(TRANSLATION) CURVES IN ABELIAN VARIETIES AND TORSION POINTS

M. RAYNAUD

Let A be an abelian variety defined over $\mathbb{C}$, T the torsion subgroup of $A(\mathbb{C})$ and X a proper, integral, non-elliptic curve in A.

Theorem I. *The set $T \cap X(\mathbb{C})$ of torsion points on X is finite.*

Recall that the analogue of this statement, where we replace T by its n-primary component ($n > 1$ an integer), was established by Bogomolov [1, Th. 3].

The idea of the proof is as follows:

Assume for simplicity that X is smooth and that X and A are defined over a number field L. Let $\mathscr{O}_L$ denote the ring of integers of L. Let U be a non-empty open subset of $\mathrm{Spec}(\mathscr{O}_L)$ such that there exists an abelian U-scheme $\mathscr{A}$ with generic fibre A and a curve $\mathscr{X}$ in $\mathscr{A}$, that is proper and smooth over U, with generic fibre X. Let $\mathscr{J}$ denote the relative Jacobian of $\mathscr{X}$ over U and $a : \mathscr{J} \to \mathscr{A}$ the Albanese morphism associated to the inclusion $\mathscr{X}$ in $\mathscr{A}$. Possibly by restricting U, we assume the following conditions hold:

i) U is unramified over $\mathrm{Spec}(\mathbb{Z})$.
ii) $\mathrm{Ker}(a)$ is smooth over U and the number of connected components n of the geometric fibres of $\mathrm{Ker}(a)$ is invertible in U.

Let v be a closed point of U over a prime p and let $\widehat{\mathscr{O}_{L,v}}$ be the completion of the local ring of v in U. By passing to the maximal unramified extension of $\widehat{\mathscr{O}_{L,v}}$, then completing, we obtain a complete discrete valuation ring R, with algebraically closed residue field k of characteristic p and fraction field K; extending L. The essential part of our proof is the following local result:

Theorem II. *For all $a \in \mathscr{A}(R)$ the points of $(\mathscr{X}+a)(k)$ that lift to points of $(\mathscr{X}+a)(R) \cap p\mathscr{A}(R)$ are finite in number, and uniformly bounded with respect to a.*

This statement immediately leads to a significant part of Theorem I: the torsion points of $\mathscr{X} + a$, of order coprime to p (which we will refer to as *p'-torsion*), are finite in number, and bounded independently of $a \in \mathscr{A}(R)$.

Changing the point v in U, we deduce an analogous result for the p-primary torsion. This comes from the finiteness of the p'-torsion and the uniform finiteness after translation of the p-primary torsion, it is then easy to deduce Theorem I (cf. 7.4).

Theorem II can be proved using *differential calculus modulo p^2*, the idea is as follows. Changing notation, let A and X be the preimages of $\mathscr{A}$ and $\mathscr{X}$ after base change $\mathrm{Spec}(R) \to U$ to the point v. Let A_0 and X_0 denote the special fibres of A and X over $R/pR = k$, and let A_1 and X_1 be the restrictions of A and X over $\mathrm{Spec}(R_1)$ where $R_1 = R/p^2R$. Let $\mathscr{I}_0$ denote the sheaf of ideals of X_0 in A_0 and $\mathscr{N}_0 = (\mathscr{I}_0/\mathscr{I}_0^2)^\vee$ denote the corresponding normal sheaf.

To establish Theorem II we have to analyse the image of $X_1(R_1) \cap pA_1(R_1)$ in $X_0(k)$. To do so we consider the blow-up E of A with centre X_0 with special fibre E_0 and V_0 the smooth open locus of E_0 over X_0. In fact V_0 is an affine space associated to the fibre bundle $\mathscr{N}_0$: it is the affine space which controls the liftings of X_0 in A_1. Locally, we can choose coordinates $x, y_1, ..., y_n$ on A, such that X_0 is given by equations $p = 0, y_1 = ... = y_n = 0$; and V is given by coordinates $x, z_1, ..., z_n$ satisfying $pz_i = y_i$. Let $h_0 : V_0 \to X_0$ denote the canonical projection. Let $(A_1, X_0)(R_1)$ denote the subset of $A_1(R_1)$ of points that reduce modulo p to points of $X_0(k)$. We then obtain a map τ allowing the following diagram to commute:

$$\begin{tikzcd}
(A_1, X_0)(R_1) \arrow[rr, "\tau"] \arrow[dr, "\text{can.}"'] & & V_0(k) \arrow[dl, "h_0"] \\
& X_0(k) &
\end{tikzcd}$$

The image of $X_1(R_1)$ under τ (resp. $(A_1, X_0) \cap pA_1(R_1)$) gives the rational points of an integral curve X_0' (resp. Y_0') in V_0. To show that the image of $X_1(R_1) \cap pA_1(R_1)$ in $X_0(k)$ is finite, it suffices to show that $X_0' \cap Y_0'$ is finite, i.e. X_0' and Y_0' are distinct. Now, h_0 induces an isomorphism $X_0' \xrightarrow{\sim} X_0$ (X_0' is the trivialisation of the bundle V_0 associated to the lift X_1 of X_0 in A_1), and we show that the radicial degree of the projection $Y_0' \to X_0$ is > 1.

We study the various lifting properties of $h : V_0 \to X_0$ in sections 2 and 3. In section 2 we study the properties of τ which are elementary in nature. In section 3, we study a lifting property connected to characteristic $p > 0$ which is useful for understanding Y_0'; it's here where we justify the introduction of V_0. To study collections of points of the form $pA_1(R_1) \cap (A_1, X_0)(R_1)$ one might have thought to use the Greenberg functor, but this hides the *radicial phenomena* which are essential for us, and are highlighted by the use of V_0.

The calculation of the radicial degree of $Y_0' \to X_0$ is done in section 4 with some preliminary results in section 1. Theorem II is proved in 4.4.1 and 6.1.1. Note that the proof, in principle, provides an upper bound for the cardinality of the image of $(\mathscr{X} + a)(R) \cap p\mathscr{A}(R)$ as a function of the fibre bundle $\mathscr{N}_0$, which will only be tractable when A is an abelian surface.

The method presented here has the disadvantage of treating the p'-torsion and p-primary torsion separately. Recently, Coleman has proposed another approach, also p-adic, which avoids this distinction. It should lead to a new proof of Theorem I and has allowed us to determine exactly the torsion points on certain Fermat curves.

Let's return to the initial problem of X in A over $\mathbb{C}$. In [5] Serge Lang poses the following problem: given a subgroup Γ in $A(\mathbb{C})$ of finite type, and the group $\bar{\Gamma}$ of division points of Γ, is $\bar{\Gamma} \cap X$ finite?

Theorem I provides an answer to this question when $\Gamma = 0$; a positive answer in general is, a priori, a stronger result than Mordell's Conjecture. As another application of Theorem II, we show that in fact Mordell's conjecture implies Lang's conjecture (for more precise statements cf. 9.2.1 and 9.2.2).

Finally, let us point out that Theorem I has natural extensions in the case where X is replaced by any subvariety of A. We will study these generalisations later in the article.

1. Curves embedded in abelian varieties in characteristic $p > 0$

1.0. In this section, k is an algebraically closed field of characteristic $p > 0$. Let S be a k-scheme. We denote by Ω_S the sheaf of differential forms of S of degree 1. For any integer $m \in \mathbb{Z}$, we write $\sigma^m : \mathrm{Spec}(k) \to \mathrm{Spec}(k)$ for the morphism which sends $a \in k$ to a^{p^m} and write $S^{(m)}$ for the k-scheme given by base change via σ^m (in other words, if S is affine, defined by polynomials $f_i = 0$ in the ring $k[T_\lambda]$, then $S^{(m)}$ is given by polynomials f_i after the coefficients are raised to the power of p^m). We then obtain a relative Frobenius morphism:

$$F : S^{(m)} \to S^{(m+1)}$$

which is a radicial k-morphism; by iterating, we obtain a k-morphism $F^n : S^{(m)} \to S^{(m+n)}$ for all $n \geq 0$. In particular, we get k-morphisms $F^n : S^{(-n)} \to S$ and $F^n : S \to S^{(n)}$.

1.1.

1.1.1. Let A be a k-abelian variety and $i : X \hookrightarrow A$ an immersion of a proper, integral k-curve. Let $\alpha : \tilde{X} \to X$ be the normalisation of X and define $\tilde{i} := i \circ \alpha : \tilde{X} \to A$. Let $J_{\tilde{X}}$ be the Jacobian of $\tilde{X}$ and $a : J_{\tilde{X}} \to A$ the Albanese morphism associated to $\tilde{i}$.

Definition 1.1.2. We will say that the immersion $i : X \hookrightarrow A$ satisfies the property $(*)$ if the following conditions are met:

i) The morphism $a : J_{\tilde{X}} \to A$ is surjective with kernel N smooth over k.
ii) The group of connected components N/N^0 of N is of order coprime to p.

Remark 1.1.3. i) The condition $(*)$ is clearly satisfied if a is an isomorphism, in particular if X is smooth and $i : X \hookrightarrow A$ is the usual embedding of X in its Jacobian.

ii) Note that part i) of $(*)$ is equivalent to the fact that the map of sections:
$$H^0(A, \Omega_A) \to H^0(\tilde{X}, \Omega_{\tilde{X}})$$
induced by $\tilde{i}$ is injective. Then condition $(*)$ is equivalent to the fact that the map:
$$H^1_{dR}(A, \Omega_A) \to H^0_{dR}(\tilde{X}, \Omega_{\tilde{X}})$$
on de Rham cohomologies is injective (we will not use this fact in what follows).

1.2.

1.2.1. Let $u : B \to A$ be an isogeny of abelian varieties, with kernel G of order a power of p and $G = G_{\text{ét}} \times G_{\text{inf}}$ the canonical decomposition of G into an étale group and an infinitesimal group. The preimage $B \times_A X$, of X under u, is not reduced as soon as the dimension of A is ≥ 2. Let Y be the unique reduced curve that is set-wise equal to $B \times_A X$ and $v : Y \to X$ the morphism induced by u. Even if X is smooth, this does not guarantee that Y is smooth; however, smoothness is preserved if G_{inf} is the kernel of an iteration of Frobenius morphisms on B (this will be the case if either of the following two conditions are fulfilled: i) $B = A$ and u is the multiplication by p map; ii) A is ordinary or A is the product of supersingular elliptic curves). We denote by $\beta : \tilde{Y} \to Y$ the normalisation of Y, $j : Y \hookrightarrow B$ the canonical immersion, $\tilde{j} := j \circ \beta$ and $\tilde{v} : \tilde{Y} \to \tilde{X}$ the normalisation of v.

Proposition 1.2.2. *Suppose $i : X \hookrightarrow A$ satisfies $(*)$ (1.1.2). Then:*

i) The curve Y is integral and it's separable degree over X is the rank of $G_{\text{ét}}$.
ii) The radicial degree of Y over X is p^s where s is the smallest integer such that F^s annihilates G_{inf}.

The fact that Y is integral (or equivalently $\tilde{Y}$ is connected) follows from part ii) of $(*)$: indeed this implies that the fibre product $B \times_A J_{\tilde{X}}$ induced by u and a is connected and we reduce to the classical case $X = \tilde{X}$ and $A = J_X$.

To establish ii), we can, even if it means dividing B by $G_{\text{ét}}$, reduce to the case $G = G_{\text{inf}}$. Let p^r be the radicial degree of Y relative to X. As G is annihilated by F^s, there is a factorisation of F^s on B:
$$F^s : B \xrightarrow{u} A \to B^{(s)}$$
and thus we get a factorization of F^s on Y:
$$F^s : Y \xrightarrow{v} X \to Y^{(s)}$$
when $r \leq s$. The reverse inequality follows from the following lemma:

Lemma 1.2.3. *Suppose that $u : B \to A$ is a radicial isogeny, $Y \to X$ is of degree p^r and that $i : X \hookrightarrow A$ satisfies condition (i) of $(*)$. Then we get a canonical factorisation:*
$$F^r : A^{(-r)} \to B \xrightarrow{u} A$$
and in particular $G = G_{\text{inf}}$ is annihilated by F^r.

