ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 26, Number 3, Summer 1996

DEPENDENCE OF LOGARITHMS ON COMMUTATIVE ALGEBRAIC GROUPS

MICHEL WALDSCHMIDT

Dedicated to Wolfgang M. Schmidt on the occasion of his sixtieth birthday

ABSTRACT. A well-known conjecture states that linearly independent logarithms of algebraic numbers are algebraically independent over the field of rational numbers. So far, it is not yet known that there exist two algebraically independent logarithms of algebraic numbers. On the other hand, D. Roy has shown that the above conjecture is equivalent to a conjectural description of the rank of matrices whose entries are either algebraic numbers or else logarithms of algebraic numbers. From this point of view, half of the conjecture is known: the actual rank of such a matrix is at least half the conjectural rank.

We consider a similar question for commutative algebraic groups. We show a connection with a density problem, and we prove a partial result by means of the theorem of the algebraic subgroup.

1. The multiplicative group: usual logarithms.

Here is the main conjecture for (usual) logarithms of algebraic numbers:

Conjecture 1. *Let $l_1, \dots, l_n$ be complex numbers which are linearly independent over the field $\mathbf{Q}$ of rational numbers. Assume that the n numbers e^{l_i}, $1 \le i \le n$, are algebraic (over $\mathbf{Q}$). Then $l_1, \dots, l_n$ are algebraically independent (over $\mathbf{Q}$).*

As a matter of notations, we shall denote by $\overline{\mathbf{Q}}$ the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$, and by $\mathcal{L}$ the $\mathbf{Q}$-vector space

$$\exp^{-1}(\overline{\mathbf{Q}}^*) = \{z \in \mathbf{C}; e^z \in \overline{\mathbf{Q}}^*\};$$

Received by the editors on December 20, 1994, and in revised form on May 26, 1995.
AMS *Mathematics Subject Classification.* Primary. 11J81, 14L10, Secondary. 11J85, 11J89.

the elements of $\mathcal{L}$ are the *logarithms of algebraic numbers*. It will be convenient to denote by $\log \alpha$ the elements of $\mathcal{L}$, but we insist that we do not fix a determination of the complex logarithm.

Each nonzero element of $\mathcal{L}$ is a transcendental number; this is the Hermite-Lindemann theorem. On the other hand, it is not yet known that there exist two elements in $\mathcal{L}$ which are algebraically independent.

This failure in all attempts to get a result of algebraic independence suggests that one should consider Conjecture 1 from a different point of view. For instance, fix a polynomial $P \in \mathbf{Q}[X_1, \dots, X_n]$; what can be said of the set of $\lambda \in \mathcal{L}^n$ such that $P(\lambda) = 0$? This question amounts to asking, what is the intersection of $\mathcal{L}^n$ with a hypersurface $P = 0$ in an affine space $\mathbf{C}^n$? In place of a hypersurface, one may consider any affine variety. With this point of view, Conjecture 1 can be restated in the following equivalent form (see [**8**, Conjecture 1]).

Conjecture 2. *Let n be a positive integer, X an algebraic affine subvariety of $\mathbf{C}^n$ defined over $\overline{\mathbf{Q}}$, P a point of X with coordinates in $\mathcal{L}$ and V the smallest vector subspace of $\mathbf{C}^n$ defined over $\mathbf{Q}$ which contains P. Then V is contained in X.*

According to this conjecture the set $X \cap \mathcal{L}^n$ should be contained in the union of all linear subspaces of $\mathbf{C}^n$ which are defined over $\mathbf{Q}$ and contained in X.

All that is known concerning this question is contained in [**8**]. Partial results are obtained there for the affine cone over the Grassmanian which parameterizes the subspaces of dimension k of $\mathbf{C}^m$. For instance the conjecture for this particular case of varieties X is reduced to the case $m = 4$ and $k = 2$, which can be stated as follows.

Conjecture 3. *Let $\mathbf{M}$ be a 4×4 skew-symmetric matrix, with entries in $\mathcal{L}$ and with $\mathbf{Q}$-linearly independent rows; assume that the $\mathbf{Q}$-vector space generated by the columns of $\mathbf{M}$ in $\mathbf{C}^4$ does not contain any nonzero element of $\mathbf{Q}^4$. Then the rank of $\mathbf{M}$ is ≥ 3.*

Here is a special case of Conjecture 3:

Conjecture 4 (Four exponentials conjecture). *Let*

$$\mathbf{M} = \begin{pmatrix} \log\alpha_{11} & \log\alpha_{12} \\ \log\alpha_{21} & \log\alpha_{22} \end{pmatrix}$$

be a 2×2 *matrix with entries in* $\mathcal{L}$*, with* $\mathbf{Q}$*-linearly independent rows and also* $\mathbf{Q}$*-linearly independent columns. Then the rank of* $\mathbf{M}$ *is* 2.

This follows from Conjecture 3 applied to the matrix

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

The situation for 3×3 matrices is not as simple as for 2×2 matrices; here is an example suggested by M. Langevin [**10**, p. 104]. The matrix

$$\begin{pmatrix} 0 & -\log 5 & \log 3 \\ \log 5 & 0 & -\log 2 \\ -\log 3 & \log 2 & 0 \end{pmatrix}$$

is of rank 2, and its rows are linearly independent, as well as its columns. The fact that the determinant of this matrix vanishes has nothing to do with the fact that the entries of $\mathbf{M}$ are in $\mathcal{L}$: the rank of the matrix

$$\begin{pmatrix} 0 & -Z & Y \\ Z & 0 & -X \\ -Y & X & 0 \end{pmatrix}$$

in $\mathbf{C}(X, Y, Z)$ is also 2.

Conjecture 1 yields a description of the rank of matrices with entries in $\mathcal{L}$ as follows (cf. [**8**]). Let $\mathbf{M} = (\lambda_{ij})$ be a matrix with entries in $\mathcal{L}$; choose a basis $\log\alpha_1, \dots, \log\alpha_n$ of the $\mathbf{Q}$-vector subspace of $\mathbf{C}$ generated by the entries $\log\alpha_{ij}$, and define matrices $\mathbf{M}_1, \dots, \mathbf{M}_n$ with rational entries by

$$\mathbf{M} = \mathbf{M}_1\log\alpha_1 + \cdots + \mathbf{M}_n\log\alpha_n.$$

Define the *structural rank* $r_{\mathrm{str}}(\mathbf{M})$ of $\mathbf{M}$ as the rank of the matrix

$$\mathbf{M}_1 X_1 + \cdots + \mathbf{M}_n X_n$$

in the field $\mathbf{C}(X_1, \dots, X_n)$ (this number $r_{\mathrm{str}}(\mathbf{M})$ clearly does not depend on the choice of the basis $\log\alpha_1, \dots, \log\alpha_n$). From Conjecture 1 one deduces:

Conjecture 5. *Let* $\mathbf{M}$ *be a matrix with entries in* $\mathcal{L}$; *then the rank of* $\mathbf{M}$ *is equal to* $r_{\mathrm{str}}(\mathbf{M})$.

In fact, it is plain that the full force of Conjecture 1 is not needed; only homogeneous polynomials come into the picture. Hence, it is sufficient to invoke the *homogeneous* (weaker) version of Conjecture 1. *Let* $\log\alpha_1, \dots, \log\alpha_n$ *be* $\mathbf{Q}$*-linearly independent elements of* $\mathcal{L}$, *and let* $P \in \mathbf{Q}[X_1, \dots, X_n]$ *be a nonzero homogeneous polynomial. Then* $P(\log\alpha_1, \dots, \log\alpha_n) \neq 0$.

An interesting fact is that this homogeneous version of Conjecture 1 is equivalent to Conjecture 5, thanks to part a) of the following result:

Lemma 6. *Let* A *be a* (*commutative*) *ring.*

a) *Denote by* $R = A[X_1, \dots, X_m]$ *the ring of polynomials in* m *variables with coefficients in* A. *Any element in* R *is the determinant of a matrix with entries in the* A*-module* $A + AX_1 + \cdots + AX_m$.

b) *Denote by* S *the ring* $A[X_1^{(1)}, \dots, X_n^{(m)}]$ *of polynomials in* mn *unknowns* $X_i^{(j)}$, $1 \le i \le n$, $1 \le j \le m$. *For* $j = 1, \dots, m$, *denote by* L_j *the sub-*A*-module of* S *generated by* $X_1^{(j)}, \dots, X_n^{(j)}$. *Then any element in* S *is the determinant of a matrix* M *of the form*

$$M = \begin{pmatrix} M_{00} & M_{01} \\ M_{10} & M_{11} \\ \vdots & \vdots \\ M_{m0} & M_{m1} \end{pmatrix}$$

where M_{ji} *has coefficients in* A *if either* i *or* j *vanishes, while* M_{j1} *has coefficients in* L_j *for* $j = 1, \dots, m$.

