Product of Local Points of Subvarieties of Almost Isotrivial Semi-Abelian Varieties Over a Global Function Field

Chia-Liang Sun
Institute of Mathematics, Academia Sinica, 6F, Astronomy-Mathematics Building, No. 1, Sec. 4, Roosevelt Road, Taipei 10617, Taiwan

Correspondence to be sent to: e-mail: csun@math.sinica.edu.tw

For a semi-abelian variety over a global function field which is isogenous to an isotrivial one, we show that on the product of local points of a subvariety satisfying a minor condition, the topological closure of a finitely generated subgroup of global points cuts out exactly the global points of the subvariety lying in this subgroup. As a corollary, on every non-isotrivial super-singular curve of genus two over a global function field, we conclude that the Brauer–Manin condition cuts out exactly the set of its rational points.

1 Introduction

Let $K$ be a global function field of characteristic $p$, that is, a finitely generated field extension over the prime field $\mathbb{F}_p$ with the transcendence degree 1. We fix an algebraic closure $\overline{K}$ and let $K^s$ denote the separable closure of $K$. Let $\Omega_K$ denote the set of all places of $K$ and let $\Omega$ denote a co-finite subset of $\Omega_K$. For each $v \in \Omega_K$, let $K_v$ denote the completion of $K$ at $v$. For an algebraic variety $X$ defined over $K$, we endow $X(K_v)$ with the natural $v$-adic topology, and then endow $\prod_{v \in \Omega} X(K_v)$ with the product topology. In this paper, we assume that $X$ is a closed subvariety of a given semi-abelian variety $A$, both are defined over $K$. We identify every subset $H \subset A(K)$ as a topological subspace of $\prod_{v \in \Omega} A(K_v)$ by the diagonal embedding, and denote by $\bar{H}$ its topological
closure; moreover, for each \( v \in \Omega_K \), the inclusion \( H \to A(K_v) \) is continuous and therefore induces a subtopology of \( H \), which will be referred to as \( v \)-adic subtopology.

Suppose \( H \) is a subgroup of \( A(K) \). The main aim of this paper is to investigate the circumstances where the equality

\[
\prod_{v \in \Omega} X(K_v) \cap H = X(K) \cap H
\]

holds. To do so, we shall assume that \( H \) is finitely generated, as Example 1 in Section 3.3 shows that the equality would not hold even in the simplest case where \( A = \mathbb{G}_m \), otherwise. On the other hand, the case where \( A \) is an abelian variety and \( H = A(K) \), has been studied by Poonen and Voloch [9]. Indeed, they propose that, in general, the equality

\[
\prod_{v \in \Omega} X(K_v) \cap \overline{A(K)} = \overline{X(K)}
\]

should hold, and they prove (1) under the hypothesis that \( A_K \) has no isotrivial quotient, \( A(K^s)[\mathbb{F}_p] \) is finite and \( X \) is coset-free [9, Conjecture C and Theorem B]. In this paper, we consider the case where \( A \) is isogenous to an isotrivial semi-abelian variety. Recall that in the category of varieties (resp. of semi-abelian varieties), an object defined over \( K \) is isotrivial if it is isomorphic over \( \overline{K} \) to the one defined over \( \mathbb{F}_p \). Our main result is the following:

**Theorem 1.** Let \( X \) be a closed subvariety of a semi-abelian variety \( A \), both are defined over \( K \). Assume that there is an isogeny \( f \) defined over \( \overline{K} \) from \( A \) to a semi-abelian variety \( A_0 \) defined over \( \mathbb{F}_p \) so that each translate \( P + f(X), P \in A_0(\overline{K}) \) of \( f(X) \) contains no positive-dimensional closed subvariety which is \( \mathbb{F}_p \)-rational in \( (A_0)_{\overline{F}_p} \). Then for every finitely generated subgroup \( H \) of \( A(K) \), the set \( X(K) \cap H \) is finite and the equality (1) holds.

Example 2 at the end of Section 4 explains why we cannot expect the conclusion of our main result to hold without any assumption on \( X \). The proof of the theorem consists of two parts which are carried out, respectively, in Sections 3 and 4, with the key ingredients, Proposition 2, Lemmas 9 and 10, proved in Section 5. The first part treats the case where \( X \) is zero-dimensional by adapting the proof of [9, Proposition 3.7] to our situation, whereas the second reduces the general case to the zero-dimensional case by the induction on the dimension of \( X \) using a different Mordell–Lang-type argument. The approach for the second part is originated from the proof of Theorem A. Part 1 in [1].
Suppose $A$ is the Jacobian of $X$ which is embedded into $A$ under an Albanese map induced from a divisor on $A$ defined over $K$ of degree 1. It is proved in [9], Section 4, that if the Tate–Shafarevich group $\text{III}(A)$ of $A$ is finite, then the set $\prod_{v \in \Omega_K} X(K_v) \cap A(K)$ is in bijection with the Brauer set of $X$ over $K$. Therefore, if Theorem 1 holds, then the Brauer–Manin condition cuts exactly the set of its $K$-rational points on $X$. A nonisotrivial projective curve can have its Jacobian isogenous to an isotrivial abelian variety; for example, super-singular curves of genus 2 have this property [7]. The following corollary is proved in Section 4.

**Corollary 1.** On any nonisotrivial projective $K$-curve with its Jacobian isogenous to an isotrivial abelian variety, the Brauer–Manin condition cuts exactly the set of its $K$-rational points.

## 2 Preliminaries

### 2.1

A *variety* over a field $F$ is a geometrically reduced and geometrically irreducible separated $F$-scheme of finite type. For a tower $E \supset L \supset F$ of field extensions and a variety $X$ over $F$, a closed subscheme $Y$ in $X_E$ is *$L$-rational* if it is the base change of a (necessarily unique) closed subscheme $Y'$ of $X_L$. Suppose that $X$ is quasi-projective, and fix an immersion of $X$ into a projective space $\mathbb{P}^N_F$ over $F$. Then there is a radical homogenous ideal $I$ and a homogeneous ideal $J$ in $F[\! [t_0,\ldots,t_N] \! ]$ such that $X$ is the intersection of the zero scheme of $I$ and the complement of the zero scheme of $J$. (The choice of $I$ can be made canonical by using the schematic closure of $X$ in $\mathbb{P}^N_F$, but $J$ is not at all canonical.) In such a situation, a closed subscheme $Y$ in $X_E$ is $L$-rational precisely when there exists a homogeneous ideal $I' \supseteq I$ in $L[\! [t_0,\ldots,t_N] \! ]$ such that $Y$ is the intersection of the zero scheme of $I'$ and the complement of the zero scheme of $J$.

Now let $C$ be the regular projective curve over $k$ with function field $K$. Given a fixed immersion of $X$ into $\mathbb{P}^N_K$ and a choice of its description using $I$ and $J$ as above, or more geometrically, a reduced closed subscheme $V$ in $\mathbb{P}^N_K$ and another closed subscheme $V'$ such that $X = V \cap (\mathbb{P}^N_K - V')$, we take $\mathcal{X} = V \cap (\mathbb{P}^N_C - V')$, where $\mathcal{V}$ and $\mathcal{V}'$ are the schematic closures of $V$ and $V'$ in $\mathbb{P}^N_C$, respectively. Since $C$ is Dedekind, both $\mathcal{V}$ and $\mathcal{V}'$ are $C$-flat, hence $\mathcal{X}$ is a $C$-flat model for $X$ as a locally closed subscheme of $\mathbb{P}^N_C$. In more algebraic terms, since the formation of these closures commutes with localization on $C$, we can describe the pullback of $\mathcal{X}$ over $O_v$ as follows: if $\mathcal{V}$ and $\mathcal{V}'$ are, respectively, defined by the vanishing of the homogeneous ideals $I$ and $J$ then the pullbacks $\mathcal{V}_v$ and $\mathcal{V}'_v$
over $O_v$ are, respectively, defined by the vanishing in $\mathbb{P}^N_{O_v}$ of the saturations $I^{(v)}$ and $J^{(v)}$ of $I$ and $J$ in $O_v[t_0, \ldots, t_N]$, where $I^{(v)}$ (resp. $J^{(v)}$) is just the subset of $I \cap O_v[X_0, \ldots, X_N]$ (resp. $J \cap O_v[X_0, \ldots, X_N]$) consisting of polynomials with some coefficients not in $m_v$. In particular, we see that $X(O_v)$ is given by the following explicit formula:

$$X(O_v) = \left\{ P \in \mathbb{P}^N(K_v) : \begin{array}{l} P = [x_0 : \ldots : x_N] \\
x_i \in O_v \text{ for all } i \\
x_{i_0} \notin m_v \text{ for some } i_0 \\
f(x_0, \ldots, x_N) = 0 \text{ for all } f \in I \\
g(x_0, \ldots, x_N) \notin m_v \text{ for some } g \in J^{(v)} \end{array} \right\}. \quad (2)$$

Likewise, for any finite subset $S \subset \Omega_K$, the set $X(O_S)$ of $O_S$-points of $X$ is given by the explicit formula:

$$X(O_S) = \bigcap_{v \in \Omega_K \setminus S} (X(K) \cap X(O_v)). \quad (3)$$

For ease of notation, we will write $X(O_v)$ and $X(O_S)$ for $X(O_v)$ and $X(O_S)$ when the projective embedding is fixed (as will generally be the case). The following result is easily proved by “denominator-chasing.”

