GLASNIK MATEMATIČKI
Vol. 51(71)(2016), 335 – 343

SOME APPLICATIONS OF THE p-ADIC ANALYTIC SUBGROUP THEOREM

Clemens Fuchs and Duc Hiep Pham
University of Salzburg, Austria and Vietnam National University, Vietnam

Abstract. We use a p-adic analogue of the analytic subgroup theorem of Wüstholz to deduce the transcendence and linear independence of some new classes of p-adic numbers. In particular we give p-adic analogues of results of Wüstholz contained in [20] and generalizations of results obtained by Bertrand in [3, 4].

1. Introduction

Transcendence theory is known as one of the fundamental questions in number theory. One of the first outstanding results in transcendence theory is Hermite's proof of the transcendence of e obtained in 1873. His work was extended by Lindemann afterwards in order to prove that e^{α} is transcendental for any non-zero algebraic number α. In particular, this showed that π is transcendental, and thus answered the problem of squaring the circle. There are many results further pushing the theory forward. Such important results are due to Gelfond, Schneider, Baker, Masser, Coates, Lang, Chudnovsky, Nesterenko, Waldschmidt, Wüstholz among others.

Especially, in the 1980's Wüstholz formulated and proved a very deep and far-reaching theorem, the so-called analytic subgroup theorem (see [21, 22] or [2]). It is known as one of the most striking theorems in the complex transcendental number theory with many applications. Wüstholz in 1983 used his analytic subgroup theorem to give a vast generalization of earlier

2010 *Mathematics Subject Classification.* 11G99,14L10, 11J86.

Key words and phrases. Commutative algebraic groups, transcendence theory, p-adic numbers.

The first author was supported by Austrian Science Fund (FWF): P24574. The second author was supported by grant PDFMP2_122850 funded by the Swiss National Science Foundation (SNSF).

results on linear independence in the complex domain (see [20]). To present the result, let k be a non-negative integer, $n_0, n_1, \ldots, n_k$ positive integers and $E_1, \ldots, E_k$ elliptic curves defined over $\overline{\mathbb{Q}}$. For each i with $1 \le i \le k$, denote by L_i the field of endomorphisms of E_i, $\wp_i$ the Weierstrass elliptic function associated with E_i and Λ_i the lattice of periods of $\wp_i$. Let $u_1, \ldots, u_{n_0}$ be non-zero elements in $\overline{\mathbb{Q}}$ and let $u_{i,1}, \ldots, u_{i,n_i}$ be elements in the set

$$\mathcal{E}_i := \{u \in \mathbb{C} \setminus \Lambda_i; \wp_i(u) \in \overline{\mathbb{Q}}\}, \quad i = 1, \ldots, k.$$

Finally, let V_0 be the vector space generated by the logarithms $\log u_1, \ldots,$ $\log u_{n_0}$ over $\mathbb{Q}$ and V_i the vector space generated by $u_{i,1}, \ldots, u_{i,n_i}$ over L_i for $i = 1, \ldots, k$. *If the elliptic curves $E_1, \ldots, E_k$ are pairwise non-isogeneous, then the dimension of the vector space V generated by $1, V_0, \ldots, V_k$ over $\overline{\mathbb{Q}}$ is determined by*

$$\dim_{\overline{\mathbb{Q}}} V = 1 + \dim_{\mathbb{Q}} V_0 + \dim_{L_1} V_1 + \cdots + \dim_{L_k} V_k.$$

It can be seen that Baker's theorem on linear forms of logarithms of algebraic numbers is the corresponding statement of the theorem without the elliptic curves $E_1, \ldots, E_k$.