Proof. For the proof of part a), see D. Roy [**5**, Proposition 4] and [**8**, Proposition 3.3]. The proof of part b) which follows is also due to D. Roy (private communication). Let $P \in S$. According to a), $P = \det N$, where N is a matrix with coefficients in

$$A \oplus L_1 \oplus \cdots \oplus L_m.$$

Hence N can be written

$$N = N_0 + N_1 + \cdots + N_m,$$

where N_0 has coefficients in A and N_j has coefficients in L_j for $j = 1, \dots, m$. Denote by I the identity matrix having the same size as N. We have

$$\begin{aligned}\det \begin{pmatrix} I & I & \cdots & I & 0 \\ I & 0 & \cdots & 0 & N_0 \\ 0 & I & \cdots & 0 & N_1 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & I & N_m \end{pmatrix} &= \det \begin{pmatrix} 0 & 0 & \cdots & 0 & -N \\ I & 0 & \cdots & 0 & N_0 \\ 0 & I & \cdots & 0 & N_1 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & I & N_m \end{pmatrix} \\ &= \pm \det N.\end{aligned}$$

The matrix on the lefthand side has the required property.

Notice that the previous identity can be seen as a consequence of the relation:

$$N = \begin{pmatrix} N_0 & N_1 & \cdots & N_m \end{pmatrix} \begin{pmatrix} I \\ I \\ \vdots \\ I \end{pmatrix}. \qquad \square$$

Using Lemma 6, we deduce the homogeneous version of Conjecture 1 from Conjecture 5 as follows. Let $P \in \mathbf{Q}[X_1, \dots, X_n]$ be a nonzero homogeneous polynomial of degree D, and let $\lambda_1, \dots, \lambda_n$ be $\mathbf{Q}$-linearly independent elements of $\mathcal{L}$. From Lemma 6 we deduce that there exists a square $d \times d$ matrix with coefficients in $\mathbf{Q} + \mathbf{Q}T_2 + \cdots + \mathbf{Q}T_n$ whose determinant is $P(1, T_2, \dots, T_n)$. It follows that there exist square $d \times d$ matrices $M_1, \dots, M_n$ with coefficients in $\mathbf{Q}$ such that

$$\det(M_1X_1 + \cdots + M_nX_n) = X_1^{d-D} P(X_1, \dots, X_n).$$

From Conjecture 5 we deduce that the matrix $M_1\lambda_1+\cdots+M_n\lambda_n$ has the same rank as $M_1X_1+\cdots+M_nX_n$, hence $P(\lambda_1,\ldots,\lambda_n)\neq 0$.

According to part b) of Lemma 6 with $m=1$, under the hypotheses of part a) in the same Lemma 6, any polynomial in R can be written

$$\det\begin{pmatrix}\mathbf{B}_0 & \mathbf{B}_1\\ \mathbf{B}_2 & \mathbf{B}_3\end{pmatrix}$$

where the matrices $\mathbf{B}_0,\mathbf{B}_1,\mathbf{B}_2$ have coefficients in A, while the matrix $\mathbf{B}_3$ has coefficients in $AX_1+\cdots+AX_n$.

Hence, in order to study the vanishing of nonhomogeneous polynomials in logarithms of algebraic numbers, it is sufficient to consider matrices of the form

$$\mathbf{M}=\begin{pmatrix}\mathbf{B}_0 & \mathbf{B}_1\\ \mathbf{B}_2 & \mathbf{L}\end{pmatrix}$$

where $\mathbf{B}_0$, $\mathbf{B}_1$ and $\mathbf{B}_2$ have rational (or algebraic) entries, while $\mathbf{L}$ has entries in $\mathcal{L}$. For such matrices also a structural rank can be defined. Write

$$\mathbf{L}=\mathbf{M}_1\log\alpha_1+\cdots+\mathbf{M}_n\log\alpha_n$$

where $\log\alpha_1,\ldots,\log\alpha_n$ are $\mathbf{Q}$-linearly independent elements in $\mathcal{L}$ and $\mathbf{M}_1,\ldots,\mathbf{M}_n$ have rational entries. Then $r_{\mathrm{str}}(\mathbf{M})$ is the *rank of the matrix*

$$\begin{pmatrix}\mathbf{B}_0 & \mathbf{B}_1\\ \mathbf{B}_2 & \mathbf{M}_1X_1+\cdots+\mathbf{M}_nX_n\end{pmatrix}.$$

From Lemma 6, it follows that Conjecture 1 is equivalent to the following fact: *All such matrices* $\mathbf{M}$ *should have a rank equal to* $r_{\mathrm{str}}(\mathbf{M})$.

With this new point of view, in spite of the fact that no result of algebraic independence is known for elements of $\mathcal{L}$, we shall see below (Corollary 10 in Section 4) that half of the conjecture is already known.

Now we show how linear algebraic groups naturally occur.

Let d_0,d_1,l_0 and l_1 be nonnegative integers such that $d=d_0+d_1$ and $l=l_0+l_1$ are positive. Consider the linear algebraic group $G=\mathbf{G}_a^{d_0}\times\mathbf{G}_m^{d_1}$; we identify its tangent space at the origin $T_G(\mathbf{C})$ with $\mathbf{C}^d$. The exponential map of this algebraic group is then

$$\exp_G(\zeta_1,\ldots,\zeta_{d_0},z_1,\ldots,z_{d_1})=(\zeta_1,\ldots,\zeta_{d_0},e^{z_1},\ldots,e^{z_{d_1}}).$$

In this space $\mathbf{C}^d$, we take first a subspace W which is rational over $\overline{\mathbf{Q}}$, of dimension $l_0 \geq 0$. This means that W is generated as a $\mathbf{C}$-vector space by l_0 elements $\beta_1, \dots, \beta_{l_0}$ of $\overline{\mathbf{Q}}^d$ which are linearly independent over $\overline{\mathbf{Q}}$.

Next we take a finitely generated subgroup Y of $\mathcal{L}_G(\overline{\mathbf{Q}}) = \overline{\mathbf{Q}}^{d_0} \times \mathcal{L}^{d_1}$, of rank l_1 over $\mathbf{Z}$: there exist $u_1, \dots, u_{l_1}$ in $\mathbf{C}^d$ such that $Y = \mathbf{Z}u_1 + \cdots + \mathbf{Z}u_{l_1}$. For $1 \leq j \leq l_1$, the coordinates of u_j can be written

$$u_j = (\beta_{1,l_0+j}, \dots, \beta_{d_0,l_0+j}; \log \alpha_{1j}, \dots, \log \alpha_{d_1 j}),$$

with algebraic β_{hj}, $1 \leq h \leq d_0$, and α_{ij}, $1 \leq i \leq d_1$. We assume that $Y \cap W = 0$.

Denote by $r(W, Y; G)$ the dimension of the smallest $\mathbf{C}$-vector space in $\mathbf{C}^d$ which contains W and Y; plainly, this number is the rank of a matrix $\mathbf{M}$, of size $d \times l$, whose l columns are the components of the given generators of W and Y in the canonical basis of $\mathbf{C}^d$. This matrix $\mathbf{M}$ can be decomposed into four blocks:

$$\mathbf{M} = \begin{array}{c} \left(\begin{array}{cc} \mathbf{B}_0 & \mathbf{B}_1 \\ \mathbf{B}_2 & L \end{array} \right) \begin{array}{l} \} \; d_0 \\ \} \; d_1 \end{array} \\ \begin{array}{cc} \underbrace{\qquad}_{l_0} & \underbrace{\qquad}_{l_1} \end{array} \end{array}$$

The matrices

$$\mathbf{B}_0 = \begin{pmatrix} \beta_{11} & \cdots & \beta_{1l_0} \\ \vdots & \ddots & \vdots \\ \beta_{d_0 1} & \cdots & \beta_{d_0 l_0} \end{pmatrix}$$

$$\mathbf{B}_1 = \begin{pmatrix} \beta_{1,l_0+1} & \cdots & \beta_{1l} \\ \vdots & \ddots & \vdots \\ \beta_{d_0,l_0+1} & \cdots & \beta_{d_0 l} \end{pmatrix}$$

$$\mathbf{B}_2 = \begin{pmatrix} \beta_{d_0+1,1} & \cdots & \beta_{d_0+1,l_0} \\ \vdots & \ddots & \vdots \\ \beta_{d1} & \cdots & \beta_{d_0} \end{pmatrix}$$

have entries in $\overline{\mathbf{Q}}$, while

$$\mathbf{L} = (\log \alpha_{ij})_{1 \leq i \leq d_1, 1 \leq j \leq l_1}$$

has entries in $\mathcal{L}$.

