\mathbb{Q}}$.*

Conjecture 3 follows from Conjecture 2, for the union of orbits of dimension less than or equal to $\dim(X)$ is a closed algebraic subset of W defined over $\overline{\mathbb{Q}}$.

In this paper, we prove Conjecture 3 for the orbits X which satisfy some additional assumptions (see Section 4). But the result we obtain is slightly more precise: for these orbits X, every $x \in X(\mathcal{L})$ belongs to some vector hyperplane of W defined over $\overline{\mathbb{Q}}$. The proof of the results stated in Section 4 involves a transcendence theorem due to Damien Roy [9], which yields a lower bound for the rank of a matrix with entries in $\mathcal{L}$ by taking into account the linear relations, with coefficients in $\overline{\mathbb{Q}}$, between its entries. This result is stated in Section 2, together with definitions and notation. Section 3 is devoted to applying this transcendence theorem. In Section 5, we provide examples to which the previous results apply; for instance, the following statement is proved:

Theorem 1.2. *Let n be an integer, and M be a square matrix of size n, with entries in $\mathcal{L}$. Assume that the n^2 entries of M are linearly independent over $\overline{\mathbb{Q}}$. Then the centralizer of M has dimension less than or equal to $(n^2+1)/2$.*

Finally, notice that all the results obtained in this paper concerning the points of $X(\mathcal{L})$ apply, in particular, to the points of $X(L)$. Let $x \in X(L)$; then x belongs to some affine hyperplane of K^q defined over $\overline{\mathbb{Q}}$ if, and only if, x belongs to some vector hyperplane of K^q defined over $\mathbb{Q}$: this follows from the theorem of Baker–Brumer ([1], Chapters 1 and 2). Consequently, it is possible, in every statement in this paper, to replace $(\overline{\mathbb{Q}}, \mathcal{L})$ by $(\mathbb{Q}, L)$.

2. Preliminaries. In what follows, all the subspaces we deal with are vector subspaces (unless otherwise specified).

2.1. *Some elementary facts about $\overline{\mathbb{Q}}$-structures.* This section is devoted to $\overline{\mathbb{Q}}$-structures; a detailed account of this can be found in [2], §8.

Let q be an integer. An element of K^q is said to be *defined over* $\overline{\mathbb{Q}}$ if it belongs to $\overline{\mathbb{Q}}^q$. A basis $(e_1, \ldots, e_q)$ of K^q is said to be *defined over* $\overline{\mathbb{Q}}$ if the vectors e_j are defined over $\overline{\mathbb{Q}}$. A K-subspace of K^q is said to be *defined over* $\overline{\mathbb{Q}}$ if it is spanned by vectors defined over $\overline{\mathbb{Q}}$; this is equivalent to being defined by linear equations with coefficients in $\overline{\mathbb{Q}}$. More generally, a closed algebraic subset of K^q is said to be *defined over* $\overline{\mathbb{Q}}$ if it is the zero locus of a collection of polynomials with coefficients in $\overline{\mathbb{Q}}$.

Let W be a vector space of dimension q over K. A $\overline{\mathbb{Q}}$-*structure* on W is any $\overline{\mathbb{Q}}$-subspace of W that is spanned, over $\overline{\mathbb{Q}}$, by a K-basis of W.

Let W be a vector space of dimension q over K, equipped with a $\overline{\mathbb{Q}}$-structure denoted by $W(\overline{\mathbb{Q}})$. There is a bijective K-linear map f, from W to K^q, that sends $W(\overline{\mathbb{Q}})$ onto $\overline{\mathbb{Q}}^q$. Thanks to f, it makes sense for a vector, basis, subspace or closed algebraic subset of W to be *defined over* $\overline{\mathbb{Q}}$; and this does not depend on the choice of f, but only on the $\overline{\mathbb{Q}}$-structure $W(\overline{\mathbb{Q}})$.

A linear map $f : W \to W'$, where W and W' are equipped with $\overline{\mathbb{Q}}$-structures, is said to be *defined over* $\overline{\mathbb{Q}}$ if $f(W(\overline{\mathbb{Q}})) \subset W'(\overline{\mathbb{Q}})$.

We denote by $W(\mathcal{L})$ the subset of W consisting of those vectors whose coordinates, in a basis of W defined over $\overline{\mathbb{Q}}$, belong to $\mathcal{L}$ (since $\mathcal{L}$ is a vector space over $\overline{\mathbb{Q}}$, the set $W(\mathcal{L})$ does not depend on the basis we choose). Moreover, if X is any subset of W, we let $X(\overline{\mathbb{Q}}) = X \cap W(\overline{\mathbb{Q}})$ and $X(\mathcal{L}) = X \cap W(\mathcal{L})$. If W is the vector space K^q, equipped with the $\overline{\mathbb{Q}}$-structure $\overline{\mathbb{Q}}^q$, this agrees with the notation $X(\mathcal{L}) = X \cap \mathcal{L}^q$ used in the introduction.

Let W be a vector space equipped with a $\overline{\mathbb{Q}}$-structure $W(\overline{\mathbb{Q}})$, and let k be an integer. Then the symmetric power $\mathrm{Sym}^k(W)$ is equipped with an induced $\overline{\mathbb{Q}}$-structure $\mathrm{Sym}^k(W(\overline{\mathbb{Q}}))$. In more concrete terms, if $(e_1, \ldots, e_q)$ is a basis of W defined over $\overline{\mathbb{Q}}$, then the corresponding basis (e_I) of $\mathrm{Sym}^k(W)$ is defined over $\overline{\mathbb{Q}}$ (where $I = (i_1, \ldots, i_q)$ runs through the q-tuples of integers such that $i_1 + \ldots + i_q = k$, and e_I is the symmetric product in which each e_j is repeated i_j times). An analogous argument applies to $W^{\otimes k}$ and $\Lambda^k(W)$.

2.2. *Statement of the transcendence theorems.* The transcendence theorem we will use in Section 3 is the following statement. It is a generalization of Theorem 2.1 of [12]; it results from Theorem 4 of [9] (see the proof of Corollary 1 of the same theorem):

THEOREM 2.1. *Let E and F be nonzero vector spaces equipped with $\overline{\mathbb{Q}}$-structures, of respective dimensions l and d. Let u be a linear map from E to F, of rank r. Assume the following*:

1. *The matrix of u, in bases of E and F defined over $\overline{\mathbb{Q}}$, has entries in $\mathcal{L}$.*
2. *The kernel of u contains no nonzero element of E defined over $\overline{\mathbb{Q}}$.*
3. *The image of u is contained in no hyperplane of F defined over $\overline{\mathbb{Q}}$.*

4. *We have* $r < dl/(d+l)$.

Then there exist vector subspaces $S \subset E$ *and* $T \subset F$, *of respective codimensions* $l_1 \geq 1$ *and* $d_1 \geq 1$, *defined over* $\overline{\mathbb{Q}}$, *with the following properties*: $u(S) \subset T$ *and there is an integer* $r_1 \geq 1$ *such that*

$$\frac{r_1}{d_1} < \frac{r}{d} \quad \textit{and} \quad r_1 \geq \frac{l_1 d_1}{l_1 + d_1}. \tag{1}$$

In this theorem, the assumptions 2 and 3 are not essential: if they are not met, we can consider the induced map $\bar{u} : E/E' \to F'$, where E' is the maximal subspace of E, defined over $\overline{\mathbb{Q}}$, that is contained in $\ker(u)$, and F' is the minimal subspace of F, defined over $\overline{\mathbb{Q}}$, that contains $\mathrm{Im}(u)$. This yields the following corollary, which is Corollary 1 of [9]:

Corollary 2.2. *Let* E *and* F *be nonzero vector spaces equipped with* $\overline{\mathbb{Q}}$*-structures, of respective dimensions* l *and* d. *Let* u *be a linear map from* E *to* F, *of rank* r, *whose matrix in bases of* E *and* F *defined over* $\overline{\mathbb{Q}}$ *has entries in* $\mathcal{L}$. *Then there exist vector subspaces* $S \subset E$ *and* $T \subset F$, *of respective codimensions* $l_1 \geq 0$ *and* $d_1 \geq 1$, *defined over* $\overline{\mathbb{Q}}$, *such that* $u(S) \subset T$ *and* $(d-r)l_1 \leq r d_1$.