Many of the results above have been transferred into the world of p-adic numbers as well. The theory of p-adic transcendence was studied by many authors following the line of arguments in the classical complex case. This development was initiated by Mahler in the 1930's (see [14,15]). He obtained the p-adic analogues of the Hermite, Lindemann and Gelfond-Schneider theorems. Afterwards several p-adic analogues of known results from the complex case were proved, and new theories of the p-adic transcendence were obtained. These contributions are due to Veldkamp (cf. [18]), Günther (cf. [12]), Brumer (cf. [7]), Adams (cf. [1]), Flicker (cf. [8,9]), Bertrand and others. Also a p-adic analogue of the Wüstholz' analytic subgroup theorem has been worked out (see [16] and the paper [11] by the authors which revisited that result and which is based on the results of [10]; observe that this statement has already been mentioned by Bertrand in [5]). Before we go on, we state the p-adic analogue of the analytic subgroup theorem of Wüstholz, since it will be the main tool for the results below. As usual, we denote by $\mathbb{C}_p$ the completion of $\overline{\mathbb{Q}_p}$ with respect to the p-adic absolute value. Let G be a commutative algebraic group defined over $\overline{\mathbb{Q}}$ and $\mathrm{Lie}(G)$ denote the Lie algebra of G. Then the set $G(\mathbb{C}_p)$ of $\mathbb{C}_p$-points of G is a Lie group over $\mathbb{C}_p$ whose Lie algebra is given by $\mathrm{Lie}(G(\mathbb{C}_p)) = \mathrm{Lie}(G) \otimes_{\overline{\mathbb{Q}}} \mathbb{C}_p$. It is known that there is the p-adic logarithm map

$$\log_{G(\mathbb{C}_p)} : G(\mathbb{C}_p)_f \to \mathrm{Lie}(G(\mathbb{C}_p)),$$

where $G(\mathbb{C}_p)_f$ is the set of $x \in G(\mathbb{C}_p)$ for which there exists a strictly increasing sequence (n_i) of integers such that x^{n_i} tends to the unity element of $G(\mathbb{C}_p)$ as i tends to ∞ (see [6, Chapter III, 7.6]). We denote by

$G_f(\overline{\mathbb{Q}}) := G(\mathbb{C}_p)_f \cap G(\overline{\mathbb{Q}})$ the set of algebraic points of G in $G(\mathbb{C}_p)_f$. The following statement is the p-adic analytic subgroup theorem:

THEOREM 1.1. *Let G be a commutative algebraic group of positive dimension defined over $\overline{\mathbb{Q}}$ and let $V \subseteq \mathrm{Lie}(G)$ be a non-trivial $\overline{\mathbb{Q}}$-linear subspace. For any $\gamma \in G_f(\overline{\mathbb{Q}})$ with $0 \neq \log_{G(\mathbb{C}_p)}(\gamma) \in V \otimes_{\overline{\mathbb{Q}}} \mathbb{C}_p$ there exists an algebraic subgroup $H \subseteq G$ of positive dimension defined over $\overline{\mathbb{Q}}$ such that $\mathrm{Lie}(H) \subseteq V$ and $\gamma \in H(\overline{\mathbb{Q}})$.*

In this paper we give some applications of the p-adic analytic subgroup theorem. It is known that in the complex domain many results on linear independence and transcendence are deduced from Wüstholz' analytic subgroup theorem. We shall show that it is also possible to obtain p-adic analogues of such results by using the p-adic analytic subgroup theorem. We will not give proofs of results which already appeared in the literature but instead concentrate on applications which do not exist in the literature so far.

2. RESULTS

We start by giving a p-adic analogue of the result of Wüstholz in [20] mentioned in the introduction. With the notations as above, but in the p-adic domain we let $\wp_{p,i}$ be the (Lutz-Weil) p-adic elliptic function associated with E_i (it is given by the same formal power series as the Weiterstrass $\wp$-function in the complex case, however the domain on which it is analytic depends on p), and $v_{i,1}, \ldots, v_{i,n_i}$ elements in the set

$$\mathcal{E}_{p,i} := \{0\} \cup \{u \in \mathscr{D}_{p,i} \setminus \{0\}; \wp_{p,i}(u) \in \overline{\mathbb{Q}}\},$$

where $\mathscr{D}_{p,i}$ is the p-adic domain of E_i for $i = 1, \ldots, k$ (see [19, 13]). We have the following result.

