Acta Math., 175 (1995), 49–73

Points whose coordinates are logarithms of algebraic numbers on algebraic varieties

by

DAMIEN ROY[1]

Université d'Ottawa
Ottawa, Canada

Introduction

The main conjecture about the set $\mathcal{L}\subset\mathbf{C}$ of logarithms of algebraic numbers is that any family of elements of $\mathcal{L}$ which is linearly independent over $\mathbf{Q}$ is algebraically independent over $\mathbf{Q}$ (see Chapter III of [13]). Our goal is to present here a new point of view on this conjecture and to establish some results in this context.

We first show that this conjecture is equivalent to saying that, for each integer $n>0$ and each algebraic subvariety X of $\mathbf{C}^n$ (irreducible or not) defined over the algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$, the set $X\cap\mathcal{L}^n$ of points of X with coordinates in $\mathcal{L}$ is contained in the union of all vector subspaces of $\mathbf{C}^n$ defined over $\mathbf{Q}$ and contained in X. Baker's theorem [2] shows that this is true when X is a linear subvariety of $\mathbf{C}^n$ defined over $\overline{\mathbf{Q}}$. Let $M_{d,l}$ be the vector space of all $d\times l$ matrices with coefficients in $\mathbf{C}$. A result of W. D. Brownawell [5] and M. Waldschmidt [20] shows that the above statement is also true when X is an affine curve defined over $\overline{\mathbf{Q}}$ contained in the variety $M_{d,l}(1)$ of all $d\times l$ matrices of rank $\leqslant 1$ provided that X is not contained in any of the subspaces of $M_{d,l}$ which are defined over $\mathbf{Q}$ and contained in $M_{d,l}(1)$. More generally, there is a result of M. Waldschmidt (Theorem 2.1 of [21]) which studies the points with coordinates in $\mathcal{L}$ on the variety $M_{d,l}(r)$ of $d\times l$ matrices of rank $\leqslant r$, for given positive integers d, l and r. It shows that these points are contained in some subspaces of $M_{d,l}$ defined over $\mathbf{Q}$. These subspaces are not necessarily contained in $M_{d,l}(r)$ but we prove in §1 that they can be chosen inside $M_{d,l}(2r)$ so that they contain a subspace of codimension $\leqslant 2r^2$ contained in $M_{d,l}(r)$.

In §2, we study the special case where X is the affine cone over the Grassmannian which parametrizes the subspaces of dimension k of $\mathbf{C}^m$ for given integers $k\geqslant 2$ and

---

(1) Research supported in part by NSERC and, at MSRI, by NSF Grant DMS 9022140.

$m \geqslant k+2$. This variety is naturally embedded in $\mathbf{C}^n$ with $n=\binom{m}{k}$ and we get that, for any $x \in X \cap \mathcal{L}^n$, the smallest subspace of $\mathbf{C}^n$ defined over $\mathbf{Q}$ which contains x is either of dimension $\leqslant 6$ or contained in X. Our result is in fact more precise and implies that if the conjecture is true for $k=2$ and $m=4$ then it is true for all values of k and m. This is translated in terms of a new conjecture about 4×4 skew-symmetric matrices with coefficients in $\mathcal{L}$, of which the four exponentials conjecture is shown to be a special case.

The proof of this result uses both Gel'fond–Schneider's theorem and the result of M. Waldschmidt mentioned above. The method goes by constructing an injective linear map $\theta: \mathbf{C}^n \to M_{d,l}$ defined over $\mathbf{Q}$, with $d=\binom{m}{k-1}$ and $l=m$, which maps X into $M_{d,l}(k)$; it thus maps the points of X with coordinates in $\mathcal{L}$ into those of $M_{d,l}(k)$.

In §3, we show that a similar construction can be done, at least locally, for any affine homogeneous algebraic variety $X \subseteq \mathbf{C}^n$ defined over $\mathbf{Q}$ where, by homogeneous affine variety, we mean the affine cone over some projective variety. This allows a priori to apply Waldschmidt's theorem to study the points of X with coordinates in $\mathcal{L}$. It implies that, if the above version of the main conjecture for logarithms is true for the varieties $M_{d,l}(r)$, then it is true for any homogeneous affine algebraic variety X defined over $\mathbf{Q}$. Finally, we indicate the limits of this method by showing that it is not capable of proving the four exponentials conjecture.

The above approach which we apply to the affine cones over Grassmannians is not intrinsic since the map θ is not unique. One would like to apply directly the transcendence methods to the variety X by constructing an exponential polynomial with integer coefficients which would be "small" on this set. Such a construction is given in §4. It does not require that X be defined over $\overline{\mathbf{Q}}$ and generalizes an earlier construction of M. Waldschmidt (Theorem 3.1 of [21]). This construction together with Liouville's inequality provides, under certain conditions, non-trivial vanishing statements for the affine cones over Grassmannians and for other varieties. It calls for a zero estimate which would be sufficiently precise to derive a conclusion from this vanishing.

Finally, our results hold also with the p-adic field $\mathbf{C}_p$ instead of $\mathbf{C}$, for any prime p. We discuss both cases simultaneously. Moreover, to avoid changes of coordinates, we prefer to work with abstract vector spaces equipped with a $\mathbf{Q}$-structure rather than working with $\mathbf{C}^n$ or $\mathbf{C}_p^n$. This is explained in §1 below.

1. Preliminaries

Let K be the field $\mathbf{C}$ or the completion $\mathbf{C}_p$ of an algebraic closure of $\mathbf{Q}_p$ for a prime number p, equipped with its usual absolute value denoted $|\cdot|$ and normalized so that $|p|=p^{-1}$ if $K=\mathbf{C}_p$. We denote by $\overline{\mathbf{Q}}$ the algebraic closure of $\mathbf{Q}$ in K, by $\mathcal{U}$ the disk of convergence of the exponential series in K, by $\exp: \mathcal{U} \to K$ the function determined by this series and by $\mathcal{L}$ the $\mathbf{Q}$-subspace of K generated by $\exp^{-1}(\bar{\mathbf{Q}}^*)$. When $K = \mathbf{C}$, $\mathcal{L}$ is simply the set of logarithms of algebraic numbers of $\mathbf{C}$.

Let F be a subfield of K and let V be a finite-dimensional vector space over K. If $v_1, \ldots, v_s$ are elements of V, we denote by $\langle v_1, \ldots, v_s \rangle_F$ the subspace of V generated by them over the field F. We recall that a $\mathbf{Q}$-*structure* on V is a $\mathbf{Q}$-subspace V' of V such that any basis of V' over $\mathbf{Q}$ is also a basis of V over K (§8, No. 1 of [4]). Given V with a $\mathbf{Q}$-structure V', we say that an algebraic subvariety X of V is *defined over* F if, for some isomorphism $f: V \to K^n$ with $f(V') = \mathbf{Q}^n$, the image of X under f is the set of zeroes of a family of polynomials with coefficients in F. This contains in particular the notion of subspace of V defined over F. If W is another finite-dimensional K-vector space equipped with a $\mathbf{Q}$-structure W', we say that a linear or affine linear map $f: V \to W$ is *defined over* $\mathbf{Q}$ if $f(V') \subseteq W'$. This gives a $\mathbf{Q}$-structure on the vector space $\mathrm{Hom}(V, W)$ of K-linear maps from V to W.

In the sequel, we denote by $V(\mathbf{Q})$ a given $\mathbf{Q}$-structure of V and by $V(\mathcal{L})$ the $\mathbf{Q}$-subspace of V generated by the products λv with $\lambda \in \mathcal{L}$ and $v \in V(\mathbf{Q})$ and, for each subset X of V, we put

$$X(\mathbf{Q}) = X \cap V(\mathbf{Q}) \quad \text{and} \quad X(\mathcal{L}) = X \cap V(\mathcal{L}).$$

For example, if $V = K^n$, we take $V(\mathbf{Q}) = \mathbf{Q}^n$ and then we have $V(\mathcal{L}) = \mathcal{L}^n$. If V is the K-vector space $M_{d,l}$ of all $d \times l$ matrices with entries in K, we choose for $M_{d,l}(\mathbf{Q})$ the set of $d \times l$ matrices with entries in $\mathbf{Q}$ and $M_{d,l}(\mathcal{L})$ becomes the space of $d \times l$ matrices with entries in $\mathcal{L}$. Moreover, for any integer $r \geqslant 0$, the set $M_{d,l}(r)$ of all elements of $M_{d,l}$ of rank $\leqslant r$ is an algebraic subvariety of $M_{d,l}$ defined over $\mathbf{Q}$.

Given V with its $\mathbf{Q}$-structure, we put on its dual V^* the dual $\mathbf{Q}$-structure $V^*(\mathbf{Q})$ which consists of all $\phi \in V^*$ such that $\phi(V(\mathbf{Q})) \subseteq \mathbf{Q}$. On each subspace W of V defined over $\mathbf{Q}$, we also put the induced $\mathbf{Q}$-structure $W(\mathbf{Q}) = W \cap V(\mathbf{Q})$. Finally, for each integer $k \geqslant 1$, we give $\bigwedge^k V$ the $\mathbf{Q}$-structure $\bigwedge^k(V(\mathbf{Q}))$. We denote by $G(k, V)$ the image of the map

$$\begin{aligned} V^k &\to \textstyle\bigwedge^k V \\ (v_1, \ldots, v_k) &\mapsto v_1 \wedge \ldots \wedge v_k. \end{aligned}$$

This is an algebraic subvariety of $\bigwedge^k V$ defined over $\mathbf{Q}$: it is the affine cone over the Grassmannian of subspaces of V of dimension k (Lecture 6 of [11]). If $V = K^n$ with $V(\mathbf{Q}) = \mathbf{Q}^n$, then the points of $G(k, V)(\mathcal{L})$ are those which come from subspaces of V of dimension k which possess at least one set of Plücker coordinates in $\mathcal{L}$.

As mentioned in the introduction, the main conjecture for logarithms says that any family of elements of $\mathcal{L}$ which is linearly independent over $\mathbf{Q}$ is also algebraically independent over $\mathbf{Q}$. We restate it in the following form:

CONJECTURE 1.1. *For each finite-dimensional K-vector space V equipped with a $\mathbf{Q}$-structure and for each algebraic subvariety X of V defined over $\overline{\mathbf{Q}}$, $X(\mathcal{L})$ is contained in the union of all vector subspaces of V defined over $\mathbf{Q}$ and contained in X.*

To see that the two conjectures are equivalent, assume first that Conjecture 1.1 is true. Given $\mathbf{Q}$-linearly independent elements $\lambda_1, \ldots, \lambda_n$ of $\mathcal{L}$, we choose $V = K^n$ and take for X the Zariski closure over $\overline{\mathbf{Q}}$ of the point $(\lambda_1, \ldots, \lambda_n)$. Since K^n is the smallest subspace of K^n defined over $\mathbf{Q}$ which contains this point, we get $K^n \subseteq X$. Thus, $\lambda_1, \ldots, \lambda_n$ are algebraically independent over $\mathbf{Q}$ and the main conjecture for logarithms is verified. Reciprocally, assume that the latter is true and let V and X be as in the statement of Conjecture 1.1. Then, the Zariski closure over $\overline{\mathbf{Q}}$ of any point $x \in X(\mathcal{L})$ is the smallest subspace S of V defined over $\mathbf{Q}$ containing x. We get $x \in S \subseteq X$ and so Conjecture 1.1 is verified.

