

MANIN–MUMFORD IN ARITHMETIC PENCILS

GREGORIO BALDI, RODOLPHE RICHARD, AND EMMANUEL ULLMO

ABSTRACT. We present a refinement of Manin–Mumford (Raynaud’s Theorem) for abelian schemes over some ring of integers. Torsion points are replaced by *special 0-cycles*, that is reductions modulo some prime (possibly varying) of Galois orbits of torsion points. There is a flat/horizontal part and a vertical one. The irreducible components of the flat part are given by the Zariski closure, over the integers, of torsion cosets of the generic fibre of the abelian scheme. The vertical components are given by translates of abelian subvarieties, which “come from characteristic zero”.

CONTENTS

1. Introduction	1
2. Preliminaries and Hindry’s method	5
3. Horizontal and weak vertical, Theorem 1.2.1	8
4. Strong vertical, Theorem 1.2.3	15
5. Purely p -adic phenomena, Theorem 1.2.6	24
Appendix A. Proof of Proposition 5.1.1	33
References	39

1. INTRODUCTION

1.1. Motivation. The following is often referred to as the *Manin–Mumford conjecture*, stated in [21]. It was first proved by Raynaud [25, 26], reproved then by Hindry [17] and more recently by Pila–Zannier [24], among others.

Theorem 1.1.1 (Raynaud). *Let A be an abelian variety over a field of k characteristic 0 and E be a subset of torsion points of $A(\bar{k})$. Then the Zariski closure of E is special: a finite union of torsion cosets $a + B$ for some abelian subvariety $B \subseteq A_{\bar{k}}$ and a torsion point $a \in A(\bar{k})$.*

Theorem 1.1.1, together with its multiplicative analogue (originally appeared in [21]), can be thought as the first instance of a more general philosophy, now referred to as *Unlikely Intersections*. Recently Richard [27] has introduced a new net of conjectures aiming to understand unlikely intersections phenomena *over the integers*. This includes new problems regarding the arithmetic of (models of) both abelian and Shimura varieties. The role of torsion points is replaced by the reduction to some residue field of positive characteristic of the Zariski closure, over the integers, of either a torsion or a CM-point. In an arithmetic family there are two perspectives:

- *Horizontal* unlikely intersections. This case corresponds to an intersection with infinitely many vertical fibres;

2020 *Mathematics Subject Classification.* 11G10, 11G35, 14K12.

Key words and phrases. Unlikely intersections, subschemes of abelian schemes, reduction modulo a prime, Galois orbits of torsion points, lifting abelian subvarieties.

Date: February 6, 2024.

- *Vertical unlikely intersections.* When the vertical fibres form a finite set.

Even formulating the vertical part for Shimura varieties is challenging. Consider $Y_0(1)/\mathbb{Z} \cong \mathbb{A}_{\mathbb{Z}}^1$, the modular curve parametrising elliptic curves. Under the generalised Riemann hypothesis for quadratic imaginary fields, Edixhoven and Richard [8] proved the vertical André–Oort for $Y_0(1) \times Y_0(1)/\mathbb{Z}$ and later, unconditionally, Richard [27] proved the horizontal André–Oort for $Y_0(1)/\mathbb{Z}$. The above conjectures contain, as special cases, new statements for subschemes of abelian schemes over some ring of integers that can be thought as an arithmetic counterpart of Theorem 1.1.1. The aim of this paper is to prove both a horizontal and vertical Manin–Mumford, as we explain in the next section.

1.2. Main results. Let K be a number field (with a fixed algebraic closure $\overline{K}$), S a finite set of finite places of K and $\mathcal{O}_{K,S}$ be the ring of S -integers of K . Write $\text{Gal}(\overline{K}/K)$ for the absolute Galois group of K . Let $\mathcal{A}$ be an abelian scheme over (the spectrum of) $\mathcal{O}_{K,S}$. We denote by $A = A_K$ its generic fibre, and by $\mathcal{A}_{\mathfrak{p}}$ its special fibre at a closed point $\mathfrak{p} \in \text{Spec}(\mathcal{O}_{K,S})$. The latter is an abelian variety over the residue field $\kappa(\mathfrak{p})$. In $\mathcal{A}$ we consider *special 0-cycles*, that is the reduction to $\kappa(\mathfrak{p})$, of positive characteristic, of the Zariski closure in $\mathcal{A}$ of a torsion point $a \in A(\overline{K})$, for some prime ideal $\mathfrak{p} \in \text{Spec}(\mathcal{O}_{K,S})$. Our main result describes the Zariski closure of a set of special 0-cycles in $\mathcal{A}$. To do so we introduce two classes of subschemes of $\mathcal{A}$:

- *Flat cycles.* Those obtained as the Zariski closure in $\mathcal{A}$ of special subvarieties of $A_{\overline{K}}$ (in the sense of Theorem 1.1.1), and
- *Torsion cycles.* The translates of an abelian subvariety of some vertical fibre $\mathcal{A}_{\mathfrak{p}}$ by a $\overline{\kappa(\mathfrak{p})}$ -point of $\mathcal{A}$.

Intersections between flat cycles and vertical fibres are particular cases of finite unions of torsion cycles, but in general torsion cycles are given by an abelian subvariety of $\mathcal{A}_{\mathfrak{p}}$ which is not, a priori, coming from a flat subvariety of $\mathcal{A}$. A closed subscheme of $\mathcal{A}$ is called *special* if it can be written as a finite union of flat and torsion cycles.

Theorem 1.2.1. *Let $\mathcal{V} \subset \mathcal{A}$ be a closed subscheme. If $\mathcal{V}$ contains a Zariski dense sequence $(E_n)_{n \geq 0}$ of special 0-cycles then $\mathcal{V}$ is special.*

It is natural to try to understand when the torsion cycles given by Theorem 1.2.1 are intersections between flat cycles and vertical fibres, but there is a *p-adic obstruction* to this, as the next example shows.

Example 1.2.2. *Let A be a geometrically simple abelian K -surface, and $\mathfrak{p}$ a prime of residue characteristic $p > 0$, such that the reduction of $A \bmod \mathfrak{p}$, denoted by $\mathcal{A}_{\mathfrak{p}}$, is isogenous to $\mathfrak{B} \times \mathfrak{B}'/\kappa(\mathfrak{p})$, with $\mathfrak{B}$ ordinary and $\mathfrak{B}'$ super-singular, that is $\mathfrak{B}'(\overline{\kappa(\mathfrak{p})})[p^\infty] \cong 0$. Let $(a_n)_n \subset A(\overline{K})$ be a sequence of points such that $\text{ord}(a_n) = p^n$. Since $\mathfrak{B}'[p^\infty] = 0$, the reduction to $\kappa(\mathfrak{p})$ of the $\text{Gal}(\overline{K}/K)$ -orbit of the a_n 's is contained in $\mathfrak{B} \times \{0_{\mathfrak{B}'}\}$. We can choose the a_n 's in such a way that the Zariski closure of $\bigcup_n E_n$ is $\mathfrak{B} \times \{0_{\mathfrak{B}'}\} \subset \mathcal{A}_{\mathfrak{p}}$ (as predicted by Theorem 1.2.1), but $\mathfrak{B} \times \{0_{\mathfrak{B}'}\}$ can not come from characteristic zero, since $A_{\overline{K}}$ is simple.*

Our second main result considers only special 0-cycles of order prime to the residue characteristics, that is cycles E associated to a torsion point a and residue field $\kappa(\mathfrak{p})$ such that $\text{ord}(a)$ is coprime with $\text{char}(\kappa(\mathfrak{p}))$.

Theorem 1.2.3. *If $(E_n)_{n \geq 0}$ is a sequence of special 0-cycles in $\mathcal{A}$ of order coprime with the residue characteristic, then the Zariski closure of $\bigcup_{n \geq 0} E_n$ is a finite union of flat cycles and intersections between flat cycles and vertical fibres.*

Each special 0-cycle $E_n \subset \mathcal{A}$, set theoretically, can be written as the image of $\text{Gal}(\overline{K}/K) \cdot a_n$, for a family of points $a_n \in A_{\text{tors}}(\overline{K})$ along a¹ map

$$A(\overline{K}) \rightarrow \mathcal{A}(\overline{\kappa(\mathfrak{p}_n)})$$

to a family of fields of positive characteristic $\kappa(\mathfrak{p}_n)$. Notice that the result is purely *vertical* when the set $\{\mathfrak{p}_n\}_{n \geq 0}$ is finite. It may be helpful to give a reformulation of Theorem 1.2.3, assuming that all special 0-cycles lie in a fixed vertical fibre $\mathcal{A}_{\mathfrak{p}}$:

Theorem 1.2.4. *Fix a prime $\mathfrak{p} \subset \mathcal{O}_{K,S}$ of residue characteristic p . Let $\mathcal{A}$ be an abelian scheme over $\mathcal{O}_{K,S}$, $(a_n)_n \subset A_{\text{tors}}$ be a sequence of torsion points of order coprime with p , and write $E_n = \pi_{\mathfrak{p}}(\text{Gal}(\overline{K}/K) \cdot a_n)$, for a map $\pi_{\mathfrak{p}} : A(\overline{K}) \rightarrow \mathcal{A}_{\mathfrak{p}}(\overline{\kappa(\mathfrak{p})})$. Then every component of $\mathcal{V}$, the Zariski closure of*

$$\bigcup_{n \geq 0} E_n \subset \mathcal{A}_{\mathfrak{p}} \subset \mathcal{A},$$

is a component of the intersection between a flat cycle $\mathcal{B} \subset \mathcal{A}$ and $\mathcal{A}_{\mathfrak{p}}$.

An interesting and simple corollary of Theorem 1.2.4 is the following.

Corollary 1.2.5. *With the notations and the assumptions of Theorem 1.2.4, if the sequence of subsets $(\text{Gal}(\overline{K}/K) \cdot a_n)_n$ is Zariski dense in A_K , then the special 0-cycles $(E_n)_{n \geq 0}$ are Zariski dense in $\mathcal{A}_{\mathfrak{p}}$.*

The final main result of the paper shows that the “ p -rank zero factor” explained in Example 1.2.2 is indeed the only obstruction to the lifting problem.

Theorem 1.2.6. *Let $\mathcal{O}_{K,S}$, $\mathfrak{p}$, p , $\pi_{\mathfrak{p}}$ and $\mathcal{A}$ be as in Theorem 1.2.4. If $(a_n)_n \subset A_{\text{tors}}$ is a sequence of torsion points (possibly of order divisible by p), then every component of the Zariski closure $\mathcal{V}$ of*

$$\bigcup_{n \geq 0} \pi_{\mathfrak{p}}(\text{Gal}(\overline{K}/K) \cdot a_n) \subset \mathcal{A}_{\mathfrak{p}} \subset \mathcal{A},$$

is of the form $\alpha + \mathfrak{B}$, and there exists an abelian subvariety $B \subseteq A$ (over $\overline{K}$) such that $\mathfrak{B} \subset B_{\mathfrak{p}}$ and the quotient $B_{\mathfrak{p}}/\mathfrak{B}$ is of p -rank zero.

Remark 1.2.7. Any of Theorem 1.2.1 or 1.2.3 implies the classical Manin–Mumford Theorem 1.1.1 (at least after it is reduced to $\overline{\mathbb{Q}}$). Let indeed be $V \subset A_{\overline{\mathbb{Q}}}$ be a component of the Zariski closure of a sequence of torsions points $(a_n)_n$. Consider the special zero cycles $E_{m,n}$ given by reducing modulo $\mathfrak{p}_m$ (the m th prime) the Galois orbit of a_n . By the horizontal Manin–Mumford (i.e. Theorem 1.2.1 for the flat components), we have a torsion coset $B \subset A_{\overline{\mathbb{Q}}}$ such that

$$E_{m,n} \subseteq B \subseteq V \subseteq A_{\overline{\mathbb{Q}}}.$$

Repeating this on A/B concludes the argument. The same proof works with the strong vertical Manin–Mumford established in Theorem 1.2.3, choosing carefully the reduction place (in both cases we need a characteristic zero abelian subvariety of A).

¹Even if there is no canonical map $\pi_{\mathfrak{p}_n} : A(\overline{K}) \rightarrow \mathcal{A}(\overline{\kappa(\mathfrak{p}_n)})$, the image of a Galois orbit in $\mathcal{A}(\overline{\kappa(\mathfrak{p}_n)})$ is well defined (i.e. does not depend on a particular choice of $\pi_{\mathfrak{p}_n}$). Indeed it is just the intersection between the vertical fibre $\mathcal{A}_{\mathfrak{p}}$ and the Zariski closure over $\mathcal{O}_{K,S}$ of a_n . We remark here that, when restricted to the prime-to-char $\kappa(\mathfrak{p})$ part of the torsion, $\pi_{\mathfrak{p}}$ is the isomorphism identifying $\pi_1^{et}(\mathcal{O}_{K,S})$ -equivariantly two geometric fibres of a locally constant constructible sheaf.

Hindry's approach to the Manin–Mumford conjecture turned out to provide a fruitful strategy for the *André–Oort conjecture*, as first envisioned by Edixhoven [7]. We refer to [20, 16] for an overview of recent results and progress. We hope that our strategy can be applied to obtain new evidences in favour of Richard's arithmetic conjectures. Finally we remark that there are also variants of the classical Manin–Mumford in positive characteristic by Hrushovsky, Pink–Rossler and Scanlon (see for example [29] and references therein). They appear to be interested in a different problem, since here it is crucial to start with an abelian scheme over some ring of integers and take Galois orbits under the Galois group of a number field.

1.3. Strategy of the proof and outline of the paper. The proof of the horizontal part of Theorem 1.2.1 is inspired by the approach of Hindry [17] to his proof of Theorem 1.1.1. Our arithmetic variant, however, presents new phenomena and new difficulties, as Remark 1.3.2 explains. The strategy for Theorem 1.2.3 and Theorem 1.2.6 is more complicated, and relies on the Tate conjecture (both the p -adic and mod p variants).

1.3.1. Horizontal and weak vertical. Let c be a positive integer and $L = L(c)$ be Lang group of c -th powers *homotheties*, as in (2.1). We L act on each $\mathcal{A}(\overline{\kappa(\mathfrak{p})})$. As for Hindry's proof, the only “Galois input” we need to know is the comparison explained in Remark 2.2.2 between the $\text{Gal}(\overline{K}/K)$ and L actions on torsion points. Therefore the following implies Theorem 1.2.1.

Theorem 1.3.1. *Let $\mathcal{V} \subseteq \mathcal{A}$ be a closed $\mathcal{O}_{K,S}$ -subscheme of $\mathcal{A}$ which admits a Zariski dense set of closed points (a_n) such that $L \cdot a_n \subseteq \mathcal{V}$. Then $\mathcal{V}$ is special.*

The strategy is based on Proposition 3.1.1. From a subvariety V of $\mathcal{A}_{\mathfrak{p}_n}$ of degree D and dimension Δ , containing $L \cdot a_n \subseteq \mathcal{A}_{\mathfrak{p}_n}$, we show that, if the $\text{ord}(a_n)$ is bigger than some function $f = f(D, \Delta)$, then there exists $0 \neq B \subseteq \mathcal{A}_{\mathfrak{p}_n}$ an abelian subvariety of $\mathcal{A}_{\mathfrak{p}_n}$ such that $a_n + B \subset V$ and $\delta := \text{ord}(a + B)$ (its order in $\mathcal{A}_{\mathfrak{p}_n}/B$) is smaller than $\text{ord}(a_n)$. After repeating the argument in $\mathcal{A}_{\mathfrak{p}_n}/B$, we may assume that $\dim B = 0$ and that $\text{ord}(a_n)$ is bounded by f .

Remark 1.3.2. If a torsion coset $a + A'$ of A is contained in a subvariety $V \subseteq A$ and in $[q](V)$, for some $q > 1$, then

$$a + A' \subseteq V \cap [q](V)$$

and in particular there is an irreducible component V' of V such that $a + A' \subseteq V'$. Compared with Hindry's approach, where everything is defined over a number field K , the main difference is that there

$$\text{Gal}(\overline{K}/K) \cdot a + A' \subset V'.$$

In an arithmetic pencil, this point becomes much more subtle, since the standard habit of reducing to irreducible components is usually incompatible with the problem. Indeed the main new difficulty we have to face is that we do not know, a priori, that every component of the reduction of $V \bmod \mathfrak{p}_n$ contains many elements of the special 0-cycle E_n , even if the cardinality of E_n is tending to infinity.

1.3.2. Vertical and lifting. Theorem 1.2.3 requires different ideas and more sophisticated tools. It turns out that, using various forms of the Tate conjecture (Faltings theorem, see Section 4.1), the only abelian subvarieties we have to consider are the ones coming from characteristic zero. This is interesting because there are many more abelian subvarieties of $\mathcal{A}_{\mathfrak{p}}$, than the one coming from characteristic zero. The analogy with Shimura varieties is less clear: what is a *special subvariety* of the reduction mod p of a Shimura variety, which does not come from characteristic zero (that is from reducing mod p a Shimura subvariety)?

We briefly explain our strategy for Theorems 1.2.3 and 1.2.4 (with the same notation as in Theorem 1.2.4). By looking at the order of the a_n , there are essentially two possibilities to keep in mind:

- (1) $\text{ord}(a_n) = \ell^n$, for all n (where ℓ is a prime different from p);
- (2) $\text{ord}(a_n)$ is the n -th prime number, for all n .

The main protagonists are (considered as $\text{Gal}(\overline{K}/K)$ -representation):

- The ℓ -adic (rational) Tate module of A (for $\ell \neq p$);
- The adelic Tate module of A (or quotients thereof).

Each object plays a similar role, depending only on the order of the a_n : the ℓ -adic Tate module in (1), and the adelic one in (2). The idea in both cases is similar, even if it may require different tools, and can be summarised as follows. Let V be one of the above *semisimple* $\text{Gal}(\overline{K}/K)$ -representations. The Galois orbits of the points a_n determine a subrepresentation $W \subset V$, such that $V = W \oplus W'$. Faltings's theorem asserts that such a decomposition is induced by an element $u \in \text{End}(A) \otimes E_V$, where $E_V \in \{\mathbb{Q}_\ell, \text{a quotient of } \widehat{\mathbb{Z}}\}$, depending on V . Theorem 1.2.1 asserts that such a decomposition is, “after reducing mod $\mathfrak{p}$ ”, induced by an element of $\text{End}(A_{\mathfrak{p}})$, and we prove that u can be found in $\text{End}(A) \otimes \mathbb{Q}$ (thanks to the formal descent lemma 4.2.1). This corresponds to lifting a torsion cycle to a flat one.

1.3.3. Points of p -torsion in characteristic p . The proof of Theorem 1.2.6 is inspired by the ℓ -adic argument presented above, but it is more subtle, as Example 1.2.2 shows. To emulate the argument of Section 1.3.2, we need to find a vector space where both $\text{End}(A) \otimes \mathbb{Q}_p$ and $\text{End}(A_{\mathfrak{p}}) \otimes \mathbb{Q}_p$ act faithfully and compatibly. This is done using some comparison theorem from p -adic Hodge theory, but it requires to extend the coefficients from $\mathbb{Q}_p$ to one of Fontaine's period rings (see Proposition 5.1.1). Such results are presented in a self contained way in the final Appendix A.

Acknowledgements. The second author would like to thank the I.H.E.S. for a research visit in September and October 2020, during which most of the work regarding the horizontal Manin–Mumford was done. Rodolphe Richard was supported by the Leverhulme grant RPG-2019-180. Finally we thank the referees for their careful reading and comments.

2. PRELIMINARIES AND HINDRY'S METHOD

In this section we first reduce the main results to the case where $\text{End}(A_K) = \text{End}(A_{\overline{K}})$. We then define the Lang group and recall its relation to the Galois action on torsion points. Finally we review some results which appear in Hindry's method for Manin–Mumford [17], and in the process we check that Hindry's results hold true also over fields of arbitrary characteristics.

2.1. A first reduction. We explain here why the statements of the results of Section 1.2 are not affected by finite field extensions K'/K . This may look surprising at first since there can be many more K' -abelian subvarieties of a K -abelian variety A , rather than K -abelian subvarieties.