**Lemma 1.** Let $\phi : X \to X$ be a $K$-morphism. Then $\phi$ extends to an $O_S$-endomorphism of $X(O_S)$ for sufficiently large $S$; in particular, $\phi$ preserves $X(O_v)$ for all but finitely many $v$. \hfill $\square$

2.2

The group operations on $A$, given by regular maps defined over $K$, are continuous with respect to the topology on $A(K_v)$, for each $v \in \Omega_K$. This implies that $A(K_v)$ is a Hausdorff topological abelian group. It is totally disconnected since $v$ is nonarchimedean. Also, formula (2) shows that $A(K_v)$ contains $A(O_v)$ as a compact open subset. Consequently, it is locally compact, and hence complete. By Hewitt and Ross [4, Theorem (7.7)], it follows that the topology of $A(K_v)$ is generated by open subgroups, and therefore so are $\prod_{v \in \Omega} A(K_v)$ and its subgroups.

**Lemma 2.** Every finitely generated subgroup $H$ of $A(K)$ admits a Hausdorff subtopology generated by subgroups with finite index. \hfill $\square$
Proof. Because $H$ is finitely generated and $\Omega_K \setminus \Omega$ is finite, there exists a place $v_0 \in \Omega$ such that $A(O_{v_0})$ is a group containing $H$. Since $A(O_{v_0})$ is a compact subgroup of $A(K_{v_0})$ whose topology is Hausdorff and generated by subgroups, the topology of $A(O_{v_0})$ is Hausdorff and generated by subgroups with finite index, and so is the $v_0$-adic subtopology of $H$. ■

Let $\mathfrak{P}(A, X, f; K)$ stand for the statement of Theorem 1.

Lemma 3. Let $A, X, f,$ and $K$ be as in Theorem 1 and let $L/K$ be a finite extension. Then $\mathfrak{P}(A, X, f; L) \Rightarrow \mathfrak{P}(A, X, f; K)$.

Proof. Note that the definition of $\bar{H}$ depends on the choice of $K$. Let $\Omega_L^0$ denote the set of places of $L$ lying above $\Omega$. Consider the natural embeddings

$$H \hookrightarrow \prod_{v \in \Omega} A(K_v) \hookrightarrow \prod_{u \in \Omega_L^0} A(L_u).$$

Since $i$ actually identifies $\prod_{v \in \Omega} A(K_v)$ as a closed subgroup of $\prod_{u \in \Omega_L^0} A(L_u)$, $\bar{H}$ will be remained the same, if $K$ is replaced by $L$. If $\mathfrak{P}(A, X, f; L)$ holds, then $\prod_{w \in \Omega_L^0} X(L_w) \cap \bar{H} = X(L) \cap \bar{H}$ is a finite set. This implies

$$\prod_{v \in \Omega} X(K_v) \cap \bar{H} = \left( \prod_{w \in \Omega_L^0} X(L_w) \cap \prod_{v \in \Omega} A(K_v) \right) \cap \bar{H}$$

$$= \prod_{w \in \Omega_L^0} X(L_w) \cap \bar{H}$$

$$= X(L) \cap H$$

$$= (X(L) \cap A(K)) \cap H$$

$$= X(K) \cap H,$$

which is also a finite set. ■

2.3

In view of Lemma 3, by replacing $K$ by certain finite extension $L$ if necessary, we can assume that $A$ is an extension of an abelian variety $B$ by a split torus $G^n_m$, for some $n \geq 0$. This is actually the definition taken by Serre [12]. Lemma 1 implies that $A(O_v)$ is
a group for all but finitely many \( v \in \Omega_K \). Therefore, if \( S \) is sufficiently large, then \( A(O_S) \) is a subgroup of \( A(K) \). In this case, it is finitely generated. To see this, we may extend \( S \) and assume that the subgroup \( \mathbb{G}_m^n(O_S) \subset A(O_S) \) coincides with \( (O_S^*)^n \). Since \( A(O_S) \) is mapped into \( B(K) \) with \( \mathbb{G}_m^n(O_S) \) as the kernel, the assertion follows from the Mordell–Weil theorem and Dirichlet’s unit theorem. Also, if \( S \) is large enough, then the finitely generated subgroup \( H \) is contained in \( A(O_S) \).

**Lemma 4.** Every isotrivial semi-abelian variety \( A_0 \) is isogenous (over \( \bar{K} \)) to the product \( \mathbb{G}_m^{n_0} \times B_0 \), for some nonnegative integer \( n_0 \), where \( B_0 \) is an abelian variety defined over \( \mathbb{F}_p \). \( \square \)

**Proof.** We may assume that \( A_0 \) is actually defined over \( \mathbb{F}_p \). Then there is a strictly exact sequence (see [12]) \( 1 \rightarrow \mathbb{G}_m^n \rightarrow A_0 \rightarrow B_0 \rightarrow 0 \), in which \( B_0 \) is an abelian variety defined over \( \mathbb{F}_p \). It remains to show that \( A_0 \) is isogenous to \( \mathbb{G}_m^{n_0} \times B_0 \).

Recall that, for any pair \((G, T)\) of commutative algebraic groups, the set of isomorphism classes of commutative algebraic groups \( E \) along with the strictly exact sequence \( 0 \rightarrow T \rightarrow E \rightarrow G \rightarrow 0 \) forms an abelian group \( \text{Ext}(G, T) \) under the Baer sum. In fact, \( \text{Ext} \) is a bifunctor from the category of pairs of commutative algebraic groups to the category of abelian groups [12]. It is routine to check that, for any commutative algebraic group \( E \) representing its class \( [E] \in \text{Ext}(G, T) \), and any positive integer \( m \), there is a natural exact sequence

\[
0 \rightarrow T[m] \rightarrow E \rightarrow E^{(m)} \rightarrow 0
\]  

(4)

defined over an algebraic closure of a field of definition of \( E \), where \( T[m] \) is the algebraic subgroup of \( m \)-torsion points in \( T \), and \( E^{(m)} \) is a commutative algebraic group representing the class \( m[E] \in \text{Ext}(G, T) \). In our case, the isomorphism class \( [A_0] \) of \( A_0 \) lies in \( \text{Ext}(B_0, \mathbb{G}_m^{n_0}) = \text{Ext}(B_0, \mathbb{G}_m)^{n_0} \), where the equality holds because \( \text{Ext} \) is a bifunctor. One knows (e.g., the comments following Theorem 6 of Chapter VII in [12]) that \( \text{Ext}(B_0, \mathbb{G}_m) \) is isomorphic to the dual abelian variety \( B_0' \) of \( B_0 \). In particular, \( [A_0] \) lies in \( (B_0'(\mathbb{F}_p))^{n_0} \) which is a torsion group. Therefore, \( m[A_0] = 0 \), for some \( m \), and hence \( \mathbb{G}_m^{n_0} \times B_0 = A_0^{(m)} \) and the isogeny is provided by (4).