In this context, the theorem of A. Baker [2] and its p-adic analog ([6], [7], [18], [19]) show that Conjecture 1.1 is verified when X is a linear subvariety of V defined over $\overline{\mathbf{Q}}$. For $K = \mathbf{C}$, we also have the result of W. D. Brownawell and M. Waldschmidt mentioned in the introduction, but its p-adic analog is not known. To study other algebraic varieties we use the following result [21]:

THEOREM 1.2 (M. Waldschmidt). *Let d, l be positive integers and let $M \in M_{d,l}(\mathcal{L})$. Assume that the rows of M are $\mathbf{Q}$-linearly independent, that the columns of M are $\mathbf{Q}$-linearly independent and that the rank r of M satisfies $r < dl/(d+l)$. Then, there exist matrices $P \in \mathrm{GL}_d(\mathbf{Q})$ and $Q \in \mathrm{GL}_l(\mathbf{Q})$ such that*

$$PMQ = \begin{pmatrix} M_1 & 0 \\ * & M_2 \end{pmatrix} \tag{1.1}$$

where M_1 is a $d_1 \times l_1$ matrix of rank $r_1 > 0$ with

$$\frac{d_1}{r_1} > \frac{d}{r} \quad \text{and} \quad d_1 l_1 \leqslant r_1(d_1 + l_1). \tag{1.2}$$

Although this theorem does not prove Conjecture 1.1 for the varieties $M_{d,l}(r)$, it implies the following:

COROLLARY 1.3. *Let d, l, r be positive integers. For each $M \in M_{d,l}(r)(\mathcal{L})$, there exist subspaces S and T of $M_{d,l}$ defined over $\mathbf{Q}$ with*

$$M \in T \subseteq M_{d,l}(2r), \quad S \subseteq T \cap M_{d,l}(r)$$

and $\dim(S) \geqslant \dim(T) - 2r^2$.

Proof. Let $M \in M_{d,l}(r)(\mathcal{L})$. Without loss of generality we may assume that the rows of M are $\mathbf{Q}$-linearly independent and that its columns are $\mathbf{Q}$-linearly independent. By replacing M by its transpose if necessary, we may also assume $d \geqslant l$. If $l \leqslant r$, the corollary is verified with $S=T=M_{d,l}$. In particular, it is verified when $d+l=2$. This allows to assume $l>r$. If $dl \leqslant r(d+l)$, we have $l \leqslant 2r$; we take for S the subspace of $M_{d,l}$ consisting of all $d \times l$ matrices whose last $l-r$ columns are zero, and put $T=M_{d,l}$. The corollary is then verified because

$$\dim(S) = dr \geqslant dl - rl \geqslant \dim(T) - 2r^2.$$

Otherwise, if $dl > r(d+l)$, we have $d > 2r$ and the hypotheses of Theorem 1.2 are satisfied. We may thus assume that M is of the form (1.1) where M_1 is a $d_1 \times l_1$ matrix of rank $r_1 > 0$ with d_1, l_1 and r_1 satisfying (1.2). Since $d > 2r$, the inequalities (1.2) imply $d_1 > 2r_1$ and $l_1 < 2r_1$. Moreover, M_2 is a $d_2 \times l_2$ matrix with coefficients in $\mathcal{L}$ and rank $r_2 > 0$ where

$$d_2 = d - d_1, \quad l_2 = l - l_1 \quad \text{and} \quad r_2 \leqslant r - r_1.$$

By induction on $d+l$, we may assume that the corollary is verified for M_2. There thus exist subspaces S_2 and T_2 of M_{d_2,l_2} defined over $\mathbf{Q}$ with

$$M_2 \in T_2 \subseteq M_{d_2,l_2}(2r_2), \quad S_2 \subseteq T_2 \cap M_{d_2,l_2}(r_2)$$

and $\dim(S_2) \geqslant \dim(T_2) - 2r_2^2$. We then take for T the set of $d \times l$ block matrices of the form

$$\begin{pmatrix} N_1 & 0 \\ N_3 & N_2 \end{pmatrix}$$

with N_1 of size $d_1 \times l_1$ and $N_2 \in T_2$, and we take for S the subspace of T consisting of all those matrices for which the $l_1 - r_1$ last columns of N_1 and N_3 are zero and for which $N_2 \in S_2$. We have $M \in T$ as required and, since $r_1 + r_2 \leqslant r$ and $l_1 < 2r_1$, we also have $T \subseteq M_{d,l}(2r)$ and $S \subseteq M_{d,l}(r)$. Finally, we get the upper bound

$$\begin{aligned} \dim(T) - \dim(S) &\leqslant d(l_1 - r_1) + 2r_2^2 \\ &\leqslant r l_1 + 2r_2^2 \quad (\text{by } (1.2)). \end{aligned}$$

Since $l_1 < 2r_1$, it implies $\dim(T) - \dim(S) \leqslant 2rr_1 + 2r_2^2 \leqslant 2r^2$ as required.

Finally, since we will need it often, we recall as a second corollary the so-called six exponentials theorem due to Siegel (historical notes of Chapter II of [13]), S. Lang [12] and K. Ramachandra [15]. We take our formulation from Corollary 1.3 of [22]:

COROLLARY 1.4 (the six exponentials theorem). *Let d, l be positive integers with $d \geqslant 3$ and $l \geqslant 2$, and let $M \in M_{d,l}(\mathcal{L})$. Assume that at least three of the d rows of M are $\mathbf{Q}$-linearly independent and that at least two of the l columns of M are $\mathbf{Q}$-linearly independent. Then the rank of M is at least 2.*

This implies that if S, T are finite-dimensional vector spaces over K equipped with $\mathbf{Q}$-structures and if $f: S \to T$ is a linear map of rank $\leqslant 1$ satisfying $f(S(\mathbf{Q})) \subseteq T(\mathcal{L})$ then

(i) either $f(S)$ is contained in a subspace of T defined over $\mathbf{Q}$ of dimension $\leqslant 2$,

(ii) or $f(S(\mathbf{Q}))$ is of dimension $\leqslant 1$ over $\mathbf{Q}$.

Remarks. (i) Define the *structural rank* of a matrix $M \in M_{d,l}(\mathcal{L})$ as the smallest integer s for which $M_{d,l}(s)$ contains a subspace of $M_{d,l}$ defined over $\mathbf{Q}$ containing M. Then, Corollary 1.3 shows that the rank r of M satisfies $r \leqslant s \leqslant 2r$. This can also be deduced from the arguments in the proof of Corollary 2.2.p of [21]. Conjecture 1.1 predicts $r = s$. Note that a classification of the subspaces of $M_{d,l}(r)$ is given in [1] and [8] for $r \leqslant 3$.

(ii) Corollary 1.3 gives the best upper bound one can expect to deduce from Theorem 1.2 for the codimension of S in T since this theorem says nothing about the elements of $M_{2r,2r}(\mathcal{L})$ of rank r and since all subspaces of $M_{2r,2r}$ contained in $M_{2r,2r}(r)$ have codimension $\geqslant 2r^2$ in $M_{2r,2r}$ ([3], [9], [10]). The space T constructed inductively in the proof is a *compression subspace* of $M_{d,l}(2r)$ in the sense of [8].

(iii) All the statements of this section and those of §§2 and 3 remain true if one replaces everywhere $\mathbf{Q}$ by $\overline{\mathbf{Q}}$ and $\mathcal{L}$ by the $\overline{\mathbf{Q}}$-vector subspace of K generated by $\mathcal{L}$, whose elements are the so-called linear forms in logarithms. The corresponding analog of Theorem 1.2 which one needs is Theorem 4 of [16]. It is also possible using this theorem to make analog statements in the situation where $\mathcal{L}$ is replaced by the $\overline{\mathbf{Q}}$-vector subspace of K generated by $\mathbf{Q} + \mathcal{L}$.

2. Affine cones over Grassmannians

Let V be a vector space over K of dimension $\geqslant 2$ equipped with a $\mathbf{Q}$-structure. The main objective of this section is to establish the following result:

THEOREM 2.1. *Let k be an integer $\geqslant 2$. Assume* $\dim V \geqslant k+2$. *Then, any element of $G(k, V)(\mathcal{L})$ belongs*

(i) *either to a subspace of $\bigwedge^k V$ defined over $\mathbf{Q}$ and contained in $G(k, V)$,*

(ii) *or to a subspace of $\bigwedge^k V$ defined over $\mathbf{Q}$ of dimension 6 of the form $v_1 \wedge \ldots \wedge v_{k-2} \wedge (\bigwedge^2 U)$ where U is a subspace of V defined over $\mathbf{Q}$ of dimension 4, and $v_1, \ldots, v_{k-2} \in V(\mathbf{Q})$.*

In this statement, the restrictions $k \geqslant 2$ and $\dim V \geqslant k+2$ exclude the trivial cases where $G(k,V)$ coincides with $\bigwedge^k V$. We first mention one consequence of this result:

COROLLARY 2.2. *For any $\alpha \in G(k,V)(\mathcal{L})$, the smallest subspace of $\bigwedge^k V$ defined over $\mathbf{Q}$ containing α contains a subspace of codimension $\leqslant 3$ which is defined over $\mathbf{Q}$ and contained in $G(k,V)$.*

In fact, it follows from Theorem 2.1 that, if it is not contained in $G(k,V)$, the smallest subspace of $\bigwedge^k V$ defined over $\mathbf{Q}$ containing α contains a subspace of codimension $\leqslant 3$ of the form $v_1 \wedge \ldots \wedge v_{k-1} \wedge W$ where W is a subspace of V defined over $\mathbf{Q}$.

The proof of Theorem 2.1 goes by steps. We begin by recalling the following result (see Exercise 6.9 (ii) in [11]):

PROPOSITION 2.3. *For any positive integer $k < \dim V$, the maximal subspaces of $\bigwedge^k V$ defined over $\mathbf{Q}$ and contained in $G(k,V)$ are of the following forms:*

(i) $v_1 \wedge \ldots \wedge v_{k-1} \wedge V$ *with* $v_1, \ldots, v_{k-1} \in V(\mathbf{Q})$,

(ii) $\bigwedge^k U$ *where U is a subspace of V defined over $\mathbf{Q}$ of dimension $k+1$.*

We also introduce some notations. Firstly, for all subspaces S of V (resp. of V^*), we denote by $S^\perp$ the subspace of V^* (resp. of V) consisting of all elements which are orthogonal to S. For each integer $k \geqslant 1$ and each $\alpha \in \bigwedge^k V$, we denote by V_α the smallest subspace W of V such that $\alpha \in \bigwedge^k W$. If $\alpha \neq 0$, its dimension is $\geqslant k$ with equality if and only if $\alpha \in G(k,V)$. We also denote by $g\colon V^* \times \bigwedge^k V \to \bigwedge^{k-1} V$ the unique bilinear map (so-called *contraction*) which satisfies

$$g(\phi, v_1 \wedge \ldots \wedge v_k) = \sum_{i=1}^{k} (-1)^{i-1} \phi(v_i) v_1 \wedge \ldots \wedge \widehat{v_i} \wedge \ldots \wedge v_k$$

for all $\phi \in V^*$ and all $v_1, \ldots, v_k \in V$. For each $\alpha \in \bigwedge^k V$, it gives a linear map

$$\begin{aligned} g_\alpha \colon V^* &\to \textstyle\bigwedge^{k-1} V \\ \phi &\mapsto g(\phi, \alpha) \end{aligned}$$

whose kernel is $V_\alpha^\perp$ and whose rank is therefore equal to $\dim V_\alpha$. To see that $\ker g_\alpha$ is $V_\alpha^\perp$, choose $\phi \in V^*$ with $\phi \neq 0$ and choose $v \in V$ with $\phi(v) = 1$. Put $U = \ker \phi$. Since $V = \langle v \rangle_K \oplus U$, we can write $\alpha = v \wedge \beta + \gamma$ with $\beta \in \bigwedge^{k-1} U$ and $\gamma \in \bigwedge^k U$. We get $g_\alpha(\phi) = \beta$. So, ϕ is in $\ker g_\alpha$ if and only if $V_\alpha \subseteq \ker \phi$. This proves our assertion. In particular, an element α of $\bigwedge^k V$ belongs to $G(k,V)$ if and only if the rank of g_α is $\leqslant k$.