In Section 6, we will use the following corollary of Theorem 2.1 ([9], Corollary 2), which is a generalization of the six exponential theorem ([6], Chapter II, Theorem 1):

Theorem 2.3. *Let* d *and* l *be integers, with* $d \geq 2$ *and* $l \geq 3$. *Let* M *be a matrix, with* d *rows and* l *columns, of rank* 1, *with entries in* $\mathcal{L}$. *Then either the rows or the columns of* M *are linearly dependent over* $\overline{\mathbb{Q}}$.

2.3. *Notation.* In what follows, we consider the following situation.

Let W be a finite dimensional vector space over K, equipped with a $\overline{\mathbb{Q}}$-structure.

Let G be an affine algebraic group defined over $\overline{\mathbb{Q}}$, that is, an affine algebraic variety defined over $\overline{\mathbb{Q}}$, equipped with a group structure such that the map $(x, y) \mapsto xy^{-1}$ is a morphism of varieties defined over $\overline{\mathbb{Q}}$. Then $G(K)$ is a Lie group; the notation $G(K)$ underlines the fact that it is equipped with complex or p-adic topology.

Let $\varrho : G \to \mathrm{GL}(W)$ be a linear representation of G, assumed to be at the same time a morphism defined over $\overline{\mathbb{Q}}$ between the algebraic varieties G and $\mathrm{GL}(W)$.

Let X be an orbit of this action. Then X is a smooth locally closed subset of W ([5], Proposition 8.3).

Let

$$d = \dim(W), \quad l = \dim(G), \quad r = \dim(X).$$

We denote by G^{op} the opposite group to G, that is, the group with underlying set that of G and law $*^{\mathrm{op}}$ defined by $a *^{\mathrm{op}} b = b * a$ for all $a, b \in G$ (where $*$ is the law of G). We denote by W^* the dual space of W, and by $\varrho^{\mathrm{op}} : G^{\mathrm{op}} \to \mathrm{GL}(W^*)$ the contragredient representation associated with ϱ, defined by $\varrho^{\mathrm{op}}(g) = {}^{\mathrm{t}}(\varrho(g))$ for all $g \in G$.

The tangent map of ϱ at the unit element (denoted by Id) of G is the map $\mathrm{Lie}(\varrho) : \mathfrak{g} \to \mathfrak{gl}(W)$, where $\mathfrak{g}$ is the Lie algebra of G and $\mathfrak{gl}(W) = \mathrm{End}(W)$ that of $\mathrm{GL}(W)$. Both Lie algebras are equipped with $\overline{\mathbb{Q}}$-structures, and $\mathrm{Lie}(\varrho)$ is defined over $\overline{\mathbb{Q}}$ ([5], §34.2).

For $A \in \mathfrak{g}$ and $\alpha \in W$, we let

$$(\mathrm{Lie}(\varrho)(A))(\alpha) = f_A(\alpha) = M_\alpha(A).$$

In this way we define linear maps (for $A \in \mathfrak{g}$ and $\alpha \in W$)

$$f_A : W \to W \quad \text{and} \quad M_\alpha : \mathfrak{g} \to W.$$

The following lemma ([3], Chapter III, §1.7, Proposition 14) implies that the union of orbits whose dimension is less than some given integer is a closed algebraic subset of W defined over $\overline{\mathbb{Q}}$:

LEMMA 2.4. *For $x \in X$, the image of M_x is the tangent space to X at x; accordingly, we have*

$$\mathrm{rk}(M_x) = \dim(X).$$

This paper originates in the following remark, due to Damien Roy: if X is an orbit of dimension less than $dl/(d+l)$, then for $x \in X(\mathcal{L})$ the map M_x has rank less than $dl/(d+l)$, therefore Theorem 2.1 may apply to M_x. This idea is developed in a more precise way in the next section.

3. Applying a transcendence theorem. In this section, we state and prove Proposition 3.1, the only arithmetical step in the proof of the results mentioned in Sections 4 and 5. This proposition follows from Theorem 2.1, the assumptions of which lead to the following definition:

DEFINITION. The pair (ϱ, X) is said to be *suitable* if the following holds:

1. The map $\mathrm{Lie}(\varrho)$ is injective.

2. There is no pair (V, ϕ), consisting of an open subgroup V of the Lie group $G^{\mathrm{op}}(K)$ and a nonzero element $\phi \in W^*$, such that ϕ is invariant under $\varrho^{\mathrm{op}}(V)$.

3. We have

$$r = \dim(X) < \frac{dl}{d+l} = \frac{\dim(W)\dim(G)}{\dim(W) + \dim(G)}.$$

For brevity, we shall sometimes say that X, rather than (ϱ, X), is suitable.

N.B. If ϱ is faithful then the first condition is met. On the other hand, the second condition is satisfied as soon as for every open subgroup V of $G^{\mathrm{op}}(K)$ there exists $g \in V$ such that 1 is not an eigenvalue of $\varrho(g)$. A sufficient condition for this to hold is the existence of $A \in \mathfrak{g}$ such that $\mathrm{Lie}(\varrho)(A) = \mathrm{Id}$.

Now we can state, and prove, the following:

PROPOSITION 3.1. *Assume (ϱ, X) is suitable. Let $x \in X(\mathcal{L})$ belong to no hyperplane of W defined over $\overline{\mathbb{Q}}$. Then there exist vector subspaces $S \subset \mathfrak{g}$ and $T \subset W$, of respective codimensions $l_1 \geq 1$ and $d_1 \geq 1$, with the following property*: $\mathrm{Im}(f_A) \subset T$ *for all $A \in S$, and there is an integer $r_1 \geq 1$ such that*

$$\frac{r_1}{d_1} < \frac{r}{d} \quad \textit{and} \quad r_1 \geq \frac{l_1 d_1}{l_1 + d_1}. \tag{2}$$

N.B. In particular, the conclusion yields $r_1 < r$ and

$$l_1 < \frac{r}{d-r} d_1. \tag{3}$$

Proof of Proposition 3.1. Let us check that Theorem 2.1 applies to M_x. First of all, the matrix of M_x in bases of $\mathfrak{g}$ and W defined over $\overline{\mathbb{Q}}$ has entries in $\mathcal{L}$ since $x \in W(\mathcal{L})$. Further, we have $\mathrm{rk}(M_x) = \dim(X) < dl/(d+l)$ by Lemma 2.4, and because (ϱ, X) is suitable.

Furthermore, let $A \in \ker(M_x)(\overline{\mathbb{Q}})$. Then x belongs to the kernel of f_A, which is a subspace of W defined over $\overline{\mathbb{Q}}$. Accordingly, this subspace is equal to W itself, that is, $\mathrm{Lie}(\varrho)(A) = 0$; by assumption, this implies $A = 0$.

Finally, let H be a hyperplane defined over $\overline{\mathbb{Q}}$ which contains the image of M_x. Then $x \in f_A^{-1}(H)$ for all $A \in \mathfrak{g}$. This yields $\mathrm{Im}(f_A) \subset H$ for all $A \in \mathfrak{g}(\overline{\mathbb{Q}})$, hence for all $A \in \mathfrak{g}$ by linearity. In the complex case, this implies (thanks to [3], Chapter III, §6.5, Proposition 13) $\varrho(g)(y) - y \in H$ for every $y \in W$ and every g in the neutral component of $G(\mathbb{C})$. In the p-adic case, we have $\mathrm{Im}(\exp(f_A) - \mathrm{Id}) \subset H$ whenever A is close enough to the origin. But there exist open subgroups (in the p-adic topology) $U \subset \mathfrak{g}(K)$ and $V \subset G(K)$, and a bijective exponential map (denoted by $\exp_U$) from U to V. Restricting U and V if necessary, we can assume $\mathrm{Im}(\exp(f_A) - \mathrm{Id}) \subset H$ for all $A \in U$, and $\varrho \circ \exp_U = \exp \circ \mathrm{Lie}(\varrho)$ on U. Then for every $g \in V$ there exists $A \in U$ such that $\exp_U(A) = g$, hence $\mathrm{Im}(\varrho(g) - \mathrm{Id}) = \mathrm{Im}(\exp(f_A) - \mathrm{Id}) \subset H$. Therefore, in the p-adic as well as in the complex case, there is an open subgroup V of $G(K)$ such that $\mathrm{Im}(\varrho(g) - \mathrm{Id}) \subset H$ for all $g \in V$. Let ϕ be a linear form whose kernel is H; the previous relation means $\phi \in \ker(\varrho^{\mathrm{op}}(g) - \mathrm{Id}_{W^*})$ for all $g \in V$; this contradicts the assumption that (ϱ, X) is suitable. Consequently, the image of M_x is contained in no hyperplane of W defined over $\overline{\mathbb{Q}}$.

