Algebraic points in analytic subgroups of algebraic groups

By GISBERT WÜSTHOLZ

1 Introduction

It is the aim of this work to prove a general result on the arithmetic properties of analytic homomorphisms between commutative algebraic groups. Many results and problems in transcendental number theory can be reduced to this question, and our main result gives an answer to a series of open problems.

It became apparent that the study of analytic homomorphisms between commutative algebraic groups has been very beneficial for transcendental number theory and leads to beautiful results. This was noted by S. Lang about twenty years ago, and he proved in [L1] that for $\overline{\mathbb{Q}}$-defined commutative algebraic groups G and elements $\alpha \neq 0$ in $\mathrm{T}(G)(\overline{\mathbb{Q}})$, the image $\exp_G(\alpha)$ under the exponential map in general does not lie in $G(\overline{\mathbb{Q}})$. Here, $\mathrm{T}(G)$ denote the tangent space of G at the identity element, $\mathrm{T}(G)(\overline{\mathbb{Q}})$ the set of $\overline{\mathbb{Q}}$-rational points of $\mathrm{T}(G)$ and $G(\overline{\mathbb{Q}})$ the subgroup of algebraic points of G. In other words, $G(\overline{\mathbb{Q}})$ is the group of $\overline{\mathbb{Q}}$-valued points of the group scheme G. From this result by Lang a whole series of results on transcendence can be derived. Among others, one can derive the transcendence of e^{α} for algebraic $\alpha \neq 0$, if we set $G = \mathbf{G}_{\mathrm{m}}$, where $\mathbf{G}_{\mathrm{m}}$ denotes the multiplicative group scheme. This is the famous Lindemann Theorem. This result corresponds to a result on one-parameter subgroups of algebraic groups. Shortly after, it was extended by Lang [L2, L3] in several directions to d-parameter subgroups of algebraic groups. All these works were based on a method developed by Schneider [Sch1, Sch2].

A second fundamental method was developed by A. Baker [Ba1, Ba2] in connection with the study of linear forms of logarithms of algebraic numbers. It will play a central role in our investigations, together with the so-called zero estimates of algebraic groups. These were developed in recent years by D.W. Masser and the author [Ma-Wü1, Ma-Wü2, Ma-Wü3] and extended by the author [Wü1] to multiplicity estimates.

In the following let G be a connected commutative algebraic group of dimension n and $\mathrm{T}(G)$ its tangent space at the identity element. As a $\overline{\mathbb{Q}}$-vector space of derivations of the local ring of G at the identity element, the latter has a $\overline{\mathbb{Q}}$-structure in

a natural manner that extends to left- and right-invariant vector fields. In particular, the exponential map can be chosen such that the analytic functions appearing in it have a power series extension at the origin with algebraic coefficients. The exponential map

$$\exp_G : \mathrm{T}(G) \to G$$

is thus also $\overline{\mathbb{Q}}$-defined (however, not in the category of schemes with respect to the Zariski topology).

If G and G' are complex Lie groups, then a homomorphism

$$\varphi : G' \to G$$

is called *analytic* if φ is a homomorphism of complex Lie groups. In the following, we only consider commutative Lie groups. It is well-known that φ induces a linear map

$$\mathrm{d}\varphi : \mathrm{T}(G') \to \mathrm{T}(G)$$

between the tangent spaces, such that the diagram

$$\begin{array}{ccc} G' & \xrightarrow{\varphi} & G \\ {\scriptstyle \exp_{G'}}\uparrow & & \uparrow{\scriptstyle \exp_G} \\ \mathrm{T}(G') & \xrightarrow{\mathrm{d}\varphi} & \mathrm{T}(G) \end{array}$$

commutes. If G' and G are $\overline{\mathbb{Q}}$-defined algebraic groups, then we call φ $\overline{\mathbb{Q}}$-*defined* if $\mathrm{d}\varphi$ is a homomorphism of $\overline{\mathbb{Q}}$-vector spaces. Note that in general $\varphi(G')$ is not a closed subgroup of G. If the differential $\mathrm{d}\varphi$ is injective, we call φ an *analytic subgroup* of G.

Main Theorem *Let G and G' be $\overline{\mathbb{Q}}$-defined connected commutative algebraic groups with* $\dim G, \dim G' > 0$ *and*

$$\varphi : G' \to G$$

a $\overline{\mathbb{Q}}$-defined analytic homomorphism. If $\varphi(G')(\overline{\mathbb{Q}}) \neq \mathbf{0}$, then there exists an algebraic subgroup $H \subseteq \varphi(G')$ defined over $\overline{\mathbb{Q}}$ with $\dim H \geq 1$.

Remarks

1. If H is a $\overline{\mathbb{Q}}$-defined algebraic subgroup of $\varphi(G')$, then clearly $H(\overline{\mathbb{Q}}) \subseteq \varphi(G')(\overline{\mathbb{Q}})$. So the Main Theorem is just the converse of this trivial fact.

2. If $H \subseteq \varphi(G')$ is the maximal $\overline{\mathbb{Q}}$-defined algebraic subgroup, then

$$H(\overline{\mathbb{Q}}) = \varphi(G')(\mathbb{C}) \cap G(\overline{\mathbb{Q}}).$$

To see this, consider the canonical homomorphism $\pi : G \to G/H$. As $H' = (\pi \circ \varphi)^{-1}(\mathbf{0})$ is a closed Lie subgroup of G', we can form G'/H' and obtain a Lie group G''. Now consider the induced homomorphism $\overline{\varphi} : G'' \to G/H$ and obtain an analytic homomorphism

$$\mathrm{T}(G'') \xrightarrow{\exp_{G''}} G'' \xrightarrow{\overline{\varphi}} G/H.$$

This one we call $\varphi_0 : \mathrm{T}(G'') \to G/H$. It is a $\overline{\mathbb{Q}}$-defined analytic homomorphism with injective differential $\mathrm{d}\varphi_0$ between two commutative algebraic groups. If $\dim \mathrm{T}(G'') = 0$ or $\dim G/H = 0$, then we are done. Otherwise we can apply the Main Theorem to find that $\varphi_0(\mathrm{T}(G'')) \cap (G/H)(\overline{\mathbb{Q}}) = \mathbf{0}$.

