ACTA ARITHMETICA
169.2 (2015)

Commutative algebraic groups and p-adic linear forms

by

CLEMENS FUCHS (Salzburg) and DUC HIEP PHAM (Hanoi)

1. Introduction. The theory of Diophantine approximation is one of the most interesting areas in number theory in which the theory of linear forms plays a central role. In 1966 Baker made a breakthrough by proving a very deep result on effective lower bounds for linear forms in logarithms of algebraic numbers (see the series of papers [1]). This result was refined by Baker and Wüstholz [2]. After Wüstholz proved a brilliant theorem, called the analytic subgroup theorem (see [3] or [23]), the problem of linear forms could be considered in higher dimensions. In the literature one can find generalizations in terms of algebraic groups, and the most general results so far are due to Hirata-Kohno [13] and Gaudron [12].

It is natural to consider p-adic analogues of such problems. The theory of p-adic linear forms plays indeed an important and fundamental role in number theory. It has been applied to many questions, in particular to solve completely a large number of Diophantine problems of different shape. One of the points of interest comes from the problem of finding lower bounds for linear forms in p-adic logarithm functions evaluated at algebraic points. Unlike in the complex case, the p-adic logarithm function is only defined locally. It is therefore more natural to study upper bounds for the p-adic valuation of expressions $\alpha_1^{b_1}\cdots\alpha_n^{b_n}-1$, where $\alpha_1,\ldots,\alpha_n$ are algebraic numbers that are multiplicatively independent and $b_1,\ldots,b_n$ are rational integers, not all zero. Such problems have been investigated by many authors (see e.g. [8]) and the most outstanding results to date are due to Yu [26–29]. In 1998 he formulated and proved a p-adic analogue of the Baker and Wüstholz theorem and afterwards in a series of papers he improved the bounds. The results of Yu were used by Stewart and himself [20] to deal with the abc-conjecture. In particular, Stewart and Yu in 2001 showed that there is an effectively computable positive number c such that for all coprime positive integers

2010 *Mathematics Subject Classification*: Primary 11G99; Secondary 14L10, 11J86.
Key words and phrases: commutative algebraic groups, linear forms, effective results, heights.

DOI: 10.4064/aa169-2-2

x, y and $z > 2$ with $x + y = z$ one has

$$z < \exp\big(cN^{1/3}(\log N)^3\big),$$

where N is the product of all the distinct prime divisors of xyz. Furthermore, with the recent refinements of Yu [29] it is possible to solve completely the generalization of a problem of Erdős to Lucas and Lehmer numbers; the original conjecture of Erdős from 1965 states that $P(2^n - 1)/n \to \infty$ as $n \to \infty$, where $P(m)$ denotes the greatest prime divisor of m for integers $m > 1$.

The generalizations to linear forms in p-adic elliptic logarithms were solved by Rémond and Urfels [18], and refined by Hirata-Kohno and Takada [14]. For higher dimensions in the p-adic setting, the best results to date are due to Bertrand and Flicker. They stated some results concerning simple abelian varieties or abelian varieties of CM-type (see [4] and [10]). Flicker [11] also obtained a lower bound for linear forms on general abelian varieties, but the bound is ineffective.

The goal of this paper is to generalize the result on p-adic linear forms when evaluating at an algebraic point of a commutative algebraic group of positive dimension satisfying a technical condition and the condition of semistability. To describe the main theorem, let K be a number field and G a commutative algebraic group such that G and the additive group $\mathbb{G}_{\mathrm{a}}$ are disjoint over K (see Section 3.2 for the definition of this notion). There are many commutative algebraic groups satisfying this property, for example the direct product of any finite copies of the multiplicative group $\mathbb{G}_{\mathrm{m}}$ or any abelian variety. More generally, we prove that every semiabelian variety also has the property.

Let p be a prime number and consider embeddings $K \hookrightarrow \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$. Denote by v the p-adic valuation which is the restriction of the p-adic valuation on $\mathbb{C}_p$ to K and K_v the completion of K with respect to v. We embed G into the projective space $\mathbb{P}^N_K$ for some positive integer N, and let $\mathrm{Lie}(G)$ denote the Lie algebra of G. Fixing a choice of basis for the vector space $\mathrm{Lie}(G)$ one can identify $\mathrm{Lie}(G)$ with the vector space K^n; here n is the dimension of G. We get the normalized analytic representation of the exponential map of $G(K_v)$ (with respect to the basis) consisting of N functions analytic on a certain neighbourhood of 0 in K_v^n. Let W be the hyperplane in K^n defined over K by the linear form

$$l(Z_1, \ldots, Z_n) = \beta_1 Z_1 + \cdots + \beta_n Z_n,$$

where $\beta_1, \ldots, \beta_n$ are elements, not all zero, in K. Let u be an element in the above neighbourhood such that its image in the p-adic Lie group $G(K_v)$ is an algebraic point γ in $G(K)$. The problem we consider is to give a lower bound for $|l(u)|_p$ when $l(u)$ is non-zero; here as usual we denote by $|\cdot|_p$

the p-adic absolute value on $\mathbb{C}_p$. The purpose of this paper is to solve the problem in the case when (G, W) is semistable over $\overline{\mathbb{Q}}$. Here we use the condition of semistability introduced in [3] over the algebraic closure $\overline{\mathbb{Q}}$, since it concerns field extensions of the ground field K. Our lower bound consists of two parts; the first one consists of effectively computable constants depending only on the group G, the field K and the choice of basis for the Lie algebra of G, and the second one is the product of the absolute logarithmic (Weil) height of the linear form l, of the algebraic point γ and of the prime number p.

The method used in this paper to solve the problem can certainly be applied to get new results in transcendence theory. We leave this as a topic for a forthcoming paper.

In Section 2 we shall state the new result in detail. In Section 3 we collect some preliminary results including a Schwarz lemma in the p-adic domain, simple facts on disjointness and semistability, on heights, on the analytic representation of the exponential map and a fact about the order of vanishing of analytic functions. In Section 4 we shall give the proof of the main result of Section 2. The proof starts by embedding G into some projective space; this involves a choice which we fix for the rest of the paper. We also choose a basis for the hyperplane. Then we work out the standard program in transcendence theory: we construct an auxiliary function with bounded height and with high order vanishing at certain points. Using the Schwarz lemma we can extrapolate and derive an upper bound. Liouville's inequality from Diophantine approximation gives a lower bound provided that we have non-vanishing. Algebraic considerations (namely multiplicity estimates) give the non-vanishing. Finally, comparing upper and lower bound gives the desired result by an appropriate choice of the parameters.

2. New result. As was mentioned above, the p-adic theory of logarithmic forms has already been developed systematically with nice applications in number theory. It is therefore natural and clearly motivated to generalize the problem to the case of higher dimensions. There are several results in this direction due to Rémond, Urfels, Hirata-Kohno, Takada, Flicker, Bertrand and others. However, the results only deal with elliptic curves or abelian varieties. We shall give here a new generalization to a class of commutative algebraic groups.

Let K be a number field over $\mathbb{Q}$ and let $\mathcal{O}_K$ be the ring of algebraic integers of K. We choose an embedding $K \hookrightarrow \overline{\mathbb{Q}}$. Let p be a prime number in $\mathbb{Z}$. We denote by $\mathbb{Q}_p$ the field of p-adic numbers and by $\mathbb{C}_p$ the completion of the algebraic closure of $\mathbb{Q}_p$. We get the embedding $\sigma : K \hookrightarrow \mathbb{C}_p$ defined by the composition of the embeddings $K \hookrightarrow \overline{\mathbb{Q}}$ and $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$. We therefore identify each element $x \in K$ with $\sigma(x) \in \mathbb{C}_p$. Let v be the valuation on K

given by

$$v(x) := -\frac{\log |x|_p}{\log p}, \quad \forall x \in K.$$

Denote by K_v the completion of K with respect to v. By completing the algebraic closure we get $K \hookrightarrow K_v \hookrightarrow \mathbb{C}_p$, which preserves the absolute values. Let G be a commutative algebraic group defined over K of dimension $n \geq 1$. According to [19] (see also [9] where explicit embeddings are constructed using exponential and Theta-functions), G can be embedded into some projective space $\mathbb{P}^N$. Let $L : \{1, \dots, n\} \to \mathrm{Lie}(G)$ be a basis, $f_L = (f_1, \dots, f_N)$ the normalized analytic function of the exponential map of $G(K_v)$ with respect to L, and Exp the map as defined in Section 3.5. We know that $f_1, \dots, f_N$ are analytic on an open disk Λ_v of K_v^n (see again Section 3.5). Let W be the hyperplane in K^n defined over $\mathcal{O}_K$ by the linear form

$$l(Z_1, \dots, Z_n) = \beta_1 Z_1 + \cdots + \beta_n Z_n,$$

where $\beta_1, \dots, \beta_n$ are elements, not all zero, in $\mathcal{O}_K$. Let u be an element in Λ_v such that $\gamma := \mathrm{Exp}(u)$ is an algebraic point in $G(K)$. Let B and H be fixed numbers such that

$$B \geq \max_{i=1,\dots,n} \{3, H(\beta_i)\}, \quad H \geq \max\{3, H(\gamma)\}.$$

Set $b = \log B$ and $h = \log H$. If $u = (u_1, \dots, u_n)$ is not contained in $W_v := W \otimes_K K_v$, i.e. $l(u) = \beta_1 u_1 + \cdots + \beta_n u_n \neq 0$, then a natural question is, "What can we say about lower bounds for $|l(u)|_p$?". We give an answer to this question in the case when $G, \mathbb{G}_\mathrm{a}$ are disjoint over K (for example, G is semiabelian, see Lemma 3.5) and (G, W) is semistable over $\overline{\mathbb{Q}}$. Let δ_L be the denominator of L which is defined in Section 3.5, and let $B^n(r_p|\delta_L|_p) = \{x = (x_1, \dots, x_n) \in \mathbb{C}_p^n; |x_i|_p < r_p|\delta_L|_p \text{ for } i = 1, \dots, n\}$, where $r_p := p^{-1/(p-1)}$. Then we have the following:

Theorem 2.1. *Let K be a number field and G a commutative algebraic group of dimension $n \geq 1$ defined over K such that G and $\mathbb{G}_\mathrm{a}$ are disjoint over K and (G, W) is semistable over $\overline{\mathbb{Q}}$. There is a positive number ω_L depending on L and there exist effectively computable positive real constants c_0 and c_1 independent of b, h and p with the following property:*

- *If $u \in \Lambda_v \cap B^n(r_p|\delta_L|_p)$ is such that* Exp(u) *is an algebraic point in $G(K)$ then $l(u) = 0$ or*

$$\log |l(u)|_p > -c_0 {\omega_L}^{n+3} b h^n (\log b + \log h)^{n+3} \log p.$$

- *If $u \in \Lambda_v$ is such that* Exp(u) *is an algebraic point in $G(K)$ then we set*

$$n(u) := \max\left\{0, \left[\frac{1}{p-1} - v(u)\right] + 1\right\},$$

and either $l(u) = 0$, *or we get the lower bound*

$$\log |l(u)|_p > -c_1 {\omega_L}^{n+3} b h^n (\log b + \log h + 2n(u) \log p)^{n+3} \log p.$$

Throughout the paper, constants do not depend on b, h or p. We write $A \ll B$ (resp. $A \gg B$) if there is an effectively computable positive constant c such that $A \leq cB$ (resp. $A \geq cB$).

We remark that although in the above theorem we only consider the case $\beta_1, \ldots, \beta_n \in \mathcal{O}_K$, the theorem is still true for $\beta_1, \ldots, \beta_n \in K$. To see this, let δ_i be the denominator of β_i for $i = 1, \ldots, n$, and δ the least common multiple of $\delta_1, \ldots, \delta_n$. Set $\beta'_i := \delta\beta_i$ for $i = 1, \ldots, n$ and $l' = \delta l$. Then $\beta'_1, \ldots, \beta'_n \in \mathcal{O}_K$ and $|l(u)|_p = |\delta^{-1}|_p |l'(u)|_p \geq |l'(u)|_p$. Using Lemma 3.8 we get $\log \delta \leq \log(\delta_1 \cdots \delta_n) = \log \delta_1 + \cdots + \log \delta_n \ll b$, and this gives $h(\beta'_i) = h(\delta\beta_i) \ll b$ for all $i = 1, \ldots, n$. Hence the statement follows by applying Theorem 2.1 to the linear form l' and using the inequality $\log |l(u)|_p \geq \log |l'(u)|_p$.

We also remark that it would be nice to remove the technical assumptions concerning disjointness and semistability in the statement. This clearly needs some further efforts. Since the paper is already quite long, we leave this for future work.

3. Background and preliminaries. In this section we discuss some basic background material which we need for the proof of the main theorem.

3.1. Some p-adic analysis. The main result of this section is a Schwarz lemma in the p-adic domain (Proposition 3.3). For any subfield F of $\mathbb{C}_p$ and for any $R \geq 0$, we set $B_F(R) := \{x \in F;\ |x|_p < R\}$ and $\overline{B}_F(R) := \{x \in F;\ |x|_p \leq R\}$. From now on, we will skip the subscript F when $F = \mathbb{C}_p$. Let $f(x) = \sum_n a_n x^n$ be an analytic function on $\overline{B}(r)$ with $r > 0$. We define

$$|f|_r := \sup_n |a_n|_p r^n = \max_n |a_n|_p r^n.$$

We start with the remark that the function $z - a$ satisfies $|z - a|_r = r$ for $r > 0$ and $a \in \overline{B}_F(r)$. Indeed, by definition we have $|z - a|_r = \max\{|a|_p, r\} = r$.

