Algebra & Number Theory

Volume 7
2013
No. 8

On the Manin–Mumford and Mordell–Lang conjectures in positive characteristic

Damian Rössler

msp

ALGEBRA AND NUMBER THEORY 7:8 (2013)
dx.doi.org/10.2140/ant.2013.7.2039

On the Manin–Mumford and Mordell–Lang conjectures in positive characteristic

Damian Rössler

We prove that in positive characteristic, the Manin–Mumford conjecture implies the Mordell–Lang conjecture in the situation where the ambient variety is an abelian variety defined over the function field of a smooth curve over a finite field and the relevant group is a finitely generated group. In particular, in the setting of the last sentence, we provide a proof of the Mordell–Lang conjecture that does not depend on tools coming from model theory.

1. Introduction

Let B be a semiabelian variety over an algebraically closed field F of characteristic $p > 0$. Let Y be an irreducible reduced closed subscheme of B. Let $\Lambda \subseteq B(F)$ be a subgroup. Suppose that $\Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ is a finitely generated $\mathbb{Z}_{(p)}$-module (here, as is customary, we write $\mathbb{Z}_{(p)}$ for the localization of $\mathbb{Z}$ at the prime p).

Let $C := \mathrm{Stab}(Y)^{\mathrm{red}}$, where $\mathrm{Stab}(Y) = \mathrm{Stab}_B(Y)$ is the translation stabilizer of Y. This is the closed subgroup scheme of B that is characterized uniquely by the fact that for any scheme S and any morphism $b : S \to B$, translation by b on the product $B \times_F S$ maps the subscheme $Y \times S$ to itself if and only if b factors through $\mathrm{Stab}_B(Y)$. Its existence is proven in [Grothendieck et al. 1970b, Exposé VIII, Exemples 6.5(e)].

The Mordell–Lang conjecture for Y and B is now the following statement:

Theorem 1.1 (Mordell–Lang conjecture [Hrushovski 1996]). *If $Y \cap \Lambda$ is Zariski dense in Y, then there are*

- *a semiabelian variety B' over F,*
- *a homomorphism with finite kernel $h : B' \to B/C$,*
- *a model $\mathbf{B}'$ of B' over a finite subfield $\mathbb{F}_{p^r} \subset F$,*
- *an irreducible reduced closed subscheme $\mathbf{Y}' \hookrightarrow \mathbf{B}'$, and*
- *a point $b \in (B/C)(F)$ such that $Y/C = b + h_*(\mathbf{Y}' \times_{\mathbb{F}_{p^r}} F)$.*

MSC2010: primary 14G05; secondary 14K12, 14G17.
Keywords: function fields, rational points, positive characteristic, Manin–Mumford, Mordell–Lang.

Here $h_*(\mathbf{Y}' \times_{\mathbb{F}_{p^r}} F)$ refers to the scheme-theoretic image of $\mathbf{Y}' \times_{\mathbb{F}_{p^r}} F$ by h. Since h is finite and $\mathbf{Y}' \times_{\mathbb{F}_{p^r}} F$ is reduced, this implies that $h_*(\mathbf{Y}' \times_{\mathbb{F}_{p^r}} F)$ is simply the set-theoretic image of $\mathbf{Y}' \times_{\mathbb{F}_{p^r}} F$ by h endowed with its reduced-induced scheme structure.

Theorem 1.1 in particular implies the following result, which will perhaps seem more striking on first reading. Suppose that there are no nontrivial homomorphisms from B to a semiabelian variety that has a model over a finite field. Then if $Y \cap \Lambda$ is Zariski dense in Y, then Y is the translate of an abelian subvariety of B.

Theorem 1.1 was first proven in 1996 by Hrushovski using deep results from model theory, in particular the Hrushovski–Zilber theory of Zariski geometries (see [Hrushovski and Zilber 1996]). An algebraic proof of Theorem 1.1 in the situation where B is an ordinary abelian variety was given by Abramovich and Voloch [1992]. In the situation where Y is a smooth curve embedded into B as its Jacobian, the theorem was known to be true much earlier. See for instance [Samuel 1966; Szpiro et al. 1981]. The earlier proofs for curves relied on the use of heights, which do not appear in the later approach of Voloch and Hrushovski, which is parallel and inspired by Buium's approach in characteristic 0 via differential equations (see below).

The *Manin–Mumford conjecture* has exactly the same form as the Mordell–Lang conjecture, but Λ is replaced by the group $\mathrm{Tor}(B(F))$ of points of finite order of $B(F)$. For the record, we state it in full.

Theorem 1.2 (Manin–Mumford conjecture [Pink and Rössler 2004]). *Suppose $Y \cap \mathrm{Tor}(B(F))$ is Zariski dense in Y. Then there are*

- *a semiabelian variety B' over F,*
- *a homomorphism with finite kernel $h : B' \to B/C$,*
- *a model $\mathbf{B}'$ of B' over a finite subfield $\mathbb{F}_{p^r} \subset F$,*
- *an irreducible reduced closed subscheme $\mathbf{Y}' \hookrightarrow \mathbf{B}'$, and*
- *a point $b \in (B/C)(F)$ such that $Y/C = b + h_*(\mathbf{Y}' \times_{\mathbb{F}_{p^r}} F)$.*

See also [Scanlon 2005] for a model-theoretic proof of the Manin–Mumford conjecture.

Remark (Important). Notice that the Manin–Mumford conjecture is *not* a special case of the Mordell–Lang conjecture because $\mathrm{Tor}(A(F))$ is not in general a finitely generated $\mathbb{Z}_{(p)}$-module (because $\mathrm{Tor}(A(F))[p^\infty]$ is not finite in general). Nevertheless, it seems reasonable to conjecture that Theorem 1.1 should still be true when the hypothesis that $\Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ is finitely generated is replaced by the weaker hypothesis that $\Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$ is finitely generated. This last statement, which is still not proven in general, is often called the *full Mordell–Lang conjecture*, and it would have Theorems 1.1 and 1.2 as special cases. See [Ghioca and Moosa 2006] for more about this.

Now suppose that the group Λ is actually finitely generated and that B arises by base-change to F from an abelian variety B_0, which is defined over a function field of transcendence degree 1 over a finite field. The main result of this text is then the proof of the fact that the Manin–Mumford conjecture in general implies the Mordell–Lang conjecture in this situation. We follow here the lead of A. Pillay, who suggested in a talk he gave in Paris on December 17, 2010 that it should be possible to establish this logical link without proving the Mordell–Lang conjecture first. See Theorem 1.3 and its corollary below for a precise statement.

The interest of an algebraic-geometric (in contrast with model-theoretic) proof of the implication Manin–Mumford $\Longrightarrow$ Mordell–Lang is that it provides in particular an algebraic-geometric proof of the Mordell–Lang conjecture.

Let K_0 be the function field of a smooth curve over $\overline{\mathbb{F}}_p$. Let A be an abelian variety over K_0, and let $X \hookrightarrow A$ be a closed integral subscheme. We shall write $+$ for the group law on A.

Let $\Gamma \subseteq A(K_0)$ be a finitely generated subgroup.

Theorem 1.3. *Suppose that for any field extension $L_0|K_0$ and any $Q \in A(L_0)$, the set $X_{L_0}^{+Q} \cap \mathrm{Tor}(A(L_0))$ is not Zariski dense in $X_{L_0}^{+Q}$. Then $X \cap \Gamma$ is not Zariski dense in X.*

Here $X_{L_0}^{+Q}$ stands for the scheme-theoretic image of X_{L_0} under the morphism $+Q : A_{L_0} \to A_{L_0}$.

Corollary 1.4. *Suppose that $X \cap \Gamma$ is Zariski dense in X. Then the conclusion of the Mordell–Lang conjecture* (*Theorem 1.1*) *holds for $F = \overline{K}_0$, $B = A_{\overline{K}_0}$, and $Y = X_{\overline{K}_0}$.*

In an upcoming article, which builds on the present one, Corpet [2012] shows that Theorem 1.3 (and thus its corollary) can be generalized; more specifically, he shows that the hypothesis that K_0 is of transcendence degree 1 can be dropped, that the hypothesis that Γ is finitely generated can be weakened to the hypothesis that $\Gamma \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ is a finitely generated $\mathbb{Z}_{(p)}$-module, and finally that it can be assumed that A is only semiabelian. In particular, he gives a new proof of Theorem 1.1.

In the present article, we deliberately focus on the situation of an abelian variety and a finitely generated group (which is probably the most important situation) in order to avoid some technical issues, which we feel would obscure the structure of the proof.

