Ann. Scuola Norm. Sup. Pisa Cl. Sci. (5)
Vol. II (2003), pp. 47-75

The Intersection of a Curve with Algebraic Subgroups in a Product of Elliptic Curves

EVELINA VIADA

Abstract. We consider an irreducible curve $\mathcal{C}$ in E^n, where E is an elliptic curve and $\mathcal{C}$ and E are both defined over $\overline{\mathbb{Q}}$. Assuming that $\mathcal{C}$ is not contained in any translate of a proper algebraic subgroup of E^n, we show that the points of the union $\bigcup \mathcal{C} \cap A(\overline{\mathbb{Q}})$, where A ranges over all proper algebraic subgroups of E^n, form a set of bounded canonical height. Furthermore, if E has Complex Multiplication then the set $\bigcup \mathcal{C} \cap A(\overline{\mathbb{Q}})$, for A ranging over all algebraic subgroups of E^n of codimension at least 2, is finite. If E has no Complex Multiplication then the set $\bigcup \mathcal{C} \cap A(\overline{\mathbb{Q}})$ for A ranging over all proper algebraic subgroups of E^n of codimension at least $\frac{n}{2} + 2$, is finite.

Mathematics Subject Classification (2000): 11D45 (primary), 11G50 (secondary)

1. – Introduction

The Manin-Mumford Conjecture states that if $\mathcal{C}$ is a nonsingular projective curve of genus ≥ 2 defined over a number field K, which is embedded in its Jacobian J, then the set $\mathcal{C} \cap \mathrm{Tor}(J)$ of points of $\mathcal{C}(\overline{K})$ whose image in J is torsion, is finite. The toric version of this Conjecture has been proven by M. Laurent [9]. M. Raynaud [13] and [16] proved that if A is an abelian variety in characteristic 0 and $\mathcal{V}$ is a subvariety of A then $\mathcal{V} \cap \mathrm{Tor}(A)$ is a finite union of cosets, proving in particular the Manin-Mumford Conjecture. M. Hindry [9] then gave a quantitative version of this result and generalized it to a subvariety $\mathcal{V}$ of a semiabelian variety G. The Manin-Mumford Conjecture can be further generalized. After fixing a subvariety $\mathcal{V}$ of a semiabelian variety G and a certain codimension c, one can study the set of points of $\bigcup \mathcal{V} \cap A(\overline{\mathbb{Q}})$, where A ranges over all proper algebraic subgroups of G of codimension c. In this way, the Manin-Mumford Conjecture deals with algebraic subgroups of dimension zero.

Pervenuto alla Redazione il 19 ottobre 2001.

Due to the structure of the algebraic subgroups of a general commutative algebraic group G, it is natural to study this problem in the cases where G is either a toric group or $G = E^n$, where E is an elliptic curve.

In 1999 E. Bombieri, D. Masser and U. Zannier [1] solved the toric part of the above problem for an irreducible curve of genus ≥ 2 defined over $\overline{\mathbb{Q}}$. They show that, if the curve $\mathcal{C}$ is embedded in a multiplicative group $\mathbb{G}_m^n$ and is not contained in any translate of a proper algebraic subgroup, then the points of $\bigcup \mathcal{C} \cap H(\overline{\mathbb{Q}})$, for H ranging over all proper algebraic subgroups of $\mathbb{G}_m^n$, form a set of bounded Weil height. Moreover the set of points $\bigcup \mathcal{C} \cap H(\overline{\mathbb{Q}})$, for H ranging over all proper algebraic subgroups of $\mathbb{G}_m^n$ of codimension at least 2, is finite.

Here we deal with the elliptic case. We consider an irreducible curve $\mathcal{C}$ transversally embedded in a product of elliptic curves E^n, where 'transversally' means that the image of $\mathcal{C}$ is not contained in any translate of a proper algebraic subgroup. We recall that by the Hurwitz formula a curve of genus zero can not be embedded in E^n and a curve of genus 1 is an abelian variety so it can not satisfy the transversal condition, hence our curve $\mathcal{C}$ has genus ≥ 2.

In Theorem 1 we prove that the points of $S_1(\mathcal{C}) := \bigcup \mathcal{C} \cap A(\overline{\mathbb{Q}})$ where A ranges over all proper algebraic subgroups of E^n form a set of bounded canonical height. More precisely, we have:

THEOREM 1. *Let E be an elliptic curve defined over $\overline{\mathbb{Q}}$. Let $\mathcal{C}$ be an irreducible curve defined over $\overline{\mathbb{Q}}$ and transversally embedded in E^n. Then the set*

$$S_1(\mathcal{C}) := \bigcup_{\mathrm{cod}(A)\geq 1} A \cap \mathcal{C}(\overline{\mathbb{Q}}),$$

where A ranges over all proper algebraic subgroups of E^n, is a subset of E^n of bounded canonical height.

In Theorem 2 we prove that if E is an elliptic curve with Complex Multiplication (C.M. for short), then the set $S_2(\mathcal{C}) := \bigcup \mathcal{C} \cap A(\overline{\mathbb{Q}})$ where A ranges over all proper algebraic subgroups of E^n of codimension at least 2, is a finite set. More precisely, we have:

THEOREM 2. *Let E be a C.M. elliptic curve and $\mathcal{C}$ an irreducible curve defined over $\overline{\mathbb{Q}}$ which is transversally embedded in E^n. Then the set*

$$S_2(\mathcal{C}) := \bigcup_{\mathrm{cod}(A)\geq 2} A \cap \mathcal{C}(\overline{\mathbb{Q}}),$$

where A ranges over all algebraic subgroups of E^n of codimension at least 2, is finite.

Since every morphism from a curve to an abelian variety factors through its Jacobian, we can deduce from our result that, if a curve can be embedded in E^n, then, not just its torsion is finite, as the Manin-Mumford Conjecture states, but also the set of points lying in an algebraic subgroup of the Jacobian of codimension at least 2 is finite.

Another immediate consequence of our theorems is that, if a curve $\mathcal{C}$ is transversally embedded in a product E^n, where E is an elliptic curve of K-rank $r < n$, then the set of K-rational points of the curve is finite. Chabauty's Theorem ([21] Section 5.1) also relates rank and dimension. He considers a curve $\mathcal{C}$ in an abelian variety A, so that $\mathcal{C}$ generates A. If Γ is a finitely generated subgroup of $A(K)$ such that $\mathrm{rk}\Gamma < \dim A$ then $\Gamma \cap \mathcal{C}$ is finite. This result is more general than our remark in the sense that it deals with a general abelian variety A and a general subgroup Γ. But our special case where we consider $\Gamma = A = E^n$ requires $\mathrm{rk}(\Gamma) \leq n^2$, instead of $\mathrm{rk}(\Gamma) \leq n$. It might be interesting to relate these two results and to give a new proof for Chabauty's theorem. However, even if the used methods are different, those are particular aspects of the more general theorem of Faltings [8] on the Mordell conjecture.

In Theorem 4 we give a slightly more general formulation for Theorems 1 and 2. Moreover we show that the hypothesis that $\mathcal{C}$ is not contained in any translate of a proper algebraic subgroup of E^n is indeed necessary. We give a counter-example to the statement of Theorem 1 under the weaker condition that $\mathcal{C}$ is not contained in any proper algebraic subgroup. It seems probable that Theorem 2 is still true assuming only that $\mathcal{C}$ is not contained in any proper algebraic subgroup of E^n, although our method, which relies on Theorem 1, proves the result under this stronger assumption.

The proof of Theorem 1 is based on some functorial properties of the height function and on the Theorem of the Cube and makes direct use of the linear dependence of the coordinates of a point in $S_1(\mathcal{C})$.

By Theorem 1 the set $S_2(\mathcal{C})$ is of bounded height. Thus, in view of Northcott's Theorem, in order to prove Theorem 2 it is enough to show that the degree of the points in $S_2(\mathcal{C})$ is absolutely bounded. For every point $P \in S_2(\mathcal{C})$ we construct a special algebraic subgroup A of codimension at least 2, passing through P, whose degree gives an upper bound for the degree of the field $K(P)$ of definition of P. Using a recent result of S. David and M. Hindry, we show that the above upper bound depends only on the order NR of the torsion of the coordinate ring $\Gamma_P = \langle x_1(P), \ldots, x_n(P) \rangle$. On the other hand the torsion of Γ_P is defined over $K(P)$, this gives a lower bound for the degree of $K(P)$ in terms of NR.

Lower and upper bounds are sharp enough to conclude the proof if we consider points in the intersection of $\mathcal{C}$ and subvarieties of codimension at least 3. The last remaining case, where the codimension of A is 2, requires a careful study of the cohomology of the Galois groups of the extensions $K(E[N])$ of K with coefficient in some k-torsion subgroup $E[k]$. This enables us to refine the upper bound for the degree of $K(P)$ and to conclude the proof of Theorem 2.

If the elliptic curve E does not have Complex Multiplication, one does not have sharp enough lower bounds for the Néron-Tate height of a K-rational point. The sharpest known bound, in this case, is due to D. Masser [12] and S.

David [6]. This bound implies the finiteness of the set $S_{n-r}(\mathcal{C})$ for $r \leq \frac{n}{2} - 2$, unfortunately this result is not optimal as it is for the C.M. case.

THEOREM 3. *Let E be a non C.M. elliptic curve defined over $\overline{\mathbb{Q}}$ and $\mathcal{C}$ an irreducible curve also defined over $\overline{\mathbb{Q}}$ and transversally embedded in E^n.*

Then the set

$$S_c(\mathcal{C}) := \bigcup_{\mathrm{cod}(A) \geq c} \mathcal{C} \cap A(\overline{\mathbb{Q}}),$$

where A ranges over all algebraic subgroup of E^n of codimension at least c, is finite for $c \geq \frac{n}{2} + 2$.

However, the case $r \leq n - 3$ of Theorem 2 for elliptic curves non C.M. follows from the generalized Lehmer Problem ([7] Conjecture 1.4), more precisely:

CONJECTURE 1. Let A be an abelian variety defined over a number field K, $\mathcal{L}$ a symmetric ample line bundle on A and n a positive integer. Then, there exists a constant $C(A, \mathcal{L}, n)$, such that, if the algebraic point $P = (P_1, \ldots, P_n) \in A^n$ has infinite order modulo every abelian subvariety of A^n, we have

$$\prod_{i=1}^{n} \hat{h}_{\mathcal{L}}(P_i) \geq C(A, \mathcal{C}, n) D^{-\frac{1}{g}},$$

where $D := [K(P) : K]$ is the degree of the field of definition of P over K.

A slightly weaker result with $1/g$ replaced by $(1/g) + \varepsilon$ would be enough for our purpose. Even weaker results about the minimal height on the lattice generated by $P_1, \ldots, P_n$ would enable us to derive probably optimal results for the non C.M. case by modifying marginally our argument.

ACKNOWLEDGEMENTS. I very warmly thank S. David for suggesting me such a nice problem and leading me through it by a lot of discussions and encouragement. It is a special pleasure for me to thank E. Bombieri and U. Zannier for the many details they explained to me and for their interest in this problem. Deep thanks go to D. Bertrand and D. Masser for their helpful suggestions and examples. Special thanks go to G. Böckle, F. Gardeyn, and G. Rémond for their help and nice remarks. I am grateful to my advisor, G. Wüstholz, for supporting my research plan and for trusting and encouraging me in doing mathematics.