THEOREM 2.1. *Let V_0 be the vector space generated by the p-adic logarithms $\mathrm{Log}_p(u_1), \ldots, \mathrm{Log}_p(u_{n_0})$ over $\mathbb{Q}$, and V_i the vector space generated by $v_{i,1}, \ldots, v_{i,n_i}$ over L_i for $i = 1, \ldots, k$. If the elliptic curves $E_1, \ldots, E_k$ are pairwise non-isogeneous, then the dimension of the vector space V generated by $1, V_0, \ldots, V_k$ over $\overline{\mathbb{Q}}$ is determined by*

$$\dim_{\overline{\mathbb{Q}}} V = 1 + \dim_{\mathbb{Q}} V_0 + \dim_{L_1} V_1 + \cdots + \dim_{L_k} V_k.$$

Following [20] we turn to abelian varieties. Let A be an abelian variety defined over $\overline{\mathbb{Q}}$ and denote by $\mathfrak{a}$ the Lie algebra of A. It is well-known that $A(\mathbb{C}_p)$ has naturally the structure of a Lie group over $\mathbb{C}_p$. By [6, Chapter III, 7.2, Prop. 3], there is an open subgroup $\mathcal{A}_p$ of $\mathrm{Lie}(A(\mathbb{C}_p)) = \mathfrak{a} \otimes_{\overline{\mathbb{Q}}} \mathbb{C}_p$ on which the p-adic exponential map $\exp_{A(\mathbb{C}_p)}$ is defined and

$$\exp_{A(\mathbb{C}_p)} : \mathcal{A}_p \to \exp_{A(\mathbb{C}_p)}(\mathcal{A}_p) \subset A(\mathbb{C}_p)$$

is an isomorphism. Its inverse is the restriction of the p-adic logarithmic map to $\exp_{A(\mathbb{C}_p)}(\mathcal{A}_p)$. We denote by $\mathcal{A}_{\overline{\mathbb{Q}}}$ the set

$$\{\alpha \in \mathcal{A}_p; \exp_{A(\mathbb{C}_p)}(\alpha) \in A(\overline{\mathbb{Q}})\}.$$

Let R be a ring operating on $\mathfrak{a}$. We say that elements $u_1, \dots, u_m$ in $\mathfrak{a}$ are linearly independent over R if whenever we have a relation $r_1u_1 + \cdots + r_mu_m = 0$ with $r_1, \dots, r_m$ in R, then it implies that $r_1 = \cdots = r_m = 0$. Finally, let $\mathrm{End}(A)$ denote the ring of endomorphisms of A and $\mathrm{End}(\mathfrak{a})$ the ring of endomorphisms of $\mathfrak{a}$ (defined over $\overline{\mathbb{Q}}$). We prove the following theorem which again is the p-adic analogue of a result of Wüstholz in [20].

Theorem 2.2. *Assume that A is a simple abelian variety. Let m be a positive integer, and $u_1, \dots, u_m$ elements of $\mathcal{A}_{\overline{\mathbb{Q}}}$ such that they are linearly independent over* $\mathrm{End}(A)$. *Then $u_1, \dots, u_m$ are linearly independent over* $\mathrm{End}(\mathfrak{a})$.

We now generalize a result of Bertrand from p-adic transcendence. To describe the results below, as usual, we identify the Lie algebra $\mathfrak{a}$ with the vector space $\overline{\mathbb{Q}}^n$, here $n := \dim A$. Under this identification it follows that $\mathcal{A}_{\overline{\mathbb{Q}}}$ is a subset of

$$\mathrm{Lie}(A(\mathbb{C}_p)) = \mathfrak{a} \otimes_{\overline{\mathbb{Q}}} \mathbb{C}_p = \overline{\mathbb{Q}}^n \otimes_{\overline{\mathbb{Q}}} \mathbb{C}_p = \mathbb{C}_p^n.$$

We say that A is an abelian variety of RM type (or with real multiplication) if there are a totally real number field F of degree n and an embedding $F \hookrightarrow \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ (hence an abelian variety of CM type is also of RM type). The following result was given by Bertrand in 1979 (see [4]): *If A is a simple abelian variety of RM type defined over $\overline{\mathbb{Q}}$, then all coordinates of u are transcendental for any non-zero element u in $\mathcal{A}_{\overline{\mathbb{Q}}}$.* We shall use the p-adic analytic subgroup theorem to give a generalization of this theorem for general simple abelian varieties. That is, we prove the following result.

