The Dissertation Committee for Chia-Liang Sun
certifies that this is the approved version of the following dissertation:

The Intersection of Closure of Global Points of a Semi-Abelian Variety with a Product of Local Points of its Subvarieties

Committee:

José Felipe Voloch, Supervisor

Jeffrey D. Vaaler

Fernando Rodriguez-Villegas

David F. Helm

Ki-Seng Tan

The Intersection of Closure of Global Points of a Semi-Abelian Variety with a Product of Local Points of its Subvarieties

by

Chia-Liang Sun, B.S.; B.S.E.; M.S.

DISSERTATION

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY

THE UNIVERSITY OF TEXAS AT AUSTIN

May 2011

Acknowledgments

First, I would like to thank my supervisor Felipe Voloch for his suggestion of the problems motivating my thesis research, his input of many key ideas toward their solutions, as well as his continuing advice and encouragement during the completion of this thesis. Moreover, I am grateful that David Harari, and Thomas Scanlon read a earlier version of Chapter 2, and made many suggestions; in particular, one of Harari's suggestions motivates the work in Chapter 3. I also thank M. Jane Ross for correcting the English in the Acknowledgments, as well as Fernando Rodriguez-Villegas for reading an earlier version of this thesis and making specific suggestions. In addition, I thank Jung-Kai Chen, David Helm, Ki-Seng Tan and Jeffrey Vaaler for answering some questions arising from my research. Furthermore, I thank Chieh Chen, who has helped me understand work in French. I have been partially supported by the Chair 4 funds of my department; I thank John Tate, William Beckner, Lorenzo Sadun, Dan Knopf, Jan Baker, Nancy Lamm, and Sandra Catlett for their involvement in my receiving this support. John Tate also gave me verbal encouragement several times during the dark period of my research. I am also grateful for the opportunity to visit The Institute of Mathematics, Academia Sinica in Taiwan, at the invitation of Tzu-Yueh Julie Wang in the summer of 2010, during which some parts of Chapter 2 were revised and the work in Chapter 3 started. Thanks to Wei-Zhe Yang, I have also been receiving financial support from Ms. K in Taiwan. Furthermore, during my first three

years in this doctoral program, I was supported by a Government Scholarship for Studying Abroad from the Ministry of Education of Taiwan. Last but not the least, being a person with physical disabilities, I cannot over-express my gratitude to both of my parents, who travel with me from Taiwan to the United States and provide assistance in my daily life; I am also grateful that Master Kong gives me treatments that improve my physical condition.

The Intersection of Closure of Global Points of a Semi-Abelian Variety with a Product of Local Points of its Subvarieties

Publication No. _____

Chia-Liang Sun, Ph.D.
The University of Texas at Austin, 2011

Supervisor: José Felipe Voloch

This thesis consists of three chapters. Chapter 1 explains how the research problems considered in this thesis fit into the investigation of local-global principle in the diophantine geometry, as well as gives a unified sketch of the proofs of the two main results in this thesis. Chapter 2 establishes a similar conclusion to Theorem B of [PV10] in another settings. Chapter 3 relates to the object considered in the main result of Chapter 2 to an old conjecture proposed by Skolem and solves some cases of its analog.

Table of Contents

Chapter 1

Introduction

The origin of diophantine geometry concerns the solution set in rational integers of an equation $F = 0$, where F is a polynomial in several variables with rational integer coefficients. Given such a polynomial F, a full description of its solution set is in general very difficult; therefore people instead investigate the question of solvability. Following earlier work, however, in 1970 Matiyasevich provided a negative answer to Hilbert's famous problem, which asks for a general algorithm to decide if the equation $F = 0$ has a solution in rational integers. Note that if $F = 0$ has a solution in the field $\mathbb{Q}$ of rational numbers, it will be eventually found after systematically testing sufficiently many candidates. However, such naive searches cannot confirm the nonexistence of such solutions. This difficulty leads to the search for necessary conditions of solvability. (If F is homogeneous, the solvability of $F = 0$ usually means having a nonzero solution.) As observed by Hensel, for all rational primes p, the solvability of $F = 0$ over the p-adic integers is decidable. In fact, there exists a general algorithm to decide the solvability of $F = 0$ over the fields of real and p-adic numbers. Since these fields account for all completions of $\mathbb{Q}$, it is natural to test the solvability of $F = 0$ over these fields when we consider the solvability over $\mathbb{Q}$; if the solvability fails over some of these fields,

it certainly fails over rational numbers. In case where F is a quadratic form, Hasse-Minkowski Theorem ensures that the converse is also true.

There are two directions for generalization of the above discussion. The equation $F = 0$ defines a geometric object in some ambient space. Instead of a single equation, we may consider those geometric objects defined by an arbitrary collection of polynomial equations; such geometric objects are called (algebraic) *varieties*. On the other hand, since roots of a polynomial generally live outside the field in which the coefficients lie, there is no good reason to restrict those coefficients lying in $\mathbb{Q}$. An obvious generalization is to consider those fields obtained from $\mathbb{Q}$ by adjoining roots of a polynomial with coefficients in $\mathbb{Q}$. These are so-called *number fields*. Also, Weil observed that function fields of a curve defined by algebraic equations with coefficients in a finite field k enjoy many properties analogous to those of number fields. Following Weil, these fields are referred as *global function fields*, which are instances of *algebraic function fields*, where we recall that an algebraic function field K over a given field k (which will be called the *constant subfield* of K) is a finitely generated extension of k with transcendence degree 1 such that k is relatively algebraically closed in K. Because of those analogies, problems proposed for number fields are also studied in the analogous settings of global function fields, or even arbitrary algebraic function fields. Putting both directions of these generalizations together, the main object investigated by diophantine geometry today is the set $X(K)$ of K-rational points of an algebraic variety X defined over K, where K is either a number field or an

algebraic function field.

Analogous to the relation of the p-adic numbers (or the real numbers) to the rational numbers, we may also consider the completion K_v of the field K with respect to a place v of K. (In the case where K is an algebraic function field, we usually consider only those places which restrict to the trivial absolute value on its constant subfield.) Denote by Ω_K the set of all places of a number field K, or the set of those places of an algebraic function field K which restrict to the trivial absolute value on its constant subfield. As in the case of rational numbers, it is easier to determine if a polynomial with coefficients in K_v has a root in K_v. In order to test if the set $X(K)$ is empty, one could therefore first test if the set $X(K_v)$ of K_v-points of X is so; if we find $X(K_v)$ is empty for some place $v \in \Omega_K$, then we immediately conclude that $X(K)$ is empty. Unfortunately, the converse statement, known as the Hasse Principle, which asserts that $\prod_{v\in\Omega_K} X(K_v) \neq \emptyset \Rightarrow X(K) \neq \emptyset$, holds only for a very restricted class of varieties, for example, those defined by quadratic forms. Since 1942, several counterexamples of the Hasse Principle over number fields have been produced.