Choose a basis $\log\alpha_1, \dots, \log\alpha_n$ of the $\mathbf{Q}$-vector space which is spanned by the numbers $\log\alpha_{ij}$ in $\mathcal{L}$, and write

$$\log\alpha_{ij} = \sum_{\nu=1}^{n} c_{ij\nu} \log\alpha_\nu,$$

with rational numbers $c_{ij\nu}$ so that

$$r_{\mathrm{str}}\,(\mathbf{M}) = \mathrm{rank}\begin{pmatrix} \mathbf{B}_0 & \mathbf{B}_1 \\ \mathbf{B}_2 & \sum_{\nu=1}^{n} X_\nu (c_{ij\nu})_{1\le i\le d_1, 1\le j\le l_1} \end{pmatrix}.$$

Therefore, Conjecture 1 can be stated as follows.

Conjecture 7.

$$r(W, Y; G) = r_{\mathrm{str}}\,(\mathbf{M}).$$

This is the situation which will be generalized in the next section to arbitrary commutative algebraic groups in place of $\mathbf{G}_a^{d_0} \times \mathbf{G}_m^{d_1}$.

As a matter of conclusion for this first section, we recall the connections between the previous conjectures:

$$\boxed{(1) \Longleftrightarrow (2) \Longleftrightarrow (7) \Longrightarrow (5) \Longrightarrow (3) \Longrightarrow (4)}$$

2. Commutative algebraic groups. Our goal is to study algebraic independence of logarithms in commutative algebraic groups in such a way that, for linear algebraic groups, we are reduced to Conjecture 7.

a) *The number* $r(W, Y; G)$. Let G be a commutative algebraic group of dimension d which is defined over a subfield K of $\mathbf{C}$; denote by $T_G(\mathbf{C})$ the tangent space at the origin of G. Let W be a vector subspace of $T_G(\mathbf{C})$ and Y be a finitely generated subgroup of $T_G(\mathbf{C})$. We define the *rank of the pair* (W, Y) as (l_0, l_1) where $l_0 = \dim_{\mathbf{C}} W$ and $l_1 = \mathrm{rank}_{\mathbf{Z}}(Y/Y\cap W)$; we shall also use the notation $l = l_0 + l_1$. Denote by $r(W, Y; G)$ the *dimension of the* $\mathbf{C}$*-vector subspace of* $T_G(\mathbf{C})$ *which* *is generated by* $W \cup Y$. In the special case $W = 0$, we write $r(Y; G)$ in place of $r(0, Y; G)$.

Plainly we have $r(W, Y; G) \leq \min\{d, l\}$. More precisely, if G^* is an algebraic subgroup of G, then

$$\begin{aligned} r(W, Y; G) \leq \dim G^* &+ \dim_{\mathbf{C}}(W/W \cap T_{G^*}(\mathbf{C})) \\ &+ \operatorname{rank}_{\mathbf{Z}}(Y/Y \cap (W + T_{G^*}(\mathbf{C}))). \end{aligned}$$

Since G is defined over K, the space $T_G(\mathbf{C})$ has a K-structure; there are two ways for a point in $T_G(\mathbf{C})$ to be *defined over* K: either it is rational over K for this K-structure, or else its image under the exponential map

$$\exp_G : T_G(\mathbf{C}) \to G(\mathbf{C})$$

is in $G(K)$. When G is not a power of $\mathbf{G}_a$, these two properties are fundamentally different (see, for instance, Lang's early results in [**3**, Chapter 2.4]); this is the very heart of the subject. Given a vector subspace W of $T_G(\mathbf{C})$ and a finitely generated subgroup Y of $T_G(\mathbf{C})$, we shall say that (W, Y) is a *K-arithmetic pair related to G* if W is rational over K, and Y is contained in $\mathcal{L}_G(K) = \exp_G^{-1}(G(K))$.

If (W, Y) is a K-arithmetic pair related to G, if G^* is an algebraic subgroup of G which is defined over K, and if we put

$$W^* = W \cap T_{G^*}(\mathbf{C}), \qquad Y^* = Y \cap T_{G^*}(\mathbf{C}),$$

and

$$W' = W/W^*, \qquad Y' = Y/Y^*,$$

then (W^*, Y^*) is a K-arithmetic pair related to G^*, and (W', Y') is a K-arithmetic pair related to $G' = G/G^*$. If (W^*, Y^*) is of rank (l_0^*, l_1^*) and (W', Y') of rank (l_0', l_1'), then the rank of (W, Y) is (l_0, l_1) with

$$l_0 = l_0^* + l_0', \qquad l_1 \geq l_1^* + l_1'.$$

Using these notations, the previous upper bound for $r(W, Y; G)$ can be written

$$r(W, Y; G) \leq d^* + l',$$

where $d^* = \dim G^*$ and $l' = l_0' + l_1'$.

When $Y \cap W = 0$ we have $l_1 = \mathrm{rank}_{\mathbf{Z}} Y$; however, the property $Y \cap W = 0$ is not stable under quotient; this is why we do not restrict the discussion to this case.

Our goal is to study the number $r(W, Y; G)$ when G is a commutative algebraic group which is defined over $\overline{\mathbf{Q}}$ and (W, Y) a $\overline{\mathbf{Q}}$-arithmetic pair. We define

$$\mathcal{L}_G = \mathcal{L}_G(\overline{\mathbf{Q}}) = \exp_G^{-1}(G(\overline{\mathbf{Q}})).$$

In the case where Y is of rank ≤ 1, we have

$$r(W, Y; G) = \min_{G^*}(d^* + l'),$$

where G^* runs over the algebraic subgroups of G defined over $\overline{\mathbf{Q}}$, d^* is the dimension of G^* and $l' = l'_0 + l'_1$, where (l'_0, l'_1) is the rank of the pair (W', Y'):

$$W' = W/W \cap T_{G^*}(\mathbf{C}), \qquad Y' = Y/Y \cap T_{G^*}(\mathbf{C}).$$

This follows from Wüstholz's theorem [**12, 13**]:

Let G be a commutative algebraic group which is defined over the field $\overline{\mathbf{Q}}$. Let W be a subspace of $T_G(\mathbf{C})$ which is rational over $\overline{\mathbf{Q}}$, and let $u \in \mathcal{L}_G \cap W$. There exists an algebraic subgroup G^* of G, which is defined over $\overline{\mathbf{Q}}$, such that $u \in T_{G^*}(\mathbf{C}) \subset W$.

Here is another consequence of Wüstholz's result. Let $T_{G^*}(\mathbf{C})$ be the largest tangent space of an algebraic subgroup G^* of G with the property that $T_{G^*}(\mathbf{C}) \subset W$. Define

$$G' = G/G^*, \qquad W' = W/T_{G^*}(\mathbf{C})$$

and

$$Y' = Y/Y \cap T_{G^*}(\mathbf{C}).$$

Then we have $Y' \cap W' = 0$ and

$$r(W, Y; G) = \dim G^* + r(W', Y'; G').$$

There is one example of an algebraic group of dimension 2 over $\overline{\mathbf{Q}}$ with a subgroup Y of $T_G(\mathbf{C})$ which is $\overline{\mathbf{Q}}$-arithmetic of rank 2 and such that $r(Y;G)=1$, while Y is not contained in the tangent space of an algebraic subgroup of G of dimension 1; namely, take $G=\mathbf{G}_a\times E$ where E is an elliptic curve over $\overline{\mathbf{Q}}$ with a nontrivial endomorphism represented by $\tau\in\mathbf{C}$, $\tau\notin\mathbf{Q}$; choose $v\in\mathcal{L}_E$ with $\exp_E v$ not torsion in $E(\overline{\mathbf{Q}})$, and define $u_1=(1,v)$, $u_2=(\tau,\tau v)$.

We expect that such a phenomenon will not occur for the algebraic group $G=\mathbf{G}_m^2$: this is related to the four exponentials Conjecture 4 as follows. We identify, as usual, $T_G(\mathbf{C})$ with $\mathbf{C}^2$ with $\exp_G(z_1,z_2)=(e^{z_1},e^{z_2})$. Assume that a matrix

$$\begin{pmatrix}\log\alpha_{11} & \log\alpha_{12}\\ \log\alpha_{21} & \log\alpha_{22}\end{pmatrix}$$

with entries in $\mathcal{L}$ has $\mathbf{Q}$-linearly independent columns and rank 1; define

$$u_1=\begin{pmatrix}\log\alpha_{11}\\ \log\alpha_{21}\end{pmatrix}\quad\text{and}\quad u_2=\begin{pmatrix}\log\alpha_{12}\\ \log\alpha_{22}\end{pmatrix}.$$

Then u_1 and u_2 belong to $\mathcal{L}_G$ and are $\mathbf{Q}$-linearly independent; hence $Y=\mathbf{Z}u_1+\mathbf{Z}u_2$ is a subgroup of $T_G(\mathbf{C})$ of rank 2 over $\mathbf{Z}$, which is $\overline{\mathbf{Q}}$-arithmetic, with $r(Y;G)=1$. The four exponentials conjecture claims that the rows of the previous matrix are linearly dependent over $\mathbf{Q}$, which means that u_1 and u_2 belong to a subspace of $T_G(\mathbf{C})=\mathbf{C}^2$ which is rational over $\mathbf{Q}$; this subspace is the tangent space at the origin of an algebraic subgroup G^* of G of dimension 1 and $T_{G^*}(\mathbf{C})\supset Y$.