The structure of the article is the following. Section 2 contains some general results on the geometry of relative jet schemes (or spaces), which are probably known to many specialists but for which there doesn't seem to be a coherent set of references in the literature. The jet spaces considered in [Moosa and Scanlon 2010] do not seem to suffice for our purposes because they are defined in an absolute situation, and the jet spaces considered in [Buium 1992] are only defined in characteristic 0 (although this is probably not an essential restriction); furthermore, the latter are defined in Buium's language of differential schemes whereas our definition has the philological advantage of being based on the older notion of Weil restriction. Section 2A contains the definition of jet schemes and a description of the various torsor structures on the latter. Section 2B contains a short discussion on the structure of the jet schemes of smooth commutative group schemes and various natural maps that are associated with them. In Section 3, we use jet schemes to construct some natural schemes in the geometrical context of the Mordell–Lang conjecture. These "critical schemes" are devised to "catch rational points"; we then proceed to show that these schemes must be of small dimension. This is deduced from a general result on the sparsity of points over finite fields that are liftable to highly p-divisible unramified points. This last result is proved in Section 4. Once we know that the critical schemes are small, it is but a small step to the proofs of Theorem 1.3 and Corollary 1.4. The terminology of the introduction is used in Sections 2 and 3, but Section 4 has its own terminology and is also technically independent of the rest of the text. A reader who would only be interested in its main result (i.e., Theorem 4.1) can skip to Section 4 directly.

The use that we make of jet schemes in this note is in many ways similar to the use that Buium [1992] makes of them in his article on the geometric Mordell–Lang conjecture in characteristic 0. In the article [Buium and Voloch 1996], where some of Buium's techniques are adapted to the context of positive characteristic, the authors give a proof of the Mordell conjecture for curves over function fields in positive characteristic, which has exactly the same structure as ours if one leaves out the proof of the result on the sparsity of liftable points mentioned above.

For more detailed explanations on this connection, see Remarks 4.8 and 4.9 at the end of the text.

2. Preliminaries

We first recall the definition and existence theorem for the Weil restriction functor. Let T be a scheme, and let $T' \to T$ be a morphism. Let Z be a scheme over T'. The Weil restriction $\mathfrak{R}_{T'/T}(Z)$ (if it exists) is a T-scheme that represents the functor $W/T \mapsto \mathrm{Hom}_{T'}(W \times_T T', Z)$. It is shown in [Bosch et al. 1990, Section 7.6] that $\mathfrak{R}_{T'/T}(Z)$ exists if T' is finite, flat, and locally of finite presentation over T. The Weil restriction is naturally functorial in Z and sends closed immersions to closed immersions. The same permanence property is satisfied for smooth and étale morphisms. Finally notice that the definition of the Weil restriction implies that there is a natural isomorphism $\mathfrak{R}_{T'/T}(Z)_{T_1} \simeq \mathfrak{R}_{T'_{T_1}/T_1}(Z_{T'_{T_1}})$ for any scheme T_1 over T (in words, Weil restriction is invariant under base-change on T). See [Bosch et al. 1990, Chapter 7.6] for all this.

2A. ***Jet schemes.*** Let k_0 be a field, let U be a smooth scheme over k_0, and let $\Delta : U \to U \times_{k_0} U$ be the diagonal immersion. Let $I_\Delta \subseteq \mathcal{O}_{U\times_{k_0}U}$ be the ideal sheaf of $\Delta_* U$. For all $n \in \mathbb{N}$, we let $U_n := \mathcal{O}_{U\times_{k_0}U}/I_\Delta^{n+1}$ be the n-th infinitesimal neighborhood of the diagonal in $U \times_{k_0} U$.

Write $\pi_1, \pi_2 : U \times_{k_0} U \to U$ for the first and second projection morphisms, respectively. Write $\pi_1^{U_n}, \pi_2^{U_n} : U_n \to U$ for the induced morphisms. We view U_n as a U-scheme via the *first* projection $\pi_1^{U_n}$.

We write $i_{m,n} : U_m \hookrightarrow U_n$ for the natural inclusion morphism.

Lemma 2.1. *The U-scheme U_n is flat and finite.*

Proof. As a U-scheme, U_n is finite because it is quasifinite and proper over U since $U_n^{\mathrm{red}} = \Delta_*(U)$. So we only have to prove that it is flat over U. For this purpose, we may view U_n as a coherent sheaf of $\mathcal{O}_U$-algebras (via the second projection).

Let $I := I_\Delta$. For any $n \geqslant 0$, there are exact sequences of $\mathcal{O}_{U_{n+1}}$-modules (and hence $\mathcal{O}_U$-modules)

$$0 \to I^{n+1}/I^{n+2} \to \mathcal{O}_{U_{n+1}} \to \mathcal{O}_{U_n} \to 0.$$

Furthermore, I^{n+1}/I^{n+2} is naturally a $\mathcal{O}_{U_0}$-module and isomorphic to $\mathrm{Sym}^{n+1}_{\mathcal{O}_{U_1}}(I/I^2)$ as a $\mathcal{O}_{U_0}$-module because I is locally generated by a regular sequence in $U \times_{k_0} U$ (U being smooth over k_0). See [Matsumura 1989, Chapters 6 and 16] for this. Hence, I^{n+1}/I^{n+2} is locally free as a $\mathcal{O}_U$-module. Since $U_0 = \Delta_*(U)$ is locally free as a $\mathcal{O}_U$-module, we may apply induction on n to prove that $\mathcal{O}_{U_n}$ is locally free, which is the claim. □

Let W/U be a scheme over U.

Definition 2.2. The n-th jet scheme $J^n(W/U)$ of W over U is the U-scheme $\mathfrak{R}_{U_n/U}(\pi_2^{U_n,*}W)$.

By $\pi_2^{U_n,*}W$ we mean the base-change of W to U_n via the morphism $\pi_2^{U_n} : U_n \to U$ described above.

If W_1 is another scheme over U and $W \to W_1$ is a morphism of U-schemes, then the induced morphism $\pi_2^{U_n,*}W \to \pi_2^{U_n,*}W_1$ over U_n leads to a morphism of jet schemes $J^n(W/U) \to J^n(W_1/U)$ over U so that the construction of jet schemes is covariantly functorial in W.

Notice that the permanence properties of Weil restrictions show that if the morphism $W \to W_1$ is a closed immersion, then the morphism $J^n(W/U) \to J^n(W_1/U)$ is too. The same is true for smooth and étale morphisms.

To understand the nature of jet schemes better, let $u \in U$ be a closed point. Suppose until the end of this paragraph that k_0 is algebraically closed. View u as a closed reduced subscheme of U. Let u_n be the n-th infinitesimal neighborhood of u in U. From the definitions, we infer that there are canonical bijections

$$\begin{aligned} J^n(W/U)(u) &= J^n(W/U)_u(k_0) = \mathrm{Hom}_{U_n}(u \times_U U_n, \pi_2^{U_n,*} W) \\ &= \mathrm{Hom}_{U_n}(u_n, W_{u_n}) = \mathrm{Hom}_{u_n}(u_n, W_{u_n}) = W(u_n). \end{aligned} \tag{1}$$

In words, (1) says the set of geometric points of the fiber of $J^n(W/U)$ over u corresponds to the set of sections of W over the n-th infinitesimal neighborhood of u; the scheme $J^n(W/U)_u$ is often called the scheme of arcs of order n at u in the literature [Moosa and Scanlon 2010, Example 2.5].

The family of U-morphisms $i_{m,n} : U_m \to U_n$ induce U-morphisms

$$\Lambda^W_{n,m} : J^n(W/U) \to J^m(W/U)$$

for any $m \leqslant n$. These morphisms will be studied in detail in the proof of the next lemma.

Lemma 2.3. *Suppose that W is a smooth U-scheme. For all $n \geqslant 1$, the morphism*

$$\mathfrak{R}_{U_n/U}(\pi_2^{U_n,*} W) \to \mathfrak{R}_{U_{n-1}/U}(\pi_2^{U_{n-1},*} W)$$

makes $\mathfrak{R}_{U_n/U}(\pi_2^{U_n,*} W)$ into a $\mathfrak{R}_{U_{n-1}/U}(\pi_2^{U_{n-1},*} W)$-torsor under the vector bundle $\Lambda^{W,*}_{n,0}(\Omega^\vee_{W/U}) \otimes \mathrm{Sym}^n(\Omega_{U/k_0})$.

Proof. Let $T \to U$ be an affine U-scheme. By definition,

$$\begin{aligned} \mathfrak{R}_{U_n/U}(\pi_2^{U_n,*} W)(T) &\simeq \mathrm{Hom}_{U_n}(T \times_U U_n, \pi_2^{U_n,*} W), \\ \mathfrak{R}_{U_{n-1}/U}(\pi_2^{U_{n-1},*} W)(T) &\simeq \mathrm{Hom}_{U_{n-1}}(T \times_U U_{n-1}, \pi_2^{U_{n-1},*} W). \end{aligned}$$

Now the immersion $U_{n-1} \hookrightarrow U_n$ gives rise to a natural restriction map

$$\mathrm{Hom}_{U_n}(T \times_U U_n, \pi_2^{U_n,*} W) \to \mathrm{Hom}_{U_{n-1}}(T \times_U U_{n-1}, \pi_2^{U_{n-1},*} W). \tag{2}$$

This is the functorial description of the morphism

$$\mathfrak{R}_{U_n/U}(\pi_2^{U_n,*} W) \to \mathfrak{R}_{U_{n-1}/U}(\pi_2^{U_{n-1},*} W).$$

Now notice that the ideal of U_{n-1} in U_n is a square-0 ideal.