For a smooth variety X defined over a number field K, Manin in 1970 gave a conceptual advance in the investigation of the Hasse Principle. Using class field theory, he defined a set $X^{\mathbf{Br}}$ satisfying

$$X(K) \subset X^{\mathbf{Br}} \subset \prod_{v\in\Omega_K} X(K_v),$$

where $X(K)$ is identified with its image under the diagonal embedding $X(K) \to$

$\prod_{v\in\Omega_K} X(K_v)$. Note that $X^{\mathbf{Br}} = \emptyset$ is a reason that the Hasse Principle could fail for X. In fact, Manin's construction explains almost all known counterexamples of the Hasse Principle. Moreover, it has been successfully verified for hundreds of diagonal cubic surfaces that this reason, known as *Brauer-Manin obstruction*, is the *only* obstruction to the Hasse Principle, by which we mean that the implication $X^{\mathbf{Br}} \neq \emptyset \Rightarrow X(K) \neq \emptyset$ holds. Besides cubic surfaces, there are also theoretical numerical results on the Brauer-Manin obstruction for many other cases. While $X^{\mathbf{Br}}$ has been calculated for many cubic surfaces X, in general it is difficult to compute explicitly. Motivated by this difficulty, in the case where X is a curve of genus at least 1 and has a divisor defined over K of degree 1, Scharaschkin [Sch99] identifies $X^{\mathbf{Br}}$ with a more tractable set involving the image of X under an Albanese map in its Jacobian J as well as J itself, provided that the Shafarevich group for J is finite. Poonen and Voloch [PV10] prove a similar characterization for $X^{\mathbf{Br}}$ when K is a global function field. In this case, due to the lack of Archimedean places, this tractable set in bijection with $X^{\mathbf{Br}}$ is exactly equal to $\prod_{v\in\Omega_K} X(K_v) \cap \overline{J(K)}$, where we denote by $\overline{J(K)}$ the topological closure of $J(K)$ in $\prod_{v\in\Omega_K} J(K_v)$, and X is identified with its image in J.

In view of this identification, Poonen and Voloch [PV10] were concerned with the intersection $\prod_{v\in\Omega} X(K_v) \cap \overline{A(K)}$ in the algebraic function field case, where now X is a subvariety of an Abelian variety A, and Ω is a cofinite subset of Ω_K; under some hypothesis, they show that this intersection is exactly $X(K)$. In Chapter 2, I prove a similar result in another setting.

More explicitly, I consider the intersection $\prod_{v\in\Omega} X(K_v) \cap \overline{H}$, where X is a subvariety of *a semi-Abelian variety* A and H is a subgroup of $A(K)$. Under some assumptions (in particular, H has to be finitely generated), I prove that this intersection is exactly $X(K) \cap H$; while I also give a couple of examples that show that none of these assumptions can be removed.

Although the consideration of $\prod_{v\in\Omega} X(K_v) \cap \overline{H}$ is motivated by the Brauer-Manin obstruction to the Hasse Principle for projective curves, we may also regard this intersection itself as an obstruction for non-emptiness of $X(K) \cap H$ for an *arbitrary* subvariety X inside some semi-abelian variety. As we will explain in Chapter 3, in the case where K is a number field, X is a subvariety of $\mathbb{G}_{\mathrm{m}}^N$ cut by a K-hyperplane in the affine space $\mathbb{A}^N$, and H is the subgroup Γ^N of $\mathbb{G}_{\mathrm{m}}^N(K)$ for a finitely generated subgroup Γ of $\mathbb{G}_{\mathrm{m}}(K)$ satisfying $H \subset \prod_{v\in\Omega} \mathbb{G}_{\mathrm{m}}^N(O_v)$, an old conjecture proposed by Skolem indeed predicts that this the only obstruction to the existence of a point in $X(K)\cap H$. However, this variety X does not satisfy the hypothesis of the main result in Chapter 2. Adopting a different approach to implement the main strategy of proof for that result, I have found a more enlightening proof of the case solved by Skolem, as well as obtained some results of the function field analog of this conjecture. These results are recorded in Chapter 3.

The two main results in this thesis as well as that of Poonen and Voloch [PV10] in the case where K has characteristic p are proved by following the same strategy. To show that $\prod_{v\in\Omega} X(K_v)\cap\overline{H}$ is not strictly larger than (hence is exactly equal to) $X(K)\cap H$, we first reduce to the case where the subvariety

X of A is of dimension zero by finding a zero-dimensional subvariety Z of X such that $\prod_{v\in\Omega} X(K_v) \cap \overline{H} \subset \prod_{v\in\Omega} Z(K_v) \cap \overline{H}$, then give a separate proof for $\prod_{v\in\Omega} Z(K_v) \cap \overline{H} \subset Z(K) \cap H$. The finiteness of $X(K) \cap H$ is a must for this strategy to work. We call the dimension-reducing step a *Mordell-Lang type argument* since its flavor is similar to a conjecture of Mordell and Lang, proved by Raynaud [Ray83] and Faltings [Fal83], which asserts that $C \cap \Gamma'$ is finite, where Γ' is the division group of a finitely generated subgroup Γ of the Jacobian of a non-singular irreducible curve C of genus at least two defined over a field of characteristic zero embedded by an Albanese map. In the next two paragraphs, I will describe those two steps in more details. From now on we suppose that K is a global function field, which is the case considered in this thesis. In the paper of Poonen and Voloch, they deal with the case where K is an arbitrary algebraic function field by reducing it to this basic case with extra arguments, or imposing some hypotheses under which $A(K)$ becomes finitely generated.

Although Mordell-Lang type arguments in the proof of the result of Poonen and Voloch as well as of mine are carried out by different approaches, the underlying idea is the same. We break H into *finitely many* pieces H_i such that for each i we are able to prove, under some hypotheses, the existence of a smaller-dimensional subvariety Y_i of X such that $X(K_v) \cap H_i^v \subset Y_i(K_v)$ for every place v, where H_i^v is the closure of H_i in $A(K_v)$. Then we put together these results for all i and v, and induct on the dimension if necessary. In the paper of Poonen and Voloch, they use model theory to break $H = A(K)$

into cosets of the image of a high iteration of the multiplication-by-p map and to find the corresponding zero-dimensional subvarieties. Instead, in my work, I decompose H into cosets of the image of a Frobenius map, which exists by the assumption that A is defined over a finite field. In Chapter 2, I find those corresponding smaller-dimensional subvarieties by investigating the relation between subfields of K and of K_v's over which ideals in the polynomial rings over with coefficients in K and in K_v's are generated; while in Chapter 3, I apply a result of Garcia and Voloch [GV87] about Wronskians and linear independence and find the zero-dimensional subvarieties desired in the Mordell-Lang type argument.