On the other hand, Langevin's above-mentioned antisymmetric matrix provides an example with $G=\mathbf{G}_m^3$, where

$$r(Y;G)<\min_{G^*}\{\dim G^*+\operatorname{rank}_{\mathbf{Z}}(Y/Y\cap T_{G^*}(\mathbf{C}))\};$$

choose three $\mathbf{Q}$-linearly independent elements in $\mathcal{L}$, say $\log\alpha$, $\log\beta$ and $\log\gamma$, and consider the subgroup Y of $\mathbf{C}^3=T_G(\mathbf{C})$ of rank 3 spanned by the three-column vectors in $\mathbf{C}^3$ of the matrix

$$\begin{pmatrix}0 & -\log\gamma & \log\beta\\ \log\gamma & 0 & -\log\alpha\\ -\log\beta & \log\alpha & 0\end{pmatrix}.$$

Then for any subspace of $T_{G^*}(\mathbf{C})$ of $\mathbf{C}^3$ which is rational over $\mathbf{Q}$,

$$\begin{cases}\operatorname{rank}_{\mathbf{Z}}(Y\cap T_{G^*}(\mathbf{C}))=0 & \text{if } \dim G^*=1,\\ \operatorname{rank}_{\mathbf{Z}}(Y\cap T_{G^*}(\mathbf{C}))=1 & \text{if } \dim G^*=2.\end{cases}$$

b) *Definition of the structural rank* $r_{\mathrm{str}}(W,Y;G)$. Conjecture 5 involves the structural rank $r_{\mathrm{str}}(M)$ of a $d\times l$ matrix $M=(\lambda_{ij})$ with coefficients in $\mathcal{L}$. This number $r_{\mathrm{str}}(M)$ is also the maximal rank of matrices in the smallest subspace of $\mathbf{C}^{dl}$ which is rational over $\mathbf{Q}$ and contains the point $(\lambda_{ij})\in\mathbf{C}^{dl}$. Hence, instead of looking at the l column vectors $u_1,\dots,u_l$ of M as l points in the tangent space of $\mathbf{G}_m^d$, we consider the single point $(u_1,\dots,u_l)$ in the tangent space of $\mathbf{G}_m^{dl}$ (compare with the argument in [**9**, Section 3e]). We perform a similar treatment in the general case.

Let G be a commutative algebraic group of dimension d which is defined over a subfield K of $\overline{\mathbf{Q}}$. We choose a basis of $T_G(\mathbf{C})$ which is rational over $\overline{\mathbf{Q}}$, and we identify $T_G(\mathbf{C})$ with $\mathbf{C}^d$. Let (W,Y) be a K-arithmetic pair of rank (l_0,l_1); put $l=l_0+l_1$. We first choose a basis $(\beta_1,\dots,\beta_{l_0})$ of W over $\mathbf{C}$, with $\beta_h\in K^d$, $1\le h\le l_0$. Next we select $u_1,\dots,u_{l_1}$ in Y which are $\mathbf{Z}$-linearly independent modulo W. We define the algebraic group $\mathcal{G}$ as the product $\mathbf{G}_a^{dl_0}\times G^{l_1}$, and we identify its tangent space at the origin $T_{\mathcal{G}}(\mathbf{C})$ with $(\mathbf{C}^d)^l$. Define

$$v=(v_1,\dots,v_l)=(\beta_1,\dots,\beta_{l_0},u_1,\dots,u_{l_1})\in T_{\mathcal{G}}(\mathbf{C}).$$

Denote by $T_{\mathcal{H}}(\mathbf{C})$ the smallest tangent space of an algebraic subgroup $\mathcal{H}$ of $\mathcal{G}$, which is defined over K, such that v belongs to $T_{\mathcal{H}}(\mathbf{C})$. We define the *structural rank* $r_{\mathrm{str}}(W,Y;G)$ of (W,Y) by

$$r_{\mathrm{str}}(W,Y;G)=\max\{\dim_{\mathbf{C}}(\mathbf{C}z_1+\cdots+\mathbf{C}z_l);(z_1,\dots,z_l)\in T_{\mathcal{H}}(\mathbf{C})\}.$$

In the special case $W=0$, we write $r_{\mathrm{str}}(Y;G)$ in place of $r_{\mathrm{str}}(0,Y;G)$.

It is easily checked that this number $r_{\mathrm{str}}(W,Y;G)$ does not depend on the choices of $\beta_1,\dots,\beta_{l_0}$ and $u_1,\dots,u_{l_1}$ in W and $Y/Y\cap W$, respectively. Obviously, we have $r(W,Y;G)\le r_{\mathrm{str}}(W,Y;G)\le\min\{l,d\}$. For the algebraic group $\mathbf{G}_a^{d_0}\times\mathbf{G}_m^{d_1}$, this extends the definitions in Section 1 of the structural rank of certain matrices.

Definition. (Property of algebraic independence). An algebraic group G which is defined over a subfield K of $\overline{\mathbf{Q}}$ satisfies *property* (A.I.) if, for any K-arithmetic pair (W,Y), equality $r(W,Y;G)=r_{\mathrm{str}}(W,Y;G)$ holds.

From the definition of K-arithmetic pairs, it follows immediately that any unipotent group $\mathbf{G}_a^d$ satisfies property (A.I.). On the other hand, we have shown at the end of Section 1 that all linear group $\mathbf{G}_a^{d_0} \times \mathbf{G}_m^{d_1}$ satisfy property (A.I.) if and only if Conjecture 1 is true.

Remark. An example of an algebraic group (namely a nontrivial extension of an abelian variety by the multiplicative group) which does not satisfy property (A.I.) follows from D. Bertrand's construction in [**2**] together with the fact that property (A.I.) implies the *density property* (see Proposition 8 below).

c) *Simple Abelian varieties.* We show how to compute the structural rank when the algebraic group G has no nontrivial subgroups and $l_0 = 0$.

Let K be a subfield of $\mathbf{C}$ and A be a simple abelian variety over K, of dimension d. Let $v_1, \dots, v_l$ be $\mathbf{Z}$-linearly independent elements of $T_A(\mathbf{C})$; define $Y = \mathbf{Z}v_1 + \cdots + \mathbf{Z}v_l$. Consider the smallest algebraic subgroup H of A^l such that $T_H(\mathbf{C}) \ni (v_1, \dots, v_l)$; since A is simple, the dimension of H is dr for some integer r with $1 \le r \le l$, and there exist endomorphisms δ_{ij} of A, $1 \le j \le l$, $1 \le i \le r$, such that $T_H(\mathbf{C})$ is the image of the $\mathbf{C}$-linear map

$$\begin{aligned} T_{A^r}(\mathbf{C}) &\longrightarrow T_{A^l}(\mathbf{C}) \\ (z_1, \dots, z_r) &\longmapsto \left(\sum_{i=1}^{r} \delta_{ij} z_i \right)_{1 \le j \le l}. \end{aligned}$$

Define, for $z = (z_1, \dots, z_r) \in T_{A^r}(\mathbf{C})$ and $1 \le j \le l$,

$$\Delta_j z = \sum_{i=1}^{r} \delta_{ij} z_i \in T_A(\mathbf{C}),$$

in such a way that

$$T_H(\mathbf{C}) = \{(\Delta_1 z, \dots, \Delta_l z); z \in T_{A^r}(\mathbf{C})\}.$$

We deduce that $r_{\mathrm{str}}(Y, A)$ is the *dimension of the* $\mathbf{C}$*-vector space spanned by* $\Delta_1, \dots, \Delta_l$ *in* $\mathrm{Hom}_{\mathbf{C}}(T_{A^r}(\mathbf{C}), T_A(\mathbf{C}))$.

Examples. 1) We consider the special case $r = 1$: if $\delta_1, \dots, \delta_l$ (with $l \ge 2$) are elements of $\mathrm{End}\, A$ which are linearly dependent over $\mathbf{C}$ in

$\mathrm{End}_{\mathbf{C}}(T_A(\mathbf{C}))$, and if $v_j = \delta_j v$ for some $v \in T_A(\mathbf{C})$ and $1 \leq j \leq l$, then $r_{\mathrm{str}}(Y, A) < l$.

2) Here is an example with $r = l - 1$: assume that $v_1, \ldots, v_{l-1}$ are linearly independent over $\mathrm{End}\, A$; this means that $\mathbf{Z}(v_1, \ldots, v_{l-1})$ is not contained in a subspace $T_H(\mathbf{C})$ for H algebraic subgroup of A^{l-1} different from A^{l-1}. Assume also that $l \leq d$; in this case we show $r_{\mathrm{str}}(Y, A) = l$.