Thus Theorem 2.1 applies, and produces some subspaces S and T defined over $\overline{\mathbb{Q}}$ such that relations (1) hold and $M_x(S) \subset T$. For $A \in S(\overline{\mathbb{Q}})$, this yields

$f_A^{-1}(T) = W$, i.e. $\mathrm{Im}(f_A) \subset T$. As A runs through a basis of S defined over $\overline{\mathbb{Q}}$, this concludes the proof of Proposition 3.1.

Proposition 3.1 will allow us to prove Conjecture 3 for some orbits X. However, applying this statement prevents us from proving more precise results on the points $x \in X(\mathcal{L})$. This is the reason why the following proposition is useful:

PROPOSITION 3.2. *Let $x \in X(\mathcal{L})$ and denote by $\mathcal{E}$ the minimal subspace of W, defined over $\overline{\mathbb{Q}}$, that contains x. Then there exist vector subspaces $S \subset \mathfrak{g}$ and $T \subset W$, of respective codimensions $l_1 \geq 0$ and $d_1 \geq 1$, such that $(d-r)l_1 \leq rd_1$ and $f_A(\alpha) \in T$ for every $A \in S$ and every $\alpha \in \mathcal{E}$.*

Proof. Corollary 2.2, applied to M_x, produces subspaces S and T, defined over $\overline{\mathbb{Q}}$, such that $M_x(S) \subset T$. For $A \in S(\overline{\mathbb{Q}})$, this implies $f_A(\mathcal{E}) \subset T$; as A runs through a basis of S defined over $\overline{\mathbb{Q}}$, this ends the proof of Proposition 3.2.

4. General results. In this section, we try to prove that every point $x \in X(\mathcal{L})$ belongs to some hyperplane of W defined over $\overline{\mathbb{Q}}$ (except in Theorem 4.2, where a stronger statement is obtained). With this aim in view, we let $x \in X(\mathcal{L})$ be a point that does not belong to any such hyperplane, and we proceed in the following way:

• We assume that (ϱ, X) is suitable, so that Proposition 3.1 applies and produces subspaces S and T.

• We make a geometric assumption on the orbits under ϱ (in Section 4.1) or under the contragredient representation ϱ^{op} (in Sections 4.3 and 4.4). This assumption allows us to derive a relation between $l_1 = \mathrm{codim}(S)$ and $d_1 = \mathrm{codim}(T)$ from the property $\mathrm{Im}(f_A) \subset T$ for all $A \in S$.

• We assume the dimension r of X to be "small enough", and sometimes we add a technical assumption, in order to derive a contradiction from the relations between l_1 and d_1.

These assumptions are of a different kind: the first one appears to be necessary to apply Proposition 3.1. The second one has an important drawback: the property $\mathrm{Im}(f_A) \subset T$ for all $A \in S$ is much stronger than the relation between l_1 and d_1 that we derive from it. Therefore it could be interesting to imagine other (geometric) assumptions than those made in this paper. Finally, the last assumption is fitted in such a way that it is possible to derive a contradiction.

4.1. *A large dimensional ϱ-orbit*

THEOREM 4.1. *Let k be an integer greater than* 1. *Assume that*:

• (ϱ, X) *is suitable*,

- *there exists a ϱ-orbit of codimension less than k in W,*
- *X has dimension $r \leq d/k$.*

Then every element $x \in X(\mathcal{L})$ belongs to some hyperplane of W defined over $\overline{\mathbb{Q}}$.

N.B. In particular, if ϱ has a Zariski-dense orbit then Theorem 4.1 applies with $k = 2$. But in this case, Theorem 4.2 stated below provides a more precise result (except if $r = d/2$).

Proof of Theorem 4.1. Assume there exists $x \in X(\mathcal{L})$ that belongs to no hyperplane of W defined over $\overline{\mathbb{Q}}$. Denote by S and T the subspaces produced by Proposition 3.1, and let α be an element of W whose orbit has codimension $c \leq k-1$. Then $M_\alpha(S) \subset T$, hence $\dim(T) \geq \dim(S) - \dim(\ker(M_\alpha))$. As $\mathrm{rk}(M_\alpha) = d - c \geq d - k + 1$ by Lemma 2.4, we obtain $d_1 \leq l_1 + k - 1$.

This inequality, together with assumption $r \leq d/k$ and inequality (3), yields

$$d_1 - k + 1 \leq l_1 < \frac{r}{d-r} d_1 \leq \frac{d_1}{k-1}, \quad \text{hence} \quad \frac{k-2}{k-1} d_1 < k - 1.$$

But inequalities (2), with $r_1 \geq 1$ and $r \leq d/k$, imply $d_1 > dr_1/r \geq k$, i.e. $d_1 \geq k+1$. Therefore $(k-2)(k+1)/(k-1) < k-1$. If $k \geq 3$, this yields a contradiction.

Assume now $k = 2$. Then $d_1 \leq l_1 + 1$, and $l_1 < d_1$ because of assumption $r \leq d/2$ and inequality (3); therefore $l_1 = d_1 - 1$. But inequalities (2) imply $d_1 > 2r_1$, that is, $d_1 \geq 2r_1 + 1$. Hence $l_1 \geq 2r_1$ and $r_1 \geq (2r_1)(2r_1+1)/(4r_1+1)$, which is impossible because $r_1 \geq 1$.

In conclusion, Theorem 4.1 is proved for any $k \geq 2$.

Actually it is possible (under stronger assumptions) to prove the following more precise description of the points $x \in X(\mathcal{L})$:

THEOREM 4.2. *Assume that*:

- *ϱ has a Zariski-dense orbit Y,*
- *X has dimension $r < d/2$.*

Then for every $x \in X(\mathcal{L})$ there is a subspace $\mathcal{E}$ of W, defined over $\overline{\mathbb{Q}}$, that contains x and is disjoint from Y.

Proof. Let $\mathcal{E}$ be the minimal subspace of W, defined over $\overline{\mathbb{Q}}$, that contains x. Assume there is an element $\alpha \in \mathcal{E}$ that belongs to Y. Then Proposition 3.2 produces subspaces S and T such that $M_\alpha(S) \subset T$, hence $d_1 \leq l_1 + d - \mathrm{rk}(M_\alpha)$. Now Lemma 2.4 implies $\mathrm{rk}(M_\alpha) = d$, thereby proving $d_1 \leq l_1$. But this contradicts the relation $(d-r)l_1 \leq rd_1$, with $r < d/2$ and $d_1 \geq 1$. This ends the proof.

4.2. *Additional notation.* We denote by $\mathfrak{g}^{\mathrm{op}}$ the Lie algebra of G^{op}. This is the Lie algebra with underlying vector space that of $\mathfrak{g}$ and bracket the opposite of the bracket of $\mathfrak{g}$.

In the same way as in Section 2.3, we use the following notation for $A \in \mathfrak{g}^{\mathrm{op}}$ and $\phi \in W^*$: $(\mathrm{Lie}(\varrho^{\mathrm{op}})(A))(\phi) = g_A(\phi) = N_\phi(A)$. For every $A \in \mathfrak{g}^{\mathrm{op}}$ and every $\phi \in W^*$, this defines linear maps $g_A : W^* \to W^*$ and $N_\phi : \mathfrak{g}^{\mathrm{op}} \to W^*$.