3 **The Zero-Dimensional Case**

In this section, we prove Theorem 1 in the case where \( \text{dim } X = 0 \).
3.1 A uniform filtration over all $v$-adic subtopologies

Suppose $A_0$ is a semi-abelian variety defined over a finite field $\mathbb{F}_q$ containing $\mathbb{F}_p$. Then the Frobenius morphism $\text{Frob} : A_0 \to A_0$ is well defined, and if $A_0$ is embedded as a subvariety of $\mathbb{P}^N$, then $\text{Frob}$ is simply the restriction of the Frobenius map on $\mathbb{P}^N$, sending $[x_0 : \ldots : x_N]$ to $[x_0^q : \ldots : x_N^q]$. Thus, $\text{Frob}$ preserves the group structure on $A_0$ and it induces an injective map $A_0(\mathcal{O}_S) \to A_0(\mathcal{O}_S)$, which we also denote by $\text{Frob}$ which is a group homomorphism, if $A_0(\mathcal{O}_S)$ is a group.

**Proposition 1.** Suppose that $f : A \to A_0$ is an isogenous defined over $\bar{K}$ and $A_0$ is an isotrival semi-abelian variety. Then for any finitely generated subgroup $H$ of $A(K)$, there exists a collection $\{U_n : n \geq 1\}$ of subgroups of $H$ with the following two properties:

1. For each $v \in \Omega_K$ and each $n \geq 1$, $U_n$ is open in every $v$-adic subtopology of $H$.
2. $\bigcap_{n \geq 1} U_n$ is contained in the torsion subgroup of $H$.

**Proof.** Without loss of generality, we may replace $K$ by one of its finite extensions and assume that $f$ is defined over $K$ and $A_0$ is defined over $\mathbb{F}_q \subset K$. Since $H \xrightarrow{f} f(H)$ is continuous with finite kernel, it is sufficient to show that $f(H)$ precesses a family of open sets satisfying the properties correspondingly. Thus, we only need to consider the case where $A = A_0$ and $f$ is the identity map.

We claim that for each $v \in \Omega_K$ and each $n \geq 1$, the subgroup $U_n := \text{Frob}^n(A(K)) \cap H \subset H$ is open in the $v$-adic subtopology. Then, (2) holds, as

$$\bigcap_{n \geq 1} U_n \subset \bigcap_{n \geq 1} \text{Frob}^n(A(K)) \subset A \left( \bigcap_{n \geq 1} K^{p^n} \right)$$

and $\bigcap_{n \geq 1} K^{p^n}$ is the maximal finite subfield of $K$.

To prove the claim, we first note that since there is no nontrivial purely inseparable finite extension of $K$ inside $K_v$, $\text{Frob}^n(A(K_v)) \cap A(K) \subset \text{Frob}^n(A(K))$, and hence $\text{Frob}^n(A(K_v)) \cap H \leq U_n$. Then it remains to show that $\text{Frob}^n(A(K_v)) \cap H$ is open in the $v$-adic subtopology of $H$. It is clear that that $\text{Frob}^n(A(K_v))$ is closed in $A(K_v)$, and consequently the quotient space $A(K_v)/\text{Frob}^n(A(K_v))$ is Hausdorff. Consider the map $H \to A(K_v)/\text{Frob}^n(A(K_v))$ induced from the inclusion $H \subset A(K_v)$. It is continuous with respect to $v$-adic subtopology of $H$. Also, as it factors through $A(\mathcal{O}_S)/\text{Frob}^n(A(\mathcal{O}_S))$, for some finite $S \subset \Omega_K$ such that $H \leq A(\mathcal{O}_S)$, the image of the map is finite, whence discrete. This completes our proof. ■
3.2 Congruence subgroup property

For an additive topological abelian group $G$, we say that $G$ has the **congruence subgroup property** if the subgroup $nG = \{nP : P \in G\}$ is open for every positive integer $n$; if $G$ is finitely generated, then the following conditions are equivalent:

1. $G$ has the congruence subgroup property.
2. Every subgroup of $G$ of finite index is open.
3. Every subgroup of $G$ is closed.

**Lemma 5.** Let $G$ be a finitely generated abelian topological groups. Let $\Sigma$ be a set consisting of natural numbers, which is closed under multiplication, satisfying the condition that every subgroup of $G$ of index in $\Sigma$ is open. Then $\Sigma$ also satisfying the corresponding condition for each subgroup $H$ of $G$, namely, every subgroup of $H$ of index in $\Sigma$ is open in $H$. In particular, if $G$ has the congruence subgroup property, then so has $H$. □

**Proof.** We may assume that each positive divisor of any element in $\Sigma$ also lies in $\Sigma$. Let $m \in \Sigma$ be the product of those natural numbers in $\Sigma$, each of which is the order of some elements in the finitely generated abelian group $G/H$. Then, for every $n \in \Sigma$, we have $H \cap mnG \leq nH$. Since $mn \in \Sigma$, it follows that $mnG$ is open in $G$. This shows that $nH$ is open in $H$ and so is every subgroup of $H$ with index $n$. ■

**Lemma 6.** Suppose that every finitely generated subgroup of $A(K)$ has the congruence subgroup property. Then for any finitely generated subgroup $H$ of $A(K)$ and any subset $J$ of $A(K)$, we have $J \cap \bar{H} = J \cap H$. □

**Proof.** Choose a finite subset $S$ of $\Omega_K$ such that $H \leq A(O_S)$ and $S \cup \Omega = \Omega_K$. Since $A(O_S)$ has the congruence subgroup property, $H$ is closed in $A(O_S)$. Consequently, $A(O_S) \cap \bar{H} = H$. Now, since $A(O_S) = A(K) \cap \bigcap_{v \in \Omega} A(O_v)$, while $A(O_v)$ is closed in $A(K_v)$, $A(O_S)$ is closed in $A(K)$, and hence $A(K) \cap \overline{A(O_S)} = A(O_S)$. This implies $J \cap \bar{H} = J \cap A(K) \cap \overline{A(O_S)} \cap \bar{H} = J \cap A(O_S) \cap \bar{H} = J \cap H$. ■

For any subgroup $J$ of $G := \prod_{v \in \Omega} A(K_v)$, its topological closure $\bar{J}$ is also a subgroup. In fact, since the map $q : G \times G \to G$ defined by $(P, Q) \mapsto P - Q$ is continuous, the preimage $q^{-1}(\bar{J})$ is a closed subset of $G \times G$ containing $J \times J$, and thus contains $\overline{J \times J} = \bar{J} \times \bar{J}$; then $q(\bar{J}, \bar{J}) = \bar{J}$ as desired. The following result generalizes [9, Lemma 3.6].
Lemma 7. If a finitely generated subgroup $H$ of $A(K)$ has the congruence subgroup property, then every torsion element of $\bar{H}$ lies in $H$. \hfill $\Box$

Proof. Write $H = T + F$, where $T$ is a finite subgroup and $F$ is torsion-free. Suppose $a \in \bar{H} \setminus T$ with $ma = 0$ for some nonzero integer $m$. Since $T$ is finite, there exists an open subgroup $U$ of $\prod_{v \in \Omega} A(K_v)$ such that $(T + U) \cap (a + U) = \emptyset$. Since $F$ is of finite index in $H$, by the congruence subgroup property of $H$, we may assume that $U \cap H \subset F$. Lemma 5 says that at least $H$ also has the congruence subgroup property, thus there exists an open subgroup $V$ of $\prod_{v \in \Omega} A(K_v)$ such that $V \cap U \cap H = m(U \cap H)$. Because $ma = 0$, the continuity of the multiplication-by-$m$ map ensures the existence of an open subgroup $W$ of $U$ such that $m(a + W) \subset U \cap V$. Now since $a \in \bar{H}$, there exist $t \in T$ and $f \in F$ such that $t + f \in H \cap (a + W)$. Consequently, $m(t + f) \in m(a + W) \cap H \subset U \cap V \cap H = m(U \cap H)$, whence $m(t + f) = mf'$ for some $f' \in U \cap H \subset F$. Then $mt \in T \cap F = \{0\}$ and $m(f - f') = 0$, which implies $f - f' \in T \cap F = \{0\}$ and $f = f' \in U$. This says $t + f \in (T + U) \cap (a + W) \subset (T + U) \cap (a + U)$, which is impossible. \hfill $\blacksquare$

Suppose $J \subset A(K)$ is a subgroup containing $H$. Then the inclusion $J \to \bar{J}$ canonically induces a group homomorphism

$$J/H \to \bar{J}/\bar{H}. \quad (5)$$

Lemma 8. Suppose every finitely generated subgroup of $A(K)$ has the congruence subgroup property. Let $H \leq J$ be subgroups of $A(K)$. If $H$ is finitely generated, then (5) is injective. If furthermore the index $[J : H]$ is finite, then (5) is actually an isomorphism. \hfill $\Box$