Theorem 2.3. *If A is a simple abelian variety of positive dimension defined over $\overline{\mathbb{Q}}$, then all coordinates of u are transcendental for any non-zero element u in $\mathcal{A}_{\overline{\mathbb{Q}}}$.*

It is known that there are homomorphisms from the additive group $\mathbb{C}_p$ to the multiplicative group $\mathbb{C}_p^*$ extending the p-adic exponential function (see [17, Chapter 5, 4.4]). Let φ_p be such a homomorphism. We get the following result which can be seen as a generalization of [3, Corollary 2].

Theorem 2.4. *If A is a simple abelian variety defined over $\overline{\mathbb{Q}}$ of dimension $n > 0$, then the elements $\varphi_p(\alpha u_1), \dots, \varphi_p(\alpha u_n)$ are transcendental for any non-zero element $u = (u_1, \dots, u_n)$ in $\mathcal{A}_{\overline{\mathbb{Q}}}$ and for any non-zero element $\alpha \in \overline{\mathbb{Q}}$.*

In the next section we give the proofs of the statements as consequence of the p-adic analytic subgroup theorem.

3. Proofs

3.1. *Proof of Theorem 2.1.* The proof is very similar to the one given in [20]. First of all, one may assume without loss of generality that $n_0 = \dim_{\mathbb{Q}} V_0$ and $n_i = \dim_{L_i} V_i$ for $0 \leq i \leq k$. Let r_i be the p-adic valuation of u_i, and define $v_i := p^{-r_i} u_i$ for $i = 1, \ldots, n_0$. Then v_i are algebraic numbers in $\mathbb{U}(1) := \{x \in \mathbb{C}_p; |x|_p = 1\}$ and

$$\mathrm{Log}_p(v_i) = \mathrm{Log}_p(u_i), \quad \forall i = 1, \ldots, n_0.$$

We therefore have to show that the elements

$$1, \mathrm{Log}_p(v_1), \ldots, \mathrm{Log}_p(v_{n_0}), u_{1,1}, \ldots, u_{1,n_1}, \ldots, u_{k,1}, \ldots, u_{k,n_k}$$

are linearly independent over $\overline{\mathbb{Q}}$. In fact, assume on the contrary that they are not linearly independent over $\overline{\mathbb{Q}}$. This means that there exists a non-zero linear form l in $n := 1 + n_0 + \cdots + n_k$ variables with coefficients in $\overline{\mathbb{Q}}$ such that

$$l(1, \mathrm{Log}_p(v_1), \ldots, \mathrm{Log}_p(v_{n_0}), u_{1,1}, \ldots, u_{1,n_1}, \ldots, u_{k,1}, \ldots, u_{k,n_k}) = 0.$$

Let V be the $\overline{\mathbb{Q}}$-vector space defined by

$$V := \{v \in \overline{\mathbb{Q}}^n; l(v) = 0\},$$

and consider the commutative algebraic group G given by

$$G = \mathbb{G}_a \times \mathbb{G}_m^{n_0} \times E_1^{n_1} \times \cdots \times E_k^{n_k}.$$

Then G is defined over $\overline{\mathbb{Q}}$ and the Lie algebra

$$\mathrm{Lie}(G) = \mathrm{Lie}(\mathbb{G}_a) \times \mathrm{Lie}(\mathbb{G}_m)^{n_0} \times \mathrm{Lie}(E_1)^{n_1} \times \cdots \times \mathrm{Lie}(E_k)^{n_k}$$

which is identified with $\overline{\mathbb{Q}}^{1+n_0+\cdots+n_k} = \overline{\mathbb{Q}}^n$. This shows that

$$\mathrm{Lie}(G(\mathbb{C}_p)) = \mathrm{Lie}(G) \otimes_{\overline{\mathbb{Q}}} \mathbb{C}_p = \mathbb{C}_p^n.$$

We write abbreviately $\exp_i$ and $\log_i$ for the p-adic exponential and logarithm map associated with E_i respectively for each $i = 1, \ldots, n$. One has

$$G(\mathbb{C}_p)_f = \mathbb{C}_p \times \mathbb{U}(1)^{n_0} \times (E_1(\mathbb{C}_p))^{n_1} \times (E_k(\mathbb{C}_p))^{n_k}$$

and the p-adic logarithm map $\log_{G(\mathbb{C}_p)} : G(\mathbb{C}_p)_f \to \mathbb{C}_p^n$ is determined by

$$(\mathrm{id}_{\mathbb{C}_p}, (\mathrm{Log}_p)^{n_0}, \log_1^{n_1}, \ldots, \log_k^{n_k}).$$