Without loss of generality, we may assume that K'/K is Galois. Let $(E_n)_{n \geq 0} \subset \mathcal{A}$ be a sequence of special zero cycles obtained as the $\mathcal{O}_{K,S}$ -Zariski closure of a sequence of torsion points $a_n \in A(\overline{K})$, and (E'_n) be the $\mathcal{O}_{K',S'}$ -Zariski closure of the a_n (for some set of K' places S' above S). Let $\mathcal{V} \subset \mathcal{A}$ (resp. $\mathcal{V}' \subset \mathcal{A}_{\mathcal{O}_{K',S'}}$) be the Zariski closure of the E_n (resp. of the E'_n). The closure of $\mathcal{V}'$ over $\mathcal{O}_{K,S}$ is $\mathcal{V}$. In particular if $\mathcal{V}'$ is special or even a finite union of flat cycles and intersections of flat cycles and vertical fibres, so is $\mathcal{V}$. Finally fix $\mathfrak{p} \subset \mathcal{O}_{K,S}$ and $\mathfrak{p}' \subset \mathcal{O}_{K',S'}$ above $\mathfrak{p}$. If every K' -component of $\mathcal{V}'$ is $F + \mathcal{B}$ (for some finite set $F \subset \mathcal{A}$ and abelian $\mathcal{O}_{K',S'}$ subscheme of $\mathcal{A}$) there exists an abelian

subvariety $B' \subset A_{K'}$ such that $\mathcal{B} \subset B_{p'}$ of p -corank zero, then the same holds for the K -components of $\mathcal{V}$.

From now on, we may and do assume that $\text{End}(A_K) = \text{End}(A_{\overline{K}})$.

2.2. Lang group and adelic Tate module. Let K be a number field, and A be a g -dimensional abelian variety over K (for some $g > 0$). Denote by $T(A)$ the $\text{Gal}(\overline{K}/K)$ -module obtained by taking the inverse limit of the $A[n]$'s, that is the (integral) *adelic Tate module* of A . We write $\widehat{\mathbb{Z}}$ for the profinite completion of the ring of integers $\mathbb{Z}$, and notice that $T(A) \cong \widehat{\mathbb{Z}}^{2g}$. The proof of the following can be found for example in [5, Theorem B]. See also [3, Corollary 1, page 702], [17, Section 2 (a)], [33], and references therein. For any $c \in \mathbb{Z}_{\geq 1}$, we define the *Lang group* $L = L(c)$ by the formula

$$(2.1) \quad L = L(c) := \ker \left(\widehat{\mathbb{Z}}^* \rightarrow \widehat{\mathbb{Z}}^* \otimes \mathbb{Z}/c\mathbb{Z} \right),$$

seen as a subgroup of $\text{GL}(T(A))$. By definition, $L = L(c)$ acts on the torsion points of A .

Theorem 2.2.1 (Bogomolov–Serre). *There exists a positive integer $c = c(A, K)$ such that the image of the map describing the action of $\text{Gal}(\overline{K}/K)$ on the torsion points,*

$$\rho_A : \text{Gal}(\overline{K}/K) \rightarrow \text{GL}(T(A)),$$

contains the c -th powers of the homotheties. That is $L(c) \subset \text{Im}(\rho_A)$.

Remark 2.2.2. As a corollary of Theorem 2.2.1, we have the following. Let $a \in A_{\text{tors}}(\overline{K})$ be of order d , and l a positive integer prime to d . Then there exists $\sigma \in \text{Gal}(\overline{K}/K)$ such that

$$\sigma \cdot a = \sigma(a) = [l^c](a).$$

2.3. Degree, stabiliser subgroup, and a criterion for specialness. We discuss Hindry's results of Bézout type in abelian varieties (see [17, Section 1]). The first use of a Bézout theorem/intersection theory to approach Lang conjecture can be dated back to Tate's proof [21, Section 2 (page 231)] of a case of the multiplicative Manin–Mumford. See also the discussion about abelian varieties in Section 3 of *op. cit.*.

Let k be an algebraically closed field of characteristic $p \geq 0$, and A be an abelian variety (of dimension > 1) over k .

Lemma 2.3.1. *Let V be an irreducible subvariety of A , and let $B \subset A$ be its stabiliser. Let q be a positive integer not divisible by p . We have*

$$(2.2) \quad \deg([q](V)) = q^{2\dim(V)} \deg(V) \cdot (\#B[q])^{-1}.$$

Proof. The proof presented in [17, Lemma 6] applies also to cover the above statement, if $p \nmid q$. $\square$

For simplicity, from now, we simply write that q is prime to p , to mean that q is non zero and not divisible by p (which makes sense both when $p = 0$ and $p > 0$).

Corollary 2.3.2. *Let A, V , and B as in Lemma 2.3.1. Let q, q' be positive integers, prime to each other and to p , such that*

$$[q](V) = [q'](V).$$

Then

$$\#B[q] = q^{2\dim(V)}, \#B[q'] = q'^{2\dim(V)}, \text{ and } \#B[qq'] = (qq')^{2\dim(V)}.$$

Proof. From Lemma 2.3.1 we have that

$$q^{2 \dim V} \#B[q]^{-1} = q'^{2 \dim V} \#B[q']^{-1}.$$

Since q and q' are coprime, the only possibility is that $\#B[q] = q^{2 \dim(V)}$ and $\#B[q'] = q'^{2 \dim(V)}$. Again by the fact that q and q' are coprime, we have $B[qq'] = B[q] \times B[q']$, concluding the proof. $\square$

Lemma 2.3.3. *Let A, V , and B as in Lemma 2.3.1. Denote by B^0 the neutral component of B , and the group of components of B by $\pi_0(B) = B/B^0$. We have*

$$\#\pi_0(B) \leq \deg(B) = \#\pi_0(B) \cdot \deg(B^0) \leq \deg(V),$$

and

$$\#B[q] = \#\pi_0(B)[q] \cdot \#B^0[q] \leq \#\pi_0(B) \cdot q^{2 \dim(B)}.$$

Assume now that $\#B[q] = q^{2 \dim(V)}$. Then

$$q^{2(\dim(V) - \dim(B))} \leq \#\pi_0(B) \leq \deg(V).$$

If moreover

$$\deg(V) < q^2,$$

then V is special.

Proof. The first formula follows from [17, Lemma 8]. For the second formula, just notice that $\#B^0[q](\bar{k}) = q^{2 \dim B^0}$, as long as q is prime to p . The third formula is a direct consequence of the previous two.

Regarding the last conclusion, we necessarily have $\dim(V) - \dim(B) = 0$, since otherwise

$$q^{2(\dim(V) - \dim(B))} \leq \#\pi_0(B) \leq \deg(V) < q^2.$$

Choose a point $v \in V$, and notice that necessarily $v + B \subset V$. As $\dim(v + B) = \dim(B) = \dim(V)$, and V is irreducible, we have that $V = v + B$ is special. $\square$

Proposition 2.3.4. *Let V be an irreducible subvariety of A , q and q' be prime to each other and to p be such that*

$$[q](V) = [q'](V), \text{ and } \deg(V)^{1/2} < q \cdot q'.$$

Then V is a special subvariety of A , and so is $[q](V)$.

Notice that the condition $\deg(V)^{1/2} < q \cdot q'$ is actually implied by $\deg(V)^{1/4} \leq q < q'$. We only use the latter condition.

Proof. Corollary 2.3.2 implies that $\#B[qq'] = (qq')^{2 \dim(V)}$. Therefore the assumption on $\#B[qq']$ (with qq' for q) in Lemma 2.3.3 is satisfied and so V is special. $\square$

Finally we check for reference that Hindry's criterion [17, Lemma 15] stays valid in any characteristics, and that it applies to subvarieties which are not necessary irreducible. See also [3, Corollary on page 703].

Corollary 2.3.5 (Hindry). *Let V be a subvariety of A . If $V = [q](V)$, for some $q > 1$ prime to p , then each component of V is special.*

Proof. Let $r \leq \deg(V)$ the number of components of V , and $r!$ be the cardinality of the symmetric group acting on a set with r elements. Since $[q]$ permutes the components of V , every component Z is stable under $[q^{r!}]$, and similarly under $[m]$, for $m := q^{\deg(V)!}$. Of course $m^2 > \deg(V)$, and Proposition 2.3.4 on Z , m and $q' = 1$ applies to conclude. $\square$

3. HORIZONTAL AND WEAK VERTICAL, THEOREM 1.2.1

From now on we introduce some novelties in the Hindry's method, since, as explained in Remark 1.3.2, the standard way of applying it is incompatible with the various reductions mod p . For example we have to use the prime number theorem, among other things, to choose the primes carefully.

3.1. Statement of the main proposition. Let $L = L(c)$ be the Lang group associated to some positive integer c , as defined in Section 2.2. The next result is the key for proving Theorem 1.3.1, and it is proven in Section 3.2. Here we consider a field k (with a fixed algebraic closure $\bar{k}$) of characteristic $p \geq 0$, and a g -dimensional abelian variety A over k (for some $g > 1$).

Proposition 3.1.1. *Let V be a subvariety of A (not necessarily irreducible) of degree D and dimension Δ , and let a be a torsion point of $A(\bar{k})$ of order d . Assume that*

$$(3.1) \quad L \cdot a \subseteq V.$$

Then there exist $\alpha \in A_{\text{tors}}$ and $B \subset A$ an abelian subvariety of A such that

$$L \cdot a \subseteq L \cdot \alpha + B \subseteq V, \text{ and } \text{ord}(\alpha + B) \leq \delta.$$

Where $\delta = \delta(D, \Delta, c)$ is a constant depending only on D , Δ , and c .

The strategy is to replace V by a special subvariety $Z \subset V$, still containing $L \cdot a$, and of degree as small as possible. In this case one can hope that not only $L \cdot a$, but most of the subgroup of A generated by a , which we denote by $\langle a \rangle$, is contained in Z (and hence in V).

Remark 3.1.2. The proof implies a stronger statement concerning torsion cosets $a + A'$ of A , rather than just torsion points.

3.2. Proof of Proposition 3.1.1. The proof of Proposition 3.1.1 consists of two lemmas, which are proven below. We first introduce some notation. Given a positive integer d , we write:

- $p(d)$ for the d -th prime number;
- $\omega(d)$ for the number of distinct prime divisors of d ;
- $g(d)$ for the *Jacobsthal's function*. That is it represents the smallest number M such that every sequence of M consecutive integers contains an integer coprime to d .

The Jacobsthal's function plays a role in providing sharp estimates. The reader not interested in explicit estimates may replace these arguments by less precise, but easier, estimates that will be explained during the proofs, indeed we only need to know that $g(d) = d^{o(1)}$.

Proposition 3.2.1. *Let d, d', a be positive integers and $d' | d$. If a is prime to d' and*

$$(3.2) \quad (a + kd') \wedge d = 1,$$

for some $k \in \mathbb{Z}$, then we can find $k' \geq 0$ satisfying (3.2), and such that

$$0 \leq k' < g(d) = d^{o(1)}.$$

In the case $0 \leq a < d'$, we have $a + k' \cdot d' \leq g(d) \cdot d'$.

Iwaniec [18] proved that

$$g(d) \leq C \cdot \omega(d)^2 \cdot \log \omega(d)^2,$$

for some unknown C . The best known explicit upper bounds

$$(3.3) \quad g(d) \leq 2^{\omega(d)}, \text{ and } g(d) \leq 2\omega(d)^{2+2e \log \omega(d)},$$

are due to Kanold [19] and Stevens [31]. In particular, $g(d) = d^{o(1)}$

Proof of Proposition 3.2.1. Set $n = \frac{d}{d'}$. We are looking for the smallest $k' \in \mathbb{N}$ such that

$$(a/d' + k') \wedge n = 1$$

where by a/d' denotes $a \cdot d'^*$ for $d'^* + n\mathbb{Z}$ an inverse of $d' + n\mathbb{Z}$ in $\mathbb{Z}/(n)^\times$. By definition of $g(d)$, this happens for some $0 \leq k' < g(d)$. $\square$

3.2.1. First lemma. The first step towards Proposition 3.1.1 consists in finding a subvariety $V' \subset V$ of degree $d^{o(1)}$.

Lemma 3.2.2. *Let V be a subvariety of A of degree D and dimension Δ , and A' an abelian subvariety of A such that*

$$(3.4) \quad L \cdot a + A' \subseteq V.$$

We have exactly one of the following.

- *A component of maximal dimension X of V is a special subvariety, say of the form $\alpha + B$, for some torsion point $\alpha \in A$ and B an abelian subvariety of A , such that for every $l \in L$, $l\alpha + B$ is a component of V and the order of each $l\alpha + B$ is bounded by $D^{O(1)} \cdot d^{o(1)}$, as $d \rightarrow +\infty$, and*

$$L \cdot a + A' \subseteq L \cdot \alpha + B \subseteq V.$$

- *There exists $V' \subset V$ such that $\dim(V') < \dim(V)$, V' satisfies (3.4), and*

$$(3.5) \quad \text{every component of } V \text{ contains a component of } L \cdot a + A',$$

and has degree bounded as follows:

$$(3.6) \quad \deg(V') \leq D^{O(1)} \cdot d^{o(1)},$$

as $d \rightarrow +\infty$.

More precisely and explicitly we prove that

$$(3.7) \quad \deg(V') \leq f(D, d) := D^2 \cdot \left(p\left(\left\lceil \sqrt[2c]{D} \right\rceil + D + \omega(d) + 1\right)^c \cdot g(d \cdot \max\{1, p\}) \right)^{2 \cdot c \cdot \Delta},$$

where $\left\lceil \sqrt[2c]{D} \right\rceil$ denotes the smallest integer bigger or equal than $\sqrt[2c]{D}$.

Two observations that follow directly from the assumptions (3.4)-(3.5), and are also at the heart of Hindry's method:

- For every integer m prime to $d = \text{ord}(a + A')$, we have $V \supseteq L \cdot a + A' = m^c \cdot L \cdot a + A' \subseteq [m^c](V)$. Hence

$$L \cdot a + A' \subseteq V \cap [m^c](V);$$

- For every component X of V , we have

$$\emptyset \neq X \cap (L \cdot a + A') \subseteq X \cap [m^c](V).$$

In Lemma 3.2.2 we did not assume that (3.5) holds, but the statements is still true, since we may discard a finite number of components of V , to assume that (3.5) holds.

Proof. Let

$$(3.8) \quad x := \left\lceil \sqrt[2c]{D} \right\rceil + D + \omega(d) + 1, \text{ and } n := p(x).$$

For simplicity one can also simply replace x by $x_D := 2D + \omega(d) + 1$, just by noticing that $x \leq x_D$. This is indeed what we will do in the second Lemma. Since x is at least 4, we can use some non-asymptotic bounds on the prime-counting function and write

$$(3.9) \quad n = p(x) \leq x \log(x)(1 + \log \log(x)),$$

see for example [28, Theorem 3, page 69]. Finally we set

$$N := n^c \cdot g(d \cdot \max\{1, p\}),$$

where $g(-)$ denotes the Jacobsthal's function, as introduced in Section 3.2. The reason why the factor $\max\{1, p\}$ appears is to deal simultaneously the cases of zero and positive characteristic.

Let X be a component of V of maximal dimension, and set

$$X' = X'(m) := X \cap [m^c](V),$$

for some $m = m(X)$ chosen in the following set

$$(3.10) \quad \Sigma = \Sigma(d, D) := \{m^c \text{ such that } m \in \{1, \dots, N\}, m \wedge d = 1, \text{ and } p \nmid m\}.$$

Assume now that there exists $m^c \in \Sigma$ such that $\dim(X') < \dim(X)$. Then the degree formula from Section 2.3, namely (2.2), and the fact that $m^c \leq N^c = n^{c^2} \cdot g(d \cdot \max\{1, p\})^c$, imply that

$$\deg(X') \leq \deg(X) \cdot \deg([m^c](V)) \leq \deg(X) \cdot \deg(V) \cdot N^{2 \cdot c \cdot \Delta}.$$

Assume now that for each component X , of maximal dimension, there exists $m^c \in \Sigma$ such that $\dim(X' = X'(m)) < \dim(X)$, and let V' be the union the X' 's and the lower dimensional components of V . In a similar way we can control the degree of V' :

$$\deg(V') \leq \deg(V)^2 \cdot N^{2 \cdot c \cdot \Delta}.$$

The above, combined with the explicit bounds for the Jacobsthal's function discussed in Section 3.2, give the second conclusion.

We are left to the case where the above assumption fails. That is the desired $m \in \Sigma$ can not be found for some Δ -dimensional component X of V . In other words

$$(3.11) \quad X \subseteq \bigcap_{m^c \in \Sigma} [m^c](V).$$

We show that, if this is the case, then the first conclusion holds. Assuming that X satisfies (3.11), it is enough to prove that the following properties hold true:

- (1) X is a special subvariety, say of the form $\alpha + B$, for some torsion point $\alpha \in A$ and B an abelian subvariety of A ;
- (2) The order of X is bounded by $\text{ord}(X) \leq n^c = d^{o(1)}$ (and the same applies for the order of $l\alpha + B$, for $l \in L$)²;
- (3) For every $l \in L$, $l\alpha + B$ is a component of V .

Letting Z be the union of such components provides the first conclusion.

Proof of (1). From the set Σ , defined in (3.10), pick

$$q_1 = (p_1)^c < q_2 = (p_2)^c < \dots < q_{D+1} = (p_{D+1})^c,$$

such that

$$(3.12) \quad \sqrt{D} \leq q_1 < q_{D+1} \leq n^c,$$

²The estimate $n^c = d^{o(1)}$ follows from the more precise (3.9).

and $p_1, \dots, p_{D+1}$ relatively prime to each other. For simplicity we can find these p_i 's among prime numbers, which are known to abound. We can actually choose the q_i 's among

$$\Sigma \cap \{p(\left\lceil \sqrt[2^c]{D} \right\rceil)^c, \dots, p(\left\lceil \sqrt[2^c]{D} \right\rceil + D + \omega(d) + 1)^c\},$$

to take care that we might have at most $\omega(d)$ primes dividing d , and to exclude at most one more prime, accounting for the characteristic p of the base field k . The lower bound in (3.12) then holds, as well as the upper bound, as n was defined for this very purpose (the choice of N will be clear later).

For every $q \in \{q_1, \dots, q_{D+1}\}$ (or more generally in the set Σ) by assumption (3.11), we have

$$X \subseteq [q](V),$$

and so there exists at least a component $Y(q)$ of V such that

$$X \subseteq [q](Y(q)).$$

Since X is a component of maximal dimension, it follows that $X = [q](Y(q))$. As q ranges through $\{q_1, \dots, q_{D+1}\}$ the numbers of distinct $Y(q_i)$ cannot be more than $\deg(V) = D$. That is, a collision must occur. We have

$$Y(q_{i_1}) = Y(q_{i_2}),$$

with $1 \leq i_1 \neq i_2 \leq D+1$ (this is why we have chosen to work with $D+1$ numbers). Write $Y := Y(q_{i_1}) = Y(q_{i_2})$, we have

$$\deg(Y) \leq \deg(V) = D \quad \text{and} \quad [q_{i_1}](Y) = X = [q_{i_2}](Y).$$

As we guaranteed that $D < (q_{i_1}q_{i_2})^2$, Proposition 2.3.4 implies that Y is special. Hence so is X . $\square$

This covers the first claim, and we are now ready to bound $\text{ord}(X)$.

Proof of (2). Thanks to (1), we can find an abelian subvariety $B \subset A$ such that $Y = \alpha_Y + B$, for some torsion point $\alpha_Y \in A$, and we may assume that $\text{ord}(Y) = \text{ord}(\alpha_Y)$ by the general assumptions. We then have

$$X = q_{i_1} \cdot \alpha_Y + B = q_{i_2} \cdot \alpha_Y + B.$$

Necessarily we have the divisibility

$$\text{ord}(Y) \mid |q_{i_1} - q_{i_2}| \leq n^c.$$

On the other hand we know, for some $l \in L$, that $la + A' \subset Y$, and so

$$\text{ord}(Y) \mid \text{ord}(l \cdot a + A') = \text{ord}(a + A') = d.$$

Hence each q in the set Σ is relatively prime to $\text{ord}(Y)$ (sine it is relatively prime to d). We deduce that $\text{ord}(X) = \text{ord}(Y) \leq n^c$, concluding the proof of (2). $\square$

Set $d' := \text{ord}(X)$. We are left to prove that for every $l \in L$, $l\alpha + B$ is a component of V . Namely, for any $1 \leq j < d'$ such that $j \wedge d' = 1$, we have

$$[j^c](X) \subseteq V.$$

To take care of the fact that such a j^c , a priori, does not lie in the set Σ (since $j \wedge d$ could be different from 1), we use some results on the Jacobsthal's function $g(d)$, as discussed in Section 3.2. It is only in this proof that we need to argue with N , rather than n .