We can identify $\tilde{Y}$ with $\tilde{X}^{(-r)}$ and $\tilde{v} : \tilde{Y} \to \tilde{X}$ with F^r. The Jacobian of $\tilde{X}^{(-r)}$ is $J_{\tilde{X}}^{(-r)}$. We then deduce from the commutative diagram:

$$\begin{tikzcd} \tilde{X}^{(-r)} \arrow[r] \arrow[d, "F^r"'] & Y \arrow[d, "v"] \\ \tilde{X} \arrow[r] & X \end{tikzcd}$$

(where the horizontal arrows are normalisations), a commutative diagram of abelian schemes:

$$\begin{tikzcd} J_{\tilde{X}}^{(-r)} \arrow[rr, "a^{(-r)}"] \arrow[dd, "F^r"'] \arrow[dr, "b"] & & A^{(-r)} \arrow[dd, "F^r"] \\ & B \arrow[dr, "u"] & \\ J_{\tilde{X}} \arrow[rr] & & A \end{tikzcd}$$

where b is the Albanese morphism associated to $\tilde{j} : \tilde{X}^{(-r)} = \tilde{Y} \to B$. But $\mathrm{Ker}(a^{(-r)}) = N^{(-r)}$ is a smooth group scheme, so its image under b is a smooth subgroup scheme of B. Again the image is contained in $\mathrm{Ker}(u) = G$ which is assumed to be radicial, this image is zero and we obtain a morphism $c : A^{(-r)} \to B$ such that $b = c \circ a^{(-r)}$. But then as $a^{(-r)}$ is surjective, $F^r : A^{(-r)} \to A$ factors through $u \circ c$, then the lemma follows.

1.3.

1.3.1. By translation, we identify the tangent space at any point of A to the tangent space at the origin and we write $\mathbb{P}_A$ for the associated projective space. The curve X embedded in A by i has an associated *Gauss map*: if x is a smooth point of X, we can associate to it a point of $\mathbb{P}_A$ defined by the tangent to X at x. We thus obtain a morphism from the smooth locus of X to $\mathbb{P}_A$ which canonically extends to a morphism $\gamma_X : \tilde{X} \to \mathbb{P}_A$. Let $\mathscr{I}$ be the sheaf of ideals of $\mathscr{O}_A$ which defines X, then we obtain an exact sequence:

$$\mathscr{I}/\mathscr{I}^2 \to \Omega_A|_X \to \Omega_X \to 0 \tag{1}$$

Pulling back this sequence via $\alpha : \tilde{X} \to X$, we obtain an exact sequence on $\tilde{X}$:

$$\alpha^*(\mathscr{I}/\mathscr{I}^2) \to \tilde{i}^*(\Omega_A) \to \alpha^*(\Omega_X) \to 0$$

If we divide $\alpha^*(\Omega_X)$ by its torsion subsheaf, then we obtain an invertible sheaf $\tilde{\Omega}_X$; a quotient of $\tilde{i}^*(\Omega_A)$, this defines a map $\gamma_X : \tilde{X} \to \mathbb{P}_A$. So we have an exact sequence of locally free sheaves on $\tilde{X}$:

$$0 \to \tilde{\mathscr{N}}_X^\vee \to \tilde{i}^*(\Omega_A) \to \tilde{\Omega}_X \to 0 \tag{2}$$

where $\tilde{\mathscr{N}}_X^\vee$ is the subsheaf of $\tilde{i}^*(\Omega_A)$ generated by the image of $\alpha^*(\mathscr{I}/\mathscr{I}^2)$. Note that $\tilde{\Omega}_X$ is simply the image of the map of differentials $\alpha^*(\Omega_X) \to \tilde{\Omega}_X$ associated to α. In particular, the degree of γ_X, which is the degree of the invertible sheaf $\tilde{\Omega}_X$, is at most $2g_{\tilde{X}} - 2$ where $g_{\tilde{X}}$ is the genus of $\tilde{X}$. Of course, when X is smooth, $\tilde{\Omega}_X = \Omega_X$ and $\tilde{\mathscr{N}}_X^\vee = \mathscr{I}/\mathscr{I}^2$ is the normal sheaf.

1.3.2. Let's return to the situation of 1.2.1 where we have an isogeny $u : B \to A$. The immersions $i : X \hookrightarrow A$ and $j : Y \hookrightarrow B$ correspond to Gauss maps: $\gamma_X : \tilde{X} \to \mathbb{P}_A$ and $\gamma_Y : \tilde{Y} \to \mathbb{P}_B$.

The map γ_X is constant if and only if $\tilde{\Omega}_X = \mathscr{O}_X$. This is the case when X is elliptic or if X is stable under translations by a radicial subgroup of rank p (for example, if $i : X \hookrightarrow A$ satisfies $(*)$ and if we take a radicial isogeny $u : B \to A$ of degree p, then γ_Y is constant). If $i : X \hookrightarrow A$ satisfies $(*)$, $H^0(X, \tilde{\Omega}_X)$ is a k-vector space of dimension at least the dimension of A, in particular, γ_X is non-constant if the genus of $\tilde{X}$ is at least 2.

Proposition 1.3.3. *Suppose the isogeny u is radicial and $i : X \hookrightarrow A$ satisfies $(*)$ (1.1.2) and that $\tilde{X}$ is of genus ≥ 2. Then we have:*

$$\mathrm{degree}(\gamma_Y) \leq \mathrm{degree}(\gamma_X)$$

In fact, if p^r is the degree of $Y \to X$ we have, as in 1.2.3, a factorisation:

$$F^r : A^{(-r)} \xrightarrow{w} B \xrightarrow{u} A$$

Then w induces a birational map, we denote again by $w : X^{(-r)} \to Y$. Let $\tilde{X}^{(-r)} = \tilde{Y}$ be the common normalisation of $X^{(-r)}$ and Y. Then using the notation of 1.3.1, we obtain inclusions $\tilde{\Omega}_Y \subset \tilde{\Omega}_{X^{(-r)}} \subset \Omega_{\tilde{X}^{(-r)}}$ and therefore $\mathrm{degree}(\gamma_Y) \leq \mathrm{degree}(\gamma_{X^{(-r)}})$. But $\mathrm{degree}(\gamma_{X^{(-r)}}) \leq \mathrm{degree}(\gamma_X)$ by translating by the isomorphism σ^r (1.0), the proposition then follows.

Corollary 1.3.4. *Let us take the isogeny u to be the multiplication by p map on A, denoted p_A. Then $i : X \hookrightarrow A$ satisfies $(*)$ and if X has genus ≥ 2, then the images of the maps γ_Y and $\gamma_X \circ p_A$ on $Y \to \mathbb{P}_A$ only have finitely many points in common.*

As Y is reduced, it suffices to show $\gamma_X \circ p_A \neq \gamma_Y$ and, a fortiori, we can do this by showing the maps have different degree. Let $A \xrightarrow{v} B \xrightarrow{u} A$ be the factorisation of p_A where v is étale and u is radicial of degree p^r. As p_A factors through the Frobenius of A, we have $r \geq 1$. The two maps $\gamma_X \circ p_A$ and γ_Y are factorisations of v, so replacing p_A with $u : B \to A$, we reduce to the case of a radicial isogeny. We then have that $\mathrm{degree}(\gamma_Y) \leq \mathrm{degree}(\gamma_X)$ by (1.3.3). But $\mathrm{degree}(\gamma_X \circ u) = p^r \mathrm{degree}(\gamma_X) > \mathrm{degree}(\gamma_X)$ (since $r \geq 1$ and $\mathrm{degree}(\gamma_X) \geq 1$) thus:

$$\mathrm{degree}(\gamma_Y) < \mathrm{degree}(\gamma_X \circ u)$$

1.3.5. In this subsection we reformulate Corollary 1.3.4 in terms of sheaves. We use the notation of 1.2.1 with $u = p_A$.

Let $\omega_1, ..., \omega_d$ be a basis for Ω_A and $[p] : p_A^*(\Omega_A) \xrightarrow{\sim} \Omega_A$ the isomorphism induced by the identity on global sections; i.e. $[p](p_A^*(\omega_i)) = \omega_i$, for $i = 1, ..., d$. Pulling back along $j : Y \hookrightarrow A$ we obtain an isomorphism $[p]_Y : (i \circ u)^*(\Omega_A) \xrightarrow{\sim} j^*\Omega_A$ which fits in the following diagram:

$$\begin{tikzcd}
v^*(\mathscr{I}/\mathscr{I}^2) \arrow[r] & (i \circ v)^*(\Omega_A) \arrow[r] \arrow[d, "{[p]_Y}"] & v^*(\Omega_X) \arrow[r] & 0 \\
\mathscr{J}/\mathscr{J}^2 \arrow[r] & j^*(\Omega_A) \arrow[r] & \Omega_Y \arrow[r] & 0
\end{tikzcd} \tag{1}$$

in which the rows are exact, the first being the pullback of the exact sequence (1) of 1.3.1 by v associated to γ_X, and the second being the analogue of (1) for γ_Y.

Taking the pullback of this diagram by the normalisation $\beta : \tilde{Y} \to Y$ and replacing the exact sequence (1) of 1.3.1 by the exact sequence (2), we obtain the following diagram with exact rows:

$$
\begin{tikzcd}
0 \arrow[r] & \tilde{v}^*(\tilde{\mathscr{N}}_X^\vee) \arrow[r] & (\tilde{i}\circ\tilde{v})^*(\Omega_A) \arrow[r] \arrow[d, "{[p]_{\tilde{Y}}}"'] & \tilde{u}^*(\tilde{\Omega}_X) \arrow[r] & 0 \\
0 \arrow[r] & \tilde{\mathscr{N}}_Y^\vee \arrow[r] & \tilde{j}^*(\Omega_A) \arrow[r] & \tilde{\Omega}_Y \arrow[r] & 0
\end{tikzcd} \tag{2}
$$

where $[p]_{\tilde{Y}}$ is the isomorphism obtained by pulling back $[p]$ along $\tilde{j}$. By composing, we obtain the following morphisms from the diagrams:

$$\gamma : v^*(\mathscr{I}/\mathscr{I}^2) \to \Omega_Y \quad \text{and} \quad \tilde{\gamma} : \tilde{v}^*(\tilde{\mathscr{N}}_X^\vee) \to \tilde{\Omega}_Y \tag{3}$$

Of course γ is identified with $\tilde{\gamma}$ on the smooth locus of Y that lies above the smooth locus of X.

Let's describe γ locally. Let a be a local section of $\mathscr{I}$ and $\bar{a}$ it's image in $\mathscr{I}/\mathscr{I}^2$ and $da = \sum_i f_i\omega_i$ the differential of a. Then the image of $\bar{a}$ in $\Omega_A|_X$ under the morphism in 1.3.1 (1) is simply $da|_X$. Then:

$$\gamma(v^*(\bar{a})) = \sum_i (f_i \circ u)\omega_i|_Y \tag{4}$$

Corollary 1.3.6. *Under the hypotheses of 1.3.4, the maps γ and $\tilde{\gamma}$ are non-zero.*

Since $\tilde{\mathscr{N}}_X^\vee$ is locally free and as γ and $\tilde{\gamma}$ coincide over a non-empty open set, it suffices to show that $\tilde{\gamma} \neq 0$. Now, if we had $\tilde{\gamma} = 0$, $[p]_{\tilde{Y}}$ would induce, by passing to the quotient in (2), an isomorphism $\tilde{v}^*(\tilde{\Omega}_X) \xrightarrow{\sim} \tilde{\Omega}_Y$ and we have already observed that γ_Y and $\gamma_X \circ p_A$ do not have the same degree (cf. 1.3.4).

Remark 1.3.7. The same degree argument show that Corollaries 1.3.4 and 1.3.6 still hold if we assume X is smooth and of genus ≥ 2, even if $i : X \hookrightarrow A$ does not satisfy $(*)$. The condition $(*)$ is used, in part, to treat the case when X is singular, and on the other hand to explicitly compute degrees (cf. 1.2.2).

2. Notes on the normal bundle

2.0. In this section, R_1 is a local ring with maximal ideal $\mathfrak{m}$, residue field k; we suppose that $\mathfrak{m}^2 = 0$ and that $\mathfrak{m}$ is a 1-dimensional k-vector space; and choose a generator π of $\mathfrak{m}$. In what follows, we will take R_1 to be the quotient of a discrete valuation ring by the square of its maximal ideal. We denote k-schemes with an index 0, in particular, if S_1 is an R_1-scheme, S_0 denotes the k-scheme $S_1 \times_{R_1} k$, induced by reduction modulo $\mathfrak{m}$ on S_1.