Let $f \in \mathrm{Hom}_{U_{n-1}}(T \times_U U_{n-1}, \pi_2^{U_{n-1},*} W)$. View f as a U_n-morphism

$$T \times_U U_{n-1} \to \pi_2^{U_n,*} W$$

via the canonical closed immersions $\pi_2^{U_{n-1},*} W \hookrightarrow \pi_2^{U_n,*} W$ and $U_{n-1} \hookrightarrow U_n$. The fiber over f of the map (2) then consists of the extensions of f to U_n-morphisms $T \times_U U_n \to \pi_2^{U_n,*} W$. The theory of infinitesimal extensions of morphisms to smooth schemes (see [Grothendieck 1963, Exposé III, Proposition 5.1]) implies that this fiber is an affine space under the group

$$H^0(T \times_U U_{n-1}, f^* \Omega^\vee_{\pi_2^{U_n,*} W/U_n} \otimes N),$$

where N is the conormal bundle of the closed immersion $T \times_U U_{n-1} \hookrightarrow T \times_U U_n$. Since U_n and U_{n-1} are flat over U, the coherent sheaf N is the pullback to $T \times_U U_{n-1}$ of the conormal bundle of the immersion $U_{n-1} \hookrightarrow U_n$. Now since the diagonal is regularly immersed in $U \times_{k_0} U$ (because U is smooth over k_0), the conormal bundle of the immersion $U_{n-1} \hookrightarrow U_n$ is $\mathrm{Sym}^n(\Omega_{U/k_0})$ (viewed as a sheaf in $\mathcal{O}_{U_{n-1}}$-modules via the closed immersion $U_0 \to U_{n-1}$). See [Matsumura 1989, Chapters 6 and 16]. Hence,

$$\begin{aligned} H^0(T \times_U U_{n-1}, f^*\Omega^{\vee}_{\pi_2^{U_n,*}W/U_n} \otimes N) \\ &\simeq H^0(T \times_U U_{n-1}, f^*\Omega^{\vee}_{\pi_2^{U_n,*}W/U_n} \otimes \mathrm{Sym}^n(\Omega_{U/k_0})) \\ &\simeq H^0(T, f_0^*\Omega^{\vee}_{W/U} \otimes \mathrm{Sym}^n(\Omega_{U/k_0})), \end{aligned}$$

where f_0 is the U-morphism $T \to W$ arising from f by base-change to U. □

2B. ***The jet schemes of smooth commutative group schemes.*** We keep the terminology of Section 2A. Let $\mathscr{C}/U$ be a commutative group scheme over U with zero-section $\epsilon : U \to \mathscr{C}$. If $n \in \mathbb{N}$, we shall write $[n]_{\mathscr{C}} : \mathscr{C} \to \mathscr{C}$ for the multiplication-by-n morphism. The schemes $J^n(\mathscr{C}/U)$ are then naturally group schemes over U. Furthermore, for each $n \geqslant m \geqslant 0$, the morphism $\Lambda^{\mathscr{C}}_{n,m} : J^n(\mathscr{C}/U) \to J^m(\mathscr{C}/U)$ is a morphism of group schemes. If $m = n-1$, the kernel of $\Lambda^{\mathscr{C}}_{n,m}$ is the vector bundle $\epsilon^*(\Omega^{\vee}_{\mathscr{C}/U}) \otimes \mathrm{Sym}^n(\Omega_{U/k_0})$. The torsor structure is realized by the natural action of $\epsilon^*(\Omega^{\vee}_{\mathscr{C}/U}) \otimes \mathrm{Sym}^n(\Omega_{U/k_0})$ on $J^n(\mathscr{C}/U)$. The details of the verification of these facts are left to the reader.

Lemma 2.4. *Let $n \geqslant 1$. Suppose that* $\mathrm{char}(k_0) = p$. *There is a U-morphism $[p^n]^\circ : \mathscr{C} \to J^n(\mathscr{C}/U)$ such that $\Lambda^{\mathscr{C}}_{n,0} \circ [p^n]^\circ = [p^n]_{\mathscr{C}}$ and $[p^n]_{J^n(\mathscr{C}/U)} = [p^n]^\circ \circ \Lambda^{\mathscr{C}}_{n,0}$.*

Proof. Let $T \to U$ be an affine U-scheme. Define a map

$$\phi_{T,n} : \mathrm{Hom}_U(T, \mathscr{C}) \to \mathrm{Hom}_{U_n}(T \times_U U_n, \pi_2^*\mathscr{C})$$

by the following recipe. Let $f \in \mathrm{Hom}_U(T, \mathscr{C})$, and take any extension $\tilde{f}$ of f to a morphism $T \times_U U_n \to (\pi_2^*\mathscr{C})_{U_n}$; then define $\phi_{T,n}(f) = p^n \cdot \tilde{f}$. To see that this does not depend on the choice of the extension $\tilde{f}$, notice that the kernel K_n of the restriction map

$$\mathrm{Hom}_{U_n}(T \times_U U_n, \pi_2^*\mathscr{C}) \to \mathrm{Hom}_U(T, \mathscr{C})$$

is obtained by successive extensions by the groups $H^0(T, f^*\Omega^{\vee}_{\mathscr{C}/U} \otimes \mathrm{Sym}^i(\Omega_{U/k_0}))$ for $i = 1, \dots, n$ (see [Grothendieck 1963, Exposé III, Corollaire 5.3] for all this). Hence, K_n is annihilated by multiplication by p^n because T is a scheme of characteristic p.

The definition of $\phi_{T,n}$ is functorial in T, and thus, by patching the morphisms $\phi_{T,n}$ as T runs over the elements of an affine cover of $\mathscr{C}$, we obtain the required morphism $[p^n]^\circ$. □

Now notice that there is a canonical map $\lambda_n^W : W(U) \to J^n(W/U)(U)$ that sends the U-morphism $f : U \to W$ to $J^n(f) : J^n(U/U) = U \to J^n(W/U)$ for any scheme W over U.

Lemma 2.5. *The maps λ_n^W have the following properties*:

(a) *For $n \geqslant m \geqslant 0$, the identity $\Lambda^W_{n,m} \circ \lambda_n^W = \lambda_m^W$ holds.*

(b) *If W/U is commutative group scheme over U, then λ_n^W is a homomorphism*; *furthermore*, *on $W(U)$ we then have the identity $[p^n]_{J^n(W/U)} \circ \lambda_n^W = [p^n]^\circ$.*

(c) *If $f : W \to W_1$ is a U-scheme morphism, then $J^n(f) \circ \lambda_n^W = \lambda_n^{W_1} \circ f$.*

Proof. This is left as an exercise for the reader. □

Remark 2.6. An interesting feature of the map λ_n^W is that it does *not* arise from a morphism of schemes $W \to J^n(W/U)$.

3. Proof of Theorem 1.3 and Corollary 1.4

We now turn to the proof of our main result. We shall use the terminology of the preliminaries. Let $k_0 := \bar{\mathbb{F}}_p$, and suppose now that U is a smooth curve over k_0 whose function field is K_0. We take U sufficiently small so that X extends to a flat scheme $\mathscr{X}$ over U and so that A extends to an abelian scheme $\mathscr{A}$ over U. We also suppose that the closed immersion $X \hookrightarrow A$ extends to a closed immersion $\mathscr{X} \to \mathscr{A}$.

Recall that the following hypothesis is supposed to hold: for any field extension $L_0|K_0$ and any $Q \in A(L_0)$, the set $X_{L_0}^{+Q} \cap \mathrm{Tor}(A(L_0))$ is not Zariski dense in $X_{L_0}^{+Q}$.

3A. ***The critical schemes.*** For all $n \geqslant 0$, we define

$$\mathrm{Crit}^n(\mathscr{X}, \mathscr{A}) := [p^n]_*(J^n(\mathscr{A}/U)) \cap J^n(\mathscr{X}/U).$$

Here $[p^n]_*(J^n(\mathscr{A}/U))$ is the scheme-theoretic image of $J^n(\mathscr{A}/U)$ by $[p^n]_{J^n(\mathscr{A}/U)}$. Notice that by Lemma 2.4, we have $[p^n](J^n(\mathscr{A}/U)) = [p^n]^\circ(\mathscr{A})$, and since $[p^n]$ is proper (because $\mathscr{A}$ is proper over U), we see that $[p^n](J^n(\mathscr{A}/U))$ is closed and that the natural morphism $[p^n]_*(J^n(\mathscr{A}/U)) \to \mathscr{A}$ is finite.