2. – Preliminaries

Let E be an elliptic curve defined over a number field K. We recall that if $\mathrm{End}(E)=\mathbb{Z}$ then E is said to be non C.M. If $\mathrm{End}(E)$ is an order $\mathcal{O}=\mathbb{Z}+\tau\mathbb{Z}$ in the ring of integers of an imaginary quadratic extension of $\mathbb{Q}$ then E is said to be C.M. If E is C.M. we replace the field K by a finite extension over which the morphism τ and the $j(E)$ invariant are defined. For S a subset of $E(\overline{\mathbb{Q}})$, we denote by $K(S)$ the minimal field extension of K over which the set S is defined.

The following lemma characterizes the algebraic subgroups of E^n.

Lemma 1 (Subgroup Lemma).

- *If E is non C.M. and A is an algebraic subgroup of codimension r in E^n, then A is characterized by r equations $\mathbb{Q}$-linearly independent, of the type $\sum_{i=1}^n n_i\pi_i = 0$ where $n_i \in \mathbb{Z}$ and the π_i are a basis of* $\mathrm{Hom}(E^n, E)$ *as $\mathbb{Z}$-module.* ([13] 3.3 Lemma 2)
- *If E is C.M. and A is an algebraic subgroup of codimension r in E^n, then there exist r equations k-linearly independent, of the type $\sum_{i=1}^n \alpha_i\pi_i$ vanishing on A, where $k = \mathcal{O}\otimes_{\mathbb{Z}}\mathbb{Q}$, $\alpha_i \in \mathcal{O}$ and the π_i are a basis of the free $\mathcal{O}$-module* $\mathrm{Hom}(E^n, E)$.

Proof. If E is non C.M., see for example [13] 3.3 Lemma 2. For the C.M. case we give, for convenience, a proof. We consider the exact sequence

$$0 \to A \to E^n \to A^\perp := E^n/A \to 0.$$

Since Hom is a left exact functor, we get the exact sequence

$$0 \longrightarrow \mathrm{Hom}(A^\perp, E) \xrightarrow{\varphi} \mathrm{Hom}(E^n, E) \xrightarrow{\psi} \mathrm{Hom}(A, E),$$

where $\mathrm{Hom}(A^\perp, E)$ has rank r over $\mathcal{O}$, because $A^\perp$ is isogenous to E^r. Let $f_1, \dots f_r$ be k-linearly independent elements of $\mathrm{Hom}(A^\perp, E)$ such that $\varphi(f_j) = \sum_{i=1}^n \alpha_{j,i}\pi_i$. Since the f_i belong to the kernel of ψ, the $\sum_{i=1}^n \alpha_{j,i}\pi_i$ are vanishing on A and they are k-linearly independent. □

Let $\mathcal{C}$ be an irreducible curve in E^n not contained in any translate of a proper algebraic subgroup of E^n. We define on the module $\mathrm{Hom}(\mathcal{C}, E)$ of morphisms from $\mathcal{C}$ to E a degree function $\deg : \mathrm{Hom}(\mathcal{C}, E) \to \mathbb{Z}$ as follows: if f is a surjective morphism then $\deg f = [K(\mathcal{C}) : f^*K(E)]$ is the index of the corresponding fields of rational functions; if f is a constant morphism then $\deg f = 0$. Equivalently we can say that if U is an open set of E on which the order of the fiber of the morphism f is constant, then $\deg f$ is the order of one fiber of this open set. This degree map is a quadratic form, therefore it induces a scalar product (see [14] Corollary 6.5).

We denote by $x_i : \mathcal{C} \to E$ for $i = 1, \dots, n$ the coordinate maps given by the composition of the immersion $x : \mathcal{C} \to E^n$ and the projection on the i-th factor $\pi_i : E^n \to E$. We call $\Gamma := \langle x_1, \dots, x_n\rangle_{\mathrm{End}(E)}$ the coordinate module. If E is C.M. and $\mathrm{End}(E) = \mathcal{O} = \mathbb{Z}+\tau\mathbb{Z}$, we define the morphisms $x_{n+i} := \tau x_i$ for $i = 1, \dots, n$. The maps $x_1, \dots, x_{2n}$ are generators of Γ as a $\mathbb{Z}$-module.

REMARK 1. From the Subgroup Lemma 1 it follows that a point P belongs to the intersection $\mathcal{C} \cap A$ with A of codimension 1 if and only if $\sum_{i=1}^n \alpha_i x_i(P) = 0$ with $\alpha_i \in \mathrm{End}(E)$. Analogously a point P belongs to the intersection $\mathcal{C} \cap A$ with A of codimension 2 if and only if $\sum_{i=1}^n \alpha_i x_i(P) = 0$ and $\sum_{i=1}^n \alpha'_i x_i(P) = 0$ with $\alpha_i, \alpha'_i \in \mathrm{End}(E)$ and α_i, α'_i $\mathrm{End}(E)$-linearly independent vectors.

For any divisor Δ of E^n we denote the associated height by h_Δ and we denote the canonical height of E by $\hat{h}$. The function $\hat{h}$ is the square of a norm induced by a scalar product on $E \otimes \mathbb{R}$ (see [23] Theorem 9.3). We consider on $\mathcal{C}$ the height defined by a a non-singular point $Q \in \mathcal{C}$ and we denote it by h_Q or simply by h if Q will be fixed once and for all.

We use the symbols "$\ll$" and "$\gg$" to denote inequalities up to a constant factor.

2.1. – The transversality Condition on $\mathcal{C}$: A Counter-Example

We say that a curve $\mathcal{C}$ is transversally embedded in an abelian variety if it is not contained in any translate of a proper algebraic subgroup. This transversality condition on a curve $\mathcal{C}$ embedded in E^n is equivalent to say that no $\mathrm{End}(E)$-linear combination of the coordinate morphisms x_i is constant. This means that the $\mathrm{End}(E)$-module Γ generated by $x_1, \ldots, x_n$ has rank n. Indeed it follows from the Subgroup Lemma 1 that if A is an algebraic subgroup of E^n then there exists a form $\sum \alpha_i \pi_i$ with $\alpha_i \in \mathrm{End}(E)$ which vanishes on A. If $A - c$ contains $\mathcal{C}$, then for every $P \in \mathcal{C}$ we have $\sum \alpha_i \pi_i x(P) = c$. By definition of the x_i this gives $\sum \alpha_i x_i = c$. Vice-versa if $\sum \alpha_i x_i = c$ then the equation $\sum \alpha_i \pi_i = 0$ defines an algebraic subgroup A such that $A - c$ contains $\mathcal{C}$.

This shows that a slightly more general formulation of Theorem 1 and 2 is as follows.

THEOREM 4. *Let $\mathcal{C}$ be an irreducible curve and E an elliptic curve defined over $\overline{\mathbb{Q}}$. Let $f_1, \ldots, f_n$ be surjective morphisms from $\mathcal{C} \to E$ such that no non-trivial linear combination with coefficients in* $\mathrm{End}(E)$ *gives a constant function, then the set of points*

$$\left\{ P \in \mathcal{C}(\overline{\mathbb{Q}}) : \mathrm{rk}_{\mathrm{End}(E)} \langle f_1(P), \ldots, f_n(P) \rangle \leq n - 1 \right\}$$

has bounded canonical height. Furthermore if E is C.M, the set of points

$$\left\{ P \in \mathcal{C}(\overline{\mathbb{Q}}) : \mathrm{rk}_{\mathrm{End}(E)} \langle f_1(P), \ldots, f_n(P) \rangle \leq n - 2 \right\}$$

is finite.

The following example shows that the assumption that $\mathcal{C}$ is not contained in any translate of a proper algebraic subgroup of E^n is necessary. We consider the curve $\mathcal{C} := P_0 \times E$ in $E \times E$ with P_0 a point of infinite order in $E(\overline{\mathbb{Q}})$. Then $\mathcal{C}$ is not contained in any proper algebraic subgroup of E^2. For each $N \in \mathbb{N}$ we shall consider the abelian subvariety A_N of E^2 which is the image of E under the morphism $\varphi_N : E \to E^2$ with $\varphi_N(P) := (P, NP)$. The subvariety A_N has codimension 1. The point (P_0, NP_0) belongs to the intersection $\mathcal{C} \cap A_N(\overline{\mathbb{Q}})$, moreover its height is $\hat{h}(P_0, N \cdot P_0) = (N^2+1)\hat{h}(P_0)$, which goes to infinity for N going to infinity. This proves that, under the weaker condition of $\mathcal{C}$ not contained in any proper algebraic subgroup of E^n, the set $S_1(\mathcal{C})$ can have unbounded height.

3. – Intersecting with Algebraic Subgroups of Codimension 1

In Proposition 1 we establish the relation between the height of a point on $\mathcal{C}$, the height of its image under a non-constant morphism from $\mathcal{C}$ to E, and the degree of the morphism. The Theorem 1 is then an immediate consequence of this proposition.

Proposition 1. *Let f be an element of the coordinate module $\Gamma = \langle x_1, \ldots, x_n \rangle_{\mathrm{End}(E)}$ different from zero. Let Q be a non singular point of $\mathcal{C}$. Then for every non-singular point P of $\mathcal{C}$ we have*

$$\hat{h}(f(P)) = 3 \deg f \left[h_Q(P) + O\left(1 + \sqrt{h_Q(P)}\right)\right]$$

where the constant depends only on E, $\mathcal{C}$ and on the module Γ.

Proof. If E is C.M. we consider Γ as a $\mathbb{Z}$-module of rank $2n$ and $\mathbb{Z}$-basis $x_1, \ldots, x_{2n}$ with $x_{n+i} = \tau x_i$. From the generators $\{\pm x_i\}$ we choose a basis $\{\mathbf{x}_i\}$ so that we can write $f = \sum_i f_i \mathbf{x}_i$ with $f_i \in \mathbb{N}$. We recall that the degree function is a positive defined quadratic form defined over $\mathbb{Z}$. Let A be the matrix representation of this degree form with respect to the chosen basis $\mathbf{x}_i$ so that $\deg f = \sum f_i a_{ij} f_j$ where $a_{ij} = \frac{1}{2}(\deg(\mathbf{x}_i + \mathbf{x}_j) - \deg \mathbf{x}_i - \deg \mathbf{x}_j)$. In view of the Theorem of the cube ([14], Theorem 6.1), for any divisor Δ on E we have

$$f^*\Delta \cong \sum_i f_i^2 \mathbf{x}_i^* \Delta + \sum_{i<j} f_i f_j \left(-\mathbf{x}_i^*\Delta - \mathbf{x}_j^*\Delta + (\mathbf{x}_i + \mathbf{x}_j)^*\Delta\right) \tag{1}$$

where $\cong$ means linearly equivalent divisors. Linearly equivalent divisors define the same height function up to an absolute constant, the constant is determined by the choice of Weil-functions. Therefore

$$h_{f^*\Delta} = h_{\sum_i f_i^2 \mathbf{x}_i^*\Delta + \sum_{i<j} f_i f_j \left(-\mathbf{x}_i^*\Delta - \mathbf{x}_j^*\Delta + (\mathbf{x}_i+\mathbf{x}_j)^*\Delta\right)}.$$

Now we choose Weil-functions such that for any two divisors Φ and Φ' we have

$$h_{\Phi+\Phi'} = h_\Phi + h_{\Phi'}$$

hence, for such a choice,

$$h_{f^*\Delta} = \sum_i f_i^2 h_{\mathbf{x}_i^*\Delta} + \sum_{i<j} f_i f_j \left(-h_{\mathbf{x}_i^*\Delta} - h_{\mathbf{x}_j^*\Delta} + h_{(\mathbf{x}_i+\mathbf{x}_j)^*\Delta}\right).$$

The support of all divisors of the form $(\mathbf{x}_i + \mathbf{x}_j)^*\Delta$ for $i, j = 1, \dots, n$ is a finite set $\{Q_{ijl}\}_{l\in\Lambda}$. By the Néron relation we have

$$h_{Q_{ijl}} = h_Q + O\left(1 + \sqrt{h_Q}\right) \tag{2}$$

where the constant depends only on the finite set of points $\{Q_{ijl}\}$ and the curve $\mathcal{C}$. Let us write $\mathbf{x}_i^*\Delta = \sum_l \alpha_{iil} Q_{iil}$ and $(\mathbf{x}_i + \mathbf{x}_j)^*\Delta = \sum_l \alpha_{ijl} Q_{ijl}$ with $\alpha_{ijl} \in \mathbb{Z}$.