2.0.1. Let S_1 be an R_1-scheme. Multiplication by π induces a morphism of $\mathscr{O}_{S_0}$-modules $\theta : \mathscr{O}_{S_0} \to \pi\mathscr{O}_{S_1} = \pi\mathscr{O}_{S_0}$. We will frequently use the fact that S_1 is flat over R_1 only if θ is an isomorphism [2, Ch. III, §5, Th. 1]. When this condition is met, we will denote by π^{-1} the inverse of θ.

2.1. Let S be a scheme and $\mathscr{M}$ a quasi-coherent $\mathscr{O}_S$-module. Recall that the vector bundle $\mathbb{V}(\mathscr{M}^\vee)$, associated to the sheaf $\mathscr{M}$, is the affine S-scheme defined by the total space of the symmetric algebra of $\mathscr{M}$; it represents the functor sending $f : T \to S$ to the set of morphisms of $\mathscr{O}_T$-modules $u : f^*(\mathscr{M}) \to \mathscr{O}_T$.

2.2. For the remainder of this section, we consider an R_1-scheme A_1 and a closed subscheme X_0 of $A_0 = A_1 \times_{R_1} k$. Let $\mathscr{I}$ (resp. $\mathscr{I}_0$) be the ideal sheaf of $\mathscr{O}_{A_1}$ (resp. $\mathscr{O}_{A_0}$) that defines X_0. Then the image of π in $\mathscr{O}_{A_1}$ is contained in $\mathscr{I}$ and we obtain exact sequences:

$$(1)\qquad \begin{array}{c} \pi\mathscr{O}_{A_0} \longrightarrow \mathscr{I} \longrightarrow \mathscr{I}_0 \longrightarrow 0 \\ \\ \pi\mathscr{O}_{X_0} \longrightarrow \mathscr{I}/\mathscr{I}^2 \longrightarrow \mathscr{I}_0/\mathscr{I}_0^2 \longrightarrow 0 \end{array}$$

Considering the vector bundle $\mathbb{V}(\mathscr{I}^\vee)$ over the scheme A_1 and let $\mathbb{V}(\mathscr{I}^\vee)^*$ denote the subscheme of $\mathbb{V}(\mathscr{I}^\vee)$ that represents the following functor: for all A_1-schemes $f : T \to A_1$, $\mathbb{V}(\mathscr{I}^\vee)^*(T)$ is the subset of $\mathbb{V}(\mathscr{I}^\vee)(T)$ given by morphisms $u : f^*(\mathscr{I}) \to \mathscr{O}_T$ that satisfy $u(\pi) = 1$ (where we abuse notation using π to mean the canonical image of π in $f^*(\mathscr{I})$).

If $u : f^*(\mathscr{I}) \to \mathscr{O}_T$ corresponds to a point of $\mathbb{V}(\mathscr{I}^\vee)^*$, we then have: $0 = u(\pi^2) = \pi \cdot 1$, so π annihilates $\mathscr{O}_T$. Moreover, $\mathscr{I} \cdot \mathscr{O}_T = u(\mathscr{I} \cdot \pi) = \pi \cdot u(\mathscr{I}) = 0$, so $\mathscr{I}$ annihilates $\mathscr{O}_T$. In other words, the structural morphism $\mathbb{V}(\mathscr{I}^\vee)^* \to A_1$ factors through X_0; in particular $\mathbb{V}(\mathscr{I}^\vee)^* = \mathbb{V}((\mathscr{I}/\mathscr{I}^2)^\vee)^*$. From now on we simply denote V_0, for the X_0-scheme $\mathbb{V}(\mathscr{I}^\vee)^*$ and $h_0 : V_0 \to X_0$ for the structural morphism.

Example 2.2.1. i) If $A_1 = A_0$, we have $\pi = 0$ in $\mathscr{O}_{A_1}$, and therefore V_0 is empty. In fact the most interesting case is when A_1 if flat over R_1.

ii) If A_1 is smooth over R_1 and if X_0 is smooth over k, then $h_0 : V_0 \to X_0$ is smooth. More precisely, suppose A_1 is affine over X_0, and defined by a regular sequence in A_0 that lift to elements t_i in $\mathscr{I}$. Then there exists unique sections T_i in $\mathscr{O}_{A_0}$, such that $t_i = \pi T_i$ (2.0.1) and V_0 is the affine space over X_0 with coordinates T_i.

2.2.2. There is a natural action of $\mathbb{V}((\mathscr{I}_0/\mathscr{I}_0^2)^\vee)$ on $\mathbb{V}(\mathscr{I}^\vee)^*$. In fact, if $f : T \to A$ is an A-scheme, we deduce from (1) the exact sequence:

$$f^*(\mathscr{O}_{X_0}) \to f^*(\mathscr{I}/\mathscr{I}^2) \xrightarrow{\tau} f^*(\mathscr{I}_0/\mathscr{I}_0^2) \to 0$$

Then if $u : f^*(\mathscr{I}/\mathscr{I}^2) \to \mathscr{O}_T$ sends π to 1, for any other morphism u' with this property we have a unique decomposition $u' = u + v \circ \tau$ for a unique map $v : f^*(\mathscr{I}_0/\mathscr{I}_0^2) \to \mathscr{O}_T$. This defines the action of $\mathbb{V}((\mathscr{I}_0/\mathscr{I}_0^2)^\vee)$ on $\mathbb{V}(\mathscr{I}^\vee)^*$ and shows that $\mathbb{V}(\mathscr{I}^\vee)^*$ is formally a principal homogeneous space under this action [10, Exp. III, p. 13].

2.3. Let S_1 be a flat R_1-scheme and $u_1 : S_1 \to A_1$ an R_1-morphism such that $u_0 : S_0 \to A_0$ factors through X_0. This last condition means we have $\mathscr{I} \cdot \mathscr{O}_{S_1} = \pi \cdot \mathscr{O}_{S_1}$. Moreover, the flatness of S_1 ensure that the multiplication by $\pi : \mathscr{O}_{S_0} \to \pi\mathscr{O}_{S_1}$ is an isomorphism (2.0.1), hence defining a morphism of $\mathscr{O}_{S_1}$-modules $u^*(\mathscr{I}) \xrightarrow{\text{can.}} \mathscr{I} \cdot \mathscr{O}_{S_1} = \pi \cdot \mathscr{O}_{S_1} \xrightarrow{\pi^{-1}} \mathscr{O}_{S_0}$ that sends $u^*(\pi)$ to 1. This then corresponds to a k-morphism $u_0' : S_0 \to V_0$ where $f_0 \circ u_0' = u_0$. We will then say that u_0' is a *lift* of u_0 through V_0.

Let $(A_1, X_0)(R_1)$ be the subset of points of $A_1(R_1)$ whose image in $A_0(k)$ lies in $X_0(k)$. The lifting operation applied to $S_1 = \mathrm{Spec}(R_1)$ gives a canonical map $\tau : (A_1, X_0)(R_1) \to V_0(k)$ that forms a commutative diagram:

$$\begin{tikzcd} (A_1, X_0)(R_1) \arrow[rr, "\tau"] \arrow[dr] & & V_0(k) \arrow[dl, "h_0"] \\ & X_0(k) & \end{tikzcd}$$

When A_1 is smooth over R_1 and X_0 is smooth over k, the map τ is surjective, as can be seen from using the coordinates in 2.2.1 ii).

Example 2.3.1. Let us return to Example 2.2.1 ii) using the notation t_i and T_i. If S_1 is a flat R_1-scheme and $u_1 : S_1 \to A_1$ an R_1-morphism such that u_0 factorises through X_0, then $t_i \circ u = \pi f_i$ for some unique sections f_i of $\mathscr{O}_{S_0}$. Then the lift u_0' of u_0 is given by the relations: $T_i \circ u_0' = f_i$.

2.4. Let X_1 be a subscheme of A_1, flat over R_1 such that $X_1 \times_{A_1} k = X_0$. Let $j_1 : X_1 \hookrightarrow A_1$ be inclusion and $\mathscr{J}$ the corresponding sheaf of ideals in $\mathscr{O}_{A_1}$ defining X_1. The lift (2.3) of j_0 is a k-morphism $j_0' : X_0 \to V_0$ such that $h_0 \circ j_0' = j_0$, then j_0' is a section of h_0. We have $\mathscr{J} \subset \mathscr{I}$ and the image of $\mathscr{I}$ in the quotient sheaf $\mathscr{O}_{X_1} = \mathscr{O}_{A_1}/\mathscr{J}$ is $\pi\mathscr{O}_{X_1} = \pi\mathscr{O}_{X_0}$. If we go back to the definition of the lift, we find that j_0' is associated to a morphism of sheaves: $\mathscr{I} \to \pi\mathscr{O}_{X_1} \to \mathscr{O}_{X_0}$ by composing the canonical surjection and the isomorphism π^{-1}. In particular, the kernel of this map is $\mathscr{J}$. Conversely, if we take a section j_0' of h_0, it arises from a morphism of sheaves $\mathscr{I} \to \mathscr{O}_{X_0}$ that sends π to 1. Let $\mathscr{J}$ be its kernel. Then we have an exact sequence:

$$0 \to \mathscr{O}_{X_0} \xrightarrow{\theta} \mathscr{O}_{A_1}/\mathscr{J} \to \mathscr{O}_{A_1}/\mathscr{I} \to 0$$

where $\mathscr{O}_{A_1}/\mathscr{I} = \mathscr{O}_{X_0}$ and where $\theta(1)$ is the image of π. If X_1 is a subscheme of A_1 defined by $\mathscr{J}$ then $X_0 = X_1 \times_{B_1} k$ is flat over R_1 (2.0.1). We have then established the following result (well known in the case where A_0 and X_0 are smooth over k [4, Cor. 5.4].

Proposition 2.4.1. *The lift (2.3) provides a canonical bijection between subschemes X_1 of A_1, which are flat over R_1 such that $X_1 \times_{B_1} k = X_0$, and the sections of $h_0 : V_0 \to X_0$.*

3. Differential calculus modulo p^2

3.0. In this section, we use the notation of the previous section, but assume further that the residue field k of R is algebraically closed with characteristic $p > 0$ and that the generator u of its maximal ideal $\mathfrak{m}$ is the image of p. In other words, R_1 is the quotient, modulo p^2, of a discrete valuation ring of mixed characteristic, unramified, with algebraically closed residue field of characteristic $p > 0$.

3.1. Let $u_1 : B_1 \to A_1$ be an R_1-morphism of smooth schemes, such that $u_0 = u_1 \times_{R_1} k : B_0 \to A_0$ has zero differential. Let $i_0 : X_0 \hookrightarrow A_0$ be a closed immersion, Y_0 the reduced preimage of X_0 in B_0 and $j_0 : Y_0 \hookrightarrow B_0$ the associated immersion. We denote by $v_0 : Y_0 \to X_0$ the morphism induced by $u_0 : B_0 \to A_0$. Let $\mathscr{I}$ (resp. $\mathscr{I}_0$) denote the ideal sheaf of X_0 in A_1 (resp. X_0 in A_0) and let $\mathscr{J}$ (resp. $\mathscr{J}_0$) denote the ideal sheaf of Y_0 in B_1 (resp. Y_0 in B_0). We have $\mathscr{I} \cdot \mathscr{O}_{B_1} \subset \mathscr{J}$ and $\mathscr{I}_0 \cdot \mathscr{O}_{B_0} \subset \mathscr{J}_0$.