The morphisms $\Lambda^{\mathscr{A}}_{n,n-1} : J^n(\mathscr{A}/U) \to J^{n-1}(\mathscr{A}/U)$ lead to a projective system of U-schemes

$$\cdots \to \mathrm{Crit}^2(\mathscr{X}, \mathscr{A}) \to \mathrm{Crit}^1(\mathscr{X}, \mathscr{A}) \to \mathscr{X}$$

whose connecting morphisms are finite. We let $\mathrm{Exc}^n(\mathscr{A}, \mathscr{X}) \hookrightarrow \mathscr{X}$ be the scheme-theoretic image of $\mathrm{Crit}^n(\mathscr{A}, \mathscr{X})$ in $\mathscr{X}$.

For any $Q \in \mathscr{A}(U) = A(K_0)$, we shall write $\mathscr{X}^{+Q} = \mathscr{X} + Q$ for the translation of $\mathscr{X}$ by Q in $\mathscr{A}$.

Proposition 3.1. *There exists $\alpha = \alpha(\mathscr{A}, \mathscr{X}) \in \mathbb{N}$ such that for all $Q \in \Gamma$, the set* $\mathrm{Exc}^{\alpha}(\mathscr{A}, \mathscr{X}^{+Q})$ *is not dense in* $\mathscr{X}^{+Q}$.

Remark 3.2. Proposition 3.1 should be compared to [Buium 1992, Theorem 1].

The following theorem, proved by Galois-theoretic methods in Section 4, will play a crucial role in the proof of Proposition 3.1.

Let $S := \mathrm{Spec}\, k_0[\![t]\!]$. Let $L := k_0((t))$ be the function field of S. For any $n \in \mathbb{N}$, let $S_n := \mathrm{Spec}\, k_0[t]/t^{n+1}$ be the n-th infinitesimal neighborhood of the closed point of S in S. Fix $\lambda_0 \in \mathbb{N}^*$, and let $R^{\mathrm{alg}} = R^{\mathrm{alg},\lambda_0} := \mathbb{F}_{p^{\lambda_0}}[\![t]\!] \subseteq k_0[\![t]\!]$. Let $S^{\mathrm{alg}} = S^{\mathrm{alg},\lambda_0} := \mathrm{Spec}\, R^{\mathrm{alg}}$. There is an obvious morphism $S \to S^{\mathrm{alg}}$.

Let $\mathfrak{D}$ be an abelian scheme over S, and let $\mathfrak{X} \hookrightarrow \mathfrak{D}$ be a closed integral subscheme. Suppose that the abelian scheme has a model $\mathfrak{D}^{\mathrm{alg}}$ over S^{alg} as an abelian scheme and that the immersion $\mathfrak{X} \hookrightarrow \mathfrak{D}$ has a model $\mathfrak{X}^{\mathrm{alg}} \hookrightarrow \mathfrak{D}^{\mathrm{alg}}$ over S^{alg}. If $c \in \mathfrak{D}(S)$, write as usual $\mathfrak{X}^{+c} := \mathfrak{X} + c$ for the translation of $\mathfrak{X}$ by c in $\mathfrak{D}$. Let D_0 and D be the fibers of $\mathfrak{D}$ over the closed and generic points of S, respectively. If $c \in \mathfrak{D}(S)$, let Z_0^{+c} and Z^{+c} be the fibers of $\mathfrak{X}^{+c}$ over the closed and generic points of S, respectively.

Notice that there is a natural inclusion $\mathfrak{D}^{\mathrm{alg}}(S^{\mathrm{alg}}) \subseteq \mathfrak{D}(S)$.

Theorem 3.3. *Suppose that* $\mathrm{Tor}(D(\bar{L})) \cap X_{\bar{L}}^{+c}$ *is not dense in* $X_{\bar{L}}^{+c}$ *for all* $c \in \mathfrak{D}^{\mathrm{alg}}(S^{\mathrm{alg}}) \subseteq \mathfrak{D}(S)$.

Then there exists a constant $n_0 = n_0(\mathfrak{D}, \mathfrak{X}) \in \mathbb{N}^*$ such that for all $c \in \mathfrak{D}^{\mathrm{alg}}(S^{\mathrm{alg}}) \subseteq \mathfrak{D}(S)$ the set

$$\{P \in Z_0^{+c}(k_0) \mid P \text{ lifts to an element of } \mathfrak{X}^{+c}(S_{n_0}) \cap p^{n_0} \cdot \mathfrak{D}(S_{n_0})\}$$

is not Zariski dense in Z_0^{+c}.

Proof. This is a special case of Corollary 4.5. □

Proof Proposition 3.1. Since $\mathscr{X}$ is flat over U and X is integral, we see that $\mathscr{X}$ is also integral (see for instance [Liu 2002, 4.3.1, Proposition 3.8] for this). Hence, it is sufficient to show that $\mathrm{Exc}^n(\mathscr{A}, \mathscr{X}^{+Q})_u$ is not Zariski dense in $\mathscr{X}_u^{+Q}$ for some (any) closed point $u \in U$. Now using (1) in the previous section, we see that

$$\begin{aligned}\mathrm{Crit}^n(\mathscr{A}, \mathscr{X}^{+Q})_u(k_0) &= ([p^n]_*(J^n(\mathscr{A}/U)))_u(k_0) \cap J^n(\mathscr{X}^{+Q}/U)_u(k_0)\\ &= \{P \in J^n(\mathscr{X}^{+Q}/U)_u(k_0) \mid \exists \tilde{P} \in J^n(\mathscr{A}/U)_u(k_0),\ p^n \cdot \tilde{P} = P\}\\ &= \{P \in \mathscr{X}^{+Q}(u_n) \mid \exists \tilde{P} \in \mathscr{A}(u_n),\ p^n \cdot \tilde{P} = P\},\end{aligned}$$

and thus,

$$\begin{aligned}&\mathrm{Exc}^n(\mathscr{A}, \mathscr{X}^{+Q})_u(k_0)\\ &\qquad = \{P \in \mathscr{X}_u^{+Q}(k_0) \mid P \text{ lifts to an element of } \mathscr{X}^{+Q}(u_n) \cap p^n \cdot \mathscr{A}(u_n)\}.\end{aligned}$$

Now notice that $\mathscr{A}$ has a model $\tilde{\mathscr{A}}$ as an abelian scheme over a curve $\tilde{U}$, which is smooth over a finite field; also since the group Γ is finitely generated, we might assume that Γ is the image of a group $\tilde{\Gamma} \subseteq \tilde{\mathscr{A}}(\tilde{U})$. Finally, we might assume that the immersion $\mathscr{X} \hookrightarrow \mathscr{A}$ has a model $\tilde{\mathscr{X}} \hookrightarrow \tilde{\mathscr{A}}$ over $\tilde{U}$. We may thus apply Theorem 3.3 to the base-change of $\mathscr{X} \hookrightarrow \mathscr{A}$ to the completion of U at u. We obtain that there is an n_0 such that the set

$$\{P \in \mathscr{X}_u^{+Q}(k_0) \mid P \text{ lifts to an element of } \mathscr{X}^{+Q}(u_{n_0}) \cap p^{n_0} \cdot \mathscr{A}(u_{n_0})\}$$

is not Zariski dense in $\mathscr{X}_u$ for all $Q \in \Gamma$. So we may set $\alpha = n_0$. □

3B. *End of proof.* The proof of Theorem 1.3 is by contradiction. So suppose that $X \cap \Gamma$ is dense in X.

Let $P_1 \in \Gamma$ be such that $(X + P_1) \cap p \cdot \Gamma$ is dense, let $P_2 \in p \cdot \Gamma$ such that $(X + P_1 + P_2) \cap p^2 \cdot \Gamma$ is dense in $X + P_1 + P_2$, and so forth. The existence of the sequence of point $(P_i)_{i \in \mathbb{N}^*}$ is guaranteed by the assumption on Γ, which implies that $p^i\Gamma/p^{i+1}\Gamma$ is finite for all $i \geqslant 0$.

Now let $\alpha = \alpha(\mathscr{A}, \mathscr{X})$ be the natural number provided by Proposition 3.1. Let $Q = \sum_{i=1}^{\alpha} P_i$. By construction, the set $\mathscr{X}^{+Q} \cap p^\alpha \cdot \Gamma$ is dense in $\mathscr{X}^{+Q}$. On the other hand, by Lemma 2.5,

$$\begin{aligned}
&\mathscr{X}^{+Q}(U) \cap p^\alpha \cdot \Gamma \\
&\qquad = \Lambda^{\mathscr{A}}_{\alpha,0}(\lambda^{\mathscr{A}}_\alpha(\mathscr{X}^{+Q}(U) \cap p^\alpha \cdot \Gamma)) \subseteq \Lambda^{\mathscr{A}}_{\alpha,0}[\lambda^{\mathscr{X}}_\alpha(\mathscr{X}^{+Q}(U)) \cap \lambda^{\mathscr{A}}_\alpha(p^\alpha \cdot \Gamma)] \\
&\qquad \subseteq \Lambda^{\mathscr{A}}_{\alpha,0}[J^\alpha(\mathscr{X}^{+Q}/U) \cap p^\alpha \cdot J^\alpha(\mathscr{A}/U)(U)] \subseteq \Lambda^{\mathscr{X}}_{\alpha,0}[\mathrm{Crit}^\alpha(\mathscr{A}, \mathscr{X}^{+Q})] \\
&\qquad = \mathrm{Exc}^\alpha(\mathscr{A}, \mathscr{X}^{+Q}),
\end{aligned}$$

and thus, we deduce that $\mathrm{Exc}^\alpha(\mathscr{A}, \mathscr{X}^{+Q})$ is dense in $\mathscr{X}^{+Q}$. This contradicts Proposition 3.1 and concludes the proof of Theorem 1.3.

