On the p-adic closure of a subgroup of rational points on an Abelian variety

Michel Waldschmidt

Afrika Matematika, to appear *December 21, 2010*

On the p-adic closure of a subgroup of rational points on an Abelian variety

by

Michel Waldschmidt[1]

Abstract

In 2007, B. Poonen (unpublished) studied the p–adic closure of a subgroup of rational points on a commutative algebraic group. More recently, J. Bellaïche asked the same question for the special case of Abelian varieties. These problems are p–adic analogues of a question raised earlier by B. Mazur on the density of rational points for the real topology. For a simple Abelian variety over the field of rational numbers, we show that the actual p–adic rank is at least the third of the expected value.

Acknowledgments The author wishes to take this opportunity to thank Jean Fresnel, who introduced him to p-adic transcendence problems long back. This research started thanks to a discussion with Bjorn Poonen in Tucson during the Arizona Winter School in March 2008. Further discussions on this subject with Cristiana Bertolin in Regensburg shortly afterwards were also useful. The motivation to write this paper was renewed by a correspondence with Joël Bellaïche early 2010 [3], while the author was visiting the Harish-Chandra Research Institute in Allahabad, where he had fruitful discussions with Chandan Singh Dalawat.

1 Introduction

Let A be a simple Abelian variety over $\mathbb{Q}$ of dimension g, Γ a subgroup of $A(\mathbb{Q})$ of rank ℓ over $\mathbb{Z}$, p a prime number, $\log : A(\mathbb{Q}_p) \to T_A(\mathbb{Q}_p)$ the canonical map from the p–adic Lie group $A(\mathbb{Q}_p)$ to the p–adic Lie algebra $T_A(\mathbb{Q}_p)$ (see § 2.1) and r the dimension of the $\mathbb{Z}_p$–space spanned by $\log\Gamma$ in $T_A(\mathbb{Q}_p)$. We have $r \le \min\{g, \ell\}$.

Conjecture 1. *Under these hypotheses,* $r = \min\{g, \ell\}$.

This conjecture trivially holds for an elliptic curve ($g = 1$).

The real analog of this conjecture is related with a conjecture of B. Mazur [13]. See also the conjectures by Yves André [1, 2].

[1]Université Pierre et Marie Curie (Paris 6), Paris, France

Theorem 2. *We have*

$$r \geq \frac{\ell g}{\ell + 2g}\cdot$$

Corollary 3. *Under the same assumptions,*

$$r \geq \frac{1}{3}\min\{g, \ell\}.$$

Moreover, if $\ell > 2g(g-1)$, then $r = g$.

Theorem 2 is a special case of Theorem 2.1 of [20], where the simple Abelian variety A over $\mathbb{Q}$ is replaced by a commutative algebraic group G over a number field. Our special case enables us to produce a much simpler proof. In particular, the zero estimate is much easier here, since there is no algebraic subgroup of G to be taken care of. Also, the main difference between our proof and the two proofs in [20] is that we use an interpolation determinant in place of an auxiliary function (Proposition 2.7 of [20]) or in place of an auxiliary functional (Proposition 2.10 of [20]): we do not need the p–adic Siegel Lemma (Lemma 3.3 of [19]). The two proofs in [20] are dual to each other, and this duality is just a transposition of the interpolation determinant of the present paper.

2 Further notations and auxiliary results

We keep the notations of § 1. We select ℓ elements $\gamma_1, \dots, \gamma_\ell$ in Γ linearly independent over $\mathbb{Z}$.

For T a positive integer, we denote by $\mathbb{Z}^g(T)$ the set of tuples $\underline{t} = (t_1, \dots, t_g)$ in $\mathbb{Z}^g$ with $0 \leq t_i < T$ $(1 \leq i \leq g)$. Similary, for $S \in \mathbb{Z}_{>0}$, $\mathbb{Z}^\ell(S)$ denotes the set of tuples $\underline{s} = (s_1, \dots, s_\ell)$ in $\mathbb{Z}^\ell$ with $0 \leq s_j < S$ $(1 \leq j \leq \ell)$. Further, $\Gamma(S)$ will denote the set of $s_1\gamma_1 + \cdots + s_\ell\gamma_\ell$ with $\underline{s} \in \mathbb{Z}^\ell(S)$. Hence $\Gamma(S)$ is a subset of $A(K)$ with S^ℓ elements.

2.1 The p–adic logarithm

We follow the paper by B. Poonen [14] which refers to N. Bourbaki [6] Chap. III, § 1 and § 7.6.