Let $\gamma \in G(\mathbb{C}_p)_f$ be the algebraic point given by

$$\big(1, v_1, \ldots, v_{n_0}, \exp_1(u_{1,1}), \ldots, \exp_1(u_{1,n_1}), \ldots, \exp_k(u_{k,1}), \ldots, \exp_k(u_{k,n_k})\big).$$

One gets

$$\log_{G(\mathbb{C}_p)}(\gamma) = (1, \mathrm{Log}_p(v_1), \ldots, \mathrm{Log}_p(v_{n_0}), u_{1,1}, \ldots, u_{1,n_1}, \ldots, u_{k,1}, \ldots, u_{k,n_k})$$

which is a non-zero element in $V \otimes_{\overline{\mathbb{Q}}} \mathbb{C}_p$. We apply the p-adic analytic subgroup theorem to G, V and γ to obtain an algebraic subgroup H of G of positive dimension defined over $\overline{\mathbb{Q}}$ such that γ is in $H(\overline{\mathbb{Q}})$ and $\mathrm{Lie}(H)$ is contained in V. Let H^0 be the connected component of H then

$$H^0 = H_{-1} \times H_0 \times \cdots \times H_k,$$

where H_{-1} is an algebraic subgroup of $\mathbb{G}_a$, H_0 is an algebraic subgroup of $\mathbb{G}_m$ and H_i is an algebraic subgroup of $E_i^{n_i}$ for $1 \leq i \leq k$. We have

$$\dim H^0 = \dim H = \dim_{\overline{\mathbb{Q}}} \mathrm{Lie}(H) \leq \dim_{\overline{\mathbb{Q}}} V = n - 1.$$

Since $\gamma \in H$ and the first coordinate of γ is 1 it follows that $H_{-1} = \mathbb{G}_a$. This means that at least one of the algebraic groups $H_0, \dots, H_k$ is contained in the corresponding factor with positive codimension. If this happens for the algebraic group H_0, i.e. H_0 is a proper algebraic subgroup of $\mathbb{G}_m$, then the Lie algebra of H_0 is defined by non-zero linear forms with integer coefficients. This means that the elements $\mathrm{Log}_p(v_1), \dots, \mathrm{Log}_p(v_{n_0})$ are linearly dependent over $\mathbb{Q}$ since $(v_1, \dots, v_{n_0}) \in H_0$, i.e. $\dim_{\mathbb{Q}} V_0 < n_0$, a contradiction. Hence there must be at least one $i \in \{1, \dots, k\}$ such that

$$\dim H_i \leq \dim(E_i^{n_i}) - 1 = n_i - 1.$$

Using the same arguments as in the proof of [2, Theorem 6.2], we conclude that the elements $u_{i,1}, \dots, u_{i,n_i}$ are linearly dependent over L_i. This is, $\dim_{L_i} V_i < n_i$, a contradiction, and the theorem follows. □

3.2. *Proof of Theorem 2.2.* Suppose that there are elements $r_1, \dots, r_m$ not all zero in $\mathrm{End}(\mathfrak{a})$ such that

$$r_1 u_1 + \cdots + r_m u_m = 0.$$

Let V be the vector space defined by

$$V := \{v = (v_1, \dots, v_m) \in \mathfrak{a}^n; r_1 v_1 + \cdots + r_m v_m = 0\}.$$