For a good choice of Weil-functions we get

$$h_{f^*\Delta} = \sum_i f_i^2 \alpha_{iil} h_{Q_{iil}} + \sum_{l,i<j} f_i f_j (-\alpha_{iil} h_{Q_{iil}} - \alpha_{jjl} h_{Q_{jjl}} + \alpha_{ijl} h_{Q_{ijl}})$$

where $\sum_l \alpha_{iil} = a_{ii} \deg \Delta$ and $\sum_{l,i<j} \alpha_{ijl} - \alpha_{iil} - \alpha_{jjl} = 2a_{ij} \deg \Delta$, we recall that $2a_{ij} = \deg(\mathbf{x}_i + \mathbf{x}_j) - \deg \mathbf{x}_i - \deg \mathbf{x}_j$. Using relation (2) we deduce

$$h_{f^*\Delta} = \deg \Delta \left[\deg f h_Q + \sum |f_i f_j a_{ij}| \left(O\left(1 + \sqrt{h_Q}\right)\right)\right].$$

We remark that $\sum |f_i f_j a_{ij}|$ induces a norm function on $\mathbb{R}^n$ which is equivalent to the degree norm. More precisely one has $\sum f_i f_j a_{ij} \le \sum |f_i f_j a_{ij}| \ll \lambda_{\max}^2 \sum f_i f_j a_{ij}$ with $\lambda_{\max}$ the greatest eigenvalue of the degree form. We deduce

$$h_{f^*\Delta} = \deg \Delta \deg f \left[h_Q + O\left(1 + \sqrt{h_Q}\right)\right]. \tag{3}$$

where the constant depends only on $\mathcal{C}$ and Γ.

Now we consider on E the very ample divisor $\Delta = 3 \cdot 0_E$. We remark that $f^*\Delta = x^*(\sum f_i \pi_i)^*\Delta$ where $x : \mathcal{C} \to E^n$ is the given immersion and $\pi_i : E^n \to E$ are the natural i-th projections. By [10], Section 4, Theorem 5.1, we have that

$$h_{f^*\Delta}(\cdot) = h_{x^*(\sum f_i\pi_i)^*\Delta} = h_{(\sum f_i\pi_i)^*\Delta}(x(\cdot)) + O(1) \tag{4}$$

where $O(1)$ depends on x. On the other hand, by [10], Section 5, Prop. 3.3, we deduce that

$$h_{(\sum f_i\pi_i)^*\Delta} = h_\Delta\left(\sum f_i \pi_i(\cdot)\right).$$

From these two relations, we see that, for any morphism f in Γ, one has

$$h_{f^*\Delta}(\cdot) = h_\Delta(f(\cdot)) + O(1) \tag{5}$$

where $O(1)$ depends on x.

Combining relations (3) and (5) and recalling that $\deg \Delta = 3$, we get

$$h_\Delta(f(\cdot)) = 3 \deg f \left[h_Q(\cdot) + O\left(1 + \sqrt{h_Q(\cdot)}\right)\right] + O(1). \tag{6}$$

The canonical height is defined as $\hat{h}(f(\cdot)) := \lim_{N\to\infty} h_\Delta(Nf(\cdot))/N^2$. Hence, passing to the limit on both sides of (6), we deduce

$$\hat{h}(f(P)) = 3 \deg f \left[h_Q(P) + O\left(1 + \sqrt{h_Q(P)}\right)\right]. \qquad \square$$

We remark that this proposition can be obviously extended to an arbitrary $\mathrm{End}(E)$-free submodule G of $\mathrm{Hom}(\mathcal{C}, E)$, finitely generated and such that no non-trivial constant function belongs to G.

Proof of Theorem 1. We recall that the maps x_i are the coordinate morphisms of $\mathcal{C}$ in E^n. Let us consider the $\mathrm{End}(E)$-module $\Gamma := \langle x_1, \dots, x_n\rangle_{\mathrm{End}(E)}$ in $\mathrm{Hom}(\mathcal{C}, E)$. Since $\mathcal{C}$ is not contained in any translate of a proper algebraic subgroup of E^n, the rank of Γ is n. If P is a point in $S_1(\mathcal{C})$ then, by Remark 1, the module $\Gamma_P := \langle x_1(P), \dots, x_n(P)\rangle_{\mathrm{End}(E)}$ has rank at most $n-1$. Thus there exists a non trivial element y in the kernel of the valuation map $v_P : \Gamma \to \Gamma_P$, where v_P is defined by $v_P(\sum \alpha_i x_i) = \sum \alpha_i x_i(P)$.

From Proposition 1 we deduce

$$\hat{h}(y(P)) = 3 \deg y \left(h_Q(P) + O\left(1 + \sqrt{h_Q(P)}\right)\right).$$

Since $\hat{h}(y(P)) = 0$ and $\deg y \neq 0$ we have

$$h_Q(P) \le C\left(1 + \sqrt{h_Q(P)}\right)$$

whence

$$h_Q(P) \le C'.$$

We recall that $\deg x_i \le 3 \deg \mathcal{C}$ so, by Proposition 1 again, we have

$$\hat{h}(x(P)) = \sum_i \hat{h}(x_i(P)) \ll 1. \qquad \square$$

4. – Intersecting with algebraic subgroups of codimension 2

In this section we give a proof of Theorem 2, we recall that E is C.M. in this case. By Theorem 1 the set $S_2(\mathcal{C})$ is of bounded height. Thus, by Northcott's Theorem, it is enough to prove that $S_2(\mathcal{C})$ is defined over a number field of finite absolute degree. The proof of this theorem is organized in different sections.

For positive integers $n > r \geq 0$ we define the set $S_{n-r}(\mathcal{C}) := \bigcup_{\mathrm{cod}(A)\geq n-r} \mathcal{C} \cap A(\overline{\mathbb{Q}})$ where A ranges over all algebraic subgroups of E^n of dimension at most r. Using some geometry of numbers, we shall prove that there exist 'good' integral generators for a Euclidean lattice. For every point $P \in S_2(\mathcal{C})$, the Siegel Lemma will allow us to construct a new abelian subvariety A of E^n, which passes through the point P and whose degree is controlled in terms of the height of the elements of the 'good' basis $g_1, \ldots, g_r$ and of the order NR of the torsion of the coordinate module Γ_P. The degree of A gives an upper bound for the degree of the field $K(P)$ of definition of P. Using a recent result of S. David and M. Hindry we make this upper bound independent of the height of the $g_1, \ldots, g_r$. On the other hand the torsion of Γ_P is defined over $K(P)$, thus we find a lower bound for the degree of $K(P)$ in terms of NR. It will turn out that, if we consider the set $S_{n-r}(\mathcal{C}) := \bigcup \mathcal{C} \cap A(\overline{\mathbb{Q}})$ for $n - r \geq 3$, the statement follows immediately from combining the above upper and lower bounds. However if we consider $S_2(\mathcal{C})$ where the union is taken over all algebraic subgroups of codimension ≥ 2, some difficulties occur. We shall deal with two different situations. In the first one we suppose that there exists a special point g of 'small' height and linearly independent with the 'good' basis $g_1, \ldots, g_r$. Proposition 4 will then give a finer upper bound. If this point does not exist, then a cohomological argument will enable us to refine the upper bound. This will conclude the proof.

For an elliptic curve E with C.M., we consider the order $\mathcal{O}$ of endomorphisms of E as a $\mathbb{Z}$-module of rank 2. In this way we will be able to apply the Siegel Lemma and some results from lattice theory.

LEMMA 2. *Let R be an integral domain and let M be an R-algebra and a free R-module of rank δ. Let τ_i be elements of M such that $M = \tau_0 R + \tau_1 R + \cdots + \tau_{\delta-1} R$. Then the elements $g_1, \ldots, g_r$ of M^m are linearly independent over M if and only if the elements $\tau_0 g_1, \ldots, \tau_0 g_r, \tau_1 g_1, \ldots, \tau_1 g_r, \ldots, \tau_{\delta-1} g_1, \ldots, \tau_{\delta-1} g_r$ are linearly independent over R.*

PROOF. Consider a linear combination $\sum_{j=1,i=0}^{r,\delta-1} \lambda_{ij}(\tau_i g_j) = 0$, with $\lambda_{ij} \in R$ then $\sum_{j=1}^{r}(\sum_{i=0}^{\delta-1} \lambda_{ij}\tau_i) g_j = 0$ with $(\sum_{i=0}^{\delta-1} \lambda_{ij}\tau_i) \in M$. The g_j are M-linearly independent if and only if for each $j = 1, \ldots r$ we have $\sum_{i=0}^{\delta-1} \lambda_{ij}\tau_i = 0$ but the τ_i are a R basis of M, hence $\lambda_{ij} = 0$. □

Let P be a point in $S_2(\mathcal{C})$, then, by the Subgroup Lemma 1, there exist two $\mathcal{O}$-linearly independent forms $\sum_{i=1}^{n} \alpha_i \pi_i$ and $\sum_{i=1}^{n} \alpha'_i \pi_i$, vanishing on an algebraic subgroup A of E^n, such that $\sum_{i=1}^{n} \alpha_i x_i(P) = 0$ and $\sum_{i=1}^{n} \alpha'_i x_i(P) = 0$.

From Lemma 2, four $\mathbb{Z}$-linearly independent equations are associated to these two $\mathcal{O}$-linearly independent equations. Namely the equations $\sum_{i=1}^{2n} m_{ji}x_i(P) = 0$ and $\sum_{i=1}^{2n} m'_{ji}x_i(P) = 0$ for $j = 1, 2$ where we have set $x_{n+i}(P) := \tau x_i(P)$ and $\alpha_i = m_{1,i} + m_{1,n+i}\tau$, $\alpha'_i = m'_{1,i} + m'_{1,n+i}\tau$, $\tau\alpha_i = m_{2,i} + m_{2,n+i}\tau$, $\tau\alpha'_i = m'_{2,i} + m'_{2,n+i}\tau$. So the module $\Gamma_P := \langle x_1(P), \dots, x_{2n}(P)\rangle_{\mathcal{O}}$ has rank r as $\mathcal{O}$-module and it has rank $2r$ as $\mathbb{Z}$-module.