Since Γ is a finitely abelian subgroup of $A(\mathbb{Q}_p)$ of rank ℓ, $\log\Gamma$ is also a finitely generated abelian subgroup of $T_A(\mathbb{Q}_p)$ of the same rank ℓ over $\mathbb{Z}$. The closure $\overline{\log\Gamma} = \log\overline{\Gamma}$ with respect to the p-adic topology is nothing else than the $\mathbb{Z}_p$–submodule of $T_A(\mathbb{Q}_p)$ spanned by $\log\Gamma$, hence is a finitely generated $\mathbb{Z}_p$–module. The dimension of $\overline{\Gamma}$ as a Lie group over $\mathbb{Q}_p$ is

$$\dim\overline{\Gamma} := \mathrm{rk}_{\mathbb{Z}_p}\overline{\log\Gamma}.$$

2.2 Heights

2.2.1 A projective embedding

We fix an embedding ι of the Abelian variety A into a projective space $\mathbb{P}_N$ over $\mathbb{Q}$, with an image which is not contained into the hyperplane $X_0 = 0$, and so that the functions $X_1/X_0, \dots, X_g/X_0$ are algebraically independent over A (recall that A has dimension g). We also assume that for $\underline{s} \in \mathbb{Z}^\ell$, $\iota(\gamma_{\underline{s}})$ does not lie in the hyperplane $X_0 = 0$ and we denote by $(1 : \gamma_{\underline{s}1} : \cdots : \gamma_{\underline{s}N})$ the coordinates of $\iota(\gamma_{\underline{s}})$ in $\mathbb{P}_N$, so that $\gamma_{\underline{s}\nu} \in \mathbb{Q}$ for $1 \le \nu \le N$ and $\underline{s} \in \mathbb{Z}^\ell$. For convenience, we also assume that the zero element of A has projective coordinates $(1 : 0 : \cdots : 0)$.

2.2.2 Absolute logarithmic height

Denote by $P = \{2, 3, 5, \dots\}$ the set of positive prime numbers and by $M_\mathbb{Q}$ the set of normalized places of $\mathbb{Q}$ indexed by $P \cup \{\infty\}$: for $c \in \mathbb{Q}^\times$ we write

$$c = \pm \prod_{p \in P} p^{v_p(c)}$$

and we have

$$\begin{cases} |c|_v = |c| = \max\{c, -c\} & \text{for } v = v_\infty \\ |c|_p = p^{-v_p(c)} & \text{for } p \in P. \end{cases}$$

The *product formula*, in this very simple case, states that, for $c \in \mathbb{Q} \setminus \{0\}$,

$$\prod_{v \in M_\mathbb{Q}} |c|_v = 1.$$

The absolute logarithmic height of $c \in \mathbb{Q}$ is defined as

$$\mathrm{h}(c) = \sum_{v \in M_\mathbb{Q}} \log \max\{1,\ |c|_v\}.$$

For $c \in \mathbb{Q}^\times$, we write $c = a/b$ where $a \in \mathbb{Z} \setminus \{0\}$ and $b \in \mathbb{Z}_{>0}$ are two relatively prime integers. Since $\min\{v_p(a),\ v_p(b)\} = 0$ for all $p \in P$, we have, for all $p \in P$,

$$\max\{|a|_p, |b|_p\} = 1, \quad \text{which means} \quad \max\{1, |c|_p\} = |b|_p^{-1}.$$

Hence, by the product formula,

$$\prod_{p \in P} \max\{1, |c|_p\} = b.$$

Multiplying both sides by $\max\{1, |c|\}$ yields

$$\mathrm{h}(c) = \log \max\{|a|, b\},$$

which can be taken as an alternative definition for the absolute logarithmic height.

Liouville's inequality is very simple in this context:

Lemma 4. *If c is a non–zero rational number and p a prime number, then*

$$\log |c|_p \ge -\mathrm{h}(c).$$

For $N \geq 1$ and $\underline{c} = (c_0 : \cdots : c_N) \in \mathbb{P}_N(\mathbb{Q})$, we set

$$\mathrm{h}(\underline{c}) = \sum_{v \in M_{\mathbb{Q}}} \log \max\{|c_0|_v,\ \ldots,\ |c_N|_v\}.$$

If $c_0, \ldots, c_N$ are rational integers, not all of which are zero, which are relatively prime, then

$$\mathrm{h}(\underline{c}) = \log \max\{|c_0|,\ \ldots,\ |c_N|\}.$$

Notice that for $c \in \mathbb{Q}$, $\mathrm{h}(c) = \mathrm{h}(1 : c)$.