The last statement can be reformulated in the following way. Put $l = \dim(V)$, $d = \dim(\bigwedge^{k-1} V)$ and identify $\mathrm{Hom}(V^*, \bigwedge^{k-1} V)$ with the space $M_{d,l}$ of $d \times l$ matrices by choosing basis in $V^*(\mathbf{Q})$ and $\bigwedge^{k-1} V(\mathbf{Q})$. Then, we get an injective linear map

$$g\colon \bigwedge^k V \to M_{d,l}$$
$$\alpha \mapsto g_\alpha$$

again denoted by g, which is defined over $\mathbf{Q}$ and induces an isomorphism between $G(k,V)$ and the intersection of $M_{d,l}(k)$ with the image of g. This determinantal presentation of $G(k,V)$ plays a central role in the proof of Theorem 2.1. Given $\alpha\in G(k,V)(\mathcal{L})$, g_α is an element of $M_{d,l}(k)(\mathcal{L})$ and we may apply Theorem 1.2 to it. This is what we will do in §2.1 for the case $k=2$ and in §2.2 for the case $k=3$ and $\dim V=5$. An induction argument in §2.3 will reduce the general case to those two special cases.

We will also need the fact that, for any $\alpha\in G(k,V)$, the image of g_α is $\bigwedge^{k-1} V_\alpha$. This is because, if $\alpha\neq 0$, both subspaces of $\bigwedge^{k-1} V$ have the same dimension, and the first is contained in the second. In particular, the image of g_α is contained in $G(k-1,V)$ and, for each $\phi\in V^*$, if we put $\beta=g_\alpha(\phi)$, then we have $V_\beta\subseteq V_\alpha$.

The following lemma is useful. We will employ it below to derive another consequence of Theorem 2.1.

LEMMA 2.4. *Let r, s be positive integers with $r+s\leqslant\dim V$ and let $\alpha\in G(r+s,V)(\mathcal{L})$ with $\alpha\neq 0$. Assume that there exist $v_1,\dots,v_r\in V(\mathbf{Q})$ and a subspace U of V defined over $\mathbf{Q}$ such that*

$$\alpha\in v_1\wedge\ldots\wedge v_r\wedge\left(\bigwedge^s U\right).$$

Then, we have $v_1,\dots,v_r\in V_\alpha$ and α can be written in the form $\alpha=v_1\wedge\ldots\wedge v_r\wedge\beta$ with $\beta\in G(s,U)(\mathcal{L})$.

Proof. Suppose first that $U\cap\langle v_1,\dots,v_r\rangle_K=0$. Under this additional assumption, we will show, by induction on r, that there is one and only one $\beta\in\bigwedge^s U$ satisfying

$$\alpha=v_1\wedge\ldots\wedge v_r\wedge\beta \tag{2.1}$$

and that this β belongs to $G(s,U)(\mathcal{L})$. This will imply that V_α is the subspace of V generated by $v_1,\dots,v_r$ and V_β; thus a fortiori $v_1,\dots,v_r\in V_\alpha$.

To prove the above claim, we use the fact that g_α maps $V^*(\mathbf{Q})$ to $G(r+s-1,V)(\mathcal{L})$, and choose $\phi\in V^*(\mathbf{Q})$ such that $\phi(v_1)=1$ and $\phi(v)=0$ for all $v\in\langle v_2,\dots,v_r\rangle_K\oplus U$. Consider $g_\alpha(\phi)$ and write α in the form (2.1) with $\beta\in\bigwedge^s U$. If $r=1$, we have $g_\alpha(\phi)=\beta$. This proves the unicity of β. Since $g_\alpha(\phi)\in G(s,V)(\mathcal{L})$ and since $V_\beta\subseteq U$, this also implies $\beta\in G(s,U)(\mathcal{L})$. If $r>1$, we have $g_\alpha(\phi)=v_2\wedge\ldots\wedge v_r\wedge\beta$. Since $g_\alpha(\phi)\in G(r+s-1,V)(\mathcal{L})$, the claim follows by the induction hypothesis applied to $g_\alpha(\phi)$.

In general, write $U=U_0\oplus U_1$ where U_0, U_1 are subspaces of V defined over $\mathbf{Q}$ such that

$$U_0 \subseteq \langle v_1, ..., v_r\rangle_K \quad \text{and} \quad U_1 \cap \langle v_1, ..., v_r\rangle_K = 0.$$

Since

$$v_1\wedge ...\wedge v_r \wedge (\textstyle\bigwedge^s U) = v_1\wedge ...\wedge v_r \wedge (\textstyle\bigwedge^s U_1),$$

the conclusion follows from the above special case of the lemma applied with U_1 instead of U.

PROPOSITION 2.5. *If Conjecture* 1.1 *is verified for the variety $G(2, K^4)$, then it is also verified for $G(k, V)$.*

Proof. Assume that Conjecture 1.1 is not satisfied for some $\alpha\in G(k, V)(\mathcal{L})$. Then, Theorem 2.1 together with Lemma 2.4 shows that there exist $v_1, ..., v_{k-2}\in V(\mathbf{Q})$ and a subspace U of V defined over $\mathbf{Q}$ of dimension 4 such that α can be written $\alpha=v_1\wedge ...\wedge v_{k-2}\wedge\beta$ with $\beta\in G(2, U)(\mathcal{L})$. This bivector β does not belong to any subspace of $\bigwedge^2 U$ defined over $\mathbf{Q}$ and contained in $G(2, U)$. Therefore, if we identify U with K^4 via a linear map defined over $\mathbf{Q}$, we find that the conjecture does not hold for $G(2, K^4)$.

2.1. The case of 2-planes

Proof of Theorem 2.1 *for* $k=2$. Let α be a non-zero element of $G(2, V)(\mathcal{L})$ and let $d=\dim V$. We may assume without loss of generality that V is the smallest subspace of V defined over $\mathbf{Q}$ which contains V_α and that its dimension d is >4. In virtue of Proposition 2.3, it remains to show that $V_\alpha\cap V(\mathbf{Q})$ contains a non-zero element v because, in this case, we get $\alpha\in v\wedge V$. To this end, consider the map

$$g_\alpha: V^* \to V.$$

Since its kernel is $V_\alpha^\perp$, this map is injective on $V^*(\mathbf{Q})$. Since its image is V_α, its rank is 2 and V is the smallest subspace of V defined over $\mathbf{Q}$ containing its image. Now, choose some basis of $V(\mathbf{Q})$ and $V^*(\mathbf{Q})$ so that g_α can be identified with an element of $M_{d,d}(2)(\mathcal{L})$. By the above, this matrix fulfils all the hypotheses of Theorem 1.2. This implies that there exist subspaces S of V^* and T of V both defined over $\mathbf{Q}$ such that $g_\alpha(S)\subseteq T$ and such that, if we put

$$l_1 = \dim(V^*/S) \quad \text{and} \quad d_1 = \dim(V/T),$$

and if we denote by r_1 the rank of the linear map from V^*/S to V/T induced by g_α, we then have $r_1>0$,

$$\frac{d_1}{r_1} > \frac{d}{2} \quad \text{and} \quad d_1 l_1 \leqslant r_1(d_1+l_1).$$

This implies $r_1=1$, $d_1\geqslant 3$ and $l_1=1$. Since $T\neq V$, T does not contain the image of g_α, and, since S is of codimension 1 in V^*, the inclusion $g_\alpha(S)\subseteq T$ forces $\ker g_\alpha\subseteq S$. As $\ker g_\alpha$ is $V_\alpha^\perp$, this gives $S^\perp\subseteq V_\alpha$ and therefore $V_\alpha\cap V(\mathbf{Q})\neq 0$.

The case where $\dim V=4$ cannot be studied by the above method but leads in terms of matrices to the following generalization of the four exponentials conjecture.

CONJECTURE 2.6. *For any 4×4 skew-symmetric matrix M with entries in $\mathcal{L}$ and rank $\leqslant 2$, either the rows of M are linearly dependent over $\mathbf{Q}$ or the column-space of M contains a non-zero element of $\mathbf{Q}^4$.*

To see how this follows from Conjecture 1.1, assume $\dim V=4$, choose a basis of $V(\mathbf{Q})$ and take the dual basis in $V^*(\mathbf{Q})$. Then, the map from $\bigwedge^2 V$ to $M_{4,4}$ which associates to an element α of $\bigwedge^2 V$ the matrix of g_α in these bases gives a bijection between $G(2,V)(\mathcal{L})$ and the set of 4×4 skew-symmetric matrices with entries in $\mathcal{L}$ and rank $\leqslant 2$. If M is such a matrix, and if α is the corresponding element of $G(2,V)(\mathcal{L})$, Conjecture 1.1 together with Proposition 2.3 shows that either we have $V_\alpha\cap V(\mathbf{Q})\neq 0$ or V_α is contained in a subspace of V defined over $\mathbf{Q}$ of dimension 3. Since V_α is the image of g_α, this means that the column space of M either contains a non-zero element of $\mathbf{Q}^4$ or is contained in a subspace of K^4 defined over $\mathbf{Q}$ of dimension 3. In the last case, the rows of M are linearly dependent over $\mathbf{Q}$.

The four exponentials conjecture (Chapter II, §1 of [13]) says that if a 2×2 matrix (λ_{ij}) with entries in $\mathcal{L}$ has rank one then, either its rows are linearly dependent over $\mathbf{Q}$, or its columns are linearly dependent over $\mathbf{Q}$. This follows from the above conjecture applied to the matrix

$$\begin{pmatrix} 0 & \lambda_{11} & \lambda_{12} & 0 \\ -\lambda_{11} & 0 & 0 & -\lambda_{21} \\ -\lambda_{12} & 0 & 0 & -\lambda_{22} \\ 0 & \lambda_{21} & \lambda_{22} & 0 \end{pmatrix}.$$

In general, the condition that a skew-symmetric 4×4 matrix $M=(x_{ij})$ has rank $\leqslant 2$ is expressed by saying that its Pfaffian is zero, that is

$$x_{12}x_{34}-x_{13}x_{24}+x_{14}x_{23}=0.$$

The algebraic variety defined by this equation can be seen as the affine cone over the variety of incidence of lines and points in projective 2-space. This suggests to look more generally at the affine cone over the variety of incidence of hyperplanes and points in projective n-space, whose defining equation in K^{2n+2} is $x_0y_0+x_1y_1+\ldots+x_ny_n=0$.