Then V is a $\overline{\mathbb{Q}}$-linear subspace of $\mathfrak{a}^m$. We consider the abelian variety $G := A^m$ and the element $\gamma := (\exp_{A(\mathbb{C}_p)}(u_1), \dots, \exp_{A(\mathbb{C}_p)}(u_m))$. Then γ is an algebraic point of

$$G(\mathbb{C}_p)_f = A(\mathbb{C}_p)_f^m = A(\mathbb{C}_p)^m,$$

and $\log_{A(\mathbb{C}_p)}(\gamma) = (u_1, \dots, u_m)$ is a non-zero element in $V \otimes_{\overline{\mathbb{Q}}} \mathbb{C}_p$. The p-adic analytic subgroup theorem then shows that there exists an algebraic subgroup H of G of positive dimension defined over $\overline{\mathbb{Q}}$ such that $\gamma \in H(\overline{\mathbb{Q}})$ and $\mathrm{Lie}(H)$ is a subspace of V. Since A is simple, H is isogeneous to A^k for a certain integer $k < m$. One can therefore define a projection π from G onto H. We get the corresponding tangent map $d\pi : \mathrm{Lie}(G) \to \mathrm{Lie}(H)$. Since $\gamma \in H(\overline{Q})$ it follows that the point $(u_1, \dots, u_m) = \log_{A(\mathbb{C}_p)}(\gamma) = \log_{H(\mathbb{C}_p)}(\gamma)$ belongs to $\mathrm{Lie}(H)$. On the other hand, we may identify $\mathrm{Lie}(G)$ and $\mathrm{Lie}(H)$ with $\mathfrak{a}^m$ and $\mathfrak{a}^k$, respectively. Then the point $(u_1, \dots, u_m)$ is in the kernel of the linear map $\mathrm{id}_{\mathrm{Lie}(G)} - d\pi$ which can be written as an $m \times m$ matrix with entries in $\mathrm{End}(A)$ (since the algebra of endomorphisms $\mathrm{End}(G)$ of G is represented on the Lie(G) by the matrix algebra $M_m(\mathrm{End}(A))$). In other words, the image of $(u_1,\dots,u_m)$ under this matrix is zero. Note that this matrix is non-zero (since $k<m$), hence there is at least one column which is non-zero. We have thus shown that there is a non-trivial dependence relation over $\mathrm{End}(A)$ among the elements $u_1,\dots,u_m$, or equivalently, $u_1,\dots,u_m$ are linearly dependent over $\mathrm{End}(A)$. This contradiction proves the theorem. □

3.3. *Proof of Theorem 2.3.* Denote by n the dimension of A. Suppose on the contrary that there is a non-zero element $u=(u_1,\dots,u_n)\in\mathcal{A}_{\overline{\mathbb{Q}}}$ with u_i algebraic over $\overline{\mathbb{Q}}$ for some $i\in\{1,\dots,n\}$. Let $G=\mathbb{G}_a\times A$ be the direct product of the additive group $\mathbb{G}_a$ with A. Then G is commutative and defined over $\overline{\mathbb{Q}}$ with

$$\mathrm{Lie}(G)=\mathrm{Lie}(\mathbb{G}_a)\times\mathrm{Lie}(A)=\overline{\mathbb{Q}}^{n+1}.$$

This gives

$$\mathrm{Lie}(G(\mathbb{C}_p))=\mathrm{Lie}(G)\otimes_{\overline{\mathbb{Q}}}\mathbb{C}_p=\mathbb{C}_p^{n+1}.$$

We have $G(\mathbb{C}_p)_f=\mathbb{C}_p\times A(\mathbb{C}_p)$ and the p-adic logarithm map $\log_{G(\mathbb{C}_p)}$ is $\mathrm{id}_{\mathbb{C}_p}\times\log_{A(\mathbb{C}_p)}$. Let V be the $\overline{\mathbb{Q}}$-vector space defined by

$$\{(v_0,\dots,v_n)\in\overline{\mathbb{Q}}^{n+1};v_0-v_i=0\}$$

and γ the algebraic point $(u_i,\exp_{A(\mathbb{C}_p)}(u))$. We observe that γ is non-zero since u is non-zero, and furthermore we have

$$\log_{G(\mathbb{C}_p)}(\gamma)=\Big(\mathrm{id}_{\mathbb{C}_p}(u_i),\log_{A(\mathbb{C}_p)}\left(\exp_{A(\mathbb{C}_p)}(u)\right)\Big)=(u_i,u_1,\dots,u_n)$$