2.2.3 Néron–Tate height

The projective embedding considered in § 2.2.1 is associated with a very ample line bundle on A, to which is associated a canonical height which is a quadratic function (see [18] Chap. 3 and [9] § B.5).

Lemma 5. *For $\underline{s} \in \mathbb{Z}^\ell(S)$,*

$$\mathrm{h}(s_1\gamma_1 + \cdots + s_\ell\gamma_\ell) = \mathrm{h}(1 : \gamma_{\underline{s}1} : \cdots : \gamma_{\underline{s}N}) \leq cS^2.$$

2.2.4 Upper bound for the height

We shall use the following result, which is a very simple case of Lemma 3.8. in [26] (where $\mathbb{Q}$ is replaced by a number field). We denote by $\mathrm{L}(f)$ the length of a polynomial f (sum of the absolute values of the coefficients).

Lemma 6. *Let $\nu_1, \ldots, \nu_L$ be positive integers. For $1 \leq i \leq L$, let $\gamma_{i1}, \ldots, \gamma_{i\nu_i}$ be rational numbers. Denote by $\underline{\gamma}$ the point $\bigl(\gamma_{ij}\bigr)_{1 \leq j \leq \nu_i, 1 \leq i \leq L}$ in $\mathbb{Q}^{\nu_1 + \cdots + \nu_L}$. Further, let f be a nonzero polynomial in $\nu_1 + \cdots + \nu_L$ variables, with coefficients in $\mathbb{Z}$, of total degree at most N_i with respect to the ν_i variables corresponding to $\gamma_{i1}, \ldots, \gamma_{i\nu_i}$. Then*

$$\mathrm{h}\bigl(f(\underline{\gamma})\bigr) \leq \log \mathrm{L}(f) + \sum_{i=1}^{L} N_i \mathrm{h}(1 \colon \gamma_{i1} \colon\ \cdots : \gamma_{i\nu_i}).$$

Proof. Let us write

$$f(\underline{X}) = \sum_{\underline{\lambda}} c_{\underline{\lambda}} \prod_{i=1}^{L} \prod_{j=1}^{\nu_i} X_{ij}^{\lambda_{ij}},$$

where $\underline{X}$ (resp. $\underline{\lambda}$) stands for the $\nu_1 + \cdots + \nu_L$ –tuple $(X_{ij})_{1 \leq j \leq \nu_i,\ 1 \leq i \leq L}$ (resp. $(\lambda_{ij})_{1 \leq j \leq \nu_i,\ 1 \leq i \leq L}$. Lemma 6 follows from the estimates

$$\begin{aligned} |f(\underline{\gamma})| &\leq \sum_{\underline{\lambda}} |c_{\underline{\lambda}}| \prod_{i=1}^{L} \prod_{j=1}^{\nu_i} \max\{1,\ |\gamma_{ij}|\}^{\lambda_{ij}} \\ &\leq \mathrm{L}(f) \prod_{i=1}^{L} \max\{1,\ |\gamma_{i1}|,\ \ldots,\ |\gamma_{i\nu_i}|\}^{N_i} \end{aligned}$$

and

$$\begin{aligned}|f(\underline{\gamma})|_p &\le \max_{\underline{\lambda}} \prod_{i=1}^{L} \prod_{j=1}^{\nu_i} \max\{1,\ |\gamma_{ij}|_p\}^{\lambda_{ij}} \\ &\le \prod_{i=1}^{L} \max\{1,\ |\gamma_{i1}|_p,\ \ldots,\ |\gamma_{i\nu_i}|_p\}^{N_i}\end{aligned}$$

for $p \in P$. □

2.3 p–adic analytic functions

2.3.1 Ultrametric power series

We follow [17]. The field $\mathbb{Q}_p$ is complete for the p–adic absolute value. Let

$$f = \sum_{n_1 \ge 0} \cdots \sum_{n_r \ge 0} a_{n_1,\ldots,n_r} z_1^{n_1} \cdots z_r^{n_r} = \sum_{\underline{n} \in \mathbb{Z}^r_{\ge 0}} a_{\underline{n}} \underline{z}^{\underline{n}}$$

be a formal series with coefficients in $\mathbb{Q}_p$. If R is a real number > 0, we set

$$|f|_R = \sup_{\underline{n} \in \mathbb{Z}^r_{\ge 0}} R^{|\underline{n}|} |a_{\underline{n}}|, \quad \text{where} \quad |\underline{n}| = n_1 + \cdots + n_r.$$