The proof of zero-dimensional case of the main results in this thesis follows that in the paper of Poonen and Voloch more closely. It consists of two key ingredients. Let J be a finitely generated subgroup of $A(K)$. First, we need to find a sequence of subsets $(U_n)_{n\geq 1}$ of J, such that for each place v, each U_n is an open neighborhood of 0 under the topology on J induced from that of $A(K_v)$, and such that $\bigcap_{n\geq 1} U_n$ consists of only torsion elements. In the work of Poonen and Voloch, after reducing to the case where $J = A(K)$ is finitely generated, they take U_n to be the images of $A(K)$ under the map of multiplication by p^n, under the finiteness assumption (which they predict to be unnecessary for their main result) on the subgroup $A(K^s)[p^\infty]$ of elements of finite p-power orders of separable points of A. Extracting the idea from their proof, under my assumption that A is defined over a finite subfield of K, I take U_n to be the intersection of J with the image of $A(K)$ under the

n-th iteration of a Frobenius map, without assuming that $A(K^s)[p^\infty]$ is finite. The other ingredient is to show that under the topology on J induced from that of $\prod_{v\in\Omega} A(K_v)$, every subgroup with a finite index is open. In the case where A is an abelian variety, this is exactly a result of Milne [Mil72], who generalizes that of Serre [Ser71] in the number field case; while in the case where $A = \mathbb{G}_{\mathrm{m}}$, I prove this desired result by establishing and reinterpreting the function field analog of an arithmetic result of Chevalley [Che51]. I also note that the semi-abelian variety considered in what follows is isogenous to a direct product of copies of $\mathbb{G}_{\mathrm{m}}$'s and an abelian variety, and hence establish the desired property by showing that it is preserved under a product and an isogeny.

Scharaschkin's work provides a new direction of investigation of the local-global principle for varieties. The obstruction $\prod_{v\in\Omega} X(K_v) \cap \overline{H}$ for non-emptiness of $X(K) \cap H$ could give an algorithm which determines whether $X(K) \cap H$ is empty. On the one hand, given an explicit finite set of generators of H, there is a naive procedure which search for a point in $X(K) \cap H$. On the other hand, under the mild assumptions that $H \subset \prod_{v\in\Omega} A(O_v)$ and Ω only consists of places over which A has good reduction, such a set of generators of H also yields a procedure which detects the situation where $\prod_{v\in\Omega} X(K_v) \cap \overline{H} = \emptyset$. Running those two procedures simultaneously, the equality $\prod_{v\in\Omega} X(K_v) \cap \overline{H} = X(K) \cap H$ ensures one of them must halt. This produces the desired algorithm. In fact, the assumption $H \subset \prod_{v\in\Omega} A(O_v)$ implies that $\overline{H}$ is compact, by which it can be shown that we are able to

determine whether $\prod_{v\in\Omega} X(K_v) \cap \overline{H}$ is empty by testing the solvability of a given set of equations over finitely many finite rings. An interesting problem is to figure out which these rings are, for its solution gives an algorithm which determine whether $X(K) \cap H$ is empty in a prior-known bounded amount of time, provided $\prod_{v\in\Omega} X(K_v) \cap \overline{H} = X(K) \cap H$ as established in the paper of Poonen and Voloch as well as in this thesis. While Scharaschkin, Poonen and Voloch consider only closed subvarieties of abelian varieties, the work of Chapter 2 makes the above idea applicable to the study of integral points of non-projective varieties. In particular, by considering its intersection with some $\mathbb{G}_{\mathrm{m}}^N$, every affine variety may be studied in this framework. This relates directly to solution sets of polynomials, which occur more often in old statements about the local-global principle, as Chapter 3 exemplifies.

Chapter 2

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

2.1 Introduction

Let K be a global function field, that is, a finitely generated field extension over its prime field with transcendence degree 1. We denote by Ω_K the set of all places of K. For each $v \in \Omega_K$, we denote by K_v the completion of K at v, by O_v the valuation ring in K_v, and by m_v the maximal ideal in O_v. For a finite subset S of Ω_K, the subring of S-integers in K is denoted by

$$O_S = \{x \in K : x \in O_v \text{ for each } v \notin S\}.$$

Throughout this thesis, we fix a co-finite subset Ω of Ω_K.

Fix an algebraic closure $\overline{K}$ of K. In the category of varieties (resp. of semi-abelian varieties), we say that an object defined over K is *isotrivial* if it is isomorphic over $\overline{K}$ to one defined over some finite subfield of $\overline{K}$. In spite of different appearances, our definition of isotriviality indeed agrees with the usual one for varieties (resp. semi-abelian varieties) defined over an arbitrary algebraic function field K, specialized to the case where the constant subfield of K is finite. From now on, fix a semi-abelian variety A defined over K. As we

will describe in Subsection 2.2.2, there is a natural topology on $\prod_{v\in\Omega} A(K_v)$ making it a complete topological group. For any subset H of $A(K)$, we define the **product topology** on H to be the coarsest topology such that the diagonal embedding $A(K) \to \prod_{v\in\Omega} A(K_v)$ is continuous on H; we also denote by $\overline{H}$ the topological closure of the image of H in $\prod_{v\in\Omega} A(K_v)$ under this diagonal embedding. For any subvariety X of A, we naturally consider $X(R)$ as a subset of $A(R)$ for any ring R whenever both sets are defined. As mentioned in Chapter 1, Poonen and Voloch show in Section 4 of [PV10] that in the case where $\Omega = \Omega_K$, and X is a curve of genus at least 1 embedded in its Jacobian A under an Albanese map induced from a divisor on A defined over K of degree 1, the subset $\prod_{v\in\Omega} X(K_v) \cap \overline{A(K)}$ of $\prod_{v\in\Omega} A(K_v)$ is in bijection with the Brauer-Manin obstruction to the Hasse principle for X over K, provided that the Tate-Shafarevich group of A is finite. In that paper, they also conjectured that in the case A is an abelian variety, $\prod_{v\in\Omega} X(K_v) \cap \overline{A(K)}$ is equal to $\overline{X(K)}$, and proved in Theorem B that this intersection is equal to $X(K)$ under some hypotheses on A and X. Those hypotheses in particular impose that A is not isotrivial. In this chapter, we investigate the case where A is isotrivial and is allowed to be non-projective, and prove that a similar statement holds in another setting, among which we need to replace $A(K)$ by one of its finitely generated subgroups. Our main result of this chapter is the following

Theorem 1. *Let H be a finitely generated subgroup of $A(K)$, and X be a closed K-subvariety of A. Suppose that A is isotrivial, and that X has no*

positive-dimensional isotrivial closed $\overline{K}$-subvarieties. Then we have

$$\prod_{v\in\Omega} X(K_v)\cap\overline{H} = X(K)\cap H, \tag{2.1}$$

where both $X(K)$ and H embedded diagonally into $\prod_{v\in\Omega} A(K_v)$. Furthermore, the common set in (2.1) is finite.

In the end of Section 2.3 and Section 2.4, we give examples which show that this equality would fail if either the hypothesis on H or that on X in Theorem 1 were removed.