4.1. – Some Geometry of Numbers

I am grateful to Prof. E. Bombieri who communicated the following proof of this lemma:

LEMMA 3. *Let Γ be a finitely generated subgroup of E of rank r over $\mathbb{Z}$. Then there are elements $g_1, \dots, g_r \in \Gamma$ which generate a subgroup isomorphic to $\Gamma/\mathrm{Tor}(\Gamma)$ and such that*

$$\hat{h}\left(\sum a_i g_i\right) \geq c(r)\left(\sum |a_i|^2 \hat{h}(g_i)\right)$$

with $a_i \in \mathbb{Z}$ and $c(r) = 2^{2r-2}/r^2(r!)^4$.

The constant can be deduced by Theorem 1.1 of Schlickewei [17]

PROOF. From [23] Proposition 9.6, we know that the height function $\hat{h}$ extends on $\Gamma_{\mathbb{R}} := \Gamma \otimes_{\mathbb{Z}} \mathbb{R}$ to the square of a norm. In particular there is an inner product $\langle P, Q\rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$ and $||P||^2 = 2\hat{h}(P)$. The group $\Gamma/\mathrm{Tor}(\Gamma)$ is a lattice in $\Gamma_{\mathbb{R}}$. Let $\tilde{p}_1, \dots, \tilde{p}_r$ be liftings on Γ of integral generators $p_1, \dots, p_r$ of $\Gamma/\mathrm{Tor}(\Gamma)$. We identify $\mathbb{R}^r$ and $\Gamma_{\mathbb{R}}$ via the isomorphism defined by the choice of the basis $p_1, \dots, p_r$. Let $V := \mathrm{vol}(p_1, \dots p_r)$ be the volume of a fundamental domain of $\Gamma/\mathrm{Tor}(\Gamma)$. Let $B := \{x \in \mathbb{R}^r : ||x|| \leq 1\}$ be the closed ball of radius 1. Let $\lambda_1, \dots \lambda_r$ be the successive minima of B with respect to the lattice $\Gamma/\mathrm{Tor}(\Gamma)$. By Minkowski's second fundamental Theorem we have

$$\lambda_1, \dots \lambda_r \mathrm{vol}(B) \leq 2^r V. \tag{7}$$

A Theorem of Mahler, [5] Section V, Lemma 8, shows that there is a basis $v_1, \dots, v_r$ of $\Gamma/\mathrm{Tor}(\Gamma)$ such that

$$\lambda_i \leq ||v_i|| \leq \max(1, i/2)\lambda_i. \tag{8}$$

Let $v_i = \sum_{j=1}^{r} v_{ij} p_i = (v_{i1}, \dots, v_{ir})$. Since $v_1, \dots, v_r$ is a basis we have

$$|\det(v_1, \dots, v_r)| = V. \tag{9}$$

We write

$$w_i = \frac{v_i}{||v_i||} \tag{10}$$

and we define B^* to be

$$B^* = \{y \in \mathbb{R}^r : ||y_1 w_1 + y_2 w_2 + \cdots + y_r w_r|| \leq 1\}, \tag{11}$$

where $y = y_1 p_1 + y_2 w_2 + \cdots + y_r p_r$. Since B is the image of B^* by the linear map $y = y_1 p_1 + y_2 p_2 + \cdots + y_r p_r \mapsto y_1 w_1 + y_2 p_2 + \cdots + y_r w_r$, we have, by (7), (8), (9) and (10), the upper bound

$$\operatorname{vol}(B^*) = \frac{\operatorname{vol}(B)}{|\det(w_1, w_2, \ldots, w_r)|} = \frac{\operatorname{vol}(B)}{V} \prod_{i=1}^{r} ||v_i|| \leq 2r!. \tag{12}$$

A lower bound is obtained as follows. Let e_j, $j = 1, \ldots, r$ be the standard basis in $\mathbb{R}^r$. Let y be a boundary point of B^*. Then for each i the set B^* contains the convex closure of the points $\pm y$ and $\pm e_j$, $j = 1, \ldots, i-1, i+1, \ldots r$. This set is the union of 2^r simplices of volume $|y_i|/r!$. Therefore we get the lower bound

$$|y_i| \frac{2^r}{r!} \leq \operatorname{vol}(B^*),$$

which, combined with (12), gives

$$\sum_{i=1}^{r} |y_i| \leq 2^{-r+1} r (r!)^2 \left|\left| \sum_{i=1}^{r} y_i w_i \right|\right|, \tag{13}$$

where the norm on the right is 1 because y is a boundary point of B^*. Now, from (10), we may rewrite (13) as

$$\left|\left| \sum_{i=1}^{r} x_i v_i \right|\right| \geq c(r) \sum_{i=1}^{r} |x_i| \cdot ||v_i||, \tag{14}$$

where $x_i = y_i/||v_i||$ and $c(r) = 2^{r-1}/r(r!)^2$. Finally, we define generators g_i for a subgroup $\overline{\Gamma}$ of Γ isomorphic to $\Gamma/\mathrm{Tor}(\Gamma)$, by setting

$$g_i = \sum_{j=1}^{r} v_{ij} \tilde{p}_j$$

where $v_i = (v_{i1}, \ldots, v_{ir})$. Thus we have

$$2\hat{h}\left(\sum_{i=1}^{r} a_i g_i\right) = ||a_i v_1 + \cdots + a_r v_r||^2.$$

Since $||v_i||^2 = 2\hat{h}(g_i)$, Lemma 3 follows from (14). $\square$

PROPOSITION 2. *Let P be a point of $S_{n-r}(\mathcal{C})$ for some integers $0 \leq r < n$. Let $K(P)$ be the field of definition of P. We consider the module $\Gamma_P := \langle x_1(P), \ldots, x_{2n}(P)\rangle_{\mathbb{Z}}$ of rank 2r over $\mathbb{Z}$, generated by the coordinate functions and their conjugates under τ. Then there exist $\mathbb{Z}$-linearly independent elements $g_1, \ldots, g_{2r} \in \Gamma_P$ such that*

1. *The g_i are defined over $K(P)$.*
2. *The set of points $g_1, \ldots, g_r$ respectively $g_{r+1}, \ldots, g_{2r}$ are $\mathcal{O}$-linearly independent.*
3. *The subgroup $\overline{\Gamma}_P = \langle g_1, \ldots, g_{2r}\rangle_{\mathbb{Z}}$ of Γ_P is isomorphic to $\Gamma_P/\mathrm{Tor}(\Gamma_P)$, moreover* $\hat{h}\big(\sum_{i=1}^{2r} a_i g_i\big) \geq c(r)\big(\sum_{i=1}^{2r} |a_i|^2 \hat{h}(g_i)\big)$.
4. *There exist torsion points P_1 and P_2 of exact order N respectively R with $R|N$, such that* $\mathrm{Tor}(\Gamma_P) = \langle P_1, P_2\rangle_{\mathbb{Z}} \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/R\mathbb{Z}$. *The group* $\mathrm{Tor}(\Gamma_P)$ *is $\mathcal{O}$ invariant and* $K(\mathrm{Tor}(\Gamma_P)) \subset K(P)$.

PROOF. (1) The g_i are a $\mathbb{Z}$ linear combination of the $x_i(P)$ which are in $K(P)$ so the g_i are defined over $K(P)$ as well.

(2) Let $\overline{\Gamma}_P$ be the free part of Γ_P, then $\overline{\Gamma}_P = \Gamma_1 + \tau\Gamma_1$. Consider a $\mathbb{Z}$-basis $g_1, \ldots, g_r$ of Γ_1. The elements $g_{r+1} = \tau g_1, \ldots, g_{2r} = \tau g_r$ are a $\mathbb{Z}$-basis of $\tau\Gamma_1$ and clearly the g_i fulfill the required conditions.

(3) Let $g_1, \ldots, g_r$ be a basis of Γ_1 given by Lemma 3. Since the sphere is compact and the spaces $\Gamma_1 \otimes \mathbb{R}$, $\tau\Gamma_1 \otimes \mathbb{R}$ have empty intersection, we get $\langle g_i, \tau g_j\rangle/\|g_i\|\,\|\tau g_j\| \leq c(r,\tau) < 1$, with $c(r,\tau)$ a constant depending on τ and r. Then the basis $g_1, \ldots, g_r, g_{r+1} = \tau g_1, \ldots, g_{2r} = \tau g_r$ satisfies the required condition.

(4) STEP I: Study of subgroups of $E[N]$.

The lattice period Λ associated to E is a projective $\mathcal{O}$-module of rank 1. In particular $E[N] \cong \Lambda/N\Lambda \cong \prod \Lambda_{\mathfrak{p}}/N\Lambda_{\mathfrak{p}} \cong \prod \mathcal{O}_{\mathfrak{p}}/N\mathcal{O}_{\mathfrak{p}} \cong \mathcal{O}/N\mathcal{O}$, where $\mathfrak{p}$ is a prime ideal, (see [20] §1). Let T_1 be a torsion point of exact order N (i.e. so that $N \cdot T = 0$ but $kT \neq 0$ for all divisors k of N). We are going to proof that the point τT_1 has order N' with $N/N' \ll 1$. We can write T_1 as $a + b\tau$ in $\mathcal{O}/N\mathcal{O}$ with the greatest common divisor (N, a, b) being 1. Let $\tau^2 = \alpha + \beta\tau$, then $\tau T_1 = b\alpha + (a + b\beta)\tau$ has order $N' = N/s$ with $s = (N, b\alpha, a + b\beta)$. Let $s_1 = (s, b)$, then $s_1|a$ and $s_1|N$, thus $s_1|(N, a, b) = 1$. It follows that $s_1 = 1$ and so $s|\alpha$. The order of τT_1 is at least $N/(N, \alpha)$, α is the real part of τ^2 and so a constant of the problem.

We want now to study the subgroup of $E[N]$ generated by $T_1, \tau T_1$. Let T_2 be a torsion point of exact order N such that $E[N] = \langle T_1, T_2\rangle_{\mathbb{Z}}$. Then $\tau T_1 = aT_1 + bT_2$ for integers a and b, thus $\langle T_1, \tau T_1\rangle = \langle T_1, bT_2\rangle$. Let $R = N/(N, b)$ if $b \neq 0$ or $R = 1$ if $b = 0$, then $\langle T_1, \tau T_1\rangle \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/R\mathbb{Z}$.

STEP II: Study of $\mathrm{Tor}(\Gamma_P)$.

We consider the equations

$$x_i(P) = \sum_{j=1}^{2r} a_{ij} g_j + T_i, \qquad i = 1, \ldots 2n \tag{15}$$

where $a_{ij} \in \mathbb{Z}$ and the T_i are torsion points such that $T_{n+i} = \tau T_i$. Since $\overline{\Gamma}_P$ is projective then $\Gamma_P/\overline{\Gamma}_P \cong \mathrm{Tor}(\Gamma_P)$, thus the T_i are generators of $\mathrm{Tor}(\Gamma_P)$. Let N_i be the order of the torsion points T_i for $i = 1, \ldots, r$ (or equivalently for $i = r+1, \ldots, 2r$). Let N be the smallest integer such that $T_i \in E[N]$ for all $i = 1, \ldots, r$, i.e. $N = \mathrm{l.c.m.}(N_1, \ldots N_r)$ is the least common multiple of the N_i. We decompose $N = p_1^{l_1} \ldots p_k^{l_k}$ with p_i different prime numbers. Then for some positive integer $j \le r$ and for any $1 \le i \le k$ we have $p_i^{l_i} | N_j$ and $(p, N_j/p^{l_i}) = 1$. We define $R_i := \frac{N_j}{p_i^{l_i}} T_j$, thus, for $i = 1, \ldots, k$, the torsion points R_i have coprime exact order $p_i^{l_i}$. From the Chinese Reminder Theorem the point $P_1 := \sum_{i=1}^n R_i$ has exact order N. By relation (15) $\mathrm{Tor}(\Gamma_P) = \langle P_1, \tau P_1 \rangle$. The assertion follows from Step I.