We have

$$|f+g|_R \le \sup\{|f|_R,\ |g|_R\}, \quad |\lambda f|_R = |\lambda| \cdot |f|_R \quad \text{and} \quad |fg|_R = |f|_R |g|_R$$

if $|f|_R$ and $|g|_R$ are finite. When $|f|_R$ is finite, the series $f(\underline{z})$ converges in the polydisc $|z_i| < R$. Moreover, it converges in the closed polydisc $|z_i| \le R$ when $R^{|\underline{n}|}|a_{\underline{n}}|$ tends to zero. We have

$$|f(\underline{z})| \le |f|_R.$$

Since the residue field of $\mathbb{Q}_p$ is infinite and the group of values of $\mathbb{Q}_p^\times$ is dense, we also have

$$|f|_R = \sup |f(\underline{z})| \quad \text{for} \quad |z_i| < R.$$

If $R' \le R$, we have $|f|_{R'} \le |f|_R$ (*maximum modulus principle*).

2.3.2 Ultrametric Schwarz Lemma

The purpose of the Schwarz's Lemma is to improve the maximum modulus principle by taking into account the zeros of f inside the polydisc $|z_i| < R'$. With the method of interpolation determinants of Laurent [26], we need only to take into account the multiplicity of the zero at the origin. For this reason, the proof reduces to the one variable case (as a matter of fact, we shall use Lemma 7 only for the case of functions of a single variable).

Lemma 7. *If f has a zero of multiplicity $\geq h$ at the origin, then for $R' \leq R$ we have*

$$|f|_{R'} \leq \left(\frac{R'}{R}\right)^h |f|_R.$$

Proof (following [17]). Let $\underline{z}$ satisfy $|f(\underline{z})| = |f|_R$ and $|z_i| \leq R$. Define $g(t) = t^{-h} f(t\underline{z})$ for $t \in \mathbb{Q}_p$ with $|t| \leq 1$. Since $R'/R \leq 1$, we deduce $|g|_{R'/R} \leq |g|_1$. Since $|g|_1 = |f|_R$ and $|g|_{R'/R} = (R/R')^h |f|_R$, Lemma 7 follows. □

A quantitative version of Lemma 7 is Lemma 3.4.p of [19].

Corollary 8. *Let $f_1, \ldots, f_L$ be power series in $\mathbb{Q}_p^r$ with $|f_\lambda|_R < \infty$ and let $\underline{z}_1, \ldots, \underline{z}_L$ be points in the polydisc $|z_i| \leq R'$ with $R' \leq R$. Then the determinant*

$$\Delta = \det\Big(f_\lambda(\underline{z}_\mu)\Big)_{1 \leq \lambda, \mu \leq L}$$

is bounded by

$$|\Delta| \leq L! \left(\frac{R'}{R}\right)^{L^{1+1/r}} \prod_{\lambda=1}^{L} |f_\lambda|_R.$$

Proof. Corollary 8 is an ultrametric version of Lemma 6.3 of [26]; it follows from Lemma 7 by means of Lemmas 6.4 and 6.5 of [26], according to which the function of one variable

$$\Psi(t) = \det\Big(f_\lambda(t\underline{z}_\mu)\Big)_{1 \leq \lambda, \mu \leq L}$$

has a zero of multiplicity greater than $(n/e)L^{1+1/n}$ at the origin.

□

2.3.3 p–adic theta functions

Since the kernel of the logarithmic map

$$\log : A(\mathbb{Q}_p) \longrightarrow T_A(\mathbb{Q}_p)$$

is the set of torsion points of $A(\mathbb{Q}_p)$, this map is locally injective near the neutral element of $A(\mathbb{Q}_p)$. Let $\mathcal{U}$ be an open neighborhood of $(1 : 0 : \cdots : 0)$ in $A(\mathbb{Q}_p)$, $\mathcal{V}$ be an open neighborhood of 0 in $T_A(\mathbb{Q}_p)$ and $\theta : \mathcal{V} \to \mathcal{U}$ be a local inverse of log:

$$u \in \mathcal{U} \implies \log u \in \mathcal{V} \quad \text{and} \quad \theta \log(u) = u,$$

$$v \in \mathcal{V} \implies \theta(v) \in \mathcal{U} \quad \text{and} \quad \log \theta(v) = v.$$

By definition of r, $\overline{\log \Gamma}$ is a $\mathbb{Z}_p$-submodule of $T_A(\mathbb{Q}_p)$ of dimension r which contains the ℓ elements $\log \gamma_j$ $(1 \leq j \leq \ell)$. Let $e_1, \ldots, e_r$ be a basis. Let $R > 0$ be a positive real number such that $z_1 e_1 + \cdots + z_r e_r \in \mathcal{V}$ for any

$\underline{z} = (z_1, \ldots, z_r) \in \mathbb{Q}_p^r$ with $|z_i|_p \le R$. For $\underline{z} = (z_1, \ldots, z_r) \in \mathbb{Q}_p^r$ with $|z_i|_p < R$, define $\theta_1(\underline{z}), \ldots, \theta_N(\underline{z})$ by

$$\theta(z_1 e_1 + \cdots + z_r e_r) = \bigl(1 : \theta_1(\underline{z}) : \cdots : \theta_N(\underline{z})\bigr).$$

Then $\theta_1, \ldots, \theta_N$ are power series in r variables with coefficients in $\mathbb{Q}_p$ and radius of convergence $\ge R$.