3. In Remark 2 we already used the fact that we can always assume without loss of generality that G' is a vector space. In fact, we only need to set $V = \mathrm{T}(G')$ and replace φ by $\varphi \circ \exp_{G'}$.

4. We may assume without loss of generality that $\mathrm{d}\varphi$ is injective, and can then identify V with a vector subspace of $\mathrm{T}(G)$.

5. The theorem is non-trivial only if $\dim \varphi(G') < \dim G$. Otherwise, $H = G$ has the desired property.

6. It is enough to prove the theorem for the case $\dim G' = n - 1$, where $n = \dim G$. In fact, by Remark 3 we may assume that G' is a d-dimensional vector space V and by Remark 4 we may assume that $d < n$. Now $\mathrm{d}\varphi$ is injective, so that we can identify V with a subalgebra of $\mathrm{T}(G)$. But this is always contained in an $n-1$-dimensional subalgebra W of $\mathrm{T}(G)$. If V is $\overline{\mathbb{Q}}$-defined, then W can also be chosen as $\overline{\mathbb{Q}}$-defined. Once we have found an algebraic subgroup $H = H(W)$, we set

$$H = \bigcap_{W \supset V} H(W),$$

where the intersection is taken over all such W. This is a non-trivial algebraic subgroup of dimension different from 0 that is contained in $\varphi(G')$ and is $\overline{\mathbb{Q}}$-defined. In fact, we have

$$H(\overline{\mathbb{Q}}) = \bigcap_{W \supset V} H(W)(\overline{\mathbb{Q}}) = \varphi(G')(\mathbb{C}) \cap G(\overline{\mathbb{Q}}).$$

If the right-hand side contains an element different from 0, then it contains infinitely many. Thus $H(\overline{\mathbb{Q}})$ is infinite and $\dim H \neq 0$.

As the perhaps most interesting application of this theorem we mention the following theorem which will be proved in a future article. Let X be a smooth quasi-projective variety over $\overline{\mathbb{Q}}$ and let γ represent a class in $\mathrm{H}_1(X, \mathbb{Z})$. If ω represents a class in $\mathrm{H}^0(X, \Omega^1_X)$, then the following holds:

Theorem *The integral $\int_\gamma \omega$ is either 0 or transcendent.*

Remark The integral depends only on the classes of γ and ω.

2 Some preliminary remarks

To employ the techniques of the theory of transcendental numbers, we need some preparations. In particular, we need an explicit description of the exponential map. This is done in [F-W], and we will briefly recall it here.

Let G be a commutative connected algebraic group. It is known that there is a maximal connected linear subgroup L of G such that G is an extension of an abelian variety A by L. After an algebraic extension of the base field, L becomes isomorphic to a product of multiplicative groups $\mathbf{G}_\mathrm{m}$ and additive groups $\mathbf{G}_\mathrm{a}$,

$$L \xrightarrow{\sim} \mathbf{G}_\mathrm{a}^{l_1} \times \mathbf{G}_\mathrm{m}^{l_2}.$$

The linear subgroup L is compactified in a suitable manner to $\overline{L}$ with L-operations, and we set $G \times \overline{L}/L = \overline{G}$. This is a fiber bundle over A with fiber $\overline{L}$. We then obtain divisors $E_1, \ldots, E_{l_1+l_2}$ on $\overline{G}$ that come from the compactification of L. Set $E' = E_1 + \ldots + E_{l_1}$, $E'' = E_{l_1+1}, \ldots, E_{l_1+l_2}$ and $E = E' + E''$. The divisor E' belongs to the additive and the divisor E'' belongs to the multiplicative part of L. If $p : \overline{G} \to A$ is the canonical projection and D an ample divisor on A, then we set

$$D_{a,b} = a \cdot p^*(D) + b \cdot E$$

for integers $a, b \geq 1$. This divisor is very ample for $a \geq 3$ and $b \geq 1$. For such numbers a and b we consider the sheaf $\mathcal{O}_{\overline{G}}(D_{a,b})$ on $\overline{G}$. Then every basis $x_0, \ldots, x_N$ of $\mathrm{H}^0(\overline{G}, \mathcal{O}_{\overline{G}(D_{a,b})})$ gives an embedding j of $\overline{G}$ into $\mathbb{P}^N$. Here, $N = \dim \mathrm{H}^0(\overline{G}, \mathcal{O}_{\overline{G}(D_{a,b})}) - 1$. This embedding is such that the divisor E is contained in the divisor on $\overline{G}$ defined by $x_0 \cdots x_N = 0$.

If $[l]$ denotes the multiplication on G with $0 \neq l \in \mathbb{N}$ that extends to a morphism on $\overline{G}$, then $[l]^* D_{a,b} \sim l^2 D_{a,b} - b Z_1$ for a positive divisor Z_1 on $\overline{G}$ with support contained in that of E. Therefore, there exist homogeneous polynomials $\Phi_0^{(l)}, \ldots, \Phi_N^{(l)}$ in $x_0, \ldots, x_N$ such that for $g \in G$ the homogeneous coordinates of lg are given by

$$(x_0, \ldots, x_N)(lg) = (\Phi_0^{(l)}, \ldots, \Phi_N^{(l)})(g).$$

Now set $\varphi_i^{(l)} = j^*\Phi_i^{(l)}$ for $0 \le i \le N$. Then $\varphi^{(l)} = (\varphi_0^{(l)}, \dots, \varphi_N^{(l)})$ defines a rational map from $\overline{G}$ to $\overline{G}$. This is undefined along a divisor $\tilde{E} \subseteq E$, but otherwise coincides with $[l]$.