Since $x_i(P)$ and g_i are defined over $K(P)$, also P_1 and P_2 are defined over $K(P)$, therefore $K(\mathrm{Tor}(\Gamma_P)) \subset K(P)$. $\square$

4.2. – Estimate for the Degree of $K(P)$

For every point $P \in S_2(\mathcal{C})$ we construct an algebraic subgroup of E^n passing through P whose degree is bounded in terms of the order of the torsion of Γ_P and of the height of the elements of the basis g_i of $\overline{\Gamma}_P$ defined by Proposition 2.

The g_i are $\mathbb{Z}$-generators of the free part $\overline{\Gamma}_P$ of Γ_P, so we can write

$$x_i(P) = \sum_{j=1}^{2r} a_{ij} g_j + T_i, \qquad i = 1, \ldots, 2n \tag{16}$$

with $a_{ij} \in \mathbb{Z}$ and N-torsion points T_i such that $T_{n+i} = \tau T_i$ for $i = 1, \ldots, n$. By Proposition 2 (3) and Theorem 1 we have

$$|a_{ij}|^2 \hat{h}(g_j) \ll \hat{h}(x_i(P)) \ll h(P) \ll 1 \tag{17}$$

where the constants involved depend only on n, E and $\mathcal{C}$. Therefore, setting

$$\nu_j = (a_{1j}, \ldots, a_{nj}) \tag{18}$$

and defining $|\nu_j| = \max_i\{|a_{ij}|, 1\}$, we see that

$$\hat{h}(g_j) \ll |\nu_j|^{-2}. \tag{19}$$

Proposition 3. *Let P be a point of $S_{n-r}(\mathcal{C})$. There exists a proper algebraic subgroup A of E^n defined over K and passing through P such that*

$$\sharp A \cap \mathcal{C} \le 3^3 |\tau|^2 \deg \mathcal{C} \left(N R \prod_{j=1}^{2r} |\nu_j| \right)^{\frac{1}{n-r}}$$

where the ν_j are defined in (18).

PROOF. From Proposition 2 (4) there exist torsion points P_1 and P_2 in Γ_P of exact order N, respectively R which are $\mathbb{Z}$-generators of $\mathrm{Tor}(\Gamma_P)$. Then we can write

$$T_i = l_i^1 P_1 + l_i^2 P_2$$

whit $l_i^j \in \mathbb{Z}$. We apply Siegel's Lemma as in [2] to the $2r+2$ linear forms $\sum_{i=1}^{2n} a_{ij} b_i = 0$, for $j = 1, \dots, 2r$, and $\sum_{i=1}^{2n} l_i^1 b_i - N b_{2n+1} = 0$, $\sum_{i=1}^{2n} l_i^2 b_i - R b_{2n+2} = 0$, in the $2n+2$ variables b_i. Then we get a nonzero vector $b = (b_1, \dots, b_{2n}) \in \mathbb{Z}^{2n}$ such that

$$\begin{cases} \sum_{i=1}^{2n} a_{ij} b_i = 0 \\ \sum_{i=1}^{2n} l_i^1 b_i \equiv 0 \bmod N \\ \sum_{i=1}^{2n} l_i^2 b_i \equiv 0 \bmod R \end{cases} \tag{20}$$

and

$$\max |b_i| \leq \left(N R \prod_{j=1}^{2r} |\nu_j| \right)^{\frac{1}{2n-2r}} \tag{21}$$

From (16) and (20) we obtain

$$\sum_{i=1}^{n} \beta_i x_i(P) = 0$$

where $\beta_i = b_i + \tau b_{n+i}$.

Then the equation

$$\sum_{i=1}^{n} \beta_i x_i = 0 \tag{22}$$

gives a proper algebraic subgroup A of E^n defined over K of codimension 1 which contains the point P.

Let us consider the morphism $\Sigma : \mathcal{C} \to E$ that sends a point $Q \in \mathcal{C}$ to the linear combination $\sum_{i=1}^{r} \beta_i x_i(Q)$, we deduce that the order of the intersection $A \cap \mathcal{C}$ is the degree of Σ. Since the degree is the square of a norm we have that $\deg \Sigma \leq \sum_i 3|\beta_i|^2 \deg x_i$ which in turn is estimated by $\deg \Sigma \leq 3^3 |\tau|^2 \deg \mathcal{C} \max |b_i|^2$ because $|\beta_i|^2 \leq 3(|b_i|^2 + |\tau b_{r+i}|^2)$ and by the Bézout Theorem $\deg x_i \leq 3 \deg \mathcal{C}$. Now the statement follows from (21). $\square$

COROLLARY 1. *Let P be a point in $S_{n-r}(\mathcal{C})$. Let $K(P)$ be the field of definition of the point P. Then*

$$d := [K(P):\mathbb{Q}] \ll \left(NR \prod_{j=1}^{2r} |\nu_j| \right)^{\frac{1}{n-r}} \tag{23}$$

PROOF. Let A be the algebraic subgroup given by Proposition 3 . Since P belongs to the intersection $A \cap \mathcal{C}$, then all its conjugates are in $A \cap \mathcal{C}$ for a certain field of definition of $\mathcal{C}$. Then $[K(P):\mathbb{Q}] \ll \sharp(A \cap C)/[K:\mathbb{Q}]$. □

We are going to make the upper bound (23) for $d := [K(P):\mathbb{Q}]$ independent from $\prod_{j=1}^{2r} |\nu_j|$. Then we will find a lower bound for the degree d which, combined with the above upper bound, will induce an absolute bound for the variables NR and d.

PROPOSITION 4. *Let $Q_1, \dots Q_r$ be $\mathcal{O}$-linearly independent points in E. Let D be the degree of the field of definition of those points. Then*

$$D^{-1-\varepsilon} \ll \prod_{i=1}^{r} \hat{h}(Q_i).$$

PROOF. We can assume that $\hat{h}(Q_1) \le \hat{h}(Q_i)$ for $i = 2, \dots, r$. Let us consider integers $\delta_1 = 1, \delta_2, \dots, \delta_r$ and points $Q'_1, \dots, Q'_r$ defined over K', satisfying

$$Q'_1 = Q_1, \;\; \delta_2 Q'_2 = Q_2, \dots, \delta_r Q'_r = Q_r \tag{24}$$

and

$$\hat{h}(Q_1) \le \hat{h}(Q'_i) \le 4\hat{h}(Q_1). \tag{25}$$

For example we can set $\delta_i := \left[\sqrt{\frac{x}{y}}\right]$ where $x := \hat{h}(Q_i)$, $y := \hat{h}(Q_1)$ and $[\cdot]$ is the integer part of a real number. We easily see that (24) is equivalent to $\left[\sqrt{\frac{x}{y}}\right] \le \sqrt{\frac{x}{y}} \le 2\left[\sqrt{\frac{x}{y}}\right]$ which is trivially true since $x \ge y$. Then

$$D' := \deg K' \le D \prod_{i=2}^{r} \delta_i^2. \tag{26}$$

Since the points $Q_1, \dots Q_r$ are $\mathcal{O}$-linearly independent points in E then also the points $Q'_1, \dots, Q'_r$ are $\mathcal{O}$-linearly independent. Thus $(Q'_1, \dots, Q'_r) \in E^r$, as well as $(Q_1, \dots Q_r)$, is a point of infinite order modulo all proper abelian subvarieties of E^r.

Now we need a recent result of S. David and M. Hindry.

LEMMA 4 ([7] Theorem 1.3). *Let A be an abelian variety of dimension g with complex multiplication defined over a number field K and $\mathcal{L}$ a symmetric ample line bundle on A. Let P be a point on A of infinite order modulo all abelian subvarieties of $A(\overline{K})$ then*

$$h_{\mathcal{L}}(P) \geq C(A, \mathcal{L}) D^{-\frac{1}{g}} \left(\frac{\log\log(3D)}{\log(3D)} \right)^{\kappa(g)}$$

where D is the degree of the field of definition of P, $h_{\mathcal{L}}$ is the height defined by the divisor associated to $\mathcal{L}$, $C(A, \mathcal{L})$ is a positive constant depending only on A and $\mathcal{L}$, and κ is a positive constant depending only on g.

After replacing $(\log\log(3D)/\log(3D))$ by $(D)^{-\varepsilon}$, for ε small enough, Lemma 4 tells us that

$$D'^{-\frac{1}{r}-\varepsilon} \ll \hat{h}(Q'_1, \ldots, Q'_r).$$

The height of $(Q'_1, \ldots, Q'_r)$ is, by definition, the sum of the heights of its components, hence, using the upper bound (26) for D', we deduce

$$\left(D \prod_{i=1}^{r} \delta_i^2 \right)^{-\frac{1}{r}-\varepsilon} \ll \sum_{i=1}^{r} \hat{h}(Q'_i),$$

and by relation (25) we have

$$D^{-1-\varepsilon} \ll \hat{h}^r(Q_1) \left(\prod_{i=1}^{r} \delta_i^2 \right)^{1+\varepsilon}.$$

Using once more relations (24) and (25) we have

$$D^{-1-\varepsilon} \ll \prod_{i=1}^{r} \hat{h}(Q_i)$$

for ε small enough. □

COROLLARY 2. *Let $P \in S_{n-r}(\mathcal{C})$, let N be the smallest integer that annihilates the torsion of Γ_P and d the degree of the field $K(P)$ of definition of P. Then*

$$(NR)^{1-\varepsilon} \ll d \ll (NR)^{\frac{1}{(n-r-1-\varepsilon)}}. \tag{27}$$

PROOF. Let $g_1, \ldots g_{2r}$ be the integral basis of the lattice $\overline{\Gamma}_P$ defined by Proposition 2 . Then the set of points $g_1, \ldots, g_r$ respectively $g_{r+1}, \ldots, g_{2r}$ are

$\mathcal{O}$-linearly independent points of $E(K(P))$. Applying Proposition 4 to these two sets of points, we deduce

$$d^{-1-\varepsilon} \ll \prod_{i=1}^{r} \hat{h}(g_i)$$

(28)

$$d^{-1-\varepsilon} \ll \prod_{i=r+1}^{2r} \hat{h}(g_i)$$

where $d := [K(P) : \mathbb{Q}]$. Multiplying left and right sides of these two relations and using (19) we have

$$\prod_{i=1}^{2r} |\nu_i| \ll d^{1+\varepsilon}. \tag{29}$$

From Corollary 1 and (29), we deduce

$$\left(\prod_{i=1}^{2r} |\nu_i|\right)^{n-r-1-\varepsilon} \ll (NR)^{1+\varepsilon} \tag{30}$$

as well as

$$d \ll (NR)^{\frac{1}{(n-r-1-\varepsilon)}}. \tag{31}$$

On the other hand, by Proposition 2 (4), the torsion $\mathrm{Tor}(\Gamma_P)$ is a finite group defined over $K(P)$ and its $\mathcal{O}$ invariant. From Corollary 3 below, we see that $\Phi(N)\Phi(R) \ll [K(\mathrm{Tor}(\Gamma_P)) : \mathbb{Q}]$, where Φ is the Euler's function, then

$$(NR)^{1-\varepsilon} \ll d \tag{32}$$

and we conclude the proof. □

4.3. – The Easy Cases

The case $n - r \geq 3$ follows immediately from Corollary 1, because $(1 - \varepsilon) - 1/(n - r - 1 - \varepsilon) > 0$ for $n - r \geq 3$ so N and d are uniformly bounded.