2.2. The case of 3-planes in 5-space

The proof of Theorem 2.1 in the case $k=3$ and $\dim V=5$ requires two preliminary lemmas.

LEMMA 2.7. *Let k be an integer $\geqslant 2$ and let $\alpha \in G(k,V)(\mathcal{L})$. Assume that α is $\neq 0$ and contained in a subspace of $\bigwedge^k V$ defined over $\mathbf{Q}$ of dimension $\leqslant 2$. Then, we have $V_\alpha \cap V(\mathbf{Q}) \neq 0$.*

Proof. We first consider the case $k=2$. In this case, there exist a basis $\mathcal{B}=\{e_1,\dots,e_d\}$ of $V(\mathbf{Q})$ and elements $\lambda, a_3,\dots,a_d,b_3,\dots,b_d$ of K such that $\alpha=\lambda v_1\wedge v_2$ with

$$v_1=e_1+a_3e_3+\dots+a_de_d \quad \text{and} \quad v_2=e_2+b_3e_3+\dots+b_de_d.$$

Choose $\mathcal{B}$ such that the $\mathbf{Q}$-subspace F of K generated by $a_3,\dots,a_d,b_3,\dots,b_d$ satisfies $F\cap\mathbf{Q}=0$. If $F=0$, then $v_1,v_2\in V_\alpha\cap V(\mathbf{Q})$ and the lemma is verified. Assume $F\neq 0$ and put $\mathcal{C}=\{e_i\wedge e_j : 1\leqslant i<j\leqslant d\}$. Since α is contained both in $\bigwedge^2 V(\mathcal{L})$ and in a subspace of $\bigwedge^2 V$ defined over $\mathbf{Q}$ of dimension $\leqslant 2$, the coordinates of α in the basis $\mathcal{C}$ generate a subspace E of $\mathcal{L}$ of dimension $\leqslant 2$. Now, E is generated by λ and the products λa_i, λb_i, $\lambda(a_ib_j-a_jb_i)$ for $i,j=3,\dots,d$. In particular, E contains $\lambda\mathbf{Q}\oplus\lambda F$ and so, F is of dimension 1 over $\mathbf{Q}$. Let $\{t\}$ be a basis of F over $\mathbf{Q}$. Then, $\{\lambda,\lambda t\}$ is a basis of E over $\mathbf{Q}$. Moreover, since t is the ratio of two elements of $\mathcal{L}$, Gel'fond–Schneider's theorem shows that t is transcendental over $\mathbf{Q}$. Therefore, λt^2 does not belong to E and so, we have $a_ib_j-a_jb_i=0$ for $i,j=3,\dots,d$. This means that the vectors $a_3e_3+\dots+a_de_d$ and $b_3e_3+\dots+b_de_d$ of $tV(\mathbf{Q})$ are linearly dependent over $\mathbf{Q}$. Thus, V_α contains a non-zero element of $\langle e_1,e_2\rangle_{\mathbf{Q}}$ and the lemma is again verified.

Assume now $k\geqslant 3$. Since $\alpha\neq 0$, there exists $\phi\in V^*(\mathbf{Q})$ such that $V_\alpha\not\subseteq\ker\phi$. Put $\beta=g_\alpha(\phi)$. We have $\beta\neq 0$, $\beta\in G(k-1,V)(\mathcal{L})$ and $V_\beta\subseteq V_\alpha$. Moreover, since the map $\gamma\mapsto g(\phi,\gamma)$ from $\bigwedge^k V$ to $\bigwedge^{k-1} V$ is linear and defined over $\mathbf{Q}$, we also have that β is contained in a subspace of $\bigwedge^{k-1} V$ defined over $\mathbf{Q}$ of dimension $\leqslant 2$. By induction over k, we may thus assume $V_\beta\cap V(\mathbf{Q})\neq 0$. Since $V_\beta\subseteq V_\alpha$, the conclusion follows.

LEMMA 2.8. *Assume $\dim V=5$ and let U be a subspace of V of dimension 3. Assume that $\bigwedge^2 U$ is contained in a subspace of $\bigwedge^2 V$ defined over $\mathbf{Q}$ of dimension $\leqslant 7$, and that we have $U\cap V(\mathbf{Q})=0$. Then, U is contained in a subspace of V defined over $\mathbf{Q}$ of dimension $\leqslant 4$.*

Proof. Choose bases $\{u_1,u_2,u_3\}$ of U and $\{e_1,\dots,e_5\}$ of $V(\mathbf{Q})$ such that

$$u_1=e_1+ae_4+be_5, \quad u_2=e_2+ce_4+de_5, \quad u_3=e_3+ge_4+he_5,$$

where $a,\dots,h\in K$ generate a $\mathbf{Q}$-subspace F of K satisfying $F\cap\mathbf{Q}=0$, and denote by U' the $\mathbf{Q}$-subspace of U generated by $\{u_1,u_2,u_3\}$.

Suppose first that U' contains an element which does not belong to any subspace of V defined over $\mathbf{Q}$ of dimension $\leqslant 2$. Then, we may assume that u_1 is such an element, so that $1, a, b$ are linearly independent over $\mathbf{Q}$. Let $\{\phi_{ij} : 1 \leqslant i < j \leqslant 5\}$ be the basis of $\bigwedge^2 V^*$ dual to the basis $\{e_i \wedge e_j : 1 \leqslant i < j \leqslant 5\}$ of $\bigwedge^2 V$. The hypothesis on U means that the $\mathbf{Q}$-subspace E of K^3 generated by the triples $(\phi_{ij}(u_1 \wedge u_2), \phi_{ij}(u_1 \wedge u_3), \phi_{ij}(u_2 \wedge u_3))$ with $1 \leqslant i < j \leqslant 5$ has dimension $\leqslant 7$. If we omit $(i, j) = (4, 5)$, we find that E contains the nine vectors:

$$\begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix}, \begin{pmatrix}a\\0\\-g\end{pmatrix}, \begin{pmatrix}b\\0\\-h\end{pmatrix}, \begin{pmatrix}0\\a\\c\end{pmatrix}, \begin{pmatrix}0\\b\\d\end{pmatrix}, \begin{pmatrix}c\\g\\0\end{pmatrix}, \begin{pmatrix}d\\h\\0\end{pmatrix}.$$

The first seven of them being linearly independent over $\mathbf{Q}$, the remaining ones are linear combinations of these. If we consider only their first two coordinates, this gives $c, d, g, h \in \langle a, b\rangle_{\mathbf{Q}}$. By replacing u_2 and u_3 by other elements of U' if necessary, we may therefore assume $c \in \langle b\rangle_{\mathbf{Q}}$ and $g = 0$. If $c \neq 0$, this implies that the eighth vector is a non-zero multiple of the fifth one, so $h = 0$, which is impossible since $e_3 \notin U$. Thus $c = 0$, and the hypothesis $U \cap V(\mathbf{Q}) = 0$ implies that 1, d and h are linearly independent over $\mathbf{Q}$. This gives a contradiction since the ninth vector is a linear combination of the first seven.

Thus, any element of U' belongs to a subspace of V defined over $\mathbf{Q}$ of dimension $\leqslant 2$. In particular, we can write

$$u_i = e_i + t_i f_i$$

with $f_i \in \langle e_4, e_5\rangle_{\mathbf{Q}}$ and $t_i \in F$ for $i = 1, 2, 3$. The condition $U \cap V(\mathbf{Q}) = 0$ implies that all products $t_i f_i$ are $\neq 0$ and $\dim_{\mathbf{Q}}\langle t_1, t_2, t_3\rangle_{\mathbf{Q}} \geqslant 2$. By permuting the u_i's if necessary, we may assume that t_1 and t_2 are linearly independent over $\mathbf{Q}$. Then, by permuting u_1 and u_2 if necessary, we may also assume that t_1 and t_3 are linearly independent over $\mathbf{Q}$ (because $t_3 \neq 0$). Since $u_1 + u_2$ and $u_1 + u_3$ belong to subspaces of V defined over $\mathbf{Q}$ of dimension $\leqslant 2$, this forces $f_2 \in \langle f_1\rangle_{\mathbf{Q}}$ and $f_3 \in \langle f_1\rangle_{\mathbf{Q}}$. Therefore, U is contained in the subspace of V generated by e_1, e_2, e_3 and f_1, and the lemma is proved.

Proof of Theorem 2.1 *for* $k=3$ *and* $\dim V = 5$. Let $\alpha \in G(3, V)(\mathcal{L})$ with $\alpha \neq 0$. If V_α is contained in a subspace of V defined over $\mathbf{Q}$ of dimension $\leqslant 4$, the theorem is verified for α. Otherwise, since $\dim V = 5$, the linear map

$$g_\alpha : V^* \to \bigwedge\nolimits^2 V$$

is injective on $V^*(\mathbf{Q})$. Assume that this is the case. Let T be the smallest subspace of $\bigwedge^2 V$ defined over $\mathbf{Q}$ which contains the image $\bigwedge^2 V_\alpha$ of g_α, and let d be its dimension. If $d \leqslant 7$, Lemma 2.8 shows that V_α contains a non-zero element v of $V(\mathbf{Q})$. We then get

$\alpha\in v\wedge(\bigwedge^2 U)$ where U is any subspace of V defined over $\mathbf{Q}$ such that $V=\langle v\rangle_K\oplus U$, and the theorem is verified for α. We may thus assume $d\geqslant 8$. In that case, we choose bases of $V^*(\mathbf{Q})$ and $T(\mathbf{Q})$ so that g_α can be identified with a matrix in $M_{d,5}(3)(\mathcal{L})$. This matrix fulfils all the hypotheses of Theorem 1.2. Therefore, there exist subspaces S_1 of V^* and T_1 of T both defined over $\mathbf{Q}$ such that $g_\alpha(S_1)\subseteq T_1$ and such that, if we put

$$l_1=\dim(V^*/S_1) \quad\text{and}\quad d_1=\dim(T/T_1),$$

and if we denote by r_1 the rank of the linear map from V^*/S_1 to T/T_1 induced by g_α, we have $r_1>0$,

$$\frac{d_1}{r_1}>\frac{d}{3} \quad\text{and}\quad d_1l_1\leqslant r_1(d_1+l_1).$$

We will show that this again implies $V_\alpha\cap V(\mathbf{Q})\neq 0$, and thus Theorem 2.1 will be verified for α. If $r_1=1$, the above inequalities give $d_1\geqslant 3$ and $l_1=1$. Since $T_1\neq T$, T_1 does not contain the image of g_α. Since it already contains $g_\alpha(S_1)$ and since S_1 is of codimension 1 in V^*, this implies $\ker g_\alpha\subseteq S_1$, thus $S_1^\perp\subseteq V_\alpha$ and so $V_\alpha\cap V(\mathbf{Q})\neq 0$ as announced. It remains the case where $r_1=2$. In that case, we get $d_1\geqslant 6$ and $l_1\leqslant 3$, so $\dim S_1\geqslant 2$. Moreover, the restriction of g_α to a linear map from S_1 to T_1 has rank $\leqslant 1$. Since it maps $S_1(\mathbf{Q})$ injectively into $T_1(\mathcal{L})$, the six exponentials theorem (Corollary 1.4) shows that $g_\alpha(S_1)$ is contained in a subspace of T_1 defined over $\mathbf{Q}$ of dimension $\leqslant 2$. Let ϕ be any non-zero element of $S_1(\mathbf{Q})$ and put $\beta=g_\alpha(\phi)$. Since β is a non-zero element of $G(2,V)(\mathcal{L})$, Lemma 2.7 gives $V_\beta\cap V(\mathbf{Q})\neq 0$. Since $V_\beta\subseteq V_\alpha$, our assertion is again verified.