In Chapter 1, we have outlined the strategy for proving (2.1), and noted that the last part of the conclusion in Theorem 1 is a formal consequence. In Section 2.3, we carry out the zero-dimensional case by adapting the proof of Proposition 3.7 in [PV10] to our situations. In contrast, the approach we adopt to work out the reduction step in Section 2.4 is totally different from that in [PV10]. Instead of the model theory, our main idea came from the proof of Theorem A. Part 1 in [AV92]. This makes us complete the reduction step by induction on the dimension of X, and also explains the inductive nature of the hypothesis we make about X in Theorem 1. The key ingredient in our approach is a question about ideals in polynomial rings over K and over K_v's; in Lemma 12, we answer this question affirmatively.

For a non-projective K-variety, one usually cares about its integral points rather than rational points. For any sufficiently large finite subset S of Ω_K, the set $A(O_S)$ of S-integral points of A is a finitely generated subgroup of

$A(K)$. Hence, the consideration of intersection of a product of local points of K-subvarieties of A with $\overline{A(O_S)}$ may provide some information about integral points of certain K-varieties. For example, take a K-variety X_0, which we want to investigate about the set $X_0(O_{S_0})$ of its S_0-integral points for some finite subset S_0 of Ω_K. Assume that X_0 may be embedded in A by a morphism defined over K, and denote by X the image of X_0 in A. By Lemma 1 in Subsection 2.2.1, there is a finite subset S of Ω_K containing S_0 such that the image of $X_0(O_{S_0})$ is contained in $X(O_S)$. Provided we use the same embedding to define the subsets $X(O_S)$ and $A(O_S)$ of $A(K)$, we have $X(O_S) \subset A(O_S)$ and therefore $X(O_S) = X(K) \cap A(O_S) \subset \prod_{v\in\Omega} X(K_v) \cap \overline{A(O_S)}$, provided that $S \cap \Omega = \emptyset$. We saw in Chapter 1 that the conclusion of Theorem 1 could yield an algorithm which decides whether $X(K) \cap A(O_S)$ is empty. Let me explain this more precisely in the generality of the discussion in Chapter 1. Consider a finitely generated subgroup H of $A(K)$ with a given finite set of generators. Using the set of generators, we may completely enumerate elements of H and test whether any of them belongs to $X(K)$. This gives a procedure which detects the case where $X(K) \cap H \neq \emptyset$. On the other hand, choose a cofinite subset Ω of Ω_K such that $H \subset \prod_{v\in\Omega} A(O_v)$ and Ω only consists of places over which A has good reduction. The property about H shows that $\prod_{v\in\Omega} X(K_v) \cap \overline{H} = \prod_{v\in\Omega} X(O_v) \cap \overline{H}$. For each $v \in \Omega_K$ and each positive integer n_v, we have the reduction map $X(O_v) \to X(O_v/m_v^{n_v})$. In fact, Hensel's Lemma implies that for each fixed v, this reduction map is surjective when n_v is sufficiently large. From these facts and the topology of $\prod_{v\in\Omega} A(O_v)$, we see that the set

$\prod_{v\in\Omega} X(K_v) \cap \overline{H}$ is empty if and only if there is a collection $\{n_v : v \in T\}$ of positive integers indexed by a finite subset T of Ω such that the image of H in $\prod_{v\in T} A(O_v/m_v^{n_v})$, under the product of reduction maps associated with A, does not intersect with $\prod_{v\in T} X(O_v/m_v^{n_v})$. By the property of good reduction, those reduction maps associated with A are group homomorphisms. Therefore, for any collection $\{n_v : v \in T\}$ of positive integers indexed by a finite subset T of Ω, since each $O_v/m_v^{n_v}$ is finite, we may use the given finite set of generators of H to compute the image of H in $\prod_{v\in T} A(O_v/m_v^{n_v})$ and test whether this image intersect with $\prod_{v\in T} X(O_v/m_v^{n_v})$ in a finite amount of time. By completely enumerating the set of finite collections of positive integers, we have a procedure which detects the case where $\prod_{v\in\Omega} X(K_v)\cap\overline{H} = \emptyset$. Running those two procedures simultaneously, the equality in the conclusion of Theorem 1 shows that one of them must finish, and hence we have an algorithm. We also remark that using the compactness of $\overline{H}$, one may prove that in order to confirm $\prod_{v\in\Omega} X(K_v) \cap \overline{H} \neq \emptyset$, it is enough to check that the image of H in $\prod_{v\in T} A(O_v/m_v^{n_v})$ does intersect with $\prod_{v\in T} X(O_v/m_v^{n_v})$ for *some* (rather than all) collection $\{n_v : v \in T\}$ of positive integers indexed by a finite subset T of Ω. If one such collection is found explicitly, we will have an algorithm deciding whether $\prod_{v\in\Omega} X(K_v)\cap\overline{H}$ is empty in a prior-known bounded amount of time.

Since any finitely generated subgroup H of $A(K)$ is contained in a finitely generated subgroup $A(O_S)$ for some finite S, it suffices to prove Theorem 1 in the case where $H = A(O_S)$ for some finite S. However, some intermediate results are worth being stated more generally; therefore I will

leave H as an arbitrary finitely generated subgroup of $A(K)$.

2.2 Preliminaries

2.2.1

All varieties considered in this thesis are subvarieties of the variety underlying a semi-abelian variety, which is known to be quasi-projective. A quasi-projective variety defined over a subfield L of $\overline{K}$ is a subvariety of some projective space $\mathbb{P}^N$ of the following form

$$\left\{ P \in \mathbb{P}^N(\overline{K}) : \begin{array}{l} f(P) = 0 \text{ for all } f \in I \\ g(P) \neq 0 \text{ for some } g \in J \end{array} \right\}, \tag{2.2}$$

where I and J are homogeneous ideals in the polynomial ring $L[X_0, \ldots, X_N]$. Now consider a quasi-projective variety V defined over K. we want to define the subset $V(O_v)$ of integral points in $V(K_v)$ for each $v \in \Omega$, and the subset $V(O_S)$ of S-integral points in $V(K)$ for each finite subset $S \subset \Omega$. Since these definitions in general depends on choices of an isomorphism copy of V inside some projective space $\mathbb{P}^N$, we fix a such choice and assume that V is of the form (2.2) with both I and J being homogeneous ideals in $K[X_0, \ldots, X_N]$. Fix a place $v \in \Omega$, and denote by $I^{(v)}$ (resp. $J^{(v)}$) the subset of $I \cap O_v[X_0, \ldots, X_N]$ (resp. $J \cap O_v[X_0, \ldots, X_N]$) which consists of polynomials with some coefficients not in m_v. We define the local integral points of V at v by

$$V(O_v) = \left\{ P \in \mathbb{P}^N(K_v) : \begin{array}{l} P = [x_0 : \ldots : x_N] \\ x_i \in O_v \text{ for all } i \\ x_{i_0} \notin m_v \text{ for some } i_0 \\ f(x_0, \ldots, x_N) = 0 \text{ for all } f \in I^{(v)} \\ g(x_0, \ldots, x_N) \notin m_v \text{ for some } g \in J^{(v)} \end{array} \right\}. \tag{2.3}$$