Indeed, this is true for $l = 1$; hence, we may assume $2 \leq l \leq d$. As before, denote by $\mathcal{H}$ the smallest algebraic subgroup of A^l over K such that $T_{\mathcal{H}}(\mathbf{C})$ contains $(v_1, \ldots, v_l)$. If $\mathcal{H} = A^l$, then the result is clear. Otherwise, $\dim \mathcal{H} = d(l-1)$, and there exist positive integers $m_1, \ldots, m_{l-1}$ as well as endomorphisms $\delta_1, \ldots, \delta_{l-1}$ of A such that

$$T_{\mathcal{H}}(\mathbf{C}) = \{(m_1 z_1, \ldots, m_{l-1} z_{l-1}, \delta_1 z_1 + \cdots + \delta_{l-1} z_{l-1}); \qquad (z_1, \ldots, z_{l-1}) \in T_{A^{l-1}}(\mathbf{C})\}.$$

Define $\Delta_1, \ldots, \Delta_l$, which are $\mathbf{C}$-linear maps $T_{A^{l-1}}(\mathbf{C}) \to T_A(\mathbf{C})$, by

$$\Delta_i(z_1, \ldots, z_{l-1}) = m_i z_i, \quad 1 \leq i \leq l-1$$

and

$$\Delta_l(z_1, \ldots, z_{l-1}) = \delta_1 z_1 + \cdots + \delta_{l-1} z_{l-1}.$$

We claim that these elements of $\mathrm{Hom}_{\mathbf{C}}(T_{A^{l-1}}(\mathbf{C}), T_A(\mathbf{C}))$ are $\mathbf{C}$-linearly independent: if $t_1, \ldots, t_{l-1}$ were complex numbers such that

$$\Delta_l = t_1 \Delta_1 + \cdots + t_{l-1} \Delta_{l-1},$$

then we would deduce $\delta_i = t_i m_i$ for $1 \leq i \leq l-1$; hence, $t_1, \ldots, t_{l-1}$ would be rational numbers (recall that A is not an elliptic curve), and the relation $v_l = t_1 m_1 v_1 + \cdots + t_{l-1} m_{l-1} v_{l-1}$, would contradict the linear independence of $v_1, \ldots, v_l$. Hence, $\Delta_1, \ldots, \Delta_l$ are $\mathbf{C}$-linearly independent in $\mathrm{Hom}_{\mathbf{C}}(T_{A^{l-1}}(\mathbf{C}), T_A(\mathbf{C}))$, and therefore $r_{\mathrm{str}}(Y, A) = l$.

d) *Product of algebraic groups of dimension* 1. Let E be an elliptic curve which is defined over the field $\overline{\mathbf{Q}}$. The algebraic groups E^d, $d \geq 1$, satisfy property (A.I.) if and only if the following statement is true:

Let $u_1, \ldots, u_n$ *in* $T_E(\mathbf{C})$ *be linearly independent over* $\mathrm{End}\, E$ *and satisfy* $\exp_E(u_j) \in E(\overline{\mathbf{Q}})$, $1 \leq j \leq n$. *If* $P \in \overline{\mathbf{Q}}[X_1, \ldots, X_n]$ *is* *a nonzero homogeneous polynomial with algebraic coefficients, then* $P(u_1, \dots, u_n) \neq 0$.

The algebraic independence of $u_1, \dots, u_n$ over $\mathbf{Q}$ (i.e., the nonvanishing of $P(u_1, \dots, u_n)$ for any nonzero polynomial $P \in \overline{\mathbf{Q}}[X_1, \dots, X_n]$) means that the algebraic groups $\mathbf{G}_a^{d_0} \times E^{d_2}$, $d_0 \geq 0$, $d_2 \geq 1$, satisfy property (A.I.). Similarly, property (A.I.) for the algebraic groups $\mathbf{G}_a^{d_0} \times \mathbf{G}_m^{d_1} \times E^{d_2}$, $d_0 \geq 0$, $d_1 \geq 0$, $d_2 \geq 0$, is equivalent to the algebraic independence of the numbers $\log \alpha_1, \dots, \log \alpha_m$, $u_1, \dots, u_n$ when $\log \alpha_1, \dots, \log \alpha_m$ are $\mathbf{Q}$-linearly independent in $\mathcal{L}$ and $u_1, \dots, u_n$ are $\operatorname{End} E$-linearly independent in $\mathcal{L}_E$. The proof of this fact uses the following special case of Lemma 6:

any polynomial in $A[X_1, \dots, X_n, Y_1, \dots, Y_k]$ *can be written*

$$\det \begin{pmatrix} \mathbf{M}_0 & \mathbf{M}_3 \\ \mathbf{M}_1 & \mathbf{M}_4 \\ \mathbf{M}_2 & \mathbf{M}_5 \end{pmatrix}$$

where the matrices $\mathbf{M}_0, \mathbf{M}_1, \mathbf{M}_2, \mathbf{M}_3$ *have coefficients in* A, *the matrix* $\mathbf{M}_4$ *has coefficients in* $AX_1 + \cdots + AX_n$ *and* $\mathbf{M}_5$ *has coefficients in* $AY_1 + \cdots + AY_k$.

It is easy to extend this discussion to the situation where E^{d_2} is replaced by a product of several elliptic curves.

3. The density property. In this section we work with a commutative algebraic group G which is defined over a subfield K of $\mathbf{R}$; we denote by $\exp_{G,\mathbf{R}} : T_G(\mathbf{R}) \to G(\mathbf{R})$ the exponential map of the real Lie group $G(\mathbf{R})$ (this is nothing else than the restriction of $\exp_G$ to $T_G(\mathbf{R})$) and by $\ker \exp_{G,\mathbf{R}}$ its kernel, which is a discrete subgroup of $T_G(\mathbf{R})$.

Our aim in this section is to show a connection between property (A.I.) (restricted to the case $l_0 = 0$) and the following one, which is introduced in [**11**]:

Definition. Let K be a number field which is embedded in $\mathbf{R}$ and G a commutative algebraic group which is defined over K. The algebraic group G is said to satisfy the *density property* if, for any finitely generated subgroup Γ of $G(K)$, and for any $(\gamma_1, \dots, \gamma_l) \in \Gamma^l$ such that $\mathbf{Z}\gamma_1 + \dots + \mathbf{Z}\gamma_l$ is a subgroup of finite index of Γ, if $\mathcal{H}$ denotes the Zariski closure in G^l over K of the subgroup $\mathbf{Z}(\gamma_1, \dots, \gamma_l)$, and if there exists $(\eta_1, \dots, \eta_l) \in \mathcal{H}(\mathbf{R})$ such that $\mathbf{Z}\eta_1 + \dots + \mathbf{Z}\eta_l$ is a dense subgroup of $G(\mathbf{R})^0$, then $\Gamma \cap G(\mathbf{R})^0$ is dense in $G(\mathbf{R})^0$.

The condition which is stated is obviously necessary: if $\Gamma \cap G(\mathbf{R})^0$ is dense in $G(\mathbf{R})^0$, we just take $\eta_j = \gamma_j$.

In the density property, the condition is on the algebraic subgroup $\mathcal{H}$, while in property (A.I.), the condition is on the tangent space T_H; the difference is significant; for an algebraic subgroup H of an algebraic group G over $\mathbf{R}$,

$$\exp_{G,\mathbf{R}}^{-1}(H(\mathbf{R})) = T_H(\mathbf{R}) + \ker \exp_{G,\mathbf{R}} .$$

As noticed in [**1**, p. 48], given an algebraic group G over a subfield K of $\mathbf{C}$ and a point $\gamma \in G(K)$, the choice of a logarithm of γ, that is the choice of a point $u \in T_G(\mathbf{C})$ with $\exp_G(u) = \gamma$ determines an action of $\mathbf{Q}$ on γ by

$$\frac{p}{q}\gamma = \exp_G(pu/q), \qquad p/q \in \mathbf{Q};$$

the Zariski closure of the orbit of γ under this action is the smallest algebraic subgroup of G whose tangent space at the origin contains u.

Proposition 8. *If a commutative algebraic group G which is defined over $\overline{\mathbf{Q}} \cap \mathbf{R}$ satisfies property (A.I.), then it also satisfies the density property.*

Proof. Let G be an algebraic group over a real number field K which satisfies property (A.I.), Γ a finitely generated subgroup of $G(K)$, $\gamma_1, \dots, \gamma_l$ in $\Gamma \cap G(\mathbf{R})^0$ span a subgroup of finite index of Γ, and $\mathcal{H}$ the Zariski closure over K of $\mathbf{Z}(\gamma_1, \dots, \gamma_l)$ in G^l.