By the *height* of a point or a polynomial we mean the *Weil height*. For $\alpha \in \mathbb{P}^n(K)$ for an algebraic number field K this is defined by

$$H(\alpha) = \prod_v \max_i(|\alpha_i|_v),$$

where $\alpha = (\alpha_0, \dots, \alpha_N)$ and $|\cdot|_v$ runs through the normed absolute values of K. If P is a polynomial of degree $d(P) \le D$ in n variables with coefficients in K, then it corresponds to a point in the projective space $\mathbb{P}^N$, where $N = \binom{D+n}{n}$. Its height is defined to be that of the corresponding point.

Proposition 2.0 *Let G be defined over $\overline{\mathbb{Q}}$ and $l \ge 1$ integer. Then there are constants $c_1, c_2 > 0$ with the following property. If $m \ge 0$ is an integer and $g, g' \in G(\overline{\mathbb{Q}})$ with $l^m g' = g$, then the logarithmic height $h(g')$ of g' can be estimated by*

$$h(g') \le c_1 l^{c_2 m}(h(g) + 1).$$

PROOF: We set $\eta_i = x_i(g)$ for $0 \le i \le N$, and

$$f_{ij} = \eta_i \varphi_j^{(l)} - \eta_j \varphi_i^{(l)} \quad (0 \le i, j \le N).$$

Furthermore, let $g^{(1)}, \dots, g^{(\delta)}$ be the solutions of $lg' = g$ and $\eta_i^{(\nu)} = x_i(g^{(\nu)})$. Then $\delta | l^{2n}$. For $s < t$ we set

$$R = R(x_s, x_t) = \prod_{j=1}^{\delta} (\eta_t^{(j)} x_s = \eta_s^{(j)} x_t),$$

so that R vanishes in $g^{(1)}, \dots, g^{(\delta)}$. If $\mu = x_0 \cdots x_N$, then μR vanishes on $(\varphi^{(l)})^{-1}(g)$. Then it holds by Hilbert's Nullstellensatz that $(\mu R)^e \in I$ for some positive exponent e, that is,

$$(\mu R)^e = \sum h_{ij} f_{ij}$$

with homogeneous polynomials h_{ij} in $x_0, \dots, x_N$. This is a system if linear equations in the coefficients of R and the h_{ij}. According to [Ma-Wü1], Chapter 4, in particular Theorem IV and Lemma 4, we find the following estimate for the height of $(\mu R)^e$,

$$\log H((\mu R)^e) \le c_1 \delta^{c_2}(h(g) + 1).$$

Since $H((\mu R)^e) = H(R^e)$, we obtain the desired inequality for $m = 1$ after some known estimates. For $m = 0$ the inequality is trivial anyway, and for $m > 1$ it follows by induction. $\diamond$

The following observation is important in what follows. If $\Gamma \subseteq G$ is a finitely generated subgroup of G, we can choose a basis $x_0, \ldots, x_N$ of $\mathrm{H}^0(\overline{G}, \mathcal{O}_{\overline{G}}(D_{a,b}))$ such that $x_0(\gamma) \neq 0$ for all $\gamma \in \Gamma$. This can be achieved via an automorphism of $\mathrm{H}^0(\overline{G}, \mathcal{O}_{\overline{G}}(D_{a,b}))$ over $\overline{\mathbb{Q}}$.

Let U denote the open affine set $\overline{G} \cap (x_0 \neq 0)$ of $\overline{G}$. As the translationally invariant vectro fields on G extend to translationally invariant vector fields on $\overline{G}$, for every vector field $\Delta : \mathcal{O}_{\overline{G}} \to \mathcal{O}_{\overline{G}}$ the induced map

$$\Delta : \Gamma(U, \mathcal{O}_{\overline{G}}) \to \Gamma(U, \mathcal{O}_{\overline{G}})$$

is a derivation. Thus Δ stabilizes the affine algebra of U. A basis of the Lie algebra of invariant vector fields induces linearly independent derivations $\partial_1, \ldots, \partial_n$ of this affine algebra.

Now let $\varphi : G' \to G$ be an analytic subgroup with image $B \subset G$. Though this is not closed, but itself a Lie group with tangent space $\mathrm{T}(B)$ in the unity element. Henceforth we will identify the analytic subgroup φ with its image B and its tangent space $\mathrm{T}(B)$ with a subspace of $\mathrm{T}(G)$. We can do this, as the Main Theorem only makes a claim about the image. Finally, we identify the algebraic group G with its image in $\mathbb{P}^N$.

Let $X_0, \ldots, X_N$ be coordinates of $\mathbb{P}^N$ with $x_i = j^* X_i$ for $0 \leq i \leq N$. Then we set for $0 \leq i \leq N$

$$f_i = X_i \circ j \circ \exp_G = x_i \circ \exp_G .$$

As $f_0, \ldots, f_N$ are sections of $\exp_G^*)(D_{a,b})$ and the latter is a trivial line bundle, we can identify $f_0, \ldots, f_N$ with functions on the tangent space $\mathrm{T}(G)$. This again can be identified with $\mathbb{C}^n$ via $\partial_1, \ldots, \partial_n$.

The function f_i are analytic and have order of growth at most 2 (see for example [F-W]). Further, we set

$$g_i = f_i / f_0 \quad (1 \leq i \leq N)$$

and obtain meromorphic functions that are analytic in a neighbourhood of the origin of $\mathrm{T}(G)$.