For each integer $n \geq 1$, we also define the set of O_v/m_v^n-valued points of V by

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

Since those copies of $V(K)$ inside $V(K_v)$ for various $v \in \Omega$ may be canonically identified, it makes sense to define, for any finite subset $S \subset \Omega$,

$$V(O_S) = \bigcap_{v \in \Omega_K \setminus S} \left(V(K) \cap V(O_v) \right). \tag{2.4}$$

Under these definition, one can prove the following useful result by Hilbert's Nullstellensatz:

Lemma 1. *Let $\phi : V \to W$ be a regular map defined over K between two quasi-projective varieties defined over K. Then ϕ maps $V(O_v)$ into $W(O_v)$ for all but finitely many $v \in \Omega_K$; in particular, ϕ maps $V(O_S)$ into $W(O_S)$ for any sufficiently large finite $S \subset \Omega_K$.* □

The topology of K_v gives rise to a natural Hausdorff topology on $V(K_v)$, which is totally disconnected since v is non-archimedean. Then $\prod_{v \in \Omega} V(K_v)$ is equipped with the product topology. Note that (2.3) shows that $V(O_v)$ is a compact subset of $V(K_v)$; also, if we identify $V(K)$ with its image in $\prod_{v \in \Omega} V(K_v)$ under the diagonal embedding, we see from (2.4) that $V(O_S)$ is closed in $V(K)$ for any finite subset $S \subset \Omega$.

2.2.2

A semi-abelian variety A is an algebraic group such that there is a non-negative integer n, an abelian variety B, and a strictly exact sequence

$$1 \to \mathbb{G}_{\mathrm{m}}^n \to A \to B \to 0$$

of morphisms between algebraic groups, where $\mathbb{G}_{\mathrm{m}}$ is the algebraic group with its underlying variety being $\mathbb{A}^1 \setminus \{0\}$, on which the group operation is given by the multiplication of coordinates. It can be shown that the group operation on A is commutative. As mentioned, the underlying variety of A is quasi-projective; if A is embedded into some projective space, since the group operations of an algebraic group are given by regular maps, the group operations on A are locally expressed by polynomials in the homogeneous coordinates. We say that A is defined over a subfield L of $\overline{K}$ if A can be embedded in some $\mathbb{P}^N$ so that its underlying variety is in the form (2.2), where I and J are homogeneous ideals in the polynomial ring $L[X_0, \ldots, X_N]$ generated by elements in $L[X_0, \ldots, X_N]$, as well as the identity element of A lies in $\mathbb{P}^N(L)$, and the group laws on A can be expressed by a collection of polynomials with coefficients in L.

Let us go back to our assumption that A is defined over K. In Subsection 2.2.1, we have defined $A(K_v)$'s, $A(O_v)$'s and $\prod_{v\in\Omega} A(K_v)$ as topological spaces, all of which are Hausdorff. In the case where $A = \mathbb{G}_{\mathrm{m}}$, our definitions naturally identify the $\mathbb{G}_{\mathrm{m}}(O_v)$'s and the $\mathbb{G}_{\mathrm{m}}(O_S)$'s respectively as the group of units of O_v's and of O_S's. Since the group operations on A are given by

regular maps defined over K, they are continuous with respect to the topology of $A(K_v)$ for each $v \in \Omega_K$; this implies that $A(K_v)$ is a Hausdorff topological abelian group. Moreover, having $A(O_v)$ as a compact subset, the topological group $A(K_v)$ is locally compact. Together with what we saw in Subsection 2.2.1, $A(K_v)$ is a locally compact and totally disconnected topological group, hence Theorem (7.7) in [HR79] shows that the topology of $A(K_v)$ is generated by open subgroups. Therefore we see that $\prod_{v\in\Omega} A(K_v)$ is also a Hausdorff topological abelian group with its topology generated by open subgroups. Furthermore, Lemma 1 implies that $A(O_v)$ is group for all but finitely many $v \in \Omega_K$; hence the definition (2.4) in the case where $V = A$ also reveals that $A(O_S)$ is a subgroup of $A(K)$ if S is *sufficiently large*, meaning that S contains those finitely many v for which $A(O_v)$ fails to be a subgroup of $A(K_v)$. In this case, it is known that $A(O_S)$ is finitely generated.

2.2.3

Note that we only assume that A is defined over a finite subfield of $\overline{K}$ in Theorem 1; for its proof, however, we may strengthen this assumption and suppose that A is defined over a finite subfield of K. To see this, we claim that it suffices to establish (2.1) with K replaced by one of its finite extensions. With this claim, our assertion follows from that an isotrivial semi-abelian variety defined over K is isomorphic as algebraic groups over a finite extension of K to a semi-abelian variety defined over some finite subfield of that extension, that the hypothesis on X in Theorem 1 is preserved under

finite extensions of K, and that an isomorphism between algebraic groups over K preserve structures of all objects involved in (2.1). In order to prove our claim, let L be a finite extension over K, and let Ω_L^0 be the subset of Ω_L which consists of those places in Ω_L lying above a place in Ω. Embedding L diagonally into $\prod_{w\in\Omega_L^0} L_w$ as well as $\prod_{v\in\Omega} K_v$ naturally into $\prod_{w\in\Omega_L^0} L_w$, it is a fact that $L\cap\prod_{v\in\Omega} K_v = K$. Then $\prod_{v\in\Omega} A(K_v)$ is a complete topological subgroup of $\prod_{w\in\Omega_L^0} A(L_w)$. Consider a subset H of $A(K)$, and is a K-subvariety X of A. Suppose that

$$\prod_{w\in\Omega_L^0} X(L_w)\cap\overline{H} = X(L)\cap H, \tag{2.5}$$

where both $X(L)$ and H embedded diagonally into $\prod_{w\in\Omega_L^0} A(L_w)$. We intersect with $\prod_{v\in\Omega} A(K_v)$ on both sides of (2.5). Since $L\cap\prod_{v\in\Omega} K_v = K$, it follows that $X(L)\cap\prod_{v\in\Omega} A(K_v) = X(L)\cap\prod_{v\in\Omega} X(K_v) = X(K)$, which gives

$$X(L)\cap H\cap\prod_{v\in\Omega} A(K_v) = \left(X(L)\cap\prod_{v\in\Omega} A(K_v)\right)\cap\left(H\cap\prod_{v\in\Omega} A(K_v)\right) = X(K)\cap H.$$

On the other hand, we have

$$\begin{aligned} & \textstyle\prod_{w\in\Omega_L^0} X(L_w)\cap\overline{H}\cap\prod_{v\in\Omega} A(K_v) \\ = \ & \left(\textstyle\prod_{w\in\Omega_L^0} X(L_w)\cap\prod_{v\in\Omega} A(K_v)\right)\cap\left(\overline{H}\cap\prod_{v\in\Omega} A(K_v)\right) \\ = \ & \textstyle\prod_{v\in\Omega} X(K_v)\cap\overline{H}. \end{aligned}$$

Hence we see that (2.1) holds. Since $\prod_{v\in\Omega} A(K_v)$ is a closed in $\prod_{w\in\Omega_L^0} A(L_w)$, we note that $\overline{H}$ is also the topological closure of the image of H in $\prod_{w\in\Omega_L^0} A(L_w)$ under the restriction of the diagonal embedding $A(L)\to\prod_{w\in\Omega_L^0} A(L_w)$, when H is naturally regarded as a subset of $A(L)$. This justifies our claim. The same idea is used in the proof of Proposition 3.7 in [PV10].