For all $A \in \mathfrak{g}$, we have ${}^{\mathrm{t}}(\mathrm{Lie}(\varrho)(A)) = \mathrm{Lie}(\varrho^{\mathrm{op}})(A)$, which reads ${}^{\mathrm{t}}f_A = g_A$. A straightforward consequence of this relation is the following:

LEMMA 4.3. *Let $S \subset \mathfrak{g}$ and $T \subset W$ be subspaces such that $\mathrm{Im}(f_A) \subset T$ for all $A \in S$. Let $T^* \subset W^*$ be the orthogonal subspace to T. Then $g_A(\phi) = N_\phi(A) = 0$ for every $A \in S$ and every $\phi \in T^*$.*

4.3. *Finite number of ϱ^{op}-orbits*

THEOREM 4.4. *Assume that*:

- *(ϱ, X) is suitable,*
- *the contragredient representation ϱ^{op} associated with ϱ has only finitely many orbits,*
- *X has dimension $r \leq d/2$.*

Then every element $x \in X(\mathcal{L})$ belongs to some hyperplane of W defined over $\overline{\mathbb{Q}}$.

Proof. Assume, on the contrary, that some $x \in X(\mathcal{L})$ belongs to no hyperplane of W defined over $\overline{\mathbb{Q}}$. Then Proposition 3.1 applies, and produces subspaces S and T.

Let q be the maximal dimension of the ϱ^{op}-orbits that intersect T^*. Let Y_0 be an orbit realizing this maximum, and let $\phi \in T^* \cap Y_0$. We have $S \subset \ker(N_\phi)$ by Lemma 4.3, hence $l_1 \geq q$ thanks to Lemma 2.4 applied to the representation ϱ^{op} and the orbit Y_0 of ϕ. On the other hand, T^* is contained in the (finite) union of the ϱ^{op}-orbits of its elements, therefore $d_1 \leq q$. Let us compare the relation $l_1 \geq q \geq d_1$ obtained here with formula (3) and assumption $r \leq d/2$; the following contradiction appears: $d_1 \leq l_1 < rd_1/(d-r) \leq d_1$. Therefore Theorem 4.4 is proved.

4.4. *Assumptions on the small ϱ^{op}-orbits.* Throughout this section, we make some assumptions on the "small" ϱ^{op}-orbits, precisely those which have dimension less than $r = \dim(X)$. Assuming that there is no such orbit (except the trivial one), the following statement is obtained:

THEOREM 4.5. *Assume that*:

- *(ϱ, X) is suitable,*
- *all nonzero ϱ^{op}-orbits have dimension at least r,*
- *X has dimension r with $d \geq r(r+1)/2$,*

- *one, at least, of the following holds*:
  1. *the union of* $\{0\}$ *and of the* ϱ^{op}*-orbits of dimension* r *contains no vector subspace of* W^* *of codimension* $r-1$,
  2. *if* ϕ *and* ϕ' *are elements of* W^* *with* ϱ^{op}*-orbits of dimension* r, *and if* $\ker(N_\phi) = \ker(N_{\phi'})$, *then* ϕ *and* ϕ' *are collinear.*

Then every element $x \in X(\mathcal{L})$ *belongs to some hyperplane of* W *defined over* $\overline{\mathbb{Q}}$.

N.B. Assume $r \leq d/2$ and ϱ^{op} has only finitely many orbits of dimension r. Then the union of $\{0\}$ and of the ϱ^{op}-orbits of dimension r has dimension at most r, with $r < d-(r-1)$; therefore assumption 1 holds.

Proof of Theorem 4.5. Assume there exists $x \in X(\mathcal{L})$ that does not belong to any hyperplane of W defined over $\overline{\mathbb{Q}}$. Then applying Proposition 3.1 yields subspaces S and T.

As $d_1 \geq 1$, there exists $\phi \in T^*$ such that $\phi \neq 0$, therefore the ϱ^{op}-orbit of ϕ has dimension at least r. We have $S \subset \ker(N_\phi)$ by Lemma 4.3, therefore Lemma 2.4 yields $l_1 \geq \mathrm{rk}(N_\phi) \geq r$.

Let us prove that the equality $l_1 = r$ does not hold. In fact, otherwise, we would have $\mathrm{rk}(N_\phi) = r$ and $S = \ker(N_\phi)$ for all nonzero $\phi \in T^*$; in particular, by Lemma 2.4, each nonzero $\phi \in T^*$ would belong to some ϱ^{op}-orbit of dimension r. Moreover, relation (3) would yield $d_1 > d-r$. Assumption 1 could not hold. Neither could assumption 2, for it would imply $d_1 \leq 1$, hence $d = r < dl/(d+l)$, which is impossible.

Therefore we have $l_1 \geq r+1$. Thanks to assumption $d \geq r(r+1)/2$ and relations (2), we obtain

$$\frac{(r+1)(d-r)}{d} \geq r-1 \geq r_1 \geq \frac{l_1 d_1}{l_1+d_1} \geq \frac{(r+1)d_1}{(r+1)+d_1}.$$

This yields $d(r+1) \geq r(d_1+r+1)$, hence the following contradiction: $r+1 \leq l_1 < rd_1/(d-r) \leq r+1$. This concludes the proof of Theorem 4.5.

Another result is the following, which applies when it is possible to control the union of "small" ϱ^{op}-orbits:

THEOREM 4.6. *Assume that*:

- (ϱ, X) *is suitable*,
- *the union of all* ϱ^{op}*-orbits of dimension less than* r *contains no vector subspace of* W^* *of dimension greater than* d/r,
- X *has dimension* $r \leq \sqrt{d}$.

Then every element $x \in X(\mathcal{L})$ *belongs to some hyperplane of* W *defined over* $\overline{\mathbb{Q}}$.

Proof. Assume some $x \in X(\mathcal{L})$ belongs to no hyperplane of W defined over $\overline{\mathbb{Q}}$. Then Proposition 3.1 produces some subspaces S and T.

As $r_1 \geq 1$, relation (2) yields $d_1 > d/r$, therefore the union of ϱ^{op}-orbits of dimension less than r contains no vector subspace of W^* of dimension d_1. In particular, T^* is not contained in this union: there exists $\phi \in T^*$ such that $\mathrm{rk}(N_\phi) \geq r$ (thanks to Lemma 2.4). As $S \subset \ker(N_\phi)$ by Lemma 4.3, we obtain $l_1 \geq r$, hence $d_1 > d - r$ and the following contradiction:

$$r - 1 \geq r_1 \geq \frac{l_1 d_1}{l_1 + d_1} > \frac{r(d-r)}{d} = r - \frac{r^2}{d} \geq r - 1.$$

This proves Theorem 4.6.

5. Special cases

5.1. *Symmetric, tensor and exterior powers.* Let V be a vector space of dimension $m \geq 2$ over K, equipped with a $\overline{\mathbb{Q}}$-structure, and let $k \geq 2$ be an integer. We fix a basis $(e_1, \ldots, e_m)$ of V.

In this section, we consider the natural action ϱ of $G = \mathrm{GL}(V)$, first on $W = \mathrm{Sym}^k(V)$, then on $W = V^{\otimes k}$, and finally on $W = \Lambda^k(V)$. We sketch the proofs of Theorems 5.1, 5.3 and 5.4 as consequences of the results obtained in Section 4. Detailed proofs are omitted, because stronger statements can be proved by other methods.

First of all, denote by W the vector space $\mathrm{Sym}^k(V)$; it is equipped with an induced $\overline{\mathbb{Q}}$-structure (see the end of Section 2.1). The action ϱ is given by $\varrho(g)(\alpha_1 \cdot \ldots \cdot \alpha_k) = g(\alpha_1) \cdot \ldots \cdot g(\alpha_k)$ for $g \in G$ and $\alpha_1, \ldots, \alpha_k \in V$. For $A \in \mathfrak{g} = \mathrm{End}(V)$ and $\alpha_1, \ldots, \alpha_k \in V$, we have

$$(\mathrm{Lie}(\varrho)(A))(\alpha_1 \cdot \ldots \cdot \alpha_k) = \sum_{i=1}^{k} \alpha_1 \cdot \ldots \cdot \alpha_{i-1} \cdot A(\alpha_i) \cdot \alpha_{i+1} \cdot \ldots \cdot \alpha_k.$$

Denote by $X = \mathcal{V}(k, V)$ the set of elements of the shape $v \cdot \ldots \cdot v$, with $v \in V$. Then $X \setminus \{0\}$ is a ϱ-orbit of dimension m, known as the affine cone (without the origin) over the Veronese variety ([4], Lecture 2).