For $r = n-2$, we shall distinguish two cases. Suppose that g_1 has minimal height among $g_1, \dots g_r$. If a conjugate of g_1 is $\mathcal{O}$-linearly independent from $g_1, \dots, g_{n-2}$ then the following lemma solves the problem.

Lemma 5. *Let $g_1, \dots, g_{n-2}$ be the $\mathcal{O}$-basis of $\overline{\Gamma}_P$ fixed above and assume that $\hat{h}(g_1) \leq \hat{h}(g_i)$ for $i = 1, \dots, n-2$. Let g be a conjugate of g_1 under* $\mathrm{Gal}(\overline{K}/K)$*, which is $\mathcal{O}$-linearly independent from $g_1, \dots, g_{n-2}$. Then NR and d are bounded independently on P.*

Proof. The field of definition of $\mathrm{Tor}(\Gamma_P)$ is normal (Corollary 3 below), so it is contained in $K(P, g)$. Using Corollary 2 we have

$$[K(P, g) : \mathbb{Q}] \leq \frac{[K(P, g_1) : \mathbb{Q}]^2}{[K(\mathrm{Tor}(\Gamma_P)) : \mathbb{Q}]} \leq (NR)^{1+\varepsilon}.$$

Let $r = n - 2$. Note that if $g, g_1, \dots g_r$ are $\mathcal{O}$-linearly independent then also $g, g_{r+1}, \dots, g_{2r}$ are $\mathcal{O}$-linearly independent. Applying Proposition 4 to $g, g_1, \dots, g_r$ and $g, g_{r+1}, \dots, g_{2r}$ respectively, we get

$$(RN)^{-1-\varepsilon} \ll \hat{h}(g_1) \cdots \hat{h}(g_r)\hat{h}(g)$$

$$(RN)^{-1-\varepsilon} \ll \hat{h}(g_{r+1}) \cdots \hat{h}(g_{2r})\hat{h}(g)$$

and so

$$(RN)^{-2-\varepsilon} \ll \hat{h}(g_1) \cdots \hat{h}(g_{2r})\hat{h}(g)^2.$$

By assumption, the height of g is minimal. Using (19) we deduce

$$(RN)^{(-1-\varepsilon)2r/2(r+1)} \ll \left(\hat{h}(g_1) \cdots \hat{h}(g_{2r})\right)^{1/2} \ll \left(\prod_{i=1}^{2r} |\nu_i|\right)^{-1},$$

so

$$\left(\prod_{i=1}^{2r} |\nu_i|\right)^{1/2} \ll (RN)^{r+\varepsilon/2(r+1)}.$$

By Corollary 1 and 2 we deduce

$$d \ll (NR)^{\frac{(2r+1}{2(r+1)}+\varepsilon},$$

which combined with the lower bound of Corollary 2 gives

$$(NR)^{1-\varepsilon} \ll d \ll (NR)^{\frac{2r+1}{2(r+1)}+\varepsilon}.$$

We see that $2(1-\varepsilon)(r+1) - (2r+1) - 2\varepsilon(r+1)$ is always larger than zero if $\varepsilon(r)$ is small enough. Thus NR and consequently d are uniformly bounded. □

4.4. – The Difficult Case

Suppose that $r = n-2$, $\hat{h}(g_1) \leq \hat{h}(g_i)$ for $i = 1, \dots, r$ and that $g, g_1, \dots, g_r$ are linearly dependent for all conjugates g of g_1 under the Galois group $\mathrm{Gal}(\overline{K}/K)$. This last case is more complicated and requires the study of the cohomology of the extensions $L(E[N])$ with L a number field.

LEMMA 6. *Let E be an elliptic curve defined over $\overline{\mathbb{Q}}$. Let $g_1, \ldots, g_r$ be $\mathcal{O}$-linearly independent algebraic points of E. Let p be a point of $E(\overline{\mathbb{Q}})$ such that $\sigma(p), g_1, \ldots, g_r$ are $\mathcal{O}$-linearly dependent for every $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Then there is a positive integer h such that $h \cdot p$ is defined over a number field of degree at most $d(r)$ over K, with $d(r)$ depending only on r.*

PROOF. If E is C.M. then the points $\sigma(p), g_1, \ldots g_r, \tau g_1, \ldots \tau g_r$ are $\mathbb{Z}$-linearly dependent. In fact by Lemma 2 we know that the equation $\beta\sigma(p) = \sum_{i=1}^r \alpha_i g_i$ with $\beta, \alpha_i \in \mathcal{O}$ give rise to the two equations $b\sigma(p) + b'\tau\sigma(p) = \sum_{i=1}^r a_i g_i + a'_i \tau g_i$ and $c\sigma(p) + c'\tau\sigma(p) = \sum_{i=1}^r d_i g_i + d'_i \tau g_i$ with coefficients in $\mathbb{Z}$ and $b + b'\tau = \tau(c + c'\tau)$. Since τ and 1 are $\mathbb{Q}$-linearly independent we have $bc' - cb' \neq 0$. Thus $(bc' - cb')\sigma(p) = \sum_{i=1}^r (c'a_i - b'd_i)g_i + (c'a'_i - b'd'_i)\tau g_i$. If E is non C.M. then the points $\sigma(p), g_1, \ldots g_r$ are $\mathbb{Z}$-linearly independent by assumption. Now, the proof follows exactly the proof of Lemma 5 in [1], for convenience we recall it. Let Λ be the $\mathcal{O}$-module generated by all conjugates of p under the Galois group $\mathrm{Gal}(\overline{K}/K)$. Then, from what above, Λ is a $\mathbb{Z}$-module of rank $s \leq 2r$ if E is C.M. and of rank $s \leq r$ if E is non C.M. Let $p_1, \ldots, p_s$ be $\mathbb{Z}$-linearly independent points in Λ. Then we get a representation ρ of $\mathrm{Gal}(\overline{K}/K)$ on $GL_s(\mathbb{Z})$ by sending σ in the $s \times s$ matrix $(m^\sigma_{i,j})_{i,j}$, where $\sigma(p_i) = \sum_j m^\sigma_{i,j} p_j + T^\sigma_i$ for some torsion point T^σ_i. Since all σ which fix the elements p_i for $i = 1, \ldots, s$ belongs to the kernel of ρ, this kernel has then finite index and so ρ has finite image. By [4] Note G, pp.479-484, the order of any finite subgroup of $GL_s(\mathbb{Z})$ has order bounded just in terms of s. There exists a positive integer h such that $hT^\sigma_i = 0$ for every σ and i. Hence the kernel of ρ fixes hp and so hp is defined over a number field L whose degree is bounded just in terms of s. □

LEMMA 7. *Let E be an elliptic curve defined over $\overline{\mathbb{Q}}$ and let u be a point of E defined over $L(E[N])$. Suppose that there exists a positive integer h such that hu is defined over L. Then, there exists a torsion point T and an integer k such that $ku + T$ is defined over L and such that $\Phi(k) \leq [L : \mathbb{Q}]$, where $\Phi(\cdot)$ is the Euler's function.*

PROOF. Let $\mathcal{I}$ be the ideal in $\mathbb{Z}$ consisting of the integers t such that $tu + T$ is defined over L for some torsion point T. Let k be the positive generator of $\mathcal{I}$. Replacing u by $u + T$ for a certain torsion point T, we can suppose that ku is defined over L. Note that, upon replacing N by a larger constant, we may suppose that the new u is still defined over an extension of the type $L(E[N])$. Let $G_N = \mathrm{Gal}(L(E[N])/L)$ be the Galois group of $L(E[N])$ over L, then the morphism $\zeta : G_N \to E[k]$ given by $\sigma \mapsto \sigma(u) - u$ is a cocycle in fact $\sigma\tau(u) - u = \sigma(\tau(u) - u) + \sigma(u) - u$. By Proposition 7 below, we know that $m^2 H^1(G_N, E[k]) = 0$ with m^2 depending only on E and L and $L(E[m^2]) = L$. So $m^2\zeta$ is a coboundary, i.e. there exists a k-torsion point T such that $m^2(\sigma(u) - u) = \sigma T - T$ or $\sigma(m^2 u - T) = m^2 u - T$ for every $\sigma \in G_N$. That implies that $m^2 u - T$ is defined over L. Then $m^2 \in \mathcal{I}$ thus $k | m^2$ and, since $L = L(E[m])$, we deduce that $\Phi(k) \leq [L : \mathbb{Q}]$. □

CONCLUSION. We can now conclude also the case $r = n - 2$, $\hat{h}(g_1) \leq \hat{h}(g_i)$, for $i = 1, \ldots, 2r$ and $\sigma(g_1), g_1, \ldots, g_r$ linearly dependent for every $\sigma \in \mathrm{Gal}(\overline{K}/K)$. By Lemma 6 there exists an integer h such that hg_1 is defined over a field L of degree at most $d(r)$ over K, where K is a field of definition of E and its j-invariant. We define $u := \sum_{\sigma \in G} \sigma(g_1)$ with $G := \mathrm{Gal}(L(P)/L(\mathrm{Tor}(\Gamma_P)))$. Since every conjugate of g_1 is of the form $g_1 + T'$ for a h-torsion point we have

$$u = ag_1 + T''$$

where T'' is a h torsion point and $a = [L(P) : L(\mathrm{Tor}(\Gamma_P))]$. Recall that $\Phi(N)\Phi(R) \ll [K(\mathrm{Tor}(\Gamma_P)) : \mathbb{Q}]$. Now using Corollary 2 we have

$$[L(P) : L(\mathrm{Tor}(\Gamma_P))] \leq [K(P) : K(\mathrm{Tor}(\Gamma_P))] \ll (NR)^{\frac{1}{(1-\varepsilon)} - (1-\varepsilon)} \leq (NR)^{\varepsilon}.$$

Note that hu is defined over L and u is defined over $L(\mathrm{Tor}(\Gamma_P))$. Applying Lemma 7, we deduce that there exist a torsion point T and an integer k such that $ku + T$ is defined over L. Since g_1 is not torsion, the point $ku + T$ can not be torsion. Moreover, the absolute degree of L depends only on n. Thus, by Northcott's Theorem, we have $\hat{h}(ku + T) \geq c > 0$, where c is a constant depending only on E and n. In particular

$$\hat{h}(g_1) = \frac{\hat{h}(ku + T)}{k^2 a^2} \geq c/(k^2[L(P) : L(\mathrm{Tor}(\Gamma_P))]^2) \gg (NR)^{-\varepsilon}.$$

This relation, combined with (19) and Corollary 1 gives $d \ll (NR)^{\frac{1+r\varepsilon}{2}}$. But we know from Corollary 2 that $(NR)^{1-\varepsilon} \ll d$. Therefore $d = \deg K(P)$ is uniformly bounded.