2.3. The general case

The inductive argument is based on the following proposition:

PROPOSITION 2.9. *Let k be an integer $\geqslant 3$. Let $\alpha\in G(k,V)(\mathcal{L})$ and $\phi\in V^*(\mathbf{Q})$, and put $\beta=g_\alpha(\phi)$. Assume $\beta\neq 0$ and let S be a subspace of V defined over $\mathbf{Q}$ which contains V_β. Then,*

(i) *either we have $V_\alpha\cap V(\mathbf{Q})\neq 0$,*

(ii) *or there exists $u\in V(\mathbf{Q})$ such that $V_\alpha\subseteq\langle u\rangle_K+S$.*

Proof. Put $U=\ker\phi$ and choose $v\in V(\mathbf{Q})$ such that $\phi(v)=1$. Since $V=\langle v\rangle_K\oplus U$, we can write $\alpha=v\wedge\gamma+\delta$ with $\gamma\in\bigwedge^{k-1}U$ and $\delta\in\bigwedge^k U$. Since $g_\alpha(\phi)=\beta$, we get $\gamma=\beta$ and therefore $V_\beta\subseteq U$. By replacing S by $S\cap U$ if necessary, this allows to assume $S\subseteq U$. Consider the decomposition

$$\textstyle\bigwedge^{k-1}V=(v\wedge(\bigwedge^{k-2}U))\oplus\bigwedge^{k-1}U$$

and let $\pi: \bigwedge^{k-1} V \to v\wedge(\bigwedge^{k-2} U)$ denote the projection on the first factor. We observe that the composite map

$$\pi\circ g_\alpha: V^* \to v\wedge(\bigwedge^{k-2} U)$$

is given by

$$(\pi\circ g_\alpha)(\psi) = -v\wedge g_\beta(\psi)$$

for all $\psi\in V^*$. This implies that $\pi\circ g_\alpha$ vanishes identically on $S^\perp$ and that its rank coincides with the rank of g_β. Since $\beta\in G(k-1, V)$ and $\beta\neq 0$, this rank is $k-1$. As g_α has rank k, the restriction of g_α to $S^\perp$ must therefore have rank $\leqslant 1$. Since $\phi\in S^\perp$ and since $g_\alpha(\phi)=\beta$, this means that g_α maps $S^\perp$ onto $\langle\beta\rangle_K$. Since moreover g_α maps $V^*(\mathbf{Q})$ to $(\bigwedge^{k-1} V)(\mathcal{L})$, the six exponentials theorem (Corollary 1.4) gives that

(i) either β belongs to a subspace of $\bigwedge^{k-1} V$ defined over $\mathbf{Q}$ of dimension $\leqslant 2$,

(ii) or g_α maps $S^\perp(\mathbf{Q})$ to $\langle\beta\rangle_{\mathbf{Q}}$.

In case (i), Lemma 2.7 gives $V_\beta\cap V(\mathbf{Q})\neq 0$ and so, we get $V_\alpha\cap V(\mathbf{Q})\neq 0$ since $V_\beta\subseteq V_\alpha$. Finally, in case (ii), there exists $u\in V(\mathbf{Q})$ such that

$$g_\alpha(\psi) = \psi(u)\beta = g_{u\wedge\beta}(\psi)$$

for all $\psi\in S^\perp$. Put $\varepsilon=\alpha-u\wedge\beta$. Then, g_ε vanishes identically on $S^\perp$. This means $V_\varepsilon\subseteq S$ and so $V_\alpha\subseteq\langle u\rangle_K+S$.

Proof of Theorem 2.1. We proceed by induction on k. The case where $k=2$ being proved, we assume $k\geqslant 3$. Let α be a non-zero element of $G(k, V)(\mathcal{L})$. If V_α contains a non-zero element v of $V(\mathbf{Q})$, we have $\alpha\in v\wedge(\bigwedge^{k-1} V)$ and so, by Lemma 2.4, we can write $\alpha=v\wedge\beta$ with $\beta\in G(k-1, V)(\mathcal{L})$. This allows, by induction on k, to assume that the theorem is verified for β. It is then also verified for α. Otherwise, that is if $V_\alpha\cap V(\mathbf{Q})=0$, we choose $\phi\in V^*(\mathbf{Q})$ such that $g_\alpha(\phi)\neq 0$ and put $\beta=g_\alpha(\phi)$. We have $\beta\neq 0$, $\beta\in G(k-1, V)(\mathcal{L})$ and $V_\beta\subseteq V_\alpha$, so $V_\beta\cap V(\mathbf{Q})=0$. By induction on k, we may assume that the theorem is verified for β. Since $k\geqslant 3$ and $V_\beta\cap V(\mathbf{Q})=0$, this implies, by Lemma 2.4, that

(i) either β belongs to a subspace T of $\bigwedge^{k-1} V$ defined over $\mathbf{Q}$ and contained in $G(k-1, V)$,

(ii) or $k=3$ and β belongs to $\bigwedge^2 S$ for a subspace S of V defined over $\mathbf{Q}$ of dimension 4.

In the first case, Lemma 2.4 and Proposition 2.3 show $T\subseteq\bigwedge^{k-1} S$ where S is a subspace of V defined over $\mathbf{Q}$ of dimension k. Thus, in each case, we have $V_\beta\subseteq S$ where S is a subspace of V defined over $\mathbf{Q}$ of dimension k if $k\geqslant 4$, of dimension $\leqslant 4$ if $k=3$. Also, by Proposition 2.9, there exists $u\in V(\mathbf{Q})$ such that $V_\alpha\subseteq\langle u\rangle_K+S$. We thus get $\alpha\in\bigwedge^k U$ where $U=\langle u\rangle_K+S$ is a subspace of V defined over $\mathbf{Q}$ of dimension $\leqslant k+1$ if $k\geqslant 4$, of dimension $\leqslant 5$ if $k=3$. If $k \geqslant 4$, this proves the theorem for α. If $k=3$, we observe that we have more precisely $\alpha \in G(3, U)(\mathcal{L})$ with $\dim U \leqslant 5$ and this brings us back to the special case where $k=3$ and $\dim V=5$ studied in §2.2. This completes the proof.

Remark. It is simpler to prove the weaker result that, for $k \geqslant 2$ and $\dim V \geqslant k+2$, any element α of $G(k, V)(\mathcal{L})$ belongs either to a subspace of $\bigwedge^k V$ defined over $\mathbf{Q}$ and contained in $G(k, V)$, or to a subspace of $\bigwedge^k V$ of the form $\bigwedge^k U$ where U is a subspace of V defined over $\mathbf{Q}$ of dimension $k+2$. This follows as above, by induction on k, using only the special case $k=2$ studied in §2.1. It thus needs the transcendence result (Theorem 1.2) only for matrices of rank $\leqslant 2$. The general result needs it for matrices of rank $\leqslant 3$.

3. General affine algebraic varieties

3.1. Embeddings into linear determinantal varieties

The intersection of a generic determinantal variety $M_{d,l}(r)$ with a linear subvariety of $M_{d,l}$ is called a linear determinantal variety. In §2, we studied the points of $G(k, V)(\mathcal{L})$ by observing that $G(k, V)$ is isomorphic to a linear determinantal variety, via a linear map defined over $\mathbf{Q}$. The following result shows that this can be done at least locally for any affine homogeneous algebraic variety defined over $\mathbf{Q}$ (compare with the remark before 9.21 in [11]):

THEOREM 3.1. *Let $X \subseteq K^n$ be any affine homogeneous algebraic variety defined over $\mathbf{Q}$ and let H be any subspace of K^n defined over $\mathbf{Q}$ of codimension 1. Then, there exist integers d, l, r with $\min\{d, l\} > r \geqslant 0$ and an injective linear map defined over $\mathbf{Q}$,*

$$\theta: K^n \to M_{d,l},$$

which induces by restriction an isomorphism between $X \cap U$ and $M_{d,l}(r) \cap \theta(U)$, where U denotes the complement of H in K^n.

Given a point $x \in X(\mathcal{L})$ with $x \notin H$, the matrix $\theta(x)$ belongs to $M_{d,l}(r)(\mathcal{L})$ and Theorem 1.2 may apply to this matrix and bring some information on x. In this spirit, we deduce:

COROLLARY 3.2. *If Conjecture 1.1 is true for the variety $M_{d,l}(r)$ for any integers d, l, r with $\min\{d, l\} > r \geqslant 0$, then it is true for any affine homogeneous algebraic variety X defined over $\mathbf{Q}$.*

Proof. Let $X \subseteq K^n$ be an affine homogeneous algebraic variety defined over $\mathbf{Q}$, let $x \in X(\mathcal{L})$ and let S be the smallest subspace of K^n defined over $\mathbf{Q}$ which contains x.

We want to show $S\subseteq X$. This is certainly true if $x=0$. Otherwise, choose a subspace H of K^n defined over $\mathbf{Q}$ of codimension 1 with $x\notin H$ and consider the map θ given by Theorem 3.1. Since θ is injective and defined over $\mathbf{Q}$, we have $\theta(x)\in M_{d,l}(r)(\mathcal{L})$, and $\theta(S)$ is the smallest subspace of $M_{d,l}$ defined over $\mathbf{Q}$ which contains $\theta(x)$. If Conjecture 1.1 is true for the variety $M_{d,l}(r)$, this implies $\theta(S)\subseteq M_{d,l}(r)$, so $S\cap U\subseteq X$, and thus $S\subseteq X$ because $S\cap U$ is Zariski dense in S.