is an element in $V\otimes_{\overline{\mathbb{Q}}}\mathbb{C}_p$. Applying the p-adic analytic subgroup theorem, we obtain an algebraic subgroup H of G of positive dimension defined over $\overline{\mathbb{Q}}$ such that $\gamma\in H(\overline{\mathbb{Q}})$ and $\mathrm{Lie}(H)\subseteq V$. Note that V is proper in $\mathrm{Lie}(G)$, and this shows that H is proper in G. Since the abelian variety A is simple, H must be either of the form $\mathbb{G}_a\times\{e\}$ or $\{0\}\times A$ where e is the identity element of A. If $H=\mathbb{G}_a\times\{e\}$ then $\exp_{A(\mathbb{C}_p)}(u)=e$, i.e. $u=0$, a contradiction. If $H=\{0\}\times A$ then the Lie algebra $\mathrm{Lie}(H)=\{0\}\times\overline{\mathbb{Q}}^n$. This contradicts with the condition $\mathrm{Lie}(H)\subseteq V$, and the theorem is proved. □

3.4. *Proof of Theorem 2.4.* Assume on the contrary that there exists $i\in\{1,\dots,n\}$ such that $\varphi_p(\alpha u_i)\in\overline{\mathbb{Q}}$. There is a sufficiently large positive integer r such that $w:=p^r\alpha u_i\in B(r_p)$, where $B(r_p)$ denotes the ball $\{x\in\mathbb{C}_p;|x|_p<r_p\}$ with $r_p:=p^{-1/(p-1)}$. Hence

$$e_p(w):=\sum_{k\geq 1}\frac{w^k}{k!}=\varphi_p(w)=\varphi_p(p^r\alpha u_i)=\varphi_p(\alpha u_i)^{p^r}$$

is also in $\overline{\mathbb{Q}}$. Let $G = \mathbb{G}_m \times A$ be the direct product of the multiplicative group $\mathbb{G}_m$ with A. Then G is commutative and defined over $\overline{\mathbb{Q}}$ with

$$\mathrm{Lie}(G) = \mathrm{Lie}(\mathbb{G}_m) \times \mathrm{Lie}(A) = \overline{\mathbb{Q}}^{n+1}.$$

This implies that

$$\mathrm{Lie}(G(\mathbb{C}_p)) = \mathrm{Lie}(G) \otimes_{\overline{\mathbb{Q}}} \mathbb{C}_p = \mathbb{C}_p^{n+1}.$$

We have

$$G(\mathbb{C}_p)_f = \mathbb{G}_m(\mathbb{C}_p)_f \times A(\mathbb{C}_p)_f = \mathbb{U}(1) \times A(\mathbb{C}_p),$$

and the p-adic logarithm map $\log_{G(\mathbb{C}_p)}$ is the product $\mathrm{Log}_p \times \log_{A(\mathbb{C}_p)}$. Let V be the $\overline{\mathbb{Q}}$-vector space defined by

$$\{(v_0, \ldots, v_n) \in \overline{\mathbb{Q}}^{n+1}; v_0 - p^r \alpha v_i = 0\}$$

and γ the algebraic point $(e_p(w), \exp_{A(\mathbb{C}_p)}(u))$. We see that γ is non-zero since u is non-zero, and furthermore

$$\log_{G(\mathbb{C}_p)}(\gamma) = \Big(\log_p\left(e_p(w)\right), \log_{A(\mathbb{C}_p)}\left(\exp_{A(\mathbb{C}_p)}(u)\right)\Big) = (p^r \alpha u_i, u_1, \ldots, u_n)$$

is a non-zero element in $V \otimes_{\overline{\mathbb{Q}}} \mathbb{C}_p$. Using the p-adic analytic subgroup theorem, we obtain an algebraic subgroup H of G of positive dimension defined over $\overline{\mathbb{Q}}$ such that $\gamma \in H(\overline{\mathbb{Q}})$ and $\mathrm{Lie}(H) \subseteq V$. Note that V is proper in $\mathrm{Lie}(G)$, and this shows that H is proper in G. Since the abelian variety A is simple, H must be either of the form $\mathbb{G}_m \times \{e\}$ or $\{1\} \times A$ where e is the identity element of A. If $H = \mathbb{G}_m \times \{e\}$ then $\exp_{A(\mathbb{C}_p)}(u) = e$, i.e. $u = 0$, a contradiction. If $H = \{1\} \times A$ then the Lie algebra $\mathrm{Lie}(H) = \{0\} \times \overline{\mathbb{Q}}^n$. This contradicts with the condition $\mathrm{Lie}(H) \subseteq V$, and the theorem is proved. □

References

[1] W. Adams, *Transcendental numbers in the p-adic domain*, Amer. J. Math. **88** (1966), 279–308.