The proof of Corollary 1.4 now follows directly from Theorem 1.3 and from the following invariance lemma:

Lemma 3.4. *Suppose that the hypotheses of Theorem 1.1 hold. Let F' be an algebraically closed field, and let $F'|F$ be a field extension. Then Theorem 1.1 holds if and only if Theorem 1.1 holds with F' in place of F, $Y_{F'} \hookrightarrow B_{F'}$ in place of $Y \hookrightarrow B$, and the image $\Lambda_{F'} \subseteq B_{F'}(F')$ of Λ in place of Λ.*

Proof. The implication $\Longrightarrow$ follows from the fact that $Y_{F'} \cap \Lambda_{F'}$ is dense in $Y_{F'}$ if and only if $Y \cap \Lambda$ is dense in Y; indeed, the morphism $\operatorname{Spec} F' \to \operatorname{Spec} F$ is universally open (see [Grothendieck 1965, Exposé IV, 2.4.10] for this).

Now we prove the implication $\Longleftarrow$. Let $C_1 := \mathrm{Stab}(Y_{F'})^{\mathrm{red}}$, and suppose that there exist

- a semiabelian variety B_1' over F',
- a homomorphism with finite kernel $h_1 : B_1' \to B_{F'}/C_1$,
- a model $\mathbf{B}_1'$ of B_1' over a finite subfield $\mathbb{F}_{p^r} \subset F'$,

- an irreducible reduced closed subscheme $\mathbf{Y}'_1 \hookrightarrow \mathbf{B}'_1$, and
- a point $b_1 \in (B_{F'}/C_1)(F')$ such that $Y_{F'}/C_1 = b_1 + h_{1,*}(\mathbf{Y}'_1 \times_{\mathbb{F}_{p^r}} F')$.

Now, first notice that since $\mathrm{Stab}(\,\cdot\,)$ represents a functor, there is a natural isomorphism $\mathrm{Stab}(Y_{F'}) \simeq \mathrm{Stab}(Y)_{F'}$ and, since F is algebraically closed, also a natural isomorphism $\mathrm{Stab}(Y_{F'})^{\mathrm{red}} \simeq (\mathrm{Stab}(Y)^{\mathrm{red}})_{F'}$. Secondly, we have $\mathbb{F}_{p^r} \subset F$ since F is algebraically closed. Thirdly, if B_2 and B_3 are semiabelian varieties over F and $\phi : B_{2,F'} \to B_{3,F'}$ is a homomorphism of group schemes over F', then ϕ arises by base-change from an F-morphism $B_2 \to B_3$. This is a consequence of the facts that the graph of ϕ has a dense set of torsion points in $B_{2,F'} \times_{F'} B_{3,F'}$ and torsion points are defined in $B_2 \times_F B_3$. Putting these facts together, we deduce that there exist

- a semiabelian variety B' over F,
- a homomorphism with finite kernel $h : B' \to B/C$,
- a model $\mathbf{B}'$ of B' over a finite subfield $\mathbb{F}_{p^r} \subset F$,
- an irreducible reduced closed subscheme $\mathbf{Y}' \hookrightarrow \mathbf{B}'$, and
- a point $b_1 \in (B_{F'}/C_{F'})(F')$ such that $Y_{F'}/C_{F'} = b_1 + h_{F',*}(\mathbf{Y}' \times_{\mathbb{F}_{p^r}} F')$,

where $C = \mathrm{Stab}(Y)^{\mathrm{red}}$. Now $\mathrm{Transp}(Y_{F'}/C_{F'}, h_{F',*}(\mathbf{Y}' \times_{\mathbb{F}_{p^r}} F'))(F') \neq \varnothing$ by the last point in the list above. Here $\mathrm{Transp}(\,\cdot\,)$ is the transporter, which is a generalization of the stabilizer (see [Grothendieck et al. 1970b, Exposé VIII, 6] for the definition). Thus, $\mathrm{Transp}(Y/C, h_*(\mathbf{Y}' \times_{\mathbb{F}_{p^r}} F))(F) \neq \varnothing$, which is to say that there also exists

- a point $b_1 \in (B/C)(F)$ such that $Y/C = b_1 + h_*(\mathbf{Y}' \times_{\mathbb{F}_{p^r}} F)$. □

4. Sparsity of highly p-divisible unramified liftings

This section can be read independently of the rest of the text, and its results do not rely on the previous ones. Also, unlike the previous sections, *the terminology of this section is independent of the terminology of Section 1*.

Let S be the spectrum of a complete discrete local ring. Let k be the residue field of its closed point. We suppose that k is a *finite field* of characteristic p. Let K be the fraction field of S. Let S^{sh} be the spectrum of the strict henselization of S, and let L be the fraction field of S^{sh}. We identify $\bar{k}$ with the residue field of the closed point of S^{sh}. For any $n \in \mathbb{N}$, we shall write S_n and S^{sh}_n for the n-th infinitesimal neighborhoods of the closed point of S in S and S^{sh} in S^{sh}, respectively.

Let $\mathscr{A}$ be an abelian scheme over S, and let $A := \mathscr{A}_K$. Write A_0 for the fiber of $\mathscr{A}$ over the closed point of S.

Theorem 4.1. *Let $\mathscr{X} \hookrightarrow \mathscr{A}$ be a closed integral subscheme. Let X_0 be the fiber of $\mathscr{X}$ over the closed point of S, and let $X := \mathscr{X}_K$.*

Suppose that $\mathrm{Tor}(A(\overline{K})) \cap X_{\overline{K}}$ *is not dense in* $X_{\overline{K}}$.

Then there exists a constant $m \in \mathbb{N}$ such that the set

$$\{P \in X_0(\bar{k}) \mid P \text{ lifts to an element of } \mathscr{X}(S_m^{\mathrm{sh}}) \cap p^m \cdot \mathscr{A}(S_m^{\mathrm{sh}})\}$$

is not Zariski dense in X_0.

Suppose for the next sentence that S is the spectrum of a complete discrete valuation ring that is absolutely unramified and is the completion of a number field along a nonarchimedean place. In this situation, Raynaud proves Theorem 4.1 and Corollary 4.5 below under the stronger hypothesis that $X_{\overline{K}}$ does not contain any translates of positive-dimensional abelian subvarieties of $A_{\overline{K}}$ [Raynaud 1983a, Proposition II.1.1]. See also [Raynaud 1983b, Theorem II, p. 207] for a more precise result in the situation where X is a smooth curve.

In the case where S is the spectrum of the ring of integers of a finite extension of $\mathbb{Q}_p$, Theorem 4.1 implies versions of the Tate–Voloch conjecture (see [Tate and Voloch 1996; Scanlon 1999]). We leave it to the reader to work out the details.

Preliminary to the proof of Theorem 4.1, we quote the following result. Let B be an abelian variety over an algebraically closed field F, and let $\psi : B \to B$ be an endomorphism. Let $R \in \mathbb{Z}[T]$ be a polynomial that has no roots of unity among its complex roots. Suppose that $R(\psi) = 0$ in the ring of endomorphisms of B.

Proposition 4.2 (Pink–Rössler). *Let $Z \subseteq B$ be a closed irreducible subset such that $\psi(Z) = Z$. Then* $\mathrm{Tor}(B(F)) \cap Z$ *is dense in Z.*

The proof of Proposition 4.2 is based on a spreading-out argument, which is used to reduce the problem to the case where F is the algebraic closure of a finite field. In this last case, the statement becomes obvious. See [Pink and Rössler 2004, Proposition 6.1] for the details.

We shall use the map $[p^\ell]^\circ : A_0(\bar{k}) \to \mathscr{A}(S_\ell^{\mathrm{sh}})$, which is defined by the formula $[p^\ell]^\circ(x) = p^\ell \cdot \tilde{x}$, where $\tilde{x}$ is any lifting of x (this does not depend on the lifting; see [Katz 1981, after Theorem 2.1]).