Proof of (3). We choose an inverse $j^* + d'\mathbb{Z}$ of $j + d'\mathbb{Z}$, represented by some $1 \leq j^* < d'$. By Proposition 3.2.1 there is some m such that $m \equiv j^* \pmod{d'}$, relatively prime to d and not divisible by p , satisfying

$$m \leq d' \cdot g((d \cdot \max\{1, p\})/d') \leq n^c \cdot g(d \cdot \max\{1, p\}) = N,$$

since, by (2), $d' \leq n^c$ (this explains our definition of N). Therefore m^c belongs to the set $\Sigma = \Sigma(d, D)$, defined in (3.10). In particular we have

$$X = [m^c](Y(m^c)),$$

for the component $Y = Y(m^c)$ of V . We know, for some $l \in L$, that $a_Y := l \cdot a$ belongs to Y and we can write $Y = a_Y + B$, for some abelian subvariety B of A . Therefore

$$X = [m^c](Y) = m^c \cdot a_Y + B.$$

Applying $[j^c]$, the above identity becomes

$$[j^c](X) = [(jm)^c](a_Y + B) = (jm)^c \cdot a_Y + B.$$

But $\text{ord}(a_Y + B) = d'$ and $jm \equiv 1 \pmod{d'}$, so $[j^c](X) = Y$ is indeed a component of V . $\square$

The proof of Lemma 3.2.2 is completed. $\square$

3.2.2. Second lemma. We refine the conclusion of Lemma 3.2.2, constructing a special subvariety in V of explicitly bounded degree.

Lemma 3.2.3. *Under the same assumptions and notations of Proposition 3.1.1, there is Z such that*

$$L \cdot a + A' \subseteq Z \subseteq V,$$

and of the form $L \cdot \alpha + B$, for some abelian subvariety $B \subset A$, and $\alpha \in A_{\text{tors}}$, such that

$$\deg(Z) \leq D^{O(1)} \cdot d^{o(1)}.$$

The proof of the above result is obtained by induction from Lemma 3.2.2. Notice that, for every $l \in L$, we have

$$\text{ord}(l\alpha + B) \leq \deg(Z) \leq D^{O(1)} \cdot d^{o(1)},$$

which is exactly what we need. During the proof we will actually prove that

$$\deg(Z) \leq \max\{D, (\omega(d) + 1)\}^{\delta(\Delta, c)} (2 \cdot g(d \cdot \max\{1, p\}))^{\delta'(\Delta, c)},$$

where $\delta(\Delta, c)$ and $\delta'(\Delta, c)$ are explicit constant depending only on Δ and c (see (3.13) for their definition).

Proof. We define inductively

$$f_0(D) = D, \quad f_{i+1}(D) = f(f_i(D), d),$$

where $f(D, d) = D^2 \cdot (n^c \cdot g(d \cdot \max\{1, p\}))^{2 \cdot c \cdot \Delta}$ was defined in (3.7), for $n = p(x)$, and $x = x_D := 2D + \omega(d) + 1$. For simplicity, from now on, we ignore the factor $\max\{1, p\}$ in the argument of the Jacobsthal's function. For example, we have

$$f_2(D, d) = (D^2 n^{2c^2 \Delta} g(d)^{2c \Delta})^2 (n_2^c g(d))^{2c \Delta} = D^2 n^{2c^2 \Delta} n_2^{2c^2 \Delta} g(d)^{6c \Delta},$$

where $n_2 = p(x_2)$, and

$$x_2 := x_{f(D, d)} = 2f(D, d) + \omega(d) + 1 = 2D^2 \cdot (n^c \cdot g(d))^{2 \cdot c \cdot \Delta} + \omega(d) + 1.$$

Set also

$$V_0 = V, \quad V_{i+1} = V'_i,$$

with V'_i to be V' constructed from Lemma 3.2.2 applied to the V_i . The latter is defined until i_0 , for some i_0 , where the first point of Lemma 3.2.2 occurs, and in this case we obtain Z with $\deg(Z) \leq \deg(V_{i_0})$ and of the form $L \cdot \alpha + B$, for some abelian subvariety $B \subset A$, and $\alpha \in A_{\text{tors}}$. This has to happen for some $i_0 \leq \Delta$, since at each step the dimension is dropping by one, and each V_i is not empty.

The functions $f_i(D)$ are increasing in both D and i , and so we can carry over upper bounds and rely on the computation below. For example, for any i , we get

$$\deg(V_i) \leq f_i(D) \leq D' := f_\Delta(D),$$

which will be bounded in an explicit way in (3.13) below.

Set $D_* := \max\{D, \omega(d) + 1\}$, and notice that

$$4 \leq x = 2D + \omega(d) + 1 \leq 3D_*.$$

In particular we can write

$$n = p(x) \leq x \log(x)(1 + \log \log(x)) \leq 3D_* \log(3D_*)(1 + \log \log(3D_*)) \leq D_*^{1+\epsilon},$$

for some $\epsilon > 0$, and

$$f_1(D) = f(D, d) = D^2 \cdot n^{2c^2\Delta} \cdot g(d)^{2 \cdot c \cdot \Delta} \leq D_*^{2(1+c^2 \cdot \Delta \cdot (1+\epsilon))} \cdot g(d)^{2 \cdot c \cdot \Delta}.$$

To bound the $f_i(D)$, for $1 < i \leq \Delta$ we argue inductively. A direct computation shows that

$$(3.13) \quad f_\Delta(D) = D' \leq D_*^{2^\Delta(1+\lambda)} \cdot (2 \cdot g(d))^{2^{(\Delta+1)}c\Delta} \quad \text{with } \lambda = c^2 \cdot \frac{\Delta^2 - \Delta}{2} \cdot (1 + \epsilon),$$

$$(3.14) \quad = \max\{D, (\omega(d) + 1)\}^\delta \cdot (2 \cdot g(d))^{\delta'} \quad \text{with } \begin{cases} \delta = \delta(\Delta, c) = 2^\Delta(1 + \lambda); \\ \delta' = \delta'(\Delta, c) = 2^\Delta \lambda / c. \end{cases}$$

where $\epsilon = 0.5$ will always do. We have therefore proven the desired bound

$$\deg(Z) \leq D^{O(1)} \cdot d^{o(1)}.$$

□

3.2.3. Proof of Proposition 3.1.1. Let V be a subvariety of A of degree D and dimension $\Delta < g$, and $a \in A_{\text{tors}}$, of order d , such that $L \cdot a \subseteq V$, where $L = L(c)$ is the Lang group as in (2.1). Consider the set Θ of subvarieties of V of the form

$$Y = L \cdot a_Y + B_Y,$$

where $a_Y \in A_{\text{tors}}$ and B_Y is an abelian subvariety of A , such that $L \cdot a \subseteq Y$. Notice that $a \in \Theta$, and in particular $\Theta \neq \emptyset$. We can choose a $Y_{\min} = L \cdot a_{\min} + B_{\min}$ such that the order of the coset $a_{\min} + B_{\min}$ is minimal among the elements in Θ . Lemma 3.2.3, applied to the pair $(a_{\min} + B_{\min} \in A_{\text{tors}}, V)$ asserts that there exists $Z = L\alpha_Z + B_Z$, containing $Y_{\min}$, and of order bounded by $d^{o(1)}$, and implicit constant depending only on D, Δ, c^3 . Let $\delta = \delta(D, \Delta, c)$ be the biggest number such that $d^{o(1)} < d$, for all $d \geq \delta$. My minimality of the order of $a_{\min}$, it follows that

$$\text{ord}(a_{\min}) \leq \min\{\delta, d\}$$

and therefore $Y_{\min} = L \cdot a_{\min} + B_{\min}$ satisfies the desired conclusion. Proposition 3.1.1 is proven.

³Here is where we needed a version of Lemma 3.2.3 for torsion cosets, rather than for just torsion points.

3.3. Proof of Theorem 1.3.1, and Theorem 1.2.1. We are ready to prove Theorem 1.3.1, which, as explained in Section 2.2, implies Theorem 1.2.1. Let $\mathcal{A}$ be an abelian scheme over $\mathcal{O}_{K,S}$.

Proof of horizontal part of Theorem 1.3.1. Let $(E_n)_{n \geq 0} \subset \mathcal{A}$ be a sequence of special 0-cycles associated to $a_n \in A_{\text{tors}}$ and $\mathfrak{p}_n \in \text{Spec}(\mathcal{O}_{K,S})$. Consider the image of the a_n along the corresponding map

$$\pi_n : A(\overline{K}) \rightarrow \mathcal{A}_{\mathfrak{p}_n}(\overline{\kappa(\mathfrak{p}_n)}).$$

Denote by d_n the order of $a_n \in A$, and by d'_n the order of $\pi_n(a_n)$ in $\mathcal{A}(\overline{\kappa(\mathfrak{p}_n)})$.

We study $\mathcal{V}$, the Zariski closure of $\bigcup_{n \geq 0} E_n$ in $\mathcal{A}$. It is a finite union of vertical fibres and horizontal components (i.e. flat over the base $\text{Spec}(\mathcal{O}_{K,S})$). We may assume that d_n and d'_n tend to infinity, as n grows, since otherwise $\mathcal{V}$ is special (by definition). Notice that, for any $n \geq 0$, we have

$$L \cdot \pi_n(a_n) = \pi_n(L \cdot a_n) \subseteq E_n.$$

We first look at the horizontal/flat part, even if the same argument applies to the vertical case, so, up to extracting a subsequence, we may assume that $|\mathfrak{p}_n| \rightarrow +\infty$. Set D for the maximum, over n , of $\deg(V_{\mathfrak{p}_n})$, $\Delta := \dim(V_K)$, and let δ for the maximum of $\delta(\deg(V_{\mathfrak{p}_n}), \Delta, c)$ be as in Proposition 3.1.1 applied to the pair $\pi_n(a_n)$ and $V_{\mathfrak{p}_n} \subset \mathcal{A}_{\mathfrak{p}_n}$ (it is a finite set, since $\deg(V_{\mathfrak{p}_n})$ takes only finitely many values as n varies). We can find a positive integer q such that

- q is a c -th power;
- q is relatively prime to δ ;
- q is relatively prime to $p_n := \text{char}(\kappa(\mathfrak{p}_n))$, for all n bigger than a given constant M .

Proposition 3.1.1 asserts that, for each torsion point $\pi_n(a_n) \in \mathcal{A}_{\mathfrak{p}_n}$, we have

$$L \cdot \pi_n(a_n) \subseteq (L \cdot \alpha_n + B_n) \subseteq \mathcal{V},$$

for some $\alpha_n \in \mathcal{A}_{\mathfrak{p}_n}$, with $\text{ord}(\alpha_n + B_n) \leq \delta$ (in particular the order of α_n does not depend on d'_n , nor on p_n), and $B_n \subset \mathcal{A}_{\mathfrak{p}_n}$ an abelian subvariety. Notice that

$$L \cdot \alpha_n + B_n$$

is stable under the multiplication by $[q]$ (by definition of L). In particular $\mathcal{V}$ can be written as the Zariski closure of the set

$$\left(\bigcup_{n \geq M} L \cdot \alpha_n + B_n \right) \subseteq \mathcal{V}.$$

As explained above, the left hand side is stable under multiplication by $[q]$, and so $\mathcal{V}$ itself is stable under $[q]$. Corollary 2.3.5, applied to $\mathcal{V}_K \subseteq A$, shows that $\mathcal{V}_K$ is special. This means, following the definitions introduced in Section 1.2, that the horizontal part of $\mathcal{V}$ is a finite union of flat cycles. $\square$

To conclude the proof of Theorem 1.3.1, we have to show that the vertical part of $\mathcal{V}$ is a finite union of torsion cycles, essentially by adapting the argument just presented. The lifting argument is more delicate, and presents some challenges depending on the order of the torsion points a_n , this will be dealt with in the next section.

Proof of the Weak vertical part of Theorem 1.3.1. We are left to consider the case where $(E_n)_{n \geq 0} \subset \mathcal{A}$ is a sequence of special 0-cycles associated to $(a_n)_n \subset A_{\text{tors}}$ and a fixed $\mathfrak{p} \in \text{Spec}(\mathcal{O}_{K,S})$. Consider the image of the a_n along the corresponding map $\pi_{\mathfrak{p}} : A(\overline{K}) \rightarrow \mathcal{A}_{\mathfrak{p}}(\overline{\kappa(\mathfrak{p})})$. Let d'_n be the order of $\pi_{\mathfrak{p}}(a_n) \in \mathcal{A}_{\mathfrak{p}}(\overline{\kappa(\mathfrak{p})})$. If the d'_n are bounded as n goes to infinity, then the set $\bigcup_{n \geq 0} E_n$ is finite and so there is nothing to prove. We may therefore assume that the d'_n are unbounded.

The argument described above implies that every component of $\mathcal{V}$ is a translate of an abelian subvariety of $\mathcal{A}_p$. Indeed, let c be the constant associated to A by Theorem 2.2.1, and let $\delta = \delta(\deg(\mathcal{V}), \dim(\mathcal{V}), c)$ be the constant given by Proposition 3.1.1 applied to $\mathcal{V} \subset \mathcal{A}_p$ (and any $\pi_p(a_n)$). We can find a positive integer q such that q is a c -th power, and $q \wedge \delta p = 1$. Proposition 3.1.1 asserts that, for each torsion point $\pi_p(a_n) \in \mathcal{A}_p$, we have

$$L \cdot \pi_p(a_n) \subseteq \pi_p(L \cdot a_n) \subseteq (L \cdot \alpha + \mathfrak{B}_n) \subseteq \mathcal{V},$$

for some $\alpha \in \mathcal{A}_p(\overline{\kappa(\mathfrak{p})})$, with $\text{ord}(\alpha + \mathfrak{B}_n) \leq \delta$, for some δ depending only on D, Δ and c (where $\mathfrak{B}_n$ is some abelian subvariety of $\mathcal{A}_p$). Notice that $L \cdot \alpha + \mathfrak{B}_n$ is stable under the multiplication by $[q]$. Since $\mathcal{V}$ is defined as the Zariski closure of the E_n , and from the fact that δ does not depend on d'_n , it follows that $\mathcal{V}$ is stable under the multiplication by $[q]$. Proposition 2.3.4 then shows that $\mathcal{V}$ is special, that is a finite union of translates by a (torsion) point of $\mathcal{A}_p(\overline{\kappa(\mathfrak{p})})$ of abelian subvarieties of $\mathcal{A}_p$. The proof of Theorems 1.2.1 and 1.3.1 is completed. $\square$

The last statement will be referred to as the *weak vertical part* of the arithmetic Manin–Mumford. The *stronger* part, that is the lift of the torsion cosets of $\mathcal{A}_p$ to K , possibly up to p -rank zero factors, is described in the next two sections.

4. STRONG VERTICAL, THEOREM 1.2.3

In this section we prove Theorem 1.2.3, which may be of independent interest from the arguments presented so far. As in Section 1.2, K denotes a number field and S a finite set of finite places of K . To explain the method of the proof we first prove the following easier statement, which appeared in the introduction as Theorem 1.2.4. It can be thought as the analogue of the main theorem of Edixhoven and Richard [8] for abelian varieties (rather than $\mathbb{A}^1 \times_{\mathbb{Z}} \mathbb{A}^1$).

Theorem 4.0.1. *Fix a prime $\mathfrak{p} \subset \mathcal{O}_{K,S}$ of residue characteristic $p > 0$. Let $\mathcal{A}$ be an abelian scheme over $\mathcal{O}_{K,S}$, $(a_n)_n \subset A_{\text{tors}}$ be a sequence of torsion points of order coprime with p and write $E_n = \pi_p(\text{Gal}(\overline{K}/K) \cdot a_n)$, where $\pi_p : A(\overline{K}) \rightarrow \mathcal{A}_p(\overline{\kappa(\mathfrak{p})})$. Then every component of the Zariski closure $\mathcal{V}$ of*

$$\bigcup_{n \geq 0} E_n \subseteq \mathcal{A}_p \subset \mathcal{A},$$

is a component of the intersection between a flat cycle $\mathcal{B} \subseteq \mathcal{A}$ and $\mathcal{A}_p$.

The novelty of Theorem 4.0.1, compared to Theorem 1.2.1, is that the components of $\mathcal{V}$ are not only given by torsion cycles of $\mathcal{A}_p$, but they actually come from characteristic zero. The case where torsion points are allowed to have order divisible by p will be addressed in Section 5. From now on, we let p be the characteristic of the residue field $\kappa(\mathfrak{p})$.

Before proving Theorem 4.0.1, we explain how it implies Theorem 1.2.3.

4.0.1. Proof of Theorem 1.2.3. Assuming Theorem 4.0.1, which will be proven in Section 4.3, we show how to conclude the proof of the more general Theorem 1.2.3, as stated in the introduction. Let E_n be a sequence of special zero cycles in $\mathcal{A}$, each one associated to $a_n \in A_{\text{tors}}$ and primes $\mathfrak{p}_n \subset \mathcal{O}_{K,S}$.

Let $\mathcal{V} \subseteq \mathcal{A}$ be the Zariski closure of the $(E_n)_n$, and write it as a finite union of flat and vertical components. From Theorem 1.2.1, which was proven in Section 3.3, we know that the flat part is a finite union of flat cycles, and that each vertical component at $\mathfrak{p}_1, \dots, \mathfrak{p}_m \subset \mathcal{O}_{K,S}$ is a torsion cycle of some $\mathcal{A}_{\mathfrak{p}_j}$ for $j \in \{1, \dots, m\}$. Theorem 4.0.1, applied at $\mathfrak{p}_1, \dots, \mathfrak{p}_m$, now implies that each torsion cycle is given as the intersection between a flat cycle and vertical fibres. That is $\mathcal{V}$ can be written as a

finite union of flat cycles and intersections between flat cycles and vertical fibres. This concludes the proof of Theorem 1.2.3.

4.1. Variants of the Tate conjecture (after Faltings et. al.) We recall Faltings's results about the *semi-simplicity of the Tate module* and the *Isogeny Theorem* (or often referred to as the *Tate conjecture*) and some variants thereof.

Theorem 4.1.1. *Let K be a number field, and A an abelian variety over K .*

- (Faltings [9].) *Let ℓ be a rational prime, and $V_\ell(A)$ the rational ℓ -adic Tate module of A . The canonical map*

$$(4.1) \quad \text{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \rightarrow \text{End}_{\text{Gal}(\overline{K}/K)}(V_\ell(A))$$

is an isomorphism.

- (Faltings, Zarhin [34, Section 5.4].) *For any ℓ large enough, the $\text{Gal}(\overline{K}/K)$ -module $A[\ell]$ is semisimple, and the canonical map*

$$(4.2) \quad \text{End}_K(A) \otimes \mathbb{Z}/\ell\mathbb{Z} \rightarrow \text{End}_{\text{Gal}(\overline{K}/K)}(A[\ell])$$

is an isomorphism.

- (Masser-Wüstholz [23, 22].) *For any positive integer m , the cokernel of the canonical map*

$$(4.3) \quad \text{End}_K(A) \rightarrow \text{End}_{\text{Gal}(\overline{K}/K)}(A[m])$$

is killed by M , for some positive integer $M \leq c(\max\{1, h(A)\})^\tau$, where τ is a constant depending only on $[K : \mathbb{Q}]$, and c depends only on $\dim A$ and $[K : \mathbb{Q}]$.

- ([12, Theorem 4.2, Ch. IV (page 147)]) *Let $(\ell_n)_{n \in \mathbb{N}}$ be a sequence of distinct prime numbers and let $R = \prod_{n \in \mathbb{N}} \mathbb{F}_{\ell_n}$. Since $R \otimes_{\mathbb{Z}} \mathbb{Q}$ is a non-zero⁴ $\mathbb{Q}$ -algebra, there exists a field E (of characteristic zero) and a ring map $R \otimes_{\mathbb{Z}} \mathbb{Q} \rightarrow E$ corresponding to some maximal ideal. Let $V_E(A) := T(A) \otimes_{\widehat{\mathbb{Z}}} R \otimes_{\mathbb{Q}} E$ be the E -Tate module of A . The canonical map*

$$(4.4) \quad \text{End}_K(A) \otimes_{\mathbb{Z}} E \rightarrow \text{End}_{\text{Gal}(\overline{K}/K)}(V_E(A))$$

is an isomorphism.

Moreover $V_\ell(A)$, $A[\ell]$, $V_E(A)$ are semisimple representation of $\text{Gal}(\overline{K}/K)$.

4.2. Preliminary results.

4.2.1. First descent lemma. We start with a formal descent lemma for idempotents in scalar extensions of semisimple algebras.