If $h_0 : V_0 \to X_0$ is associated to $\mathscr{I}$ as in 2.2, then we have a map (2.3) $\tau : (A_1, X_0)(R_1) \to V_0(k)$. Similarly, let $(B_1, Y_0)(R_1)$ be the preimage of $Y_0(k)$ in $B_1(R_1)$ via the canonical map $B_1(R_1) \to B_0(k)$. Since the differential of u_0 is zero, the map $B_1(R_1) \to A_1(R_1)$ induced by u factorises through $B_0(k)$. A fortiori, the map $(B_1, Y_0)(R_1) \to (A_1, X_0)(R_1)$ induced by u factorises through $Y_0(k)$ via $\bar{u} : Y_0(k) \to (A_1, X_0)(R_1)$. Composing $\bar{u}$ with τ, we obtain a map of sets $Y_0(k) \to V_0(k)$. In this section, we construct a canonical k-morphism $v_0' : Y_0 \to V_0$ which, on points, is equal to $\tau \circ \bar{u}$. We will then calculate the differential of v_0'. Putting this all together we obtain a commutative diagram:

(1)
$$\begin{tikzcd}
(B_1, Y_0)(R_1) \arrow[r, "u"] \arrow[d] & (A_1, X_0)(R_1) \arrow[r, "\tau"] \arrow[d] & V_0(k) \arrow[dl, "h_0"] \\
Y_0(k) \arrow[r, "v_0"] \arrow[ur, "\bar{u}"] \arrow[urr, "v_0'"] & X_0(k) &
\end{tikzcd}$$

3.2. Let a and b be sections of $\mathscr{O}_{A_1}$, over an open set U, a_0, b_0 (resp. $\underline{a}$ and $\underline{b}$ and resp. $\underline{a}_0$ and $\underline{b}_0$) their images in $\mathscr{O}_{A_0}$ (resp. $\mathscr{O}_{B_1}$ and resp. $\mathscr{O}_{B_0}$. As k is perfect and B_0 is smooth, and as the differential of u_0 is zero, $\underline{a}$ and $\underline{b}$ are p^{th} powers in $\mathscr{O}_{B_0}$: $\underline{a}_0 = \alpha_0^p$, $\underline{b}_0 = \beta_0^p$. Let α and β be lifts of α_0 and β_0 in $\mathscr{O}_{B_1}$. Then α^p is the unique lift of $\underline{a}_0$ in $\mathscr{O}_{B_1}$ that is a p^{th} power; it is the *Teichmuller lift* of $\underline{a}_0$ which we denote by $\underline{a}_0^*$. Similarly, let $\underline{b}_0^* = \beta^p$. We then have relations:

$$(\underline{ab})_0^* = \underline{a}_0^*\underline{b}_0^*; \quad (\underline{a+b})_0^* = \underline{a}_0^* + \underline{b}_0^* + pS(\alpha_0, \beta_0) \tag{2}$$

where $S(U,V)$ is the degree p homogeneous polynomial in $\mathbb{Z}[U,V]$ given by:

$$S(U,V) = [(U+V)^p - U^p - V^p]/p$$

Since B_1 is flat over R_1 and $\underline{a}$ and $\underline{a}_0^*$ are both lifts of $\underline{a}_0$, there exists by 2.0.1 a unique section $\Phi(a)$ of $\mathscr{O}_{B_0}$, such that:

$$\underline{a} = \underline{a}_0^* + p\Phi(a) \tag{3}$$

From (2) we deduce the identities:

$$\begin{aligned} \Phi(a+b) &= \Phi(a) + \Phi(b) + S(\alpha_0, \beta_0) \\ \Phi(ab) &= \underline{a}_0\Phi(b) + \underline{b}_0\Phi(a) \\ \Phi(p) &= 1 \end{aligned} \tag{4}$$

Suppose $a \in \mathscr{I}$, then $\underline{a}_0 = \alpha_0^p \in \mathscr{J}_0$ and since Y_0 is reduced, $\alpha_0 \in \mathscr{J}_0$ and therefore $\underline{a}_0 \in \mathscr{J}_0^p$. The identities (4) then show that Φ is linear modulo $\mathscr{J}_0^p$ and, a fortiori, defines a morphism of sheaves: $u_1^*(\mathscr{I}) \to \mathscr{O}_{B_0}/\mathscr{J}_0$ that sends p to 1. By the definition of V_0 (2.2), the morphism of sheaves corresponds to a k-morphism $v_0' : Y_0 \to V_0$. We now show that map $\tau \circ \bar{u} : Y_0(k) \to V_0(k)$ is induced by v_0' (which describes it completely as Y_0 is reduced and k is algebraically closed). For this we note that if $f_1 : C_1 \to B_1$ is an R_1-morphism with C_1 smooth over R_1, and if Z_0 is the preimage of Y_0 under f_0, then the previous construction of v_0' is functorial with respect to f, i.e. it associates to f a morphism $v_0' \circ f_0 : Z_0 \to V_0$. We apply this to the case $C_1 = \operatorname{Spec}(R_1)$ and for $f_1 : \operatorname{Spec}(R_1) \to B_1$ a point of $(B_1, Y_0)(R_1)$. Then $Z_0 = \operatorname{Spec}(k)$, and the construction above associates to f_1 a unique linear map: $I \xrightarrow{\text{can}} \mathfrak{m} \xrightarrow[\sim]{p^{-1}} k$ therefore corresponding to the lift of f_1 in the sense of 2.3.

3.3. In the remainder of this section, we calculate the differential of v_0'. The definition of $V_0 = \mathbb{V}(\mathscr{I}^\vee)^*$ (2.2) implies that the relative sheaf of differentials Ω_{V_0/X_0} of V_0 over X_0 is canonically isomorphic to $h_0^*(\mathscr{I}_0/\mathscr{I}_0^2)$, hence giving an exact sequence:

$$h_0^*(\Omega_{X_0}) \to \Omega_{V_0} \to h_0^*(\mathscr{I}_0/\mathscr{I}_0^2) \to 0 \tag{5}$$

As the differential of u_0 is zero, the differential of v_0' comes from, by passing to the quotient, the following map:

$$\delta : (v_0')^*(\Omega_{V_0/X_0}) = v_0^*(\mathscr{I}_0/\mathscr{I}_0^2) \to \Omega_{Y_0} \tag{6}$$

which we will determine.

Let $\bar{a}_0$ be a local section of $\mathscr{I}_0/\mathscr{I}_0^2$; the image of a local section a of $\mathscr{I}$. Using the notation of 3.2, with a:

$$\delta v_0^*(\bar{a}_0) = d\Phi(a)|_{Y_0}$$

But according to (3) we have:

$$du_1^*(a) = u_1^*(da) = p(d\alpha_0 + d\Phi(a))$$

Then $u_1^*(da) = p\Psi(a)$ where $\Psi(a)$ is the unique local section of Ω_{B_0} such that

$$\Psi(a) = d\alpha_0 + d\Phi(a)$$

As $\alpha_0 \in \mathscr{J}_0$, we have $\Psi(a)|_{Y_0} = d\Phi(a)|_{Y_0}$ therefore is equal to $\delta v_0^*(\bar{a}_0)$.

In summary, we have the following result:

Proposition 3.3.1. *Under the hypotheses of 3.1, there exists a unique k-morphism $v_0' : Y_0 \to V_0$, such that $h_0 \circ v_0' = v_0$ and which, on rational points is equal to the map $\tau \circ \bar{u} : Y_0(k) \to V_0(k)$. The map δ (6) describes the differential of v_0' and is calculated as follows: let a be a local section of $\mathscr{I}$, with image $\bar{a}_0$ in $\mathscr{I}_0/\mathscr{I}_0^2$. Then $\delta v_0^*(\bar{a}_0) = \Psi(a)|_{Y_0}$ where $\Psi(a)$ is the unique local section of Ω_{B_0}, such that $u_1^*(da) = p\Psi(a)$.*

4. Applications of calculus modulo p^2 to abelian schemes

4.0. In this section R_1 is a local ring of the type considered in 3.0.

Let A_1 be an abelian R_1-scheme, $i_0 : X_0 \hookrightarrow A_0 = A_1 \times_{R_1} k$ the inclusion of a proper, integral curve with associated sheaf of ideals $\mathscr{I}$ (resp. $\mathscr{I}_0$) over A_1 (resp. over A_0). We denote $h_0 : V_0 \to X_0$ for the X_0-scheme $\mathbb{V}(\mathscr{I}^\vee)^*$ considered in 2.2. Let $(A_1, X_0)(R_1)$ be the preimage of $X_0(k)$ in $A_1(R_1)$ under the reduction modulo p map $A_1(R_1) \to A_0(k)$. Then the lifting operation (2.3) provides a canonical map τ which makes the following diagram commute:

$$\begin{tikzcd}
(A_1, X_0)(R_1) \arrow[rr, "\tau"] \arrow[dr, "\text{can.}"'] & & V_0(k) \arrow[dl, "h_0"] \\
& X_0(k) &
\end{tikzcd}$$

4.1. Let p_{A_1} (resp. p_{A_0}) represent multiplication by p on A_1 (resp. A_0). Since the differential of p_{A_0} is zero, we are in the situation of the previous section, taking $B_1 = A_1$ and $u_1 = p_{A_1}$. Let Y_0 be the reduced preimage of X_0 under p_{A_0} and $v_0 : Y_0 \to X_0$ the morphism induced by p_{A_0}.

The multiplication map $p_{A_1} : A_1(R_1) \to A_1(R_1)$ defines, by passage to the quotient, a map $\bar{p} : A(k) \to A_1(R_1)$; this induces a map $\bar{p}_{Y_0} : Y_0(k) \to (A_1, X_0)(R_1)$. The image of $\bar{p}_{Y_0}$ is formed of the points of $pA_1(R_1)$ which are lifts of points of $X_0(k)$. From 3.3.1, there exists a canonical k-morphism $v_0' : Y_0 \to V_0$ that factors as $h_0 \cdot v_0' = v_0$ which, on k-valued points, coincides with $\tau \circ \bar{p}_{Y_0}$. We then obtain the following commutative diagram:

(1)
$$\begin{tikzcd}
Y_0(k) \arrow[r, "\bar{p}_{Y_0}"'] \arrow[rr, bend left, "v_0'"] \arrow[dr, "v_0"'] & (A_1, X_0)(R_1) \arrow[r, "\tau"'] \arrow[d, "\text{can.}"] & V_0(k) \arrow[dl, "h_0"] \\
& X_0(k) &
\end{tikzcd}$$

We will reuse the notation of section 1, except now k-schemes and k-morphisms will be given an index 0. The closed immersions $X_0 \hookrightarrow A_0$ and $Y_0 \hookrightarrow A_0$ correspond to Gauss maps (1.3.2) γ_{X_0} and γ_{Y_0} and a morphism of sheaves $\gamma : v_0^*(\mathscr{I}_0/\mathscr{I}_0^2) \to \Omega_{Y_0}$ (1.3.5 (3)) that measures the *difference* between $\gamma_{X_0} \circ v_0$ and γ_{Y_0}. Moreover, and as v_0 has zero differential, the differential of v_0' comes from the map $\delta : v_0^*(\mathscr{I}_0/\mathscr{I}_0^2) \to \Omega_{Y_0}$ (3.3 (5)).

Lemma 4.1.1. *The maps $\gamma, \delta : v_0^*(\mathscr{I}_0/\mathscr{I}_0^2) \to \Omega_{Y_0}$ coincide.*

Indeed, suppose that $\omega_1, ..., \omega_d$ is a basis of sections of Ω_{A_1} and a a local section of $\mathscr{I}$ with image $\bar{a}_0$ in $\mathscr{I}_0/\mathscr{I}_0^2$ and let $da = \sum_i f_i \omega_i$ be the differential of a. Then according to (4) in 1.3.5, we have:

$$\gamma(v_0^*(\bar{a}_0)) = \sum_i (f_i \circ v_0)\omega_i|_{Y_0}$$

Moreover, $p_{A_1}^*(\omega_i) = p\omega_i$, thus $p_{A_1}^*(da) = p(\sum_i (f_i \circ p_{A_0})\omega_i)$ and consequently, using the notation of 3.3.1, $\psi(a) = \sum_i (f_i \circ p_{A_0})\omega_i|_{A_0}$. We deduce from 3.3.1 that:

$$\delta(v_0^*(\bar{a}_0)) = \sum_i (f_i \circ v_0)\omega_i|_{Y_0}$$

hence the lemma.

Let Y_0' be the scheme-theoretic image of Y_0 under v_0' and let $h_0' : Y_0' \to X_0$ denote the restriction of h_0 to Y_0'. As v_0 is finite, so is h_0'.

Proposition 4.1.2. *Suppose that $i_0 : X_0 \hookrightarrow A_0$ satisfies $(*)$ (1.1.2) and that the normalisation $\tilde{X}_0$ of X_0 has genus ≥ 2. Then the map $Y_0 \to Y_0'$ induced by v_0' is generically étale.*

Note first that the property $(*)$ guarantees that Y_0, and thus also Y_0' is integral (1.2.2). Moreover, according to 1.3.6, we can take a non-empty open set U_0 of X_0 above which X_0 and Y_0 are smooth and γ is surjective. By 4.1.1 v_0' is unramified over U_0. If we then restrict U_0 so that Y_0' is also smooth over this open set, then $Y_0 \to Y_0'$ is étale over U_0.