Lemma 3.1. *Let f be an analytic function on $\overline{B}_F(r)$ with $r > 0$, and s, t real numbers such that $0 < s \leq t \leq r$. If f has k zeros in the disk $\overline{B}_F(s)$ then*

$$|f|_s \leq \left(\frac{s}{t}\right)^k |f|_t.$$

Proof. The statement is trivially true if $f \equiv 0$. Otherwise, the Weierstrass preparation theorem (see [16, Theorem 2.14]) says that $f = P \cdot g$ with $P(z) = (z - a_1) \cdots (z - a_k)$ for $a_1, \ldots, a_k \in \overline{B}_F(s)$ and with a certain analytic function g on $\overline{B}_F(r)$. By the remark above we get

$$|P|_s = |z - a_1|_s \cdots |z - a_k|_s = s^k,$$

and similarly for $|P|_t$. Hence

$$|f|_s = s^k|g|_s \le s^k|g|_t = \left(\frac{s}{t}\right)^k t^k|g|_t = \left(\frac{s}{t}\right)^k |f|_t. \ \blacksquare$$

LEMMA 3.2. *Let f be an analytic function on $\overline{B}(r)$ with $r > 0$, and let $0 < s \le t \le r$. Let m be the number of zeros (counted with multiplicities) of f in $B(t)$. Then*

$$|f|_t \le \left(\frac{t}{s}\right)^m |f|_s.$$

Proof. The statement is trivial if $f \equiv 0$ or $s = t$. Otherwise, let $b_1, \dots, b_m$ be the zeros of f in $B(t)$ (counted with multiplicities) and fix t' with

$$\max\{|b_1|_p, \dots, |b_m|_p\} < t' < t.$$

Let l be the number of zeros (counted with multiplicities) of f in $\overline{B}(s)$. Without loss of generality, we may assume that $b_1, \dots, b_l$ are the l zeros of f in $\overline{B}(s)$. By the Weierstrass preparation theorem there are $\alpha_1, \alpha_2 \in \mathbb{C}_p$ and functions g_1, g_2 such that g_1 is analytic on $\overline{B}(s)$ and g_2 is analytic on $\overline{B}(t)$, $g_1(0) = g_2(0) = 1$, $|g_1|_s = |g_2|_r = 1$, and $f(z) = \alpha_1(z - b_1)\cdots(z - b_l)g_1 = \alpha_2(z - b_1)\cdots(z - b_m)g_2$. Combining this with the above remark we get

$$\begin{aligned} |f|_s &= |\alpha_1|_s|z - b_1|_s \cdots |z - b_l|_s|g_1|_s = |\alpha_1|_p s^l, \\ |f|_{t'} &= |\alpha_2|_{t'}|z - b_1|_{t'} \cdots |z - b_m|_{t'}|g_2|_{t'} = |\alpha_2|_p t'^m. \end{aligned}$$

Hence

$$|f|_t = \lim_{t' \to t} |f|_{t'} = |\alpha_2|_p t^m.$$

On the other hand, since $g_1(0) = g_2(0) = 1$ it follows that

$$f(0) = \alpha_1(-1)^l b_1 \cdots b_l = \alpha_2(-1)^m b_1 \cdots b_m$$

which leads to $|\alpha_1|_p = |\alpha_2|_p|b_{l+1} \cdots b_m|_p$. This shows that

$$\frac{|f|_t}{|f|_s} = \frac{|\alpha_2|_p}{|\alpha_1|_p}\,\frac{t^m}{s^l} = \frac{t^m}{s^m}\,\frac{s^{m-l}}{|b_{l+1} \cdots b_m|_p}.$$

Since $b_{l+1}, \dots, b_m \in B(t) \setminus \overline{B}(s)$ it follows that $|b_{l+1} \cdots b_m|_p \ge s^{m-l}$. Hence

$$\frac{|f|_t}{|f|_s} \le \frac{t^m}{s^m}. \ \blacksquare$$

We are now able to prove the following proposition, which is called the *Schwarz lemma.*

PROPOSITION 3.3. *Let $t \ge s$ be positive real numbers, f an analytic function on $\overline{B}_F(t)$, and Γ a finite subset of $\overline{B}_F(s)$ of cardinality $l \ge 2$. Define*

$$\delta := \inf\{|\gamma - \gamma'|_p;\ \gamma, \gamma' \in \Gamma,\ \gamma \ne \gamma'\}$$

and

$$\mu := \sup\{|f^{(n)}(\gamma)|_p;\ n = 0, \ldots, k-1,\ \gamma \in \Gamma\}$$

with a positive integer k and with $f^{(n)}$ the nth derivative of f. Assume that $\delta \le 1$. Then

$$|f|_s \le \max\left\{\left(\frac{s}{t}\right)^{kl} |f|_t, \mu\left(\frac{s}{\delta}\right)^{kl-1} r_p^{-(k-1)}\right\}.$$

Proof. The proposition is trivially true if $f \equiv 0$, so assume that f is non-zero. If f has at least kl zeros in the disc $\overline{B}(s)$ then Lemma 3.1 gives

$$|f|_s \le \left(\frac{s}{t}\right)^{kl} |f|_t.$$

Otherwise f has at most $kl-1$ zeros in $\overline{B}(s)$. By the definition of δ, the sets $B(\gamma, \delta)$, $\gamma \in \Gamma$, are disjoint. In fact, suppose that there exist distinct γ_1 and γ_2 in Γ such that there is $x \in B(\gamma_1, \delta) \cap B(\gamma_2, \delta)$. This leads to the following contradiction:

$$|\gamma_1 - \gamma_2|_p \le \max\{|x - \gamma_1|_p, |x - \gamma_2|_p\} < \delta.$$

Furthermore these l sets $B(\gamma, \delta)$, $\gamma \in \Gamma$, are subsets of $\overline{B}(s)$ since $\Gamma \subset \overline{B}_F(s)$, and this shows that there exists $\gamma_0 \in \Gamma$ such that f has at most $k-1$ zeros in $B(\gamma_0, \delta)$. Since $\gamma_0 \in \overline{B}_F(s)$, this gives $|f(z-\gamma_0)|_r = |f(z)|_r$ for any r such that $s \le r \le t$. We may therefore assume that $\gamma_0 = 0$. Let $n(\delta, f)$ be the number of zeros (counted with multiplicities) of f in $B(\delta)$. It is clear that $n(\delta, f) \le k-1$, and this shows that

$$|f|_\delta = \sup_{n \le k-1} \left|\frac{f^{(n)}(0)}{n!}\right|_p \delta^n.$$

On the other hand, it is known that

$$\left|\frac{1}{n!}\right|_p \le p^{\frac{n-1}{p-1}} = r_p^{-(n-1)} \le r_p^{-(k-1)}.$$

Combining this with $\delta \le 1$, we get

$$|f|_\delta \le \mu r_p^{-(k-1)}.$$

Finally, since f has at most $kl-1$ zeros in $\overline{B}(s)$, Lemma 3.2 gives

$$|f|_s \le \left(\frac{s}{\delta}\right)^{kl-1} |f|_\delta. \ \blacksquare$$

3.2. Semiabelian varieties. Let G be an algebraic group defined over a field K. It is well-known from Chevalley's theorem that there is a unique short exact sequence of algebraic groups

$$1 \to H \to G \to A \to 1$$

with H a linear algebraic group and A an abelian variety defined over K. We call G a *semiabelian variety* if H is a torus, i.e. $H_{\overline{K}} \cong (\mathbb{G}_{\mathrm{m}} \otimes \overline{K})^k$ for some $k \geq 0$; here $\mathbb{G}_{\mathrm{m}}$ denotes the multiplicative group. One can show that G is semiabelian defined over K if and only if $G_{\overline{K}}$ is semiabelian defined over $\overline{K}$. It is known that every semiabelian variety is commutative (see [25, Proposition 2.3]). We recall the following definition given by Masser and Wüstholz [15]: Let $G_1, \ldots, G_k$ be algebraic groups defined over K. We say that they are (mutually) *disjoint over* K if every connected algebraic K-subgroup H of $G := G_1 \times \cdots \times G_k$ has the form $H_1 \times \cdots \times H_k$ for algebraic K-subgroups $H_1, \ldots, H_k$ of $G_1, \ldots, G_k$ respectively.

Lemma 3.4. *For S semiabelian,* $\mathrm{Hom}(S, \mathbb{G}_{\mathrm{a}}) = (0)$.

Proof. Notice that $S(\overline{K})_{\mathrm{tor}}$ is Zariski dense in S, and any homomorphism $\alpha : S \to \mathbb{G}_{\mathrm{a}}$ maps $S(\overline{K})_{\mathrm{tor}}$ to $\mathbb{G}_{\mathrm{a}}(\overline{K})_{\mathrm{tor}} = (0)$. Hence $\alpha(S) = (0)$. ■

Lemma 3.5. *Every semiabelian variety defined over K and the additive group $\mathbb{G}_{\mathrm{a}}$ are disjoint over K.*

Proof. Let $\mathscr{H}$ be an arbitrary algebraic K-subgroup of $\mathscr{G} := \mathbb{G}_{\mathrm{a}} \times G$. By making a base change to $\overline{K}$ we may assume that $K = \overline{K}$. We denote by π_{a} and π the projections of $\mathscr{H}$ on $\mathbb{G}_{\mathrm{a}}$ and on G respectively. Set $H_{\mathrm{a}} := \pi_{\mathrm{a}}(\mathscr{H} \cap (\mathbb{G}_{\mathrm{a}} \times \{e\}))$ and $H := \pi(\mathscr{H} \cap (\{0\} \times G))$. Then H_{a} is an algebraic K-subgroup of $\mathbb{G}_{\mathrm{a}}$, and H is an algebraic K-subgroup of G. Let P be the image of $\mathscr{H}$ under the projection

$$\mathbb{G}_{\mathrm{a}} \times G \to (\mathbb{G}_{\mathrm{a}} \times G)/(H_{\mathrm{a}} \times H) \cong (\mathbb{G}_{\mathrm{a}}/H_{\mathrm{a}}) \times (G/H).$$

Define p_{a} and p to be the projections of $(\mathbb{G}_{\mathrm{a}}/H_{\mathrm{a}}) \times (G/H)$ onto $\mathbb{G}_{\mathrm{a}}/H_{\mathrm{a}}$ and G/H respectively. We show that $P \cong p_{\mathrm{a}}(P)$ and $P \cong p(P)$. For the first isomorphism, since p_{a} is surjective it is sufficient to show that the restriction of p_{a} to P is injective. In fact, let $(x, y) \in \mathscr{H}$ be such that $p_{\mathrm{a}}((x, y)(H_{\mathrm{a}} \times H)) = H_{\mathrm{a}}$, so $x \in H_{\mathrm{a}}$. But $H_{\mathrm{a}} = \pi_{\mathrm{a}}(\mathscr{H} \cap (\mathbb{G}_{\mathrm{a}} \times \{e\}))$, and hence $(x, e) \in \mathscr{H}$. Combining this with $(x, y) \in \mathscr{H}$ we see that $(0, y) \in \mathscr{H}$. Thus $y = \pi(0, y) \in \pi(\mathscr{H} \cap (\{0\} \times G)) = H$, and so $(x, y) \in H_{\mathrm{a}} \times H$. By the same argument, we also get the second isomorphism.

Since G is semiabelian, G/H is semiabelian as well. It follows that $P \cong p(P)$ is semiabelian. By Lemma 3.4 we get $\mathrm{Hom}(P, \mathbb{G}_{\mathrm{a}}) = (0)$. Furthermore, it is clear that H_{a} is either trivial or $\mathbb{G}_{\mathrm{a}}$, hence $p_{\mathrm{a}}(P) \subseteq \mathbb{G}_{\mathrm{a}}$. This says that $p_{\mathrm{a}} \in \mathrm{Hom}(P, \mathbb{G}_{\mathrm{a}}) = (0)$, which gives $P \cong p_{\mathrm{a}}(P) = (0)$ and implies that $\mathscr{H} = H_{\mathrm{a}} \times H$. ■

3.3. Semistability. We recall the following notion, due to Wüstholz [3, Chapter 6]. Let G be an algebraic group defined over a field K, and V a K-linear subspace of the Lie algebra $\mathrm{Lie}(G)$ of G. We associate with (G, V)

the index

$$\tau(G,V) := \begin{cases} \dfrac{\dim V}{\dim G} & \text{if } \dim G > 0, \\ 1 & \text{otherwise.} \end{cases}$$

The pair (G,V) is called *semistable* (*over* K) if for any proper quotient $\pi : G \to H$ defined over K, we have $\tau(G,V) \le \tau(H, \pi_*(V))$ where $\pi_* : \mathrm{Lie}(G) \to \mathrm{Lie}(H)$ is the K-linear map induced by π. Let F/K be a field extension. We say that (G,V) is *semistable over* F if $(G_F, V \otimes_K F)$ is semistable.

3.4. Heights. Let K be a number field of degree d over $\mathbb{Q}$, and M_K the set of places of K. For $v \in M_K$ we write K_v for the completion of K at v, and introduce the normalized absolute value $|\cdot|_v$ as follows. If $v \mid p$ we define $|p|_v := p^{-[K_v:\mathbb{Q}_p]}$. If $v \mid \infty$ then v corresponds to the embedding τ_v of K into $\mathbb{C}$, and we define $|x|_v := |\tau_v(x)|^{[K_v:\mathbb{R}]}$ for any $x \in K_v$. One can show that

$$\prod_{v \in M_K} |x|_v = 1, \quad \forall x \in K \setminus \{0\},$$

and this is called the *product formula.* Let $P \in \mathbb{P}^n(K)$ be a point represented by a homogeneous non-zero vector x with coordinates $x_0, \dots, x_n$. We set

$$h_K(x) := \sum_{v \in M_K} \max_i \log |x_i|_v.$$

The *absolute logarithmic* (*Weil*) *height* H on $\mathbb{P}^n(\overline{\mathbb{Q}})$ is defined by

$$h(P) := \frac{1}{[K:\mathbb{Q}]} h_K(x)$$

where K is any number field containing P, and the *absolute* (*Weil*) *height* of P is defined by $H(P) := e^{h(P)}$.