Lemma 4.2.1. *Let M, N be semisimple (associative, non necessarily commutative, finite dimensional) $\mathbb{Q}$ -algebras, with M a subalgebra of N . Let $E/\mathbb{Q}$ be a field extension, and*

$$i_E : N \otimes_{\mathbb{Q}} E \hookrightarrow \text{End}_E(V)$$

be a faithful representation on V , a finite dimensional E -linear vector space. If u is an idempotent of N , and $w \in M \otimes_{\mathbb{Q}} E$ is such that $i_E(w) \cdot V \subseteq i_E(u) \cdot V$, then there exists an idempotent $v \in M$ satisfying

$$i_E(w) \cdot V \subseteq i_E(v) \cdot V \subseteq i_E(u) \cdot V.$$

⁴The kernel of the map $R \rightarrow R \otimes_{\mathbb{Z}} \mathbb{Q}$ is the set of elements $r \in R$ such that $M \cdot r = 0$ for some $M \in \mathbb{Z}_{>1}$. Let $r = 1 \in R$, and M arbitrary. There exists $\ell_n \nmid M$, and, as $M \cdot 1 \neq 0$ in $\mathbb{F}_{\ell_n}$, we have $M \cdot r \neq 0 \in R$. Thus r has non zero image in $R \otimes \mathbb{Q}$.

In the proof of Lemma 4.2.1 we use the following standard fact about semisimple $\mathbb{Q}$ -algebras. Let M be a semisimple associative finite dimensional $\mathbb{Q}$ -algebra, then any $\mathbb{Q}$ -linear subspace X of M is a right ideal if and only if it is of the form vM for some idempotent v of M .

Proof of Lemma 4.2.1. Consider $Y = uN$, as a right N linear submodule of N . Let $X := Y \cap M$ be the associated right M -module. By the previous fact, there is at least one idempotent $v \in M$ with the following property: for any m in M we have $u \cdot m = m$ if and only if $v \cdot m = m$. Otherwise stated, we have $X = v \cdot M$. The same property holds true with elements in $M \otimes E$. It is indeed enough to notice, just by computing dimensions, that we have $(Y \otimes_{\mathbb{Q}} E) \cap (M \otimes_{\mathbb{Q}} E) = X \otimes_{\mathbb{Q}} E$.

As $\text{Im}(i_E(w))$ is a submodule of $\text{Im}(i_E(u))$, by assumption, and $i_E(u)$ is an idempotent, we conclude that $i_E(u \cdot w) = i_E(w)$. By faithfulness of i_E , we have also $u \cdot w = w \in N \otimes_{\mathbb{Q}} E$.

Let $v \in M$ be the idempotent associated to $u \in N$ as above. It follows that

$$i_E(v) \cdot i_E(w) = i_E(w),$$

that is

$$\text{Im}(i_E(w)) \subseteq \text{Im}(i_E(v)).$$

Finally, as $v \in vM \subset uN$, we get $u \cdot v = v$, and likewise

$$\text{Im}(i_E(v)) \subseteq \text{Im}(i_E(u)).$$

In another writing, this is indeed

$$i_E(w) \cdot V \subseteq i_E(v) \cdot V \subseteq i_E(u) \cdot V.$$

□

4.2.2. Applications. We first present the simplest result we use to lift torsion cycles, it encompasses the power of (4.1), making it ready to be applied for our purposes. Let A be an abelian variety over K , $\mathcal{A}_{\mathfrak{p}}$ its reduction mod $\mathfrak{p}$, a place of good reduction. Set $p = \text{char}(\kappa(\mathfrak{p})) > 0$, and

$$M^0 := \text{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}, \quad N^0 := \text{End}_{\kappa(\mathfrak{p})}(\mathcal{A}_{\mathfrak{p}}) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

The reduction mod $\mathfrak{p}$ defines a canonical embedding $M^0 \hookrightarrow N^0$, and, for every $\ell \neq p$, we have

$$M^0 \otimes \mathbb{Q}_{\ell} \hookrightarrow N^0 \otimes \mathbb{Q}_{\ell} \hookrightarrow \text{End}_{\mathbb{Q}_{\ell}}(V_{\ell}(A)),$$

thanks to the identification $V_{\ell}(A) \cong V_{\ell}(\mathcal{A}_{\mathfrak{p}})$ given again by the reduction mod $\mathfrak{p}$.

Proposition 4.2.2. *Let W be a $\text{Gal}(\overline{K}/K)$ -invariant subspace of $V_{\ell}(A)$ and let $\mathfrak{B} \subseteq \mathcal{A}_{\mathfrak{p}}$ be an abelian subvariety such that*

$$W \subseteq V_{\ell}(\mathfrak{B}) \subseteq V_{\ell}(A).$$

There exists an abelian subvariety D of A , defined over K , such that

$$W \subseteq V_{\ell}(D) \subseteq V_{\ell}(\mathfrak{B}).$$

Notice that Proposition 4.2.2 can be rewritten in purely algebraic terms. Here M^0 and N^0 are finite dimensional semisimple $\mathbb{Q}$ -algebras. Moreover $\mathfrak{B} \subseteq \mathcal{A}_{\mathfrak{p}}$ corresponds to an idempotent $u = u^2 \in N^0$ such that

$$W \subseteq u \cdot V_{\ell}(A),$$

and Proposition 4.2.2 asserts that there exists an idempotent v in M^0 such that

$$W \subseteq v \cdot V_{\ell}(A) \subseteq u \cdot V_{\ell}(A).$$

Proof of Proposition 4.2.2. Since $V_\ell(A)$ is a semisimple Galois representation, as explained at the end of Theorem 4.1.1, we have that $W \subseteq V_\ell(A)$ is of the form $e \cdot V_\ell(A)$ for some idempotent $e \in \text{End}_{\text{Gal}(\bar{K}/K)}(V_\ell(A))$. By the Tate conjecture ((4.1) in Theorem 4.1.1) we can actually write

$$W = w \cdot V_\ell(A)$$

for some $w \in M^0 \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ (and such w is unique by faithfulness). Lemma 4.2.1, applied with $E = \mathbb{Q}_\ell$, shows how to get v in M^0 (rather than in $M^0 \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$) such that the conclusion holds. $\square$

Replacing in the proof of Proposition 4.2.2 the role of the ℓ -adic Tate conjecture by the *adelic Tate conjecture* (4.4), we obtain:

Proposition 4.2.3. *Let $(\ell_n)_{n \geq 0}$ be a sequence of distinct primes different from p , and let E be the field associated to $\mathbb{Q} \otimes \prod_n \mathbb{F}_{\ell_n}$ as in (4.4). Let W be a $\text{Gal}(\bar{K}/K)$ -invariant subspace of $V_E(A)$ and let $\mathfrak{B} \subseteq \mathcal{A}_p$ be an abelian subvariety such that*

$$W \subseteq V_E(\mathfrak{B}) \subseteq V_E(A).$$

There exists an abelian subvariety D of A , defined over K , such that

$$W \subseteq V_E(D) \subseteq V_E(\mathfrak{B}).$$

4.2.3. Combinatorial result. We describe a combinatorial result that will be used in the proof of Proposition 4.3.1. Let ℓ be a prime number, $\mathbb{F} := \mathbb{F}_\ell$ the field with ℓ elements and d a positive integer.

Proposition 4.2.4. *Let $\mathbb{F}^d$ be a d -dimensional $\mathbb{F}$ -vector space and let $a \in \mathbb{F}^d$. Let $G \leq \text{GL}_d(\mathbb{F})$ be a subgroup. If $V \subseteq \mathbb{F}^d$ is a subvector space such that, for some $1 \leq C \leq \infty$,*

$$\#\{G \cdot a \cap V\} \geq \frac{1}{C} \#\{G \cdot a\},$$

then there exists a non trivial subvector space $W \subseteq V$ such that

$$(4.5) \quad [G : \text{Stab}_G(W)] \leq 3 \cdot C^{4^{\dim(V)}}.$$

Moreover $G \cdot a \cap W \neq \emptyset$ and it generates W .

Corollary 4.2.5. *With the notation of Proposition 4.2.4, in particular W and V contain the orbit $H \cdot g \cdot a$, for some $g \in G$, under the subgroup $H = \text{Stab}_G(W) \subseteq G$, and $[G : H] \leq 3 \cdot C^{4^{\dim V}}$.*

The proof is inspired by the arguments of [4, Section 3].

Proof of Proposition 4.2.4. Given a subset $S \subseteq G \cdot a$ and $W \subseteq \mathbb{F}^d$, we set

$$\varepsilon(S) := \frac{\#S}{\#G \cdot a}, \quad \varepsilon(W) := \varepsilon(G \cdot a \cap W) = \frac{\#\{G \cdot a \cap W\}}{\#G \cdot a}.$$

Write $\langle S \rangle = \sum_{s \in S} \mathbb{F} \cdot s$ for the subvector space of $\mathbb{F}^d$ generated by S . Notice that $0 \leq \varepsilon(W) \leq 1$.

We argue considering subvector spaces $W \subseteq V$ chosen to be of minimal dimension among all subvector spaces of V and maximizing the quantity

$$\varepsilon(W)^{4^{\dim(W) - \dim(V)}}.$$

Such W exists since there are only finitely many possibilities for $\varepsilon(W)$ and $\dim(W)$. In particular we have

$$(4.6) \quad \varepsilon(W)^{4^{\dim(W) - \dim(V)}} \geq \varepsilon(V)^{4^0} > 0,$$

and

$$(4.7) \quad (1/\varepsilon(W)) \leq (1/\varepsilon(V))^{4(\dim(V)-\dim(W))} \leq (1/\varepsilon(V))^{4\dim(V)} \leq C^{4\dim(V)}.$$

Comparing W to all its subvector spaces $W' \subsetneq W$, we also have

$$(4.8) \quad \varepsilon(W') < \varepsilon(W)^{4(\dim(W)-\dim(W'))} \leq \varepsilon(W)^4 \leq \varepsilon(W).$$

We consider $S := W \cap (G \cdot a)$, and notice that it generates W , since otherwise $W_S = \langle S \rangle$ would contradict the inequality (4.8). The following simple observations will be useful for the sequel:

- If $gW = W$, then $gS = g(G \cdot a \cap W) = gG \cdot a \cap gW = G \cdot a \cap W = S$;
- Reciprocally, if $gS = S$ then $gW = g\langle S \rangle = \langle gS \rangle = \langle S \rangle = W$.

Denote by $G(W) \subseteq G$ the stabiliser of W in G (which is also the stabiliser of S). If $gS \neq S$, the vector space $W' := gW \cap W$ satisfies $W' < W$, as well as

$$gS \cap S \subseteq gW \cap W < W.$$

The inequality (4.8) then gives

$$\frac{\#gS \cap S}{\#G \cdot a} \leq \frac{\#(G \cdot a \cap W')}{\#G \cdot a} = \varepsilon(W') < \varepsilon(W)^4.$$

More generally, given $g \cdot G(W) \neq g' \cdot G(W)$, we similarly find

$$(4.9) \quad \frac{\#gS \cap g'S}{\#G \cdot a} \leq \frac{\#g'^{-1}gS \cap S}{\#G \cdot a} < \varepsilon(W)^4.$$

To ease the notation, from now on, we simply set $\varepsilon = \varepsilon(W)$. Let $c = [G : G(W)]$ and choose some representative $g_1 \cdot G(W), \dots, g_c \cdot G(W)$ of $G/G(W)$. We are left to prove that $c \leq 3 \cdot 1/\varepsilon$.

Proof of the bound for c . If $c > 3 \cdot 1/\varepsilon$, we set $\gamma = \lceil 1/\varepsilon + 1 \rceil$. Recall that $0 < \varepsilon \leq 1$, and the evident bounds $1/\varepsilon + 1 \leq \gamma < 1/\varepsilon + 2$ and $\gamma \leq c$ (since $2 \leq 2 \cdot (1/\varepsilon)$). We can also notice that

$$(4.10) \quad \gamma \cdot \varepsilon \geq (1/\varepsilon + 1) \cdot \varepsilon = 1 + \varepsilon$$

$$(4.11) \quad \frac{\gamma(\gamma - 1)}{2} \cdot \varepsilon^4 < \frac{(1/\varepsilon + 1) \cdot 1/\varepsilon}{2} \cdot \varepsilon^4 = \frac{\varepsilon^2 + \varepsilon^3}{2} \leq \varepsilon^2.$$

From the above we see that the classes $g_1 \cdot G(W), \dots, g_\gamma \cdot G(W)$ are well defined and all distinct. Thanks to inclusion-exclusion we estimate:

$$(4.12) \quad \#G \cdot a \geq \# \bigcup_{i=1}^{\gamma} g_i S \geq \sum_{i=1}^{\gamma} \#g_i S - \sum_{1 \leq i < j \leq \gamma} \#(g_i S \cap g_j S).$$

The number of terms of the last summation is $(\gamma(\gamma - 1))/2$, and each term is bounded, via (4.9), by $\varepsilon^4 \cdot \#G \cdot a$. Therefore

$$(4.13) \quad \sum_{1 \leq i < j \leq \gamma} \# \{g_i S \cap g_j S\} \leq \frac{\gamma(\gamma - 1)}{2} \cdot \varepsilon^4 \cdot \#G \cdot a$$

For the second to last summation in (4.12), we notice that

$$(4.14) \quad \sum_{i=1}^{\gamma} \#g_i S = \gamma \cdot \varepsilon \cdot \#G \cdot a \geq (1/\varepsilon + 1) \cdot \varepsilon \cdot \#G \cdot a = (1 + \varepsilon) \cdot \#G \cdot a.$$

Substituting (4.14) and (4.13) in (4.12), and simplifying by $\#G \cdot a > 0$, we obtain the inequality

$$1 > 1 + \varepsilon - \varepsilon^2,$$

which is the contradiction we were aiming for, since the right hand side satisfies $1 + \varepsilon - \varepsilon^2 \geq 1$. $\square$

To conclude the proof of Proposition 4.2.4, we are left to show that

$$c = [G : G(W)] \leq 3/\varepsilon.$$

This concludes the proof of the Proposition. $\square$

4.3. Proof of Theorem 4.0.1. As we show in Section 4.3.1, the proof of Theorem 4.0.1 follows from Theorem 1.2.1 (the weak vertical Manin–Mumford) and the following:

Proposition 4.3.1. *Let $\mathcal{O}_{K,S}, \mathfrak{p}, p, A$ and $\pi_{\mathfrak{p}}$ be as in Theorem 4.0.1. For $i = 1, \dots, C$, let $\mathfrak{B}_i \subset A_{\mathfrak{p}}$ be abelian subvarieties of $A_{\mathfrak{p}}$. Let D_i/K be the biggest abelian subvariety of A whose reduction mod $\mathfrak{p}$ is contained in $\mathfrak{B}_i$. Let $(a_n)_{n \geq 0} \subset A_{\text{tors}}$ be a sequence of torsion points of order coprime with p and, for every n , let $E_n = \pi_{\mathfrak{p}}(\text{Gal}(\overline{K}/K) \cdot a_n)$. If*

$$\bigcup_n E_n \subset \bigcup_{i=1}^C \beta_i + \mathfrak{B}_i,$$

then there exists a finite set $F \subset A$ such that, for all n ,

$$a_n \in F + \bigcup_{i=1}^C D_i.$$

Proof. We first reduce the proof to the case in which $I := \{i \in \{1; \dots; C\} \mid D_{i,\mathfrak{p}} = \mathfrak{B}_i\}$ is $\emptyset$.

For every $i = 1, \dots, r$ let $\tilde{\beta}_i \in A_{\text{tors}}$ be a lift of β_i and let $F_i = \text{Gal}(\overline{K}/K) \cap \tilde{\beta}_i$. Let n be such that

$$(4.15) \quad \exists i \in I \text{ such that } E_n \cap \beta_i + \mathfrak{B}_i \neq \emptyset.$$

Then $\text{Gal}(\overline{K}/K) \cap a_n \cap \tilde{\beta}_i + D_i \neq \emptyset$. It follows that $\text{Gal}(\overline{K}/K) \cap a_n \subseteq F_i + D_i$. This proves the conclusion n satisfying (4.15).

We may thus assume that for every $i \in I$ and n , we have $E_n \cap \beta_i + \mathfrak{B}_i = \emptyset$. We may thus replace $\bigcup_{i \in \{1; \dots; r\}} \beta_i + \mathfrak{B}_i$ by $\bigcup_{i \in \{1; \dots; r\} \setminus I} \beta_i + \mathfrak{B}_i$.

We are reduced to the case $I = \emptyset$.

We now reduce the proof to the case in which $\beta_1 = \dots = \beta_r = 0$.

Let m_i be the order of β_i and let $m = m_1 \cdot \dots \cdot m_r$. The order of $a'_n = m \cdot a_n$ is coprime to p and the corresponding E'_n satisfy $\bigcup_n E'_n = m \cdot \bigcup_n E_n \subseteq \bigcup_{i=1}^r \mathfrak{B}_i$. Assume that, for some finite set F' , we have $a'_n \in F' + \bigcup_{i=1}^C D_i$. Then the set $F = \{a \in A \mid m \cdot a \in F'\}$ is finite and $a_n \in F + \bigcup_{i=1}^C D_i$.

It follows that we may substitute a_n with the a'_n , and assume $\beta_1 = \dots = \beta_r = 0$.

We argue by contradiction.

In particular we may pass to a subsequence of $(a_n)_n$ for which, for every $i = 1, \dots, C$, we have

$$\text{ord}(a_n + D_i/D_i) \rightarrow +\infty,$$

as $n \rightarrow +\infty$. The strategy is to find some $1 \leq i \leq C$ and a non-zero abelian subvariety $A' \subset A/D_i$ such that $A'_{\mathfrak{p}} \subseteq \mathfrak{B}_i/D_{i,\mathfrak{p}}$. The preimage of A' along the quotient map $A \rightarrow A/D_i$ would then contradict the maximality of D_i .

For every n there exists an $1 \leq i \leq C$ such that

$$\#\{\pi_{\mathfrak{p}}(\text{Gal}(\overline{K}/K) \cdot a_n) \cap \mathfrak{B}_i\} \geq \frac{1}{C} \#\{\text{Gal}(\overline{K}/K) \cdot a_n\}.$$

Extracting a subsequence, we may assume that i is fixed. For simplicity set $D = D_i$, $\mathfrak{B} = \mathfrak{B}_i$ and

$$d_n = \text{ord}(a_n), \text{ and } d'_n = \text{ord}(a_n + D/D).$$

By assumption d'_n goes to infinity. Possibly extracting a subsequence, at least one of the following is true:

- (1) There exist a rational prime number $\ell (\neq p)$ and a sequence $(k_n) \subset \mathbb{Z}_{\geq 0}$ going to infinity, as $n \rightarrow +\infty$, such that

$$\forall n, \ell^{k_n} \text{ divides } d'_n.$$

- (2) There exists an infinite sequence of distinct prime numbers $\ell_n (\neq p)$ such that

$$\forall n, \ell_n \text{ divides } d'_n.$$

We argue each case separately. The strategy is the same but the techniques is different.

Proof in Case (1). We set

$$a'_n := [d'_n / \ell^{k_n}] a_n + D/D,$$

which is an element of order ℓ^{k_n} of A/D . We say that a sequence $b_n \in A/D[\ell^{k_n}]$, of elements of order ℓ^{k_n} , converges to some $b_\infty \in T_\ell(A/D)$, the $\mathbb{Z}_\ell$ -Tate module of A/D , if there exist ϵ_n converging to $0 \in T_\ell(A/D)$ such that b_n is the reduction modulo ℓ^{k_n} of $b_\infty + \epsilon_n$. Thanks to the compactness of $T_\ell(A/D)$, we may assume that a'_n converges to some non-zero $a'_\infty \in T_\ell(A/D)$ (indeed we can pick some lifts $\tilde{a}'_n \in T_\ell(A/D)$ of a'_n and write $\tilde{a}'_n = \tilde{a}'_\infty + \epsilon_n$, with $\epsilon_n \rightarrow 0$ in $T_\ell(A/D)$).

Let $\mathcal{G}_\ell$ be the image of the natural continuous representation

$$\text{Gal}(\overline{K}/K) \rightarrow \text{GL}(V_\ell(A/D)).$$

For all n , we have⁵

$$(4.16) \quad \# \{ (\pi_{\mathfrak{p}}(\text{Gal}(\overline{K}/K) \cdot a'_n)) \cap \mathfrak{B}/D_{\mathfrak{p}} \} \geq \frac{1}{C} \# \{ \text{Gal}(\overline{K}/K) \cdot a'_n \}.$$

We define the set

$$\Sigma_n := \{ \sigma \in \mathcal{G}_\ell : \pi_{\mathfrak{p}}(\sigma \cdot a'_n) \in \mathfrak{B}/D_{\mathfrak{p}} \}.$$

For any sequence $(\sigma_n)_n \in \mathcal{G}_\ell$ such that $\sigma_n \in \Sigma_n$ for every n , for any limit of any subsequence (for the ℓ -adic topology) σ_∞ we have, along such subsequence

$$\sigma_n \cdot a'_n \rightarrow \sigma_\infty \cdot a'_\infty.$$

As $\pi_{\mathfrak{p}}(\sigma \cdot a'_n)$ belongs to $\mathfrak{B}/D_{\mathfrak{p}}$, we see that

$$\sigma_\infty \cdot a'_\infty \in V_\ell(\mathfrak{B}/D_{\mathfrak{p}}) \subseteq V_\ell(A/D),$$

where we identify $V_\ell(A/D)$ with $V_\ell(\mathcal{A}_{\mathfrak{p}}/D_{\mathfrak{p}})$ (since p different from ℓ). We define Σ_∞ to be the set of the $\sigma_\infty \in \mathcal{G}_\ell$ obtained as above.