4.2. Let G_1 (resp. G_0) be the kernel of p_{A_1} (resp. p_{A_0}). Then G_0 is the product of its connected component $(G_0)_{\mathrm{inf}}$ and étale component $(G_0)_{\text{ét}}$. However, over R_1 we have only a short exact sequence of flat groups schemes:

$$0 \to (G_1)_{\mathrm{inf}} \to G_1 \to (G_1)_{\text{ét}} \to 0 \tag{1}$$

where $(G_1)_{\mathrm{inf}}$ lifts $(G_0)_{\mathrm{inf}}$ and $(G_1)_{\text{ét}}$ lifts $(G_0)_{\text{ét}}$.

Proposition 4.1.2 implies that the radicial degree of $h_0' : Y_0' \to X_0$ is equal to the radicial degree of $v_0 : Y_0 \to X_0$. Hence, according to 1.2.2:

Corollary 4.2.1. *With the hypotheses of 4.1.2, the radical degree of h_0' is p^s, where s is the smallest integer such that F^s annihilates $(G_0)_{\mathrm{inf}}$; in particular $s \geq 1$.*

Remark 4.2.2. What can we say about the separable degree of v_0'? Of course, it is bounded above by the separable degree of v_0 which is equal to the rank of $(G_0)_{\text{ét}}$. We can refine this upper bound by taking into account the lift A_1 of A_0. Indeed, there is a unique, maximal étale subgroup H of $(G_1)_{\text{ét}}$, above which the exact sequence (1) will split. We then choose an étale group subscheme H_1 of G_1 that lifts H and let B_1 be the quotient A_1/H_1. We then get the following factorisation of p_{A_1}:

$$A_1 \xrightarrow{w_1} B_1 \xrightarrow{u_1} A_1$$

We can apply the construction of section 3 to u_1 instead of p_{A_1}. We then deduce that if Z_0 is the reduced scheme-theoretic preimage of X_0 in B_0, the morphism $v_0' : Y_0 \to Y_0'$ factorises through Z_0. Thus, the separable degree of v_0' is at most the separable degree of $u_0 : B_0 \to A_0$ which is equal to the rank of $(G_1)_{\text{ét}}/H$.

Example 4.2.3. Suppose A_0 is an ordinary abelian variety. Then we have $H = (G_1)_{\text{ét}}$ if and only if the exact sequence (1) is split, i.e. A_1 is the *canonical lifting* of A_0 in the sense of Serre-Tate [8, §5]. In this case the degree of h_0' is equal to the radicial degree which is $p^s = p$.

4.3. Let X_1 be a flat curve over R_1 which lifts X_0 and let $i_1 : X_1 \hookrightarrow A_1$ be a closed immersion which extends i_0. i_1 then corresponds to a section i'_0 of $h_0 : V_0 \to X_0$ by 2.4.1, in particular, V_0 is now a principal homogenous space via the action of $\mathbb{V}((\mathscr{I}_0/\mathscr{I}_0^2)^\vee)$ (2.2.2) trivialised by i'_0. Note that h_0 induces an isomorphism $X'_0 \xrightarrow{\sim} X_0$ where X'_0 is the image of X_0 under i'_0.

Let $x \in pA_1(R_1) \cap X_1(R_1)$ and let $\tau(x) \in V_0(k)$ be the lift of x (2.2.2). Then $\tau(x) \in X'_0(k)$ and by (4.1), $\tau(x)$ is also in the image of v'_0, so is in $Y'_0(k)$. We then obtain the following commutative diagram:

$$\begin{tikzcd} pA_1(R_1) \cap X_1(R_1) \arrow[rr, "\tau"] \arrow[dr, "\text{can.}"'] & & X'_0(k) \cap Y'_0(k) \arrow[dl, hook', "h_0|_{X'_0(k)}"] \\ & X_0(k) & \end{tikzcd}$$

Lemma 4.3.1. *The image of $pA_1(R_1) \cap X_1(R_1)$ in $X_0(k)$ is contained in the image of $X'_0(k) \cap Y'_0(k)$ and they are equal over the smooth locus of X_0.*

The first statement is clear from the above diagram. Suppose $\sigma \in X'_0(k) \cap Y'_0(k)$ is a point of $V_0(k)$ which projects onto a smooth point $x_0 \in X_0$. We show that σ is the image of a point of $pA_1(R_1) \cap X_1(R_1)$ under τ. As $\sigma \in Y'_0(k)$, there exists a point $y_0 \in Y_0(k)$ such that $v'_0(y_0) = \sigma$. As A_1 is smooth over R_1 we can lift y_0 to $y_1 \in A_1(R_1)$ say. Then $x = py_1 = \bar{p}(y_0)$ is a point of $pA_1(R_1)$ that lifts x_0 and we have $\tau(x) = \sigma$. It suffices to show that $x \in X_1(R_1)$ as we know $\tau(x) \in X'_0(k)$. But we suppose that X_0 is smooth over k at x_0, therefore X_1 is smooth over R_1 near x_0 and locally the sheaf of ideals that defines X_1 in A_1 is given by a regular sequence $(t_1, ..., t_{d-1})$. The choice of t_i corresponds to coordinates $T_1, ..., T_{d-1}$ in the X_0-scheme V_0 such that a point $x \in A_1(R_1)$ sends t_i to pf_i, $i = 1, ..., d-1$, $f_i \in k$. Then its lift $\tau(x)$ is a point of V_0 given by $T_i = f_i$ (2.3.1). It follows that X'_0 is given by equations $T_i = 0, i = 1, ..., d-1$ in V_0. Therefore, $\tau(x) \in X'_0(k) \Leftrightarrow f_i = 0$, $i = 1, ...d-1 \Leftrightarrow x \in X_1(R_1)$.

4.4. Let $\tilde{Y}'_0$ be the normalisation of Y'_0 and $\tilde{h}'_0 : \tilde{Y}'_0 \to X_0$ the composition of the normalisation map and the projection h'_0. Let $\mathscr{M}_0$ be the locally free sheaf on $\tilde{Y}'_0$ given by the quotient of $\tilde{h}'^*_0(\mathscr{I}_0/\mathscr{I}_0^2)$ by its torsion subsheaf. For example, if X_0 is smooth, or more generally if X_0 is locally a complete intersection of A_0, then $\mathscr{M}_0 = \tilde{h}'^*_0(\mathscr{I}_0/\mathscr{I}_0^2)$. Lastly, let $\mathscr{M}_0^\vee$ be the dual of $\mathscr{M}_0$.

If $a \in A_1(R_1)$, we denote $X_1 + a$ for the curve given by the translation of X_1 by a. We can now demonstrate the essential part of the proof of Theorem II that was outlined in the introduction.

Theorem 4.4.1. *Suppose that $i_0 : X_0 \hookrightarrow A_0$ satisfies $(*)$ (1.1.2) and that the genus of the normalisation of X_0 is ≥ 2. Then, for all $a \in A_1(R_1)$, the image of $pA_1(R_1) \cap (X_1 + a)(R_1)$ in $(X_0 + a)(k)$ is finite, and is bounded above by the maximal degree μ_0 of the invertible subsheaves of $\mathscr{M}_0^\vee$.*

First we consider the case $a = 0$. Let E be the image of $pA_1(R_1) \cap (X_1)(R_1)$ in $X_0(k)$; we will prove that it is finite. If we identify X_0 with X'_0 via the projection h_0, the result of 4.3.1 shows that E is contained in $X'_0(k) \cap Y'_0(k)$ (and moreover they are equal if E lies over the smooth locus of X_0). It suffices to show that $X'_0 \cap Y'_0$ is finite, or equivalently that these integral curves are distinct. Indeed, X'_0 is of degree 1 over X_0, whereas the radicial degree of Y'_0 relative to X_0 is > 1 by 4.2.1.

This being said, let's use the section X'_0 of $h : V_0 \to X_0$ to identify the X_0-scheme V_0 with the vector bundle $\mathbb{V}((\mathscr{I}_0/\mathscr{I}_0^2)^\vee)$ (2.2.2). The immersion $Y'_0 \hookrightarrow V_0$ corresponds to a morphism of sheaves $h'^*_0(\mathscr{I}_0/\mathscr{I}_0^2) \to \mathscr{O}_{Y'_0}$ that is zero at precisely the points of $X'_0 \cap Y'_0$. As this set is finite, this morphism is non-zero and by pulling back to $\tilde{Y}'_0$, and passing to the quotient of $h'^*_0(\mathscr{I}_0/\mathscr{I}_0^2)$ by its torsion subsheaf, we get a non-zero morphism:

$$\epsilon : \mathscr{M}_0 \to \mathscr{O}_{\tilde{Y}'_0}$$

The dual map $\epsilon^\vee : \mathscr{O}_{\tilde{Y}'_0} \to \mathscr{M}_0^\vee$ is then injective and its image is the invertible subsheaf $\mathscr{O}_{\tilde{Y}'_0}(\Delta)$ of $\mathscr{M}_0^\vee$ where Δ is a positive divisor on $\tilde{Y}'_0$ with support on the preimage of $X'_0(k) \cap Y'_0(k)$; in particular the size of this intersection is bounded above by the degree of Δ, and so the size of E is bounded above by the maximum of the degrees of invertible sub sheaves of $\mathscr{M}_0^\vee$.

We now prove the more general case. An element a in $A_1(R_1)$ is of the form $pb + c$ where b and c are in $A_1(R_1)$ and c is in the kernel of the reduction map $A_1(R_1) \to A_0(k)$. If we replace X_1 by the translation $X_1 + pb$, E gets sent to $E + pb$. Note that the cardinality of these sets is the same. If now we replace X_1 by $X_1 + c$, V_0 and Y'_0 remain unchanged, only the section X'_0 of h_0 changes. In other words, using the previous notations, and replacing ϵ with $\epsilon + (h'_0)^*(\eta)$ for a particular morphism $\eta : \mathscr{I}_0/\mathscr{I}_0^2 \to \mathscr{O}_{X_0}$, we obtain the same upper bound as in the case $a = 0$.

Example 4.4.2. i) Suppose A_0 is an abelian surface. Then X_0 is locally a complete intersection and V_0 is smooth over X_0. Then the cardinality of $X'_0(k) \cap Y'_0(k)$ is bounded above by the intersection number $X'_0 \cdot Y'_0$ which is also equal to the degree of $\mathscr{M}_0^\vee$. The degree is equal to $p^{r+s}(X_0 \cdot X_0)$ where $X_0 \cdot X_0$ is the self-intersection of X_0 in A_0 and p^{r+s} is the degree of h'_0 which factors as the following:
- p^s is the radicial degree of h'_0 as in 4.2.1
- p^r is the maximal separable degree of h'_0 as in 4.2.2

As X_0 is non-elliptic then we have $(X_0 \cdot X_0) > 0$ and from 4.3.1 if X_0 is smooth, $X_1(R_1)$ always contains at least one point of $pA_1(R_1)$.

ii) Suppose A_0 has dimension ≥ 3 and that X_0 is smooth. Then if c is a point of $\mathrm{Ker}(A_1(R_1) \to A(k))$, then $(X_1 + c)(R_1)$ does not intersect $pA_1(R_1)$. In fact, we can identify $\mathrm{Ker}(A_1(R_1) \to A(k))$ with a Lie algebra L of A_0. For all $y \in V_0(k)$, the points c of L such that the section of $h_0 : V_0 \to X_0$ associated to $(X_1 + c)$ (cf. 2.4) passes through y, correspond to the points of an algebraic curve L_y in L. The union of the curves L_y over $y \in Y'_0(k)$ is a constructible set of L of dimension ≤ 2, therefore distinct from L and it suffices to choose c is in its complement.

Remark 4.4.3. Under the hypotheses of 4.4.1, $pA_1(R_1) \cap X_1(R_1)$ is finite and in fact the kernel of the map $pA_1(R_1) \to A_0(k)$ under reduction modulo p is finite (for example it is a quotient of the kernel of multiplication by p on $A_0(k)$).

5. Rational and Ramified Torsion (Local Case)

5.0. In this section, R is a complete discrete valuation ring with fraction field K of characteristic 0, and algebraically closed residue field k of characteristic $p > 0$. We assume that the valuation group of K is $\mathbb{Z}$ and let e denote the valuation of p (e is the absolute ramification index of R).

Let $\bar{K}$ be an algebraic closure of K and G the Galois group of $\bar{K}/K$.

5.1. Let A be an abelian R-scheme, A_K the generic fibre, A_0 the special fibre and T the torsion subgroup of $A(\bar{K})$, equipped with the natural action of G. We have $T = T_p \bigoplus T_{p'}$, where T_p is the p-primary torsion of T and $T_{p'}$ is coprime-to-p torsion. As A is an abelian R-scheme and k is algebraically closed, we have $T_{p'} \subseteq A(K) = A(R)$ and in particular, G acts trivially on $T_{p'}$.