Let α be a nonzero element of $\mathrm{Sym}^k(V)$. Denote by g_n the linear automorphism of V which sends e_j to $t_j e_1 + u_n e_j$ for every $j \in \{1, \ldots, m\}$, where $t_1, \ldots, t_m$ are elements of K and (u_n) is a sequence of elements of $K \setminus \{0, -t_1\}$ which tends to zero. Then $g_n(\alpha)$ tends to $\lambda e_1 \cdot \ldots \cdot e_1$ for the norm topology on $\mathrm{Sym}^k(V)$, where $\lambda \in K$ is nonzero if $t_1, \ldots, t_m$ are chosen in a proper way: the closure, for the norm topology, of the orbit Y_α of α intersects X. Therefore the Zariski closure of Y_α, which is a union of ϱ-orbits ([5], Proposition 8.3), contains X. This proves that X lies in the Zariski closure of any nonzero ϱ-orbit. Now, the contragredient representation ϱ^{op} is isomorphic to the representation ϱ^* of $\mathrm{GL}(V^*)$ on $\mathrm{Sym}^k(V^*)$. Therefore every nonzero ϱ^{op}-orbit has dimension at least m, with equality only for the affine cone

$X^* \setminus \{0\}$ over the Veronese variety in $\mathrm{Sym}^k(V^*) \simeq (\mathrm{Sym}^k(V))^*$. Assume $(k,m) \neq (2,2)$ and $(k,m) \neq (3,2)$; then (ϱ, X) is suitable. Accordingly the remark following Theorem 4.5 applies (with $r = m$ and $d = \binom{k+m-1}{m-1}$), thereby proving the following:

THEOREM 5.1. *Assume $(k,m) \neq (2,2)$ and $(k,m) \neq (3,2)$. Then Conjecture 2 holds for the affine cone $\mathcal{V}(k,V)$ over the Veronese variety.*

Actually it is possible, as soon as $(k,m) \neq (2,2)$, to prove a more precise result: see Theorem 6.2 below.

Let us now move to $W = V^{\otimes k}$ and $X = \mathcal{T}(k,V) = \{v \otimes \ldots \otimes v : v \in V\}$. The situation is quite similar to the previous one, except that there may be nonzero ϱ-orbits of dimension less than $m = \dim(X \setminus \{0\})$. For instance, if $k = m$, the orbit of $\alpha = \sum_{\sigma \in \mathfrak{S}_k} \varepsilon_\sigma e_{\sigma(1)} \otimes \ldots \otimes e_{\sigma(k)}$ has dimension 1 (in this formula, ε_σ is the sign of σ).

We are going to apply Theorem 4.6 (with $r = m$ and $d = m^k$); to do this, we need to control the orbits of dimension less than m. With this aim in view, we consider the basis (e_I) of $V^{\otimes k}$, where $I = (i_1, \ldots, i_k)$ runs through $\{1, \ldots, m\}^k$, and its dual basis (e_I^*).

Two families $I = (i_1, \ldots, i_k)$ and $I' = (i'_1, \ldots, i'_k)$ are said to be *anagrams* if there exists a permutation σ of $\{1, \ldots, k\}$ such that $i'_1 = i_{\sigma(1)}, \ldots, i'_k = i_{\sigma(k)}$.

For any family $I = (i_1, \ldots, i_k)$ and any integer $s \in \{1, \ldots, m\}$, we denote by $\mathcal{N}_s(I)$ the number of indices $j \in \{1, \ldots, k\}$ such that $i_j = s$. Two families I and I' are anagrams if, and only if, $\mathcal{N}_s(I) = \mathcal{N}_s(I')$ for all s.

These definitions allow us to prove the following lemma:

LEMMA 5.2. *Let $\alpha = \sum_I \alpha_I e_I$ be a nonzero element of $V^{\otimes k}$ with orbit of dimension less than m. Then k is a multiple of m, and the families I such that $\alpha_I \neq 0$ are anagrams of the family $(1, \ldots, 1, 2, \ldots, 2, \ldots, m)$ in which every integer from 1 to m is repeated k/m times.*

Sketch of proof. Assume the conclusion does not hold. Considering the linear automorphism of V which maps e_j to $\mu_j e_j$, for suitable values of $\mu_1, \ldots, \mu_m \in K$, makes it possible to find a family I_0 and a nonzero element β of $V^{\otimes k}$ with the following properties:

• Either k is not a multiple of m, or I_0 is not an anagram of the family $(1, \ldots, 1, 2, \ldots, 2, \ldots, m)$ in which every integer from 1 to m appears k/m times.

• The element β lies in the closure (for the norm topology, and therefore for the Zariski topology) of the orbit of α.

• We have $\beta = \sum_I \beta_I e_I$ where $\beta_I = \alpha_I$ if I is an anagram of I_0, and $\beta_I = 0$ otherwise; moreover, $\beta_{I_0} = \alpha_{I_0} \neq 0$.

Then the orbit of β is contained in the Zariski closure of that of α, hence has dimension less than m. By Lemma 2.4, this implies $\mathrm{rk}(M_\beta) < m$. We shall now construct m families $J_1, \ldots, J_m$ such that $(e^*_{J_1} \circ M_\beta, \ldots, e^*_{J_m} \circ M_\beta)$ are m linearly independent linear forms; this will give the desired contradiction.

Let H be the set of elements $s \in \{1, \ldots, m\}$ such that $\mathcal{N}_s(I_0) = u$, where u is chosen in such a way that H is neither empty nor $\{1, \ldots, m\}$. Denote by M the complement of H in $\{1, \ldots, m\}$, and let $(s', s'') \in H \times M$. Let $\mathcal{J}_{s',s''}$ be the set of families that can be obtained from I_0 by replacing exactly one occurrence of s' by s''. For $J \in \mathcal{J}_{s',s''}$, let $\lambda_J = \sum_I \alpha_I$, where the sum is taken over all anagrams I of I_0 that can be obtained from J by replacing exactly one occurrence of s'' by s'. Then the relation $e^*_J(M_\beta(A)) = \lambda_J a_{s'',s'}$ holds for any $A \in \mathrm{End}(V)$ identified with its matrix $(a_{i,j})$ in the basis $(e_1, \ldots, e_m)$. Define $\mathcal{J}_{s'',s'}$ in the same way; then for any $J \in \mathcal{J}_{s'',s'}$ there is $\lambda_J \in K$ such that $e^*_J(M_\beta(A)) = \lambda_J a_{s',s''}$ for every A. Now there exists a family $J(s', s'')$, which belongs either to $\mathcal{J}_{s',s''}$ or to $\mathcal{J}_{s'',s'}$, such that $\lambda_{J(s',s'')} \neq 0$. As (s', s'') ranges through $H \times M$, we obtain in this way $(\#H)(\#M) \geq m - 1$ families $J(s', s'')$ among which we select $J_1, \ldots, J_{m-1}$. We let $J_m = I_0$; then an easy computation shows that $(e^*_{J_1} \circ M_\beta, \ldots, e^*_{J_m} \circ M_\beta)$ are linearly independent linear forms. This proves Lemma 5.2.

THEOREM 5.3. *Assume $(k, m) \neq (2, 2)$. Then Conjecture 2 holds for the subset $\mathcal{T}(k, V)$ of $V^{\otimes k}$.*

Again, a more precise result can be obtained (see Theorem 6.4 in Section 6).

Proof of Theorem 5.3. If k is a multiple of m, let I_1 be the family $(1, \ldots, 1, 2, \ldots, 2, \ldots, m)$ in which every integer from 1 to m is repeated k/m times, and denote by F the subspace of $V^{\otimes k}$ spanned by those vectors e_I such that I is an anagram of I_1. If k is not a multiple of m, let $F = \{0\}$. Then, in both cases, F has dimension less than or equal to m^{k-1}, and contains every ϱ-orbit of dimension less than m thanks to Lemma 5.2. Further, $(\varrho, X \setminus \{0\})$ is suitable as soon as $(k, m) \neq (2, 2)$, and ϱ^{op} is isomorphic to ϱ^* (in the same way as in the proof of Theorem 5.1). Therefore Theorem 4.6 applies.

Finally, let us turn to $W = \Lambda^k(V)$. Let $X = G(k, V) = \{v_1 \wedge \ldots \wedge v_k \in \Lambda^k(V) : \ v_1, \ldots, v_k \in V\}$ be the affine cone over the Grassmannian whose points are the k-dimensional subspaces of V. Then $X \setminus \{0\}$ is a ϱ-orbit of dimension $r = k(m - k) + 1$ ([4], Lecture 6).