2.3 Zero-Dimensional Case

Recall that the product topology on $A(K)$ is that induced by the diagonal embedding $A(K) \to \prod_{v\in\Omega} A(K_v)$. For each $v \in \Omega$, we also define the *v-adic topology* on $A(K)$ to be the subspace topology with respect to the natural inclusion into $A(K_v)$, which is a topological group as described in Subsection 2.2.2. Obviously, the product topology on $A(K)$ is finer than the v-adic topology for any $v \in \Omega$.

Since we have defined several different topologies on the same underlying set, we introduce the following terminologies: When $A(K)$ is endowed with the product topology, we refer its topological subgroup as **product topological subgroups**. For each $v \in \Omega$, when $A(K)$ is endowed with the v-adic topology, we refer its topological subgroup as **v-adic topological subgroups**.

We shall need the following property about product topological subgroups of $A(K)$:

Lemma 2. *For any finitely generated product topological subgroup of $A(K)$, there exists a collection of open subgroups with finite index which generates a Hausdorff topology on the underlying group.*

Proof. Let H be a finitely generated subgroup of $A(K)$. Note that for every $v \in \Omega$, the product topological group H has more open sets than the v-adic topological group H topology on H, which is Hausdorff by construction. Hence we only need to show that for some $v \in \Omega$, the v-adic topological group H has its topology generated by open subgroups with finite index. From the

assumption that H is finitely generated and that $\Omega_K \setminus \Omega$ is finite, it holds for all but finitely many $v \in \Omega$ that $A(O_v)$ is a group containing H. Pick one among those v's. Since the v-adic topological group H is a topological subgroup of $A(O_v)$, it suffices to show that the topological group $A(O_v)$ has its topology generated by open subgroups with finite index. But this just follows from that $A(O_v)$ is a compact subgroup of $A(K_v)$ whose topology is generated by open subgroups. □

As shown in Subsection 2.2.3, it suffices to prove Theorem 1 under the assumption that A is defined over a finite subfield k of K. In this case, there exists a Frobenius morphism $\mathrm{Frob} : A \to A$ and an embedding of A as a subvariety of $\mathbb{P}^N$ in which Frob simply sends $[x_0 : \ldots : x_N]$ to $[x_0^{|k|} : \ldots : x_N^{|k|}]$. Hence we see that Frob preserves the group structure on A. From the definition (2.3) and (2.4) in Subsection 2.2.1, it is clear that Frob induces an injective map $A(O_S) \to A(O_S)$, which we also denote by Frob. If $A(O_S)$ is a group, then this map is a group homomorphism.

Proposition 1. *Suppose that A is defined over a finite subfield of K. Consider a Frobenius endomorphism* $\mathrm{Frob} : A \to A$. *Let H be a finitely generated subgroup of $A(K)$. Then for any place $v \in \Omega_K$ and any positive integer n, the subgroup* $\mathrm{Frob}^n(A(K)) \cap H$ *is open in the v-adic topological group H.*

Proof. Fix a place $v \in \Omega_K$ and a positive integer n. First, from the definition of Frob, it is clear that that $\mathrm{Frob}^n(A(K_v))$ is closed in $A(K_v)$, which is equivalent to the quotient space $A(K_v)/\mathrm{Frob}^n(A(K_v))$ being Hausdorff since $A(K_v)$ is a

metrizable space. Choose a finite subset S of Ω_K such that $H \leq A(O_S)$. Since Frob is injective and preserves the finitely generated abelian group $A(O_S)$, we see that $A(O_S)/\operatorname{Frob}^n(A(O_S))$ is finite. Now consider the composition of the two continuous map $H \to A(O_S)/\operatorname{Frob}^n(A(O_S)) \to A(K_v)/\operatorname{Frob}^n(A(K_v))$, induced respectively by the inclusion $H \subset A(O_S)$ of v-adic topological groups and the inclusion $A(O_S) \subset A(K_v)$, which defines the v-adic topology of $A(O_S)$. The image of H in $A(K_v)/\operatorname{Frob}^n(A(K_v))$ under this composition is a finite subset of a Hausdorff space, hence is discrete. Therefore there is an open subgroup U of $A(K_v)$ such that $U \cap H = \operatorname{Frob}^n(A(K_v)) \cap H$, and we see that $\operatorname{Frob}^n(A(K_v)) \cap H$ is open in the v-adic topological group H.

To complete the proof, we show that $\operatorname{Frob}^n(A(K_v)) \cap H \leq \operatorname{Frob}^n(A(K)) \cap H$, which follows from a more general statement $\operatorname{Frob}^n(A(K_v)) \cap A(K) \subset \operatorname{Frob}^n(A(K))$ we shall prove below. Let $P = \operatorname{Frob}^n(Q) \in A(K)$ with $Q \in A(K_v)$. By definition of Frob, it is clear that Q is defined over a purely inseparable algebraic extension of K. Since K is the only such extension inside K_v, we conclude that $Q \in A(K)$, i.e. $P \in \operatorname{Frob}^n(A(K))$. □

For a topological abelian group G with additive notation, we say that G has the **congruence subgroup property** if for every positive integer n, the subgroup $\{nP : P \in G\}$, denoted by nG, is open. It is clear that G has the congruence subgroup property if and only if every subgroup of finite index is open, which holds if and only if every subgroup of finite index is closed. As a consequence, if G is a finitely generated abelian group which has the

congruence subgroup property, then every subgroup is closed since it is equal to an intersection of a collection of subgroups of G of finite index.

Our next goal of this section is to show that every finitely generated product topological subgroup of $A(K)$ has the congruence subgroup property under the assumption that A is isotrivial. First, we treat the case where A is either $\mathbb{G}_{\mathrm{m}}$ or an abelian variety.

For the $\mathbb{G}_{\mathrm{m}}$-case, the desired result would essentially be Theorem 1 in [Che51] if K were a number field and Ω consisted of only non-Archimedean places. In the following lemma, we prove its function field analogue in the form relevant to our purpose. For each finite subset S of Ω_K, we put

$$U_S = \left\{ (x_v) \in \prod_{v \in \Omega_K} \mathbb{G}_{\mathrm{m}}(K_v) : x_v - 1 \in m_v \text{ for each } v \in S \right\}$$

and note that it is an open *subgroup* of $\prod_{v \in \Omega_K} \mathbb{G}_{\mathrm{m}}(K_v)$.