Henceforth we will also assume that G as well as φ is $\overline{\mathbb{Q}}$-defined. The the functions $g_1, \ldots, g_N$ satisfy a system of algebraic differential equations with algebraic coefficients, since the derivations $\partial_1, \ldots, \partial_n$ form a basis of the vector space of derivations of $\Gamma(U, \mathcal{O}_{\overline{G}})$ over $\overline{\mathbb{Q}}$. Let $\boldsymbol{z} = (z_1, \ldots, z_n)$ be the coordinates of $\mathrm{T}(G)$ in this basis. Then the functions $g_i(\boldsymbol{z})$ $(0 \leq i \leq N)$ have power series expansions

with algebraic coefficients at the origin. The functions $f_0(\boldsymbol{z}), \ldots, f_N(\boldsymbol{z})$ and the functions $g_1(\boldsymbol{z}), \ldots, g_N(\boldsymbol{z})$ have order of growth ≤ 2. Hence

$$\log |f_i(\boldsymbol{z})| \leq c_1 \|\boldsymbol{z}\|^2 \quad (0 \leq i \leq N), \tag{1}$$

where we set $\|\boldsymbol{z}\|^2 = (|z_1|^2 + \ldots + |z_n|^2)^{\frac{1}{2}}$, with a positive constant c_1 independent of $\boldsymbol{z}$. Moreover, $f_0(\boldsymbol{u}) \neq 0$ for $\boldsymbol{u} \in \exp_G^{-1}(\Gamma)$, where Γ denotes the group introduced before.

The addition $+ : G \times G \to G$ extends to a morphism $+ : \overline{G} \times \overline{G} \to \overline{G}$ ([Se]). Instead of $+$ we shall occasionally write m. So the following lemma holds:

Lemma 2.1 *There is a finite set E, an integer $b > 0$, a map $\nu : \Gamma \to E$ and bihomogeneous polynomials*

$$E_{e,i}(Y_0, \ldots, Y_N; X_0, \ldots, X_n) \quad (e \in E, - \leq i \leq N)$$

of bidegree b with coefficients in $\overline{\mathbb{Q}}$, as well as open affine sets $U_e \subset \overline{G} \times G$ with $(\gamma, 0) \in U_{\nu(\gamma)}$, such that the following holds:

(i) *The sets U_e, $e \in E$, cover all of $\overline{G} \times G$.*

(ii) *For $(g, g') \in U_e$,*

$$t(g, g') \cdot X_i(g + g') = E_{e,i}(Y_0(g), \ldots, Y_N(g); X_0(g'), \ldots, X_n(g'))$$

for $0 \leq i \leq N$ and $0 \neq t(g, g') \in \overline{\mathbb{Q}}$ independent of i.

(iii) *The height of the polynomials $E_{e,i}$ is bounded by a constant $c_2 > 0$.*

Remark The X_i, Y_i $(0 \leq i \leq N)$ are actually sections of a line bundle. Upon restriction to open affine sets we may view them as functions. In fact, the pullback of a line bundle via the inclusion map of an affine set is trivial.

PROOF: (of Lemma 2.1) It all follows immediately from the fact that the addition on G is a morphism $G \times G \to G$ and the topological space G with the Zariski topology is noetherian. $\diamond$

We now fix the analytic subgroup B with $0 < d = \dim B < \dim G$. Its tangent space $\mathrm{T}(B)$ is identified with the Lie algebra of B. This is a subalgebra of $\mathfrak{Lie}(G) = \mathrm{T}(G)$. A basis of $\mathrm{T}(G)$ is given by $\partial_1, \ldots, \partial_n$. As we assumed that B is $\overline{\mathbb{Q}}$-defined, there exists a basis $\Delta_1, \ldots, \Delta_d$ of $\mathfrak{Lie}(B)$ with

$$\Delta_i = \alpha_{i1}\partial_1 + \ldots + \alpha_{in}\partial_n \quad (1 \leq i \leq d)$$

and $\alpha_{11}, \ldots, \alpha_{dn} \in \overline{\mathbb{Q}}$.

If $P(X_0, \ldots, X_N)$ is a homogeneous polynomial and $g \in G$ such that $X_0(g) \neq 0$, the define the *order* of $P(X_0, \ldots, X_N)$ in g as the minimal t for which there exist non-negative numbers $t_1, \ldots, t_d$ with $t_1 + \ldots + t_d = t$ and

$$\Delta_1^{t_1} \ldots \Delta_d^{t_d} P\left(1, \frac{x_1}{x_0}, \ldots, \frac{x_N}{x_0}\right)(g) \neq 0.$$

The order is thus a non-negative integer or infinite. In particular, all elements in the homogeneous ideal $I(G)$ of G have order infinite. The definition of order of course depends on B, and we also call it the *order along* B. We write $\mathrm{ord}_{g,B}(P)$.

As the derivations $\Delta_1, \ldots, \Delta_d$ are invariant under translations, it immediately follows that the order of $P(X_0, \ldots, X_N)$ in $\gamma \in \Gamma$ equals the order of

$$P(E_{\nu(\gamma),0}(\boldsymbol{Y}(\gamma); \boldsymbol{X}), \ldots, E_{\nu(\gamma),N}(\boldsymbol{Y}(\gamma); \boldsymbol{X}))$$

in the point 0, where $\boldsymbol{Y} = (Y_0, \ldots, Y_N)$ and $\boldsymbol{X} = (X_0, \ldots, X_N)$ (see [Wü2] for details).

The following remark will be important later on. If G, B and Γ are $\overline{\mathbb{Q}}$-defined, then there exists an algebraic number field K over which these objects are defined.

We now show that we can find an "addition rule" on G that is valid on all points of Γ. For this, let κ be the cardinality of E in Lemma 2.1 and $L \subseteq K$ the smalles algebraic number field such that G and Γ are defined over L. Then we want to choose K large enough for $[K : L] \geq \kappa$ to hold, and choose elements $\omega_e \in K$, $e \in E$, that span an L-vector space of dimension κ. We then set

$$E_i(\boldsymbol{Y}, \boldsymbol{X}) = \sum_{e \in E} \omega_e E_{e,i}(\boldsymbol{Y}; \boldsymbol{X})$$

for $0 \leq i \leq N$. Then there exists a neighbourhood $V \supset \Gamma \times \mathbf{0}$ with the property that for $(g, g') \in V$ and some $t \neq 0$,

$$t \cdot X_i(g + g') = E_i(\boldsymbol{Y}, \boldsymbol{X})(g, g') \quad (0 \leq i \leq N).$$

In fact, either all $E_{e,i}(\boldsymbol{Y}(g); \boldsymbol{X}(g'))$ are zero, or the coordinate of $g + g'$ up to a multiplicative factor $t_e(g, g')$ which is independent of i. In particular, $E_0(\boldsymbol{Y}, \boldsymbol{X})(\gamma, 0) \neq 0$, since $X_0(\gamma) \neq 0$ by the choice of the coordinates. The addition rule will be called

$$\boldsymbol{E}(\boldsymbol{Y}, \boldsymbol{X}) = (E_0(\boldsymbol{Y}, \boldsymbol{X}), \ldots, E_N(\boldsymbol{Y}, \boldsymbol{X})).$$

In other words, $\boldsymbol{E}(\boldsymbol{Y}, \boldsymbol{X})(g, g')$ are the coordinates of $g + g'$.