Let $\alpha \in \overline{\mathbb{Q}}$. We define $h(\alpha)$ as the absolute logarithmic height of the point in $\mathbb{P}^1(K)$ with projective coordinates $1, \alpha$. It is known that

$$h(\alpha_1 \cdots \alpha_r) \le h(\alpha_1) + \cdots + h(\alpha_r),$$
$$h(\alpha_1 + \cdots + \alpha_r) \le \log r + h(\alpha_1) + \cdots + h(\alpha_r)$$

with $r \ge 1$ and with $\alpha_1, \dots, \alpha_r \in \overline{\mathbb{Q}}$. Let $x = (x_1, \dots, x_n) \in \mathbb{A}^n(K)$. We define

$$|x|_v := \max_i |x_i|_v, \quad \forall v \in M_K,$$

and

$$h_{\max}(x) := \sum_{v \in M_K} \log |x|_v$$

for $x \ne 0$, otherwise we set $h_{\max}(0) := 0$. It is convenient to introduce the function

$$h_{L^2}(x) := \sum_{v \in M_K} \log |x|_{L^2,v}$$

where

$$|x|_{L^2,v} = \begin{cases} \max_i |x_i|_v, & v \text{ non-archimedean,} \\ (\sum_i \tau_v(x_i)^2)^{1/2}, & v \text{ real,} \\ \sum_i \tau_v(x_i)\overline{\tau_v(x_i)}, & v \text{ complex.} \end{cases}$$

We write $\log^+ t$ for $\max\{0, \log t\}$ for any positive real number t, extended by $\log^+ 0 = 0$. Set

$$H^+_{\max} := \prod_{v \in M_K} \max\{|x|_v, 1\},$$

$$h^+_{\max}(x) := \log H^+_{\max}(x) = \sum_{v \in M_K} \log^+ |x|_v, \qquad h^+_{L^2}(x) = \sum_{v \in M_K} \log^+ |x|_{L^2,v}.$$

These heights are related by

$$h_{\max} \le h_{L^2} \le h_{\max} + \frac{d}{2}\log(n+1), \qquad h^+_{\max} \le h^+_{L^2} \le h^+_{\max} + \frac{d}{2}\log(n+1).$$

If we identify each point $x = (x_1, \ldots, x_n) \in \mathbb{A}^n(K)$ with the projective point $(1 : x_1 : \ldots : x_n)$ then by definition one gets $h_K(x) = h^+_{\max}(x)$.

One can extend the notation above to polynomials in n variables $T_1, \ldots, T_n$ with coefficients in K. In more detail, let $P = \sum_i a_i T^i$ be such a polynomial with $i : \{1, \ldots, n\} \to \mathbb{N}^n$ a multi-index and $T^i = T_1^{i(1)} \cdots T_n^{i(n)}$. It corresponds to a point $a = (\ldots, a_i, \ldots)$ in an affine space $\mathbb{A}^N(K)$, and we define

$$|P|_v := |a|_v, \qquad |P|_{L^2,v} := |a|_{L^2,v},$$

and the heights of P as 0 for $P = 0$ and for $P \neq 0$ as

$$h_{\max}(P) = \sum_{v \in M_K} \log |P|_v, \qquad h_{L^2}(P) = \sum_{v \in M_K} \log |P|_{L^2,v}.$$

We shall also use

$$h^+_{\max}(P) = \sum_{v \in M_K} \log^+ |P|_v, \quad h^+_{L^2}(P) = \sum_{v \in M_K} \log^+ |P|_{L^2,v}.$$

Proposition 3.6 (Siegel's lemma, [6, Corollary 11]). *Let $N > M > 0$ be integers and let $l_1, \ldots, l_M$ be linear forms in N variables $T_1, \ldots, T_N$ with coefficients in K. Then there exists a non-trivial solution $x = (x_1, \ldots, x_N) \in \mathcal{O}_K^N$ of the system of linear equations $l_1(T_1, \ldots, T_N) = \cdots = l_M(T_1, \ldots, T_N) = 0$ such that*

$$h^+_{\max}(x) \le \frac{1}{2}\log|\mathrm{disc}(K)| + \frac{M}{N-M}\max_i h_{L^2}(l_i)$$

where $\mathrm{disc}(K)$ *denotes the field discriminant of* K.

We recall Liouville's inequality for number fields which is simple but has an important role in the proof of the main theorem below.

Proposition 3.7 (Liouville's inequality, [5, Corollary 2.9.2]). *Let K be a number field and let α be a non-zero element in K. Then*

$$\log|\alpha|_v \geq -\frac{h(\alpha)}{[K:\mathbb{Q}]}, \quad \forall v \in M_K.$$

For an algebraic number $\alpha \in K$, the *denominator* δ of α is defined as the smallest positive integer for which the element $\delta\alpha$ is in $\mathcal{O}_K$. For a polynomial P with coefficients a_i, $i \in I$, in K, we define the *denominator* $\delta(P)$ of P as the smallest positive integer for which $\delta(P)a_i \in \mathcal{O}_K$ for all $i \in I$. The following lemma gives an inequality between the height and the denominator of an algebraic number.

Lemma 3.8. *Let $\alpha \in K$ and δ be its denominator. Then*

$$\log\delta \leq \frac{h(\alpha)}{[K:\mathbb{Q}]}.$$

Proof. For $v \in M_K \setminus M_K^\infty$ let p be the residue characteristic of v. By definition

$$|\alpha|_v = |N_{K_v/\mathbb{Q}_p}(\alpha)|_p^{1/[K_v:\mathbb{Q}_p]} = |N_{K_v/\mathbb{Q}_p}(\alpha)|_p^{1/n_v}$$

with n_v the degree of K_v over $\mathbb{Q}_p$. Since $N_{K_v/\mathbb{Q}_p}(\alpha) \in \mathbb{Q}_p$ and the value group of $\mathbb{Q}_p$ is $\mathbb{Z}$, the element

$$m_v := \frac{n_v}{\log p}\max\{\log|\alpha|_v, 0\}$$

is a non-negative integer. Let $S := \{(p,v);\ p$ the residue characteristic of v, $v \in M_K \setminus M_K^\infty$, $|\alpha|_v > 1\}$. It is a finite set. We see that

$$\prod_{(p,v)\in S} p^{m_v}\alpha \in \mathcal{O}_K.$$

This shows, by definition of the denominator of α, that

$$\delta \leq \prod_{(p,v)\in S} p^{m_v},$$

and therefore

$$\log\delta \leq \frac{h(\alpha)}{[K:\mathbb{Q}]}. \ \blacksquare$$

3.5. Analytic representation of exponential maps. Let K be a number field and let G be an algebraic group defined over K. We denote by $\overline{G}$ the Zariski closure of G in $\mathbb{P}^N$. Let U be the open affine subset defined by $\overline{G} \cap \{X_0 \neq 0\}$. We know that the affine algebra $\Gamma(U, \mathcal{O}_{\overline{G}})$ is stable under the action of any element in $\mathfrak{g} = \mathrm{Lie}(G)$, and it is generated by $\xi_1, \ldots, \xi_N$, where

$$\xi_i := \left(\frac{X_i}{X_0}\right)\bigg|_U, \quad \forall i = 1, \ldots, N$$

(see [23]). We call a map $L : \{1,\dots,n\} \to \mathfrak{g}$ a *basis* if $L(1),\dots,L(n)$ is a basis for $\mathfrak{g}$. With such a basis L, one gets a system of polynomials $P_{i,L(j)}$ in N variables such that

$$L(j)\xi_i = P_{i,L(j)}(\xi_1,\dots,\xi_N), \quad \forall i = 1,\dots,N,\ \forall j = 1,\dots,n.$$

This means that

$$\mathcal{L}_j := L(j)(\mathcal{O}_K[\xi_1,\dots,\xi_N])$$

is an $\mathcal{O}_K$-module in $K[\xi_1,\dots,\xi_N]$ for any $j = 1,\dots,n$. Set $\mathcal{L} = \mathcal{L}_1 + \dots + \mathcal{L}_n$ and define

$$\mathcal{I}_L := (\mathcal{O}_K[\xi_1,\dots,\xi_N] : \mathcal{L}) = \{t \in \mathcal{O}_K;\, t\mathcal{L} \subset \mathcal{O}_K[\xi_1,\dots,\xi_N]\}.$$

Then $\mathcal{I}_L$ is an ideal of $\mathcal{O}_K$ and its norm $N_{K:\mathbb{Q}}(\mathcal{I}_L)$ is an ideal in $\mathbb{Z}$, which has to be principal, say (δ_L) for some positive integer δ_L. We call δ_L the *denominator* of L.

Denote by $\partial_1,\dots,\partial_n$ the canonical basis of $\mathrm{Lie}(K_v^n)$ defined as $\partial_i x_j = \delta_{ij}$ for all $i = 1,\dots,n$ and for all $j = 1,\dots,N$, where δ_{ij} is Kronecker's delta and x_i are the coordinate functions of K_v^n. We define the isomorphisms

$$\partial : K_v^n \to \mathrm{Lie}(K_v^n), \quad x = (x_1,\dots,x_n) \mapsto x_1\partial_1 + \dots + x_n\partial_n,$$

and

$$\iota : \mathrm{Lie}(K_v^n) \to \mathrm{Lie}(G(K_v)), \quad \iota(\partial_1) = L(1),\dots,\iota(\partial_n) = L(n).$$

We now consider the set $G(K_v)$ of K_v-points of G. It is known that $G(K_v)$ is a Lie group over K_v. By [7, Chapter III, §7], there is a map exp (the exponential map) defined and locally analytic on an open disk U_v of $\mathrm{Lie}(G(K_v))$. The functions

$$f_i := \xi_i \circ \mathrm{Exp}, \qquad i = 1,\dots,N,$$

are analytic on $\Lambda_v := (\iota \circ \partial)^{-1}(U_v)$ in K_v^n, where $\mathrm{Exp} = \exp \circ\, \iota \circ \partial$.

Let $\mathcal{O}_{G(K_v)}$, $\mathcal{O}_{U_v}$, $\mathcal{O}_{\partial(\Lambda_v)}$ and $\mathcal{O}_{\Lambda_v}$ be the sheaves of analytic functions on $G(K_v)$, U_v, $\partial(\Lambda_v)$ and Λ_v respectively. So we get commutative diagrams

$$\begin{tikzcd}
\mathcal{O}_{G(K_v)} \arrow[r, "\exp^*"] \arrow[d, "L(j)"] & \mathcal{O}_{U_v} \arrow[r, "\iota^*"] & \mathcal{O}_{\partial(\Lambda_v)} \arrow[r, "\partial^*"] & \mathcal{O}_{\Lambda_v} \arrow[d, "\partial_j"] \\
\mathcal{O}_{G(K_v)} \arrow[r, "\exp^*"] & \mathcal{O}_{U_v} \arrow[r, "\iota^*"] & \mathcal{O}_{\partial(\Lambda_v)} \arrow[r, "\partial^*"] & \mathcal{O}_{\Lambda_v}
\end{tikzcd}$$

for all $j = 1,\dots,n$. This leads to

$$(\partial_j \circ \mathrm{Exp}^*)(\xi_i) = (\mathrm{Exp}^* \circ L(j))(\xi_i), \qquad \forall i = 1,\dots,N,$$

i.e.

$$\partial_j(f_i) = L(j)(\xi_i) \circ \mathrm{Exp} = P_{i,L(j)}(\xi_1,\dots,\xi_N) \circ \mathrm{Exp} = P_{i,L(j)}(f_1,\dots,f_N)$$

for any $i = 1,\dots,N$ and $j = 1,\dots,n$.

The map $f_L = (f_1, \dots, f_N) : \Lambda_v \to K_v^N$ is called the *normalized analytic representation of the exponential map* exp with respect to the basis L. We define

$$d_L := \max_{i,j} \deg P_{i,L(j)}, \quad e_L := v(\delta_L), \quad h_L := \max_{i,j} h(P_{i,L(j)})$$

and

$$\omega_L := \max\{1, e_L\}(h_L + \log \delta_L + \log d_L);$$

here by convention, $\log d_L = 0$ if $d_L = 0$.

We fix the following notation. For $m = (m_1, \dots, m_k) \in \mathbb{N}^k$ with $0 \le k \le n$, we write

$$\partial^m := \partial_1^{m_1} \cdots \partial_k^{m_k}, \quad L^m := L(1)^{m_1} \cdots L(k)^{m_k}, \quad |m| := m_1 + \cdots + m_k.$$

LEMMA 3.9. *Let $L : \{1, \dots, n\} \to \mathfrak{g}$ be a basis and $P(T_1, \dots, T_N)$ a polynomial in N variables with coefficients in K of total degree $\le D$. Let T be a non-negative integer and $t = (t_1, \dots, t_n) \in \mathbb{N}^n$ be such that $T = t_1 + \cdots + t_n$. There exists a polynomial $P_t \in K[T_1, \dots, T_N]$ such that*

$$\partial^t P(f_1, \dots, f_N) = P_t(f_1, \dots, f_N),$$

satisfying

- $\deg P_t \le D + T(d_L - 1)$,
- $\log |P_t|_v \ll \log |P|_v + T(h_L + \log(D + Td_L))$ *for all* $v \in M_K$.