Lemma 3. *Denote by $d_K : \mathbb{G}_m(K) \to \prod_{v \in \Omega_K} \mathbb{G}_m(K_v)$ the diagonal embedding. Let H be a finitely generated subgroup of $\mathbb{G}_m(K)$. Then for any finite subset $T \subset \Omega_K$ and any prime-to-p positive integer $m \in \mathbb{N}$, there is a finite subset $S \subset \Omega_K$, which is disjoint from T, such that $H \cap d_K^{-1}(U_S) \subset H^m$.*

Proof. Let H_0 be the preimage of the torsion subgroup of $\mathbb{G}_{\mathrm{m}}(K)/H$ under the quotient map $\mathbb{G}_{\mathrm{m}}(K) \to \mathbb{G}_{\mathrm{m}}(K)/H$. As H is finitely generated, there is a finite subset S_0 of Ω_K such that $|x|_v = 1$ for any $x \in H$ and $v \notin S_0$. Then we see that H_0 is finitely generated, for it is contained in the finitely generated group $\mathbb{G}_{\mathrm{m}}(O_{S_0})$. Since the finitely generated abelian group H_0/H consists of

only torsion elements, it is a group of finite order, say n. For any $m \in \mathbb{N}$, it is clear that $H \cap \mathbb{G}_{\mathrm{m}}(K)^{mn} \subset H^m$. Therefore, to prove Lemma 3, it suffices to show:

(*) For any finite subset $T \subset \Omega_K$ and any prime-to-p positive integer $m \in \mathbb{N}$, there is a finite subset $S \subset \Omega_K$, which is disjoint from T such that $H \cap d_K^{-1}(U_S) \subset \mathbb{G}_{\mathrm{m}}(K)^m$.

Following the ideas in the proof of Theorem 1 in [Che51], we proceed with several reductions. First, we note that it suffices to prove (*) in the case where m is a prime power. In fact, if, for each $i \in \{1, \ldots, r\}$, there is a finite $S_i \subset \Omega_K$ such that (*) holds with m replaced by a prime power $q_i^{e_i}$ and S replaced by S_i, then it is not hard to see that (*) holds with m replaced by $\prod_{i=1}^r q_i^{e_i}$ and S replaced by $\bigcup_{i=1}^r S_i$. Then, we want to show that, without loss of generality, one may assume that K contains a primitive m-th root ξ_m of unity when proving (*) in the case where m is some power of a prime q. We demonstrate this in two steps. First we claim that it does no harm to assume that $\xi_4 \in K$ in the proof of (*) in the case where $q = 2$. In this case, the characteristic of our global field K is not 2, hence there is an $s \in \mathbb{N}$ such that $\xi_{2^s} \in K(\xi_4)$ but $\xi_{2^{s+1}} \notin K(\xi_4)$. Then one shows

$$\mathbb{G}_{\mathrm{m}}(K) \cap \mathbb{G}_{\mathrm{m}}(K(\xi_4))^{2^{e+s}} \subset \mathbb{G}_{\mathrm{m}}(K)^{2^e}, \tag{2.6}$$

which justifies our claim. Next, under the assumption that $\xi_4 \in K$ in the case where $q = 2$, one shows that, for any $e \in \mathbb{N}$,

$$\mathbb{G}_{\mathrm{m}}(K) \cap \mathbb{G}_{\mathrm{m}}(K(\xi_{q^e}))^{q^e} \subset \mathbb{G}_{\mathrm{m}}(K)^{q^e} \tag{2.7}$$

which means that, to prove (*) in the case where m is a prime power, we may assume that $\xi_m \in K$. In fact, (2.7) is an immediate consequence of the following assertion: For any $e \in \mathbb{N}$ and $h \in \{0, \ldots, e-1\}$,

$$\mathbb{G}_{\mathrm{m}}(K) \cap \mathbb{G}_{\mathrm{m}}(K(\xi_{q^{h+1}}))^{q^e} \subset \mathbb{G}_{\mathrm{m}}(K(\xi_{q^h}))^{q^e}. \tag{2.8}$$

In his proof of Theorem 1 in [Che51], Chevalley established (2.6) and (2.8) with K being replaced by a number field F. In addition to general field theory, he only used the facts that the degree $[F(\xi_q) : F]$ divides $q-1$, and that for $h > 0$, the Galois group of $F(\xi_{q^{h+1}})/F(\xi_{q^h})$ is either trivial or cyclic of order q. In the case where q differs from p, these statements still hold with the number field F being replaced by our global function field K; therefore, one may verify (2.6) and (2.8) by following Chevalley's argument verbatim.

To complete the proof of Lemma 3, it remains to prove (*) in the case where $m = q^e$ is a prime power under the additional hypothesis $\xi_m \in K$. Let L be the field extension generated by all m-th roots of elements in H. Since H is finitely generated and $\xi_m \in K$, the extension L/K is finite Galois with degree a power of q. Suppose that $L \neq K$, for otherwise we are done. Let $L_1, \ldots, L_s$ be all subfields of L which have degree q over K. For each L_i, there are infinitely many places of K which extends uniquely and unramifiedly to L_i, and therefore there exists a such place $v_i \in \Omega_K$ which does not belong to T. For each i, we still denote by v_i the unique extension of $v_i \in \Omega_K$ to L_i, then we have

$$[(L_i)_{v_i} : K_{v_i}] = [L_i : K] = q. \tag{2.9}$$

Now take $S = \{v_1, \ldots, v_s\}$. We claim that (*) holds for this choice of S. Suppose $x \in H \cap d_K^{-1}(U_S)$. Let M be the field extension generated over K by an m-th root of x. Note that M is independent of choices of the m-th root of x. We want to show $K = M$, which completes the proof. If M does not contain any of L_i's, then we are done by the construction of the L_i's and the fact L/K is Galois with degree a power of q. Otherwise, assume that $K \subset L_j \subset M$ for some j. Let w be a place of M above v_j. We have $K_{v_j} \subset (L_j)_{v_j} \subset M_w$. Note that $|m|_{v_j} = 1$ since m is prime to p, and that $|x-1|_{v_j} < 1$ since $v_j \in S$ and $d_K(x) \in U_S$. Hensel's lemma now implies that x is a m-th power in K_{v_j}, Since M_w is generated over K_{v_j} by an m-th root of x, we have $M_w = K_{v_j}$, and therefore $(L_j)_{v_j} = K_{v_j}$, which contradicts to (2.9). □

Corollary 1. *Let H be a finitely generated subgroup of $\mathbb{G}_m(K)$. Then every subgroup of H with finite prime-to-p index is open in the product topological group H.*