5.2. Let A_{p^∞} be the p-divisible R-group constructed from the kernels of multiplication by powers of p on A. We have an exact sequence of p-divisible R-groups:

$$0 \to (A_{p^\infty})_{\mathrm{inf}} \to (A_{p^\infty}) \to (A_{p^\infty})_{\text{ét}} \to 0 \tag{1}$$

where $(A_{p^\infty})_{\mathrm{inf}}$ is the p-divisible group associated with formal completion of A along the zero section and $(A_{p^\infty})_{\text{ét}}$ is étale, isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^h$ where h is the p-rank of A_0.

The exact sequence (1) induces the following exact sequence on torsion points with values in $\bar{K}$ as G-modules:

$$(2) \qquad 0 \to T_{\inf} \to T_p \to (T_p)_{\text{ét}} \to 0$$

Let T'_p be the maximal divisible subgroup of $T_p(K)$.

Lemma 5.2.1. *Suppose that the ramification index e of R is $< p-1$. Then T'_p is a factor of the G-module T_p.*

In fact, as T'_p is unramified over R, the specialisation lemma of [6, §1, Prop. 1.1] implies $T'_p \cap (T_p)_{\inf} = 0$. Then the composition $T'_p \hookrightarrow T_p \to (T_p)_{\text{ét}}$ is injective and as T'_p is p-divisible the image is a factor of the trivial Galois module $(T_p)_{\text{ét}} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^h$. Let T_1 be the supplement of the image, then the preimage of T_1 in T_p is a supplement of T'_p; invariant under the Galois action.

From now on we assume $e < p-1$ and we choose a supplement T'' of T'_p in T_p, closed under the Galois action. Then, by construction, the torsion subgroup give a p-divisible subgroup A'' of A_{p^∞}. The following lemma shows the importance of the Galois action of G on $T''(\bar{K})$.

Lemma 5.2.2. *The cardinality of the orbits of G in $T''(\bar{K})$ tend to ∞ with the order of the elements of $T''(\bar{K})$ (i.e. $\forall N > 0$, there exists an integer $r > 0$ such that, if $x \in T''(\bar{K})$ has order $> p^r$, then the G-orbit of x has cardinality $> N$).*

In fact, let $M'' = \mathrm{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, T'')$ the Tate module associated to T''. It is a free $\mathbb{Z}_p$-module of finite rank, with a continuous G-action. Let M^* denote the open subset of M (with respect to the p-adic topology) formed of the elements whose image in M/pM is non-zero. An immediate compactness argument shows that the lemma is equivalent to the fact that G has no finite orbits in M^*. Now let M_1 be the largest $\mathbb{Z}_p$-submodule of M on which G acts through a finite group. We will show $M_1 = 0$. Then $T_1 = \varinjlim_n M_1/p^n M_1$ is a divisible subgroup of T', on which G acts by a finite group. It follows, for example by theorems of Tate [11, Cor. 1, p. 181] that $T_1 \cap (T_p)_{\inf}$ is finite. Then the composition $T_1 \to T_p \to (T_0)_{\text{ét}}$ has finite kernel. As G acts trivially on $(T_p)_{\text{ét}}$ and as T_1 is divisible, G acts trivially on T_1. Thus $T_1 = 0$, as can be seen through the maximal character of T'_p.

Example 5.2.3. i) If the p-rank h of A_0 is zero, then $T'_p = 0$, $T'' = T_p = T_{\inf}$.

ii) If A_0 is ordinary, then $T'_p = (T_p)_{\text{ét}}$ (and so $T'' = T_{\inf}$) if and only if A is the *canonical lift* of A_0 in the sense of Serre-Tate. On the other hand, if A is a more general lift of A_0, $T'_p = 0$ and $T'' = T_p$.

5.3. We have a (non-canonical) decomposition, compatible with G: $T = T' \bigoplus T''$ where $T' = T_{p'} \bigoplus T'_p$.

We say (abusively) that T' is the *rational* torsion of A and that T'' (defined for $e < p-1$) is the *ramified* torsion of A. The rational torsion has the following properties:

i) The action of G on T' is trivial and $T' \subseteq A(K) = A(R)$.

ii) T' is p-divisible.

iii) The specialisation map

$$T' \hookrightarrow A(K) \xrightarrow{\sim} A(R) \to A(k)$$

is injective (in fact we have $T' \cap T_{\inf} = T'_p \cap T_{\inf} = 0$).

6. Curves and Rational Torsion (Local Case)

6.0. We reuse the notations of 5.0 and 5.1. Moreover, in addition to an abelian R-scheme A, suppose we have an R-curve X that is flat and immersed in A via $i : X \hookrightarrow A$ and satisfies the following conditions:

i) The fibres of X are integral; the normalisation $\tilde{X}$ of X is smooth over R, with fibres of genus ≥ 2. In particular, the special fibre $\tilde{X}_0$ of $\tilde{X}$ is the normalisation of X_0. Let J be the Jacobian of $\tilde{X}$ and $a : J \to A$ the Albanese morphism associated to $\tilde{X} \to X \overset{i}{\hookrightarrow} A$.

ii) Suppose that a is surjective with kernel N smooth over R and the group of connected components of N: N/N_0 has order coprime to p.

Note that condition ii) depends only on the special fibre and so is equivalent to $i_0 : X_0 \hookrightarrow A_0$ satisfying $(*)$ as in 1.1.2. Moreover, when the ramification index e of R satisfies $e < p-1$, by a result in [6, §1, Prop. 1.2], condition ii) can also be tested on the generic fibre.

6.1. We start by proving a corollary of 4.4.1.

Corollary 6.1.1. *Suppose that R is unramified (i.e. $e = 1$) and the conditions of 6.0 are satisfied. Then, for all $a \in A(R) = A(K)$, the image of $(X + a)(R) \cap pA(R)$ in $(X_0 + a_0)(k)$ is finite and bounded above by μ_0 (4.4.1).*

Indeed, set $R_1 = R/p^2R$, $A_1 = A \times_R R_1$, $X_1 = X \times_R R_1$. Then the ring R_1 is of the type considered in 4.0 and we can apply Theorem 4.4.1 to A_1 and X_1. Then the image of $(X + a)(R) \cap pA(R)$ in $(X_0 + a_0)(k)$ is contained in the image of $(X_1 + a_1)(R_1) \cap pA_1(R_1)$, and the corollary follows.

Remark 6.1.2. In fact, for $e = 1$, it follows from the integrality properties of the logarithm and exponential relative to the formal completion of A along the unit section [7, Ch. III] that the elements of $\mathrm{Ker}(A(R) \to A_1(R_1))$ is contained in $pA(R)$. Then the image of $(X + a)(R) \cap pA(R)$ in $(X_0 + a_0)(k)$ is in fact equal to the image of $(X_1 + a_1)(R_1) \cap pA_1(R_1)$.

6.2. Let p_A denote multiplication by p on A, Y the proper, flat R-curve which is set wise equal to the preimage of X under p_A and $\tilde{Y}$ the normalisation of Y. We then see under the conditions of 6.0 that the special fibre $\tilde{Y}_0$ of $\tilde{Y}$ is irreducible.

Proposition 6.2.1. *Under the hypotheses of 6.1.1 $\tilde{Y}_0$ is not reduced (i.e. appears with multiplicity > 1).*

Let $x \in X(R) \cap pA(R)$. Then, apart from a finite number of points x that, after restricting to the generic fibre, pass through the singular points of X_K, the points of $pA(R) \cap X(R)$ are precisely the images of points of $\tilde{X}(R)$. Corollary 6.1.1 is thus equivalent to the fact that there are only a finite number of points of $\tilde{Y}_0(k)$ which lift to points of $\tilde{Y}(R)$. This condition is equivalent to the fact that $\tilde{Y}_0$ is not reduced; moreover, when $\tilde{Y}_0$ is not reduced, the only points of $\tilde{Y}_0$ which lift to points of $\tilde{Y}(R)$ are the points y of $\tilde{Y}_0$ which are singular in $\tilde{Y}$ (i.e. points such that $\mathscr{O}_{\tilde{Y},y}$ is not regular).

Remark 6.2.2. We could give a direct proof of 6.2.1, valid under the assumptions of 6.0 and the condition $e \leq p - 1$, then deduce 6.1.1. However, the approach presented is more elementary and gives a relatively explicit bound and lends itself better to replacing X by a translate. Nevertheless, it would be interesting to study the singularities of $\tilde{Y}$.

6.3. In 5.3 we introduced the rational torsion T' of A.

Theorem 6.3.1. *Under the hypotheses of 6.1.1, for all $a \in A(K)$, $T' \cap (X + a)(K)$ is finite and bounded by μ_0 (4.4.1).*

This follows immediately from 6.1.1 and from the fact that the points of T' are in $pA(R)$ and are determined by their reductions in $A_0(k)$ (5.3).

6.4. We will now consider $T' \cap (X + a)(\bar{K})$, for $a \in A(\bar{K}) \setminus A(K)$.

6.4.0. Note first that as X is non-elliptic, the subgroup scheme H_1 of A formed from translations that leave X fixed is finite. Let H be the closure in H_1 of its generic fibre. Then H is R-flat, with an action on X that extends to an action on $\tilde{X}$. As $\tilde{X}$ has fibres of genus ≥ 2, $\tilde{X}$ has no infinitesimal morphisms and therefore is étale. Let $Z \subseteq A \times A$ be the inverse image of X under the morphism:

$$A \times A \to A; \quad (a, b) \mapsto b - a$$

Consider $Z \cap (A \times X)$ as an A-scheme via the first projection. Then the fibre over a point $a \in A(\bar{K})$ is $X \cap (X + a)$. The morphism $Z \cap (A \times X) \to A$, induced by the first projection, is proper and therefore finite over $(A \backslash H)_K$. In particular, the cardinality of the fibres over $(A \backslash H)(\bar{K})$ are bounded, say by μ_1.

Example 6.4.1. If A is dimension 2 over R, we can take μ_1 to be the self-intersection $X_0 \cdot X_0$ of X_0 in A_0.

Proposition 6.4.2. *For all $a \in A(\bar{K}) \setminus A(K)$, $T' \cap (X + a)$ is finite, with cardinality $\leq \mu_1$.*

We note the following corollary of 6.3.1 and 6.4.2:

Corollary 6.4.3. *Under the assumptions of* 6.1.1*, for all $a \in A(\bar{K})$, $T' \cap (X + a)$ is finite with cardinality $\leq \mu = \max(\mu_0, \mu_1)$.*

Proof of 6.4.2. Let B be the quotient of A by the finite étale subgroup H (6.4.0) and let b be the image of a in $B(\bar{K})$. As H is étale, and R complete with algebraically closed residue field, the hypothesis $a \in A(\bar{K}) \backslash A(K)$, implies $b \in B(\bar{K}) \backslash B(K)$, and consequently, there exists $g \in \mathrm{Gal}(\bar{K}/K)$ such that $a^g - a \notin H$.

Moreover, the points of T' that are contained in $X + a$, being K-rational, are also contained in $X + a^g$ and therefore in $(X + a) \cap (X + a^g)(\bar{K})$. By translating by $-a$, this intersection is in bijection with $X \cap (X + a^g - a)(\bar{K})$ which is finite of cardinality $\leq \mu_1$, as $a^g - a \notin H$. ☐

7. Proof of Theorem I

7.0. Let c be an algebraically closed field of characteristic 0, A an abelian variety over c, X a non-elliptic, proper, integral curve and $i : X \hookrightarrow A$ an immersion; X and i defined over c. Let $T \subset A(c)$ be the torsion subgroup of $A(c)$. We claim that $X \cap T$ is finite.

7.1. Let $B \subset A$ be the abelian subvariety generated by the set of differences $(x - x')$, $(x, x' \in X(c))$. Then there exists $a \in A(c)$ such that X is contained in $B + a$. If the image of a in A/B is not torsion, $T \cap X = \emptyset$. Otherwise, by translating X by a torsion point, we can reduce to the case where $X \subset B$.

Suppose now that $B = A$. Let $\tilde{X}$ be the normalisation of X, J the Jacobian of $\tilde{X}$, $a : J \to A$ the Albanese morphism associated with the composition $\tilde{X} \to X \hookrightarrow A$, N the kernel, N^0 the connected component of the identity of N and h the order of N/N^0. The assumption $B = A$ is equivalent to the fact that a is surjective.