Proof. We use induction on $T = |t|$. The lemma is trivially true for $|t| = 0$. Assume that it is true for any $t \in \mathbb{N}^n$ with $|t| = T \ge 0$. Let now $t = (t_1, \dots, t_n) \in \mathbb{N}^n$ be such that $t_1 + \cdots + t_n = T + 1$. We may assume that $t_1 \ge 1$. Set $\tau = (t_1 - 1, \dots, t_n)$. By induction hypothesis,

$$\partial^\tau P(f_1, \dots, f_N) = P_\tau(f_1, \dots, f_N)$$

with

$$D_\tau := \deg P_\tau \le D + Td_L, \quad \log |P_\tau|_v \ll \log |P|_v + T(h_L + \log(D + Td_L)).$$

We write

$$P_\tau = \sum_{m_1 + \cdots + m_N \le D_\tau} a(m_1, \dots, m_N) T_1^{m_1} \cdots T_N^{m_N} = \sum_m a(m) T_1^{m_1} \cdots T_n^{m_n}$$

and

$$P_{i,L(1)} = \sum_{m_{i,1} + \cdots + m_{i,N} \le d_L} a(m_{i,1}, \dots, m_{i,N}) T_1^{m_{i,1}} \cdots T_N^{m_{i,N}}$$

with $a(m_{i,1}, \dots, m_{i,N}) \in K$ for all $1 \le i \le N$. This gives

$$\partial_1 f_i = \sum_{m_{i,1} + \cdots + m_{i,N} \le d_L} a(m_{i,1}, \dots, m_{i,N}) f_1^{m_{i,1}} \cdots f_N^{m_{i,N}}, \quad \forall i = 1, \dots, N.$$

Since $\partial^t = \partial_1 \partial_1^{t_1 - 1} \cdots \partial_n^{t_n} = \partial_1 \partial^\tau$ it follows that

$$\begin{aligned}\partial^t P(f_1, \ldots, f_N) &= \partial_1 \partial^\tau P(f_1, \ldots, f_N) = \partial_1 P_\tau(f_1, \ldots, f_N) \\ &= \sum_m a(m) \sum_{i=1}^N m_i \Big(\prod_{j \neq i} f_j^{m_j} \Big) f_i^{m_i - 1} \partial_1 f_i,\end{aligned}$$

which is expanded as

$$\sum_m \sum_{i=1}^N \sum_{m_{i,1} + \cdots + m_{i,N} \leq d_L} m_i a(m) a(m_{i,1}, \ldots, m_{i,N}) \Big(\prod_{j \neq i} f_j^{m_j + m_{i,j}} \Big) f_i^{m_i + m_{i,i} - 1}.$$

This shows that $\partial^t P(f_1, \ldots, f_N) = P_t(f_1, \ldots, f_N)$ for a certain polynomial

$$P_t(T_1, \ldots, T_N) = \sum_l q(l) T_1^{l_1} \cdots T_N^{l_N}$$

with $q(l) = \sum m_i a(m) a(m_{i,1}, \ldots m_{i,N})$; here the sum is taken over the set $\{(m_1, \ldots, m_N, i, m_{i,1}, \ldots, m_{i,N});\ m_j + m_{i,j} = l_j$ for $j \neq i$ and $m_i + m_{i,i} = l_i + 1$, $1 \leq i \leq N$, $m_{i,1} + \cdots + m_{i,N} \leq d_L$, $m_1 + \cdots + m_N \leq D_\tau\}$ such that

$$\begin{aligned}\deg P_t &\leq \max_i (m_1 + \cdots + m_N + m_{i,1} + \cdots + m_{i,N} - 1) \\ &\leq D_\tau + d_L - 1 \leq D + T(d_L - 1) + d_L - 1 \leq D + (T+1)(d_L - 1).\end{aligned}$$

Furthermore,

$$|q(l)|_v \leq \sum m_i |a(m)|_v |a(m_{i,1}, \ldots, m_{i,N})|_v \leq (d_L + 1)^N D_\tau |P_\tau|_v \max_{i,j} |P_{i,L(j)}|_v.$$

This shows that

$$\begin{aligned}\log |q(l)|_v &\leq N \log(d_L + 1) + \log D_\tau + \log |P_\tau|_v + h_L \\ &\ll \log |P|_v + T\big(h_L + \log(D + T \log d_L)\big) + N \log(d_L + 1) + h_L \\ &\ll \log |P|_v + (T+1)\big(h_L + \log(D + (T+1) d_L)\big)\end{aligned}$$

for all $v \in M_K$, and the lemma follows. ∎

Let k be a non-negative integer. We define $\mathcal{L}(k)$ as the sum of the images of $\mathcal{O}_K[\xi_1, \ldots, \xi_N]$ under all differentials of order $\leq k$, i.e.

$$\mathcal{L}(k) := \sum_{t \in \mathbb{Z}_{\geq 0}^n,\, |t| \leq k} L^t(\mathcal{O}_K[\xi_1, \ldots, \xi_N]).$$

Let $\mathcal{I}(k)$ be the ideal $(\mathcal{O}_K[\xi_1, \ldots, \xi_N] : \mathcal{L}(k))$ in $\mathcal{O}_K$.

Lemma 3.10.

$$\mathcal{I}(k) \supset (\mathcal{I}_L)^k, \quad \forall k \in \mathbb{N}.$$

Proof. We use induction on k. If $k = 0$, the lemma is trivially true. Assume it is true for $k = m \geq 0$. One has to show that

$$a_1 \cdots a_{m+1} L^t(\xi_i) \in \mathcal{O}_K[\xi_1, \ldots, \xi_N]$$

for $i = 1, \ldots, n$, for $a_1, \ldots, a_{m+1} \in \mathcal{I}_L$ and for $t = (t_1, \ldots, t_n) \in \mathbb{N}^n$ with $|t| = m + 1$. There is at least one $j \in \{1, \ldots, n\}$ such that $t_j \geq 1$. Set $\tau = (t_1, \ldots, t_{j-1}, t_j - 1, t_{j+1}, \ldots, t_n)$. We see that

$$a_1 \cdots a_{m+1} L^t(\xi_i) = a_1 \cdots a_m L^\tau(a_{m+1} L(j)(\xi_i)).$$

Since $a_{m+1} \in \mathcal{I}_L$ it follows that

$$a_{m+1} L(j)(\xi_i) = Q_{i,j}(\xi_1, \ldots, \xi_N), \quad \forall i = 1, \ldots, N,$$

for some polynomials $Q_{i,j}(T_1, \ldots, T_N)$ with coefficients in $\mathcal{O}_K$. By induction with $|\tau| = m$, we have $a_1 \cdots a_m \in \mathcal{I}_L^m \subset \mathcal{I}(m)$. In particular,

$$a_1 \cdots a_m L^\tau(Q_{i,j}(\xi_1, \ldots, \xi_N)) \in \mathcal{O}_K[\xi_1, \ldots, \xi_N]. \ \blacksquare$$

LEMMA 3.11. *For $t = (t_1, \ldots, t_n) \in \mathbb{N}^n$ with $|t| = T$ and for a polynomial $P(T_1, \ldots, T_N) \in \mathcal{O}_K[T_1, \ldots, T_N]$ we have*

$$\delta_L^T \partial^t P(f_1, \ldots, f_N) \in \mathcal{O}_K[f_1, \ldots, f_N].$$

Hence $\delta_L^T \partial^t f_i(0) \in \mathcal{O}_K$ for $i = 1, \ldots, N$.

Proof. There exists a polynomial $P_t(T_1, \ldots, T_N)$ with coefficients in K such that

$$L^t P(\xi_1, \ldots, \xi_N) = P_t(\xi_1, \ldots, \xi_N).$$

By Lemma 3.10, the polynomial $\delta_L^T P_t$ has coefficients in $\mathcal{O}_K$. Note that

$$\partial^t P(f_1, \ldots, f_N) = P_t(f_1, \ldots, f_N),$$

and so

$$\delta_L^T \partial^t P(f_1, \ldots, f_N) \in \mathcal{O}_K[f_1, \ldots, f_N].$$

Finally, since $f_i(0) = 0$ for $i = 1, \ldots, N$ it follows that

$$\delta_L^T \partial^t f_i(0) = P_t(f_1(0), \ldots, f_N(0)) \in \mathcal{O}_K, \quad \forall i = 1, \ldots, N. \ \blacksquare$$

PROPOSITION 3.12. *The functions f_i satisfy*

$$|f_i(x)|_p < 1, \quad \forall x \in B^n(|\delta_L|_p r_p).$$

Proof. This follows from the previous lemma and by considering the Taylor expansion of f_i at 0 together with the fact $|n!|_p \geq r_p^{n-1}$ for all positive integers n. $\blacksquare$

3.6. The order of vanishing of analytic functions. In this section let F denote a complete subfield of $\mathbb{C}_p$. Let V be a vector subspace of $\mathrm{Lie}(G(F))$, and f a non-zero p-adic analytic function on a neighborhood of $z \in F^n$. We say that f has a *zero at z of order $\geq T$ along V* if $(v_1 \cdots v_k f)(z) = 0$ for any $0 \leq k < T$ and for any $v_1, \ldots, v_k \in V$; and f has a *zero at z of exact order T along V* if it has order $\geq T$ at z along V and furthermore there are $w_1, \ldots, w_T$ in V such that $(w_1 \cdots w_T f)(z) \neq 0$.

Proposition 3.13. *With notation as above, let d be the dimension of V and let $\Delta_1, \dots, \Delta_d$ be a basis for V. Then f has a zero at z of order $\geq T$ along V if and only if $(\Delta_1^{t_1} \dots \Delta_d^{t_d} f)(z) = 0$ for $(t_1, \dots, t_d) \in \mathbb{N}^d$ with $t_1 + \dots + t_d < T$; and f has a zero at z of exact order T along V if it has order $\geq T$ at z along V and furthermore there is a d-tuple $\tau = (\tau_1, \dots, \tau_d) \in \mathbb{N}^d$ such that $|\tau| = T$ and $(\Delta_1^{\tau_1} \dots \Delta_d^{\tau_d} f)(z) \neq 0$.*

Proof. We prove the first statement. In fact, it suffices to show that if $(\Delta_1^{t_1} \cdots \Delta_d^{t_d} f)(z) = 0$ for any $(t_1, \dots, t_d) \in \mathbb{N}^d$ with $t_1 + \dots + t_d < T$, then f has a zero at z of order $\geq T$ along V. Let k be an integer with $0 \leq k < T$, and let $v_1, \dots, v_k \in V$. For $i = 1, \dots, k$ one can write $v_i = a_{i1}\Delta_1 + \dots + a_{id}\Delta_d$ with $a_{i1}, \dots, a_{id} \in F$. For $t = (t_1, \dots, t_d) \in \mathbb{N}^d$ with $|t| < T$, we expand

$$(v_1 \cdots v_k f)(z) = \Big(\prod_{i=1}^{k}(a_{i1}\Delta_1 + \dots + a_{id}\Delta_d) f\Big)(z) = \sum_{\alpha \in I} a_\alpha (\Delta_1^{\alpha_1} \cdots \Delta_d^{\alpha_d} f)(z).$$

Since $k < T$ it follows that $|\alpha| = \alpha_1 + \dots + \alpha_d < T$ for every $\alpha \in I$. Hence the sum vanishes, and this shows the first statement. It is clear that the second statement follows at once from the definition and the first statement. ∎

4. Proofs

4.1. Proof of the second statement of Theorem 2.1. We shall show that the first assertion of the theorem implies the second one. Let $u \in \Lambda_v$ be such that $\mathrm{Exp}(u)$ is an algebraic point in $G(K)$. We define

$$n(u) := \max\Big\{0, \Big[\frac{1}{p-1} - v(u)\Big] + 1\Big\} \quad \text{and} \quad u' := p^{n(u)}u.$$

Then $u' \in \Lambda_v$ and

$$|u'|_p = |p^{n(u)}|_p |u|_p = p^{-n(u)-v(u)} = p^{\frac{1}{p-1}-v(u)-n(u)} r_p < r_p.$$

Moreover, if $l(u) \neq 0$ then $l(u') = p^{n(u)} l(u) \neq 0$, and applying the first statement of Theorem 2.1 to u' in $\Lambda_v \cap B^n(r_p|\delta_L|_p)$ one gets

$$\log|l(u')|_p > -c_0 {\omega_L}^{n+3} b h'^n (\log b + \log h')^{n+3} \log p;$$

here $h' := \max\{1, h(\gamma')\}$ with $\gamma' := \mathrm{Exp}(u') = p^{n(u)}\mathrm{Exp}(u) = \gamma^{p^{n(u)}}$ where $\gamma := \mathrm{Exp}(u)$. By [19, Prop. 5] one has

$$h(\gamma^{p^{n(u)}}) \leq (p^{n(u)})^2 h(\gamma) \leq p^{2n(u)} h,$$

and this implies that $h' \leq p^{2n(u)} h$. Hence

$$n(u)\log p + \log|l(u)|_p > -c_0 {\omega_L}^{n+3} b h^n (\log b + \log h + 2n(u)\log p)^{n+3} \log p.$$

Therefore

$$\log|l(u)|_p > -c_1 {\omega_L}^{n+3} b h^n (\log b + \log h + 2n(u)\log p)^{n+3} \log p$$

for some positive constant c_1.

4.2. A projective embedding. Following [19] (cf. also [9] and [24]), there exist a positive integer N and an embedding $\varphi : G \hookrightarrow \mathbb{P}^N$ with G as in the statement of Theorem 2.1, which is defined over a number field K of degree m. Without loss of generality, we may assume that the identity element $e \in G(K)$ under φ has coordinates $(1 : 0 : \ldots : 0)$ in $\mathbb{P}^N$.

LEMMA 4.1. *There exists an embedding $\psi : G \to \mathbb{P}^N$ defined over a number field of degree $m(N+1)$ such that $\psi(e) = (1 : 0 : \ldots : 0)$ and $X_0(\psi(g)) \neq 0$ for all $g \in G(K)$, where X_0 denotes the first projective coordinate on $\mathbb{P}^N$.*

Proof. We choose a field extension K_1 of K of degree $N+1$, and a basis $\epsilon_0, \ldots, \epsilon_N$ of K_1 over K. The degree of the extension $K_1 \supseteq \mathbb{Q}$ is therefore $m(N+1)$. It is clear that the vectors

$$(\epsilon_0, 0, \ldots, 0), \quad (-\epsilon_1, \epsilon_0, 0, \ldots, 0), \ \ldots, \ (-\epsilon_N, 0, \ldots, 0, \epsilon_0)$$

form a basis of K_1^{N+1}, which gives rise to a unique element in $\mathrm{GL}_{N+1}(K_1)$ mapping this basis to the standard basis of K_1^{N+1}. This linear isomorphism is expressed explicitly by the matrix

$$A = \begin{pmatrix} \epsilon_0^{-1} & \epsilon_0^{-2}\epsilon_1 & \ldots & \epsilon_0^{-2}\epsilon_N \\ 0 & \epsilon_0^{-1} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \epsilon_0^{-1} \end{pmatrix}.$$

We let ψ be the composition of A with the embedding φ as above. Then $\psi(e)$ has projective coordinates $(1 : 0 : \ldots : 0)$, and $X_0(\psi(g)) \neq 0$ for all $g \in G(K)$. Indeed, let $(x_0 : x_1 : \ldots : x_N)$ be the projective coordinates of $\varphi(g)$. By the construction of ψ, we obtain

$$\begin{aligned} \psi(g) &= (\epsilon_0^{-1}x_0 + \epsilon_0^{-2}\epsilon_1 x_1 + \cdots + \epsilon_0^{-2}\epsilon_N x_N : \epsilon_0^{-1}x_1 : \ldots : \epsilon_0^{-1}x_N) \\ &= (\epsilon_0 x_0 + \epsilon_1 x_1 + \cdots + \epsilon_N x_N : \epsilon_0 x_1 : \ldots : \epsilon_0 x_N). \end{aligned}$$

Thus $\psi(e) = (1 : 0 : \ldots : 0)$. In addition, since $\epsilon_0, \ldots, \epsilon_N$ is a basis of K_1 over K and $x_0, \ldots, x_N$ are in K and not all zero, it follows that $X_0(\psi(g))$ is non-zero. Note that the embedding ψ is defined over K_1. ■

We shall fix the embedding $\psi : G \hookrightarrow \mathbb{P}^N$ for the rest of the paper, and identify each $g \in G$ with its image $\psi(g)$ in $\mathbb{P}^N$. By [23, Section 2], there is a finite field extension K_2 of K_1 (the degree of this extension is a positive constant) with the following property: There exist bihomogeneous polynomials $E_0, \ldots, E_N$ in $Z_0, \ldots, Z_N$ and $X_0, \ldots, X_N$ of bidegree (b, b) with coefficients in K_2 and with heights bounded above by a positive constant, and a Zariski open set $U \subset G \times G$ containing $\Gamma(\gamma) \times \Gamma(\gamma)$ such that for $(g, g') \in U$ the homogeneous coordinates of $g + g'$ are $(E_0(g, g') : \ldots :$

$E_N(g,g'))$; here $\Gamma(\gamma)$ denotes the subgroup generated by γ in $G(K)$ with $\gamma := \mathrm{Exp}(u)$. The degree of K_2 over K is also a positive constant. We may therefore assume, without loss of generality, that K is already equal to K_2 and has degree d over $\mathbb{Q}$. We call $(E_1,\dots,E_N)$ an *addition formula* for G, and from now on we fix such an addition formula $E=(E_1,\dots,E_N)$.