Let μ be the Haar probability measure on $\mathcal{G}_\ell$. From the equation (4.16), we see that $\mu(\Sigma_n)$ has Haar measure at least $(1/C)$, for every n . Therefore Σ_∞ has measure at least $1/C$. Let $H_\ell/\mathbb{Q}_\ell$ be the Zariski closure of $\mathcal{G}_\ell$ in $\text{GL}(V_\ell(A/D))$ and H_ℓ^0 its neutral component. Recall that, from the Bogomolov-Serre theorem [3], $\mathcal{G}_\ell$ has finite index in $H_\ell(\mathbb{Z}_\ell)$. The Zariski closure of Σ_∞ in $\text{GL}(V_\ell(A/D))$ contains one irreducible component $H_\ell^0 \cdot \sigma_0$, for some $\sigma_0 \in \Sigma_\infty$. Let U be the subvector space of $V_\ell(A/D)$ given by $V_\ell(\mathfrak{B}/D_{\mathfrak{p}})$, and W be the $\mathbb{Q}_\ell$ -subvector space generated by $H_\ell^0(\mathbb{Q}_\ell) \cdot \sigma_0 \cdot a'_\infty$.

By Zariski density, we have that $H_\ell^0(\mathbb{Q}_\ell) \cdot \sigma_0 \cdot a'_\infty \subset U$. Notice that, by construction, W is H_ℓ^0 invariant. Let $\mathcal{G}_\ell^0 = \mathcal{G}_\ell \cap H_\ell^0$. It is a finite index subgroup of $\mathcal{G}_\ell$ which corresponds to a finite extension

⁵By abuse of notation we still denote by $\pi_{\mathfrak{p}}$ the reduction mod $\mathfrak{p}$ map $A/D(\overline{K}) \rightarrow \mathcal{A}_{\mathfrak{p}}/D_{\mathfrak{p}}(\overline{\kappa(\mathfrak{p})})$, induced by the map $\pi_{\mathfrak{p}} : A(\overline{K}) \rightarrow \mathcal{A}_{\mathfrak{p}}(\overline{\kappa(\mathfrak{p})})$.

of fields K_ℓ/K . We apply Proposition 4.2.2, with $E = \mathbb{Q}_\ell$ -coefficients to W and U . So we get a K_ℓ -abelian subvariety $A'' \subseteq (A/D)_{K_\ell}$ such that

$$(4.17) \quad V_\ell(A'') \subseteq V_\ell(\mathfrak{B}/D_{\mathfrak{p}}),$$

and

$$\mathrm{Gal}(\overline{K}/K_\ell) \cdot \sigma \cdot a'_\infty \subset W \subseteq V_\ell(A'').$$

By the reduction of Section 2.1, we have that the same holds true for some abelian subvariety $A'/K \subseteq A/D$. By definition of D , thanks to (4.17), we see that $A' = 0$, but since $0 \neq a'_\infty \in V_\ell(A')$, we must also have that $A' \neq 0$. This is the contradiction we were aiming for. $\square$

Proof in Case (2). In this case, we set

$$a'_n := [d'_n/\ell_n]a_n + D/D,$$

which is an element of order ℓ_n of A/D . Consider the ring $R := \prod_{n \geq 0} \mathbb{F}_{\ell_n}$. The sequence $(a'_n)_n$ is naturally an element of $T_{\widehat{\mathbb{Z}}}(A/D) \otimes R$, where $T_{\widehat{\mathbb{Z}}}(A/D)$ is the adelic Tate module of A/D . By assumption, we know that the order of a'_n is going to infinity, as $n \rightarrow +\infty$, and in particular $(a'_n)_n$ is not a torsion element. The image of $(a'_n)_n$ in

$$T_{\widehat{\mathbb{Z}}}(A/D) \otimes R \otimes \mathbb{Q} \cong (R \otimes \mathbb{Q})^{2 \dim(A/D)}$$

is non-zero. There exists a field E and a ring map $R \otimes \mathbb{Q} \rightarrow E$ such that the image $a'_\infty \in T_{\widehat{\mathbb{Z}}}(A/D) \otimes E$ is non-zero.

Notice that, for every n ,

$$\#\{(\pi_{\mathfrak{p}}(\mathrm{Gal}(\overline{K}/K) \cdot a'_n) \cap \mathfrak{B}/D_{\mathfrak{p}})\} \geq \frac{1}{C} \#\{\mathrm{Gal}(\overline{K}/K) \cdot a'_n\}.$$

Let $G_{\ell,n}$ be the image of $\mathrm{Gal}(\overline{K}/K)$ in $\mathrm{GL}(A/D[\ell_n])$. We can apply the combinatorial result of Section 4.2.3 (with $V = \mathfrak{B}/D_{\mathfrak{p}}[\ell_n]$) to guarantee the existence a subgroup $H_{\ell,n}$ of $G_{\ell,n}$, and a $\sigma_n \in \mathrm{Gal}(\overline{K}/K)$, such that

$$[G_{\ell,n} : H_{\ell,n}] \leq \psi(C) = 3 \cdot C^{4^2 \dim A/D},$$

and

$$\pi_{\mathfrak{p}}(H_{\ell,n} \cdot \sigma_n \cdot a'_n) \subset \mathfrak{B}/D_{\mathfrak{p}}.$$

Let $K_{H_{\ell,n}}/K$ be the finite extension of fields corresponding to $H_{\ell,n}$, and notice that $[K_H : \mathbb{Q}] \leq \psi(C)[K : \mathbb{Q}]$. Let M be the constant appearing in (4.3) from Theorem 4.1.1, for an abelian variety A/D over $K_{H_{\ell,n}}$, and notice that M is bounded independently of n . Upon extraction, we may assume that ℓ_n is strictly bigger than M for every n . Let W_n be the $\mathbb{F}_{\ell_n}$ -subvector space of $A/D[\ell_n]$ generated by $H_{\ell,n} \cdot \sigma_n \cdot a'_n$. Notice that W_n is invariant under the action of $\mathrm{Gal}(\overline{K}/K_{H_{\ell,n}})$, and so by the semisimplicity of (4.3), there exists an element $f \in \mathrm{End}(A) \otimes \mathbb{F}_{\ell_n}$, such that

$$W_n = f(A[\ell_n]).$$

Since K is such that all endomorphism of $A_{\overline{K}}$ are defined over K , we see that W_n is actually $\mathrm{Gal}(\overline{K}/K)$ -invariant. So we have, for every n ,

$$\pi_{\mathfrak{p}}(\mathrm{Gal}(\overline{K}/K) \cdot \sigma_n \cdot a'_n) \subset \mathfrak{B}/D_{\mathfrak{p}}.$$

In particular we see that

$$\mathrm{Gal}(\overline{K}/K) \cdot \sigma_\infty \cdot a'_\infty \subset V_E(\mathfrak{B}/D_{\mathfrak{p}}) \subset V_E(A/D).$$

We now conclude as in the previous case. Let indeed W be the E -subvector space generated by $\text{Gal}(\overline{K}/K) \cdot a'_\infty$. We apply Proposition 4.2.3, with E -coefficients to W and $u \in \text{End}(\mathcal{A}_p/D_p) \otimes \mathbb{Q}$ an idempotent corresponding to $\mathfrak{B}/D_p \subset \mathcal{A}_p/D_p$. So we get an abelian subvariety $A' \subseteq A/D$ such that

$$(4.18) \quad V_E(A') \subseteq V_E(\mathfrak{B}/D_p),$$

and

$$\text{Gal}(\overline{K}/K) \cdot a'_\infty \subset W \subseteq V_E(A').$$

By definition of D , thanks to (4.18), we see that $A' = 0$, but since $0 \neq a'_\infty \in V_E(A')$, we must also have that $A' \neq 0$. This is the contradiction we were aiming for. $\square$

The proof of Proposition 4.3.1 is complete. $\square$

We can now prove Theorem 4.0.1.

4.3.1. Reduction of Theorem 4.0.1 to Cor. 1.2.5. We first reduce Theorem 4.0.1 to Cor. 1.2.5, using⁶ the classical Manin-Mumford theorem (Th. 1.1.1).

Let $(a_n)_{n \geq 0}$ be a sequence in $A(\overline{K})_{tors}$, where each a_n is of order coprime to p .

Let K'/K be a finite extension and let us write $\text{Gal}(\overline{K}/K) = \text{Gal}(\overline{K}/K') \sigma_1 \cup \dots \cup \text{Gal}(\overline{K}/K') \sigma_{[K:K']}$. We observe that Theorem 4.0.1 for the sequence $(a_n)_{n \in \mathbb{Z}_{\geq 0}}$ over the field K is equivalent to Theorem 4.0.1 for the sequence $(\sigma_i(a_n))_{n \in \mathbb{Z}_{\geq 0}, 1 \leq i \leq [K':K]}$ over the field K' .

According to the classical Manin-Mumford theorem (Th. 1.1.1) we may write, in the abelian $\overline{K}$ -variety A ,

$$(4.19) \quad \overline{\bigcup_{n \in \mathbb{Z}_{\geq 0}} \text{Gal}(\overline{K}/K) \cdot a_n}^{Zar} = \bigcup_{i=1}^r b_i + A_i$$

for some $b_1, \dots, b_r \in A(\overline{K})_{tors}$ and abelian subvarieties $A_1, \dots, A_r \leq A$.

There is a finite extension K'/K such that the b_i are in $A(K')$ and the A_i are defined over K' . By the observation above we may assume $K' = K$. In particular, for $a \in b_i + A_i(\overline{K})$ we have $\text{Gal}(\overline{K}/K) \cdot a \subseteq b_i + A_i(\overline{K})$. Thus, for $1 \leq i \leq r$,

$$(4.20) \quad \left(\bigcup_{n \in \mathbb{Z}_{\geq 0}} \text{Gal}(\overline{K}/K) \cdot a_n \right) \cap (b_i + A_i) = \bigcup_{a_n \in b_i + A_i} \text{Gal}(\overline{K}/K) \cdot a_n.$$

We also assume that, in (4.19), each $b_i + A_i$ is an irreducible component. It follows that, for $1 \leq i \leq r$,

$$b_i + A_i = \overline{\bigcup_{a_n \in b_i + A_i} \text{Gal}(\overline{K}/K) \cdot a_n}^{Zar}.$$

It is enough to prove Theorem 4.0.1 for each of the subsequences $(a_m)_{m \in \{n \in \mathbb{Z}_{\geq 0} \mid a_n \in b_i + A_i\}}$. We may thus assume $r = 1$. Substituting a_n with $a_n - b_1$, we may also assume $b_1 = 0$.

Replacing A by A_1 , it is enough to prove Cor. 1.2.5.

⁶Note that Th. 1.1.1 is a consequence of Th. 1.2.1.

4.3.2. *Proof of Cor. 1.2.5.* In proving Cor. 1.2.5, we may replace $(a_n)_{n \geq 0}$ be a subsequence that is generic in A . It is in particular a strict subsequence. Namely, for every proper abelian subvariety $D \subsetneq A$, the sequence $(a_n + D)_{n \in \mathbb{Z}_{\geq 0}}$ of A/D satisfies

$$(4.21) \quad \text{ord}(a_n + D) \rightarrow +\infty.$$

We apply Theorem 1.2.1 and deduce that we may write, in $\mathcal{A}_p$,

$$\overline{\bigcup_{n \in \mathbb{Z}_{\geq 0}} E_n}^{\text{Zar}} = \bigcup_{i=1}^C \beta_i + \mathfrak{B}_i.$$

We apply Prop. 4.3.1 and deduce that, with the notations of Prop. 4.3.1,

$$(4.22) \quad a_n \in F + \bigcup_{i=1}^C D_i.$$

Assume by contradiction that every $D_i \subseteq A$ is a proper subvariety. Then (4.21) implies

$$\forall 1 \leq i \leq C, \text{ord}(a_n + D_i) \rightarrow +\infty.$$

This contradicts (4.22).

We have proved Cor. 1.2.5. This finishes the proof of Theorem 4.0.1.

5. PURELY p -ADIC PHENOMENA, THEOREM 1.2.6

In this final section we prove Theorem 1.2.6, which, for the convenience of the reader, is recalled below.

Theorem 5.0.1. *Fix a prime $p \in \mathcal{O}_{K,S}$ of residue characteristic p . Let A be an abelian scheme over $\mathcal{O}_{K,S}$, $(a_n)_n \subset A_{\text{tors}}(\overline{K})$ (possibly of order divisible by p), and write $E_n = \pi_p(\text{Gal}(\overline{K}/K) \cdot a_n)$, for a map $\pi_p : A(\overline{K}) \rightarrow \mathcal{A}_p(\overline{\kappa(p)})$. Then for every component $\alpha + \mathfrak{B}$ of the Zariski closure $\mathcal{V}$ of*

$$\bigcup_{n \geq 0} E_n \subset \mathcal{A}_p \subset A$$

there exists $B \subseteq A$ an abelian subvariety such that $\mathfrak{B} \subset B_p$ and the quotient $B_p/\mathfrak{B}$ is of p -rank zero.

The key input needed to adapt the strategy of the proof of Theorem 4.0.1 to the above, is the following p -adic version of the arguments of Section 4.2. Compared to the ℓ -adic argument, the crux is to have some control on the reduction map from $T_p(A)$ to $T_p(\mathcal{A}_p)$ and to find a faithful representation of the endomorphism algebra of A and $\mathcal{A}_p$. All this is summarised in the statement of Proposition 5.1.1, which we first use as a black box, and then explain its proof (in the appendix).

Theorem 5.0.2. *Let W be a $\text{Gal}(\overline{K}/K)$ -invariant subspace of $V_p(A)$ and denote by W_p its image in $V_p(\mathcal{A}_p)$. If there exists $u \in \text{End}(A) \otimes \mathbb{Q}$ such that*

$$W_p \subseteq u \cdot V_p(\mathcal{A}_p),$$

then there is an idempotent $v \in \text{End}(A) \otimes \mathbb{Q}$ such that

$$W_p \subseteq v \cdot V_p(\mathcal{A}_p) \subseteq u \cdot V_p(\mathcal{A}_p).$$

Assume moreover that $u \cdot V_p(\mathcal{A}_p) = V_p(\mathfrak{B})$ where $\mathfrak{B} \subset \mathcal{A}_p$ is the smallest abelian subvariety such that $W_p \subset V_p(\mathfrak{B})$. Then $v \cdot V_p(A) = V_p(B)$ and $v \cdot V_p(\mathcal{A}_p) = V_p(B_p)$ with $B = vA$, as an abelian subvariety. Furthermore $\mathfrak{B} \subset B_p$, and the quotient $B_p/\mathfrak{B}$ is of p -rank zero (i.e. $B_p[p^\infty] = \mathfrak{B}[p^\infty]$).

5.1. Preliminaries.

5.1.1. *Statement of a key proposition.* To prove Theorem 5.0.2 we need the following result about abelian varieties A over local fields $L := K_{\mathfrak{p}}$ with good reduction over the residue field $k := \kappa(\mathfrak{p})$. Set $V := V_p(A_L)$.

Proposition 5.1.1. *There exist a field extension E of L , and a polynomial $Q(X)$ with coefficients in $\overline{\mathbb{Q}} \cap \mathbb{Q}_p$ such that:*

(1) *The left action $\text{End}(A_L)$ on $V \otimes_{\mathbb{Q}_p} E$ extends to an E -linear left action*

$$\rho : \text{End}(A_k) \rightarrow \text{End}_E(V \otimes_{\mathbb{Q}_p} E);$$

(2) *The kernel of the reduction map, which we call the ramified part of V and denote by*

$$V^r := \ker(V_p(A_L) \rightarrow V_p(A_k)),$$

and the Frobenius endomorphism $\text{Frob}_{A_k} \in \text{End}(A_k)$ satisfy the identity of E -linear subspaces

$$\pi(V \otimes E) = V^r \otimes E,$$

where $\pi = Q(\rho(\text{Frob}_{A_k}))$ is seen as an element of $\text{End}_E(V \otimes_{\mathbb{Q}_p} E)$. Moreover π is a central idempotent;

(3) *Consider $V \otimes E$ modulo $V^r \otimes E$. Via ρ , it is an $\text{End}(A_k) \otimes E$ -module, and it can naturally be identified with the $\text{End}(A_k) \otimes E$ -module $V_p(A_k) \otimes E$ (where the action on the latter is the natural one coming from the naïve p -adic Tate module of A_k , as an $\text{End}(A_k)$ -module).*

The proof appears in Section A.5, after all required objects are introduced and described (for example E is one of Fontaine's famous period rings).

5.1.2. *Variant of Lemma 4.2.1 (with an extra central idempotent).*

Proposition 5.1.2. *Let M, N be semisimple finite dimensional $\mathbb{Q}$ -algebras, with M a subalgebra of N . Let $E/\mathbb{Q}$ be a field extension, $\pi \in N \otimes E$ a central idempotent, and*

$$(N \otimes_{\mathbb{Q}} E) \hookrightarrow \text{End}_E(V)$$

be a faithful representation in V a finite dimensional E linear vector space. Let u be an idempotent of N , and w be an idempotent of $M \otimes_{\mathbb{Q}} E$ such that

$$w \cdot V + \pi \cdot V \subseteq u \cdot V + \pi \cdot V.$$

Then there exists an idempotent $v \in M$, such that

$$w \cdot V + \pi \cdot V \subseteq v \cdot V + \pi \cdot V \subseteq u \cdot V + \pi \cdot V.$$

Remark 5.1.3. Let B be a semisimple algebra, and π be a *central* idempotent. Then we can write, as $\mathbb{Q}$ -algebras

$$B = \pi B \oplus (1_B - \pi)B.$$

Let I be a left (resp. right) ideal of B containing π , we may write

$$I = \pi B \oplus I',$$

for $I' := (1_B - \pi)I$. So we have a correspondence between left (resp. right) ideals of B containing π , and left (resp. right) ideals of $(1_B - \pi)B$.

For the proof of Proposition 5.1.2, we need two lemmas (the first is a simple fact).

Lemma 5.1.4. *Let $M \subset B$ be a semisimple algebras, π a central idempotent such that $B = M[\pi]$. Then M surjects onto $B/(\pi)$, and every idempotent of $B/(\pi)$, comes from an idempotent of M .*

Lemma 5.1.5. *Let M, B, π be as in Lemma 5.1.4, and V be a $\mathbb{Q}$ -vector space with a faithful action of B . Let u be an idempotent of B , and consider the ideal of B*

$$I := uB + \pi B \subset B.$$

An element $b \in B$ belongs to I if and only if

$$b \cdot V + \pi \cdot V \subseteq u \cdot V + \pi \cdot V.$$

Proof. We need only to prove $\Leftarrow$, the other implication is evident. Let $b \in B$ be such that $b \cdot V + \pi \cdot V \subseteq u \cdot V + \pi \cdot V$. We write

$$b = \pi b + (1 - \pi)b.$$

We also have an induced decomposition on V :

$$V = \ker(\pi \cdot) \oplus \text{Im}(\pi \cdot).$$

As u and b commute with π , they are compatible with the above direct sum decomposition, that is u acts on $\ker(\pi \cdot)$ as $(1 - \pi)u$ and on $\text{Im}(\pi \cdot)$ as πu , and similarly for b . We have

$$\text{Im}((1 - \pi)b) \oplus \text{Im}(\pi) = \text{Im}(b) + \text{Im}(\pi) \subseteq \text{Im}(u) + \text{Im}(\pi) = \text{Im}((1 - \pi)u) \oplus \text{Im}(\pi).$$

Hence $\text{Im}((1 - \pi)b) \subseteq \text{Im}((1 - \pi)u)$. But $(1 - \pi)u$ is unipotent, by Lemma 4.2.1, $(1 - \pi)b$ belongs to $(1 - \pi)uB$, say

$$(1 - \pi)b = (1 - \pi)ux,$$

for some $x \in B$. Finally $b = \pi b + (1 - \pi)b = \pi b + (1 - \pi)ux = \pi b + u(1 - \pi)x \in I$. $\square$

Proof of Proposition 5.1.2. We first consider

$$X_\pi := (uN[\pi] + \pi N[\pi]) \cap (M[\pi]),$$

where $u \in N$ acts diagonally on $N[\pi]$. It is a right ideal of $M[\pi]$, and as such it is generated by an idempotent $m = m^2$ of $M[\pi]$ (as recalled before the proof of Lemma 4.2.1):

$$X_\pi = mM[\pi].$$

Notice that X_π contains (π) , and so, by Lemma 5.1.4 (applied to $B = M[\pi]$), we can write $X_\pi = vM[\pi] + \pi M[\pi]$, where v is an idempotent of M such that

$$v \mod (\pi) = m \mod (\pi),$$

that is $v + (\pi) = m + (\pi)$. Hence $mM[\pi] = mM[\pi] + \pi mM[\pi] = vM[\pi] + \pi M[\pi]$.