3 A lemma on differentiation

For the following we need precise estimates for the growth and height of derived polynomials, depending on the degree of the differential operators. For this, we first give an explicit description of the differential operators.

We fix an algebraic number field K over which G, A, $\boldsymbol{E}$ and Γ are defined. The affine algebra $\Gamma(U, \mathcal{O}_{\overline{G}})$ of U is generated by $\xi_i = \frac{x_i}{x_0}$ for $1 \leq i \leq N$ and can be written as $K[\xi_1, \ldots, \xi_N]$. As the derivations $\partial_1, \ldots, \partial_n$ stabilize the algebra $K[\xi_1, \ldots, \xi_N]$, we have

$$\partial_i \xi_j = p_{ij}(\xi_1, \ldots, \xi_N) \quad (1 \leq i \leq n; 1 \leq j \leq N)$$

with polynomials p_{ij} in $\xi_1, \ldots, \xi_N$ with coefficients in K. If P is a homogeneous polynomial in $X_0, \ldots, X_N$, then $P \circ \boldsymbol{E}$ is bihomogeneous in $X_0, \ldots, X_N$ and $Y_0, \ldots, Y_N$, respectively. We can then apply the derivations $\Delta_1, \ldots, \Delta_d$ to

$$(P \circ \boldsymbol{E})(X_0, \ldots, X_N; 1, \xi_1, \ldots, \xi_N)$$

and obtain the following proposition:

Proposition 3.1 *If P has degree D and height H, $t_1, \ldots, t_d$ are non-negative integers with $t_1 + \ldots + t_d = T$ and $\Delta = \Delta_1^{t_1} \cdots \Delta_d^{t_d}$, then*

$$\Delta(P \circ \boldsymbol{E})(X_0, \ldots, X_N; 1, \xi_1(0), \ldots, \xi_N(0))$$

is a homogeneous polynomial P_Δ in $X_0, \ldots, X_N$ with

(i) $\deg P_\Delta = bD$.

(ii) $\log H(P_\Delta) \leq c(D + T)\log(D + T) + \log H$.

Here, c is a constant which is independent of D, T, H.

PROOF: A simple exercise using induction. ◇

4 The auxiliary polynomial

As before, let G be defined over an algebraic number field K, let G' be a vector space (or a vector group), assume φ to be injective and $d = n - 1$. We identify G' with a subspace of $\mathrm{T}(G)$. Then we choose $0 \neq \boldsymbol{u} \in \varphi^{-1}(G(\overline{\mathbb{Q}}))$ and set

$\gamma_0 = \varphi(\boldsymbol{u})$. By assumption, we can choose $\boldsymbol{u}$ such that $\gamma_0 \neq 0$. Let Γ denote the subgroup generated by γ_0 and e its order. For positive S, set

$$\Gamma(S) = \{s \cdot \gamma_0 \mid 0 \leq s \leq S\}.$$

The differential operators $\Delta_1, \ldots, \Delta_{n-1}$ generate a multiplicative monoid $\mathscr{D}$ whose elements have the form $\Delta_1^{t_1} \cdots \Delta_{n-1}^{t_{n-1}}$ with integers $t_1, \ldots, t_{n-1} \geq 0$. For integers $T \geq 0$ we consider the subset $\mathscr{D}(T)$ of those elements for which $t_1 + \ldots + t_{n-1} \leq T$ holds. Finally, let $m = [K : \mathbb{Q}]$ and choose the coordinates $X_0, \ldots, X_N$ such that $X_0(\gamma_0) = 1$. We now choose positive integers S, T, D with

$$D^n \geq 2nm(T+n)^{n-1}|\Gamma(S)|. \tag{2}$$

Further assume that T is sufficiently large to "swallow up" the constants $c_1, c_2, \ldots$ appearing below.

Lemma 4.1 *There exists a homogeneous polynomial $P(X_0, \ldots, X_N)$ with integer coefficients that is not contained in $I(G)$, and has degree D such that for all $\Delta \in \mathscr{D}(\frac{T}{2})$ and all $\gamma \in \Gamma(S)$:*

(i) $\operatorname{ord}_{\gamma,B} P_\Delta \geq \frac{T}{2}$.

(ii) $\log H(P_\Delta) \leq c_1(D+T)\log(D+T) + c_2 DS^2$.

PROOF: Since $\dim G = n$, we may assume without loss of generality that the homogeneous coordinates $X_0, \ldots, X_n$ are algebraically independent modulo the ideal $I(G)$. Then let $P(X_0, \ldots, X_n)$ be a homogeneous polynomial with yet undefined coefficients whose degree is D. The number of unknowns is then

$$\binom{D+n}{n} \geq \frac{D^n}{n!}.$$

We will now determine it so that

$$P_\Delta(\boldsymbol{X}(\gamma)) = 0 \tag{3}$$

holds for $\Delta \in \mathscr{D}(T)$, $\gamma \in \Gamma(S)$. This is a homogeneous system of linear equations with coefficients in K in the yet undetermined coefficients of P, since we can choose $X_i(\gamma) \in K$ due to $\Gamma \subseteq G(K)$ for $0 \leq i \leq N$. The number of equations is at most

$$m \cdot \binom{T+n-1}{n-1} \cdot |\Gamma(S)| \leq m\frac{(T+n)^{n-1}}{(n-1)!}|\Gamma(S)|.$$