5. – The non-Complex Multiplication Case

In this section we are going to prove Theorem 3. The proof uses the same method of the C.M. cases. The Proposition 4 is replaced by Proposition 5. The lower bound for the height of points in E given by D. Masser in Lemma 8 is worse that the lower bound given by S. David and H. Hindry in Lemma 4. This is the reason of a weaker result in the non-C.M. case.

Let P be a point of $S_{n-r}(\mathcal{C})$. We consider the coordinate module $\Gamma := \langle x_1, \ldots, x_n \rangle_{\mathbb{Z}}$ of rank n over $\mathbb{Z}$ and the module $\Gamma_P := \langle x_1(P), \ldots, x_n \rangle_{\mathbb{Z}}$ of rank r over $\mathbb{Z}$. Let $K(P)$ be the field of definition of P. In view of Proposition 2 we can choose generators $g_1, \ldots, g_r$ of Γ_P defined over $K(P)$ such that $\overline{\Gamma}_P = \langle g_1, \ldots, g_r \rangle_{\mathbb{Z}}$ is isomorph to $\Gamma_P/\mathrm{Tor}(\Gamma_P)$. Let

$$x_i = \sum a_{ij} g_j + T_i$$

with $a_{ij} \in \mathbb{Z}$ and T_i torsion points defined over $K(P)$. Let N be the smallest annihilator of $\mathrm{Tor}(\Gamma_P)$. Then a linear combination of the T_i gives a torsion point T of exact order N defined over $K(P)$. Then $\mathrm{Tor}(\Gamma_P) \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/R\mathbb{Z}$ for an integer $R|N$. From relations (36) and (37) we see that $\Phi(R)^2\Phi(N)^2 \ll [K(P):\mathbb{Q}]$, whit Φ the Euler's function. Thus we find the lower bound

$$(RN)^{2-\varepsilon} \ll d = [K(P):\mathbb{Q}]. \tag{33}$$

In analogy to Proposition 3 and Corollary 1 we can find an algebraic subgroup A of E^n passing through P and of bounded degree. This bound induces the upper bound

$$d := [K(P):\mathbb{Q}] \ll \left(RN \prod_{j=1}^{r} |\nu_j| \right)^{\frac{2}{n-r}} \tag{34}$$

where $|\nu_j| = \max_i |a_{ij}|$.

In order to relate d and $\prod_{j=1}^{r} |\nu_j|$ we need to use a result of Masser which induces the best known lower bound for the height of independent points of a non C.M. elliptic curve in terms of their degree.

PROPOSITION 5. *Let $g_1, \dots, g_r$ be $\mathbb{Z}$-linearly independent points of a non C.M. elliptic curve E defined over $\overline{\mathbb{Q}}$. Let D be the degree of their field of definition. Then*

$$\prod_{i=1}^{r} \hat{h}(g_i) \gg \frac{1}{D^{r+2} \log D^2}$$

PROOF. We recall the result of Masser and we show how to deduce our proposition from it.

LEMMA 8 ([12], Theorem). *There are positive effective constants C and C' depending only on the field of definition K and on the height of the elliptic curve E, such that for any $D \geq 1$ and any extension L of K of relative degree at most D, we have*

$$\sharp \left\{ P \in E(L) : \hat{h}(P) \leq \frac{C}{D} \right\} \leq C' D \log D.$$

Without loss of generality we can suppose $\hat{h}(g_i) < 1/D$. Let

$$h(g_i) = \frac{1}{D^{1+a_i}} \tag{35}$$

with $a_i \in \mathbb{R}$. We consider the set L of points of E

$$L = \left\{ \sum_{j=1}^{r} l_j g_j \ \text{ such that } \ l_j \in \mathbb{Z} \ \text{ and } \ |l_j| \leq D^{a_j/2} \right\}.$$

The height of each point in L is then smaller than $1/D$, thus from Masser's result we deduce that there exists a constant C_2 such that

$$|L| \leq C_2 D \log D.$$

On the other hand we have $D^{\frac{1}{2}\sum_j a_j}$ different r-tuple $(\alpha_1, \dots, \alpha_r)$, thus

$$|L| \geq D^{\frac{1}{2}\sum_j a_j}.$$

It follows that

$$D^{\frac{1}{2}\sum_j a_j} \ll D \log D$$

whence

$$\frac{1}{2}\sum_j a_j \ll 1 + \frac{\log\log D}{\log D}.$$

Combining this relation with relation (35) we deduce our claim. $\square$

Now we apply Lemma 5 to the basis $g_1, \dots, g_r$ of $\overline{\Gamma}_P$. The g_i are defined over the field $K(P)$ of degree d. We deduce

$$\prod_{i=1}^{r} \hat{h}(g_i) \gg \frac{1}{d^{r+2+\varepsilon}}$$

but $\hat{h}(g_i) \ll |\nu_i|^{-2}$ thus

$$\prod_{i=1}^{r} |\nu_i|^{2/n-r} \ll d^{\frac{r+2+\varepsilon}{(n-r)}}. \tag{36}$$

This relation together with the upper bound (34) gives

$$d \ll (RN)^{\frac{2}{n-2r-2-\varepsilon}}.$$

In conclusion we have proven the bound $(RN)^{2-\varepsilon} \ll d \ll (RN)^{\frac{2}{n-2r-2-\varepsilon}}$. We conclude that if $2 - \varepsilon - \frac{2}{n-2r-2-\varepsilon} > 0$, i.e. if $n - 3 > 2r$, then the degree d is absolutely bounded and so, by Northcott Theorem, $S_{n-r}(\mathcal{C})$ is finite. Unfortunately the result is not optimal as it is for the C.M. case.

6. – Some Cohomology

In this section, we study the cohomology of the Galois group of the extensions $L(E[N])$ of a number fiels L. The idea is that, except for a finite set of prime numbers, the Galois group $\mathrm{Gal}(L(E[p^n]/L)$ contains a suitable subgroup of dilatations. Studying the exact sequence associated to this normal subgroup we conclude that the cohomology is trivial. For the remaining 'bad' primes, the subgroup of dilatations will be big enough to reduce the cohomology to some m^2-torsion group, with m depending only on E and L.

Definition of the Serre number m for an elliptic curve E defined over L

- Let E be a non C.M. elliptic curve, then, by [18] (3) and (7), there exists an integer m, depending only on L and E, such that, for all $n \in \mathbb{N}$ and p prime, we have

$$\mathrm{Gal}(L(E[p^n])/L(E[m])) \cong GL_2(\mathbb{Z}/p^n\mathbb{Z}) \qquad \text{if } p \not| m \tag{36}$$

$$\mathrm{Gal}(L(E[p^n])/L(E[m])) \cong \{M \equiv I \bmod p^r\} \ \ \text{if } p^r || m \tag{37}$$

where I is the identity 2×2-matrix and $M \in GL_2(\mathbb{Z}/p^n\mathbb{Z})$.

- Let E be a C.M. elliptic curve. We recall that $\mathcal{O}$ is the ring of endomorphisms of E. By [18] Section 4 n. 4.5, there exists an integer m depending only on L and E such that we have

$$\mathrm{Gal}(L(E[p^n])/L) \cong \left(\mathcal{O}/p^n\mathcal{O}\right)^* \qquad \text{if } p \not| m \tag{38}$$

$$\mathrm{Gal}(L(E[p^n])/L) \cong \left(p^r\mathcal{O}/p^n\mathcal{O}\right)^* \quad \text{if } p^r || m, \tag{39}$$

for all $n \in \mathbb{N}$ and p prime.

After replacing L by an extension of finite degree $d(m)$, we may assume that $E[4]$ is defined over L and that $L = L(E[m])$, so $4|m$ and $E[m]$ is all the torsion defined over L. We call m the Serre number of E.

Corollary 3. *Let E be a C.M. elliptic curve and let G be a torsion subgroup isomorphic to $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/R\mathbb{Z}$ with $R|N$. Suppose that G is invariant under the action of $\mathcal{O}$. Then $L(G)$ is normal and*

$$\mathrm{Gal}(L(G)/L) \cong (m_1\mathbb{Z}/N\mathbb{Z})^* \times (m_2\mathbb{Z}/R\mathbb{Z})^*$$

with $m_1 = (N, m)$ and $m_2 = (R, m)$.

PROOF. Note that $G \subset E[N]$. The isomorphisms ρ in (39) and (40) are defined by the condition $\rho(\sigma)T = T^\sigma$ for $T \in E[N]$. This shows that $L(E[N])$ is normal. Let $\rho(\sigma) = a + b\tau \in (\mathcal{O}/N\mathcal{O})^*$, then the restriction of σ to $L(G)$ is defined by the condition $\sigma(T) = (a + b\tau)T$ for $T \in G$. Since G is invariant under the action of $\mathcal{O}$ the restriction $\sigma_{|L(G)}$ is an automorphism of $L(G)$, so $L(G)$ is normal. Moreover the sequence

$$0 \to \mathrm{Gal}(L(E[N])/L(G)) \to \mathrm{Gal}(L(E[N])/L) \to \mathrm{Gal}(L(G)/L) \to 0$$

is exact. Note that the exactness on the right follows for a question of orders. We then see that $\mathrm{Gal}(L(E[N])/L(G))$ is isomorphic to the group $\{a + b\tau \in \rho(\mathrm{Gal}(L(E[N])/L)) : (a + b\tau)_{|G} = id_G\}$ and $\mathrm{Gal}(L(T)/L)$ is isomorphic to the group of $\{a + b\tau \in \mathrm{Aut}(G) \cap \rho(\mathrm{Gal}(L(E[p^n])/L))$, where $\mathrm{Aut}(G)$ is identified with a subgroup of $(\mathcal{O}/N\mathcal{O})^*$ via the embedding of G in $E[N]$ and the invariance of G under $\mathcal{O}$.

The proof can also be given directly following the proof of [22] Theorem 2.3, p. 108. Note that the representation

$$\rho : \mathrm{Gal}(\overline{L}/L) \to \mathrm{Aut}(G)$$

given by $\rho(\sigma)(T) = T^\sigma$ for $T \in G$, is defined because G is invariant under the action of $\mathcal{O}$. □

PROPOSITION 6. *Let E be an elliptic curve. For any natural numbers n and $s \le n$ and any prime number p, we have*

$$\begin{aligned} H^1(\mathrm{Gal}(L(E[p^n])/L), E[p^s]) &= 0 \qquad \text{if } p \nmid m \\ p^r H^1(\mathrm{Gal}(L(E[p^n])/L), E[p^s]) &= 0 \qquad \text{if } p^r || m \end{aligned} \tag{40}$$

where m is the Serre number defined above.

PROOF. The group $(\mathbb{Z}/p^n\mathbb{Z})^*$ is diagonally embedded in $GL_2(\mathbb{Z}/p^n\mathbb{Z})$. On the other hand the group $(\mathbb{Z}/p^n\mathbb{Z})^*$ is trivially isomorphic to a subgroup of $(\mathcal{O}/p^n\mathcal{O})^*$.