7.2. There exists a $\mathbb{Z}$-algebra of finite type E over c, such that X, A and $i : X \hookrightarrow A$ extend over $S = \mathrm{Spec}(E)$. By potentially restricting S to a non-empty open set, we can assume the following:

i) A is an abelian S-scheme
ii) X is a proper, flat S-curve, with geometrically integral fibres and $i : X \hookrightarrow A$ an immersion.
iii) The normalisation $\tilde{X}$ of X is a proper, smooth S-curve with geometric fibres of genus ≥ 2. Let J be the relative Jacobian of $\tilde{X}$ over S and $a : J \to A$ the Albanese morphism associated with the composition $\tilde{X} \to X \hookrightarrow A$. Then a is surjective and its kernel N is smooth over S (note that N is smooth over the generic point η of S which is in characteristic 0). Finally, if N^0 is the connected component of the identity of N then N/N^0 is finite étale of rank h.

7.3. Let s be a closed point of the fibre of S over $\mathbb{Q}$. Note that the number of torsion points contained in a geometric fibre of X can only increase by specialisation in characteristic 0, in particular when specialising from η to s. Even if it means changing the original curve, we can replace S by an open set of the closure of s in S. We therefore reduce to the case where S is a non-empty open set of the spectrum of the ring of integers of a number field L. Even it means restricting S, we can assume that in addition to the conditions of 7.2 we have:

iv) S is unramified over $\mathrm{Spec}(\mathbb{Z})$ and $2h$ is invertible in S.

If v is a finite place of S, with valuation ring E_v, and completion $\widehat{E_v}$, then v divides a prime p and if R denotes the completion of the maximal unramified extension of E_v, R is of the type considered in 5.0 with $e = 1$. If we abuse notation and denote again by X and A the preimages of X and A under $E \to R$, then X and A satisfy the conditions of 4.4.1.

Proposition 7.3.1. *Let l be a prime and T_l the l-primary component of the torsion of A_L. Then there exists an integer v_l having the following property: for any algebraically closed extension L' of L and for all $a \in A(L')$, $T_l \cap (X + a)(L')$ is finite and of cardinality $\leq v_l$.*

Indeed, choose a finite place v over E which divides some prime $p \neq l$. From this we obtain a local ring R and let $\bar{K}$ be the algebraic closure of its field of fractions. Then the l-primary component of the torsion T of $A(\bar{K})$ is contained in the p'-torsion $T_{p'}$, and a fortiori in the rational torsion $\mathcal{T}'$ relative to R (5.3). By 6.4.3, there exists v_l such that for all $a \in A(\bar{K})$, the cardinality of $T_l \cap (X + a)(\bar{K})$ is finite and bounded by v_l.

If now L' is an algebraically closed extension of L, even if it means enlarging L', we can assume $\bar{K} \subset L'$. Let $a \in A(L')$. Then a is in $A(S')$ where S' is the spectrum of a $\bar{K}$-algebra of finite type over L'. Let s' be a point of $S'(\bar{K})$. Then, by the previous specialisation argument, we can pass from the generic point of S', to the point s', and return to the case where $a \in A(\bar{K})$. Hence the proposition.

Remark 7.3.2. Proposition 7.3.1 can also be obtained directly from results of Bogomolov [1].

7.4. To complete the proof of Theorem I, we choose a finite place v of E, corresponding to a ring R. Suppose R has residue characteristic p; $\bar{K}$ is the algebraic closure of the field of fractions of K of R, and G the Galois group of $\bar{K}/K$.

As $e = 1$ and $p \neq 2$, we have $e < p - 1$ and we can decompose the torsion T of A_K into $T = T' \bigoplus T''$ (5.3), where T' is the rational torsion and T'' is the ramified torsion contained in the p-primary component of T. We recall the finiteness results already obtained:

i) There exists an integer μ, such that for all $a \in A(\bar{K})$, $T' \cap (X + a)(\bar{K})$ has cardinality $\leq \mu$ (6.4.3).

ii) There exists an integer v_p such that for all $a \in A(\bar{K})$, $T'' \cap (X + a)(\bar{K})$ has cardinality bounded by v_p (applying 7.3.1 with $l = p$).

Let $x \in T \cap (X + a)(\bar{K})$. We have $x = x' + x''$, with $x' \in T'(\bar{K})$ and $x'' \in T''(\bar{K})$.

Then x'' is a point of $T'' \cap (X - x)(\bar{K})$. As x' and X are defined over K and as T'' is stable under G, it follows that the orbit of x'' under G is contained in $T'' \cap (X - x')(\bar{K})$. Then by ii) above, this orbit has at most v_p elements. It then follows from 5.2.2 that the order of x'' is bounded, independently of x', i.e. there are only finitely many possibilities for the element x''.

Moreover, for a fixed x'', $x' \in T' \cap (X - x'')(\bar{K})$ therefore takes at most μ distinct values according to i) above. Overall, there are only many finitely many decompositions $x = x' + x''$.

8. The inductive system X_n

8.0. In this section, preliminary to the study of Lang's conjecture; L is a field of characteristic 0, A an abelian L-scheme and X a proper, geometrically integral, non-elliptic curve contained in A, defined over L. We denote by $\bar{L}$ an algebraic closure of L. We saw in 6.3 that only a finite subgroup

H of A acts on X by translation. If $B = A/H$ and if Y is the image of X in B, then Y is not fixed by any non-zero translation of B.

8.1. For an integer $n > 0$, let n_A denote the multiplication by n map on A, ${}_nA$ the kernel, X_n the image of X under n_A and S_n the singular locus of X_n. In particular, $X = X_1$ and S_1 is the singular locus of X. For $n|n'$, multiplication on A by n'/n induces a map $j_n^{n'} : X_n \to X_{n'}$, so that we obtain a filtered inductive system $(X_n, j_n^{n'})$ indexed by integers > 0, endowed with order relations given by divisibility.

Proposition 8.1.1. *Suppose that $H = 0$ (8.0). Then, for all $n > 0$, the morphism $X \to X_n$ induced by n_A is birational. In particular, if $x \in X(\bar{L})$ is such that $nx \in A(L)$, then, either $x \in X(L)$ or $nx \in S_n(L)$.*

Indeed, let Y_n be the preimage of X_n under n_A, so that $Y_n \to X_n$ is étale and X is an irreducible component of Y_n. To establish the first part, even if it means replacing L by $\bar{L}$ we can assume L to be algebraically closed. Then $Y_n \to X_n$ is an étale Galois covering with group ${}_nA(L)$; this group acts transitively on the irreducible components of Y_n and since $H = 0$, the stabiliser of the component X is 0, thus ${}_nA(L)$ also acts freely on the set of components. It follows that each component is of degree 1 over X, hence the first assertion; the second follows immediately.

Remark 8.1.2. The singularities of X_n are the images of the singularities of Y_n, thus consisting of, on one hand, the singularities S_1 of X and, on the other hand, the images in X of the points of Y_n that lie in multiple components.

We note the following corollary of Theorem I:

Corollary 8.1.3. *The fibres of the canonical map $X(\bar{L}) \to \varinjlim_n X_n(\bar{L})$ are finite.*

Indeed, let $x \in X(\bar{L})$; even if it means translating by $-nx$ on X_n, we may reduce to the case $x = 0$. Then the fibre of $X(\bar{L}) \to \varinjlim_n X_n(\bar{L})$ over 0 is the torsion lying on X, thus is finite by Theorem I.

8.2. Write R, K, $\bar{K}$, G as in (5.0) and let A and X be R-schemes satisfying the conditions of (6.0).

Proposition 8.2.1. *The set of $\bar{x} \in X(\bar{K}) \setminus X(K)$ for which there exists an integer $n > 0$ with $n\bar{x} \in A(K)$ is finite.*

Let H be the étale subgroup scheme (6.4.0) of A formed of translations under which X is stable and let Y be the image of X in $B = A/H$. Since H is étale and R is complete with algebraically closed residue field, a point of $A(\bar{K})$ has image in $B(K)$ if and only if it is a point of $A(K)$. We then replace X by Y and A by B, and to establish 8.2.1 we suppose $H = 0$.

Let $\bar{x} \in X(\bar{K}) \setminus X(K)$ such that $n\bar{x} \in A(K)$. Write $n = p^r m$ where $(m, p) = 1$. Since multiplication by m on A is étale, the previous argument shows that $p^r\bar{x} \in A(K)$ and we can restrict to the case where $n = p^r$.

We again take the exact sequence of p-divisible groups over R of 5.2 (1) and suppose for simplicity that $A'' = (A_{p^\infty})_{\mathrm{inf}}$, $A' = (A_{p^\infty})_{\text{ét}}$. Finally, let ${}_rA$, ${}_rA'$, ${}_rA''$ be the respective kernels of multiplication by p^r on A, A', A''. We then have an exact sequence of finite, flat group schemes over R:

$$0 \to {}_rA \to {}_rA' \to {}_rA'' \to 0;$$

so that, if $A^{(r)}$ is the abelian R-scheme quotient of A by ${}_rA''$, we have a factorisation of $(p^r)_A$: $A \xrightarrow{u_r} A^{(r)} \xrightarrow{v_r} A$. Since v_r is étale, then again $u_r(\bar{x}) \in A^{(r)}(K)$.

Then let v_p be an integer > 0 as in 7.4 ii) and let n_0 be an integer such that $p^{n_0} \geq v_p$. Denote by n_0' the smallest integer such that, if a'' is a torsion point of $A''(\bar{K})$ with order $> p^{n_0}$, then the orbit of a'' under G has cardinality $> v_p$ (5.2.2). Suppose $m = p^{n_0+n'_0}$. We then prove that $m\bar{x} \in A(K)$. Then, by 8.1.1, we will then have that $m\bar{x} \in S_m(K)$, which leaves only a finite number of possibilities for $\bar{x}$.

Note that the fibre of $u_r : A \to A^{(r)}$ over a rational point $u_r(\bar{x})$ is a K-torsor P_r under the group scheme ${}_rA''_K$, the generic fibre of ${}_rA''$. The point $\bar{x} \in P_r(\bar{K})$ has an image x in the scheme P_r. Let $K(x)$ be the residue field of x. From the definition of $v_{p_{n_1}}$, the degree h of $K(x)$ over K is $\le v_p$. We write $h = h_1 p$ where $(p, h_1) = 1$. We then have $n_1 \le n_0$ by the definition of n_0. It follows from [9, Prop. 6, p. 127] that the torsor P_r is trivialised by multiplication by h and thus by multiplication by p^{n_1} (since ${}_rA''(\bar{K})$ is a p-group), and by multiplication by p^{n_0}. We thus obtain a K-morphism from P_r to the trivial torsor ${}_rA''_K$. Let y be the image of x in ${}_rA''_K$. We have $[K(y) : K] \le [K(x) : K] \le v_p$. It then follows from the definition of n'_0 that y is a point of ${}_{n'_0}A''_K \cap {}_rA''_K$. Finally, the image of x under multiplication by $m = p^{n_0+n'_0}$ is indeed a rational point.

9. Around the conjecture of Serge Lang

9.0. In this section, we reuse the notation L, $\bar{L}$, A, X of 8.0. We denote by G the Galois group of $\bar{L}/L$. Let Γ be a subgroup of finite type of $A(L)$. We denote by $\bar{\Gamma}$ the subgroup of $A(\bar{L})$ of division points of Γ:

$$\bar{\Gamma} = \{x \in A(\bar{L}) \mid \exists n \ge 1 \text{ such that } nx \in \Gamma\}$$

We then have an exact sequence of groups with an action of G:

$$0 \to T(\bar{L}) \to \bar{\Gamma} \to V \to 0 \tag{1}$$

where $T(\bar{L})$ is the torsion subgroup of $A(\bar{L})$ and V is the $\mathbb{Q}$-vector space $\Gamma \otimes_{\mathbb{Z}} \mathbb{Q}$ on which G acts trivially.

We will study the finiteness properties of $\bar{\Gamma} \cap X(\bar{L})$ and of the subgroup of $\bar{\Gamma}$ generated by $\bar{\Gamma} \cap X(\bar{L})$. We first study the case where L is a local field, then the case where L is an extension of finite type over $\mathbb{Q}$.