Notice that

$$X_\pi \otimes E = ((uN[\pi] + \pi N[\pi]) \otimes E) \cap (M[\pi] \otimes E).$$

We may apply Lemma 5.1.5 to $b = v \in I = uN[\pi] \otimes E + \pi N[\pi] \otimes E$, to get

$$v \cdot V + \pi \cdot V \subseteq u \cdot V + \pi \cdot V.$$

Again applying Lemma 5.1.5 $w \in uN[\pi] \otimes E + \pi N[\pi] \otimes E$, since we know that

$$w \cdot V + \pi \cdot V \subseteq u \cdot V + \pi \cdot V.$$

By construction $w \in M[\pi] \otimes E$, so $w \in X_\pi \otimes E$, and we can write

$$w \cdot V + \pi \cdot V \subseteq v \cdot V + \pi \cdot V.$$

$\square$

5.2. Proof of Theorem 5.0.2. The place $\mathfrak{p}$ is a place of good reduction for A and have

$$\mathrm{End}_K(A_K) = \mathrm{End}_{K_{\mathfrak{p}}}(A_{K_{\mathfrak{p}}}),$$

since the endomorphism ring of an abelian variety does not change under extensions of algebraically closed field of characteristic zero⁷ (recall also the reductions from Section 2.1 that guarantee that $\mathrm{End}_K(A_K) = \mathrm{End}_{\overline{K}}(A_{\overline{K}})$). As a $\mathbb{Q}_p$ -vector spaces of dimension $2g$, we may also naturally identify $V_p(A_K)$ with $V_p(A_{K_{\mathfrak{p}}})$, via the map induced by $\overline{K} \rightarrow \overline{K}_{\mathfrak{p}}$. We now use some facts that will be explained in details in Appendix A (where we let L to be $K_{\mathfrak{p}}$). Set $V := V_p(A_K)$. Let $E/\mathbb{Q}$ be the field extension of Proposition 5.1.1, and consider $V \otimes E$ with its natural action of $\mathrm{End}(A_K) \otimes \mathbb{Q}_p$ and the ρ -action of $\mathrm{End}(\mathcal{A}_{\mathfrak{p}}) \otimes \mathbb{Q}_p$ coming from (1) of Proposition 5.1.1.

We can consider the element

$$(5.1) \quad \pi \in (\mathrm{End}(\mathcal{A}_{\mathfrak{p}}) \otimes \overline{\mathbb{Q}}) \cap (\mathrm{End}(\mathcal{A}_{\mathfrak{p}}) \otimes \mathbb{Q}_p),$$

defined in (2) of Proposition 5.1.1. By construction, π is a central element (it is a $(\mathbb{Q}_p \cap \overline{\mathbb{Q}})$ -combination of powers of the Frobenius endomorphism $F_{A, \mathfrak{p}} \in \mathrm{End}(\mathcal{A}_{\mathfrak{p}})$). Thanks to (4.1) (the Tate conjecture with $\mathbb{Q}_p$ -coefficients), there is some idempotent $w \in \mathrm{End}(A_K) \otimes \mathbb{Q}_p$ such that $W \otimes E = w \cdot V \otimes E$. The key point of Proposition 5.1.1 is that

$$(5.2) \quad \rho(\pi)(V \otimes E) = V^r \otimes E$$

where V^r denotes the kernel of the reduction map $V \rightarrow V_p(A_{K(\mathfrak{p})})$. By assumption, W modulo V^r is in the naïve Tate module of $\mathfrak{B}$, which is $u \cdot V_p(A_{K(\mathfrak{p})})$. Thanks to (3) of Proposition 5.1.1, we may identify the $W \otimes E$, modulo $V^r \otimes E$, with $\rho(u) \cdot V \otimes E$.

Thanks to the definition of π from (5.1), and (5.2), we have an inclusion, modulo V^r :

$$(5.3) \quad \mathrm{Im}(w) \otimes E \subseteq \mathrm{Im}(\rho(u)).$$

We can now apply Proposition 5.1.2: there exists an idempotent $v \in \mathrm{End}(A_K) \otimes \mathbb{Q}$ such that

$$w \cdot V \otimes E + V^r \otimes E \subseteq v \cdot V \otimes E + V^r \otimes E \subseteq \rho(u) \cdot V \otimes E + V^r \otimes E.$$

The image of v gives, up to a quasi-isogeny, the desired abelian subvariety $B \subset A$, satisfying

$$(5.4) \quad W_{\mathfrak{p}} \subset T_p(B_{\mathfrak{p}}) \subset T_p(\mathfrak{B}).$$

For the final part of the statement, assume that $u \cdot V_p(\mathcal{A}_{\mathfrak{p}}) = V_p(\mathfrak{B})$ where $\mathfrak{B} \subset \mathcal{A}_{\mathfrak{p}}$ is the smallest abelian subvariety such that $W_{\mathfrak{p}} \subset V_p(\mathfrak{B})$. By the above construction of B (and $B_{\mathfrak{p}}$) we must have $T_p(B_{\mathfrak{p}}) = T_p(\mathfrak{B})$ and $\mathfrak{B} \subset B_{\mathfrak{p}}$. Therefore $B_{\mathfrak{p}}[p^{\infty}] = \mathfrak{B}[p^{\infty}]$, and so the quotient abelian variety $B_{\mathfrak{p}}/\mathfrak{B}$ is of p -rank zero.

5.3. Let us recall that A is an abelian variety over a number field K such that $\mathrm{End}_K(A) = \mathrm{End}_{\overline{K}}(A)$, and that $\mathcal{A}_{\mathfrak{p}}$ denotes its reduction at a prime $\mathfrak{p}$ of good reduction.

We recall that the action of $\mathrm{Gal}(\overline{K}/K)$ on $V_p(A)$ is semisimple.

We denote by red the map of $\mathbb{Q}_p$ -Tate modules

$$\mathrm{red} : V_p(A) \rightarrow V_p(\mathcal{A}_{\mathfrak{p}}).$$

Let us introduce the $\mathrm{Gal}(\overline{K}/K)$ -invariant $\mathbb{Q}_p$ -linear subspace

$$L := \bigcap_{\sigma \in \mathrm{Gal}(\overline{K}/K)} \sigma(\ker(\mathrm{red})) \leq V_p(A).$$

⁷This follows from the fact that the functor $\mathrm{End}_K(A)$ is representable by an étale commutative K -group scheme.

In other words, L is the biggest $\text{Gal}(\overline{K}/K)$ -invariant subspace contained in $\ker(\text{red})$. Observe that the $\text{Gal}(\overline{K}/K)$ -invariant subspaces of $V_p(A)$ are also the images of the endomorphisms $u \in \text{End}_K(A) \otimes \mathbb{Q}_p$ acting on $V_p(A)$. Since $\text{End}_K(A) = \text{End}_{\overline{K}}(A)$, we have, for any finite extension E/K ,

$$(5.5) \quad L = \bigcap_{\sigma \in \text{Gal}(\overline{K}/E)} \sigma(\ker(\text{red})) \leq V_p(A).$$

By semisimplicity, there exists a $\text{Gal}(\overline{K}/K)$ -invariant $\mathbb{Q}_p$ -linear subspace $L' \leq V_p(A)$ such that $V_p(A) = L \oplus L'$.

Using the identification

$$A[p^\infty] = V_p(A)/T_p(A)$$

we define the subgroups

$$(5.6) \quad \Lambda = L/T_p(A) \text{ and } \Lambda' = L'/T_p(A).$$

We have $\Lambda \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^{\dim(L)}$ and $\Lambda' \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^{\dim(L')}$.

Since $V_p(A) = L + L'$ we have $\#\Lambda \cap \Lambda' < +\infty$ and

$$A[p^\infty] = \Lambda + \Lambda'.$$

For $a \in A[p^\infty]$ decomposed as $a = a' + l$ with $a' \in \Lambda'$ and $l \in \Lambda$, we have

$$\pi_p(\text{Gal}(\overline{K}/K) \cdot a) = \pi_p(\text{Gal}(\overline{K}/K) \cdot a').$$

5.4. Proof of Theorem 1.2.6. The following is a version of Proposition 4.3.1 that works also for points of order divisible by p , the main difference is in the definition of the D_i . Here we denote by red the map

$$\text{red} : T_p(A) \rightarrow T_p(\mathcal{A}_p).$$

Proposition 5.4.1. *We consider Λ' as in (5.6). Let $(a_n)_n \subset \Lambda'$ and $(E_n)_n = \pi_p(\text{Gal}(\overline{K}/K) \cdot a_n)$. Let $\mathfrak{B}_1, \dots, \mathfrak{B}_C$ be abelian subvarieties of $\mathcal{A}_p$. For $i = 1, \dots, C$, let $D_i \leq A$ be the biggest abelian subvariety such that $T_p(D_{i,p}) \subseteq T_p(\mathfrak{B}_i)$.*

Assume that, for some $\beta_1, \dots, \beta_C$ in $\mathcal{A}_p$,

$$\bigcup_n E_n \subseteq \bigcup_{i=1}^C \beta_i + \mathfrak{B}_i.$$

Then there exists a finite set $F \subset A$ such that for all n

$$a_n \in F + \bigcup_{i=1}^C D_i.$$

Proof. We follow the strategy of the proof of Prop. 4.3.1.

By multiplying by the product of the orders of the β_i , we may assume that every $\beta_i = 0$.

For every n there exists an $1 \leq i \leq C$ such that

$$\#\{(\text{Gal}(\overline{K}/K) \cdot a_n) \cap \pi_p^{-1}(\mathfrak{B}_i)\} \geq \frac{1}{C} \#\{\text{Gal}(\overline{K}/K) \cdot a_n\}.$$

For every n we choose such an i . We decompose the sequence a_n into finitely many subsequences according to the corresponding i . We may argue with each subsequence independently. Without loss of generality we may assume that i does not depend on n . We write $\mathfrak{B} = \mathfrak{B}_i$ and $D = D_i$, and we have $\pi_p(a_n) \in \mathfrak{B}$, for every n .

We will prove that there exists a finite set $F \subseteq A$ such that $a_n \in F + D$ for all n . The Proposition 5.4.1 will follow.

Assume by contradiction that $\text{ord}(a_n + D) \rightarrow +\infty$, as $n \rightarrow +\infty$.

As in (1) Proposition 4.3.1, we can construct a non-zero $a_\infty \in V_p(A/D)$, and a finite extension E/K such that

$$\text{Gal}(\overline{K}/E) \cdot a_\infty \subset \text{red}^{-1} V_p(\mathfrak{B} + D/D).$$

Since $a_n \in \Lambda'$ for every n , we have $a_\infty \in L'$. Let $W \leq V_p(A)$ be the $\mathbb{Q}_p$ -linear subspace generated by $\text{Gal}(\overline{K}/E) \cdot a_\infty$.

Since L' is $\text{Gal}(\overline{K}/E)$ -invariant, we have $W \leq L'$. It implies $W \cap L = \{0\}$. By (5.5) we have,

$$\forall w \in W \setminus \{0\}, \pi_p(\text{Gal}(\overline{K}/E) \cdot w) \neq \{0\}.$$

For $w = a_\infty$, we get

$$W_p := \text{red}(W) \neq \{0\}.$$

Thanks to Theorem 5.0.2, there exists $A'' \subset A/D$ such that

$$W_p \subset \text{red} V_p(A''_p) \subset V_p(\mathfrak{B} + D_p/D_p).$$

As $W_p \neq \{0\}$, we have $A'' \neq 0$.

Let $D \leq D' \leq A$ be the abelian subvariety such that $D'/D = A''$. Then $V_p(D'_p) \leq V_p(\mathfrak{B})$ and $D < D'$. This contradicts the maximality property in the definition of D . $\square$

5.4.1. The p -power order case of Theorem 1.2.6.

Proposition 5.4.2. *Let a_n be a generic sequence in A such that $a_n \in \Lambda'$ for every n , and let $E_n = \pi_p(\text{Gal}(\overline{\mathbb{Q}}/K) \cdot a_n)$. Then*

$$\overline{\bigcup_{n \in \mathbb{Z}_{\geq 0}} E_n}^{\text{Zar}} = \overline{\mathcal{A}_p[p^\infty]}^{\text{Zar}}.$$

Proof. We have $\overline{\bigcup_{n \in \mathbb{Z}_{\geq 0}} E_n}^{\text{Zar}} \subseteq \overline{\mathcal{A}_p[p^\infty]}^{\text{Zar}}$ because that $E_n \subseteq \mathcal{A}_p[p^\infty]$ for every n .

We apply Theorem 1.2.1 and deduce that we may write, in $\mathcal{A}_p$,

$$\overline{\bigcup_{n \in \mathbb{Z}_{\geq 0}} E_n}^{\text{Zar}} = \bigcup_{i=1}^C \beta_i + \mathfrak{B}_i.$$

For each i , there exists n and $\alpha \in E_n$ such that $\alpha + \mathfrak{B}_i = \beta_i + \mathfrak{B}_i$. Therefore, we may assume that $\beta_i \in \mathcal{A}_p[p^\infty]$.

We apply Prop. 5.4.1 and deduce that, with the notations of Prop. 5.4.1,

$$(5.7) \quad a_n \in F + \bigcup_{i=1}^C D_i.$$

As a_n is generic in A , we have $D_i = A$ for some i . By definition of D_i , we have

$$\mathcal{A}_p[p^\infty] = \mathcal{D}_{i_p}[p^\infty] \subseteq \mathfrak{B}_i.$$

As $\beta_i \in \mathcal{A}_p[p^\infty]$, we have $\mathcal{A}_p[p^\infty] \subseteq \beta_i + \mathfrak{B}_i$. Thus

$$\overline{\mathcal{A}_p[p^\infty]}^{\text{Zar}} \subseteq \beta_i + \mathfrak{B}_i \subseteq \overline{\bigcup_{n \in \mathbb{Z}_{\geq 0}} E_n}^{\text{Zar}}.$$

We proved the conclusion of Proposition 5.4.2 by double inclusion. $\square$

5.4.2. Factoring the prime-to- p order part and the power-of- p order part.

Lemma 5.4.3. *Let A be an abelian variety over an algebraically closed field (in any characteristic). Let p be a prime and let $\Sigma \subseteq A \times A$ be a subset such that*

$$\Sigma \subseteq \left(\sum_{\ell \neq p} A[\ell^\infty] \right) \times A[p^\infty].$$

We denote by $\pi_1, \pi_2 : A \times A \rightarrow A$ the first and second projection maps.

We assume that there exist torsion points $b_1, \dots, b_k \in A_{tors} \times A_{tors}$ and abelian subvarieties $B_1, \dots, B_k \leq A \times A$ such that

$$(5.8) \quad \overline{\Sigma}^{Zar} = \bigcup_{i=1}^k b_i + B_i,$$

and such that

$$(5.9) \quad \text{each } b_i + B_i \text{ is an irreducible component of } \overline{\Sigma}^{Zar}.$$

Then

$$\forall i \in \{1; \dots; k\}, B_i = \pi_1(B_i) \times \pi_2(B_i).$$

Proof. We reduce the proof to the case $k = 1$ and $b_i = 0$.

For each $i \in \{1; \dots; k\}$, let us define $\Sigma_i := \Sigma \cap (b_i + B_i)$. Then (5.9) implies that $\overline{\Sigma}_i^{Zar} = b_i + B_i$. In particular there exists an element $\sigma_i \in \Sigma_i$. We then have $\sigma_i + B_i = b_i + B_i$. Then the set $\Sigma'_i = \{\sigma - \sigma'_i \mid \sigma \in \Sigma_i\}$ satisfies (5.8) and $\overline{\Sigma}'_i = B_i$.

It is enough to prove, for each $i = 1, \dots, k$, the Lemma 5.4.3 for $\Sigma = \Sigma'_i$.

We now assume $k = 1$ and $b_i = 0$ and write $B := B_1$.

For every $(b_1, b_2) \in \Sigma$, we have $\gcd\{\text{ord}(b_1); \text{ord}(b_2)\} = 1$. There exists thus $m_1, m_2 \in \mathbb{Z}$ such that $m_1 \cdot \text{ord}(b_1) + m_2 \cdot \text{ord}(b_2) = 1$. Let $m := m_2 \cdot \text{ord}(b_2)$. Then $m \equiv 1 \pmod{\text{ord}(b_1)}$ and

$$(\pi_1(b_1, b_2), 0) = (b_1, 0) = m \cdot (b_1, b_2) \in m \cdot B = B.$$

We deduce $\pi_1(\Sigma) \times \{0\} \subseteq B$. We have

$$\overline{\pi_1(\Sigma)}^{Zar} = \overline{\pi_1(\overline{\Sigma}^{Zar})}^{Zar} = \overline{\pi_1(B)}^{Zar} = \pi_1(B).$$

Thus $\pi_1(B) \times \{0\} \subseteq B$. Similarly $\{0\} \times \pi_2(B) \subseteq B$. This proves

$$\pi_1(B) \times \pi_2(B) = \pi_1(B) \times \{0\} + \{0\} \times \pi_2(B) \subseteq B + B = B.$$

Obviously $B \subseteq \pi_1(B) \times \pi_2(B)$. We conclude $B = \pi_1(B) \times \pi_2(B)$. $\square$

5.4.3. General case of Theorem 1.2.6. We have

$$(5.10) \quad A_{tors} \simeq \left(\bigoplus_{\ell \neq p} A[\ell^\infty] \right) \oplus A[p^\infty]$$

$$(5.11) \quad \simeq \left(\sum_{\ell \neq p} A[\ell^\infty] \right) \oplus (\Lambda + \Lambda').$$

We can write accordingly $a_n = a'_n + \lambda_n + \lambda'_n$. For every $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/K)$ and every n , we have

$$\pi_p(\sigma(a_n - \lambda_n)) = \pi_p(\sigma(a_n)) - \pi_p(\sigma(\lambda_n)) = \pi_p(\sigma(a_n))$$

and thus $E_n = \pi_p(\text{Gal}(\overline{\mathbb{Q}}/K) \cdot a_n) = \pi_p(\text{Gal}(\overline{\mathbb{Q}}/K) \cdot (a_n - \lambda_n))$. In proving Theorem 1.2.6, we may thus assume $\lambda_n = 0$ for every n .

We consider $\tilde{a}_n := (a'_n, \lambda'_n) \in A \times A$ and $\tilde{E}_n := \pi_p(\text{Gal}(\overline{\mathbb{Q}}/K) \cdot \tilde{a}_n)$. Let $\alpha : A \times A \rightarrow A$ be the addition map. We have

$$\alpha(\tilde{E}_n) = E_n.$$

Since α is a proper map, we have

$$\alpha \left(\overline{\bigcup_{n \in \mathbb{Z}_{\geq 0}} \tilde{E}_n}^{\text{Zar}} \right) = \overline{\bigcup_{n \in \mathbb{Z}_{\geq 0}} \alpha(\tilde{E}_n)}^{\text{Zar}} = \overline{\bigcup_{n \in \mathbb{Z}_{\geq 0}} E_n}^{\text{Zar}}.$$

Therefore, it is enough to prove Theorem 1.2.6 for the sequence $\tilde{a}_n$ instead of the sequence a_n .

According to Theorem 1.1.1, we may express

$$\overline{\{\tilde{a}_n \mid n \in \mathbb{Z}_{\geq 0}\}}^{\text{Zar}(A_K \times A_K)} = \bigcup_{i=1}^k d_i + D_i$$

for some $d_1, \dots, d_k \in A(\overline{K})_{\text{tors}} \times A(\overline{K})_{\text{tors}}$ and abelian subvarieties $D_1, \dots, D_k \leq (A \times A)_{\overline{K}}$. We assume that each $d_i + D_i$ is actually a component of $\overline{\{\tilde{a}_n \mid n \in \mathbb{Z}_{\geq 0}\}}^{\text{Zar}(A_K \times A_K)}$. For every i , we may assume that $d_i \in \bigcup_{n \in \mathbb{Z}_{\geq 0}} \text{Gal}(\overline{\mathbb{Q}}/K) \cdot \tilde{a}_n \subseteq \left(\bigoplus_{\ell \neq p} A[\ell^\infty] \right) \times \Lambda'$ and

$$(5.12) \quad \forall n \in \mathbb{Z}_{\geq 0}, i \in \{1; \dots; k\}, \tilde{a}_n - d_i \in \left(\bigoplus_{\ell \neq p} A[\ell^\infty] \right) \times \Lambda'.$$

By Lemma 5.4.3, we have

$$\forall i \in \{1; \dots; k\}, D_i = \pi_1(D_i) \times \pi_2(D_i).$$

We define $\Delta_i := \pi_1(D_i)_p$ and $\Delta'_i := \overline{\pi_2(D_i)_p[p^\infty]}^{\text{Zar}}$ and $\delta_i := \pi_p(d_i)$.