Proof of Theorem 4.1. Let ϕ be a topological generator of $\mathrm{Gal}(\bar{k}|k)$. By the Weil conjectures for abelian varieties, there is a polynomial

$$Q(T) := T^{2g} - (a_{2g-1}T^{2g-1} + \cdots + a_0)$$

with $a_i \in \mathbb{Z}$ such that $Q(\phi)(x) = 0$ for all $x \in A_0(\bar{k})$ and such that $Q(T)$ has no roots of unity among its complex roots. Let M be the matrix

$$\begin{bmatrix} 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \\ a_0 & a_1 & \cdots & a_{n-2} & a_{2g-1} \end{bmatrix}.$$

We view M as an endomorphism of abelian S-schemes $\mathcal{A}^{2g} \to \mathcal{A}^{2g}$. Let $\tau \in \mathrm{Aut}_S(S^{\mathrm{sh}})$ be the canonical lifting of ϕ. By construction, τ induces an element of $\mathrm{Aut}_{S_n}(S_n^{\mathrm{sh}})$ for any $n \geqslant 0$, which we also call τ. The reduction map $\mathcal{A}(S^{\mathrm{sh}}) \to \mathcal{A}(S_n^{\mathrm{sh}})$ is compatible with the action of τ on both sides. Write

$$u(x) := (x, \tau(x), \tau^2(x), \dots, \tau^{2g-1}(x)) \in \Big(\prod_{s=0}^{2g-1} \mathcal{A}\Big)(S^{\mathrm{sh}})$$

for any element $x \in \mathcal{A}(S^{\mathrm{sh}})$. Abusing notation, we shall also write

$$u(x) := (x, \tau(x), \tau^2(x), \dots, \tau^{2g-1}(x)) \in \Big(\prod_{s=0}^{2g-1} \mathcal{A}\Big)(S_n^{\mathrm{sh}})$$

for any element $x \in \mathcal{A}(S_n^{\mathrm{sh}})$. By construction, for any $x \in \mathcal{A}(S^{\mathrm{sh}})$ and $x \in \mathcal{A}(S_n^{\mathrm{sh}})$, the equation $Q(\tau)(x) = 0$ implies the vector identity $M(u(x)) = u(\tau(x))$, respectively.

Now consider the closed S-subscheme of $\mathcal{A}^{2g}$

$$\mathcal{Z} := \bigcap_{t \geqslant 0} M_*^t \Big(\bigcap_{r \geqslant 0} M^{r,*} \Big(\prod_{s=0}^{2g-1} \mathcal{X} \Big)\Big),$$

where for any $r \geqslant 0$, M^r is the r-th power of M. The symbol $M_*^t(\,\cdot\,)$ refers to the scheme-theoretic image, and the intersections are the scheme-theoretic intersections. The intersections are finite by noetherianity.

Let $\lambda : J \to \mathcal{A}^{2g}$ be a morphism of schemes. The construction of $\mathcal{Z}$ implies that if

(i) $M^r \circ \lambda$ factors through $\prod_{s=0}^{2g-1} \mathcal{X}$ for all $r \geqslant 0$ and

(ii) for all $r \geqslant 0$, there is a morphism $\phi_r : J \to \bigcap_{r \geqslant 0} M^{r,*}\big(\prod_{s=0}^{2g-1} \mathcal{X}\big)$ such that $\lambda = M^r \circ \phi_r$,

then λ factors through $\mathcal{Z}$.

In particular, if (i) is verified and $M^{r_\lambda} \circ \lambda = \lambda$ for some $r_\lambda \geqslant 1$, then λ factors through $\mathcal{Z}$.

Remark 4.3. In particular, this implies that if $x \in \mathcal{X}(S^{\mathrm{sh}})$ and $x \in \mathcal{X}(S_n^{\mathrm{sh}})$ have the property that $Q(\tau)(x) = 0$, then $u(x) \in \mathcal{Z}(S^{\mathrm{sh}})$ and $u(x) \in \mathcal{Z}(S_n^{\mathrm{sh}})$, respectively.

Lemma 4.4. *There is a set-theoretic identity $M(\mathcal{Z}) = \mathcal{Z}$.*

Proof. Since M is proper, we have a set-theoretic identity

$$\mathcal{Z} = \bigcap_{t \geqslant 0} M^t \Big(\bigcap_{r \geqslant 0} M^{r,-1} \Big(\prod_{s=0}^{2g-1} \mathcal{X} \Big)\Big).$$

Now directly from the construction, we have

$$M\Big(\bigcap_{r\geqslant 0} M^{r,-1}\Big(\prod_{s=0}^{2g-1}\mathscr{X}\Big)\Big) \subseteq \bigcap_{r\geqslant 0} M^{r,-1}\Big(\prod_{s=0}^{2g-1}\mathscr{X}\Big),$$

and hence, we have inclusions

$$\bigcap_{r\geqslant 0} M^{r,-1}\Big(\prod_{s=0}^{2g-1}\mathscr{X}\Big) \supseteq M\Big(\bigcap_{r\geqslant 0} M^{r,-1}\Big(\prod_{s=0}^{2g-1}\mathscr{X}\Big)\Big) \supseteq M^2\Big(\bigcap_{r\geqslant 0} M^{r,-1}\Big(\prod_{s=0}^{2g-1}\mathscr{X}\Big)\Big) \supseteq \cdots,$$

and thus, by noetherianity

$$M^{\ell}\Big(\bigcap_{r\geqslant 0} M^{r,-1}\Big(\prod_{s=0}^{2g-1}\mathscr{X}\Big)\Big) = M^{\ell+1}\Big(\bigcap_{r\geqslant 0} M^{r,-1}\Big(\prod_{s=0}^{2g-1}\mathscr{X}\Big)\Big)$$

for some $\ell \geqslant 0$. This implies the result. □

Now we apply Proposition 4.2 and obtain that $\mathfrak{X}_{\bar{K},\mathrm{red}} \cap \mathrm{Tor}(\prod_{s=0}^{2g-1} A(\bar{K}))$ is dense in $\mathfrak{X}_{\bar{K},\mathrm{red}}$. Hence, the projection onto the first factor $\mathfrak{X}_K \to X$ is not surjective by hypothesis.

Let T be the scheme-theoretic image of the morphism $\mathfrak{X} \to \mathscr{X}$ given by the first projection. Notice that X_0 is a closed subscheme of T because every element P of $X_0(\bar{k})$ satisfies the equation $Q(\phi)(P) = 0$. Let H be the closed subset of T that is the union of the irreducible components of T that surject onto S. A reduced irreducible component I of T that surjects onto S is flat over S; since $H \neq \mathscr{X}$, we have in particular $I \neq \mathscr{X}$, and so we see that the dimension of the fiber of I over the closed point of S is strictly smaller than the dimension of X_0. Hence, the intersection of H and X_0 is a proper closed subset of X_0. Let T_1 be the open subscheme $T \setminus H$ of T. From the previous discussion, we see that the underlying set of T_1 is a *nonempty open subset of* X_0.

We are now in a position to complete the proof of Theorem 4.1. The proof will be by contradiction. So suppose that for all $\ell \in \mathbb{N}$, the set

$$\{P \in X_0(\bar{k}) \mid P \text{ lifts to an element of } \mathscr{X}(S_\ell^{\mathrm{sh}}) \cap p^\ell \cdot \mathscr{A}(S_\ell^{\mathrm{sh}})\}$$

is Zariski dense in X_0.

Choose an arbitrary $\ell \in \mathbb{N}$, and let $P \in T_1(\bar{k})$ be a point that lifts to an element of $\mathscr{X}(S_\ell^{\mathrm{sh}}) \cap p^\ell \cdot \mathscr{A}(S_\ell^{\mathrm{sh}})$. This exists because the set of points in $X_0(\bar{k})$ with this property is assumed to be dense in X_0. Let $\tilde{P} \in \mathscr{A}(S_\ell^{\mathrm{sh}})$ be such that $p^\ell \cdot \tilde{P} \in \mathscr{X}(S_\ell^{\mathrm{sh}})$ and such that $p^\ell \cdot \tilde{P}_0 = P$. Here $\tilde{P}_0 \in A_0(\bar{k})$ is the $\bar{k}$-point induced by $\tilde{P}$. Since the map $[p^\ell]^\circ : \mathscr{A}_0(\bar{k}) \to \mathscr{A}(S_\ell^{\mathrm{sh}})$ intertwines ϕ and τ, we see that

$$Q(\tau)([p^\ell]^\circ(\tilde{P}_0)) = 0.$$

By Remark 4.3, we thus have

$$u([p^\ell]^\circ(\tilde{P}_0)) \in \mathfrak{X}(S_\ell^{\mathrm{sh}}).$$

Hence,

$$[p^\ell]^\circ(\tilde{P}_0) \in T_1(S_\ell^{\mathrm{sh}}) \subseteq T(S_\ell^{\mathrm{sh}}).$$

This shows that $T_1(S_\ell^{\mathrm{sh}}) \neq \varnothing$. Since ℓ was arbitrary, this shows that the generic fiber $T_{1,K}$ of T_1 is not empty, which is a contradiction. □

Corollary 4.5. *We keep the hypotheses of Theorem 4.1. We suppose furthermore that* $\mathrm{Tor}(A(\bar{K})) \cap X_{\bar{K}}^{+c}$ *is not dense in* $X_{\bar{K}}^{+c}$ *for all* $c \in \mathcal{A}(S)$. *Then there exists a constant* $m \in \mathbb{N}$ *such that for all* $c \in \mathcal{A}(S)$ *the set*

$$\{P \in X_0^{+c}(\bar{k}) \mid P \textit{ lifts to an element of } \mathcal{X}^{+c}(S_m^{\mathrm{sh}}) \cap p^m \cdot \mathcal{A}(S_m^{\mathrm{sh}})\}$$

is not Zariski dense in X_0^{+c}.