9.1. Let R, K, $\bar{K}$, k be as in 5.0 and let A and X satisfy conditions i) and ii) of 6.0. Finally, let Γ be a subgroup of finite type of $A(K) = A(R)$ and $\bar{\Gamma} \subseteq A(\bar{K})$; the group of division points of Γ. We denote by Γ' the subgroup of $\bar{\Gamma}$ generated by $\bar{\Gamma} \cap X(\bar{K})$, $\Gamma'(K) = \Gamma' \cap A(K)$ and $\tilde{\Gamma}$ the subgroup of $A(K)$ generated by $\bar{\Gamma} \cap X(K)$. We then have the inclusions:

$$\tilde{\Gamma} \subseteq \Gamma'(K) \subseteq \Gamma'$$

Theorem 9.1.1. *Under the hypotheses above, we have the following finiteness properties:*

i) The group $\Gamma/\tilde{\Gamma}$ is of finite type.
ii) The image of $\bar{\Gamma} \cap X(K) = \bar{\Gamma} \cap X(R)$ in $X(k)$ is finite and the image of $\Gamma'(K)$ in $A(k)$ is a group of finite type.
iii) The torsion subgroup of Γ' is finite.

Proof of i). The group $\Gamma'/\tilde{\Gamma}$ is generated by the image of $\bar{\Gamma} \cap (X(\bar{K}) \setminus X(K))$, which is a finite set by 8.2.1 thus $\Gamma'/\tilde{\Gamma}$ is of finite type. ☐

To establish ii), consider $\bar{\Gamma}(K) = \bar{\Gamma} \cap A(K)$.

Lemma 9.1.2. *The group $\bar{\Gamma}/p\bar{\Gamma}(K)$ is finite.*

Indeed, we have the exact sequence (1) of 9.0:

$$0 \to T(\bar{K}) \to \bar{\Gamma} \to V \to 0$$

Taking the invariant subgroups under the Galois group of $\bar{K}/K$, we obtain the exact sequence:

$$0 \to T(K) \to \bar{\Gamma}(K) \to W \to 0$$

where W is the image of $\bar{\Gamma}(K)$ in V.

To establish the lemma, it suffices to show that $T(K)/pT(K)$ and W/pW are finite. But W is a subgroup of V, finite dimensional over $\mathbb{Q}$, thus W/pW is finite. Moreover, $T(K)$, the group of torsion points of $A(K)$, is the direct sum of a finite group and a p-divisible group (denoted by T' in 5.3), thus $T(K)/pT(K)$ is finite.

Let then γ_i, $i \in I$, be a finite family of representatives in $\bar{\Gamma}(K)$ of $\bar{\Gamma}(K)/p\bar{\Gamma}(K)$. Denote by X_i the curve $X - \gamma_i$ the translation of X by $-\gamma_i$. Then, for each element of $\bar{\Gamma}(K)$ write $\gamma = \gamma_i + pa$, for a suitable choice of i and $a \in A(K)$. If moreover γ is in $X(K)$, $pa = \gamma - \gamma_i$ is in $X_i(K) \cap pA(K) = X_i(R) \cap pA(R)$. By 6.1.1, the image of $X_i(R) \cap pA(R)$ in $X_i(K)$ is finite, thus the image of $\bar{\Gamma}(K) \cap X(K)$ in $X(k)$ is finite. Since $\bar{\Gamma}(K) \cap X(K) = \bar{\Gamma} \cap X(K)$, we have established the first part of ii). Since $\bar{\Gamma} \cap X(K)$ is generated by the group $\tilde{\Gamma}$ by definition, we then deduce that the image of $\tilde{\Gamma}$ in $A(k)$ is a group of finite type. Moreover, it follows from i) that $\Gamma'(K)/\tilde{\Gamma}$ is a group of finite type. Combining these results, we then deduce that the image of $\Gamma'(K)$ in $A(k)$ is of finite type, hence ii).

Proof of iii). Taking into account i), it suffices to show that the torsion subgroup of $\bar{\Gamma}(K)$ is finite. But, the specialisation map $A(R) \to A(k)$, restricted to torsion points, has a finite kernel (and even is injective if $p \neq 2$), thus iii) follows form ii). □

Remark 9.1.3. i) Considering the integral closure $\bar{R}$ of R in $\bar{K}$ which is a valuation ring (non-discrete) with residue field k, we define a specialisation map $A(\bar{K}) \xrightarrow{\sim} A(\bar{R}) \to A(k)$. It then follows from assertions i) and ii) of 9.1.1 that the image of $\bar{\Gamma}$ in $A(k)$ is a group of finite type, and it follows from the proof of 9.1.1 that the image of $\bar{\Gamma} \cap X(\bar{K})$ in $X(k)$ is finite.

ii) Under the hypotheses of 9.1, suppose that the restriction of the specialisation map $A(K) \to A(k)$ to Γ is injective, then 9.1.1 ii) implies that $\Gamma \cap X(K)$ is finite. Let us point out, without proof, that this remark leads to a new proof of the Mordell conjecture over function fields of characteristic 0.

9.2.

Theorem 9.2.1. *We take the hypotheses of* 9.0 *and suppose further that L is of finite type over $\mathbb{Q}$, so that $M = A(L)$ is a group of finite type. Let H be the finite subgroup scheme of A formed by the translations under which X is stable* (6.3) *and set $B = A/H$, $Y = A/H$, $N = B(L)$. Then:*

i) The subgroup of $\bar{M}$ generated by $\bar{M} \cap X(\bar{L})$ is of finite type.
ii) $\bar{N} \cap (Y(\bar{L}) \setminus Y(L))$ is finite.
iii) $\bar{M} \cap X(\bar{L})$ is finite if and only if $Y(L)$ is finite, that is to say if and only if the curve Y satisfies the Mordell conjecture over the field L.
iv) The inductive system $\varinjlim_n S_n(L)$ of (8.1) *is stationary.*

Note that assertion iii) shows that the conjecture of Serge Lang [5] follows from the Mordell conjecture for curves. Specifically, we have the following result:

Corollary 9.2.2. *Let c be an algebraically closed field of charcteristic* > 0, *A an abelian variety over c, X a non-elliptic, proper, integral curve in A, Y the curve X/H where H is defined as in* 9.2.1. *Let Γ be a subgroup of finite type of $A(c)$ and let L be a subgrield of c, finite type over $\mathbb{Q}$, such that A and Y are defined over L and that $\Gamma \subseteq A(L)$. Then if $Y(L)$ is finite, $\bar{\Gamma} \cap X(c)$ is finite.*

We prove the main assertion i) of 9.2.1. Let M' be the subgroup of $\bar{M}$ generated by $\bar{M} \cap X(\bar{L})$. Note that M' is unchanged if we replace L by any finite extension. We can thus suppose that $X(L) \neq \emptyset$. Replacing A by an abelian subvariety, we can suppose that A is generated by the differences of points of X.

Let E be a $\mathbb{Z}$-algebra of finite type, contained in L, with field of fractions L and let $S = \mathrm{Spec}(E)$. Even if it means replacing S by a non-empty open subset, we can assume that X and A extend to S-schemes (denoted again by A and X) that satisfies conditions i), ii) and iii) of 7.2. On the other hand, we can no longer reduce to the case where L is a number field. If we restrict S, we can suppose that the following condition holds:

(iv)' S is smooth over $\mathrm{Spec}(\mathbb{Z})$ and $2h$ (or h as in 7.1) is invertible in S.

The image of S in $\mathrm{Spec}(\mathbb{Z})$ is a non-empty open set. Let then $p \in \mathrm{Spec}(\mathbb{Z})$ be a prime in the image of S and let η be the generic point of the fibre of S over p. Condition (iv)' implies that the local ring $\mathscr{O}_{S,\eta}$ of S at η is a discrete valuation ring, the maximal ideal of which is generated by p. By [3, Ch. III, 10.3.1], we can extend $\mathscr{O}_{S,\eta}$ to a discrete valuation ring R, so that the maximal ideal of R is again generated by p and the residue field k of R is an algebraic closure of the residue field of $\mathscr{O}_{S,\eta}$.

Suppose further that R is complete, then R is of the type considered in 5.0 and the field of fractions K of R is an extension of L. Moreover, the preimages of A and X under the base change $\mathrm{Spec}(R) \to S$ satisfy the conditions i) and ii) of 6.0.

We can then apply 9.1.1 and take Γ to be the group $A(L) \subset A(K)$. The group denoted by Γ' in 9.1.1 is then equal to the group M'. Then by 9.1.1 iii), M' is a torsion subgroup that is finite.

Let n be an integer ≥ 1 that annihilates the torsion of M'. It follows, for example by the exact sequence (1) of 9.0 with $\Gamma = A(L)$, that nM' is identified with a subgroup of $A(L)$, thus is of finite type and consequently M' is of finite type.

We now prove assertion ii) of 9.2.1. Assertion i) applied to the curve Y in B shows that the subgroup N' of $\bar{N}$ generated by $\bar{N} \cap Y(\bar{L})$ is of finite type. Let n be an integer ≥ 1 that annihilates the torsion of N'. As above we see that $nN' \subseteq B(L)$, thus if $y \in Y(\bar{L}) \cap \bar{N}$, $ny \in B(L)$. Since the curve Y is not stable under any non-zero translations of B, it follows from 8.1.1 that $(Y(\bar{L}) \setminus Y(L)) \cap \bar{N}$ is finite, hence ii).

Proof of iii). If $\bar{M} \cap X(\bar{L})$ is finite, it is clear that $Y(L)$ is finite. Conversely, if $Y(L)$ is finite, it follows from ii) that $\bar{N} \cap Y(\bar{L})$ is finite, thus $\bar{M} \cap X(\bar{L})$ (which is contained in the preimage of $\bar{N} \cap Y(\bar{L})$ under the projection $A(\bar{L}) \to B(\bar{L})$) is also finite. □

Proof of iv). To analyse the inductive system $\varinjlim_n S_n(L)$, we can restrict ourselves to integers n that are multiples of the order of the finite group $H(\bar{L})$, which allows us to replace X by Y and thus we suppose $H = 0$.

Let $S_\infty(L) = \varinjlim_n S_n(L)$. By 8.1.3, to see that the inductive system $S_n(L)$ is stationary, it suffices to show that $S_\infty(L)$ is finite. Note that a point of $S_\infty(L)$ belongs to at least one of the three sets:

a) The image of $\bar{M} \cap (X(\bar{L}) \setminus X(L))$, which is a finite set by 9.2.1 ii) and the fact that $H = 0$.

b) The image of $S_1(L)$ which is clearly finite.

c) The set of images of points $x_n \in S_n(L)$, $n > 1$, such that the fibre of $X \to X_n$ over x_n contains the rational points x and x', with $x - x'$ of exact order n. Since the torsion group of $A(L)$ is finite, only a finite number of integers n arise, thus the latter type concerns only a finite number of points of $S_\infty(L)$.

These considerations imply that $S_\infty(L)$ is finite and complete the proof of 9.2.1.

□

References

[1] Fedor Bogomolov. Sur l'algébricité des représentations l-adiques. *Comptes Rendus de l'Académie des Sciences Ser. A-B*, 290(15):A701–A703, 1980.

[2] Nicolas Bourbaki. *Commutative algebra: chapters 1-7*, volume 1. Springer Science & Business Media, 1998.

[3] Jean Alexandre Dieudonne and Alexandre Grothendieck. *Éléments de géométrie algébrique*, volume 166. Springer Berlin Heidelberg New York, 1971.
[4] Alexander Grothendieck. Techniques de construction et théoremes d'existence en géométrie algébrique. iv. les schémas de hilbert. *Séminaire Bourbaki*, 6(221):249–276, 1960.
[5] Serge Lang. Division points on curves. *Annali di Matematica Pura ed Applicata*, 70:229–234, 1965.
[6] Barry Mazur and Dorian Goldfeld. Rational isogenies of prime degree. *Inventiones mathematicae*, 44:129–162, 1978.
[7] William Messing. The crystals associated to barsotti-tate groups. *The crystals associated to Barsotti-Tate groups: with applications to abelian schemes*, pages 112–149, 2006.
[8] Jean-Pierre Serre. Groupes p-divisibles. *Séminaire Bourbaki*, 67, 1966.
[9] Jean Pierre Serre. Corps locaux. *(No Title)*, 1968.
[10] A SGA. Grothendieck, revêtements étales et groupe fondamental. *Séminaire de géométrie algébrique du Bois Marie*, 1961, 1960.
[11] John T Tate. p-divisible groups. In *Proceedings of a Conference on Local Fields: NUFFIC Summer School held at Driebergen (The Netherlands) in 1966*, pages 158–183. Springer, 1967.