Write

$$\log \gamma_j = \sum_{i=1}^{r} \eta_{ji} e_i \quad \text{and} \quad y_j = (\eta_{j1}, \ldots, \eta_{jr}) \in \mathbb{Q}_p^r \quad (1 \le j \le \ell).$$

Further, select $M \in \mathbb{Z}_{>0}$ such that

$$\max_{\substack{1 \le j \le \ell \\ 1 \le i \le r}} |M \eta_{ji}|_p < R.$$

Then, for any $\underline{s} \in \mathbb{Z}^\ell$ with $M | s_j$ for $1 \le j \le \ell$,

$$s_1 \log \gamma_1 + \cdots + s_\ell \gamma_\ell \in \mathcal{V}$$

and

$$\theta(s_1 \log \gamma_1 + \cdots + s_\ell \log \gamma_\ell) = \bigl(1 : \gamma_{\underline{s}1} : \cdots : \gamma_{\underline{s}N}\bigr).$$

Hence $\gamma_{\underline{s}\nu} = \theta_\nu(y_{\underline{s}})$ for all $\underline{s} \in \mathbb{Z}^\ell$ with $M | s_j$ and for all ν with $1 \le \nu \le N$.

3 The zero estimate and the interpolation determinant

The zero–estimate of Masser–Wüstholz (Main Theorem of [12]) is valid for a quasi–projective commutative algebraic group variety over a field K of zero characteristic. We need it only for a simple Abelian variety, which makes the statement shorter, since there is no algebraic subgroup to worry about.

Let again A be a simple Abelian variety of dimension g embedded into a projective space $\mathbb{P}_N$. When $P \in K[Y_0, \ldots, Y_N]$ is a non–zero homogenous polynomial, we denote by $Z(P)$ the hypersurface $P = 0$ of $\mathbb{P}_N(K)$.

Lemma 9 (Zero estimate)**.** *There exists a constant $c > 0$ depending only on A and on the embedding of A into $\mathbb{P}_N$ with the following property. Let $\gamma_1, \ldots, \gamma_\ell$ be $\mathbb{Z}$–linearly independent elements in $A(K)$. Let $P \in K[Y_0, \ldots, Y_N]$ be a homogenous polynomial of total degree $\le D$, such that $Z(P)$ does not contain $A(K)$ but contains*

$$\Gamma(S) = \bigl\{ s_1 \gamma_1 + \ldots + s_\ell \gamma_s \; ; \; \underline{s} \in \mathbb{Z}^\ell(S) \bigr\}.$$

Then

$$D > c(S/g)^{\ell/g}.$$

Like in [20], § 2.b, we could replace the zero estimate by an interpolation lemma due to D.W. Masser ([11] and Theorem 2.1 of [20]). The idea is just to consider the transposed matrix.

Coming back to the notations of § 2 (recall in particular the integer $M > 0$ introduced in § 2.3.3), we deduce from Lemma 9:

Corollary 10. *There exist two integers $c_1 > 1$ and $N_0 > 1$, depending on A and $\gamma_1, \dots, \gamma_\ell$, with the following property: if N is a positive integer with $N \geq N_0$ and if we set*

$$L = N^{\ell g}, \quad T = N^\ell, \quad S = c_1 N^g,$$

then there exists a subset $\mathcal{S} = \{\underline{s}_1, \dots, \underline{s}_L\}$ of $\mathbb{Z}^\ell(S)$ with L elements $\underline{s}_\mu = (s_{\mu,j})_{1 \leq j \leq \ell}$ $(1 \leq \mu \leq L)$, such that $M | s_{\mu,j}$ for $1 \leq j \leq \ell$ and $1 \leq \mu \leq L$, and such that the determinant

$$\Delta = \det \left(\gamma_{\underline{s}1}^{t_1} \cdots \gamma_{\underline{s}g}^{t_g} \right)_{\underline{s} \in \mathcal{S},\, \underline{t} \in \mathbb{Z}^g(T)}$$

does not vanish.