4.3. Basis of the hyperplane. We define the linear form in $n+1$ variables

$$\mathscr{L}(Z_0,Z_1,\dots,Z_n) := Z_0 - l(Z_1,\dots,Z_n).$$

This gives the vector space

$$\mathscr{W} := \{(z_0,z_1,\dots,z_n)\in K_v^{n+1};\ z_0 = l(z_1,\dots,z_n)\} \subset K_v^{n+1}.$$

Let $e_1,\dots,e_n$ be the basis for $\mathscr{W}$ defined by

$$e_1=(\beta_1,1,0,\dots,0),\quad e_2=(\beta_2,0,1,0,\dots,0),\ \dots,\ e_n=(\beta_n,0,\dots,0,1).$$

This gives differential operators (corresponding to the isomorphism ∂ introduced in Section 3.5)

$$\Delta_1=\partial(e_1)=\beta_1\partial_0+\partial_1, \Delta_2=\partial(e_2)=\beta_2\partial_0+\partial_2,\dots,\Delta_n=\partial(e_n)=\beta_n\partial_0+\partial_n;$$

here $\partial_0,\dots,\partial_n$ is the standard basis for $\mathrm{Lie}(K_v^{n+1})$. Let $\mathbf{u}_0 := (0,u_1,\dots,u_n)$ and $\mathbf{u} := (u_0,u_1,\dots,u_n)$ be vectors in K_v^{n+1} with $u_0 := l(u)$. Then

$$\mathbf{u} = u_1e_1+\cdots+u_ne_n,$$

and this shows that $\mathbf{u}\in\mathscr{W}$. We furthermore see that

$$\mathbf{u}-\mathbf{u}_0 = (l(u),0,\dots,0).$$

Define

$$\Delta^t := \Delta_1^{t_1}\cdots\Delta_n^{t_n} \qquad \text{for } t=(t_1,\dots,t_n)\in\mathbb{N}^n.$$

4.4. The auxiliary function. In this section we shall construct an auxiliary polynomial by using Siegel's lemma. Let $\mathscr{G} := \mathbb{G}_{\mathrm{a}}\times G$. The exponential map of the Lie group $\mathscr{G}(K_v)$ is $\exp_{\mathscr{G}(K_v)} = \mathrm{id}_{K_v}\times\exp$. Note that for $u\in\Lambda_v$ we have $X_0(\mathrm{Exp}(u))\neq 0$; here $\mathrm{Exp}:\Lambda_v\to G(K_v)$ is defined in Section 3.5. We introduce the function

$$\Psi_P := (\mathrm{id}_{K_v}\times\mathrm{Exp})^*P\left(Y,1,\frac{X_1}{X_0},\dots,\frac{X_N}{X_0}\right)$$

for each polynomial P in $N+2$ variables $Y,X_0,\dots,X_N$. This means that $\Psi_P(w)=P(y,1,f_1(x_1,\dots,x_n),\dots,f_N(x_1,\dots,x_n))$ is analytic on $K_v\times\Lambda_v^n$, where $w=(y,x)\in K_v^{n+1}$ with $x=(x_1,\dots,x_n)\in\Lambda_v^n$.

We define the *order* $\mathrm{ord}_{g,\mathscr{W}}P$ of P at $g=(\mathrm{id}_{K_v}\times\mathrm{Exp})(w)$ *along* $\mathscr{W}$ to be infinity if Ψ_P is identically zero in a neighborhood of x, and to be the order of Ψ_P at w along $\mathscr{W}$ otherwise.

Let S_0,D_0,D,T be positive integers. We apply Siegel's lemma to construct a polynomial P in $N+2$ variables with coefficients in $\mathcal{O}_K$ such that

P does not vanish identically on $\mathscr{G}$ and has height $h(P)$ bounded above by a quantity depending on L, S_0, D_0, D, T, b, h. We further require that $\mathrm{ord}_{s\mathbf{u}_0,\mathscr{W}} \Psi_P \gg T$ for all $0 \le s < S_0$.

PROPOSITION 4.2. *There are positive constants c_2 and c_3 such that if $D_0 D^n \ge c_2 S_0 T^n$ there is a polynomial P in $N+2$ variables $Y, X_0 \dots, X_N$ with coefficients in $\mathcal{O}_K$, homogeneous in $X_0, \dots, X_N$ of degree D, and with $\deg P_Y \le D_0$ such that*

(1) *P does not vanish identically on $\mathscr{G}$,*
(2) *$(\Delta^t \Psi_P)(s\mathbf{u}_0) = 0$, $0 \le s < S_0$, $t = (t_1, \dots, t_n)$, $0 \le t_1, \dots, t_n < 2T$,*
(3) *$h(P) \le c_3(T(h_L + \log \delta_L + \log(D + T \log d_L)) + D_0 b + D S_0^2 h)$.*

Proof. Since the dimension of G is n, we may assume that $X_0, \dots, X_n$ are algebraically independent modulo the ideal of G. We shall construct a non-zero polynomial P in $n+2$ variables Y and $X_0, \dots, X_n$ which is homogeneous in $X_0, \dots, X_n$ of degree D (and therefore satisfies (1) of the proposition) such that $\deg_Y P \le D_0$ and such that (2) and (3) of the proposition are satisfied. Such a polynomial can be written in the form

$$P(Y, X) = \sum_{i=0}^{D_0} \sum_{j=1}^{D_1} p_{ij} Y^i M_j(X_0, \dots, X_n),$$

where D_1 is the number of homogeneous monomials of degree D in the $n+1$ variables $X_0, \dots, X_n$, and $M_1, \dots, M_{D_1}$ are all these monomials. An easy computation shows that $D_1 = \binom{D+n}{n}$. For short, we write Ψ for Ψ_P. Let $E = (E_1, \dots, E_N)$ be the addition formula for G as above. By abuse of notation, we set

$$E_i(z, x) := E_i(1, f_1(z), \dots, f_N(z), 1, f_1(x), \dots, f_N(x))$$

for z, x in Λ_v. For $y \in K_v$ we also define

$$\Psi_s(y, x) := \Psi(y, su + x) E_0(su, x)^D.$$

Set

$$I := \{(s, t);\ 0 \le s < S_0,\ t = (t_1, \dots, t_n),\ 0 \le t_1, \dots, t_n < 2T\}.$$

For any $(s, t) \in I$ we shall determine the coefficients p_{ij} such that

$$(\Delta^t \Psi_s)(0, 0) = 0, \quad \forall (s, t) \in I.$$

By the property of the addition formula E, for any x in a neighbourhood of 0 small enough that $E(su, x) \ne 0$, one gets

$$f_i(su + x) = \frac{E_i(su, x)}{E_0(su, x)}, \quad i = 1, \dots, N.$$

This leads to

$$M_j(1, f_1(su+x), \dots, f_n(su+x)) = M_j\left(1, \frac{E_1(su,x)}{E_0(su,x)}, \dots, \frac{E_n(su,x)}{E_0(su,x)}\right)$$
$$= E_0(su,x)^{-D} M_j(E_0(su,x), \dots, E_n(su,x)).$$

Therefore

$$\Psi_s(y,x) = \Psi(y, su+x) E_0(su,x)^D = \sum_{i,j} p_{ij} y^i M_j(E_0(su,x), \dots, E_n(su,x)).$$

On the other hand, for each s, we can express $E_i(su,x)$ as

$$E_i(su,x) = F_i(f_1(x), \dots, f_N(x)), \quad i = 0, \dots, n,$$

where F_i are polynomials in N variables with polynomials (which have coefficients in K) in the $f_1(su), \dots, f_N(su)$ as coefficients. Since

$$\gamma^s = \mathrm{Exp}(su) = (1 : f_1(su) : \ldots : f_N(su))$$

and since $h(\gamma^s) \ll s^2 h$ (see [19, Prop. 5]), we may estimate the heights, $h(F_i) \ll s^2 h$ for $i = 0, \dots, n$. One can therefore choose a common denominator $\mathrm{d}_s \ll s^2 h$ for the polynomials $F_0, \dots, F_n$. Since M_j is a monomial of degree D, there is a polynomial $Q_{j,s}$ in N variables of degree $\ll D$ with $\log |Q_{j,s}|_v \ll D s^2 h$ for $v \in M_K$ such that

$$M_j(E_0(su,x), \dots, E_n(su,x)) = Q_{j,s}(f_1(x), \dots, f_N(x))$$

for each $j = 1, \dots, D_1$. Then

$$\Psi_s(y,x) = \sum_{i,j} p_{ij} y^i Q_{j,s}(f_1(x), \dots, f_N(x)),$$

which gives

$$(\Delta^t \Psi_s)(0,0) = \sum_{i,j} p_{ij} (\Delta^t (y^i Q_{j,s}(f_1, \dots, f_N)))(0,0).$$

Define

$$a_{ij}^{st} := (\Delta^t (y^i Q_{j,s}(f_1, \dots, f_N)))(0,0)$$

for $i = 0, \dots, D_0$, $j = 1, \dots, D_1$ and $(s,t) \in I$. Note that $\partial_0 = \partial/\partial y$. We expand

$$\begin{aligned}
a_{i,j}^{st} &= \big(\Delta_1^{t_1} \cdots \Delta_n^{t_n} (y^i Q_{j,s}(f_1, \dots, f_N))\big)(0,0) \\
&= \big((\beta_1 \partial_0 + \partial_1)^{t_1} \cdots (\beta_n \partial_0 + \partial_n)^{t_n} (y^i Q_{j,s}(f_1, \dots, f_N))\big)(0,0) \\
&= \sum_{i_1=0}^{t_1} \cdots \sum_{i_n=0}^{t_n} \binom{t_1}{i_1} \cdots \binom{t_n}{i_n} \beta_1^{t_1-i_1} \cdots \beta_n^{t_n-i_n} \\
&\quad \cdot \left(\left(\frac{\partial}{\partial y}\right)^{(t_1+\cdots+t_n)-(i_1+\cdots+i_n)} \partial_1^{i_1} \cdots \partial_n^{i_n} (y^i Q_{j,s}(f_1, \dots, f_N))\right)(0,0)
\end{aligned}$$

$$= \sum_{i_1=0}^{t_1} \cdots \sum_{i_n=0}^{t_n} \binom{t_1}{i_1} \cdots \binom{t_n}{i_n} \beta_1^{t_1-i_1} \cdots \beta_n^{t_n-i_n}$$
$$\cdot \left(\left(\frac{\partial}{\partial y} \right)^{(t_1+\cdots+t_n)-(i_1+\cdots+i_n)} y^i \right)(0) \big(\partial_1^{i_1} \cdots \partial_n^{i_n} (Q_{j,s}(f_1, \ldots, f_N)) \big)(0).$$

For $m \in \mathbb{N}^n$, Lemma 3.9 yields

$$\partial^m (Q_{j,s}(f_1, \ldots, f_N)) = Q_{j,s,m}(f_1, \ldots, f_N)$$

for some polynomial $Q_{j,s,m}$ in N variables with

$$\begin{aligned} \log |Q_{j,s,m}|_v &\ll \log |Q_{j,s}|_v + |m|(h_L + \log(D + |m| d_L)) \\ &\ll |m|(h_L + \log(D + |m| d_L)) + Ds^2 h, \quad \forall v \in M_K. \end{aligned}$$

This means that

$$\log \left| (\partial^m (Q_{j,s}(f_1, \ldots, f_n)))(0) \right|_v \ll |m|(h_L + \log(D + |m| d_L)) + Ds^2 h$$

for $v \in M_K$. In particular,

$$\begin{aligned} &\log \left| \big(\partial_1^{i_1} \cdots \partial_n^{i_n} (Q_{j,s}(f_1, \ldots, f_N)) \big)(0) \right|_v \\ &\qquad \ll T(h_L + \log(D + T d_L)) + Ds^2 h, \quad \forall v \in M_K. \end{aligned}$$

Furthermore,

$$\begin{aligned} &\left(\left(\frac{\partial}{\partial y} \right)^{(t_1+\cdots+t_n)-(i_1+\cdots+i_n)} y^i \right)(0) \\ &\qquad = \begin{cases} 0 & \text{if } (t_1 + \cdots + t_n) - (i_1 + \cdots + i_n) \neq i, \\ i! & \text{if } (t_1 + \cdots + t_n) - (i_1 + \cdots + i_n) = i. \end{cases} \end{aligned}$$