THEOREM 5.4. *Assume that $2 \leq k \leq m - 2$ and $(k, m) \neq (2, 4)$. Then Conjecture 2 holds for $G(k, V)$.*

Theorem 5.4 is a weaker statement than Theorem 2.1 of [10]. It can be proved as a consequence of Theorems 4.1 and 4.5, except for a few pairs (k, m). Indeed, changing k and V into $m - k$ and V^* if necessary, we may assume $k \leq m/2$. If $k = 2$, each element α of $\Lambda^2(V)$ has an even rank $p \leq m$, which is the only nonnegative integer such that α can be written $v_1 \wedge v_2 + \ldots + v_{p-1} \wedge v_p$ with linearly independent vectors $v_1, \ldots, v_p$ ([7], pages 177 and 192). There are $[m/2] + 1$ ϱ-orbits, each of them corresponding to a value p of the rank. One of them (with $p = m$ or $p = m - 1$) is dense, therefore Theorem 4.1 applies if $m \geq 8$. On the other hand, if $3 \leq k \leq m-3$ and $m \geq 25$ then $d = \binom{m}{k} \geq r(r+1)/2$. Moreover, ϱ^{op} is isomorphic to the natural representation of $\mathrm{GL}(V^*)$ on $\Lambda^k(V^*)$, hence every ϱ^{op}-orbit has dimension greater than r, except $\{0\}$ and $G(k, V^*) \setminus \{0\}$. This allows us to apply Theorem 4.5. To conclude the proof of Theorem 5.4, that is, to deal with the pairs (k, m) such that $k \in \{2, m-2\}$ and $5 \leq m \leq 7$, or $3 \leq k \leq m - 3$ and $m \leq 24$, we apply Proposition 3.1, Lemma 4.3, and we use arguments that are specific to $X = G(k, V)$ (for instance, we bound from below the rank of f_A as soon as $A \in \mathfrak{gl}(V)$ is nonzero). As far as the remaining pair $(k, m) = (2, 4)$ is concerned, nothing can be deduced from Proposition 3.1 because $(\varrho, X \setminus \{0\})$ is not suitable. It may also be noted that Theorem 2.1 of [10] is trivial when $(k, m) = (2, 4)$; nothing is known about the points of $G(2, K^4)(\mathcal{L})$.

5.2. *Centralizers of matrices.* In this section, we consider the action of $\mathrm{GL}_n(K)$ on $\mathrm{Mat}_n(K)$ by conjugation. For $M \in \mathrm{Mat}_n(K)$, let $\mathcal{C}(M)$ be the centralizer of M, that is, the space of all matrices A such that $[A, M] = 0$ (where $[A, M] = AM - MA$). Then the orbit of M under the action of $\mathrm{GL}_n(K)$ has dimension equal to the codimension, in $\mathrm{Mat}_n(K)$, of $\mathcal{C}(M)$. This enables us to prove Theorem 1.2 stated in the introduction, as a corollary of the following statement:

Proposition 5.5. *Let M be a square matrix of size n, with entries in $\mathcal{L}$, whose centralizer $\mathcal{C}(M)$ has dimension greater than $(n^2 + 1)/2$. Then there exist vector subspaces U and V of $\mathrm{Mat}_n(K)$, defined over $\overline{\mathbb{Q}}$, with the following properties*:

- $\dim(U) + \dim(V) \geq n^2 + 2$.
- *For every $A \in U$ and every $B \in V$, $\mathrm{Trace}(M[A, B]) = 0$.*

To deduce Theorem 1.2 from Proposition 5.5, it suffices to exclude the case where $[A, B] = 0$ for any $A \in U$ and any $B \in V$. This is done in the following lemma, whose proof was communicated to me by Gaël Rémond:

Lemma 5.6. *Let U and V be vector subspaces of $\mathrm{Mat}_n(K)$ such that each element of U commutes with each element of V. Then*

$$\dim(U) + \dim(V) \leq n^2 + 1.$$

Proof. This statement is obvious for $n = 1$; let us prove it by induction on n. First of all, it is possible to replace U and V by $U \cap V$ and $U + V$, so we can assume $U \subset V$. Now, if $U \subset K\,\mathrm{Id}$ then the conclusion holds trivially, therefore we can assume there is a matrix $M \in U$ such that $M \notin K\,\mathrm{Id}$. Let λ be an eigenvalue of M, and $F = \ker(M - \lambda\,\mathrm{Id})$. Then F is stable under every matrix that commutes with M, in particular under every matrix of V. Choose a basis of K^n whose first $\dim(F)$ vectors belong to F. In this basis, the elements of V are of the shape $\left(\begin{smallmatrix} A & B \\ 0 & C \end{smallmatrix}\right)$.

Let U' (respectively V') be the set of those matrices A for which there exist matrices B and C such that $\left(\begin{smallmatrix} A & B \\ 0 & C \end{smallmatrix}\right) \in U$ (respectively $\left(\begin{smallmatrix} A & B \\ 0 & C \end{smallmatrix}\right) \in V$). In the same way, define U'' (respectively V'') to be the set of those matrices C for which there exist matrices A and B such that $\left(\begin{smallmatrix} A & B \\ 0 & C \end{smallmatrix}\right) \in U$ (respectively $\left(\begin{smallmatrix} A & B \\ 0 & C \end{smallmatrix}\right) \in V$).

Then U is contained in the set of all matrices $\left(\begin{smallmatrix} A & B \\ 0 & C \end{smallmatrix}\right)$ such that $A \in U'$ and $C \in U''$. This implies

$$\dim(U) \leq \dim(U') + \dim(U'') + (\dim(F))(\mathrm{codim}(F)).$$

An analogous inequality holds for V; by summing up and applying induction to (U', V') and (U'', V''), we obtain

$$\dim(U)+\dim(V) \leq 1+(\dim(F))^2+1+(\mathrm{codim}(F))^2+2(\dim(F))(\mathrm{codim}(F)).$$

This inequality means $\dim(U) + \dim(V) \leq n^2 + 2$; in order to conclude the proof, it suffices to check that equality does not hold. Assume it does. Then U is equal to the set of all matrices $\left(\begin{smallmatrix} A & B \\ 0 & C \end{smallmatrix}\right)$ such that $A \in U'$ and $C \in U''$, and V is equal to the set of matrices $\left(\begin{smallmatrix} A & B \\ 0 & C \end{smallmatrix}\right)$ such that $A \in V'$ and $C \in V''$. Moreover, we then have $\dim(U') + \dim(V') = 1 + (\dim(F))^2$, therefore U' contains a nonzero matrix A. There is a matrix B, with $\dim(F)$ rows and $\mathrm{codim}(F)$ columns, such that $AB \neq 0$. But $\left(\begin{smallmatrix} A & B \\ 0 & 0 \end{smallmatrix}\right) \in U$ commutes with $\left(\begin{smallmatrix} 0 & B \\ 0 & 0 \end{smallmatrix}\right) \in V$, that is, $AB = 0$. This contradiction concludes the proof of Lemma 5.6.

N.B. Using the same kind of methods, it is possible to prove that under the assumptions of Lemma 5.6, if $\dim(U) + \dim(V) = n^2 + 1$ then $U = K\,\mathrm{Id}$ or $V = K\,\mathrm{Id}$.

Proof of Proposition 5.5. Denote by H the space of those matrices A such that $\mathrm{Trace}(A) = 0$; it is equipped with a $\overline{\mathbb{Q}}$-structure $H(\overline{\mathbb{Q}})$ consisting of those matrices with entries in $\overline{\mathbb{Q}}$. Let M be a square matrix of size n, whose n^2 entries belong to $\mathcal{L}$ and whose centralizer $\mathcal{C}(M)$ has codimension r, with $r < (n^2 - 1)/2$.

Let $u = \mathrm{ad}\,M$ be the endomorphism of H which sends any matrix N to $[M, N]$. Then u has rank r, and Corollary 2.2 (applied with E and F equal to H) produces subspaces S and T of H, defined over $\overline{\mathbb{Q}}$, such that $l_1 < d_1$

and $[M, A] \in T$ for all $A \in S$. Denote by T^* the subspace orthogonal to T for the nondegenerate symmetric bilinear form $(X, Y) \mapsto \mathrm{Trace}(XY)$ on H. Then for every $A \in S$ and every $B \in T^*$,

$$0 = \mathrm{Trace}([M, A]\, B) = \mathrm{Trace}(M\, [A, B]).$$

Let $U = S \oplus K\,\mathrm{Id}$ and $V = T^* \oplus K\,\mathrm{Id}$; then $\dim(U) + \dim(V) \geq n^2 + 2$, thereby proving Proposition 5.5.