Proof. Consider the matrix

$$\left(\gamma_{\underline{s}1}^{t_1} \cdots \gamma_{\underline{s}g}^{t_g} \right)_{\underline{t}, \underline{s}},$$

where the index of rows is $\underline{t} \in \mathbb{Z}^g(T)$, while the index of columns $\underline{s}$ runs over the elements in $\mathbb{Z}^\ell(S)$ for which M divides s_j. Our goal is to prove that this matrix has maximal rank L. Consider a system of relations among the rows of the matrix

$$\sum_{\underline{t} \in \mathbb{Z}^g(T)} p_{\underline{t}} \gamma_{\underline{s}1}^{t_1} \cdots \gamma_{\underline{s}g}^{t_g} = 0 \qquad (\underline{s} \in \mathbb{Z}^\ell(S),\ M | s_j)$$

with $p_{\underline{t}} \in k$ for all $\underline{t} \in \mathbb{Z}^g(T)$. The polynomial

$$\sum_{\underline{t} \in \mathbb{Z}^g(T)} p_{\underline{t}} X_1^{t_1} \cdots X_g^{t_g}$$

has degree $\leq T$ in each of the variables $X_1, \dots, X_g$ and vanishes at all points of $\gamma_{\underline{s}} \in \Gamma(S)$ for which $M | s_j$ $(1 \leq j \leq \ell)$. Use Lemma 9 with $\gamma_1, \dots, \gamma_\ell$ replaced by $M\gamma_1, \dots, M\gamma_\ell$. Taking $c_1 > Mg(g/c)^{g/\ell}$, so that $gN^\ell < c(c_1 N^g / gM)^{\ell/g}$, it follows that this polynomial is 0, hence $p_{\underline{t}} = 0$ for all $\underline{t} \in \mathbb{Z}^g(T)$. $\square$

4 Upper bound for the height and lower bound for the absolute value of the interpolation determinant

Under the assumptions of Theorem 2, we give an upper bound for the height of the determinant Δ introduced in Corollary 10.

Proposition 11. *There exists a positive integer $c_2 > 1$, depending on A and $\gamma_1, \dots, \gamma_\ell$, such that, for all $N \geq N_0$,*

$$\mathrm{h}(\Delta) \leq c_2 LTS^2.$$

Proof. From Lemma 5, we deduce, for any $\underline{s} \in \mathbb{Z}^\ell(S)$,

$$\mathrm{h}\left(1 : \gamma_{\underline{s}1} : \dots : \gamma_{\underline{s}N}\right) \leq cS^2.$$

Proposition 11 now follows from Lemma 6 with

$$\nu_1 = \dots = \nu_L = g, \quad N_1 = \dots = N_L = T \quad \text{and} \quad \mathrm{L}(f) \leq L!$$

$\square$

Liouville's inequality (Lemma 4) implies:

Corollary 12. *With the notations of Proposition 11,*

$$\log |\Delta|_p \geq -c_2 LTS^2.$$

5 Analytic estimate: upper bound for the absolute value of the interpolation determinant

Proposition 13. *There exists a positive integer $c_3 > 1$, depending on A and $\gamma_1, \dots, \gamma_\ell$, such that, for all $N \geq N_0$,*

$$\log |\Delta|_p \leq -c_3 L^{1+1/r}.$$

Proof. Proposition 13 follows from Corollary 8 with the set of functions

$$\{f_1, \dots, f_L\} = \left\{\theta_1^{t_1} \cdots \theta_g^{t_g} \; ; \; \underline{t} \in \mathbb{Z}_{\geq 0}(T)\right\}$$

and the points $\underline{z}_\mu = s_{\mu 1} y_1 + \dots + s_{\mu \ell} y_\ell$ $(1 \leq \mu \leq L)$. $\square$

6 Proof of the main transcendence result

Proof ot Theorem 2. Since $TS^2 = c_1^2 L^{(1/g)+(2/\ell)}$, the conclusions of corollary 12 and proposition 13 imply

$$\frac{1}{r} \leq \frac{1}{g} + \frac{2}{\ell}\cdot$$

$\square$

7 Remarks

- **7.1.** In place of the rational number field and the prime number p, one may work with an algebraic number field and a finite place v, replacing $\mathbb{Q}_p$ with the completion k_v. One main difference is in § 2.2.2, where, in the case of a number field, one needs to introduce height functions on the field of algebraic numbers in place of the rational number field. See [26] Chap. 3 § 2, [9], § B.2, [18], Chap. 2, [4] Chap. 1, [10] Chap. 4.