Proof. The first assertion follows from Lemma 6. The congruence subgroup property of $J$ implies that if $[J : H]$ is finite, then $H$ is open in $J$. Thus, $H = U \cap J$, for some open subgroup $U$ of $\prod_{v \in \Omega} A(K_v)$. Let $y$ be an arbitrary point of $\bar{J}$. Then $y \in z + U$ for some $z \in J$, and for any open subgroup $V$ of $U$, $(y - z + V) \cap J \neq \emptyset$. On the other hand, we have

$$(y - z + V) \cap J \subset (y - z + V) \cap (U \cap J) = (y - z + V) \cap H.$$

As the topology of $\prod_{v \in \Omega} A(K_v)$ is generated by subgroups, it follows that $y - z \in \bar{H}$. This shows the surjectivity of (5). \hfill $\blacksquare$

The proof of the following proposition is postponed to Section 5.1.
**Proposition 2.** If $A$ is isogenous to $\mathbb{G}_m^N \times B$ for some nonnegative integer $N$ and some abelian variety $B$ defined over $K$, then every finitely generated subgroup of $A(K)$ has the congruence subgroup property. In particular, the same conclusion holds if $A$ is isogenous to an isotrivial semi-abelian variety defined over $K$. □

### 3.3 The proof

**Proof of Theorem 1 in the case where dim $X = 0$:** We write $X = Z$ to reflect this zero-dimensional situation. As $Z$ is zero-dimensional, by Lemma 3, we may replace $K$ by a finite extension if necessary and assume that every point of $Z$ actually belongs to $Z(K)$. In particular, the restriction $i_v|_{Z(K)}$ of the natural map $A(K) \longrightarrow A(K_v)$ is a bijection.

In view of Lemma 6, we only have to show $\prod_{v \in \Omega} Z(K_v) \cap \tilde{H} \subset Z(K)$. Let $J$ be the subgroup of $A(K)$ generated by $H$ and $Z(K)$. By Proposition 1, there exists a collection $\{U_n: n \geq 1\}$ of subgroups of $J$, which are open in every $v$-adic subtopology, such that $\bigcap_{n \geq 1} U_n$ is contained in the torsion subgroup of $J$. Let $Q = (Q_v)_{v \in \Omega}$, with each $Q_v \in Z(K_v)$, denote an element of $\prod_{v \in \Omega} Z(K_v)$. Suppose $Q$ is also contained in $\tilde{H}$. Then there is a sequence $(P_n)_{n \geq 1} \in H$ such that at each $v$, the sequence $(i_v(P_n))_{n \geq 1}$ has $Q_v$ as its limit point in $A(K_v)$. Write $Q_v = i_v^{-1}(Q_v) \in Z(K)$. Since each $U_n$ is open in the $v$-adic subtopology, for each $r \geq 1$, there exists an $N$ such that $P_n - Q_v \in U_r$, for $n \geq N$. It follows that for every pair $v, w \in \Omega$, the difference $Q_v - Q_w$ belongs to $\bigcap_{r \geq 1} U_r$, whence a torsion point. Since the set $(Q_v)_{v \in \Omega}$ is finite, there exists a nonzero integer $m$ such that $m(Q_v - Q_w) = 0$, for each pair $v$ and $w$. Fix a $w \in \Omega$. Then the difference $Q - Q_w = (Q_v - Q_w)_{v \in \Omega} \in \tilde{H}$ is torsion, and hence, by Proposition 2 and Lemma 7, it is actually contained in $J$. In particular, $Q \in J$ is a global point.

**Example 1.** The conclusion in Theorem 1 would fail, even in the case where dim $X = 0$, if the hypothesis that $H$ is finitely generated were removed. To see this, let $K$ be the field $\mathbb{F}_p(t)$ of rational functions over $\mathbb{F}_p$. Fix a place $v_0$ of $K$ such that $t \notin O_{v_0}$. Let $\alpha, \beta \in K^*$ with $\beta - \alpha = \frac{a}{b}$, where $a, b \in \mathbb{F}_p[t]$. Denote by $Z$ the $K$-subvariety $\{\alpha, \beta\}$ of $\mathbb{G}_m$, and by

$$K^* \longrightarrow K_v^* \quad \text{the natural inclusion. Consider the sequence}$$

$$x_n = \frac{\left(\prod_{i=1}^{n} \pi_i\right)^n + a}{\left(\prod_{i=1}^{n} \pi_i\right)^{2n} + b} + \alpha, \quad (6)$$
where \( \pi_1, \pi_2, \pi_3, \ldots \) are all irreducibles in \( \mathbb{F}_p[t] \). Then the sequence \( (x_n) \) has a limit \( Q = (Q_v)_{v \in \Omega_K} \) in \( \prod_{v \in \Omega_K} K_v^* \), where \( Q_v = i_v(\alpha) \) and \( Q_v = i_v(\beta) \) for every \( v \in \Omega_K \setminus \{v_0\} \), because

\[
x_n - \beta = \frac{(\prod_{i=1}^{n} \pi_i^n)(b - a \prod_{i=1}^{n} \pi_i^n)}{b(\prod_{i=1}^{n} \pi_i^{2n} + b)}.
\]

(i) If \( \alpha \neq \beta \), then \( Q \in \prod_{v \in \Omega_K} Z(K_v) \cap G_\mathbb{F}_m(K) \setminus Z(K) \).
(ii) Suppose \( \alpha = \beta \neq 1 \) and set \( b = 1 \) in (6). Then \( \{x_n : n \geq 1\} \not\subset O_S^* \) for any finite \( S \subset \Omega_K \); hence, by taking a subsequence, we may assume that every nonzero power of \( x_n \) does not belong to the subgroup of \( G_\mathbb{F}_m(K) \) generated by \( \{\alpha, x_1, \ldots, x_{n-1}\} \). Letting \( H \) be the subgroup of \( G_\mathbb{F}_m(K) \) generated by \( \{x_n : n \geq 1\} \), we have \( Q \in \prod_{v \in \Omega_K} Z(K_v) \cap \tilde{H} = Z(K) \cap \tilde{H} \setminus H \). □

4 The Inductive Step

In this section, we complete the proof of Theorem 1 by reducing the general case to the zero-dimensional case which is established in Section 3.3. Focusing on the case where the isogeny \( f \) is the identity map until the very end of the reduction, the following Lemmas 9 and 10 are crucial to our inductive procedure. Their proofs, being long and independent of the rest of the materials in this section, will be postponed until Section 5.2.

**Lemma 9.** Let \( N \) be a nonnegative integer and \( m \) a natural number. For each \( v \in \Omega \), let \( I_v \) be an ideal of \( K_v[X_0, \ldots, X_N] \), generated by elements of \( K_v^{pm}[X_0, \ldots, X_N] \). Then \( \bigcap_{v \in \Omega} (I_v \cap K[X_0, \ldots, X_N]) \) is generated by elements of \( K^{pm}[X_0, \ldots, X_N] \). □

**Lemma 10.** Let \( N \) and \( m \) be nonnegative integers. For each \( v \in \Omega_K \), the ideal generated by those homogeneous polynomials in \( K_v[X_0, \ldots, X_N] \) vanishing on a subset of \( \mathbb{P}^N(K_v^{pm}) \) is actually generated by elements in \( K_v^{pm}[X_0, \ldots, X_N] \). □

Then applications of the above are in order.