For the proof of Theorem 3.1, we need:

PROPOSITION 3.3. *Let R be a Noetherian ring and let I be an ideal of $R[Y_1,\dots,Y_m]$. Then, there exist integers d,l,r with $\min\{d,l\}>r\geqslant 0$ and a $d\times l$ matrix M with entries in $R+RY_1+\dots+RY_m$ such that I is generated by the minors of order $r+1$ of M.*

Proof. We first observe that, if E and F are R-submodules of $R[Y_1,\dots,Y_m]$, and if N is a matrix with coefficients in the submodule EF of $R[Y_1,\dots,Y_m]$ generated by the products fg with $f\in E$ and $g\in F$, then N can be written (in a non-unique way) as the product AB of a matrix A with coefficients in E by a matrix B with coefficients in F. We also observe that, if A,B are matrices with coefficients in $R[Y_1,\dots,Y_m]$ of respective sizes $d\times s$ and $s\times l$, and if t is an integer $\geqslant 0$, then the ideal J of $R[Y_1,\dots,Y_m]$ generated by the minors of order $t+1$ of the product AB coincides with the ideal generated by the minors of order $s+t+1$ of the matrix

$$\begin{pmatrix} I_s & B \\ -A & 0 \end{pmatrix},$$

where I_s denotes the $s\times s$ identity matrix. To see this, multiply this matrix on the left by

$$\begin{pmatrix} I_s & 0 \\ A & I_d \end{pmatrix}$$

and on the right by

$$\begin{pmatrix} I_s & -B \\ 0 & I_l \end{pmatrix}$$

where I_d and I_l are respectively the $d\times d$ and $l\times l$ identity matrices. Since these matrices have determinant 1, this does not change the ideal generated by the minors of order $s+t+1$. The result is the matrix

$$\begin{pmatrix} I_s & 0 \\ 0 & AB \end{pmatrix}$$

for which it is simpler to verify our claim.

For each integer $k\geqslant 1$, we denote by E_k the R-submodule of $R[Y_1,\dots,Y_m]$ consisting of all polynomials of degree $\leqslant k$. We thus have $E_1=R+RY_1+\dots+RY_m$ and $E_k=E_1E_{k-1}$ for each integer $k\geqslant 2$. So, the preceding observations imply that, for each integer $k\geqslant 2$, each integer $t \geqslant 0$ and each matrix N with coefficients in E_k, there exist a matrix M with coefficients in E_{k-1} and an integer $r \geqslant 0$ such that the ideal generated by the minors of order $t+1$ of N coincides with the ideal generated by the minors of order $r+1$ of M. By induction on k, this matrix M can also be taken with coefficients in E_1. The conclusion follows by choosing $t=0$ and N to be any matrix whose coefficients generate the ideal I.

Proof of Theorem 3.1. Without loss of generality, we may assume that H is the subspace of K^n defined by $Y_n=0$. Let E be the translate of H defined by $Y_n=1$, and let I be the ideal of all polynomials of $\mathbf{Q}[Y_1, ..., Y_{n-1}]$ vanishing identically on $X \cap E$. Put $m=n-1$ and let d, l, r and M be as given by Proposition 3.3 for this choice of I. Viewing the coefficients of M as affine linear functions on E, we get an affine linear map $\phi: E \to M_{d,l}$ defined over $\mathbf{Q}$ for which $X \cap E = \phi^{-1}(M_{d,l}(r))$. If $0 \notin \phi(E)$ and if ϕ is injective, the linear map $\theta: K^n \to M_{d,l}$ which extends ϕ has all the required properties. Otherwise, we can rectify the situation by replacing M by

$$\begin{pmatrix} L & 0 \\ 0 & M \end{pmatrix}$$

where L is the row matrix $(1, Y_1, ..., Y_{n-1})$, and by replacing d, l and r by $d+1$, $l+n$ and $r+1$ respectively.

Remark. Proposition 3.3 also shows that any affine algebraic variety defined over $\mathbf{Q}$ is isomorphic to a linear determinantal variety via an affine linear map defined over $\mathbf{Q}$. Therefore, if Conjecture 1.1 is true for all translates $A+M_{d,l}(r)$ with $A \in M_{d,l}(\mathbf{Q})$, then it is true for all affine algebraic varieties defined over $\mathbf{Q}$ and therefore it is true in general (see also [17]).

3.2. Homogeneous surfaces

The preceding sections show how Theorem 1.2 can be applied in order to study the points with coordinates in $\mathcal{L}$ on homogeneous affine algebraic varieties defined over $\mathbf{Q}$. This method however has its limits. When $X \subseteq K^3$ is an absolutely irreducible homogeneous surface defined over $\mathbf{Q}$ of degree $\geqslant 2$, it cannot lead to a proof of Conjecture 1.1 for X. In particular, it cannot lead to a proof of the four exponentials conjecture: take for X the zero set of $xy-z^2$. Indeed, the conjecture predicts that $X(\mathcal{L})$ does not contain any point whose coordinates are linearly independent over $\mathbf{Q}$. However, X contains infinitely many points $(\lambda_1, \lambda_2, \lambda_3)$ whose coordinates are linearly independent over $\overline{\mathbf{Q}}$ and we cannot exclude the possibility that these points belong to $X(\mathcal{L})$ because for each linear local embedding of X into some $M_{d,l}(r)$, the image of those points are matrices which formally satisfy Theorem 1.2. This follows from the following result (see [17] for other related results):

5-950414 *Acta Mathematica* 175. Imprimé le 1 septembre 1995

THEOREM 3.4. *Let d, l be positive integers, let $\lambda_1, \lambda_2, \lambda_3$ be elements of K which are linearly independent over $\overline{\mathbf{Q}}$, and let M be a $d \times l$ matrix with coefficients in $\langle \lambda_1, \lambda_2, \lambda_3 \rangle_{\mathbf{Q}}$. Assume that the rows of M are $\mathbf{Q}$-linearly independent and that its columns are $\mathbf{Q}$-linearly independent. Then its rank r satisfies $4r \geqslant d+l$ and so $r(d+l) \geqslant dl$.*

Proof. Let $L_0 = \langle \lambda_1, \lambda_2, \lambda_3 \rangle_{\mathbf{Q}}$ and let E be the $\mathbf{Q}$-subspace of L_0^l generated by the rows of M. For each non-zero $u \in E$, consider the smallest subspace U of K^l defined over $\mathbf{Q}$ containing u. Among those u, choose u_1 such that the dimension of U is minimal, and put

$$d_1 = \dim_{\mathbf{Q}}(E \cap U), \quad l_1 = \dim_K U, \quad r_1 = \dim_K \langle E \cap U \rangle_K.$$

We claim that $d_1 + l_1 \leqslant 4r_1$.

To prove this inequality, let L_1 be the $\mathbf{Q}$-subspace of L_0 generated by the coordinates of u_1. Since $l_1 = \dim_{\mathbf{Q}} L_1$, we have $l_1 \leqslant 3$. Moreover, let $\phi: U \to K$ be any non-zero linear form on U defined over $\mathbf{Q}$. By the choice of u_1, we have $E \cap \ker \phi = 0$. Since $\phi(E \cap U) \subseteq L_0$, this implies $d_1 \leqslant 3$, thus $d_1 + l_1 \leqslant 4r_1$ in the case $r_1 \geqslant 2$. Assume $r_1 = 1$. Then, each element of $E \cap U$ is of the form tu_1 where $t \in K$ satisfies $tL_1 \subseteq L_0$. Since $\lambda_1, \lambda_2, \lambda_3$ are linearly independent over $\overline{\mathbf{Q}}$, the dimension over $\mathbf{Q}$ of the set of all $t \in K$ such that $tL_1 \subseteq L_0$ is 1 if $l_1 = 3$, $\leqslant 2$ if $l_1 = 2$ and $\leqslant 3$ if $l_1 = 1$. This implies $d_1 + l_1 \leqslant 4$ in all cases.

If $r_1 = r$, we have $U = K^l$, so $d_1 = d$, $l_1 = l$ and the theorem is proved. Otherwise, choose $P \in \mathrm{GL}_d(\mathbf{Q})$ such that the first d_1 rows of PM form a basis of $E \cap U$ over $\mathbf{Q}$. Then, choose $Q \in \mathrm{GL}_l(\mathbf{Q})$ such that

$$PMQ = \begin{pmatrix} M_1 & 0 \\ * & M_2 \end{pmatrix}$$

where M_1 is a $d_1 \times l_1$ matrix of rank r_1. Since the rank r_2 of M_2 is $\leqslant r - r_1$, we may assume, by induction on r, that $(d-d_1)+(l-l_1) \leqslant 4r_2$. This gives $d+l \leqslant 4r$ as announced.

4. Construction of an auxiliary function on an algebraic variety

We present here a construction of an auxiliary function which generalizes an earlier result of M. Waldschmidt (Theorems 3.1 and 3.1.p of [21]). We consider simultaneously both the Archimedean case where $K = \mathbf{C}$ and the p-adic case where $K = \mathbf{C}_p$. We also give an application of this construction.

First, we fix a closed locally compact subfield $\mathcal{K}$ of K and we denote by $\mathcal{K}_0$ the topological closure of $\mathbf{Q}$ in K. In the Archimedean case, $\mathcal{K}_0$ is $\mathbf{R}$ and $\mathcal{K}$ is $\mathbf{R}$ or $\mathbf{C}$. In the p-adic case, $\mathcal{K}_0$ is $\mathbf{Q}_p$ and $\mathcal{K}$ is an algebraic extension of $\mathbf{Q}_p$ of finite degree. In both cases, we denote by ν the degree of $\mathcal{K}$ over $\mathcal{K}_0$. We also fix a positive integer d. For each d-tuple $r=(r_1,\dots,r_d)$ of non-negative real numbers, we denote by $B(r)$ the closed polydisc

$$B(r)=\{(z_1,\dots,z_d)\in K^d : |z_i|\leqslant r_i \text{ for } 1\leqslant i\leqslant d\}$$

and, when F is a function defined on $B(r)$ with values in K, we write

$$|F|_r=\sup\{|F(z)| : z\in B(r)\}.$$

Finally, if I is an ideal of $\mathcal{K}[Y_1,\dots,Y_d]$, we denote by $H(I;T)$ the Hilbert function of I. Its value at a real number $T\geqslant 0$ is the dimension over $\mathcal{K}$ of the quotient of the $\mathcal{K}$-vector space $\mathcal{E}$ consisting of all polynomials of $\mathcal{K}[Y_1,\dots,Y_d]$ of degree $\leqslant T$ modulo the subspace $\mathcal{F}=\mathcal{E}\cap I$. For all integers T sufficiently large, $H(I;T)$ is given by a polynomial in T whose degree is equal to the dimension of the zero set of I in K^d.

THEOREM 4.1. *Let d and L be positive integers, let I be an ideal of $\mathcal{K}[Y_1,\dots,Y_d]$, let S, U be positive real numbers, let $r=(r_1,\dots,r_d)$ be a d-tuple of positive real numbers, and let $\phi_1,\dots,\phi_L$ be a family of K-valued continuous functions on $B(er)$ which are analytic in the interior of $B(er)$ and which map $\mathcal{K}^d\cap B(er)$ to $\mathcal{K}$. Assume*

$$3\leqslant U,\quad S\leqslant U\quad \textit{and}\quad \sum_{\lambda=1}^{L}|\phi_\lambda|_{er}\leqslant e^U$$

in the Archimedean case, and

$$\log p\leqslant U,\quad S\leqslant U\quad \textit{and}\quad \max\{|\phi_\lambda|_{er} : \lambda=1,\dots,L\}\leqslant e^U$$

in the p-adic case. Assume also

$$LS\geqslant 4\nu U H(I;4U).$$

Then, there exist integers $p_1,\dots,p_L$ not all zero, with $-e^S\leqslant p_1,\dots,p_L\leqslant e^S$, and a polynomial $Q\in I$ such that

$$\left|\sum_{\lambda=1}^{L}p_\lambda\phi_\lambda-Q\right|_r\leqslant e^{-U}.$$

The construction of M. Waldschmidt mentioned above corresponds to the special case of this result when $I=0$. The proof of our result follows the same lines. We start by establishing a Siegel lemma:

LEMMA 4.2. *Let b, B be positive real numbers with $b\leqslant B$, let $\mathcal{E}$ be a finite-dimensional vector space over $\mathcal{K}$ equipped with a norm $\|\cdot\|$, let $\mathcal{F}$ be a subspace of $\mathcal{E}$, and let $(x_i)_{i\in J}$ be a family of elements in $\mathcal{E}$ of norm $\leqslant B$. Assume that*

$$\operatorname{card}(J)>\varrho^{\nu\dim_{\mathcal{K}}(\mathcal{E}/\mathcal{F})} \tag{4.1}$$

where $\varrho=1+2B/b$ in the Archimedean case and $\varrho=pB/b$ in the p-adic case. Then, there exist $i,j\in J$ with $i\neq j$ and $y\in\mathcal{F}$ such that $\|x_i-x_j-y\|\leqslant b$.