Here as usual $\mathcal{X}^{+c} = \mathcal{X} + c$ is the translate inside $\mathcal{A}$ of $\mathcal{X}$ by $c \in \mathcal{A}(S)$. Slightly abusing notation, we write X^{+c} for $(\mathcal{X}^{+c})_K$ and X_0^{+c} for $(\mathcal{X}^{+c})_k$.

Proof. We prove by contradiction. Write $m(\mathcal{X}^{+c})$ for the smallest integer m such that

$$\{P \in X_0^{+c}(\bar{k}) \mid P \text{ lifts to an element of } \mathcal{X}^{+c}(S_m^{\mathrm{sh}}) \cap p^m \cdot \mathcal{A}(S_m^{\mathrm{sh}})\}$$

is not Zariski dense in X_0. Suppose that there exists a sequence $(a_n \in \mathcal{A}(S))_{n \in \mathbb{N}}$ such that $m(\mathcal{X}^{+a_n})$ strictly increases. Replace $(a_n \in \mathcal{A}(S))_{n \in \mathbb{N}}$ by one of its subsequences so that $\lim_n a_n = a \in \mathcal{A}(S)$, where the convergence is for the topology given by the discrete valuation on the ring underlying S (notice that $\mathcal{A}(S)$ is compact for this topology because S is complete and has a finite residue field at its closed point). Replace $(a_n \in \mathcal{A}(S))_{n \in \mathbb{N}}$ by one of its subsequences again so that the image of a_n in $\mathcal{A}(S_n)$ equals the image of a in $\mathcal{A}(S_n)$. By construction, we have $m(\mathcal{X}^{+a_n}) \geqslant n$, and hence, by definition $m(\mathcal{X}^a) \geqslant n$. Since this is true for all $n \geqslant 0$, this contradicts Theorem 4.1. □

The following corollary should be viewed as a curiosity only since it is a special case of Theorem 1.3. The interest lies in its proof, which avoids the use of jet schemes, unlike the proof of Theorem 1.3.

Corollary 4.6. *We keep the notation and assumptions of Corollary 4.5. Suppose furthermore that* S *is a ring of characteristic* p *and that the fibers of* $\mathcal{A}$ *over* S *are ordinary abelian varieties. We also suppose that* $\mathcal{X}$ *is smooth over* S. *Let* $\Gamma \subseteq A(K)$ *be a finitely generated subgroup. Then the set* $X \cap \Gamma$ *is not Zariski dense in* X.

We shall call the topology on $A(K)$ induced by the discrete valuation *the* v*-adic topology*.

Before the proof of the corollary, recall a simple but crucial lemma of Voloch (see [Abramovich and Voloch 1992, Lemma 1]).

Lemma 4.7 (Voloch). *Let L_0 be a field, and let T be a reduced scheme of finite type over L_0. Then $T(L_0^{\mathrm{sep}})$ is dense in T if and only if T is geometrically reduced.*

Proof of Corollary 4.6. The proof is by contradiction. We shall exhibit a translate of X by an element of $A(K)$, which violates the conclusion of Theorem 4.1. Suppose that $X \cap \Gamma$ is Zariski dense in X. Let $P_1 \in \Gamma$ be such that $(X + P_1) \cap p \cdot \Gamma$ is dense, let $P_2 \in p \cdot \Gamma$ such that $(X + P_1 + P_2) \cap p^2 \cdot \Gamma$ is dense in X, and so forth. The existence of the sequence of points (P_i) is guaranteed by the assumption on Γ, which implies that the group $p^\ell \Gamma / p^{\ell+1}\Gamma$ is finite for all $\ell \geqslant 0$. Since the v-adic topology on the set $A(K)$ is compact (because S is a discrete valuation ring with a finite residue field), the sequence $Q_i = \sum_{\ell \geqslant 1}^{i} P_\ell$ has a subsequence that converges in $A(K)$. Let Q be the limit point of such a subsequence. By construction, $(X + Q) \cap p^\ell \cdot A(K)$ is dense for all $\ell \geqslant 0$. Let $\mathscr{X}^{+Q} := \mathscr{X} + Q$.

Consider the morphism $([p^\ell]^* \mathscr{X}^{+Q})_{\mathrm{red}} \to \mathscr{X}^{+Q}$. There is a diagram

$$\begin{array}{ccccc} ([p^\ell]^*\mathscr{X}^{+Q})_{\mathrm{red}} \hookrightarrow & ([p^\ell]^*\mathscr{X}^{+Q}) & \xrightarrow{\qquad [p^\ell] \qquad} & & \mathscr{X}^{+Q} \\ & \big\downarrow & & & \big\downarrow \\ & \mathscr{A} & \xrightarrow{\mathrm{Frob}^\ell_{\mathscr{A}/S}} \mathscr{A}^{(p^\ell)} & \xrightarrow{\mathrm{Ver}^\ell} & \mathscr{A} \end{array}$$

where F_S is the absolute Frobenius morphism on S, $\mathscr{A}^{(p^\ell)} = F_S^{\ell,*}\mathscr{A}$ is the base-change of $\mathscr{A}$ by $F_S^{\ell,*}$, $\mathrm{Frob}_{\mathscr{A}/S}$ is the Frobenius morphism relatively to S, and Ver is the Verschiebung (see [Grothendieck et al. 1970a, Exposé $\mathrm{VII_A}$, 4.3] for the latter). The square is cartesian (by definition). By assumption, the morphism Ver is étale. Hence, $\mathrm{Ver}^{\ell,*}(\mathscr{X}^{+Q})$ is a disjoint union of schemes that are integral and smooth over S. Let $\mathscr{X}_1 \hookrightarrow \mathrm{Ver}^{\ell,*}(\mathscr{X}^{+Q})$ be an irreducible component such that $\mathscr{X}_{1,K} \cap \mathrm{Frob}^\ell_{A/K}(A(K))$ is dense. Let $\mathscr{X}_2 := (\mathrm{Frob}^{\ell,*}_{\mathscr{A}/S}(\mathscr{X}_1))_{\mathrm{red}}$ be the corresponding reduced irreducible component.

Now notice that $\mathscr{X}_{2,K}$ is geometrically reduced since $\mathscr{X}_2(K)$ is dense in $\mathscr{X}_{2,K}$ (Lemma 4.7). Furthermore, $\mathscr{X}_2$ is flat over S because it is reduced and dominates S. Hence, $(\mathscr{X}_2)^{(p^\ell)}$ is also flat over S. Furthermore, by its very construction $(\mathscr{X}_{2,K})^{(p^\ell)}$ is reduced since $\mathscr{X}_{2,K}$ is geometrically reduced. Hence, $(\mathscr{X}_2)^{(p^\ell)}$ is reduced [Liu 2002, 4.3.8, p. 137]. Recall that $(\mathscr{X}_2)^{(p^\ell)}$ stands for the base-change of $\mathscr{X}_2$ by $F_S^{\ell,*}$. Notice that we have a commutative diagram

$$\begin{array}{ccc} \mathscr{X}_2 & \xrightarrow{\mathrm{Frob}^\ell_{\mathscr{X}_2/S}} & (\mathscr{X}_2)^{(p^\ell)} \\ \big\downarrow & & \big\downarrow \\ \mathscr{A} & \xrightarrow{\mathrm{Frob}^\ell_{\mathscr{A}/S}} & \mathscr{A}^{(p^\ell)} \end{array}$$

and that $\mathrm{Frob}^\ell_{\mathscr{X}_2/S}$ is bijective. Hence, $(\mathscr{X}_2)^{(p^\ell)}$ is isomorphic to $\mathscr{X}_1$. Now, since F_S is faithfully flat and $\mathscr{X}_2$ is flat over S, we see that $\mathscr{X}_2$ is actually smooth over S because

$\mathscr{X}_1$ is smooth over S. Hence, every point of $\mathscr{X}_2(\bar{k})$ can be lifted to a point in $\mathscr{X}_2(S^{\text{sh}})$ (see for instance [Liu 2002, Corollary 6.2.13, p. 224]). Since the morphism $[p^\ell]$ is finite and flat and the scheme $\mathscr{X}^{+Q}$ is integral, we see that the map $\mathscr{X}_2 \to \mathscr{X}^{+Q}$ is surjective. This implies that the map $\mathscr{X}_2(\bar{k}) \to \mathscr{X}^{+Q}(\bar{k})$ is surjective. We conclude that *every element of* $\mathscr{X}^{+Q}(\bar{k})$ *is liftable to an element in* $\mathscr{X}^{+Q}(S^{\text{sh}}) \cap p^\ell \cdot \mathscr{A}(S^{\text{sh}})$. Since ℓ was arbitrary, this contradicts Theorem 4.1. □

Now we want to conclude by:

Remark 4.8. Buium [1992] also introduces an "exceptional set", which is very similar to the set Exc considered here, and he makes a similar use of it (catching rational points). There is nevertheless one important difference between Buium's and our methods: the proof of Theorem 3.3, which is crucial in our study of the structure of Exc, uses "Galois equations" and not differential equations. In this sense, our techniques also differ from the techniques employed in [Hrushovski 1996], which is close in spirit to [Buium 1992] and where the Galois-theoretic language is not used either.