N.B. We actually proved that it is enough, in Theorem 1.2, to assume that there is no hyperplane of $\mathrm{Mat}_n(K)$, defined over $\overline{\mathbb{Q}}$, which contains both M and Id. A weaker assumption might be sufficient; such an improvement of Theorem 1.2 could be derived from an answer to the following question. Let U and V be vector subspaces of $\mathrm{Mat}_n(K)$ such that $\dim(U) + \dim(V) \geq n^2 + 2$. How small can the vector space spanned by $[U, V]$ be?

In another direction, if the Algebraic Independence Conjecture holds, then a result stronger than Theorem 1.2 follows:

PROPOSITION 5.7. *Take for granted the Algebraic Independence Conjecture. Let M be a square matrix of size n, whose n^2 entries belong to $\mathcal{L}$ and are linearly independent over $\overline{\mathbb{Q}}$. Then the centralizer of M has dimension n.*

Proof. Assume, on the contrary, that $\mathcal{C}(M)$ has dimension greater than n. Then not all eigenvalues of M are simple, and the characteristic polynomial χ_M of M has zero discriminant. Apply Conjecture 1 stated in the introduction: M belongs to a linear affine subspace E of $\mathrm{Mat}_n(K)$, defined over $\overline{\mathbb{Q}}$ and contained in the set of matrices N such that χ_N has zero discriminant. We can assume that E is an affine hyperplane of $\mathrm{Mat}_n(K)$, otherwise E would be contained in a vector hyperplane and the n^2 entries of M would not be linearly independent over $\overline{\mathbb{Q}}$. Moreover, we can assume $n \geq 3$, otherwise Proposition 5.7 holds trivially. Consider now the linear affine subspace consisting of those matrices which are upper triangular with diagonal entries $(1, 2, \ldots, n)$. This subspace has dimension at least 2, therefore it intersects E; this is impossible because for every $N \in E$ the polynomial χ_N has zero discriminant. This ends the proof.

N.B. Following the same lines as in this section, it is possible to study the space of symmetric (or skew-symmetric, or triangular) matrices commuting with a given symmetric (or skew-symmetric, or triangular) matrix M with entries in $\mathcal{L}$.

6. Proof of Conjecture 1 in special cases. Let k and m be positive integers. The following notation is analogous to that used in Section 5.1:

$$\mathcal{V}(k, m) = \{v \cdot \ldots \cdot v : v \in K^m\} \subset \mathrm{Sym}^k(K^m),$$
$$\mathcal{T}(k, m) = \{v \otimes \ldots \otimes v : v \in K^m\} \subset (K^m)^{\otimes k}.$$

When $k = 1$ or $m = 1$, we have $\mathcal{V}(k,m) = \mathrm{Sym}^k(K^m)$ and $\mathcal{T}(k,m) = (K^m)^{\otimes k}$; Conjecture 1 holds trivially for these subsets. This is the reason why we now assume $k \geq 2$ and $m \geq 2$.

In order to prove Theorems 6.2 and 6.4 stated below, we shall use the following lemma:

LEMMA 6.1. *Let $\lambda_1, \ldots, \lambda_q$ be nonzero elements of $\mathcal{L}$ in geometric progression with transcendental ratio. Then $q \leq 3$.*

Proof. Let t be the ratio; then $\lambda_j = \lambda_1 t^{j-1}$ for all $j \in \{1, \ldots, q\}$. The matrix

$$M = \begin{pmatrix} \lambda_1 & \lambda_1 t & \ldots & \lambda_1 t^{q-2} \\ \lambda_1 t & \lambda_1 t^2 & \ldots & \lambda_1 t^{q-1} \end{pmatrix}$$

has rank 1 and entries in $\mathcal{L}$; if $q \geq 4$, Theorem 2.3 shows that either the rows or the columns of M are linearly dependent over $\overline{\mathbb{Q}}$. In the former case, t would be algebraic, which is impossible. In the latter case, t would be a root of a nonzero polynomial with coefficients in $\overline{\mathbb{Q}}$, which is also impossible. This ends the proof.

Let us now state our result concerning the sets $\mathcal{V}(k,m)$. It is helpful to view $\mathrm{Sym}^k(K^m)$ as the space of homogeneous polynomials of degree k, in m variables, with coefficients in K; then $\mathcal{V}(k,m)$ consists of those polynomials which are the kth power of a linear form.

THEOREM 6.2. *Let k and m be integers greater than or equal to 2. Let P be a homogeneous polynomial of degree k, in m variables, with coefficients in $\mathcal{L}$. Assume that P is the kth power of a linear form Λ with coefficients in K.*

1. If $k \geq 3$ then there exist a linear form ϕ, with coefficients in $\overline{\mathbb{Q}}$, and an element a of $\mathcal{L}$ such that $P = a\phi^k$.

2. If $k = 2$ then there exist two linear forms ϕ_1 and ϕ_2, with coefficients in $\overline{\mathbb{Q}}$, and two elements a and b of K such that $P = (a\phi_1 + b\phi_2)^k$.

COROLLARY 6.3. *1. Conjecture 1 holds for $\mathcal{V}(k,m)$ as soon as $k \geq 3$.*

2. If Conjecture 1 holds for $\mathcal{V}(2,2)$ then it holds for $\mathcal{V}(k,m)$ for any pair (k,m).

Proof of Theorem 6.2. Let n be the minimal integer such that there exist linear forms $\phi_1, \ldots, \phi_n$, with coefficients in $\overline{\mathbb{Q}}$, and elements $c_1, \ldots, c_n$ of K such that $\Lambda = \sum_{i=1}^n c_i \phi_i$. Then $c_1, \ldots, c_n$ are linearly independent over $\overline{\mathbb{Q}}$; on the other hand, $\phi_1, \ldots, \phi_n$ are algebraically independent over K: we denote them by $Y_1, \ldots, Y_n$ and write $\Lambda = \sum_{i=1}^n c_i Y_i$. Furthermore, we let $P = \Lambda^k = \sum p_{i_1,\ldots,i_n} Y_1^{i_1} \ldots Y_n^{i_n}$; note that the coefficients $p_{i_1,\ldots,i_n}$ belong to $\mathcal{L}$ since $\phi_1, \ldots, \phi_n$ are defined over $\overline{\mathbb{Q}}$ and linearly independent over K. To begin with, we shall prove that n is at most 2.

Assume $n \geq 3$. Let $Q = (\partial/\partial Y_1)^{k-2}P$. Then Q is a nonzero homogeneous polynomial of degree 2 in $Y_1, \ldots, Y_n$, with coefficients in $\mathcal{L}$, such that $Q = (k!/2)c_1^{k-2}\Lambda^2$. Let δ be a square root of $(k!/2)c_1^{k-2}$, and $\Lambda' = \delta\Lambda$; then $Q = \Lambda'^2$. Now, associate with each homogeneous polynomial $R = \sum_{i,j} r_{i,j}Y_iY_j$ of degree 2 (written in such a way that $r_{i,j} = r_{j,i}$ for all $i, j \in \{1, \ldots, n\}$) the symmetric matrix $\widetilde{R} = (r_{i,j})$ of size n. Denote by $u \in K^n$ the coordinate vector $(\delta c_1, \ldots, \delta c_n)$ of Λ'; the relation $Q = \Lambda'^2$ yields $\widetilde{Q} = u^{\mathrm{t}}u$. Consequently, $\widetilde{Q}$ is a square matrix, of size $n \geq 3$, of rank 1, with entries in $\mathcal{L}$, and Theorem 2.3 applies to $\widetilde{Q}$. Therefore the n coordinates of Λ' are linearly dependent over $\overline{\mathbb{Q}}$, and so are $c_1, \ldots, c_n$, in contradiction with the definition of n.