**Proposition 3.** Let \( m \) be a natural number. Let \( A_0 \) be a semi-abelian variety defined over the largest finite subfield \( \mathbb{F}_q \subset K \), and \( X \) a closed \( K \)-subvariety which is not \( K^{pm} \)-rational in \( (A_0)_{\mathbb{F}_q} \). Then there is a proper closed \( K \)-subvariety \( Y \) of \( X \) such that \( X(K_v) \cap A_0(K_v^{pm}) \subset Y(K_v) \) for all \( v \in \Omega \). □
Proof. Since $X$ is not $K^{p^n}$-rational in $(A_0)_{\mathbb{F}_q}$, we have an embedding of $A_0$ into some $\mathbb{P}^N$ so that its underlying variety is

$$\left\{ P \in \mathbb{P}^N(\overline{K}) : \begin{array}{l} f(P) = 0 \text{ for all } f \in I \\ g(P) \neq 0 \text{ for some } g \in J \end{array} \right\}$$

for some homogeneous ideals $I$ and $J$ in $\mathbb{F}_q[X_0, \ldots, X_N]$, and that $X$ is defined by (7) except $I$ is replaced by a homogeneous radical ideal $I_X$ in $\overline{K}[X_0, \ldots, X_N]$ generated by elements of $K[X_0, \ldots, X_N]$, but not by those of $K^{p^n}[X_0, \ldots, X_N]$. For each $v \in \Omega$, consider the ideal $\tilde{I}_v$ in $K_v[X_0, \ldots, X_N]$ generated by homogeneous polynomials vanishing on the subset $X(K_v) \cap A_0(K^{p^n})$ of $\mathbb{P}^N(K_v)$. Let $Y$ be the closed subvariety of $A_0$ given by (7) except $I$ is replaced by the homogeneous ideal

$$I_Y := \left( \bigcap_{v \in \Omega} (\tilde{I}_v \cap K[X_0, \ldots, X_N]) \right) \cap K^{p^n}[X_0, \ldots, X_N].$$

Thus, $X(K_v) \cap A_0(K^{p^n}) \subset Y(K_v)$ for all $v \in \Omega$. We shall show $Y \subset X$ by showing

$$I_X \subset \overline{K}[X_0, \ldots, X_N] \cdot I_Y.$$  \hspace{1cm} (8)

To do so, we first apply Lemma 10 to deduce that $\tilde{I}_v$ is generated by elements in $K_v^{p^n}[X_0, \ldots, X_N]$. Then, by Lemma 9, we conclude that $\bigcap_{v \in \Omega} (\tilde{I}_v \cap K[X_0, \ldots, X_N])$ is generated by elements in $K^{p^n}[X_0, \ldots, X_N]$, and that the right-hand side of (8) equals to $\overline{K}[X_0, \ldots, X_N] \cdot \bigcap_{v \in \Omega} (\tilde{I}_v \cap K[X_0, \ldots, X_N])$. Since $I_X$ is not generated by elements of $K^{p^n}[X_0, \ldots, X_N]$, it proves (8). \hfill \blacksquare

**Proposition 4.** Let $A_0$ be a semi-abelian variety defined over the largest finite subfield $\mathbb{F}_q \subset K$, and $X$ be a positive-dimensional closed $K$-subvariety of $A_0$ such that all the largest dimensional irreducible components of the translates $X + P$, $P \in A_0(\overline{K})$, are not $\overline{F}_p$-rational in $(A_0)_{\mathbb{F}_q}$. Let $H$ be a finitely generated subgroup of $A_0(K)$, then there exists a closed $K$-subvariety $Y$ of $X$ with a smaller dimension, satisfying $\prod_{v \in \Omega} X(K_v) \cap \tilde{H} \subset \prod_{v \in \Omega} Y(K_v)$. \hspace{1cm} \Box

**Proof.** Let $\text{Frob} : A_0 \to A_0$ be the Frobenius endomorphism. By taking $H_0 = A_0(O_S)$ for some large enough finite $S \subset \Omega_K$, we assert that that there is a finitely generated subgroup $H_0$ of $A_0(K)$ such that $H \leq H_0$ and $\text{Frob}(H_0) \leq H_0$. Since $\prod_{v \in \Omega} X(K_v) \cap \tilde{H} \subset$
Theorem A. Part 1 in [1] using the Hilbert scheme associated to equivalent compactification of $A_0$, and conclude that there is a positive integer $N$ such that for every $\gamma \in H$ the translate $X_\gamma = X - \gamma$ is not $K^{p^N}$-rational in $(A_0)_{F_q}$. Therefore, Proposition 3 implies that there is a proper closed $K$-subvariety $Y_\gamma$ of $X_\gamma$ such that $X_\gamma(K_v) \cap A(K_v^{p^N}) \subset Y_\gamma(K_v)$ for all $v \in \Omega$.

Since the Frobenius endomorphism gives rise to an injection $H \xrightarrow{\text{Frob}^N} H$, the index $[H : \text{Frob}^N(H)]$ is finite, and hence Lemma 8 implies that there are finitely many $\alpha_i$'s in $H$ such that $H = \bigcup_i (\alpha_i + \overline{\text{Frob}^N(H)})$. Now, $Y_{\alpha_i} + \alpha_i$ is a proper closed $K$-subvariety of $X$ such that $X(K_v) \cap (\alpha_i + A_0(K_v^{p^N})) \subset (Y_{\alpha_i} + \alpha_i)(K_v)$ for all $v \in \Omega$. Then, we prove the proposition by taking $Y = \bigcup_i (Y_{\alpha_i} + \alpha_i)$.

In general, write $X = X_1 \cup \cdots \cup X_m \cup \cdots \cup X_{m+n}$ where each $X_i$ is irreducible and $\dim X_j = \dim X$, for $j = 1, \ldots, m$; $\dim X_i < \dim X$, for $i = m+1, \ldots, m+n$. Then, for $j = 1, \ldots, m$, choose a closed proper $K$-subvariety $Y_j$ of $X_j$ satisfying $X_j(K_v) \cap H \subset Y_j(K_v)$ for all $v \in \Omega$. For $i = m+1, \ldots, m+n$, simply put $Y_i = X_i$. Then, we complete the proof by taking $Y = \bigcup_i^{m+n} Y_i$.

Proof of Theorem 1. In view of Lemma 3, we may assume that the isogeny $f: A \to A_0$ is defined over $K$, that $A_0$ is defined over some finite subfield of $K$, and that every point in the kernel of $f$ lies in $A(K)$. If $\dim X = 0$, then the theorem is proved in Section 3.3. In general, we prove by the induction on $\dim X$.

Write $X_0 = f(X)$. Proposition 4 applied to $A_0$ ensures the existence of a closed $K$-subvariety $Y_0$ of $X_0$ of smaller dimension such that

$$\prod_{v \in \Omega} X_0(K_v) \cap \overline{f(H)} \subset \prod_{v \in \Omega} Y_0(K_v).$$

Write $Y = f^{-1}(Y_0) \cap X$. Then the above implies

$$\prod_{v \in \Omega} X(K_v) \cap \overline{H} \subset \prod_{v \in \Omega} X(K_v) \cap \prod_{v \in \Omega} f^{-1}(Y_0)(K_v) = \prod_{v \in \Omega} Y(K_v).$$

The assumption in Theorem 1 is preserved when $X$ is replaced by $Y$, hence the induction hypothesis implies that $Y(K) \cap H$ is finite and

$$\prod_{v \in \Omega} Y(K_v) \cap \overline{H} = Y(K) \cap H.$$
Therefore,
\[
\prod_{v \in \Omega} X(K_v) \cap \tilde{H} \subset Y(K) \cap H \subset X(K) \cap H \subset \prod_{v \in \Omega} X(K_v) \cap \tilde{H}.
\]

This completes the proof. ■

In order to deduce Corollary 1 from Theorem 1, we need the following result.

**Lemma 11.** Let \( C_1 \to C \to C_0 \) be a chain of nonconstant maps between projective curves defined over \( \overline{K} \) with \( C \) smooth. Suppose that both \( C_0 \) and \( C_1 \) as well as the composition \( C_1 \to C_0 \) are defined over \( \mathbb{F}_p \). Then \( C \) is also defined over \( \mathbb{F}_p \). □

**Proof.** The given chain of maps induces the following diagram of their function fields:

\[
\begin{array}{ccc}
\mathbb{F}_p(C_1) & \longrightarrow & \tilde{K}(C_1) \\
\downarrow & & \downarrow \\
\mathbb{F}_p(C_0) & \longrightarrow & \tilde{K}(C_0)
\end{array}
\]

where both columns are finite extensions, and the maps in both rows are \( \otimes_{\mathbb{F}_p} \tilde{K} \). To prove this lemma, since \( C \) is smooth, it suffices to find a field \( F \) with transcendence degree 1 over \( \mathbb{F}_p \) such that \( F \otimes_{\mathbb{F}_p} \tilde{K} \) is \( \tilde{K} \)-isomorphic to \( \tilde{K}(C) \). First, we assume that \( \mathbb{F}_p(C_1) \) is separable over \( \mathbb{F}_p(C_0) \). Let \( N \) be the normal closure of \( \mathbb{F}_p(C_1) \) over \( \mathbb{F}_p(C_0) \). Identifying all fields involved as subfields of \( N \otimes_{\mathbb{F}_p} \tilde{K} \), we take \( F = N \cap \tilde{K}(C) \). Galois theory shows that \( [N \otimes_{\mathbb{F}_p} \tilde{K} : \tilde{K}(C)] = [N : F] \). Since \( F \otimes_{\mathbb{F}_p} \tilde{K} \subset \tilde{K}(C) \) and \( [N \otimes_{\mathbb{F}_p} \tilde{K} : F \otimes_{\mathbb{F}_p} \tilde{K}] \leq [N : F] \), we conclude that \( F \otimes_{\mathbb{F}_p} \tilde{K} = \tilde{K}(C) \) as desired.