Proof. Assume first that $\mathcal{F}=0$. We choose a Haar measure on $\mathcal{E}$ and consider the closed balls

$$\mathcal{C}_0=\{x\in\mathcal{E}:\|x\|\leqslant r_0\}\quad\text{and}\quad \mathcal{C}=\{x\in\mathcal{E}:\|x\|\leqslant r\}$$

where $r_0=\frac{1}{2}b$ and $r=B+\frac{1}{2}b$ in the Archimedean case, and $r_0=b$ and $r=B$ in the p-adic case. By hypothesis, the translates $x_i+\mathcal{C}_0$ with $i\in J$ are all contained in $\mathcal{C}$ and their volumes are equal to the volume of $\mathcal{C}_0$. Now, choose $\alpha\in\mathcal{K}$ with $|\alpha|=\varrho$ if $K=\mathbf{C}$, or with $\varrho\geqslant|\alpha|\geqslant\varrho/p$ if $K=\mathbf{C}_p$. Since multiplication by α maps $\mathcal{C}_0$ to a ball which contains $\mathcal{C}$, we obtain

$$\mathrm{vol}(\mathcal{C})\leqslant|\alpha|^{\nu\dim_{\mathcal{K}}(\mathcal{E})}\,\mathrm{vol}(\mathcal{C}_0)<\sum_{i\in J}\mathrm{vol}(x_i+\mathcal{C}_0).$$

There must therefore exist distinct elements i,j of J for which the balls $x_i+\mathcal{C}_0$ and $x_j+\mathcal{C}_0$ intersect. This implies $\|x_i-x_j\|\leqslant b$ and proves the lemma when $\mathcal{F}=0$.

In the general case, let $\pi:\mathcal{E}\to\mathcal{E}/\mathcal{F}$ be the canonical projection. We give $\mathcal{E}/\mathcal{F}$ the quotient norm $\|\cdot\|'$ defined by

$$\|z\|'=\inf\{\|x\|:x\in\pi^{-1}(z)\}$$

for all $z\in\mathcal{E}/\mathcal{F}$. Since $\|\pi(x_i)\|'\leqslant\|x_i\|\leqslant B$ for all $i\in J$, the special case of the lemma proved above applies to the quotient $\mathcal{E}/\mathcal{F}$ and to the family of points $(\pi(x_i))_{i\in J}$ for the same values of b and B. There thus exist distinct $i,j\in J$ such that $\|\pi(x_i)-\pi(x_j)\|'\leqslant b$ and, for this choice of i and j, there exists $y\in\mathcal{F}$ such that $\|x_i-x_j-y\|\leqslant b$.

To state the analytic estimates which we need, we recall the notations of [21]. For each $t=(t_1,\dots,t_d)\in\mathbf{N}^d$ and each $z=(z_1,\dots,z_d)\in K^d$, we put $t!=t_1!\dots t_d!$, $\|t\|=t_1+\dots+t_d$, $z^t=z_1^{t_1}\dots z_d^{t_d}$ and $D^t=(\partial^{t_1}/\partial z_1^{t_1})\dots(\partial^{t_d}/\partial z_d^{t_d})$.

LEMMA 4.3. *Let d,T be positive integers, let $r=(r_1,\dots,r_d)$ be a d-tuple of positive real numbers, and let $F:B(er)\to K$ be a continuous function which is analytic in the interior of $B(er)$. We put*

$$f(z)=\sum_{\|t\|<T}\frac{1}{t!}D^tF(0)z^t.$$

Then, we have

$$|F-f|_r\leqslant e^{-T}|F-f|_{er},\tag{4.2}$$

and also

$$|f|_{er}\leqslant\begin{cases}\sqrt{T}\cdot|F|_{er} & \text{if } K=\mathbf{C},\\ |F|_{er} & \text{if } K=\mathbf{C}_p.\end{cases}\tag{4.3}$$

Proof. The first inequality follows from Schwarz's lemma. In the Archimedean case, the second one is a consequence of Parseval's inequality as in the proof of Lemma 3.4 of [21]; for the p-adic case, see §3 of the second part of [21].

Proof of Theorem 4.1. Let $T=[4U]+1$. We denote by $\mathcal{E}$ the subspace of $\mathcal{K}[Y_1, ..., Y_d]$ consisting of all polynomials of degree $<T$ and we put $\mathcal{F}=\mathcal{E}\cap I$. The dimension of $\mathcal{E}/\mathcal{F}$ over $\mathcal{K}$ is thus $H(I;4U)$. We equip $\mathcal{E}$ with the supremum norm on $B(r)$. We also denote by J the set of all $(p_1, ..., p_L)\in \mathbf{Z}^L$ with $0\leqslant p_\lambda \leqslant e^S$ for $1\leqslant \lambda \leqslant L$, and, to each $(p_1, ..., p_L)\in J$, we associate the polynomial

$$\sum_{\lambda=1}^{L} p_\lambda \sum_{\|t\|<T} \frac{1}{t!} D^t \phi_\lambda(0)\cdot Y^t.$$

This defines a family of elements of $\mathcal{E}$ indexed by J because, for each $\lambda=1, ..., L$, the function ϕ_λ maps $\mathcal{K}^d \cap B(er)$ to $\mathcal{K}$ and so its derivatives $D^t\phi_\lambda(0)$ all belong to $\mathcal{K}$. In the Archimedean case, the inequality (4.3) applied to the functions ϕ_λ together with the hypothesis $\sum |\phi_\lambda|_{er} \leqslant e^U$ shows that the norm of these elements of $\mathcal{E}$ is $\leqslant \sqrt{T}\, e^{S+U}$. In this case, we put $b=\frac{1}{2}e^{-U}$ and $B=\sqrt{T}\,e^{S+U}$. This gives

$$1+2B/b=1+4\sqrt{T}\,e^{S+2U} \leqslant 1+4\sqrt{4U+1}\cdot e^{3U} \leqslant e^{4U},$$

since $T\leqslant 4U+1$, $S\leqslant U$ and $U\geqslant 3$. In the p-adic case, the same inequality (4.3) applied to the same functions together with the hypothesis $\max |\phi_\lambda|_{er} \leqslant e^U$ shows that the norm of the same elements of $\mathcal{E}$ is $\leqslant e^U$. We then put $b=e^{-U}$ and $B=e^U$. This gives

$$pB/b=pe^{2U} \leqslant e^{3U}$$

since $U\geqslant \log p$. In both cases, the number ϱ of Lemma 4.2 is bounded above by e^{4U} and the main condition of this lemma is fulfilled since

$$\varrho^{\nu \dim_{\mathcal{K}}(\mathcal{E}/\mathcal{F})} \leqslant e^{4\nu U H(I;4U)} \leqslant e^{LS} < \mathrm{card}(J).$$

This lemma thus applies and shows that there exist integers $p_1, ..., p_L$ not all zero, of absolute value $\leqslant e^S$, and a polynomial $Q\in I$ of degree $<T$, such that the polynomial

$$f(Y)=\sum_{\lambda=1}^{L} p_\lambda \sum_{\|t\|<T} \frac{1}{t!} D^t \phi_\lambda(0)\cdot Y^t$$

satisfies $|f-Q|_r \leqslant b$. For this choice of integers $p_1, ..., p_L$, we put

$$F=\sum_{\lambda=1}^{L} p_\lambda \phi_\lambda.$$

In the Archimedean case, we obtain, by Lemma 4.3,

$$\begin{aligned}|F-Q|_r &\leqslant |f-Q|_r+|F-f|_r\\ &\leqslant \tfrac{1}{2}e^{-U}+e^{-T}|F-f|_{er}\\ &\leqslant \tfrac{1}{2}e^{-U}+\bigl(1+\sqrt{T}\bigr)e^{-T}|F|_{er}\end{aligned}$$

and, since $|F|_{er}\leqslant e^S\sum|\phi_\lambda|_{er}\leqslant e^{2U}$, this gives

$$|F-Q|_r\leqslant \tfrac{1}{2}e^{-U}+\bigl(1+\sqrt{4U+1}\bigr)e^{-2U}\leqslant e^{-U}$$

as required. In the p-adic case, using the same lemma, we obtain

$$\begin{aligned}|F-Q|_r &\leqslant \max\{|f-Q|_r,\ |F-f|_r\}\\ &\leqslant \max\{e^{-U},\ e^{-T}|F-f|_{er}\}\\ &\leqslant \max\{e^{-U},\ e^{-T}|F|_{er}\}.\end{aligned}$$

Since $|F|_{er}\leqslant \max|\phi_\lambda|_{er}\leqslant e^U$, this implies $|F-Q|_r\leqslant e^{-U}$ as required.

For each $\alpha\in\overline{\mathbf{Q}}$, we denote by $h(\alpha)$ the absolute logarithmic height of α equal to $[\mathbf{Q}(\alpha):\mathbf{Q}]^{-1}\log M(\alpha)$ where $M(\alpha)$ is the Mahler measure of α. As in §1, we also denote by $\mathcal{U}$ the disc of convergence of the exponential series in K. Theorem 4.1 then implies:

THEOREM 4.4. *Let n,d be positive integers with $n<d$, let X be an algebraic subvariety of K^d defined over $\mathcal{K}$ of dimension n, let $\mathcal{L}_0$ be a finitely generated subgroup of $\mathcal{L}\cap\mathcal{K}$ contained in $\mathcal{U}$, and let $\delta_1,\dots,\delta_d$, $\varrho_1,\dots,\varrho_d$ be non-negative real numbers with*

$$\delta_1+\dots+\delta_d>n\cdot\max\{\varrho_1+\delta_1,\dots,\varrho_d+\delta_d\}.$$

Then, for each sufficiently large integer $N>0$, there exists a non-zero polynomial

$$P_N(Y_1,\dots,Y_d)\in\mathbf{Z}[Y_1,\dots,Y_d]$$

of degree $\leqslant N^{\delta_i}$ in Y_i for $i=1,\dots,d$, which satisfies

$$P_N(\exp(x_1),\dots,\exp(x_d))=0$$

for all $(x_1,\dots,x_d)\in X\cap\mathcal{L}_0^d$ with $|x_i|\leqslant N^{\varrho_i}$ and $h(\exp(x_i))\leqslant N^{\varrho_i}$ for $i=1,\dots,d$.