Theorem 1.2.6 for the sequence $\tilde{a}_n$ is a direct consequence of the following.

Proposition 5.4.4. *We have*

$$(5.13) \quad \overline{\bigcup_{n \in \mathbb{Z}_{\geq 0}} \tilde{E}_n}^{\text{Zar}} = \bigcup_{i=1}^k \delta_i + \Delta_i \times \Delta'_i.$$

Proof of Proposition 5.4.4. Passing to a finite extension of K , we may assume

$$(5.14) \quad d_1, \dots, d_k \in A(K)$$

and, by [30, N.136, §2, Th. 1 p. 34], that we have the “ ℓ -independence property”

$$(5.15) \quad \forall \sigma', \sigma'' \in \text{Gal}(\overline{\mathbb{Q}}/K), \exists \sigma \in \text{Gal}(\overline{\mathbb{Q}}/K), \forall n \in \mathbb{Z}_{\geq 0}, \sigma(a'_n, \lambda'_n) = (\sigma'(a'_n), \sigma''(\lambda'_n)).$$

The inclusion $\overline{\bigcup_{n \in \mathbb{Z}_{\geq 0}} \tilde{E}_n}^{\text{Zar}} \subseteq \bigcup_{i=1}^k \delta_i + \Delta_i \times \Delta'_i$ is immediate. We need to prove that, for every $i \in \{1; \dots; k\}$, we have

$$(5.16) \quad \delta_i + \Delta_i \times \Delta'_i \subseteq \overline{\bigcup_{n \in \mathbb{Z}_{\geq 0}} \tilde{E}_n}^{\text{Zar}}.$$

We fix i in $\{1; \dots; k\}$. In proving (5.16), we can always pass to a subsequence of $\tilde{a}_n$. Without loss of generality, we may assume that $\dim(D_i) > 0$. Then passing to an infinite subsequence of $\tilde{a}_n$, we may assume that $\tilde{a}_n \in d_i + D_i$ for every n , and that $\tilde{a}_n$ is a generic sequence in $d_i + D_i$. By (5.12), we may translate by $-d_i$ and assume $d_i = 0$. Therefore the sequences $\pi_1(\tilde{a}_n)$ and $\pi_2(\tilde{a}_n)$ are generic in $\pi_1(D_i)$ and $\pi_2(D_i)$ respectively.

By Corollary 1.2.5, the subset

$$\bigcup_{n \in \mathbb{Z}_{\geq 0}} \pi_p(\pi_1(\text{Gal}(\overline{\mathbb{Q}}/K) \cdot \tilde{a}_n)) \subseteq \Delta_i$$

is Zariski dense. Passing to a subsequence, there exists a sequence σ'_n in $\text{Gal}(\overline{\mathbb{Q}}/K)$ such that $\pi_p(\pi_1(\sigma'_n(\tilde{a}_n)))$ is generic in Δ_i .

By Proposition 5.4.2, we have

$$\bigcup_{n \in \mathbb{Z}_{\geq 0}} \pi_p(\pi_2(\text{Gal}(\overline{\mathbb{Q}}/K) \cdot \tilde{a}_n)) \subseteq \Delta'_i$$

is Zariski dense. Passing to a subsequence, there exists a sequence σ''_n in $\text{Gal}(\overline{\mathbb{Q}}/K)$ such that $\pi_p(\pi_2(\sigma''_n(\tilde{a}_n)))$ is generic in Δ'_i .

By (5.15), there exist $\sigma_n \in \text{Gal}(\overline{\mathbb{Q}}/K)$ be such that

$$\forall n, \sigma_n(a'_n, \lambda'_n) = (\sigma'_n(a'_n), \sigma''_n(\lambda'_n)).$$

By Theorem 1.2.1, we can write

$$\overline{\bigcup_{n \in \mathbb{Z}_{\geq 0}} \tilde{E}_n}^{\text{Zar}} = \bigcup_{j=1}^m \beta_j + \mathfrak{B}_j.$$

By Lemma 5.4.3, we have

$$\forall j \in \{1; \dots; m\}, \mathfrak{B}_j = \pi_1(\mathfrak{B}_j) \times \pi_2(\mathfrak{B}_j).$$

Passing to an infinite subsequence, there exists j such that

$$\forall n, \pi_p(\sigma_n(\tilde{a}_n)) \in \beta_j + \mathfrak{B}_j.$$

Thus, the sequence $\pi_p(\pi_1(\sigma_n(\tilde{a}_n))) = \pi_p(\sigma'_n(a'_n))$ in $\pi_1(\beta_j + \mathfrak{B}_j)$ is dense in Δ_i . Thus

$$\Delta_i \subseteq \beta_j + \mathfrak{B}_j.$$

On the other hand, we have

$$\beta_j + \mathfrak{B}_j \subseteq \bigcup_{j=1}^m \beta_j + \mathfrak{B}_j = \overline{\bigcup_{n \in \mathbb{Z}_{\geq 0}} \tilde{E}_n}^{\text{Zar}} \subseteq \Delta_i \times \Delta'_i.$$

Thus $\pi_1(\mathfrak{B}_j) = \Delta_i = \pi_1(\beta_j + \mathfrak{B}_j)$. Similarly, $\pi_2(\mathfrak{B}_j) = \Delta'_i = \pi_2(\beta_j + \mathfrak{B}_j)$. Thus

$$\Delta_i \times \Delta'_i = \pi_1(\mathfrak{B}_j) \times \pi_2(\mathfrak{B}_j) = \mathfrak{B}_j \subseteq \overline{\bigcup_{n \in \mathbb{Z}_{\geq 0}} \tilde{E}_n}^{\text{Zar}}.$$

This proves (5.16). This concludes the proof of the Proposition 5.4.4 □

This implies Theorem 1.2.6 for the sequence $\tilde{a}_n$, and therefore Theorem 1.2.6 for the sequence a_n .

APPENDIX A. PROOF OF PROPOSITION 5.1.1

A.1. Some p -adic Hodge theory (for abelian varieties with good reduction). To conclude the paper we have to prove Proposition 5.1.1, which was used in Theorem 5.0.2. Here we try to make our argument as understandable as possible, by recalling some standard facts, but the reader fluent in p -adic Hodge theory may simply skip to the proof given in Section A.5.

A.1.1. Notation. Let p be a rational prime number, L be a finite extension of $\mathbb{Q}_p$, $\mathcal{O}_L$ its ring of integers and k its residue field. Let A be an abelian scheme over $\mathcal{O}_L$, of relative dimension $g > 0$, and denote its special and generic fibres respectively by A_k and A_L . We choose $\bar{L}$ an algebraically closed extension of L and denote $\bar{k}$ the corresponding residue field extension of k , so that we can define the $\mathbb{Z}_p$ -linear Tate modules:

$$(A.1) \quad T_p(A_k) := \text{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, A_k[p^\infty](\bar{k})) \text{ and } T_p(A_L) := \text{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, A_L[p^\infty](\bar{L}))$$

The former is the *naïve* Tate module (accounting for the p -rank of A), whereas $T_p(A_L)$ has rank $2g$.

We denote by $\bar{\mathbb{Q}}$ the algebraic closure of $\mathbb{Q}$ inside of $\bar{L}$, so that the field $\bar{\mathbb{Q}} \cap \mathbb{Q}_p$ is properly defined.

We write the corresponding $\mathbb{Q}_p$ -linear Tate modules as follows

$$V_p(A_k) = T_p(A_k) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq \text{Hom}(\mathbb{Q}_p, A_k[p^\infty](\bar{k})),$$

and

$$V_p(A_L) = T_p(A_L) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq \text{Hom}(\mathbb{Q}_p, A_L[p^\infty](\bar{L})).$$

We are interested in the reduction map $A_L(\bar{L}) \rightarrow A_k(\bar{k})$ induced by

$$A_L(\bar{L}) \xleftarrow{\sim} \mathcal{A}(\mathcal{O}_{\bar{L}}) \rightarrow A_k(\bar{k}).$$

Passing to the Tate modules there is a reduction map $T_p(A_L) \rightarrow T_p(A_k)$, which is equivariant with respect to the covariant action of $\text{End}(A_L) \subseteq \text{End}(A_{\bar{L}})$ whereas

$$\text{End}(A_k) \subseteq \text{End}(A_{\bar{k}})$$

acts a priori only on $T_p(A_k)$.

In $\text{End}(A_k)$ there is a specific element, the Frobenius of A_k relative to k ,

$$(A.2) \quad \text{Frob}_{A_k} : A_k \rightarrow A_k$$

associated to the q -power map, where $q = |k|$. On coordinates $A(\bar{k}) \rightarrow A(\bar{k})$ it acts with the Frobenius map

$$\text{Frob}_{\bar{k}/k} : \bar{k} \xrightarrow{x \mapsto x^q} \bar{k}.$$

(This is just the morphism of local ringed spaces given by the identity at the topological level and the $|k|$ -power at the level of structural sheaves.)

A.1.2. Witt vectors notations. Two standard references for crystalline cohomology are [1, 2]. Let $W(k)$ be the ring of Witt vectors with coefficients in k (and $L_0 = \mathbb{Q}_q$ its fraction field), and $F := F_{W(k)}$, $V := V_{W(k)} \in \text{End}_{W(\mathbb{F}_p)}(W(k))$ the *Frobenius* and *Verschiebung* operators.

In practice: the first acts on the Witt coordinates by applying on each coordinate the p -th power map $\text{Frob}_{k/\mathbb{F}_p}$, the second acts by shifting those coordinates.

Of relevance is the Dieudonné ring $W(k)[F_{W(k)}, V_{W(k)}]$ as the (non commutative) $W(k)$ -algebra of additive endomorphisms of $W(k)$ generated by $W(k)$ acting by ring multiplication, and $F_{W(k)}$ and $V_{W(k)}$ just defined. One usually recovers V from $F \circ V = p = V \circ F$.

A.2. Crystalline-étale comparison theorem. On the category of $\mathcal{O}_L$ -abelian schemes $\mathcal{A}$, we consider the crystalline and p -adic étale cohomologies as contravariant functors

$$(A.3) \quad H_{\text{crys}}^1(A_k) \text{ and } H_{\text{ét}}^1(A_{\bar{L}}, \mathbb{Z}_p).$$

The first is a free $W(k)$ -module of rank $2g$ functorial in the special fibre A_k , and comes equipped with a $W(\mathbb{F}_p)$ -linear endomorphism $\phi \in \text{End}_{W(\mathbb{F}_p)}(H_{\text{crys}}^1(A_k))$ which is semi-linear with respect to $F_{W(k)}$: mapping $F_{W(k)}$ to ϕ makes $H_{\text{crys}}^1(A_k)$ a $W(k)[F_{W(k)}, V_{W(k)}]$ -module which is free as a $W(k)$ -module.

The following comparison theorem holds for whichever of the Fontaine rings $E = B_{\text{dR}}$ (and then generalises to varieties, according to Faltings) or, sufficiently for abelian schemes, $E = B_{\text{crys}}$. Those constructions depend a priori on L and $\bar{L}$, but the resulting rings not, up to the relevant isomorphism. The construction of period rings, with all details, can be found in [15]. We following is a special case of the so called C_{crys} -theorem (for H^1 s and abelian varieties with good reduction). The general case is due to Faltings [10].

Theorem A.2.1. *There is a field extension E of the fraction field L_0 of $W(k)$ and a natural isomorphism*

$$(A.4) \quad \gamma_{\text{crys}}(A) : E \otimes_{W(k)} H_{\text{crys}}^1(\mathcal{X}_k) \xrightarrow{\sim} E \otimes_{\mathbb{Z}_p} H_{\text{ét}}^1(\mathcal{X}_{\bar{L}}, \mathbb{Z}_p).$$

of functors from the category of smooth projective varieties $\mathcal{X}$ over $\mathcal{O}_L$ to that of E -vector spaces.

The next remark explains the reason why we need to consider B_{crys} -coefficients (rather than $\mathbb{C}_p$).

Remark A.2.2. Originally Tate [32] proved the so called Hodge-Tate decomposition for the first étale cohomological group of abelian varieties. That is that the existence of a canonical equivariant isomorphism

$$H_{\text{ét}}^1(A_{\bar{L}}, \mathbb{Q}_p) \otimes \mathbb{C}_p \cong H^1(A, \mathcal{O}_A) \otimes \mathbb{C}_p(-1) \oplus H^0(A, \Omega^1) \otimes \mathbb{C}_p.$$

By the degeneration of the Hodge to de Rham spectral sequence in characteristic zero, the RHS is isomorphic to $H_{\text{dR}}^1(A/\mathbb{C}_p)$. The problem is that an such isomorphism is, in general, not canonical.

On the homology side, we get the covariant $W(k)$ -dual and $\mathbb{Z}_p$ -dual functors

$$H_1^{\text{crys}}(A_k) := \text{Hom}_{W(k)}(H_{\text{crys}}^1(A_k), W(k)) \text{ and } H_1^{\text{ét}}(A_{\bar{L}}) := \text{Hom}_{\mathbb{Z}_p}(H_{\text{ét}}^1(A_{\bar{L}}, \mathbb{Z}_p))$$

and, passing to the E -linear duals, a natural isomorphism

$$(A.5) \quad \gamma_{\text{crys}}^\vee(A) : E \otimes_{W(k)} H_1^{\text{crys}}(A_k) \xleftarrow{\sim} E \otimes_{\mathbb{Z}_p} H_1^{\text{ét}}(A_{\bar{L}}, \mathbb{Z}_p).$$

A.3. The connected-étale exact sequence. We consider the reduction map

$$(A.6) \quad \text{red} : A(\bar{L})[p^\infty] \rightarrow A(\bar{k})[p^\infty],$$

in terms of the connected-étale exact sequence.

We first recall some notions from p -divisible groups and Dieudonné theory, following Demazure's classical reference [6] (both over L and k). To the abelian scheme $\mathcal{A}$, and the abelian varieties A_L and A_k , Tate attached p -divisible groups

$$\mathcal{G}_{\mathcal{A}} = \varinjlim_{n \in \mathbb{Z}_{\geq 0}} \mathcal{A}[p^n] \hookrightarrow \mathcal{A}[p^{n+1}],$$

and its generic and special fibres

$$\mathcal{G}_{A_L} = \varinjlim_{n \in \mathbb{Z}_{\geq 0}} A_L[p^n] \hookrightarrow A_L[p^{n+1}] \text{ and } \mathcal{G}_{A_k} = \varinjlim_{n \in \mathbb{Z}_{\geq 0}} A_k[p^n] \hookrightarrow A_k[p^{n+1}].$$

These are *ind-schemes* of group schemes: its functor of points is tested against $\mathcal{O}_L$ -algebras R and is $\mathcal{G}_{\mathcal{A}}(R) = \mathcal{A}(R)[p^n]$.

We denote the neutral connected components (with respect to the union of Zariski topologies) as $\mathcal{G}_{\mathcal{A}}^0$, $\mathcal{G}_{A_L}^0$, and $\mathcal{G}_{A_k}^0$. The first and third are actually the formal Lie groups attached to $\mathcal{A}$ and A_k .

The corresponding quotients are well defined as p -divisible groups and there are short exact sequences of p -divisible groups:

$$(A.7) \quad 0 \rightarrow \mathcal{G}_{\mathcal{A}}^0 \xrightarrow{\iota} \mathcal{G}_{\mathcal{A}} \xrightarrow{\varpi} \mathcal{G}_{\mathcal{A}}^{\text{ét}} \rightarrow 0 \quad \text{over } \mathcal{O}_L,$$

$$(A.8) \quad \text{and } 0 \rightarrow \mathcal{G}_{A_k}^0 \xrightarrow{\iota_k} \mathcal{G}_{A_k} \xrightarrow{\varpi_k} \mathcal{G}_{A_k}^{\text{ét}} \rightarrow 0 \quad \text{over } k.$$

The (co)homologies we evoked in (A.3) factor as functor through the “passing to the attached p -divisible groups over $\mathcal{O}_L$ ”, and H_{crys}^1 , resp. $H_{\text{ét}}^1$, factors even more through “passing to the special (resp. generic) fibre”. We can moreover identify respectively

$$H_1^{\text{crys}}(A_k) \text{ and } H_1^{\text{ét}}(A_{\bar{L}}; \mathbb{Z}_p)$$

with the *covariant Dieudonné module* $M(\mathcal{G}_{A_k})$ of $\mathcal{G}_{A_k}$, and its *Tate module*

$$T(\mathcal{G}_{A_{\bar{L}}}) = \text{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, \mathcal{G}_{A_{\bar{L}}}(\bar{L})).$$

It is important that the Dieudonné module (resp. Tate module) makes sense for any the p -divisible groups appearing in (A.8) and (A.7) respectively. Even though these are not the full p -divisible group of an abelian variety, or of an abelian scheme resp. We still get covariant functors

$$\mathbf{M}() \text{ and } \mathbf{T}()$$

on the category of p -divisible groups over k and L respectively, to that of free $W(k)$ -modules and $\mathbb{Z}_p$ -modules respectively.

Applying the functors $\mathbf{T}()$ and $\mathbf{M}()$ to (A.7) and (A.8) respectively gives us exact sequences that we relabel

$$(A.9) \quad 0 \rightarrow T^0 \rightarrow T \rightarrow T^{\text{ét}} \rightarrow 0 = 0 \rightarrow \mathbf{T}(\mathcal{G}_{\mathcal{A}}^0) \xrightarrow{\mathbf{T}(\iota)} \mathbf{T}(\mathcal{G}_{\mathcal{A}}) \xrightarrow{\mathbf{T}(\varpi)} \mathbf{T}(\mathcal{G}_{\mathcal{A}}^{\text{ét}}) \rightarrow 0$$

$$(A.10) \quad \text{and } 0 \rightarrow M^0 \rightarrow M \rightarrow M^{\text{ét}} \rightarrow 0 = 0 \rightarrow \mathbf{M}(\mathcal{G}_{A_k}^0) \xrightarrow{\mathbf{M}(\iota_k)} \mathbf{M}(\mathcal{G}_{A_k}) \xrightarrow{\mathbf{M}(\varpi_k)} \mathbf{M}(\mathcal{G}_{A_k}^{\text{ét}}) \rightarrow 0.$$

Fact. We will use the following explicit description of the Dieudonné module of an étale p -divisible group $\mathcal{G}$ over k . We have, as $W(k)$ -modules, a natural identification

$$\mathbf{T}(\mathcal{G}) \otimes_{\mathbb{Z}_p} W(k) \simeq \mathbf{M}(\mathcal{G}).$$

We won't need to explicit semi-linear action making it a *Dieudonné module*, but we stress that the above identification is functorial, and in particular receives a left action of $\text{End}(\mathcal{G})$.

The reduction map red factors through the above exact sequences, by which we mean the commutativity of the square

$$\begin{array}{ccc} \mathcal{G}_{\mathcal{A}}[p^{\infty}](\mathcal{O}_{\bar{L}}) & \xrightarrow{\varpi} & \mathcal{G}_{\mathcal{A}}^{\text{ét}}[p^{\infty}](\mathcal{O}_{\bar{L}}) \\ \downarrow \text{red} & & \downarrow \sim \\ \mathcal{G}_{A_k}[p^{\infty}](\bar{k}) & \xrightarrow{\varpi_k} & \mathcal{G}_{A_k}^{\text{ét}}[p^{\infty}](\bar{k}). \end{array}$$

Applying the dualising $\mathrm{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, -)$ to pass to the Tate modules, we get equivalently

$$\begin{array}{ccc} T & \longrightarrow & T^{\text{ét}} \\ \downarrow & & \downarrow \sim \\ T_p(A_k[p^\infty](\bar{k})) & \xlongequal{\quad} & T_p(A_k[p^\infty](\bar{k})). \end{array}$$

where in the bottom row is the naïve Tate module of A_k : its rank as a free $\mathbb{Z}_p$ module is the p -rank of A_k .