  As pointed out in [14] (Remark 6.4), one cannot deduce the general case of a number field from the special case of the rational numbers by means of the restriction of scalars.

- **7.2.** As mentioned in [21] (§ 6a p. 643), similar results hold when the simple Abelian variety A is replaced by a commutative algebraic group G. There is a condition in [21] for the ultrametric case that a subgroup of finite index of Γ is contained in a compact subgroup of $A(k_v)$ – for an Abelian variety A, the group $A(k_v)$ is compact and this condition is always satisfied.

  Let us write, like in [21], $G = \mathbb{G}_A^{d_0} \times \mathbb{G}_m^{d_1} \times G'$, where G' has dimension d_2 (and therefore G has dimension $d = d_0 + d_1 + d_2$). Roughly speaking, in this general sitting, one replaces

$$\frac{\ell g}{\ell + 2g} \quad \text{by} \quad \frac{\ell d}{\ell + d_1 + 2d_2}.$$

  However, one needs to take into account possible degeneracies occurring from the algebraic subgroups of G. We refer to [21] for precise statements.

  In the case of a power of the multiplicative group $G = \mathbb{G}_m^d$, the transcendence result yields lower bounds for the p–adic rank of the units of an algebraic number field (namely partial results towards Leopoldt's Conjecture).

- **7.3.** Following [14], consider a commutative algebraic group G over $\mathbb{Q}$ and a finitely generated subgroup Γ of $G(\mathbb{Q})$ contained in the union of compact subgroups of $\mathbb{G}(\mathbb{Q}_p)$. The number $\dim(\overline{\Gamma})$ can be defined exactly like in § 2.1 as the dimension of the $\mathbb{Z}_p$–submodule of the tangent space at the origine $\mathrm{Lie}(G)$ spanned by the image of Γ under the logarithmic map. Another function $d(\Gamma)$ of Γ is introduced by B. Poonen in [14]:

$$d(\Gamma) := \min_{H \subset G} \bigl\{ \dim H + \mathrm{rk}_{\mathbb{Z}}(\Gamma/\Gamma \cap H) \bigr\},$$

  where the minimum is over all algebraic subgroups H of G over $\mathbb{Q}$. The inequality $\dim(\overline{\Gamma}) \leq d(\Gamma)$ is always true. Here is an example where this inequality is strict (compare with Langevin's example in [23] p. 1201 and 1209 for $\mathbb{G}_m^3$). Consider an elliptic curve E over $\mathbb{Q}$ with three linearly independent algebraic points $\gamma_1, \gamma_2, \gamma_3$ in $E(\mathbb{Q})$. Let Γ be the subgroup of $E^3(\mathbb{Q})$ generated by $(0, \gamma_3, -\gamma_2)$, $(-\gamma_3, 0, \gamma_1)$, $(\gamma_2, -\gamma_1, 0)$. Then $\dim \overline{\Gamma} = 2$, while $d(\Gamma) = 3$.

  To produce a lower bound for the p–adic rank amounts to produce lower bounds for the rank of certain matrices whose entries are p–adic logarithms of algebraic points. From a conjectural point of view, the answer is given by the *structural rank* introduced by D. Roy. See [26] for the case of linear algebraic groups.

- **7.4.** Further applications of the algebraic subgroup theorem in the ultrametric case are given by D. Roy in [15].
- **7.5.** Our p–adic result Theorem 2 is an ultrametric version of [21, 22] (see also [16]). In the Archimedean case, quantitative refinements are given in [25], they are based on the results of [24]. See also [8]. Since the method is "effective", it is also possible to produce quantitative refinements of Theorem 2.
- **7.6.** An alternative proof of the main result (Theorem 2) can be given by means of Arakelov's geometry and Bost slope inequality. See the papers by J.B. Bost [5] and A. Chambert–Loir [7].

References

[1] Y. André, *G-functions and geometry*, Aspects of Mathematics, E13, Friedr. Vieweg & Sohn, Braunschweig, 1989.

[2] ——, *Une introduction aux motifs (motifs purs, motifs mixtes, périodes)*, vol. 17 of Panoramas et Synthèses, Société Mathématique de France, Paris, 2004.

[3] J. Bellaiche, *Personal communication*. February 2010.

[4] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, vol. 4 of New Mathematical Monographs, Cambridge University Press, Cambridge, 2006.

[5] J.-B. Bost, *Périodes et isogenies des variétés abéliennes sur les corps de nombres (d'après D. Masser et G. Wüstholz)*, Astérisque, (1996), pp. 115–161. Séminaire Bourbaki, Exp. No. 795, 4, Vol. 1994/95.