In other words,

$$\log \left| \left(\left(\frac{\partial}{\partial y} \right)^{(t_1+\cdots+t_n)-(i_1+\cdots+i_n)} y^i \right)(0) \right|_v \ll \log(T!) \ll T \log T, \quad \forall v \in M_K^\infty.$$

We deduce that

$$\log |a_{ij}^{st}|_v \ll T(h_L + \log(D + T d_L)) + Ds^2 h, \quad \forall v \in M_K^\infty.$$

Since $h(\beta_i) \leq b$ for $i = 1, \ldots, n$, $\log |\beta_i|_v \leq b$ for $v \in M_K$. By noting that $\mathrm{d}_s {\delta_L}^{|m|} Q_{j,s,m}$ has coefficients in $\mathcal{O}_K$, we find that $\mathrm{d}_s {\delta_L}^{2nT} a_{ij}^{st}$ is also in $\mathcal{O}_K$ and

$$\log |\mathrm{d}_s {\delta_L}^{2nT} a_{ij}^{st}|_v \ll D_0 b + T(\log \delta_L + h_L + \log(D + T \log d_L)) + DS_0^2 h$$

for $(s,t) \in I$ and for $v \in M_K^\infty$. We now consider the linear forms in $n_0 := D_0 D_1$ variables T_{ij},

$$l_{st} := \sum_{i,j} b_{ij}^{st} T_{ij},$$

where $b_{ij}^{st} := \mathrm{d}_s {\delta_L}^{2nT} a_{ij}^{st}$ for all $(s,t) \in I$. Let m_0 be the number of these linear forms; then $m_0 \ll S_0 T^n$ and $n_0 = D_0 D_1 = D_0\binom{D+n}{n} \gg D_0 D^n$. Since $b_{ij}^{st} \in \mathcal{O}_K$ we get

$$\begin{aligned} h_{\max}(l_{st}) &= \sum_{v \in M_K^\infty} \log \max_{i,j} |b_{ij}^{st}|_v \\ &\ll D_0 b + T(h_L + \log \delta_L + \log(D + T \log d_L)) + D S_0^2 h. \end{aligned}$$

We now apply Siegel's lemma: under the condition $D_0 D^n \gg S_0 T^n$ there is a non-zero vector $p_0 = (p_{ij})$ with coordinates in $\mathcal{O}_K$ such that $l_{st}(p_0) = 0$ and

$$h(p_0) \le \frac{m_0}{n_0 - m_0} \max_{s,t} h_{L^2}(l_{st}).$$

But using $h_{L^2}(l_{st}) \ll h_{\max}(l_{st}) + \log n_0$ gives

$$h(P) \ll D_0 b + T(h_L + \log \delta_L + \log(D + T d_L)) + D S_0^2 h.$$

It remains to show that $(\Delta^t \Psi)(s\mathbf{u}_0) = 0$. In fact, since $l_{st}(p_0) = 0$ one gets $(\Delta^t \Psi_s)(0,0) = 0$ for $(s,t) \in I$. Set

$$\Psi_s^*(y,x) := \Psi(y, su + x), \quad E_s(x) := E_0(su, x)^D;$$

then $\Psi_s^* = \Psi_s E_s^{-D}$. Therefore, by Leibniz' rule,

$$(\Delta^t \Psi)(s\mathbf{u}_0) = (\Delta^t \Psi)(0, su) = (\Delta^t \Psi_s^*)(0,0) = (\Delta^t(\Psi_s E_s^{-D}))(0,0) = 0.$$

This completes the proof. ∎

From now on until Section 4.8, we shall fix a polynomial P as in Proposition 4.2 and let $\Psi = \Psi_P$ be the analytic function associated with P.

4.5. Extrapolation. In this section we use the p-adic Schwarz lemma to give an upper bound for $|(\Delta^t \Psi)(s\mathbf{u})|_p$ (with $|t| < T$). We need

LEMMA 4.3. *Let Q be a polynomial in $k+1$ variables $X_0, \ldots, X_k$ with coefficients in the ring $\mathcal{O}_v$ of algebraic integers of K_v and $\deg_{X_0} Q \le l$ with $l \in \mathbb{N}$, $l \ge 1$. Then*

$$|Q(x_0, x) - Q(0, x)|_p \le \max_{1 \le i \le l} |x_0|_p^i$$

for any $x_0 \in K_v$ and $x \in \mathcal{O}_v^k$.

Proof. We define the polynomial $Q_x(X) := Q(X, x)$ in one variable X. By assumption and by the ultrametric inequality, Q_x has coefficients in $\mathcal{O}_v$. We write $Q_x(X) = a_l X^l + \cdots + a_0$ with $a_0, \ldots, a_l \in \mathcal{O}_v$. Then

$$|Q_x(x_0) - Q_x(0)|_p = |a_l x_0^l + \cdots + a_1 x_0|_p \le \max_{1 \le i \le l} |a_i x_0^i|_p \le \max_{1 \le i \le l} |x_0|_p^i. \ ∎$$

LEMMA 4.4. *For $0 \le s < S$ and for $t = (t_1, \ldots, t_n) \in \mathbb{N}^n$ such that $0 \le t_1, \ldots, t_n < 2T$ we have*

$$|(\Delta^t \Psi)(s\mathbf{u}) - (\Delta^t \Psi)(s\mathbf{u}_0)|_p \le |\delta_L^{-1}|_p^{2nT} |l(u)|_p.$$

Proof. We can write again

$$P(Y,X_0,\dots,X_N)=\sum_{i,j}p_{ij}Y^iM_j(X_0,\dots,X_N).$$

Set $R_j(x)=M_j(1,f_1(x),\dots,f_N(x))$; then

$$\begin{aligned}\Delta^t\Psi&=\sum_{i,j}p_{ij}(\Delta^t(y^iR_j))=\sum_{i,j}p_{ij}\big((\beta_1\partial_0+\partial_1)^{t_1}\cdots(\beta_n\partial_0+\partial_n)^{t_n}(y^iR_j)\big)\\&=\sum_{i,j}p_{ij}\sum_{i_1=0}^{t_1}\cdots\sum_{i_n=0}^{t_n}\binom{t_1}{i_1}\cdots\binom{t_n}{i_n}\beta_1^{t_1-i_1}\cdots\beta_n^{t_n-i_n}\\&\qquad\cdot\bigg(\Big(\frac{\partial}{\partial y}\Big)^{(t_1+\dots+t_n)-(i_1+\dots+i_n)}\partial_1^{i_1}\cdots\partial_n^{i_n}(y^iR_j)\bigg)\\&=\sum_{i,j}p_{ij}\sum_{i_1=0}^{t_1}\cdots\sum_{i_n=0}^{t_n}\binom{t_1}{i_1}\cdots\binom{t_n}{i_n}\beta_1^{t_1-i_1}\cdots\beta_n^{t_n-i_n}\\&\qquad\cdot\bigg(\Big(\frac{\partial}{\partial y}\Big)^{(t_1+\dots+t_n)-(i_1+\dots+i_n)}y^i\bigg)(\partial_1^{i_1}\cdots\partial_n^{i_n}R_j).\end{aligned}$$

Using the fact that

$$\Big(\frac{\partial}{\partial y}\Big)^{(t_1+\dots+t_n)-(i_1+\dots+i_n)}y^i=0\quad\text{if}\quad(t_1+\dots+t_n)-(i_1+\dots+i_n)>i,$$

and that $\partial_1^{i_1}\cdots\partial_n^{i_n}R_j$ is a polynomial in $f_1,\dots,f_N$ with denominator bounded above by $\delta_L^{|t|}$ by Lemma 3.11, we deduce that

$$\delta_L^{|t|}\beta_1^{t_1-i_1}\cdots\beta_n^{t_n-i_n}\bigg(\Big(\frac{\partial}{\partial y}\Big)^{(t_1+\dots+t_n)-(i_1+\dots+i_n)}y^i\bigg)(\partial_1^{i_1}\cdots\partial_n^{i_n}R_j)$$

is a polynomial in $y,f_1,\dots,f_N$ with coefficients in $\mathcal{O}_K$. On the other hand, the coefficients p_{ij} are in $\mathcal{O}_K$, and this implies that

$${\delta_L}^{|t|}(\Delta^t\Psi)=Q_t(y,f_1,\dots,f_N)$$

for some polynomial $Q_t(Y,X_1,\dots,X_N)$ with coefficients in $\mathcal{O}_K$, and with $\deg_Y Q_t\le D_0$. This means that

$$\begin{aligned}&|(\Delta^t\Psi)(s\mathbf{u})-(\Delta^t\Psi)(s\mathbf{u}_0)|_p\\&\qquad=|\delta_L|_p^{-|t|}|Q_t(su_0,f_1(su),\dots,f_N(su))-Q_t(0,f_1(su),\dots,f_N(su))|_p.\end{aligned}$$

Since $u\in\Lambda_v\cap B^n(r_p|\delta_L|_p)$, we get $|f_1(su)|_p,\dots,|f_N(su)|_p<1$ by Proposition 3.12, and taking into account that $r_p|\delta_L|_p<1$ and $\beta_1,\dots,\beta_n\in\mathcal{O}_K$, we find that

$$|su_0|_p=|s|_p|u_0|_p\le|u_0|_p=|\beta_1u_1+\dots+\beta_nu_n|_p<1.$$

By Lemma 4.3 we obtain

$$|(\Delta^t\Psi)(s\mathbf{u}) - (\Delta^t\Psi)(s\mathbf{u}_0)|_p \le |\delta_L|_p^{-2nT} \max_{1\le i\le D_0} |su_0|_p^i$$
$$\le |\delta_L^{-1}|_p^{2nT}|u_0|_p = |\delta_L^{-1}|_p^{2nT}|l(u)|_p. \ ■$$

PROPOSITION 4.5. *For $0 \le s < S_0$ and for $t = (t_1,\dots,t_n) \in \mathbb{N}^n$ such that $0 \le t_1,\dots,t_n < 2T$ we have*

$$|(\Delta^t\Psi)(s\mathbf{u})|_p \le |\delta_L^{-1}|_p^{2nT}|l(u)|_p.$$

Proof. By Proposition 4.4, for $0 \le s < S_0$ and for $t = (t_1,\dots,t_n) \in \mathbb{N}^n$ with $0 \le t_1,\dots,t_n < 2T$ one has

$$|(\Delta^t\Psi)(s\mathbf{u}) - (\Delta^t\Psi)(s\mathbf{u}_0)|_p \le |\delta_L^{-1}|_p^{2nT}|l(u)|_p.$$

Moreover by Proposition 4.2, for $0 \le s < S_0$ and for $t = (t_1,\dots,t_n) \in \mathbb{N}^n$ with $0 \le t_1,\dots,t_n < 2T$ we have

$$(\Delta^t\Psi)(s\mathbf{u}_0) = 0.$$

This gives the desired conclusion. ■

For each n-tuple $t \in \mathbb{N}^n$ such that $|t| < T$ we introduce the function

$$f(z) := (\Delta^t\Psi)(z\mathbf{u})$$

in the variable z. It is analytic on $\overline{B}(1)$. Our next step is to apply Proposition 3.3 to the function f. We shall prove an upper bound for the derivatives of f on a certain finite set. Thanks to Proposition 4.5, one gets

PROPOSITION 4.6. *For $\tau, s \in \mathbb{Z}$ such that $0 \le \tau < T$ and $0 \le s < S_0$ we have*

$$|f^{(\tau)}(s)|_p \le |\delta_L^{-1}|_p^{2nT}|l(u)|_p.$$

Proof. By recalling that $\mathbf{u} = u_1e_1 + \cdots + u_ne_n$ and using the composition rule for derivatives we get

$$\begin{aligned} f^{(\tau)}(z) &= \big((u_0\partial_0 + \cdots + u_n\partial_n)^\tau \Delta^t\Psi\big)(z\mathbf{u}) \\ &= \big(((\beta_1u_1 + \cdots + \beta_nu_n)\partial_0 + u_1\partial_1 + \cdots + u_n\partial_n)^\tau \Delta^t\Psi\big)(z\mathbf{u}) \\ &= \big((u_1(\beta_1\partial_0 + \partial_1) + \cdots + u_n(\beta_n\partial_0 + \partial_n))^\tau \Delta^t\Psi\big)(z\mathbf{u}) \\ &= \big((u_1\Delta_1 + \cdots + u_n\Delta_n)^\tau \Delta^t\Psi\big)(z\mathbf{u}). \end{aligned}$$

Since $|u_i|_p < 1$ for $i = 1,\dots,n$, the multinomial expansion together with the ultrametric inequality gives

$$|f^{(\tau)}(z)|_p \le \max_{0\le i_1,\dots,i_n\le\tau;\, i_1+\cdots+i_n=\tau} |(\Delta_1^{i_1}\cdots\Delta_n^{i_n}\Delta^t\Psi)(z\mathbf{u})|_p.$$

Since τ and $|t|$ are $< T$, the assertion follows from Proposition 4.5. ■

LEMMA 4.7. *Let $\alpha \ne 0$ in K_v be such that $|\alpha|_p < p^{-1/(p-1)}$. Then*

$$v(\alpha) - \frac{1}{p-1} \ge \frac{1}{2d^2}.$$

Proof. We know that $v(K_v^\times) = (1/d_v)\mathbb{Z}$ with $d_v := [K_v : \mathbb{Q}_p]$. Since $|\alpha|_p = p^{-v(\alpha)} < p^{-1/(p-1)}$, there is a positive integer a such that

$$v(\alpha) = \frac{a}{d_v} > \frac{1}{p-1}.$$

This implies that $a(p-1) - d_v \geq 1$. If $p-1 \geq 2d_v$ then

$$v(\alpha) - \frac{1}{p-1} \geq \frac{1}{d_v} - \frac{1}{p-1} \geq \frac{1}{2d_v} \geq \frac{1}{2d} \geq \frac{1}{2d^2}.$$

Otherwise, if $p-1 < 2d_v$ then

$$v(\alpha) - \frac{1}{p-1} = \frac{a(p-1)-d_v}{d_v(p-1)} \geq \frac{1}{d_v(p-1)} > \frac{1}{2d_v^2} \geq \frac{1}{2d^2}. \quad \blacksquare$$

From now on we set $\epsilon := 1/(3d^2)$. Combining Lemma 4.7 and Proposition 4.6 together with Proposition 3.3, we will get