As in the proof of Proposition 3.1 one verifies that the coefficients of this system of equations are bounded by

$$(D+T)^{c_3(D+T)}\Big(\max_{0\le i\le N}|X_i(\gamma)|\Big)^{c_4D}.$$

By Proposition 5 in [Se], the second factor in this estimate satisfies

$$\max_{0\le i\le N}|X_i(\gamma)|^{c_4D}\le c_5^{DS^2},$$

as γ is of the form $s\gamma_0$ with $s\le S$. Overall, we obtain the following estimate for the coefficients and their conjugates,

$$(D+T)^{c_3(D+T)}c_5^{DS^2}.$$

One obtains a similar estimate for the denominator which is the same up to the constants. According to Siegel's Lemma and considering (2) and Proposition 3.1 (ii), we obtain a polynomial P with (ii) and (3). It remains to show that (3) implies condition (i). This follows from Proposition 2 in [Wü2]. ◇

5 Some estimates

The coordinates in $\mathrm{T}(G)=\mathfrak{Lie}(G)$ are denoted by $\boldsymbol{z}=(z_1,\dots,z_n)$. The point $\boldsymbol{u}=(u_1,\dots,u_n)$ now defines a one-parameter subgroup of G in the following way: Define the linear map

$$L:\mathbb{C}\to\mathfrak{Lie}(G),\quad z\mapsto z\cdot\boldsymbol{u}.$$

Then $\exp_G\circ L$ is the one-parameter group we are looking for. Note: It is not defined over $\overline{\mathbb{Q}}$. This is the main difficulty with Baker's method.

On the other hand, we have the subspace $\mathfrak{Lie}(B)$ in $\mathfrak{Lie}(G)$ of codimension 1 which is defined over K. Thus it can be defined by a linear equation

$$\beta_nz_n=\beta_1z_1+\ldots+\beta_{n-1}z_{n-1}$$

with $\beta_1,\dots,\beta_n\in K$ and, without loss of generality, $\beta_n=1$. The vector $\boldsymbol{u}$ lies in $\mathfrak{Lie}(B)$ and thus satisfies the equation

$$u_n=\beta_1u_1+\ldots+\beta_{n-1}u_{n-1}.$$

We now set

$$\Delta_i=\partial_i+\beta_i\partial_n\quad(0\le i\le n-1).$$

Then

$$\frac{\mathrm{d}}{\mathrm{d}z} = u_1\Delta_1 + \ldots + u_{n-1}\Delta_{n-1}.$$

For $r > 0$ and homogeneous polynomials $P(X_0, \ldots, X_N)$ in $\mathbb{C}[X_0, \ldots, X_N]$ we set

$$\|P\|_r = \max_{\|z\| \le r} |(P \circ \exp_G)(\boldsymbol{z})|$$

and

$$\|P\|_{r,L} = \max_{\|z\| \le r} |(P \circ \exp_G \circ L)(\boldsymbol{z})|.$$

If P is the polynomial from Lemma 4.1, then the following lemma holds.

Lemma 5.1

(i) *For $\Delta \in D(\frac{T}{2})$ we have the estimate*

$$\log \|P_\Delta\|_r \le c_6(D+T)\log(D+T) + c_7 D(S^2 + r^2).$$

(ii) *For $\Delta \in D(\frac{T}{2})$ and $r > r' > S$,*

$$\log \|P_\Delta\|_{r',L} \le \log \|P_\Delta\|_{\|\boldsymbol{u}\| r} + \frac{ST}{2}\log\left(\frac{2rr'}{r^2 + r'^2}\right).$$

PROOF: The estimate in (i) follows immediately from Lemma 4.1 together with the estimates $f_i(\boldsymbol{z})$ $(i = 0, \ldots, N)$ at the beginning. To see the estimate (ii), set

$$\Psi(z) = P_\Delta \circ \exp_G \circ L(z).$$

From the representation for $\frac{\mathrm{d}}{\mathrm{d}z}$ and Lemma 4.1 it follows that $\Psi(z)$ has zeros in $z = s$ for $0 \le s \le S$, which have at least multiplicity $\frac{T}{2}$. For a function F that is holomorphic in $|z| \le r$ we set

$$|F|_R = \max_{|z|=R} |F(z)|.$$

If n_s is the order of Ψ in s and we set

$$h(z) = \prod_{s=0}^{S} \left(\frac{r^2 - sz}{r(z-s)}\right)^{n_s},$$

then Ψh is holomorphic in $|z| \le r$, so that by the Maximum Principle

$$|\Psi h|_{r'} \le |\Psi h|_r.$$

If one also considers that $|h|_r = 1$ holds, and for $|z| = r'$ the inequality

$$\left|\frac{r^2 - sz}{r(z-s)}\right| \geq \frac{r^2 + r'^2}{2rr'}$$

holds, then, considering $n_s \geq \frac{T}{2}$ for $0 \leq s \leq S$, we obtain the inequality

$$|\Psi|_{r'} \leq |\Psi|_r \cdot \left(\frac{2rr'}{r^2 + r'^2}\right)^{ST/2}.$$

Now $|\Psi|_r \leq \|P_\Delta\|_{\|\boldsymbol{u}\|r}$, from which the claimed inequality follows. $\diamond$

We now consider the multiplication in G by a positive number $l \geq 1$ of the form $l = 2^M$ for some $M \geq 0$. This is given by $g \mapsto l \cdot g$ for $g \in G$. Now choose $\boldsymbol{v} \in \mathrm{T}(A)$ with $l \cdot \boldsymbol{v} = \boldsymbol{u}$ and set $\gamma_0' = \exp_G(\boldsymbol{v})$. Then $l \cdot \gamma_0' = \gamma_0$ and thus $\gamma_0' \in G(\overline{K})$. Finfally, let Γ' be the subgroup of G generated by γ_0'. As the degree of the multiplication-by-l map is at most l^{2n}, there is an algebraic number field $L \supseteq K$ with $[L : K] \leq l^{2n}$ and $\Gamma' \subseteq G(L)$.