In another formulation, we have the identity

$$(A.11) \quad \ker(\mathbf{T}(\varpi) : T \rightarrow T^{\text{ét}}) = \ker(T(\text{red}) : T \rightarrow T_p(A_k[p^\infty](\bar{k})))$$

A.4. Unit root eigenspaces. We study the connected-étale exact sequence of Dieudonné modules:

$$0 \rightarrow M^0 \rightarrow M \rightarrow M^{\text{ét}} \rightarrow 0.$$

A.4.1. Dieudonné-Manin semilinear eigenspaces. We recall a notion of eigenspaces for semilinear actions. Let M' be any free Dieudonné module over k , namely a finite rank free module over $W(k)$ equipped with a $W(\mathbb{F}_p)$ -linear endomorphism ϕ which is semi-linear with respect to $W(k)$. We have the following notion of eigenspace on the L_0 -linear vector space $D = M' \otimes_{W(k)} L_0$. Pick any $W(k)$ basis of M' over L_0 , the representative matrix Φ of ϕ applied to this basis has associated (generalised) eigenspaces in $D \otimes_{L_0} \bar{L}$, and these are defined over L_0 when the corresponding eigenvalue belongs to L_0 . A change of basis of matrix B will change $\Phi' = \Phi \mapsto F_{W(k)}(B)\Phi B^{-1}$, each eigenvalue obtained from the λ by some operation

$$\lambda \mapsto \lambda' = F_{W(k)}(c_\lambda)/c_\lambda \cdot \lambda$$

for some invertible $c(\lambda)$ in $W(k) \subseteq L_0^{\text{nr}}$. As $F_{W(k)}$ preserves the p -adic absolute values $||_p : L_0 \mapsto \mathbb{R}_{\geq 0}$, we will have the invariance

$$|\lambda|_p = |\lambda'|_p.$$

For every real number μ , we let $\bar{V}_\mu$ be the sum, in $\bar{D} = D \otimes_{L_0} \bar{L}$, of the generalised eigenspaces for eigenvalues λ having valuation $\mu = -\log_p |\lambda|_p$. Then $\bar{D}_\mu$ does not depend on the choice of basis, and is defined over L_0 .

This can be approached another way. Denote $f = [k : \mathbb{F}_p]$, so that $W(k)^f$ will actually be the identity of $W(k)$. But the power ϕ^f , since $W(k)^f$ -semi-linear, will actually be $W(k)$ -linear. We let $P(X)$ be its characteristic polynomial, and $P_\mu(X)$ be, in $\bar{L}[X]$, its maximal unitary factor whose roots with roots λ have valuation $f\mu = -f \cdot \log |\lambda|_p$. Then $P_\mu(X)$ is actually defined over L_0 , and the kernel $D_\mu = \ker P_\mu(\phi)$ will produce $\bar{D}_\mu = D_\mu \otimes_{L_0} \bar{L}$.

These “Dieudonné modules” M' are also known as *crystals*, the corresponding D as *isocrystals*, and the subspace D_0 as a *unit root isocrystal*.

A.4.2. Unit root isosplitting of étale quotient. It happens that the exact sequence

$$0 \longrightarrow M^0 \otimes_{W(k)} L_0 \xrightarrow{t} M \otimes_{W(k)} L_0 \xrightarrow{\pi} M^{\text{ét}} \otimes_{W(k)} L_0 \longrightarrow 0$$

$\swarrow \quad \searrow$
 s

is (uniquely) split as an exact sequence of $(F_{W(k)}$ -semi-linear) modules, and that a (unique semi-linear) splitting is given by the unit root subspace

$$s(D^{\text{ét}}) = D_0 \text{ of } D = M \otimes_{W(k)} L_0, \text{ letting } D^{\text{ét}} := M^{\text{ét}} \otimes_{W(k)} L_0.$$

A.4.3. Spectral projector π and functorial Frobenius. Let π be the corresponding eigenspace projector $D \rightarrow D$ with kernel D_0 . It can be recovered in terms of ϕ^f in the following usual way. Let $K_0 \subseteq L_0$ be any field containing the coefficients of the factor $P_\mu(X)$ of the characteristic polynomial $P(X)$ of ϕ^f . There is a polynomial $Q(X) \in K_0[X]$, uniquely defined up to $P(X)$, such that $Q \equiv 0 \pmod{P_\mu(X)}$ and $Q \equiv 1 \pmod{P_\phi(X)/P(X)}$. For any such polynomial, $\pi = Q(\phi^f)$ is the spectral projector with kernel D_0 .

We now consider the q -th powers Frobenius endomorphism $\text{Frob}_{A_k} \in \text{End}(A_k)$ from (A.2) of the abelian variety A_k with respect to the field k . We let $\text{End}(A_k)$ act on $\mathcal{G}_{A_k}$ as well.

Applying the functor $\mathbf{M}()$ to it turns out to give again

$$(A.12) \quad \mathbf{M}(F_{A_k}) = \phi^f \text{ on } M.$$

We now define $\pi := Q(\text{Frob}_{A_k}) \in \text{End}(A_k) \otimes_{\mathbb{Q}} K$.

We may extend $D : \text{End}(A_k) \rightarrow \text{End}_{L_0}(D(\mathcal{G}_{A_k}))$ by L_0 -linearity, and now define

$$\mathbf{D}_{K_0} : \text{End}(A_k) \otimes_{\mathbb{Q}} K_0 \rightarrow \text{End}(A_k) \otimes_{\mathbb{Q}} L_0 \rightarrow \text{End}_{L_0}(D(\mathcal{G}_{A_k}))$$

and finally the element

$$\mathbf{D}_{K_0}(\pi) \in \text{End}_{L_0}(D)$$

is well defined, and (A.12) implies that $\mathbf{D}_{K_0}(\pi) = Q(\phi^f) = \pi$ in $\text{End}_{L_0}(D)$.

A.4.4. Comparison Theorem for p -divisible groups. We now review the connected-étale sequence in our comparison by factoring, for abelian varieties, the crystalline étale comparison through the categories of p -divisible groups on $\mathcal{O}_L$ and on k .

We refer to the dedicated book [14] of Fontaine, and most notably Appendix B therein. A more recent exposition can be found for example in [13, Chapter 4]. See also [11, Section 6]. In *op. cit.* Faltings describes more delicate problems about an *integral comparison* and works with $B^+(\mathcal{O}_L)$, rather than B_{crys} , but it is easy to see that those results imply the following.

Theorem A.4.1 (Comparison for p -divisible groups). *Let E be a period ring as in Theorem A.4. There exists a natural (E -linear) isomorphism*

$$(A.13) \quad \gamma(\mathcal{G}) : E \otimes_{W(k)} H_{\text{crys}}^1(\mathcal{G}_k) \xrightarrow{\sim} E \otimes_{\mathbb{Z}_p} H_{\text{ét}}^1(\mathcal{G}_{\bar{L}}, \mathbb{Z}_p).$$

of functors from the category of p -divisible groups $\mathcal{G}$ over $\mathcal{O}_L$ to that of vector spaces over E .

Remark A.4.2. We actually know that $\gamma(\mathcal{G})$ extends the map $\gamma_{\text{crys}}(A)$ from Theorem A.2.1.

We again use the E -linear dual comparisons

$$\gamma^\vee(\mathcal{G}) : \mathbf{M}(\mathcal{G}) \otimes_{W(k)} E \xleftarrow{\sim} \mathbf{T}(\mathcal{G}) \otimes_{\mathbb{Z}_p} E$$

or equivalently, with the isocrystal $D(\mathcal{G}) = \mathbf{M}(\mathcal{G}) \otimes_{W(k)} L_0$ and the $\mathbb{Q}_p$ -linear Tate module $V(\mathcal{G}) = \mathbf{T}(\mathcal{G}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, with abuse of notations,

$$\gamma^\vee(\mathcal{G}) : D(\mathcal{G}) \otimes_{L_0} E \xleftarrow{\sim} V(\mathcal{G}) \otimes_{\mathbb{Q}_p} E.$$

A.5. Assembling everything together. The following enhances Proposition 5.1.1 into a more precise statement, which we are ready to prove.

Proposition A.5.1. *Set $D_\pi := \text{Im } \mathbf{D}_{K_0}(\pi)$ for the L_0 -linear subspace of $D = \mathbf{D}(\mathcal{G}_{A_k})$ given by the image of π . We consider the comparison isomorphism*

$$\gamma_A^\vee := \gamma^\vee(A) : V \otimes_{\mathbb{Q}_p} E \rightarrow D \otimes_{L_0} E.$$

- (1) Then γ is equivariant with respect to the covariant (i.e. on the left) action of $\text{End}(A_L) \otimes_{\mathbb{Z}} E$ on both side given by
- the $\mathbf{M}()$ -functorial action of $\text{End}(A_L)$ on the $\mathbb{Z}_p$ -module M , extended E -linearly to $V \otimes_{\mathbb{Q}_p} E$;
 - the composition of the reduction $\text{End}(A_L) \xleftarrow{\sim} \text{End}(A_L) \hookrightarrow \text{End}(A_k)$ with the $\mathbf{D}()$ -functorial action of $\text{End}(A_k)$ on the $\mathbb{Q}_p$ -linear vector space D , extended E -linearly.
- (2) With the notation of Proposition 5.1.1, we have the identity

$$(A.14) \quad \gamma_A^\vee(V^r \otimes E) = D_c \otimes_{L_0} E$$

of E -linear vector subspaces of $D \otimes_{L_0} E$.

Proof. The first part is only an explicit formulation of the functoriality in $\mathcal{A}$ of the comparison isomorphisms, that is that $\gamma^\vee$ is a morphism of *functors*. This requires only the abelian varieties comparison recalled as Theorem A.2.1.

For $e \in \text{End}(\mathcal{A})$ we apply $\gamma^\vee$ to e to get the commutativity of

$$\begin{array}{ccccc} V \otimes_{\mathbb{Q}_p} E & \xrightarrow{\gamma^\vee(\mathcal{A})} & D \otimes_{L_0} E & & \\ \downarrow \gamma^\vee(e) & & \downarrow V(e) & & \downarrow D(e) \\ V \otimes_{\mathbb{Q}_p} E & \xrightarrow{\gamma^\vee(\mathcal{A})} & D \otimes_{L_0} E. & & \end{array}$$

The second part involves the connected-étale sequence, p -divisible groups and the rest of the theory. We apply $\gamma^\vee$ to the exact sequence

$$0 \longrightarrow \mathcal{G}_A^0 \xrightarrow{\iota} \mathcal{G}_A \xrightarrow{\varpi} \mathcal{G}_A^{\text{ét}} \longrightarrow 0,$$

and get the isomorphism of exact sequences, in notations (A.9) and (A.10),

$$\begin{array}{ccccccc} 0 & \longrightarrow & T^0 \otimes_{\mathbb{Z}_p} E & \xrightarrow{\mathbf{T}(\iota) \otimes E} & T \otimes_{\mathbb{Z}_p} E & \xrightarrow{\mathbf{T}(\varpi) \otimes E} & T^{\text{ét}} \otimes_{\mathbb{Z}_p} E \longrightarrow 0 \\ & & \downarrow \gamma^\vee(\mathcal{G}_A^0) & & \downarrow \gamma^\vee(\mathcal{G}_A) & & \downarrow \gamma^\vee(\mathcal{G}_A^{\text{ét}}) \\ 0 & \longrightarrow & M^0 \otimes_{W(k)} E & \xrightarrow{\mathbf{M}(\iota) \otimes E} & M \otimes_{W(k)} E & \xrightarrow{\mathbf{M}(\varpi) \otimes E} & M^{\text{ét}} \otimes_{W(k)} E \longrightarrow 0. \end{array}$$

In particular the kernel of $V(\iota) \otimes E$ is sent to the kernel of $D(\iota) \otimes E$. We have to check that the equality $\gamma(\ker V(\varpi) \otimes E) = \ker(D(\varpi) \otimes E)$ is the equality (A.14) we seek.

We can already determinate the upper kernel before passing to E from (A.11) via identity of sequences:

$$\begin{array}{ccccccc} 0 & \longrightarrow & T(\mathcal{G}_A^0) & \xrightarrow{T(\iota)} & T(\mathcal{G}_A) & \xrightarrow{T(\text{red})} & T(\mathcal{G}_A^{\text{ét}}) \longrightarrow 0 \\ & & \parallel & & \parallel & & \downarrow \sim \\ 0 & \longrightarrow & T^0 & \longrightarrow & T(A_L) & \xrightarrow{T(\varpi)} & T^{\text{ét}} \longrightarrow 0. \end{array}$$

Thanks to (A.11), we can identify T^0 with $\ker(T(\text{red}))$.

Likewise, we determinate, the lower kernel before passing from $W(k)$ to E , from the sequence

$$0 \longrightarrow M^0 \xrightarrow{\iota} M \xrightarrow{\varpi} M^{\text{ét}} \longrightarrow 0.$$

We note that $\text{End}(\mathcal{G}_k)$ acts $\mathbb{Z}_p$ -linearly on this sequence: it acts on each term and the maps are functorial. The kernel of idempotent (to prove) $\mathbf{D}_{K_0}(\pi)$ is the unit root lift $D_0 \subseteq D$ of $D^{\text{ét}}$. We want to

check that its image $D_\pi = \mathbf{D}_{K_0}(\pi)(D)$ is indeed the image of $D^0 := M^0 \otimes_{W(k)} L_0$. By exactness and dimensionality, it amounts to show that the image of D_π in $D^{\text{ét}}$ is $\{0\}$.

The map $\mathcal{G}_{A_k} \rightarrow \mathcal{G}_{A_k}^{\text{ét}}$ is $\text{End}(A_k)$ -equivariant: namely, the connected component of $\mathcal{G}_{A_k}$ is invariant under $\text{End}(A_k)$. By $\mathbf{M}()$ functoriality so is the map $M \rightarrow M^{\text{ét}}$, and equivariance extends L_0 -linearly to an action of $\text{End}(A_k) \otimes_{\mathbb{Q}} L_0$ on $D \rightarrow D^{\text{ét}}$.

We asserted that the unit root $D_0 \subseteq D$ is a linear lift of $D \rightarrow D^{\text{ét}}$. By construction, D_0 is invariant under $\mathbf{M}(\text{Frob}_{A_k})$. It follows the restriction map $D_0 \rightarrow D^{\text{ét}}$ is $L_0[\text{Frob}_{A_k}]$ -equivariant. Since $\mathbf{D}_{K_0}(\pi) = Q(\mathbf{M}(\text{Frob}_{A_k}))$ will be 0 on D_0 hence, by equivariance, on $D^{\text{ét}}$. This ends the proof of Proposition A.5.1. $\square$

REFERENCES

- [1] P. Berthelot. *Cohomologie cristalline des schemas de caractéristique $p > 0$* , volume 407. Springer, Cham, 1974.
- [2] P. Berthelot and A. Ogus. Notes on crystalline cohomology. Mathematical Notes. Princeton, New Jersey: Princeton University Press. Tokyo: University of Tokyo Press. VI, not consecutively paged., 1978.
- [3] F. A. Bogomolov. Sur l’algébricité des représentations ℓ -adiques. *C. R. Acad. Sci., Paris, Sér. A*, 290:701–703, 1980.
- [4] B. Bollobás, S. Janson, and O. Riordan. On covering by translates of a set. *Random Struct. Algorithms*, 38(1-2):33–67, 2011.
- [5] A. Cadoret and B. Moonen. Integral and adelic aspects of the Mumford-Tate conjecture. *J. Inst. Math. Jussieu*, 19(3):869–890, 2020.
- [6] M. Demazure. *Lectures on p -divisible groups*, volume 302. Springer, Cham, 1972.
- [7] B. Edixhoven. Special points on the product of two modular curves. *Compos. Math.*, 114(3):315–328, 1998.
- [8] B. Edixhoven and R. Richard. A $\bmod p$ variant of the André-Oort conjecture. *Rend. Circ. Mat. Palermo (2)*, 69(1):151–157, 2020.
- [9] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73:349–366, 1983.
- [10] G. Faltings. p -adic Hodge theory. *J. Am. Math. Soc.*, 1(1):255–299, 1988.
- [11] G. Faltings. Integral crystalline cohomology over very ramified valuation rings. *J. Am. Math. Soc.*, 12(1):117–144, 1999.
- [12] G. Faltings and G. Wüstholz, editors. *Rational points. Seminar Bonn/Wuppertal 1983/84.*, volume E6 of *Aspects Math.* Braunschweig: Friedr. Vieweg & Sohn, 3. enlarged ed. edition, 1992.
- [13] L. Fargues and J.-M. Fontaine. *Courbes et fibrés vectoriels en théorie de Hodge p -adique*, volume 406. Paris: Société Mathématique de France (SMF), 2018.
- [14] J.-M. Fontaine. *Groupes p -divisibles sur les corps locaux*, volume 47-48. Société Mathématique de France (SMF), Paris, 1977.
- [15] J.-M. Fontaine. Sur certains types de représentations p -adiques du groupe de Galois d’un corps local; construction d’un anneau de Barsotti-Tate. *Ann. Math. (2)*, 115:529–577, 1982.
- [16] P. Habegger, G. Rémond, T. Scanlon, E. Ullmo, and A. Yafaev. *Autour de la conjecture de Zilber-Pink*, volume 52. Paris: Société Mathématique de France (SMF), 2017.
- [17] M. Hindry. Autour d’une conjecture de Serge Lang. (Around a conjecture by Serge Lang). *Invent. Math.*, 94(3):575–603, 1988.
- [18] H. Iwaniec. On the problem of Jacobsthal. *Demonstr. Math.*, 11:225–231, 1978.
- [19] H.-J. Kanold. Über eine zahlentheoretische Funktion von Jacobsthal. *Math. Ann.*, 170:314–326, 1967.
- [20] B. Klingler, E. Ullmo, and A. Yafaev. Bi-algebraic geometry and the André-Oort conjecture. In *Algebraic geometry: Salt Lake City 2015*, volume 97 of *Proc. Sympos. Pure Math.*, pages 319–359. Amer. Math. Soc., Providence, RI, 2018.
- [21] S. Lang. Division points on curves. *Ann. Mat. Pura Appl. (4)*, 70:229–234, 1965.
- [22] D. W. Masser and G. Wüstholz. Factorization estimates for Abelian varieties. *Publ. Math., Inst. Hautes Étud. Sci.*, 81:5–24, 1995.
- [23] D. W. Masser and G. Wüstholz. Refinements of the Tate conjecture for abelian varieties. In *Abelian varieties. Proceedings of the international conference held in Egloffstein, Germany, October 3-8, 1993*, pages 211–223. Berlin: Walter de Gruyter, 1995.

- [24] J. Pila and U. Zannier. Rational points in periodic analytic sets and the Manin-Mumford conjecture. *Atti Accad. Naz. Lincei, Cl. Sci. Fis. Mat. Nat., IX. Ser., Rend. Lincei, Mat. Appl.*, 19(2):149–162, 2008.
- [25] M. Raynaud. Courbes sur une variété abélienne et points de torsion. *Invent. Math.*, 71:207–233, 1983.
- [26] M. Raynaud. Sous-variétés d’une variété abélienne et points de torsion. Arithmetic and geometry, Pap. dedic. I. R. Shafarevich, Vol. I: Arithmetic, Prog. Math. 35, 327–352., 1983.
- [27] R. Richard. A two dimensional arithmetic André-Oort problem. *arXiv e-prints*, page arXiv:1808.07900, Aug. 2018.
- [28] J. B. Rosser and L. Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois J. Math.*, 6(1):64–94, 03 1962.
- [29] T. Scanlon. A positive characteristic Manin-Mumford theorem. *Compos. Math.*, 141(6):1351–1364, 2005.
- [30] J.-P. Serre. *Œuvres. Collected papers. IV*. Springer-Verlag, Berlin, 2000. 1985–1998.
- [31] H. R. Stevens. On Jacobsthal’s $g(n)$ -function. *Math. Ann.*, 226:95–97, 1977.
- [32] J. T. Tate. p -divisible groups. Proc. Conf. local Fields, NUFFIC Summer School Driebergen 1966, 158–183., 1967.
- [33] J.-P. Wintenberger. Démonstration d’une conjecture de Lang dans des cas particuliers. *J. Reine Angew. Math.*, 553:1–16, 2002.
- [34] Y. G. Zarhin. A finiteness theorem for unpolarized Abelian varieties over number fields with prescribed places of bad reduction. *Invent. Math.*, 79:309–321, 1985.

I.H.E.S., UNIVERSITÉ PARIS-SACLAY, CNRS, LABORATOIRE ALEXANDRE GROTHENDIECK. 35 ROUTE DE CHARTRES, 91440 BURES-SUR-YVETTE (FRANCE)

E-mail address, G. Baldi: baldi@ihes.fr E. Ullmo: ullmo@ihes.fr

UNIVERSITY COLLEGE LONDON, DEPARTMENT OF MATHEMATICS, GOWER STREET, WC1E 6BT, LONDON, UK

E-mail address, R. Richard: rodolphe.richard@normalesup.org