Remark 4.9. Although Corollary 1.4 shows that the Mordell–Lang conjecture may be reduced to the Manin–Mumford conjecture under the assumptions of Theorem 1.3, the difficulty of circumventing the fact that the underlying abelian variety might not be ordinary (which was a hurdle for some time) is not thus removed. Indeed, the most difficult part of the algebraic-geometric proof of the Manin–Mumford conjecture given in [Pink and Rössler 2004] concerns the analysis of endomorphisms of abelian varieties, which are not globally the composition of a separable isogeny with a power of a relative Frobenius morphism.

Acknowledgments

As many people, I am very much indebted to O. Gabber, who pointed out a flaw in an earlier version of this article and who also suggested a way around it. Many thanks to R. Pink for many interesting exchanges on the matter of this article. I also want to thank M. Raynaud for his reaction to an earlier version of the text and A. Pillay for interesting discussions and for suggesting that the method used in this article should work. Finally, I would also like to thank E. Bouscaren and F. Benoist for their interest and A. Buium for his very interesting observations.

References

[Abramovich and Voloch 1992] D. Abramovich and J. F. Voloch, "Toward a proof of the Mordell–Lang conjecture in characteristic p", *Internat. Math. Res. Notices* 5 (1992), 103–115. MR 94f:11051 Zbl 0787.14026

[Bosch et al. 1990] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) **21**, Springer, Berlin, 1990. MR 91i:14034 Zbl 0705.14001

[Buium 1992] A. Buium, "Intersections in jet spaces and a conjecture of S. Lang", *Ann. of Math.* (2) **136**:3 (1992), 557–567. MR 93j:14055 Zbl 0817.14021

[Buium and Voloch 1996] A. Buium and J. F. Voloch, "Lang's conjecture in characteristic p: an explicit bound", *Compositio Math.* **103**:1 (1996), 1–6. MR 98a:14038 Zbl 0885.14010

[Corpet 2012] C. Corpet, "Around the Mordell–Lang and Manin–Mumford conjectures in positive characteristic", preprint, 2012. arXiv 1212.5193

[Ghioca and Moosa 2006] D. Ghioca and R. Moosa, "Division points on subvarieties of isotrivial semi-abelian varieties", *Int. Math. Res. Not.* (2006), Art. ID 65437, 23. MR 2008c:14058 Zbl 1119.14017

[Grothendieck 1963] A. Grothendieck, *Revêtements étales et groupe fondamental. Fasc. I: Exposés 1 à 5*, vol. 1960/61, Séminaire de Géométrie Algébrique, Institut des Hautes Études Scientifiques, Paris, 1963.

[Grothendieck 1965] A. Grothendieck, "Éléments de géométrie algébrique, IV: Étude locale des schémas et des morphismes de schémas, II", *Inst. Hautes Études Sci. Publ. Math.* 24 (1965), 5–231. MR 33 #7330 Zbl 0135.39701

[Grothendieck et al. 1970a] A. Grothendieck, M. Demazure, M. Artin, J. Bertin, P. Gabriel, M. Raynaud, and J.-P. Serre, "Schémas en groupes, I: Propriétés générales des schémas en groupes", pp. xv+564 in *Séminaire de Géométrie Algébrique* (*SGA 3*) (Bois Marie, France, 1962–1964), edited by M. Demazure and A. Grothendieck, Lecture Notes in Mathematics **151**, Springer, Berlin, 1970. MR 43 #223a Zbl 0207.51401

[Grothendieck et al. 1970b] A. Grothendieck, M. Demazure, M. Raynaud, M. Artin, and J.-P. Serre, "Schémas en groupes, II: Groupes de type multiplicatif, et structure des schémas en groupes généraux", pp. ix+654 in *Séminaire de Géométrie Algébrique* (*SGA 3*) (Bois Marie, France, 1962–1964), edited by M. Demazure and A. Grothendieck, Lecture Notes in Mathematics **152**, Springer, Berlin, 1970. MR 43 #223b Zbl 0209.24201

[Hrushovski 1996] E. Hrushovski, "The Mordell–Lang conjecture for function fields", *J. Amer. Math. Soc.* **9**:3 (1996), 667–690. MR 97h:11154 Zbl 0864.03026

[Hrushovski and Zilber 1996] E. Hrushovski and B. Zilber, "Zariski geometries", *J. Amer. Math. Soc.* **9**:1 (1996), 1–56. MR 96c:03077 Zbl 0843.03020

[Katz 1981] N. Katz, "Serre–Tate local moduli", pp. 138–202 in *Surfaces algébriques* (Orsay, 1976–1978), edited by J. Giraud et al., Lecture Notes in Math. **868**, Springer, Berlin, 1981. MR 83k:14039b Zbl 0477.14007

[Liu 2002] Q. Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics **6**, Oxford University Press, Oxford, 2002. MR 2003g:14001 Zbl 0996.14005

[Matsumura 1989] H. Matsumura, *Commutative ring theory*, 2nd ed., Cambridge Studies in Advanced Mathematics **8**, Cambridge University Press, 1989. MR 90i:13001 Zbl 0666.13002

[Moosa and Scanlon 2010] R. Moosa and T. Scanlon, "Jet and prolongation spaces", *J. Inst. Math. Jussieu* **9**:2 (2010), 391–430. MR 2011d:14019 Zbl 1196.14008

[Pink and Rössler 2004] R. Pink and D. Rössler, "On ψ-invariant subvarieties of semiabelian varieties and the Manin–Mumford conjecture", *J. Algebr. Geom.* **13**:4 (2004), 771–798. MR 2005d:14061 Zbl 1072.14054

[Raynaud 1983a] M. Raynaud, "Around the Mordell conjecture for function fields and a conjecture of Serge Lang", pp. 1–19 in *Algebraic geometry* (Tokyo/Kyoto, 1982), edited by M. Raynaud and T. Shioda, Lecture Notes in Math. **1016**, Springer, Berlin, 1983. MR 85e:11041 Zbl 0525.14014

[Raynaud 1983b] M. Raynaud, "Courbes sur une variété abélienne et points de torsion", *Invent. Math.* **71**:1 (1983), 207–233. MR 84c:14021 Zbl 0564.14020

[Samuel 1966] P. Samuel, "Compléments à un article de Hans Grauert sur la conjecture de Mordell", *Inst. Hautes Études Sci. Publ. Math.* 29 (1966), 55–62. MR 34 #4272 Zbl 0144.20102

[Scanlon 1999] T. Scanlon, "The conjecture of Tate and Voloch on p-adic proximity to torsion", *Internat. Math. Res. Notices* 17 (1999), 909–914. MR 2000i:11100 Zbl 0986.11038

[Scanlon 2005] T. Scanlon, "A positive characteristic Manin–Mumford theorem", *Compos. Math.* **141**:6 (2005), 1351–1364. MR 2006k:03065 Zbl 1089.03030

[Szpiro et al. 1981] L. Szpiro, A. Beauville, M. Deschamps, M. Flexor, R. Fossum, L. Moret-Bailly, and R. Menegaux, *Séminaire sur les pinceaux de courbes de genre au moins deux*, edited by L. Szpiro, Astérisque **86**, Société Mathématique de France, Paris, 1981. MR 83c:14020 Zbl 0463.00009

[Tate and Voloch 1996] J. Tate and J. F. Voloch, "Linear forms in p-adic roots of unity", *Internat. Math. Res. Notices* 12 (1996), 589–601. MR 97h:11065 Zbl 0893.11015

Communicated by Ehud Hrushovski
Received 2012-07-16 Revised 2012-10-26 Accepted 2012-11-23

rossler@math.univ-toulouse.fr *Institut de Mathématiques, Equipe Emile Picard, Université Paul Sabatier, 118 Route de Narbonne, 31062 Toulouse cedex 9, France*
http://www.math.univ-toulouse.fr/~rossler

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2013 is US $200/year for the electronic version, and $350/year (+$40, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 7 No. 8 2013

1937-0652(2013)7:8;1-5