[2] A. Baker and G. Wüstholz, Logarithmic forms and Diophantine geometry, Cambridge University Press, Cambridge, 2007.

[3] D. Bertrand, *Sous-groupes à un paramètre p-adique de variétés de groupe*, Invent. Math. **40** (1977), 171–193.

[4] D. Bertrand, *Problèmes locaux*, Astérisque **69-70** (1979), 163–189.

[5] D. Bertrand, *Lemmes de zèros et nombres transcendants*, Séminaire Bourbaki Vol. 1985/86, Astérisque **145-146** (1987), 21–44.

[6] N. Bourbaki, Elements of Mathematics. Lie groups and Lie algebras. Part I: Chapters 1-3. English translantion., Actualities scientifiques et industrielles, Herman. Adiwes International Series in Mathematics. Paris: Hermann, Publishers in Arts and Science; Reading, Mass.: Addison-Wesley Publishing Company. XVII, 1975.

[7] A. Brumer, *On the units of algebraic numbers fields*, Mathematika **14** (1967), 121–124.

[8] Y. Z. Flicker, Transcendence theory over local fields, PhD dissertation, University of Cambridge, 1978.

[9] Y. Z. Flicker, *Linear forms on arithmetic Abelian varieties: ineffective bounds*, Mém. Soc. Math. France (N.S.) (1980/81), 41–47.

[10] C. Fuchs and D. H. Pham, *Commutative algebraic groups and p-adic linear forms*, Acta Arith. **169** (2015), 115–147.

[11] C. Fuchs and D. H. Pham, *The p-adic analytic subgroup theorem revisited*, p-Adic Numbers, Ultrametric Anal. Appl. **7** (2015), 143–156.

[12] A. Günther, *Über transzendente $\mathfrak{p}$-adische Zahlen. I*, J. Reine Angew. Math. **192** (1953), 155–166.

[13] E. Lutz, *Sur l'équation $Y^2 = AX^3 - AX - B$ dans les corps p-adiques*, J. Reine Angew. Math. **177** (1937), 238–247.

[14] K. Mahler, *Ein Beweis der Transzendenz der P-adischen Exponentialfunktion*, J. Reine Angew. Math. **169** (1933), 61–66.

[15] K. Mahler, *Über transzendente P-adische Zahlen*, Compositio Math. **2** (1935), 259–275.

[16] T. Matev, *The p-adic analytic subgroup theorem and applications*, http://arxiv.org/pdf/1010.3156v1.pdf.

[17] A. M. Robert, A course in p-adic analysis, GTM **198**, Springer-Verlag, 2000.

[18] G. Veldkamp, *Ein Transzendenz-Satz für p-adische Zahlen*, J. London Math. Soc. **15** (1940), 183–192.

[19] A. Weil, *Sur les fonctions elliptiques $\mathfrak{p}$-adiques*, C. R. Acad. Sc. Paris **203** (1936), 22–24.

[20] G. Wüstholz, *Some remarks on a conjecture of Waldschmidt*, in: Diophantine approximations and transcendental numbers, Birkhäuser Boston, Boston, MA, 1983, 329–336.

[21] G. Wüstholz, *Algebraische Punkte auf Analytischen Untergruppen algebraischer Gruppen*, Ann. of Math. (2) **129** (1989), 501–517.

[22] G. Wüstholz, *Multiplicity estimates on group varieties*, Ann. of Math. (2) **129** (1989), 471–500.

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

D. H. Pham
University of Education
Vietnam National University, Hanoi
144 Xuan Thuy, Cau Giay, Hanoi
Vietnam
E-mail: phamduchiepk6@gmail.com

Received: 3.12.2014.
Revised: 15.9.2015. & 24.10.2015.