In the general case, let \( L \) be the separable closure of \( \mathbb{F}_p(C_0) \) in \( \mathbb{F}_p(C_1) \). The preceding argument yields a field \( F' \) with transcendence degree 1 over \( \mathbb{F}_p \) such that \( F' \otimes_{\mathbb{F}_p} \tilde{K} \) is \( \tilde{K} \)-isomorphic to \( \tilde{K}(C) \cap (L \otimes_{\mathbb{F}_p} \tilde{K}) \). Since \( \tilde{K}(C) \) is purely inseparable over \( \tilde{K}(C) \cap (L \otimes_{\mathbb{F}_p} \tilde{K}) \), the property of the Frobenius map shows that \( \tilde{K}(C) \cap (L \otimes_{\mathbb{F}_p} \tilde{K}) = \tilde{K}(C)^q \) for some power \( q \) of \( p \), and since \( \mathbb{F}_p \) is perfect, the field \( F = F'^{1/4} \) is the one we look for. ■

**Proof of Corollary 1.** Let \( X \) be a nonisotrivial smooth projective \( K \)-curve with its Jacobian \( J \) isogenous to an isotrivial abelian variety \( A_0 \). Without loss of generality, we...
can assume that $A_0$ is defined over $\overline{\mathbb{F}}_p$. Denote by $f: J \to A_0$ the isogeny and by $\tilde{f}: A_0 \to J$ its dual. Let $m$ be the positive integer such that $f \circ \tilde{f}$ is the multiplication-by-$m$ map on $A_0$, and $\tilde{f} \circ f$ is the multiplication-by-$m$ map on $J$. In view of the discussion given in Section 1, we need to show that $\text{III}(J)$ is finite and each translate $f(X) + P$, $P \in A_0(\overline{\mathbb{K}})$ is not $\mathbb{F}_p$-rational.

Now, since $A_0$ is isotrivial, $\text{III}(A_0)$ is finite, by Tate [13]. Choose a prime $l$ not dividing $pm$. The isogenies $f$ and $\tilde{f}$ induce a chain

$$\text{III}(J)[l^\infty] \to \text{III}(A_0)[l^\infty] \to \text{III}(J)[l^\infty]$$

of maps between the $l$-primary part of $\text{III}(J)$ and of $\text{III}(A_0)$ such that the composition is an isomorphism. In particular, $\text{III}(A_0)[l^\infty] \to \text{III}(J)[l^\infty]$ is surjective, hence $\text{III}(J)[l^\infty]$ is finite as $\text{III}(A_0)[l^\infty]$ is. By another result of Tate [13], it follows that $\text{III}(J)$ is finite as desired.

Suppose $C_0 := f(X) + P$ is $\overline{\mathbb{F}}_p$-rational in $A_0$. Write $C = X + Q$, for some $Q \in f^{-1}(P)$ and let $C_1$ be an irreducible component of the pre-image of $C_0$ under $A_0 \xrightarrow{m} A_0$. Then Lemma 11 is applicable to the chain $C_1 \xrightarrow{\tilde{f}} C \xrightarrow{f} C_0$. Consequently, $C$ is defined over $\overline{\mathbb{F}}_p$, and hence $X$, being isomorphic to $C$, is isotrivial. This is a contradiction. 

**Example 2.** The conclusion in Theorem 1 would fail if no hypothesis were put on $X$. To see this, let $K$ be the field $\mathbb{F}_p(t)$ of rational functions over $\mathbb{F}_p$, and $H = \langle t \rangle$ be the cyclic subgroup of $\mathbb{G}_m(K)$ generated by $t$. Take a cofinite subset $\Omega$ of $\Omega_K$ such that $t \in O_v^*$ for every $v \in \Omega$. For any $m \geq n$, we have

$$t^{p^n} - t^{p^m} = (t^{p^n p^{m-1}} - t)^{p^m}.$$ 

Thus, the sequence $(t^{p^m})_{m \geq 1}$ in $H$ is Cauchy, and admits a limit $Q = (Q_v)_{v \in \Omega} \in \tilde{H}$ by compactness. Note that $Q_{v_{t-1}} = 1$, where $v_{t-1} \in \Omega$ is the unique one satisfying $t - 1 \in m_{v_{t-1}}$; while $Q_v \neq 1$ for each $v \in \Omega \setminus \{v_{t-1}\}$. Hence $Q \in \prod_{v \in \Omega} \mathbb{G}_m(K_v) \cap \tilde{H} \setminus \mathbb{G}_m(K)$. 

5 The proofs of key intermediate results

5.1 The proof of Proposition 2

In this section, we fix a finitely generated subgroup $H \subset A(K)$. The number field counter part of the following lemma (for $\Omega$ consisting of only non-Archimedean places) is just a
reinterpretation of Chevalley [2, Theorem 1], and it can actually be carried over to the function field case. I thank the referee for pointing out the present much shorter proof using Galois cohomology.

**Lemma 12.** If \( A = \mathbb{G}_m \), then every subgroup of \( H \) of index prime to \( p \) is open. \( \square \)

**Proof.** In view of Lemma 5, we only need to consider the case where \( H = \mathbb{G}_m(O_T) = O_T^* \) for a finite \( T \subset \Omega_K \). For any finite subset \( S \subset \Omega \), consider the open subgroup \( U_S = \prod_{v \in S} 1 + m_v \) of \( \prod_{v \in S} K_v^* \). We shall prove the lemma by showing that for any natural number \( m \) prime to \( p \), there is some \( U_S \) such that \( O_T^* \cap U_S \subset (O_T^*)^m \).

Now, Kummer theory gives rise to the following commutative diagram:

\[
\begin{array}{ccc}
O_T^*/(O_T^*)^m & \rightarrow & K^*/(K^*)^m \\
\downarrow & & \downarrow \\
\prod_{v \in \Omega} O_v^*/(O_v^*)^m & \rightarrow & \prod_{v \in \Omega} K_v^*/(K_v^*)^m \\
\downarrow & & \downarrow \\
\prod_{v \in \Omega} H^1(K_v, \mu_m) & \rightarrow & \prod_{v \in \Omega} H^1(K_v, \mu_m)
\end{array}
\]

where the two injections are clear. As the Galois group of \( K(\mu_m)/K \) is cyclic, by Milne [6, Lemma I.9.3], the right vertical arrow is an injection, and hence so is the left one. Since \( O_T^*/(O_T^*)^m \) is finite, there exists a finite subset \( S \subset \Omega \) such that the left vertical arrow induces an injection \( O_T^*/(O_T^*)^m \hookrightarrow \prod_{v \in S} O_v^*/(O_v^*)^m \). Hensel’s lemma shows \( U_S \subset \prod_{v \in S} (O_v^*)^m \), whence \( O_T^* \cap U_S \subset (O_T^*)^m \) as desired. \( \square \)

**Lemma 13.** If \( A = \mathbb{G}_m \), then every subgroup of \( H \) of \( p \)-power index is open in the \( v \)-adic subtopology, for every \( v \in \Omega_K \). \( \square \)

**Proof.** Again, by Lemma 5, we only need to consider the case where \( H = O_T^* \). Now, we have \( (O_T^*)^{m} = O_T^* \cap (K^*)^{m} \), which is shown in the proof of Proposition 1 to be an open subgroup in \( O_T^* \) in the \( v \)-adic subtopology, for every \( v \in \Omega_K \). \( \square \)

**Corollary 2.** If \( A = \mathbb{G}_m^N \), then every finitely generated subgroup of \( A(K) \) has the congruence subgroup property. \( \square \)

In the case where \( A \) is an abelian variety, the first assertion of Proposition 2 is essentially proved by Milne, who generalizes a result of Serre [11] in the case where \( K \) was a number field.
Proposition 5. Suppose that \( A \) is an abelian variety defined over \( K \). Then every subgroup \( H \) of \( A(K) \) has the congruence subgroup property. □

Proof. The case where \( H = A(K) \) is exactly [5, Corollary 1]. Then other cases follow from Lemma 5. ■

Proof of Proposition 2. Let \( H \) be a finitely generated subgroup of \( A(K) \). We need to show that \( nH \subset H \) is open for every \( n \). Suppose we are given the isogeny \( \phi: A \to \mathbb{G}_m^N \times B \).