Therefore $n \leq 2$: Theorem 6.2 is proved if $k = 2$. Assume now $k \geq 3$ and $n = 2$. Then $P = (c_1Y_1 + c_2Y_2)^k = \sum_{j=0}^{k} a_jY_1^jY_2^{k-j}$, with $a_0, \ldots, a_k \in \mathcal{L}$. Let $t = c_1/c_2 \in K$ and $a_j = \binom{k}{j}a'_j$ for all $j \in \{0, \ldots, k\}$; then $a'_j = t^ja'_0$. But t is transcendental, because c_1 and c_2 are linearly independent over $\overline{\mathbb{Q}}$. This contradicts Lemma 6.1, thereby proving Theorem 6.2.

Proof of Corollary 6.3. Let P be as in Theorem 6.2. If $k \geq 3$ then $P = a\phi^k$ belongs to the subspace $K\phi^k$, which is contained in $\mathcal{V}(k, m)$ and defined over $\overline{\mathbb{Q}}$. Assume now that $k = 2$, and that Conjecture 1 holds for $\mathcal{V}(2, 2)$. Let $P = (a\phi_1 + b\phi_2)^2$ be a polynomial with coefficients in $\mathcal{L}$, and consider (in the same way as in the proof of Theorem 6.2) $P_1 = (aY_1 + bY_2)^2$. Then P_1 belongs to a linear affine subspace E_1 contained in $\mathcal{V}(2, 2)$ and defined over $\overline{\mathbb{Q}}$. Let E be the linear affine subspace of $\mathrm{Sym}^2(K^m)$ consisting of those polynomials Q such that there is $Q_1 \in E_1$ with $Q(X_1, \ldots, X_m) = Q_1(\phi_1(X_1, \ldots, X_m), \phi_2(X_1, \ldots, X_m))$. Then $P \in E$, E is defined over $\overline{\mathbb{Q}}$ and $E \subset \mathcal{V}(2, m)$, thereby proving Corollary 6.3.

The proof of Theorem 6.2 given above can be easily translated in terms of symmetric powers; dealing with tensor powers, the following result is obtained in a similar way:

THEOREM 6.4. *Let k and m be integers greater than or equal to 2. Let $v \in K^m$ be such that $x = v \otimes \ldots \otimes v$ belongs to $(K^m)^{\otimes k}(\mathcal{L})$. Then*:

1. *If $k \geq 3$, there exist $a \in \mathcal{L}$ and $v' \in \overline{\mathbb{Q}}^m$ such that $x = av' \otimes \ldots \otimes v'$.*

2. *If $k = 2$, there exists a vector subspace F of K^m, defined over $\overline{\mathbb{Q}}$, of dimension 2, which contains v.*

COROLLARY 6.5. 1. *Conjecture 1 holds for $\mathcal{T}(k, m)$ as soon as $k \geq 3$.*

2. *If Conjecture 1 holds for $\mathcal{T}(2, 2)$ then it holds for $\mathcal{T}(k, m)$ for any pair (k, m).*

Proof of Theorem 6.4. Let F be the smallest vector subspace of K^m, defined over $\overline{\mathbb{Q}}$, that contains v. Let $n = \dim(F)$.

First of all, assume $n \geq 3$. Let ξ be a nonzero linear form on F, defined over $\overline{\mathbb{Q}}$; then $\langle \xi, v \rangle \neq 0$. Denote by D the linear endomorphism of the tensor algebra $T(F)$ which maps any $\alpha = \alpha_1 \otimes \ldots \otimes \alpha_q$ to

$$D(\alpha) = \sum_{j=1}^{q} \langle \xi, \alpha_j \rangle \alpha_1 \otimes \ldots \otimes \alpha_{j-1} \otimes \alpha_{j+1} \otimes \ldots \otimes \alpha_q.$$

Let $Q = D^{k-2}(x) = (k!/2)\langle \xi, v \rangle^{k-2} v \otimes v$ and $v' = \delta v$ where δ is a square root of $(k!/2)\langle \xi, v \rangle^{k-2}$. Choose a basis $(f_1, \ldots, f_n)$ of F, defined over $\overline{\mathbb{Q}}$, and associate with any $R = \sum_{i,j} r_{i,j} f_i \otimes f_j$ the matrix $\widetilde{R} = (r_{i,j})$. Then $\widetilde{Q} = u^{\mathrm{t}} u$ where u is the coordinate vector of v' in the basis $(f_1, \ldots, f_n)$. As $n \geq 3$, Theorem 2.3 shows that v' belongs to some vector hyperplane of F defined over $\overline{\mathbb{Q}}$; then so does v, in contradiction with the definition of F.

Therefore $n \leq 2$, and Theorem 6.4 is proved if $k = 2$. Assume $k \geq 3$ and $n = 2$. Let (f_1, f_2) be a basis of F defined over $\overline{\mathbb{Q}}$; since $n = 2$, we can write $v = a(f_1 + t f_2)$ with $a, t \in K^*$. Then, for every $j \in \{0, \ldots, k\}$, $a^k t^j$ belongs to $\mathcal{L}$: Lemma 6.1 implies $t \in \overline{\mathbb{Q}}$, in contradiction with the definition of F. This ends the proof of Theorem 6.4; Corollary 6.5 immediately follows.

N.B. As Damien Roy pointed out to me, Theorems 6.2 and 6.4 can be easily deduced from each other by considering the linear embedding of $\mathrm{Sym}^k(K^m)$ into $(K^m)^{\otimes k}$ which sends $v_1 \cdot \ldots \cdot v_k$ to $(1/k!) \sum v_{\sigma(1)} \otimes \ldots \otimes v_{\sigma(k)}$, where the sum is over all permutations σ of $\{1, \ldots, k\}$. Indeed, this embedding maps $\mathcal{V}(k, m)$ onto $\mathcal{T}(k, m)$.

N.B. The following conjectures are equivalent:

1. Conjecture 1 holds for $\mathcal{V}(2, 2)$.
2. Conjecture 1 holds for $\mathcal{T}(2, 2)$.
3. It is possible to replace $q \leq 3$ by $q \leq 2$ in the conclusion of Lemma 6.1.

These conjectures are consequences of the four exponential conjecture (i.e. the assertion that Theorem 2.3 holds when $d = l = 2$). There seems to be a gap between these conjectures and the theorems proved up to now; actually, it is impossible ([8], Proposition 2) to derive "algebraically" any of these conjectures from Theorem 2.1.

Acknowledgements. I am grateful to Michel Waldschmidt and Damien Roy for the time they spent with me, in discussions I always found exciting.

References

[1] A. Baker and D. W. Masser (eds.), *Transcendence Theory*: *Advances and Applications*, Proceedings of a Conference held in Cambridge in 1976, Academic Press, 1977.

[2] N. Bourbaki, *Algèbre*, Chapitre II, 3rd ed., Hermann, 1962.
[3] —, *Groupes et algèbres de Lie*, Chapitres II et III, Hermann, 1972.
[4] J. Harris, *Algebraic Geometry, A First Course*, Grad. Texts in Math. 133, Springer, 1992.
[5] J. E. Humphreys, *Linear Algebraic Groups*, Grad. Texts in Math. 21, Springer, 1975.
[6] S. Lang, *Introduction to Transcendental Numbers*, Addison-Wesley, 1966.
[7] C. Mutafian, *Algebra Multilineal*, Instituto Cubano del Libro, 1974.
[8] D. Roy, *Sur la conjecture de Schanuel pour les logarithmes de nombres algébriques*, Problèmes Diophantiens 1988-89, Publ. Math. Univ. Paris VI 90.
[9] —, *Matrices whose coefficients are linear forms in logarithms*, J. Number Theory 41 (1992), 22–47.
[10] —, *Points whose coordinates are logarithms of algebraic numbers on algebraic varieties*, Acta Math. 175 (1995), 49–73.
[11] D. Roy et M. Waldschmidt, *Approximation diophantienne et indépendance algébrique de logarithmes*, Ann. Sci. École Norm. Sup. (4) 30 (1997), 753–796.
[12] M. Waldschmidt, *Transcendance et exponentielles en plusieurs variables*, Invent. Math. 63 (1981), 97–127.

Département de Mathématiques et Applications
École Normale Supérieure
45, rue d'Ulm
75230 Paris Cedex 05, France
E-mail: fischler@dma.ens.fr

Received on 5.4.2000
and in revised form on 19.12.2000 (3795)