We choose a basis $(\omega_1, \dots, \omega_\kappa)$ over $\mathbf{Z}$ of the kernel of the exponential map of the Lie group $G(\mathbf{R})$; we also choose $(y_1, \dots, y_l)$ in $T_{\mathcal{H}}(\mathbf{R})$ such that $\exp_{G^l}(y_1, \dots, y_l) = (\gamma_1, \dots, \gamma_l)$. What we will say will not depend on these choices, in the same way as the density property does not depend on the choice of $\gamma_1, \dots, \gamma_l$. Notice that $\mathbf{Z}\omega_1 + \dots + \mathbf{Z}\omega_\kappa +$

$\mathbf{Z}y_1+\cdots+\mathbf{Z}y_l$ is a subgroup of finite index in $\exp_{G,\mathbf{R}}^{-1}(\Gamma)$ and that $\mathcal{H}$ is the smallest algebraic subgroup of G^l over K such that $T_{\mathcal{H}}(\mathbf{R})$ contains $(y_1,\dots,y_l)$.

We denote by $\mathcal{H}$ the smallest algebraic subgroup of $G^{\kappa+l}$, which is defined over K, such that $T_H(\mathbf{R})$ contains the point $(\omega_1,\dots,\omega_\kappa,y_1,\dots,y_l) \in T_G^{\kappa+l}(\mathbf{R})$. We claim

$$(0)^\kappa\times\mathcal{H}\subset H\subset G^\kappa\times\mathcal{H}.$$

The first inclusion is proved as follows: since $(\omega_1,\dots,\omega_\kappa,y_1,\dots,y_l)\in T_H(\mathbf{R})$, we have

$$(0,\dots,0,\gamma_1,\dots,\gamma_l)\in H(\mathbf{R})\cap(\{0\}^\kappa\times G^l(\mathbf{R})).$$

If $p: G^{\kappa+l}\to G^l$ denotes the projection with kernel $G^\kappa\times\{0\}^l$, then $p(H\cap(\{0\}^\kappa\times G^l))$ is an algebraic subgroup of G^l over K which contains $(\gamma_1,\dots,\gamma_l)$; we deduce from the definition of $\mathcal{H}$:

$$p(H\cap(\{0\}^\kappa\times G^l))\supset\mathcal{H},$$

and the first inclusion follows.

For the second one, we notice that $G^\kappa\times\mathcal{H}$ is an algebraic subgroup of $G^{\kappa+l}$ over K whose tangent space at the origin contains $(\omega_1,\dots,\omega_\kappa,y_1,\dots,y_l)$; hence, this algebraic subgroup contains H. This completes the proof of the claim.

It immediately follows that if $p': G^{\kappa+l}\to G^\kappa$ denotes the projection with kernel $\{0\}^\kappa\times G^l$, then $H=H'\times\mathcal{H}$, where $H'=p'(H)$. Therefore, $(\omega_1,\dots,\omega_\kappa)\in T_{H'}(\mathbf{R})$ and $(\omega_1,\dots,\omega_\kappa,0,\dots,0)\in T_H(\mathbf{R})$.

Assume that $\Gamma\cap G(\mathbf{R})^0$ is not dense in $G(\mathbf{R})^0$. Then the subgroup $\mathbf{Z}\omega_1+\cdots+\mathbf{Z}\omega_\kappa+\mathbf{Z}y_1+\cdots+\mathbf{Z}y_l$ is not dense in $T_G(\mathbf{R})$; hence, there exist $\kappa+l-1$ elements $u_1,\dots,u_{\kappa+l-1}$ in this subgroup, which are $\mathbf{Q}$-linearly independent and belong to a real hyperplane of $T_G(\mathbf{R})$. Therefore, the subgroup $Y=\mathbf{Z}u_1+\cdots+\mathbf{Z}u_{\kappa+l-1}$ of $T_G(\mathbf{R})$ satisfies

$$r(Y;G)<\dim G.$$

For $1\le i\le\kappa+l-1$, write u_i as a linear combination of $\omega_1,\dots,\omega_\kappa,y_1,\dots,y_l$ with rational integer coefficients; this gives a matrix of size $(\kappa+l-1)\times(\kappa+l)$ with rational integer coefficients and rank $\kappa+l-1$. Hence, a surjective linear map

$$\pi: T_G(\mathbf{R})^{\kappa+l}\longrightarrow T_G(\mathbf{R})^{\kappa+l-1}$$

with $\pi(\omega_1,\dots,\omega_\kappa,y_1,\dots,y_l) = (u_1,\dots,u_{\kappa+l-1})$. We also denote by π the corresponding morphism $G^{\kappa+l} \to G^{\kappa+l-1}$. It is easy to check that $H'' = \pi(H)$ is the smallest algebraic subgroup of G^{k+l-1} defined over K such that $(u_1,\dots,u_{\kappa+l-1}) \in T_{H''}(\mathbf{R})$, and hence also the smallest algebraic subgroup of $G^{\kappa+l-1}$ defined over K such that $(u_1,\dots,u_{\kappa+l-1}) \in T_{H''}(\mathbf{C})$.

Assume now that Γ does not satisfy the density property: there exists $(\eta_1,\dots,\eta_l)$ in $\mathcal{H}(\mathbf{R})$ such that $\mathbf{Z}\eta_1 + \cdots + \mathbf{Z}\eta_l$ is a dense subgroup of $G(\mathbf{R})^0$. We choose an element $(v_1,\dots,v_l)$ in $T_{\mathcal{H}}(\mathbf{R})$ with $\exp_{G^l}(v_1,\dots,v_l) = (\eta_1,\dots,\eta_l)$, so that $\mathbf{Z}\omega_1+\cdots+\mathbf{Z}\omega_\kappa+\mathbf{Z}v_1+\cdots+\mathbf{Z}v_l$ is a dense subgroup of $T_G(\mathbf{R})$. Hence, any family of $\kappa+l-1$ elements in this subgroup which are linearly independent over $\mathbf{Z}$ contains a basis of $T_G(\mathbf{R})$ over $\mathbf{R}$.

Define

$$(z_1,\dots,z_{\kappa+l-1}) = \pi(\omega_1,\dots,\omega_\kappa,v_1,\dots,v_l);$$

we have $(\omega_1,\dots,\omega_\kappa,v_1,\dots,v_l) \in T_H(\mathbf{R})$. Hence, $(z_1,\dots,z_{\kappa+l-1}) \in T_{H''}(\mathbf{R})$. Since $\mathbf{R}z_1+\cdots+\mathbf{R}z_{\kappa+l-1} = T_G(\mathbf{R})$ we also have $\mathbf{C}z_1+\cdots+\mathbf{C}z_{\kappa+l-1} = T_G(\mathbf{C})$, and this implies

$$r_{\text{str}}(Y;G) = \dim G.$$

We deduce $r(Y;G) < r_{\text{str}}(Y;G)$; hence, G does not satisfy property (A.I.). □

4. A partial result.

When G is a commutative algebraic group, we define $\varrho = \varrho(G)$ by

$$\varrho = \begin{cases} 1 & \text{if } G \text{ is a linear algebraic group,} \\ 2 & \text{otherwise.} \end{cases}$$

Theorem 9. *Let G be a commutative algebraic group which is defined over a number field K, and let (W,Y) be a K-arithmetic pair. Then*

$$r(W,Y;G) \ge \frac{1}{\varrho+1} r_{\text{str}}(W,Y;G).$$

The case $\varrho = 1$, i.e., $G = \mathbf{G}_a^{d_0} \times \mathbf{G}_m^{d_1}$ over $\overline{\mathbf{Q}}$, can be stated as follows:

Corollary 10. *For a matrix* $\mathbf{M}$ *of the form*

$$\mathbf{M} = \begin{pmatrix} \mathbf{B}_0 & \mathbf{B}_1 \\ \mathbf{B}_2 & \mathbf{L} \end{pmatrix},$$

where $\mathbf{B}_0$, $\mathbf{B}_1$ *and* $\mathbf{B}_2$ *have algebraic entries while* $\mathbf{L}$ *has entries in* $\mathcal{L}$, *the lower bound*

$$\operatorname{rank}(\mathbf{M}) \geq \frac{1}{2} r_{\mathrm{str}}(\mathbf{M})$$

holds.

This Corollary 10 has been generalized by D. Roy [**4, 7**] to matrices whose entries are linear forms with algebraic coefficients in logarithms of algebraic numbers.

The main tool in the proof of Theorem 9 is the *theorem of the algebraic subgroup.* There are several (equivalent) statements; a thorough study of this question has been done by D. Roy. Here, we shall apply Théorème 6.7 of [**6**] which we state now. We deal with commutative algebraic groups G which are defined over $\mathbf{C}$. When $s : G \to G'$ is a surjective morphism of algebraic groups, we denote by ds the associated linear map $T_G(\mathbf{C}) \to T_{G'}(\mathbf{C})$ on the tangent spaces at the origin.