It follows from Corollary 2 and Proposition 5 that \( \phi(H) \) has the congruence subgroup property. In particular, \( mn\phi(H) \subset \phi(H) \) is an open subgroup, for every \( m \). Denote

\[
T = \ker \left[ A(K) \xrightarrow{\phi} \mathbb{G}_m^N(K) \times B(K) \right].
\]

Since \( T \) is finite, Lemma 2 implies the existence of an open subgroup \( U \) of \( H \) of a finite index \( m \) such that \( U \cap T \) is trivial.

Now, since \( nmH + T = \phi^{-1}(nm\phi(H)) \) is open in \( H + T = \phi^{-1}(\phi(H)) \), the subgroup \( H \cap (nmH + T) \) is open in \( H \). Also, since \( nmH \subset mH \subset U \) and \( U \cap T \) is trivial, we see that \( U \cap (nmH + T) = nmH \). Therefore, \( nmH \) is open in \( H \), and thus so is \( nH \). ■

5.2 The proofs of Lemmas 9 and 10

Our tool for proving Lemmas 9 and 10 is the iterative derivation. An iterative derivation on a field \( L \) is a sequence \( \{D^{(i)}\}_{i \geq 0} \) of elements in the \( L \)-algebra of additive endomorphisms on \( L \) such that

(i) \( D^{(0)} \) is the identity operator.

(ii) \( D^{(i)}(xy) = \sum_{j=0}^{i} D^{(j)}(x)D^{(i-j)}(y) \), for \( i \geq 0 \) and \( x, y \in L \).

(iii) \( D^{(i)}D^{(j)} = \binom{i+j}{i} D^{(i+j)} \) for \( i, j \geq 0 \), where \( D^{(i)}D^{(j)} \) denotes the composition of \( D^{(i)} \) and \( D^{(j)} \), and the rational integer \( \binom{i+j}{i} \) is the binomial coefficient.

Assume that \( L \) is of characteristic \( p \). Then the following Lucas’s lemma (see, e.g., [10]), is useful for telling if \( \binom{i+j}{i} \neq 0 \) in \( L \). For each nonnegative integer \( i \), let \( i = \sum_{n=0}^{d} i_np^n \), \( 0 \leq i_n < p \), denote its base \( p \) expansion.

Lemma 14. The binomial coefficient \( \binom{i}{j} \) is not divisible by \( p \) if and only if \( i_n \geq j_n \) for all \( n \). □
The defining property (iii) implies \( D^{(i)} \circ D^{(j)} = D^{(j)} \circ D^{(i)} \). Also, repeated applications of the property (iii) gives

\[
\prod_{n=0}^{d} (D^{(p^n)})^{i_n} = c_i D^{(i)},
\]

where

\[
c_i = \prod_{n=0}^{d} \left[ \left( \sum_{s=0}^{n} i_s p^s \right) \prod_{a=1}^{i_n} \left( a p^n \right) \right].
\]

Now, Lemma 14 implies \( c_i \in L^* \), and hence

\[
D^{(i)} = c_i^{-1} \cdot \prod_{n=0}^{d} (D^{(p^n)})^{i_n}.
\]

(9)

Inspired by the proof of Ogus [8, Claim 2.2.3], we consider the operator

\[
\Delta_m := \sum_{i=0}^{p^m-1} (-t)^i D^{(i)}
\]
on \( L \) for some \( t \in L \) satisfying

\[
D^{(i)}((-t)^j) = (-1)^i \binom{j}{i} t^{j-i} \quad \text{for each } i, j \geq 0.
\]

(10)

For each \( m \geq 0 \), let \( L_m = \{ x \in L : D^{(l)}(x) = 0, \text{ if } 1 \leq l < p^m \} \), which is a subfield of \( L \).

**Lemma 15.** For every \( c \in L \) and every \( m \geq 0 \), the element \( \Delta_m(c) \in L_m \).

**Proof.** In view of (9), we only need to show that for every natural number \( s < m \),

\[
D^{(p^s)}(\Delta_m(c)) = 0.
\]

For simplicity, set \( j = p^s \). It follows from property (iii) and assumption (10) that

\[
D^{(j)}(\Delta_m(c)) = \sum_{i=0}^{p^m-1} \sum_{l=0}^{j} (-1)^i \binom{i}{l} \binom{i+j-l}{i} (-t)^{i-l} D^{(i+j-l)}(c).
\]
Lemma 14 implies that \(\binom{i+j-l}{i}\) is a multiple of \(p\) unless both \(i_n \geq l_n\) and \(j_n \geq l_n\) hold for all \(n\), which occurs only when \(l \in \{0, j\}\), since \(j_s = 1\) and \(j_n = 0\) for all \(n \neq s\). We also note that in case where \(l = j\), those terms with \(i < j\) vanish as \(\binom{i}{j} = 0\). Putting these together, we obtain

\[
D^{(j)}(\Delta_m(c)) = \sum_{i=0}^{p^m-1} \binom{i+j}{i} (-t)^i D^{(i+j)}(c) + \sum_{i=0}^{p^m-1} (-1)^j \binom{i}{j} (-t)^{i-j} D^{(i)}(c)
\]

\[
= \sum_{i=j}^{j+p^m-1} \binom{i}{j} (-t)^{i-j} D^{(i)}(c) + \sum_{i=j}^{p^m-1} (-1)^j \binom{i}{j} (-t)^{i-j} D^{(i)}(c)
\]

\[
= \sum_{i=p^m}^{p^m+p^s-1} \binom{i}{p^s} (-t)^{i-p^s} D^{(i)}(c),
\]

where the last equality holds because \(1 + (-1)^j = 1 + (-1)^p = 0\) in \(K\). Finally, since \(s < m\), for every \(i\) satisfying \(p^m \leq i \leq p^m + p^s - 1\), we have \(i_s = 0\), and hence \(\binom{i}{p^s}\) is a multiple of \(p\), by Lemma 14. Thus, each term in the last sum vanishes. This finishes the proof. ■

For each \(i \geq 0\), we extend \(D^{(i)}\) to an additive endomorphism on the polynomial ring \(L[X_0, \ldots, X_N]\) by sending \(X_i\) to 0 for every \(i \in \{0, 1, \ldots, N\}\). It is easy to verify that for all \(i \geq 0\), \(f, g \in L[X_0, \ldots, X_N],\)

\[
D^{(i)}(fg) = \sum_{j=0}^{i} D^{(j)}(f) D^{(i-j)}(g),
\]

and, for all \(m \geq 0\),

\[
L_m[X_0, \ldots, X_N] = \{g \in L[X_0, \ldots, X_N]: D^{(i)}(g) = 0, \text{ if } 1 \leq i < p^m\}.
\]

**Lemma 15.** For any positive integer \(m\), an ideal \(I\) of \(L[X_0, \ldots, X_N]\) is generated by elements of \(L_m[X_0, \ldots, X_N]\) if and only if the condition \(D^{(i)}(I) \subseteq I\) holds for all \(1 \leq i < p^m\).