Lemma 5.2 *Let $\Delta \in D(\frac{T}{2})$ and s an integer with $0 \leq s \leq l \cdot S$, and let*

$$\delta = P_\Delta(\boldsymbol{X})(s\gamma_0).$$

Then either $\delta = 0$, or

$$\log|\delta| \geq -c_8 l^{2n}\big((D+T)\log(D+T) + D(S^2 + l^{c_9})\big).$$

PROOF: Because of $\Gamma' \subseteq G(L)$, $\delta \in L$. This is an algebraic number field of degree at most $m l^{2n}$. We now compute the height of $s\gamma_0'$. To this end, write $s = s'l + s''$ with $0 \leq s'' < l$ and $0 \leq s' \leq S$. Then $s\gamma_0' = s'\gamma_0 + s''\gamma_0$. By the addition law,

$$h(s\gamma_0') \leq c_{10}(h(s'\gamma_0) + h(s''\gamma_0')).$$

We estimate an upper bound for the height $h(s''\gamma_0')$ using Proposition 2.0,

$$c_1 l^{c_2}(h(s''\gamma_0) + 1)$$

and obtain via [Se] the estimate

$$h(s\gamma_0') \leq c_{11}(s^2 + l^{c_2+2}).$$

With this, we find as in Lemma 4.1 the height δ for the estimate

$$h(\delta) \leq c_{12}(D+T)\log(D+T) + c_{13}D(S^2 + l^{c_{14}}).$$

If now $\delta \neq 0$, then we have

$$\log|\delta| \geq -h(\delta),$$

which is easily verified from the product formula using known properties of the height. From this, the desired inequality immediately follows. $\diamond$

6 The extrapolation

We now choose a constant $\kappa \geq 5$ and a sufficiently large integer parameter $M \geq 0$. Then set $S = l^{(2n+1)c_9}$ and $S' = |\Gamma(S)|$. With this, set

$$D = 2mnS' \cdot S^{(n-1)\kappa},$$
$$T = 2mnS' \cdot S^{n\kappa} - n.$$

Clearly, (2) is satisfied, and the following lemma holds.

Lemma 6.1 *For $\gamma' \in \Gamma'(lS)$,*

$$\mathrm{ord}_{\gamma',B}(P) \geq \left\lfloor \frac{T}{2} \right\rfloor.$$

PROOF: By using Proposition 2 in [Wü2], it is enough to show that for $\Delta \in D(\frac{T}{2})$, we have

$$P_\Delta(\boldsymbol{X}(\gamma')) = 0.$$

We have called the number on the left δ. Now we write $\gamma' = s\gamma'_0$ for some $0 \leq s \leq S$ and set $\boldsymbol{v}' = s\boldsymbol{v}$, and $\delta' = P_\Delta(\exp_G(\boldsymbol{v}'))$. This number was estimates in Lemma 5.1 (ii). We set $r = S^2$, $r' = S + 1$ and using (i) we obtain

$$\log|\delta'| \leq c_{15}S'S^{n\kappa}\log S - \frac{1}{2}TS\log\frac{S}{4}.$$

On the other hand, because of Lemma 5.2 and if $\delta \neq 0$, we have the estimate

$$\log|\delta| \geq -c_{16}S'S^{n\kappa}l^{2n}\log S.$$

If we set $\zeta_i = f_i(\boldsymbol{v}')$ and $\xi'_i = X_i(\gamma')$ for $0 \leq i, j \leq N$, then the ζ_i and the ξ'_i determine the same point in $\mathbb{P}^N$. Thus, for all i, j with $0 \leq i, j \leq N$,

$$\xi'_i\zeta_j = \xi'_j\zeta_i,$$

from which

$$\xi_i'^{bD}\delta' = \zeta_i^{bD}\delta$$

follows. Together with the estimates for δ, δ' and the height of $\boldsymbol{X}(\gamma')$, we obtain the estimate

$$bD\log\max_i(|\zeta_i|) \leq -\varepsilon''TS\log S,$$

and then

$$\log\max_i(|\zeta_i|) \leq -\varepsilon' S^5\log S$$

for positive ε, ε'. If we take into account that $\|\boldsymbol{v}'|$
$leqc_{17}S$, it follows at last that

$$\log \max_i(|f_i(\boldsymbol{v}')|) \leq -\varepsilon\|\boldsymbol{v}'\|^5.$$

The following lemma then yields the desired contradiction. $\diamond$

We set $\delta(\boldsymbol{z}) = \log \max_i(|f_i(\boldsymbol{z})|)$ and let p denote map from $\mathfrak{Lie}(G)$ to $\mathfrak{Lie}(A)$ induced by the projection from G to A.

Lemma 6.2

(i) *If G is unipotent, then*

$$\delta(\boldsymbol{z}) \geq \log(c_{18}\|\boldsymbol{z}\|).$$

(ii) *If G is not unipotent, but linear, then*

$$\delta(\boldsymbol{z}) \geq -c_{19}\|\boldsymbol{z}\|.$$

(iii) *If G is not linear, then*

$$\delta(\boldsymbol{z}) \geq -c_{20}(\|\boldsymbol{z}\|^2 + 1).$$

PROOF: The statements (i) and (ii) are trivial due to the particular nature of the exponential map in these cases. In case (iii), there is a subset of the f_i ($i = 0, \ldots, N$) of the form $\{p^*g_0, \ldots, p^*g_M\}$ such that the g_i yield an embedding ι of A into $\mathbb{P}^M$. The line bundle $\iota^*\mathcal{O}(1)$ is the assigned a positive definite Hermitian form. We set $\delta'(p(\boldsymbol{z})) = \log \max_i(|g_i(p(\boldsymbol{z}))|)$. Then the function $\mathrm{e}^{\delta'-\pi H}$ is periodic and bounded from below by some $c_{21} > 0$. Hence $\mathrm{e}^{\delta'} \geq c_{21}\mathrm{e}^{\pi H}$. From the estimate $H(p(\boldsymbol{z}), p(\boldsymbol{z})) \geq c_{22}\|p(\boldsymbol{z})\|^2$ it follows that

$$\delta(\boldsymbol{z}) \geq \delta'(p(\boldsymbol{z})) \leq \log c_{21} + c_{22}\|p(\boldsymbol{z})\|^2.$$