Theorem 11 (Theorem of the algebraic subgroup). *Let* G *be a commutative algebraic group which is defined over the field* $\overline{\mathbf{Q}}$ *of complex algebraic numbers and* V *a subspace of* $T_G(\mathbf{C})$ *which is not* $T_G(\mathbf{C})$. *Among the surjective morphisms of algebraic groups* $s : G \to G'$, *defined over* $\overline{\mathbf{Q}}$, *for which* $ds(V) \neq T_{G'}(\mathbf{C})$, *and for which the quotient*

$$\dim_{\mathbf{C}}(ds(V))/\dim G'$$

is minimal, we select one for which $\dim G'$ *is minimal. Then, if we set* $V' = ds(V)$, *and if we denote by* $\mathcal{W}$ *the maximal subspace of* V' *which is rational over* $\overline{\mathbf{Q}}$, *we have*

$$\dim_{\mathbf{Q}}(V' \cap \mathcal{L}_{G'}) \leq \varrho \dim G' \frac{\dim_{\mathbf{C}}(V'/\mathcal{W})}{\dim_{\mathbf{C}}(T_{G'}(\mathbf{C})/V')}.$$

Notice that Théorème 6.7 of [**6**] involves a function $\alpha(G)$ which we have replaced, for simplicity, by $\varrho \dim G$ (the arguments of [**6**] imply this result, as explained in [**6**, p. 266]).

We state this result in a slightly different way which is closer to our own notations.

Corollary 12. *Let G be a commutative algebraic group of dimension d which is defined over a number field $K \subset \mathbf{C}$, and let (W, Y) be a K-arithmetic pair of rank (l_0, l_1) with $l_0 + l_1 = l$. Assume that the number $r = r(W, Y; G)$ satisfies $r < d$. Then there exists an algebraic subgroup G^* of G, defined over K, of dimension $d - d'$ with $1 \leq d' \leq d$, such that, if we set*

$$G' = \frac{G}{G^*}, \qquad W' = \frac{W}{W \cap T_{G^*}(C)}, \qquad Y' = \frac{Y}{Y \cap T_{G^*}(\mathbf{C})},$$

and

$$l'_0 = \operatorname{rank}_{\mathbf{Z}} W', \qquad l'_1 = \operatorname{rank}_{\mathbf{Z}}(Y'/Y' \cap W'), \qquad r' = r(W', Y'; G'),$$

then

$$\frac{r}{d} \geq \frac{r'}{d'} \geq \frac{l'_1 + \varrho\, l'_0}{l'_1 + \varrho\, d'}.$$

We deduce Corollary 12 from Theorem 11 as follows. Let V be the subspace of $T_G(\mathbf{C})$ which is generated by W and Y; Theorem 11 provides the existence of some morphism $s : G \to G'$. Define

$$G^* = \ker s, \qquad W' = ds(W), \qquad Y' = ds(Y), \qquad V' = ds(V);$$

the dimension of V' is $r' = r(W', Y'; G')$. Hence, $r/d \geq r'/d'$. Since the maximal subspace $\mathcal{W}$ of V' which is rational over $\overline{\mathbf{Q}}$ contains $ds(W)$, we have $\dim_{\mathbf{C}} \mathcal{W} \geq l'_0$. Further, $V' \cap \mathcal{L}_{G'}$ contains $ds(Y)$ which is of rank $\geq l'_1$; it follows that we have $\dim_{\mathbf{Q}}(V' \cap \mathcal{L}_{G'}) \geq l'_1$. Therefore, Theorem 11 yields

$$l'_1 \leq \varrho\, d' \frac{r' - l'_0}{d' - r'},$$

which provides the conclusion of Corollary 12. □

The proof of Theorem 9 involves three further lemmas.

Lemma 13. *Let G be a commutative algebraic group which is defined over a subfield K of $\mathbf{C}$, and let (W, Y) be a K-arithmetic pair related to G. Then there exists a subspace W^* of W and a subgroup Y^* of Y such that $W^* \cap Y^* = 0$, and such that the rank (l_0^*, l_1^*) of the pair (W^*, Y^*) satisfies*

$$l_0^* + l_1^* = r_{\mathrm{str}}\,(W^*, Y^*; G) = r_{\mathrm{str}}\,(W, Y; G).$$

Proof. We choose a basis $\{\beta_1, \dots \beta_{l_0}\}$ of the $\mathbf{C}$-vector space W, and we choose $u_1, \dots, u_{l_1}$ in Y which are $\mathbf{Z}$-linearly independent modulo W. We define $l^* = r_{\mathrm{str}}\,(W, Y; G)$, and we denote by $\mathcal{H}$ the smallest algebraic subgroup of $\mathcal{G} = \mathbf{G}_a^{dl_0} \times G^{l_1}$, defined over K, such that the point

$$(v_1, \dots, v_l) = (\beta_1, \dots, \beta_{l_0}, u_1, \dots, u_{l_1}) \in T_{\mathcal{G}}(\mathbf{C})$$

belongs to $T_{\mathcal{H}}(\mathbf{C})$. According to the definition of r_{str}, there exists $(z_1, \dots, z_l)$ in $T_{\mathcal{H}}(\mathbf{C})$ such that

$$\dim_{\mathbf{C}}(\mathbf{C}z_1 + \cdots + \mathbf{C}z_l) = l^*.$$

We choose l^* elements among $\{z_1, \dots, z_l\}$, linearly independent over $\mathbf{C}$. For simplicity of notation, say that $z_1, \dots, z_{l_0^*}, z_{l_0+1}, \dots, z_{l_0+l_1^*}$ are linearly independent over $\mathbf{C}$, with $l_0^* + l_1^* = l^*$. We define $W^* = \mathbf{C}\beta_1 + \cdots + \mathbf{C}\beta_{l_0^*}$ and $Y^* = \mathbf{Z}u_1 + \cdots + \mathbf{Z}u_{l_1^*}$. Plainly, we have $W^* \cap Y^* = 0$, and the pair (W^*, Y^*) has rank (l_0^*, l_1^*).

We denote by $\mathcal{H}^*$ the smallest algebraic subgroup of $\mathcal{G} = \mathbf{G}^{dl_0^*} \times G^{l_1^*}$ which is defined over K and such that $(\beta_1, \dots, \beta_{l_0^*}, u_1, \dots, u_{l_1^*})$ belongs to $T_{\mathcal{H}^*}(\mathbf{C})$. We also put

$$\mathcal{G}^{**} = \mathbf{G}_a^{d(l_0 - l_0^*)} \times G^{l_1 - l_1^*},$$

in such a way that $(v_1, \dots, v_l)$ belongs to $T_{\mathcal{H}^*}(\mathbf{C}) \times T_{\mathcal{G}^{**}}(\mathbf{C})$. Hence, $\mathcal{H} \subset \mathcal{H}^* \times \mathcal{G}^{**}$, which implies that $(z_1, \dots, z_{l_0^*}, z_{l_0+1}, \dots, z_{l_0+l_1^*})$ belongs to $T_{\mathcal{H}^*}(\mathbf{C})$, and consequently

$$r_{\mathrm{str}}\,(W^*, Y^*; G) = l^*. \qquad \square$$

Lemma 14. *Let G be a commutative algebraic group which is defined over a subfield K of $\mathbf{C}$, and let (W, Y) be a K-arithmetic pair of rank*

(l_0, l_1). Define $l = l_0 + l_1$ and assume $r_{\mathrm{str}}(W, Y; G) = l$. If G^* is an algebraic subgroup of G defined over K, W^* is a subspace of W and Y^* a subgroup of Y such that $W^* \subset T_{G^*}(\mathbf{C})$ and $Y^* \subset T_{G^*}(\mathbf{C})$, then

$$r_{\mathrm{str}}(W^*, Y^*; G^*) = l_0^* + l_1^*$$

where (l_0^*, l_1^*) is the rank of the pair (W^*, Y^*).