[6] N. Bourbaki, *Lie groups and Lie algebras. Chapters 1–3*, Elements of Mathematics (Berlin), Springer-Verlag, Berlin, 1998. Translated from the French, Reprint of the 1989 English translation.

[7] A. Chambert-Loir, *Théorèmes d'algébricité en géométrie diophantienne (d'après J.-B. Bost, Y. André, D. & G. Chudnovsky)*, Astérisque, (2002), pp. 175–209. Séminaire Bourbaki, Exp. No. 886, viii, Vol. 2000/2001.

[8] A. Ghosh, A. Gorodnik, and A. Nevo, *Diophantine approximation and automorphic spectrum*. July 4, 2010 `http://arxiv.org/abs/1007.0593`.

[9] M. Hindry and J. H. Silverman, *Diophantine geometry*, vol. 201 of Graduate Texts in Mathematics, Springer-Verlag, New York, 2000. An introduction.

[10] P.-C. Hu and C.-C. Yang, *Distribution theory of algebraic numbers*, vol. 45 of de Gruyter Expositions in Mathematics, Walter de Gruyter GmbH & Co. KG, Berlin, 2008.

[11] D. W. Masser, *Interpolation on group varieties*, in Diophantine approximations and transcendental numbers (Luminy, 1982), vol. 31 of Progr. Math., Birkhäuser Boston, Mass., 1983, pp. 151–171.

[12] D. W. Masser and G. Wüstholz, *Zero estimates on group varieties. I*, Invent. Math., 64 (1981), pp. 489–516.

[13] B. Mazur, *Speculations about the topology of rational points: an update*, Astérisque, (1995), pp. 165–182. Columbia University Number Theory Seminar (New York, 1992).

[14] B. Poonen, *The p–adic closure of a subgroup of rational points on a commutative algebraic group,* 2006 (unpublished) . `http://www-math.mit.edu/ poonen/papers/leopoldt.pdf`.

[15] D. Roy, *On the v-adic independence of algebraic numbers*, in Advances in number theory (Kingston, ON, 1991), Oxford Sci. Publ., Oxford Univ. Press, New York, 1993, pp. 441–451.

[16] D. Roy and M. Waldschmidt, *Autour du théorème du sous-groupe algébrique*, Canad. Math. Bull., 36 (1993), pp. 358–367.

[17] J.-P. Serre, *Dépendance d'exponentielles p–adiques*, Séminaire Delange–Pisot–Poitou. Théorie des Nombres, t. **7**, n °2 (1965–66), exp. n° 15, (1966), pp. 1–14 . `http://archive.numdam.org/article/SDPP_1965-1966__7_2_A4_0.pdf`.

[18] ——, *Lectures on the Mordell-Weil theorem*, Aspects of Mathematics, E15, Friedr. Vieweg & Sohn, Braunschweig, (first edition 1989) third ed., 1997. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre.

[19] M. Waldschmidt, *Transcendance et exponentielles en plusieurs variables*, Invent. Math., 63 (1981), pp. 97–127.

[20] ——, *Dépendance de logarithmes dans les groupes algébriques*, in Diophantine approximations and transcendental numbers (Luminy, 1982), vol. 31 of Progr. Math., Birkhäuser Boston, Mass., 1983, pp. 289–328.

[21] ——, *Sous-groupes analytiques de groupes algébriques*, Ann. of Math. (2), 117 (1983), pp. 627–657.

[22] ——, *Densité des points rationnels sur un groupe algébrique*, Experiment. Math., 3 (1994), pp. 329–352. Erratum: vol. 4 (3) 1995), 255.

[23] ———, *Dependence of logarithms on commutative algebraic groups*, Rocky Mountain J. Math., 26 (1996), pp. 1199–1223. Symposium on Diophantine Problems (Boulder, CO, 1994).

[24] ———, *Approximation diophantienne dans les groupes algébriques commutatifs. I. Une version effective du théorème du sous-groupe algébrique*, J. Reine Angew. Math., 493 (1997), pp. 61–113.

[25] ———, *Density measure of rational points on abelian varieties*, Nagoya Math. J., 155 (1999), pp. 27–53.

[26] ———, *Diophantine approximation on linear algebraic groups*, vol. 326 of Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], Springer-Verlag, Berlin, 2000. Transcendence properties of the exponential function in several variables.

Michel WALDSCHMIDT
Université P. et M. Curie (Paris VI)
Institut de Mathématiques de Jussieu – CNRS UMR 7586
4, Place Jussieu
F–75252 PARIS Cedex 05 FRANCE
e-mail: miw@math.jussieu.fr
URL: http://www.math.jussieu.fr/~miw/