Since $\|p(\boldsymbol{z})\|^2 \geq -\|\boldsymbol{z}\|^2$, we obtain the desired inequality. $\diamond$

7 The zero estimate

The element γ_0' generates the subgroup Γ'. In Section 4 we constructed a homogeneous polynomial $P(X_0, \ldots, X_N)$ that is not identically zero on G and has degree D. We showed in Section 6 that this polynomial vanishes in $\Gamma'(lS)$ along the analytic subgroup A with order at least

$$T' = \left\lfloor \frac{T}{2} \right\rfloor.$$

We can always arrange that

$$\Gamma'(lS) = l\Gamma(S)$$

holds. In fact, if γ_0 is of infinite order, this is immediately clear. Otherwise, if t is the order of γ_0, we may assume without loss of generality that the t-torsion elements of G are K-rational. This can be achieved by a finite field extension. Moreover, we want to assume without loss of generality that $\gamma_0 \notin 2G_t(K)$, where $G_t(K)$ denotes the group of t-torsion elements. If t' is the order of γ_0', then $t'|2^M t$, and we write $t' = 2^r t''$ with $\gcd(2, t'') = 1$. We consider $\gamma_0'' = 2^r\gamma_0'$. Then $t''\gamma_0'' = 0$, so $\gamma_0'' \in G_t(K)$. It follows from this that $r \geq M$, since otherwise $\gamma_0 \in 2G_t(K)$ would follow and from this $\gamma_0'' = 2^{r-M}\gamma_0$. Thus the order of γ_0'' is $2^{M-r}t = t''$. This implies $t' = 2^M t$.

We now show that there exists an algebraic subgroup H with $H \subseteq A$ which is defined over $\overline{\mathbb{Q}}$ and has positive dimension. To prove this, it is sufficient to show that the index $\sigma = \sigma(A; G)_{\overline{\mathbb{Q}}}$, defined in [Wü1], satisfies the inequality

$$\sigma < \frac{n-1}{n}. \tag{4}$$

Moreover, it is proved in [Wü1] that $\sigma(A; G)_{\overline{\mathbb{Q}}} = \tau(A; G)_{\overline{\mathbb{Q}}}$. So the inequality (4) holds if

$$\tau < \frac{n-1}{n} \tag{5}$$

holds. But this follows from the Main Theorem in [Wü1]. In fact, after choosing S, T, l, D it holds with the constants from there that

$$\left(\frac{T'}{n}\right)^r \geq (cD)^r \quad (1 \leq r \leq n),$$

if S is sufficiently large, and moreover,

$$\left(\frac{T'}{n}\right)^{n-1} \left|\Gamma'\left(l\frac{S}{n}\right)\right| \geq \left(\frac{T'}{n}\right)^{n-1} l \cdot \frac{S'}{n} \geq (cD)^n,$$

again by the choice of parameters.

Since the polynomial P is not identically zero on G, it follows from this that at least one τ_r for $1 \leq r < n$ satisfies the inequality

$$\tau_r < \tau.$$

This means that there exists an algebraic subgroup $H \subset G$ of codimension r which is $\overline{\mathbb{Q}}$-defined and contained in A. As $r < n$, it follows that

$$\dim H = n - r > 0.$$

This concludes the proof of the Main Theorem.

References

[Ba1] A. Baker, *Linear forms in the logarithms of algebraic numbers I*, Mathematika 13 (1966), 204-216

[Ba2] A. Baker, *Linear forms in the logarithms of algebraic numbers II*, Mathematika 14 (1967), 102-107

[F-W] G. Faltings, G. Wüstholz, *Einbettungen kommutativer algebraischer Gruppen und einige ihrer Eigenschaften*, Journal für reine und angewandte Mathematik 354 (1984), 175-205

[L1] S. Lang, *Transcendental points on group varieties*, Topology 1 (1962), 313-318

[L2] S. Lang, *Algebraic values of meromorphic maps I*, Topology 3 (1965), 183-191

[L3] S. Lang, *Algebraic values of meromorphic maps II*, Topology 5 (1966), 363-370

[Ma-Wü1] D.W. Masser, G. Wüstholz, *Zero estimates on group varieties*, Inventiones Mathematicae 64 (1981), 489-516

[Ma-Wü2] D.W. Masser, G. Wüstholz, *Fields of large transcendence degree generated by values of elliptic functions*, Inventiones Mathematicae 72 (1983), 407-464

[Ma-Wü3] D.W. Masser, G. Wüstholz, *Zero estimates on group varieties II*, Inventiones Mathematicae 80 (1985), 233-267

[Sch1] Th. Schneider, *Zur Theorie der Abelschen Funktionen und Integrale*, Journal für reine und angewandte Mathematik 183 (1941), 110-128

[Sch2] Th. Schneider, *Ein Satz über ganzwertige Funktionen als Prinzip für Transzendenzbeweise*, Mathematische Annalen 121 (1949), 133-140

[Se] J-P. Serre, *Quelques propriétés des groupes algébriques commutatifs*, Astérisque 69-70 (1979), 191-202

[Wü1] G. Wüstholz, *Multiplicity estimates on group varieties*, Annals of Mathematics 129 (1989), 471-500

[Wü2] G. Wüstholz, *Über das abelsche Analogon des Lindemannschen Satzes I*, Inventiones Mathematicae 72 (1983), 363-388

Original: *Algebraische Punkte auf analytischen Untergruppen algebraischer Gruppen*, Annals of Mathematics 129, 1989, 501-517

Translation by Wolfgang Globke, Version of June 6, 2016.