We denote by $G_p := \mathrm{Gal}(L(E[p^n])/L)$ the Galois group of $L(E[p^n])$ over L.

CASE I: $p \nmid m$.

By (36), if E is non C.M. then $G_p = GL_2(\mathbb{Z}/p^n\mathbb{Z})$.

By (38), if E is C.M. then $G_p = (\mathcal{O}/p^n\mathcal{O})^*$. Since 2 divides m we can suppose $p \neq 2$. The Euler ϕ function and the Sylow Theorems tell us that the group $(\mathbb{Z}/p^n\mathbb{Z})^*$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/p^{n-1}\mathbb{Z})$. Then, using the identification above, there exists a normal subgroup Δ_p isomorphic to $(\mathbb{Z}/p\mathbb{Z})^*$ inside G_p for both cases E being C.M. or non C.M.

The exact sequence

$$0 \to \Delta_p \to G_p \to G_p/\Delta_p \to 0.$$

yields the inflation sequence

$$0 \to H^1(G_p, /\Delta_p, E[p^s]^{\Delta_p}) \to H^1(G_p, E[p^s]) \to H^1(\Delta_p, E[p^s])^{(G_p/\Delta_p)}.$$

We recall that $p \neq 2$, so the subgroup Δ_p is non-trivial and has order coprime with p. Therefore $H^1(\Delta_p, E[p^s]) = 0$. Moreover $E[p^s]^{\Delta_p} = 0$ because no p-torsion is defined over L. It follows that the left and the right term of the exact cohomology sequence are 0 and so $H^1(G_p, E[p^s]) = 0$ as well.

CASE II: $p^r || m$.

By (37), if E is non C.M. then $G_p = \{M \equiv I \bmod p^r\} \subset GL_2(\mathbb{Z}/p^n\mathbb{Z})$.

By (39), if E is C.M. then $G_p = (p^r\mathcal{O}/p^n\mathcal{O})^* \subset (\mathcal{O}/p^n\mathcal{O})^*$.

We consider inside G_p the normal subgroup of dilatations $\Delta_p := \{M \in (\mathbb{Z}/p^n\mathbb{Z})^* : M \equiv 1 \bmod p^r\}$, where 1 is the identity matrix and we use the above identification of $(\mathbb{Z}/p^n\mathbb{Z})^*$ with a subgroup of $GL_2(\mathbb{Z}/p^n\mathbb{Z})$ if E is non C.M, and we use the natural identification of $(\mathbb{Z}/p^n\mathbb{Z})^*$ with a subgroup of $(\mathcal{O}/p^n\mathcal{O})^*$ if E is C.M.

Since 4 divides m we can suppose $p^r > 2$. Then, independently of p, the group Δ_p is isomorphic to $(\mathbb{Z}/p^{n-r}\mathbb{Z})$ and a generator of Δ_p in $(\mathbb{Z}/p^n\mathbb{Z})^*$ is $(1 + p^r)$. We define $\mathcal{D}$ to be the multiplication by p^r. The norm of a group is given by the sum of all its elements. By the definition of Δ_p we see that the classes $1 + ip^r \in (\mathbb{Z}/p^n\mathbb{Z})^*$ for $i = 1, \dots, p^{n-r}$ represent all elements of Δ_p. We define $\mathcal{N}$ to be the multiplication by the norm of Δ_p. So we have

$$\begin{aligned} \mathcal{N} &\equiv \sum_{i=1}^{p^{n-r}} 1 + ip^r \bmod p^n \\ &\equiv p^{n-r} + p^n(p^{n-1} + 1)/2 \bmod p^n, \end{aligned}$$

whence

$$\begin{aligned} &\mathcal{N} \equiv p^{n-r} \bmod p^n && \text{if } p \neq 2 \\ &\mathcal{N} \equiv 2^{n-r}(1 + 2^{r-1}(1 + 2^{n-1})) \bmod 2^n && \text{if } p = 2. \end{aligned} \tag{41}$$

From the exact sequence

$$0 \to \Delta_p \to G_p \to G_p/\Delta_p \to 0,$$

we deduce the inflation sequence

$$0 \to H^1(G_p, /\Delta_p, E[p^s]^{\Delta_p}) \to H^1(G_p, E[p^s]) \to H^1(\Delta_p, E[p^s])^{G_p/\Delta_p}. \tag{42}$$

By [19] Section 4, we have

$$H^1(\Delta_p, E[p^s]) = \ker\mathcal{N}/\mathrm{Im}\mathcal{D}.$$

If $p \neq 2$, by (41), we deduce $\ker\mathcal{N} = \mathrm{Im}\mathcal{D}$ and so $H^1(\Delta_p, E[p^s]) = 0$. We recall that we assumed $4|m$ so, in the case $p = 2$, we have that $(1 + 2^{r-1}(1 + 2^{n-1}))$ is odd hence an automorphism of $E[2^s]$. Therefore, by (41), $\ker\mathcal{N} = \ker 2^{n-r} = \mathrm{Im}\mathcal{D}$ and we again deduce that $H^1(\Delta_p, E[p^s]) = 0$. It follows that the right term of the exact cohomology sequence (42) is trivial, thus

$$H^1(G_p, /\Delta_p, E[p^s]^{\Delta_p}) \cong H^1(G_p, E[p^s]).$$

The torsion points fixed by Δ_p are exactly the ones defined over L and so $E[p^s]^{\Delta_p} = E[p^r]$. Therefore $H^1(G_p/\Delta_p, E[p^r]) \cong H^1(G_p, E[p^s])$. Since the coefficient group $E[p^r]$ is annihilated by p^r, the result follows. □

PROPOSIZIONE 7. *Let E be an elliptic curve. For any positive integer N and any divisor k of N we have*

$$\delta^2 \cdot H^1(\mathrm{Gal}(L(E[N])/L), E[k]) = 0$$

where δ is the greatest common divisor of m and N, and m is the Serre number.

PROOF. Let p be a prime number, we set $N' := N/p^n$ where $p^n||N$. We use the following notation

$$\begin{aligned} G_N &:= \mathrm{Gal}(L(E[N])/L),\\ G_p &:= \mathrm{Gal}(L(E[p^n])/L),\\ G_{N'} &:= \mathrm{Gal}(L(E[N])/L(E[p^n]). \end{aligned} \tag{43}$$

We recall that $H^1(G_N, E[k]) = \oplus_p H^1(G_N, E[p^s])$ with $p^s||k$. The short exact sequence

$$0 \to G_{N'} \to G_N \to G_p \to 0$$

yields the inflation sequence

$$0 \to H^1(G_p, E[p^s]^{G_{N'}}) \to H^1(G_N, E[p^s]) \to H^1(G_{N'}, E[p^s])^{G_p}. \tag{44}$$

The group $G_{N'}$ fixes the p^s-torsion, so $E[p^s]^{G_{N'}} = E[p^s]$. Therefore

$$H^1(G_p, E[p^s]^{G_{N'}}) = H^1(G_p, E[p^s]). \tag{45}$$

Since p and N' are coprime, the groups G_p and $G_{N'}$ commute, it follows that

$$H^1(G_{N'}, E[p^s])^{G_p} = H^1(G_{N'}, E[p^s]^{G_p}). \tag{46}$$

CASE I:

If $p \nmid m$ then $E[p^s]^{G_p} = 0$ and, by relation (46), $H^1(G_{N'}, E[p^s])^{G_p} = 0$. By Proposition 6 and relation (45) we deduce $H^1(G_p, E[p^s]^{G_{N'}}) = 0$. Therefore the sequence (44) is trivial and

$$H^1(G_N, E[p^s]) = 0.$$

CASE II:

If $p^r||m$ then $E[p^s]^{G_p} = E[p^r]$. Therefore p^r annihilates the coefficients of (46) and so $p^r H^1(G_{N'}, E[p^s])^{G_p} = 0$. By Proposition 6 and relation (45) we deduce $p^r H^1(G_p, E[p^s]^{G_{N'}}) = 0$. Thus the left and the right term of the exact sequence (44) are annihilated by p^r, we deduce that

$$p^{2r} H^1(G_N, E[p^s]) = 0. \qquad \square$$

REFERENCES

[1] E. BOMBIERI – D. MASSER – U. ZANNIER, "Intersecting a Curve with Algebraic Subgroups of Multiplicative Groups", International Mathematics Research Notices 20, 1999.

[2] E. BOMBIERI – J. D. VAALER, *On Siegel's Lemma*, Invent. Math. **73** (1983), 11-32.

[3] E. BOMBIERI – J. D. VAALER, *Addendum to: On Siegel's Lemma*, Invent. Math. **75** (1984), 377.

[4] W. BURNSIDE, "Theory of Groups of Finite Order", 2 ed., Dover Publ., New York, 1955.

[5] J. W. S. CASSELS, "An Introduction to the Geometry of Numbers", Springer-Verlag, 1971.

[6] S. DAVID, *Points de petite hauteur sur les courbes elliptiques*, J. Number Theory **64** (1997), 104-129.

[7] S. DAVID – M. HINDRY, *Minoration de la hauteur de Néron-Tate sur le variétés abéliennes de type C.M.*, J. Reine Angew. Math. **529** (2000) 1-74.

[8] G. FALTINGS, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349-366.

[9] M. HINDRY, *Autour d'une conjecture de Serge Lang*, Invent. Math. **94** (1988), 570-603.

[10] S. LANG, "Fundamentals of Diophantine Geometry", Springer-Verlag, 1993.

[11] M. LAURENT, *Equations diophantiennes exponentielles*, Invent. Math. **78** (1984), 299-327.

[12] D. MASSER, *Counting points of small height on elliptic curves*, Bull. Soc. Math. France 117, 1989, no. 2, 247-265.

[13] D. MASSER – G. WÜSTHOLZ, *Fields of Large Transcendence Degree Generated by Values of Elliptic Functions*, Invent. Math. **72** (1983), 407-464.

[14] J. S. MILNE, *Abelian Varieties*, In: "Arithmetic Geometry", G. Cornell – J. Silverman (eds), Springer-Verlag, 1986.

[15] M. RAYNAUD, *Courbes sur une variété abélienne et points de torsion*, Invent. Math. **71** (1983), 207-233.

[16] M. RAYNAUD, *Sous-variétés d'une variété abélienne et points de torsion*, In: "Arithmetic and Geometry", (dédié à Shafarevich), Birkhäuser, 1, 1983, 327-352.

[17] H. P. SCHLICKEWEI, *Lower bounds for heights on finitely generated groups*, Monatsh. Math. **123** (1997), 171-178.

[18] J-P. SERRE, *Proprieté Galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259-331.

[19] J-P. SERRE, "Corps locaux", Hermann Paris, 1968.

[20] J-P. SERRE, *Local class field theory*, In: "Algebraic Number Theory", J. W. S. Cassels – A. Fröhlich (eds.), Academic Press, London, 1967, 129-162.

[21] J-P. SERRE, "Lectures on the Mordell-Weil Theorem", Friedr. Vieweg & Sohn, 1989.

[22] J. SILVERMAN, "Advanced Topics in the Arithmetic of Elliptic Curves", Springer-Verlag, 1994.

[23] J. SILVERMAN, "The Arithmetic of Elliptic Curves", Springer-Verlag, 1986.

D-Math, ETH Zürich
Rämistrasse 101
8092 Zürich - CH
viada@math.ethz.ch