**Proof.** Suppose \(D^{(i)}(I) \subseteq I\) for all \(1 \leq i < p^m\). Let \(J\) be the ideal of \(L[X_0, \ldots, X_N]\) generated by \(I \cap L_m[X_0, \ldots, X_N]\). To complete the proof, we only need to show \(I = J\), as the implication in the opposite direction is clear. Choose a lexicographic order on the set of monomials in \(X_0, \ldots, X_N\). With respect to this order, for each nonzero polynomial \(f \in K[X_0, \ldots, X_N]\), the degree of \(f\) is defined to be the largest monomial appearing in the expression of \(f\) with a nonzero coefficient, and \(f\) is monic if this coefficient is 1.
Suppose that $I \setminus J$ is a nonempty set and let $f \in I \setminus J$ be an element of the smallest degree. We also choose $f$ to be monic. Since $D^{(i)}(1) = 0$, for all positive integer $i$, the degree of $D^{(i)}(f)$ is smaller than that of $f$. Consequently, $D^{(i)}(f) \not\in I \setminus J$, by the choice of $f$. On the other hand, since for every $1 \leq i < p^m$, $D^{(i)}(f) \in D^{(i)}(I) \subset I$, we must have $D^{(i)}(f) \in J$. Now, consider the element

$$g = f + \sum_{i=1}^{p^m-1} (-t)^i D^{(i)}(f) \in L[X_0, \ldots, X_N].$$

By the above argument, $g \in I$, and by Lemma 15, $g \in L_m[X_0, \ldots, X_N]$. Hence, $g \in J$ and $f = g - \sum_{i=1}^{p^m-1} (-t)^i D^{(i)}(f) \in J$, a contradiction. ■

Now we construct a desired iterative derivation on $K$. Choose an element $t \in K$ such that $K$ is a finite separable extension of the function field $\mathbb{F}_p(t)$ of one variable over $\mathbb{F}_p$. Choose a place $v_0 \in \Omega_K$ which restricts to a place $w \in \Omega_{\mathbb{F}_p(t)}$ corresponding to a separable irreducible polynomial in $\mathbb{F}_p[t]$ such that $\mathbb{F}_p(t)_w = K_{v_0}$. Let $\alpha$ be a root of this polynomial. Then $\mathbb{F}_p(t)_w$ is a natural subfield of $\mathbb{F}_p((t - \alpha))$ and we have a tower $\mathbb{F}_p((t - \alpha)) \subset K(\alpha) \subset \mathbb{F}_p((t - \alpha))$ of fields. By Remark 1 in [3], there exists an iterative derivation $\{D^{(i)}_{K(\alpha)}\}_{i \geq 0}$ on $K(\alpha)$ such that $D^{(j)}_{K(\alpha)}(t - \alpha)^i = (i/j)(t - \alpha)^{i-j}$ and $(K(\alpha))^{p^m} = \{x \in K(\alpha) : D^{(l)}_{K(\alpha)}(x) = 0, \text{ for } 1 \leq l < p^m\}$, for $i, j, m \geq 0$. Denoting by $D^{(i)}_K$ the restriction of $D^{(i)}_{K(\alpha)}$ on $K$, we obtain an iterative derivation $\{D^{(i)}_K\}_{i \geq 0}$ on $K$. It is not hard to check that $D^{(j)}_K(t^i) = (i/j)(t)^{i-j}$, whence (10) holds for $D = D_K$. Also, from the separability assumption, we have $K^{p^m} = \{x \in K : D^{(l)}_K(x) = 0, \text{ for } 1 \leq l < p^m\}$, for $m \geq 0$. Moreover, using the fact $[K : K^p] = p$, one can show that for each $i$, the endomorphism $D^{(i)}_K$ is continuous with respect to every place of $K$. Therefore, for each place $v \in \Omega$, we extend $\{D^{(i)}_K\}_{i \geq 0}$ and obtain an iterative derivation $\{D^{(i)}_K\}_{i \geq 0}$ on $K_v$.

**Proof of Lemma 9.** Since $I_v$ is generated by elements of $K_v^{p^m}[X_0, \ldots, X_N]$, which lie in the kernel of those $D^{(i)}_K$ with $1 \leq i < p^m$, it follows that for these $i$ we have $D^{(i)}_K(I_v) \subset I_v$ for each $v \in \Omega$. But then

$$D^{(i)}_K \left( \bigcap_{v \in \Omega} (I_v \cap K[X_0, \ldots, X_N]) \right) \subset \bigcap_{v \in \Omega} (D^{(i)}_K(I_v) \cap K[X_0, \ldots, X_N])$$

$$\subset \bigcap_{v \in \Omega} (D^{(i)}_K(I_v) \cap K[X_0, \ldots, X_N])$$

$$\subset \bigcap_{v \in \Omega} (I_v \cap K[X_0, \ldots, X_N])$$

for all $1 \leq i < p^m$. Then we complete the proof by applying Lemma 16. ■
Proof of Lemma 10. Fix a subset \( \Sigma \) of \( \mathbb{P}^N(K_v^{\mathbb{P}^m}) \) for some place \( v \in \Omega_K \) and some positive integer \( m \), and denote by \( I_v \) the ideal in \( K_v[X_0, \ldots, X_N] \) generated by homogeneous polynomials which vanish on \( \Sigma \). Let \( f \in I_v \) be a homogeneous polynomial and \( P \in \Sigma \). By the definition of \( D^{(i)}_K(f) \) and the assumption \( P \in \mathbb{P}^N(K_v^{\mathbb{P}^m}) \), we have \( 0 = D^{(i)}_K(f(P)) = D^{(i)}_K(f)(P) \) for each \( 1 \leq i < p^m \). This shows \( D^{(i)}_K(I_v) \subset I_v \) for all \( 1 \leq i < p^m \). Again, we complete the proof by using Lemma 16. 


Acknowledgement

I thank the referee for his/her careful comments on an earlier version of this paper, which generalizes a part of my dissertation completed under the advise of José Felipe Voloch; I am also thankful that Brian Conrad helped me rewrite Section 2.1 in terms of modern algebro-geometric terminology. Also, I appreciate the conversations with Ming-Lun Hsieh, Andreas Schweizer, Ki-Seng Tan, and Julie Wang during my revision. My special thanks to Tan for showing me examples of succinct writing.


Funding

While completing this work, C.-L.S. was supported by (i) the doctoral program in Department of Mathematics in the University of Texas, (ii) Government scholarship for studying abroad from the Ministry of Education of Taiwan, (iii) a special scholarship from Ms K in Taiwan, and (iv) Postdoctoral fellowship from Institute of Mathematics, Academia Sinica, Taiwan.


References

[1] Abramovich, D. and J. F. Voloch. “Toward a proof of the Mordell–Lang conjecture in characteristic \( p \).” International Mathematics Research Notices, no. 5 (1992): 103–15.
[2] Chevalley, C. “Deux théorèmes d’arithmétique.” Journal of the Mathematical Society of Japan 3 (1951): 36–44.
[3] García, A. and J. F. Voloch. “Wronskians and linear independence in fields of prime characteristic.” Manuscripta Mathematica 59, no. 4 (1987): 457–69.
[4] Hewitt, E. and K. A. Ross. Abstract Harmonic Analysis, vol. 1. New York: Springer, 1979.
[5] Milne, J. S. “Congruence subgroups of abelian varieties.” Bulletin des Sciences Mathématiques. Second Series 96 (1972): 333–8.
[6] Milne, J. S. Arithmetic Duality Theorems, 2nd ed. Charleston, SC: BookSurge, LLC, 2006.
[7] Moret-Bailly, L. “Familles de courbes et de variétés abéliennes sur \( \mathbb{P}^1 \).” Séminaire sur les pinceaux de courbes de genre au moins deux, Astérisque 86 (1981): 109–40.
[8] Ogus, A. “\( F \)-crystals and Griffiths Transversality.” In Proceedings of the International Symposium on Algebraic Geometry (Kyoto University, Kyoto, 1977), 15–44. Tokyo: Kinokuniya Book Store, 1978.
[9] Poonen, B. and J. F. Voloch. “The Brauer–Manin obstruction for subvarieties of abelian varieties over function fields.” *Annals of Mathematics. Second Series* 171, no. 1 (2010): 511–32.

[10] Schmidt, F. K. “Die Wronskische Determinante in beliebigen differenzierbaren Funktionenkörpern.” *Mathematische Zeitschrift* 45, no. 1 (1939): 62–74.

[11] Serre, J.-P. “Sur les groupes de congruence des variétés abéliennes. II.” *Izvestiya Akademii Nauk SSSR. Seriya Matematicheskaya* 35 (1971): 731–7.

[12] Serre, J.-P. *Algebraic Groups and Class Fields*. Graduate Texts in Mathematics 117. New York: Springer, 1988. Translated from the French.

[13] Tate, J. “On the conjectures of Birch and Swinnerton–Dyer and a geometric analog.” In *Séminaire Bourbaki*, vol. 9, pages Exp. No. 306, 415–40. Paris: Society of Mathematicians France, 1995.