PROPOSITION 4.8. *For $s \in \mathbb{N}$ and $t = (t_1, \ldots, t_n) \in \mathbb{N}^n$ such that $|t| < T$ we have*

$$|(\varDelta^t \varPsi)(s\mathbf{u})|_p \leq p^{-(\epsilon S_0 - e_L)T} \max\{1, p^{((2n-1)e_L + \epsilon S_0 + \frac{1}{p-1})T} S_0^{S_0 T} |l(u)|_p\}.$$

Proof. As above, we consider the function $f(z) = (\varDelta^t \varPsi)(z\mathbf{u})$, and apply the p-adic Schwarz lemma to f. We first show that f is analytic on $\overline{B}(R)$, where $R := p^\epsilon$. It suffices to show that $zu_i \in B(r_p|\delta_L|_p)$ for $z \in \overline{B}(R)$ and $i = 1, \ldots, n$. In fact, if $u_i = 0$ then this is trivially true. Otherwise, since $|\delta_L^{-1} u_i|_p < p^{-1/(p-1)}$, it follows from Lemma 4.7 that

$$v(\delta_L^{-1} u_i) - \frac{1}{p-1} \geq \frac{1}{2d^2}.$$

Hence

$$v(\delta_L^{-1} u_i) - \epsilon = \frac{1}{p-1} + \left(v(\delta_L^{-1} u_i) - \frac{1}{p-1} - \frac{1}{3d^2} \right) > \frac{1}{p-1},$$

which leads to

$$R|\delta_L^{-1}|_p |u_i|_p = p^\epsilon p^{-v(\delta_L^{-1} u_i)} = p^{-(v(\delta_L^{-1} u_i) - \epsilon)} < p^{-1/(p-1)},$$

or equivalently to $R|u_i|_p < r_p |\delta_L|_p$. This means that $zu_i \in B(r_p|\delta_L|_p)$ for $z \in \overline{B}(R)$. Next we establish an upper bound for $|f|_R$. As in the proof of Proposition 4.4, there is a polynomial $Q(Y, X_1, \ldots, X_N)$ with coefficients in $\mathcal{O}_K$ such that $\deg_Y Q \leq D_0$ and

$$f(z) = \delta_L^{-T} Q(zu_0, f_1(zu), \ldots, f_N(zu)).$$

We note that

$$\begin{aligned} |zu_0|_p &= |\beta_1 z u_1 + \cdots + \beta_n z u_n|_p \leq |zu_1 + \cdots + zu_n|_p \\ &\leq \max\{|zu_1|_p, \ldots, |zu_n|_p\} < 1, \end{aligned}$$

and deduce from Proposition 3.12 that $|f_i(zu)|_p < 1$ for $i = 1, \ldots, N$ and for $z \in \overline{B}(R)$. This gives $|Q(zu_0, f_1(zu), \ldots, f_N(zu))|_p \le 1$, which leads to

$$|f(z)|_p \le |\delta_L^{-1}|_p^T, \quad \forall z \in \overline{B}(R).$$

In other words,

$$|f|_R \le |\delta_L^{-1}|_p^T.$$

Finally, let $\Gamma := \{s \in \mathbb{Z};\, 0 \le s < S_0\}$ and let δ be the minimum of $|s - s'|_p$ for $s \neq s'$ in Γ. The cardinality of Γ is S_0 and we have $\delta \le 1$. We define

$$\mu := \sup\{|f^{(\tau)}(s)|_p;\, 0 \le \tau < T,\, s \in \Gamma\}.$$

Using Lemma 4.6 we get $\mu \le |\delta_L^{-1}|_p^{2nT} |l(u)|_p$. We apply Proposition 3.3 to obtain

$$\begin{aligned}
|f|_1 &\le \max\{(1/R)^{S_0T}|f|_R, \mu(1/\delta)^{S_0T-1} r_p^{-(T-1)}\} \\
&\le \max\left\{p^{-\epsilon S_0 T}|\delta_L^{-1}|_p^T, |\delta_L^{-1}|_p^{2nT}|l(u)|_p \delta^{-(S_0T-1)} r_p^{-T}\right\} \\
&\le \max\left\{p^{-\epsilon S_0 T} p^{e_L T}, p^{2ne_L T} p^{\frac{T}{p-1}} \delta^{-(S_0T-1)}|l(u)|_p\right\} \\
&\le \max\left\{p^{-(\epsilon S_0 - e_L)T}, p^{(2ne_L + \frac{1}{p-1})T} \delta^{-(S_0T-1)}|l(u)|_p\right\}.
\end{aligned}$$

Moreover, for $s, s' \in \Gamma$ such that $s \neq s'$ one has

$$|s - s'|_p \ge \frac{1}{|s - s'|} > \frac{1}{S_0}.$$

This gives $\delta^{-1} < S_0$. Thus we obtain

$$\begin{aligned}
|f|_1 &\le \max\{p^{-(\epsilon S_0 - e_L)T}, p^{(2ne_L + \frac{1}{p-1})T} S_0^{S_0T}|l(u)|_p\} \\
&= p^{-(\epsilon S_0 - e_L)T} \max\{1, p^{((2n-1)e_L + \epsilon S_0 + \frac{1}{p-1})T} S_0^{S_0T}|l(u)|_p\}.
\end{aligned}$$

The proposition therefore follows from the fact that $|(\Delta^t\Psi)(s\mathbf{u})|_p = |f(s)|_p \le |f|_1$ for all integers $s \ge 0$. ∎

Proposition 4.9. *There is a positive constant c_4 such that if*

$$\log|l(u)|_p \le -c_4\left(\left(S_0 + \frac{1}{p-1} + e_L\right)T\log p + S_0T\log S_0\right)$$

then

$$\log|(\Delta^t\Psi)(s\mathbf{u}_0)|_p \le -\big(\epsilon S_0 - e_L)T\log p$$

for $t \in \mathbb{N}^n$ with $|t| < T$ and for $s \in \mathbb{N}$.

Proof. By Lemma 4.4,

$$|(\Delta^t\Psi)(s\mathbf{u}) - (\Delta^t\Psi)(s\mathbf{u}_0)|_p \le |\delta_L^{-1}|_p^{2nT}|l(u)|_p = p^{2ne_LT}|l(u)|_p,$$

and by Proposition 4.8,

$$|(\Delta^t\Psi)(s\mathbf{u})|_p \le p^{-(\epsilon S_0 - e_L)T} \max\{1, p^{((2n-1)e_L + \epsilon S_0 + \frac{1}{p-1})T} S_0^{S_0T}|l(u)|_p\}.$$

Hence

$$\begin{aligned}|(\Delta^t\Psi)(s\mathbf{u}_0)|_p \le\ & \max\{|(\Delta^t\Psi)(s\mathbf{u})|_p, |(\Delta^t\Psi)(s\mathbf{u})-(\Delta^t\Psi)(s\mathbf{u}_0)|_p\}\\ &\le p^{-(\epsilon S_0-e_L)T}\max\{1, p^{((2n-1)e_L+\epsilon S_0+\frac{1}{p-1})T}S_0^{S_0T}|l(u)|_p,\\ &\qquad\qquad p^{((2n-1)e_L+\epsilon S_0)T}|l(u)|_p\}\\ &\le p^{-(\epsilon S_0-e_L)T}\max\{1, p^{((2n-1)e_L+\epsilon S_0+\frac{1}{p-1})T}S_0^{S_0T}|l(u)|_p\}.\end{aligned}$$

On the other hand,

$$p^{((2n-1)e_L+\epsilon S_0+\frac{1}{p-1})T}S_0^{S_0T}|l(u)|_p \le 1$$

if and only if

$$|l(u)|_p \le p^{-((2n-1)e_L+\epsilon S_0+\frac{1}{p-1})T}S_0^{-S_0T}.$$

In other words, if

$$\log|l(u)|_p \le -\Big((2n-1)e_L+\epsilon S_0+\frac{1}{p-1}\Big)T\log p - S_0T\log S_0,$$

then

$$|(\Delta^t\Psi)(s\mathbf{u}_0)|_p \le p^{-(\epsilon S_0-e_L)T}.$$

This means that there is a positive constant c_4 such that if

$$\log|l(u)|_p \le -c_4\Big(\Big(S_0+\frac{1}{p-1}+e_L\Big)T\log p + S_0T\log S_0\Big)$$

then

$$\log|(\Delta^t\Psi)(s\mathbf{u}_0)|_p \le -(\epsilon S_0-e_L)T\log p. \ ■$$

4.6. A lower bound. Using Liouville's inequality, we derive the following result that will be crucial in the proof of the main result.

PROPOSITION 4.10. *Let s be an integer such that $0 \le s < S$. Assume that Ψ has a zero at $s\mathbf{u}_0$ of exact order T' along $\mathscr{W}$ for some positive integer T'. Let $t \in \mathbb{Z}^n_{\ge 0}$ with $|t| = T'$ be such that $(\Delta^t\Psi)(s\mathbf{u}_0) \ne 0$. Then*

$$\log|(\Delta^t\Psi)(s\mathbf{u}_0)|_p > -c_5\big(T'(h_L+\log\delta_L+\log(D+T'd_L))+D_0b+DS^2h\big)$$

for some positive constant c_5.

Proof. As in the proof of Proposition 4.2, for $y \in K_v$ and $x \in \Lambda_v^n$ we define

$$\Psi_s^*(y,x) := \Psi(y, su+x),\quad E_s(x) := E_0(su,x),\quad \Psi_s(y,x) := \Psi_s^*(y,x)E_s(x)^D.$$

By our assumption

$$0 = (\Delta^\tau\Psi)(s\mathbf{u}_0) = (\Delta^\tau\Psi)(0,su) = (\Delta^\tau\Psi_s^*)(0,0)$$

for $\tau \in \mathbb{N}^n$ with $|\tau| < T'$. Leibniz' rule gives

$$(\Delta^\tau\Psi_s)(0,0) = (\Delta^\tau(\Psi_s^*E_s^D))(0,0) = 0.$$

Using Leibniz' rule again, one gets

$$(\Delta^t\Psi)(s\mathbf{u}_0) = (\Delta^t(\Psi_s E_s^{-D}))(0,0) = (\Delta^t\Psi_s)(0,0)E_s^{-D}(0).$$

The same arguments as in the proof of Proposition 4.2 (just replace S_0 by S) show that

$$h((\Delta^t\Psi_s)(0,0)) \ll T'(h_L + \log\delta_L + \log(D + T'\log d_L)) + D_0 b + DS^2 h.$$

Furthermore,

$$h(E_s^{-D}(0)) = h(E_0(su,0)^{-D}) = Dh(E_0(su,0)) \ll DS^2 h.$$

Since $(\Delta^t\Psi)(s\mathbf{u}_0) \neq 0$, Liouville's inequality gives

$$\begin{aligned}\log|(\Delta^t\Psi)(s\mathbf{u}_0)|_p &\gg -h((\Delta^t\Psi)(s\mathbf{u}_0)) = -h\big((\Delta^t\Psi_s)(0,0)E_s(0)^{-D}\big)\\ &\gg -\big(T'(h_L + \log\delta_L + \log(D + T'd_L)) + D_0 b + DS^2 h\big),\end{aligned}$$

and the proposition follows. ∎

4.7. Multiplicity estimates. Another crucial point for proving the theorem is the following lemma. For the proof we use [17], but we also refer to [21] (and to [22], where the multiplicity estimates part has been published); the result of [17] is a modification of the multiplicity estimate part of the habilitation thesis [21].

LEMMA 4.11. *Let $\eta := (0,\gamma)$ and $\Gamma(\eta) := \{\eta^i;\ i \in \mathbb{N}\}$. Let $H(\mathscr{H}; D_0, D)$ and $H(\mathscr{G}; D_0, D)$ be the Hilbert–Samuel functions associated with the ideals of $\mathscr{H}$ and $\mathscr{G}$ respectively. If Ψ vanishes at any point of $\{s\mathbf{u}_0;\ 0 \le s < S\}$ along $\mathscr{W}$ of order $\ge T$, then there are a connected algebraic subgroup $\mathscr{H}$ defined over K distinct from $\mathscr{G}$ and a positive constant c_6 such that*

$$\binom{T + \operatorname{codim}_{\mathscr{W}_p}\mathscr{W}_p \cap T_{\mathscr{H}}}{\operatorname{codim}_{\mathscr{W}_p}\mathscr{W}_p \cap T_{\mathscr{H}}} \operatorname{card}((\Gamma(\eta) + \mathscr{H})/\mathscr{H}) H(\mathscr{H}; D_0, D) \le c_6 H(\mathscr{G}; D_0, D),$$

where $\mathscr{W}_p := \mathscr{W} \otimes_{K_v} \mathbb{C}_p$ and $T_{\mathscr{H}} = \mathrm{Lie}(\mathscr{H}) \otimes_K \mathbb{C}_p$.

Proof. We associate with P the bihomogeneous polynomial P^h in $N+2$ variables $Y_0, Y_1, X_0, \ldots, X_N$ of degree D_0 in Y_0, Y_1 and degree D in $X_0, \ldots, X_N$ defined by

$$P^h(Y_0, Y_1, X_0, \ldots, X_N) := Y_0^{D_0} P(Y_1/Y_0, X_0, \ldots, X_N).$$

Since $\mathrm{ord}_{s\mathbf{u}_0,\mathscr{W}}\Psi \ge T$, the order at any point $s\mathbf{u}_0$ along $\mathscr{W}$ of the analytic function $P^h(1, y, 1, f_1(x), \ldots, f_N(x))$ is at least T. This also means that the order of $P^h(1, y, 1, f_1(x), \ldots, f_N(x))$ along $\mathscr{W}_p$ at any point $s\mathbf{u}_0$ is at least T. Therefore the lemma follows immediately from [17, Theorem 2.1]. ∎

4.8. Choice of parameters and proof of Theorem 2.1. We choose parameters as follows. Let c be a large enough positive constant and

$$S_0 = [c\omega_L(\log b + \log h)], \qquad S = [c^2 S_0],$$
$$D_0 = [c^{5n+1} S_0^{n+1} h^n], \qquad D = [c^{5n+1} S_0^n b h^{n-1}], \qquad T = [c^{5n+6} S_0^{n+1} b h^n],$$

where $[\cdot]$ denotes the integer part. Our parameters satisfy $D_0 D^n \geq c_2 S_0 T^n$. Proposition 4.2 gives a polynomial P in $N+2$ variables $Y, X_0 \ldots, X_N$ with coefficients in $\mathcal{O}_K$, homogeneous in $X_0, \ldots, X_N$ of degree D, and with $\deg P_Y \leq D_0$, such that

- P does not vanish identically on $\mathscr{G}$,
- $(\varDelta^t \varPsi)(s\mathbf{u}_0) = 0$ for all $0 \leq s < S_0$ and $t = (t_1, \ldots, t_n)$, $0 \leq t_1, \ldots, t_n < 2T$,
- $h(P) \leq c_3(T(h_L + \log \delta_L + \log(D + Td_L)) + D_0 b + DS_0^2 h)$;

here we write $\varPsi$ for $\varPsi_P$.