Proof. Assume $r_{\mathrm{str}}(W^*, Y^*; G^*) < l^*$ where $l^* = l_0^* + l_1^*$. Choose first a basis $(\beta_1, \dots, \beta_{l_0})$ of W so that $(\beta_1, \dots, \beta_{l_0^*})$ is a basis of W^*, and next elements $u_1, \dots, u_{l_1}$ in Y which are linearly independent over $\mathbf{Z}$ modulo W, while $u_1, \dots, u_{l_1^*}$ belong to Y^*. Further, let $\mathcal{H}^*$ be an algebraic subgroup of minimal dimension of $\mathbf{G}_a^{dl_0^*} \times \{G^*\}^{l_1^*}$ such that $(\beta_1, \dots, \beta_{l_0^*}, u_1, \dots, u_{l_1^*})$ belongs to $T_{\mathcal{H}^*}(\mathbf{C})$. From the assumption $r_{\mathrm{str}}(W^*, Y^*; G^*) < l^*$ we deduce that any $(z_1, \dots, z_{l_0^*}, z_{l_0+1}, \dots, z_{l_0+l_1^*})$ in $T_{\mathcal{H}^*}(\mathbf{C})$ satisfies

$$\dim_{\mathbf{C}}(\mathbf{C}z_1 + \cdots + \mathbf{C}z_{l_0^*} + \mathbf{C}z_{l_0+1} + \cdots + \mathbf{C}z_{l_0+l_1^*}) < l^*.$$

On the other hand, if we introduce the algebraic group

$$\mathcal{G}^{**} = \mathbf{G}_a^{d(l_0 - l_0^*)} \times G^{l_1 - l_1^*},$$

then we have

$$(\beta_1, \dots, \beta_{l_0}, u_1, \dots, u_{l_1}) \in T_{\mathcal{H}^*}(\mathbf{C}) \times T_{\mathcal{G}^{**}}(\mathbf{C}),$$

and for each $(z_1, \dots, z_l) \in T_{\mathcal{H}^*}(\mathbf{C}) \times T_{\mathcal{G}^{**}}(\mathbf{C})$, we have

$$(z_1, \dots, z_{l_0^*}, z_{l_0+1}, \dots, z_{l_0+l_1^*}) \in T_{\mathcal{H}^*}(\mathbf{C}),$$

hence

$$\dim_{\mathbf{C}}(\mathbf{C}z_1 + \cdots + \mathbf{C}z_l) < l,$$

which proves $r_{\mathrm{str}}(W, Y; G) < l$. □

Lemma 15. *Let G be a commutative algebraic group which is defined over $\mathbf{C}$, G^* an algebraic subgroup of G, W a subspace of $T_G(\mathbf{C})$ and Y a finitely generated subgroup of $T_G(\mathbf{C})$. Define*

$$W^* = W \cap T_{G^*}(\mathbf{C}), \qquad Y^* = Y \cap T_{G^*}(\mathbf{C})$$

and

$$G' = \frac{G}{G^*}, \qquad W' = \frac{W}{W^*} \subset T_{G'}(\mathbf{C}), \qquad Y' = \frac{Y}{Y^*} \subset T_{G'}(\mathbf{C}).$$

Then

$$r(W, Y; G) \geq r(W', Y'; G') + r(W^*, Y^*; G^*).$$

Proof. We choose a basis of $T_{G^*}(\mathbf{C})$ which we complete into a basis of $T_G(\mathbf{C})$. We denote by (l_0, l_1) the rank of the pair (W, Y) and by (l_0^*, l_1^*) the rank of the pair (W^*, Y^*). Next we choose a basis $(\beta_1, \dots, \beta_{l_0})$ of W such that $(\beta_{l_0 - l_0^* + 1}, \dots, \beta_{l_0})$ is a basis of W^*. Finally, we choose $u_1, \dots, u_{l_1}$ in Y which are linearly independent over $\mathbf{Z}$ modulo W, and such that $u_{l_1 - l_1^* + 1}, \dots, u_{l_1}$ belong to Y^*. The matrix of the components of $\beta_1, \dots, \beta_{l_0}$, $u_1, \dots, u_{l_1}$ in the given basis of $T_G(\mathbf{C})$ can be written

$$M = \begin{pmatrix} M' & 0 \\ M'' & M^* \end{pmatrix},$$

where M is of the rank $r(W, Y; G)$, M' is of rank $r(W', Y'; G')$ and M^* is of rank $r(W^*, Y^*; G^*)$. □

Proof of Theorem 9. According to Lemma 13, there is no loss of generality to assume $Y \cap W = 0$ and $r_{\text{str}}(W, Y; G) = l = l_0 + l_1$ where $l_0 = \dim_{\mathbf{C}} W$ and $l_1 = \operatorname{rank}_{\mathbf{Z}} Y$. Therefore, $l \leq d$. Also, we may (and will) assume that there no algebraic subgroup G^* other than G which is defined over K and such that $W + \mathbf{C}Y \subset T_{G^*}(\mathbf{C})$; otherwise, we just replace G by the smallest G^* with this property. Finally, thanks to the assumption $r_{\text{str}}(W, Y; G) = l$, we may assume that the vector space W does not contain any nonzero $T_{\tilde{G}}(\mathbf{C})$ for $\tilde{G}$ an algebraic subgroup of G over K of positive dimension (otherwise we replace G by the quotient $G/\tilde{G}$).

We prove the lower bound $r \geq l/(\varrho+1)$ for the number $r = r(W, Y; G)$ by induction on l. For $l = l_0$, we plainly have $r = l_0$, and the estimate holds true. We assume now that $l_1 \geq 1$ and that the result has already been proved for the K-arithmetic pairs (W^*, Y^*) of $T_G(\mathbf{C})$ of rank (l_0^*, l_1^*) for which $l_0^* + l_1^* < l$. We use the theorem of the algebraic subgroup above: there exists an algebraic subgroup G^* of G, defined over K, of dimension $d-d'$ with $1 \leq d' \leq d$, such that, with the notations of Corollary 12,

$$\frac{r}{d} \geq \frac{r'}{d'} \geq \frac{l_1' + \varrho\, l_0'}{l_1' + \varrho\, d'}.$$

We now define $l' = l_0' + l_1'$, and we consider two cases:

a) Assume that $d' \leq l'$. In this case, $d' \leq (\varrho+1)l_0' + l_1'$ and

$$\frac{l_1' + \varrho\, l_0'}{l_1' + \varrho\, d'} \geq \frac{1}{\varrho+1},$$

which implies

$$r \geq \frac{d}{\varrho+1} \geq \frac{l}{\varrho+1}.$$

This completes the proof in case a).

b) Assume that $d' \geq l'$. Then we have

$$d'(l_1' + \varrho^2 l_0') \geq l' l_1';$$

hence,

$$(\varrho+1)d'(l_1' + \varrho\, l_0') \geq l'(l_1' + \varrho\, d'),$$

which implies

$$r' \geq \frac{l'}{\varrho+1}.$$

We define $W^* = W \cap T_{G^*}(\mathbf{C})$, $Y^* = Y \cap T_{G^*}(\mathbf{C})$, and $l^* = l_0^* + l_1^*$ where (l_0^*, l_1^*) is the rank of the pair (W^*, Y^*). Since $W + \mathbf{C}Y$ is not contained in $T_{G^*}(\mathbf{C})$, we have $l^* < l$. Using Lemma 14 we deduce $r_{\mathrm{str}}(W^*, Y^*; G^*) = l^*$, hence the induction hypothesis implies

$$r^* = r(W^*, Y^*; G^*) \geq l^*/(\varrho+1).$$

finally we conclude with Lemma 15:

$$r \geq r' + r^* \geq \frac{l^*}{\varrho+1} + \frac{l^*}{\varrho+1} = \frac{l}{\varrho+1}. \qquad \square$$

Acknowledgments. The author wishes to thank Daniel Bertrand for his help during the preparation of this paper, and Damien Roy whose comments on a preliminary version induced substantial modifications.

REFERENCES

1. D. Bertrand, *Galois representations and transcendental numbers*, in *New advances in transcendence theory* (A. Baker, ed.), Cambridge University Press, 1988, 31–55.

2. ———, *Points rationnels sur les sous-groupes compacts des groupes algébriques*, Experimental Mathematics **4** (1995), 165–151.

3. S. Lang, *Introduction to transcendental numbers*, Addison Wesley, 1966.

4. D. Roy, *Matrices dont les coefficients sont des formes linéaires de logarithmes*, Prog. Math. **81** (1990), 273–281.

5. ———, *Sur la conjecture de Schanuel pour les logarithmes de nombres algébriques*, Publ. Math. Univ. Paris VI **90** (1988), 269–276.

6. ———, *Transcendence et questions de répartition dans les groupes algébriques*, in *Approximations diophantiennes et nombres transcendants* (P. Philippon, ed.), W. de Gruyter, 1992.

7. ———, *Matrices whose coefficients are linear forms in logarithms*, J. Number Theory **41** (1992), 22–47.

8. ———, *Points whose coordinates are logarithms of algebraic numbers on algebraic varieties*, Acta Math. **175** (1995), 69–73.

9. M. Waldschmidt, *Dépendance de logarithmes dans les groupes algébriques*, Prog. Math. **31** (1983), 289–328.

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

11. ———, *Densité de points rationnels sur les groupes algébriques*, Experimental Mathematics **3** (1994), 329–352. Errata, Ibid., **4** (1995) 255.

12. G. Wüstholz, *Some remarks on a conjecture of Waldschmidt*, Prog. Math. **31** (1983), 329–336.

13. ———, *Algebraische Punkte auf analytischen Untergruppen algebraischer Gruppen*, Ann. Math. **129** (1989), 501–517.

Institut de Mathématiques, Problèmes Diophantiens, Université P. et M. Curie (Paris 6), T. 45-46, 5ème Et., Case 247, 4, Place Jussieu F-75252 Paris Cedex 05, France
E-mail address: miw@ccr.jussieu.fr