Proof. Let $s=\max\{\varrho_1+\delta_1,\dots,\varrho_d+\delta_d\}$ and let I be the ideal of all polynomials of $\mathcal{K}[Y_1,\dots,Y_d]$ vanishing on X. Since X is defined over $\mathcal{K}$, X is the zero set of I and therefore we have $H(I;T)\leqslant cT^n$ for some constant $c>0$ and all $T>1$. In the Archimedean case, we apply Theorem 4.1 with the parameters $S=N^s$, $U=N^s\log N$, $r=(N^{\varrho_1},\dots,N^{\varrho_d})$ and the functions

$$\exp(\lambda_1 z_1+\dots+\lambda_d z_d)\quad (0\leqslant\lambda_1\leqslant N^{\delta_1},\dots,0\leqslant\lambda_d\leqslant N^{\delta_d}).$$

In the p-adic case, we choose a real number $r_0>0$ such that the closed disc $B(er_0)$ of $\mathbf{C}_p$ is contained in $\mathcal{U}$ and an integer $m\geqslant 0$ such that $p^m\mathcal{L}_0\subseteq B(r_0)$. We then apply Theorem 4.1 with the parameters $S=N^s$, $U=N^s\log N$, $r=(p^m r_0,\dots,p^m r_0)$ and the functions

$$\exp(\lambda_1 p^m z_1+\dots+\lambda_d p^m z_d)\quad (0\leqslant\lambda_1\leqslant p^{-m}N^{\delta_1},\dots,0\leqslant\lambda_d\leqslant p^{-m}N^{\delta_d}).$$

For any large enough integer N, the conditions of this theorem are fulfilled and therefore, there exists a non-zero polynomial $P_N\in\mathbf{Z}[Y_1,\dots,Y_d]$ of height $\leqslant e^S$ and degree $\leqslant N^{\delta_i}$ in Y_i for $i=1,\dots,d$, such that the function

$$F_N(z_1,\dots,z_d)=P_N(\exp(z_1),\dots,\exp(z_d))$$

satisfies

$$\sup\{|F_N(z)|: z\in X\cap B(r)\}\leqslant e^{-U}.$$

Let $x=(x_1,\dots,x_d)\in X\cap\mathcal{L}_0^d$ with $|x_i|\leqslant N^{\varrho_i}$ and $h(\exp(x_i))\leqslant N^{\varrho_i}$ for $i=1,\dots,d$. It remains to show $F_N(x)=0$ independently of the choice of x when N is large enough. Since $x\in X\cap B(r)$, we have $|F_N(x)|\leqslant e^{-U}$. On the other hand, $F_N(x)$ belongs to the extension E of $\mathbf{Q}$ generated by the numbers $\exp(\lambda)$ with $\lambda\in\mathcal{L}_0$. Since E has finite degree over $\mathbf{Q}$, Liouville's inequality together with $|F_N(x)|\leqslant e^{-U}$ implies $F_N(x)=0$ if $U>[E:\mathbf{Q}]h(F_N(x))$. This is true for large enough N because

$$\begin{aligned} h(F_N(x)) &\leqslant \log\Big(e^S\prod_{i=1}^d (N^{\delta_i}+1)\Big)+\sum_{i=1}^d N^{\delta_i}h(\exp(x_i))\\ &\leqslant S+\sum_{i=1}^d N^{\delta_i}+\sum_{i=1}^d N^{\delta_i+\varrho_i}\leqslant (2d+1)S. \end{aligned}$$

Thus, for sufficiently large values of N, the polynomial P_N has all the required properties.

Application. Let k,m be integers with $m\geqslant k+2\geqslant 4$ and let $X=G(k,K^m)$. Put $d=\binom{m}{k}$, and identify $\bigwedge^k K^m$ with K^d by the choice of a basis taken in $\bigwedge^k\mathbf{Q}^m$. Then, X becomes a subvariety of K^d of dimension $n=k(m-k)+1$ (Lecture 11 of [11]). Now, choose a point $y=v_1\wedge\dots\wedge v_k$ in $X(\mathcal{L})$. Assume that the coordinates of y in K^d belong to $\mathcal{U}$ and are linearly independent over $\mathbf{Q}$. Denote by $\mathcal{L}_0$ the subgroup of $\mathcal{L}$ that they generate. We get a map

$$\begin{aligned} \sigma\colon \mathrm{GL}_m(\mathbf{Z}) &\to X(\mathcal{L}_0)\\ A &\mapsto \Big(\bigwedge\nolimits^k A\Big)(y)=Av_1\wedge\dots\wedge Av_k. \end{aligned}$$

For each integer $N \geqslant 1$, denote by S_N the image under σ of the set of all elements of $\mathrm{GL}_m(\mathbf{Z})$ with entries in $\{0, ..., N\}$. Finally, choose real numbers δ and ϱ with

$$\varrho > k \quad \text{and} \quad \delta > \frac{n\varrho}{d-n}.$$

There exists a constant $c_1 > 0$ such that each $(x_1, ..., x_d) \in S_N$ satisfies both $|x_i| \leqslant c_1 N^k$ and $h(\exp(x_i)) \leqslant c_1 N^k$ for $i = 1, ..., d$. Thus, for large enough values of N, Theorem 4.4 shows that there exists a non-zero polynomial $P_N \in \mathbf{Z}[Y_1, ..., Y_d]$ of degree $\leqslant N^\delta$ in each variable, which satisfies

$$P_N(\exp(x_1), ..., \exp(x_d)) = 0 \quad \text{for each } (x_1, ..., x_d) \in S_N.$$

If we view this as a system of linear equations in the coefficients of P_N, then the preceding statement is non-trivial as soon as the cardinality of S_N exceeds the upper bound $(N^\delta + 1)^d$ for the number of coefficients of P_N. Now, the map σ is injective on the set of elements of $\mathrm{GL}_m(\mathbf{Z})$ with entries $\geqslant 0$ because, if matrices $A, B \in \mathrm{GL}_m(\mathbf{Z})$ satisfy $\sigma(A) = \sigma(B)$, then the hypotheses on y imply $\bigwedge^k A = \bigwedge^k B$. Thus, they satisfy $A(U) = B(U)$ for each subspace U of K^m of dimension k. Since $0 < k < m$ and since A and B are invertible, they also satisfy the same condition for each subspace U of K^m of dimension 1. From this we deduce $A = \lambda B$ with $\lambda \in K$. Thus $\lambda^k = 1$ and so $A = B$ if A and B have entries $\geqslant 0$. Note also that the set of elements of $\mathrm{GL}_m(\mathbf{Z})$ with entries in $\{0, ..., N\}$ has cardinality $\geqslant c_2 N^{m^2}$ for some constant $c_2 > 0$. The cardinality of S_N is thus $\geqslant c_2 N^{m^2}$, and the existence of P_N becomes non-trivial for large values of N when $m^2 > d\delta$. This condition is achieved for suitable choices of ϱ and δ if

$$\frac{m^2}{d} > \frac{nk}{d-n}. \tag{4.4}$$

This in turn is verifed when $m \geqslant k^2 + 2k$ because, since $n < k(m-1)$, we have for such values of m

$$m^2 - nk > m^2 - k^2(m-1) > 2mk,$$

and thus

$$d(m^2 - nk) > \binom{m}{2} 2mk = m^2(m-1)k > m^2 n.$$

A more careful computation in the case $k = 2$ shows that (4.4) is verified for all $m \geqslant 7$. However, the present zero estimates which deal with non-commutative algebraic groups do not lead to the expected contradiction for these values of m (see [14]).

Acknowledgements. This research was completed during a special half year in Transcendence at the Mathematical Sciences Research Institute in Berkeley during winter 1993. The author thanks the organizers A. Baker, W. D. Brownawell, W. Schmidt and P. Vojta for their invitation. He also thanks M. Waldschmidt for his advice concerning many aspects of this work.

References

[1] ATKINSON, M. D., Primitive spaces of matrices of bounded rank, II. *J. Austral. Math. Soc. Ser. A*, 34 (1983), 306–315.

[2] BAKER, A., Linear forms in logarithms of algebraic numbers, I, II, III. *Mathematika*, 13 (1966), 204–216; 14 (1967), 102–107; 14 (1967), 220–228.

[3] BEASLEY, L. B., The null space of spaces of singular matrices. *Linear and Multilinear Algebra*, 18 (1985), 249–254.

[4] BOURBAKI, N., *Éléments de mathématiques. Algèbre,* chapitre 2. Hermann, Paris, 1970.

[5] BROWNAWELL, W. D., The algebraic independence of certain numbers related by the exponential function. *J. Number Theory*, 6 (1974), 22–31.

[6] BRUMER, A., On the units of algebraic number fields. *Mathematika*, 14 (1967), 121–124.

[7] COATES, J., An effective p-adic analogue of a theorem of Thue (I). *Acta Arith.*, 15 (1969), 279–305.

[8] EISENBUD, D. & HARRIS, J., Vector spaces of matrices of low rank. *Adv. in Math.*, 70 (1988), 135–155.

[9] FILLMORE, P., LAURIE, C. & RADJAVI, H., On matrix spaces with zero determinant. *Linear and Multilinear Algebra*, 18 (1985), 255–266.

[10] FLANDERS, H., On spaces of linear transformations with bounded rank. *J. London Math. Soc.*, 37 (1962), 10–16.

[11] HARRIS, J., *Algebraic Geometry: A First Course.* Springer-Verlag, New York, 1992.

[12] LANG, S., Nombres transcendants, in *Séminaire Bourbaki*, volume 1965/66, exposé 305. W. A. Benjamin, New York–Amsterdam, 1966.

[13] — *Introduction to Transcendental Numbers.* Addison-Wesley, Reading, MA, 1966.

[14] NAKAMAYE, M., Multiplicity estimates and the product theorem. To appear.

[15] RAMACHANDRA, K., Contributions to the theory of transcendental numbers. *Acta Arith.*, 14 (1968), 65–88.

[16] ROY, D., Matrices whose coefficients are linear forms in logarithms. *J. Number Theory*, 41 (1992), 22–47.

[17] — Sur la conjecture de Schanuel pour les logarithmes des nombres algébriques, in *Groupe d'étude sur les problèmes diophantiens* 1988/89. Publ. Math. Univ. Paris VI, 90.

[18] SPRINDŽUK, V. G., Concerning Baker's theorem on linear forms in logarithms. *Dokl. Akad. Nauk. BSSR*, 11 (1967), 767–769.

[19] — Estimates of linear forms with p-adic logarithms of algebraic numbers. *Vestsī Akad. Navuk BSSR Ser. Fīz.-Mat. Navuk*, 4 (1968), 5–14.

[20] WALDSCHMIDT, M., Solution du huitième problème de Schneider. *J. Number Theory*, 5 (1973), 191–202.

[21] — Transcendance et exponentielles en plusieurs variables. *Invent. Math.*, 63 (1981), 97–127.

[22] — Dependence of logarithms of algebraic points. *Colloq. Math. Soc. János Bolyai*, 51 (1987), 1013–1035.

DAMIEN ROY
Département de mathématiques
Université d'Ottawa
585 King Edward
Ottawa, Ontario
Canada K1N 6N5
droy@mathstat.uottawa.ca

Received November 18, 1993