Lemma 4.12.

$$\log |l(u)|_p > -c_4\biggl(\biggl(S_0 + \frac{1}{p-1} + e_L\biggr) T \log p + S_0 T \log S_0\biggr).$$

Proof. On assuming that

$$\log |l(u)|_p \leq -c_4\biggl(\biggl(S_0 + \frac{1}{p-1} + e_L\biggr) T \log p + S_0 T \log S_0\biggr)$$

Proposition 4.9 gives

$$\log |(\varDelta^t \varPsi)(s\mathbf{u}_0)|_p \leq -(\epsilon S_0 - e_L) T \log p.$$

We shall show that the order of $\varPsi$ along $\mathscr{W}$ at any point of $\{s\mathbf{u}_0;\ 0 \leq s < S\}$ is at least T. Otherwise there is some point $s_0\mathbf{u}_0$ with $0 \leq s_0 < S$ at which the exact order along $\mathscr{W}$ is $T_0 < T$. This means that there exists $\tau \in \mathbb{N}^n$ such that $|\tau| = T_0$ and $(\varDelta^\tau \varPsi)(s_0\mathbf{u}_0) \neq 0$. We apply Proposition 4.10 to get

$$\log |(\varDelta^\tau \varPsi)(s_0\mathbf{u}_0)|_p > -c_5\bigl(T_0(h_L + \log \delta_L + \log(D + T_0 d_L)) + D_0 b + DS^2 h\bigr).$$

The comparison with the lower bound above implies that

$$-(\epsilon S_0 - e_L) T \log p \geq -c_5\bigl(T(h_L + \log \delta_L + \log(D + Td_L)) + D_0 b + DS^2 h\bigr).$$

This yields

$$(\epsilon S_0 - e_L) T \log p \leq c_5\bigl(T(h_L + \log \delta_L + \log(D + Td_L)) + D_0 b + DS^2 h\bigr)$$

and shows that

$$\biggl(\frac{1}{3d^2} \log 2\biggr) T(S_0 - e_L) \leq c_5\bigl(T(h_L + \log \delta_L + \log(D + Td_L)) + D_0 b + DS^2 h\bigr).$$

This means that there is a positive constant c_7 satisfying

$$T(S_0 - e_L) \le c_7\big(T(h_L + \log\delta_L + \log(D + Td_L)) + D_0 b + DS^2 h\big).$$

We get a contradiction because this cannot hold if c is sufficiently large. Therefore Ψ vanishes at any point of $\{s\mathbf{u}_0;\, 0 \le s < S\}$ of order at least T along $\mathscr{W}$. By Lemma 4.11, there is a connected algebraic subgroup $\mathscr{H}$ defined over K distinct from $\mathscr{G}$ and such that

$$\binom{T + \operatorname{codim}_{\mathscr{W}_p}\mathscr{W}_p \cap T_{\mathscr{H}}}{\operatorname{codim}_{\mathscr{W}_p}\mathscr{W}_p \cap T_{\mathscr{H}}} \operatorname{card}((\Gamma(\eta) + \mathscr{H})/\mathscr{H}) H(\mathscr{H}; D_0, D) \le c_6 H(\mathscr{G}; D_0, D).$$

Since G and $\mathbb{G}_{\mathrm{a}}$ are disjoint, there are subgroups H_{a} of $\mathbb{G}_{\mathrm{a}}$ and H of G (defined over K) such that $\mathscr{H} = H_{\mathrm{a}} \times H$. Let n_{a} be the dimension of H_{a} and n' be the dimension of H. We know that $H(\mathscr{H}; D_0, D) \gg D_0^{n_{\mathrm{a}}} D^{n'}$ and $H(\mathscr{G}; D_0, D) \ll D_0 D^n$. The above inequality gives

$$\binom{T + \operatorname{codim}_{\mathscr{W}_p}\mathscr{W}_p \cap T_{\mathscr{H}}}{\operatorname{codim}_{\mathscr{W}_p}\mathscr{W}_p \cap T_{\mathscr{H}}} \operatorname{card}((\Gamma(\eta) + \mathscr{H})/\mathscr{H}) \ll D_0^{1-n_{\mathrm{a}}} D^{n-n'}.$$

We shall show that H must be the trivial group $\{e\}$. Indeed, if not, then we get a proper quotient $\pi : G \to G/H$ inducing a linear map $\pi_* : \mathfrak{g} \to \mathfrak{g}/\mathfrak{h}$ of Lie algebras which maps the hyperplane W onto $(W + \mathfrak{h})/\mathfrak{h}$; here $\mathfrak{g}$ and $\mathfrak{h}$ denote the Lie algebras of G and H respectively. Furthermore, $\tau(G, W) = (n-1)/n$, and since (G, W) is semistable over $\overline{\mathbb{Q}}$, it is also semistable over K. This gives

$$\tau(G, W) \le \tau(G/H, \pi_*(W)) = \frac{\dim(W + \mathfrak{h}) - \dim\mathfrak{h}}{\dim G - \dim H} = \frac{\dim(W + \mathfrak{h}) - n'}{n - n'}.$$

But

$$n - 1 = \dim W \le \dim(W + \mathfrak{h}) \le n,$$

and this shows that $\dim(W + \mathfrak{h}) = n$, i.e. $\dim(\mathscr{W}_p + T_{\mathscr{H}}) = n$. This gives

$$\operatorname{codim}_{\mathscr{W}_p}\mathscr{W}_p \cap T_{\mathscr{H}} = \dim(\mathscr{W}_p + T_{\mathscr{H}}) - \dim T_{\mathscr{H}} = n + 1 - n_{\mathrm{a}} - n',$$

and shows that

$$\binom{T + n + 1 - n_{\mathrm{a}} - n'}{n + 1 - n_{\mathrm{a}} - n'} \ll D_0^{1-n_{\mathrm{a}}} D^{n-n'}.$$

We deduce that

$$T^{n+1-n_{\mathrm{a}}-n'} \le c_8 D_0^{1-n_{\mathrm{a}}} D^{n-n'}$$

for some positive constant c_8, a contradiction to $T > cD_0, cD$. Thus $H = \{e\}$, and therefore $T_{\mathscr{H}} \cap \mathscr{W}_p$ must be trivial. One gets

$$\operatorname{codim}_{\mathscr{W}_p} \mathscr{W}_p \cap T_{\mathscr{H}} = \dim \mathscr{W}_p = n.$$

Moreover, $\varGamma(\gamma) \cap \mathscr{H}$ must also be trivial and hence

$$\operatorname{card}((\varGamma(\gamma) + \mathscr{H})/\mathscr{H}) = \operatorname{card} \varGamma(\eta) = S.$$

We obtain

$$\binom{T+n}{n} S \ll D_0^{1-n_{\mathrm{a}}} D^n \le D_0 D^n.$$

This shows that $T^n S \le c_9 D_0 D^n$ for some positive constant c_9, and again gives a contradiction because of the choice of the parameters. ■

In order to finish the proof of the theorem, we use the above lemma and the fact that $\log r_p^{-1} = \frac{\log p}{p-1} < 2$ to get

$$\begin{aligned} \log |l(u)|_p &> -c_{10}(S_0 T \log p + S_0 T \log S_0 + T e_L \log p) \\ &> -c_{11}(S_0^{n+2} b h^n \log p + S_0^{n+2} (\log S_0) b h^n) > -c_{12} S_0^{n+3} b h^n \log p \end{aligned}$$

for some positive constants c_{10}, c_{11} and c_{12}. In other words, there is a positive constant c_0 independent of b, h, p such that

$$\log |l(u)|_p > -c_0 \omega_L^{n+3} b h^n (\log b + \log h)^{n+3} \log p.$$

The first assertion of the theorem is thus proved; together with Section 2.2, this completes the proof.

Acknowledgements. The authors are grateful to Professor G. Wüstholz for insightful discussions and for constant encouragement to work on this topic. Moreover, the authors thank an anonymous referee for careful reading of the manuscript. The first author was supported by the Austrian Science Fund (FWF): P24574. The second author was supported by grant PDFMP2_122850 funded by the Swiss National Science Foundation (SNSF).

References

[1] A. Baker, *Linear forms in the logarithms of algebraic numbers I, II, III, IV*, Mathematika 13 (1966), 204–216; 14 (1967), 102–107; 14 (1967), 220–228; 15 (1968), 204–216.

[2] A. Baker and G. Wüstholz, *Logarithmic forms and group varieties*, J. Reine Angew. Math. 442 (1993), 19–62.

[3] A. Baker and G. Wüstholz, *Logarithmic Forms and Diophantine Geometry*, New Math. Monogr. 9, Cambridge Univ. Press, 2007.

[4] D. Bertrand and Y. Z. Flicker, *Linear forms on abelian varieties over local fields*, Acta Arith. 38 (1980/1981), 47–61.

[5] E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, New Math. Monogr. 4, Cambridge Univ. Press, 2006.

[6] E. Bombieri and J. Vaaler, *On Siegel's lemma*, Invent. Math. 73 (1983), 11–32.

[7] N. Bourbaki, *Elements of Mathematics. Lie Groups and Lie Algebras. Part I: Chapters 1–3*, Hermann, Paris, and Addison-Wesley, Reading, MA, 1975.

[8] J. Coates, *An effecitve p-adic analogue of a theorem of Thue*, Acta Arith. 15 (1969), 279–305.

[9] G. Faltings und G. Wüstholz, *Einbettungen kommutativer algebraischer Gruppen und einige ihrer Eigenschaften*, J. Reine Angew. Math. 354 (1984), 175–205.

[10] Y. Z. Flicker, *Transcendence theory over local fields*, PhD dissertation, Univ. of Cambridge, 1978.

[11] Y. Z. Flicker, *Linear forms on arithmetic Abelian varieties: ineffective bounds*, Mém. Soc. Math. France 1980, no. 2, 41–47.

[12] É. Gaudron, *Mesure d'indépendance linéaire de logarithmes dans un groupe algébrique commutatif*, C. R. Math. Acad. Sci. Paris 333 (2001), 1059–1064; Invent. Math. 162 (2005), 137–188.

[13] N. Hirata-Kohno, *Formes linéaires de logarithmes de points algébriques sur les groupes algébriques*, Invent. Math. 104 (1991), 401–433.

[14] N. Hirata-Kohno and R. Takada, *Linear forms in two elliptic logarithms in the p-adic case*, Kyushu J. Math. 64 (2010), 239–260.

[15] D. Masser and G. Wüstholz, *Zero estimate on group varieties II*, Invent. Math. 80 (1985), 233–267.

[16] D. H. Pham, *p-adic Nevanlinna theory*, MSc thesis, ETH Zürich, 2009.

[17] P. Philippon, *Lemmes de zéros dans les groupes algébriques commutatifs*, Bull. Soc. Math. France 114 (1986), 355–383; Errata et addenda, ibid. 115 (1987), 393–395.

[18] G. Rémond et F. Urfels, *Approximation diophantienne de logarithmes elliptiques p-adiques*, J. Number Theory 57 (1996), 133–169.

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

[20] C. L. Stewart and K. Yu, *On the abc conjecture I, II*, Math. Ann. 291 (1991), 225–230; Duke Math. J. 108 (2001), 169–181.

[21] G. Wüstholz, *Neue Methoden in der Theorie der transzendenten Zahlen*, Habilitationsschrift, Wuppertal, 1982.

[22] G. Wüstholz, *Multiplicity estimates and group varieties*, Ann. of Math. 129 (1989), 471–500.

[23] G. Wüstholz, *Algebraische Punkte auf Analytischen Untergruppen algebraischer Gruppen*, Ann. of Math. 129 (1989), 501–517.

[24] G. Wüstholz, *Computations on commutative group varieties*, in: Arithmetic Geometry (Cortona, 1994), Symposia Math. 37, F. Catanese (ed.), Cambridge Univ. Press, 1997, 279–300.

[25] F. Yan, *Tate property and isogeny estimate for semiabelian varieties*, Diss. Math. Wiss. ETH Zürich, 1994.

[26] K. Yu, *Linear forms in the p-adic logarithms I–III*, Acta Arith. 53 (1989), 107–186; Compos. Math. 74 (1990), 15–113; Compos. Math. 91 (1994), 241–276; Erratum to II, Compos. Math. 76 (1990), 307.

[27] K. Yu, *p-adic logarithmic forms and group varieties I–III*, J. Reine Angew. Math. 502 (1998), 29–92; Acta Arith. 89 (1999), 337–378; Forum Math. 19 (2007), 187–280.

[28] K. Yu, *Report on p-adic logarithmic forms*, in: A Panorama of Number Theory or the View from Baker's Garden, G. Wüstholz (ed.), Cambridge Univ. Press, 2002, 11–25.

[29] K. Yu, *p-adic logarithmic forms and a problem of Erdős*, Acta Math. 211 (2013), 315–382.

Clemens Fuchs
Department of Mathematics
University of Salzburg
Hellbrunnerstr. 34
5020 Salzburg, Austria
E-mail: clemens.fuchs@sbg.ac.at

Duc Hiep Pham
Department of Mathematics
Hanoi National University of Education
136 Xuan Thuy, Cau Giay
Hanoi, Vietnam
E-mail: phamduchiepk6@gmail.com

Received on 16.4.2014
and in revised form on 4.12.2014 (7776)