Proof. Let E be a subgroup of H with a prime-to-p index m. Then $H^m \leq E$. It is enough to show that H^m is open in the product topological group H. Similar as the notation d_K in Lemma 3, we denote by $d : \mathbb{G}_{\mathrm{m}}(K) \to \prod_{v\in\Omega} \mathbb{G}_{\mathrm{m}}(K_v)$ the diagonal embedding. Taking $T = \Omega_K \setminus \Omega$ in Lemma 3, we conclude that there is a finite subset $S \subset \Omega$ such that $H \cap d_K^{-1}(U_S) \subset H^m$. Denote by $i : \prod_{v\in\Omega} \mathbb{G}_{\mathrm{m}}(K_v) \to \prod_{v\in\Omega_K} \mathbb{G}_{\mathrm{m}}(K_v)$ the natural group monomorphism, and note that it is continuous. Although $d_K \neq i \circ d$ in the case where $\Omega \neq \Omega_K$, we do have $d_K^{-1}(U_S) = d^{-1}\left(i^{-1}(U_S)\right)$ since $S \subset \Omega$. Hence we obtain

$H \cap d^{-1}\left(i^{-1}(U_S)\right) \subset H^m$, which shows that H^m is open in in the product topological group H since $i^{-1}(U_S)$ is an open subgroup in $\prod_{v\in\Omega} \mathbb{G}_{\mathrm{m}}(K_v)$. $\square$

Lemma 4. *For any finite subset S of Ω_K, the product topological subgroup $\mathbb{G}_m(O_S)$ has the congruence subgroup property.*

Proof. Note that $\mathbb{G}_{\mathrm{m}}$ is defined over any field and that the multiplication-by-p map on $\mathbb{G}_{\mathrm{m}}$ is a Frobenius endomorphism. Since $\mathbb{G}_{\mathrm{m}}(K)^n \cap \mathbb{G}_{\mathrm{m}}(O_S) = \mathbb{G}_{\mathrm{m}}(O_S)^n$ for any positive integer n, it follows from Proposition 1 that for any $v \in \Omega_K$, every subgroup of $\mathbb{G}_{\mathrm{m}}(O_S)$ with a finite p-power index is open in the v-adic topological group $\mathbb{G}_{\mathrm{m}}(O_S)$. Recall that the product topological group $\mathbb{G}_{\mathrm{m}}(O_S)$ has no fewer open sets than the v-adic topological group $\mathbb{G}_{\mathrm{m}}(O_S)$ for any $v \in \Omega$. Now Corollary 1 yields this lemma, for any subgroup of $\mathbb{G}_{\mathrm{m}}(O_S)$ with finite index is an intersection of a subgroup with finite p-power index and a subgroup with finite prime-to-p index. $\square$

In order to pass the congruence subgroup property from those product topological subgroups $\mathbb{G}_{\mathrm{m}}(O_S)$ to every finitely generated product topological subgroup of $\mathbb{G}_{\mathrm{m}}(K)$, we give the following technical lemma.

Lemma 5. *Let G be a topological group whose group structure is abelian. Suppose that G has the congruence subgroup property, and that H is a subgroup of G such that the torsion subgroup of (G/H) is finite. Then H has the congruence subgroup property.*

Proof. We need to show that mH is open in H for any $m \in \mathbb{N}$. By assumption, there is an integer n such that $n(G/H)$ is torsion-free; therefore we have $mnG \cap H \leq mH$, which completes the proof since mnG is open in G by the congruence subgroup property of G. □

Proposition 2. *Every finitely generated product topological subgroup of* $\mathbb{G}_m(K)$ *has the congruence subgroup property.*

Proof. This proposition just follows from Lemma 4 and Lemma 5, for any finitely generated subgroup of $\mathbb{G}_{\mathrm{m}}(K)$ is is contained in some finitely generated abelian group $\mathbb{G}_{\mathrm{m}}(O_S)$, where S is a finite subset of Ω_K. □

For the abelian-variety case, we first state a special case of Corollary 1 in [Mil72], in which Milne generalizes a result of Serre [Ser71] in the case where K were a number field.

Proposition 3. *Suppose that A is an abelian variety defined over K. Then $A(K)$ has the congruence subgroup property.* □

Corollary 2. *Suppose that A is an abelian variety defined over K. Then every finitely generated product topological subgroup of $A(K)$ has the congruence subgroup property.*

Proof. This corollary follows from Lemma 5 since $A(K)$ has the congruence subgroup property by Proposition 3 and is finitely generated by Mordell-Weil Theorem. □

Now we begin to treat the case where A is a general isotrivial semi-abelian variety defined over K. In view of Subsection 2.2.3, we only need to establish the desired result under the stronger assumption that A is defined over a finite subfield of K for the sake of proving Theorem 1; however, this stronger assumption does not simplify our proof, in which we need to go up to some finite extension of K. This motivates the following construction.

Write Ω_K^0 for Ω. For any finite extension L over K, let Ω_L^0 be the subset of Ω_L which consists of those places of L lying above some place in Ω_K^0. Fix a finite extension L over K, and a subset H of $A(L)$. We define the product topology on H to be the coarsest topology such that the diagonal embedding $H \to \prod_{w\in\Omega_L^0} A(L_w)$ is continuous, where the topology of $\prod_{w\in\Omega_L^0} A(L_w)$ is naturally induced from that of each L_w, as explained in Subsection 2.2.1. For a tower $K \subset L_1 \subset L_2$ of finite extensions, we have the following commutative diagram

$$\begin{array}{ccc} A(L_1) & \longrightarrow & \prod_{w\in\Omega_{L_1}^0} A\left((L_1)_w\right) \\ \downarrow & & \downarrow \\ A(L_2) & \longrightarrow & \prod_{u\in\Omega_{L_2}^0} A\left((L_2)_u\right) \end{array}$$

where the horizontal maps are diagonal embeddings, and the vertical maps are the embeddings induced respectively by the inclusion $L_1 \subset L_2$ and by the natural embedding $\prod_{w\in\Omega_{L_1}^0} (L_1)_w \to \prod_{u\in\Omega_{L_2}^0} (L_2)_u$. Under the vertical map of the right-hand side, $\prod_{w\in\Omega_{L_1}^0} A\left((L_1)_w\right)$ is isomorphic as topological groups to its image, which is endowed the subspace topology from $\prod_{u\in\Omega_{L_2}^0} A\left((L_2)_u\right)$. It follows that the product topology on the subset H of $A(L)$ is well-defined, independent of choices of the finite extension L over K such $H \subset A(L)$. Since

the group $A(\overline{K})$ is the union of the product topological groups $A(L)$ over all finite extensions L over K, there is therefore a unique topology on $A(\overline{K})$ such that it makes $A(\overline{K})$ a topological group, and that for any finite extension L over K and any subset H of $A(L)$, the subspace topology induced on H from $A(\overline{K})$ is equal to the product topology defined above. In view of this property, we also refer this topology on $A(\overline{K})$, and the induced subspace topology, as **product topology** .

In view of this construction, instead of proving that every finitely generated product topological subgroup of $A(K)$ has the congruence subgroup property under the assumption that A is isotrivial, we will show that this property holds for every finitely generated product topological subgroup of $A(\overline{K})$ under the same assumption. Although those two statements are in fact equivalent, our proof for the second one will be much clearer.

Proposition 4. *Suppose either that $A = \mathbb{G}_m$ or A is an abelian variety defined over K. Then every finitely generated product topological subgroup of $A(\overline{K})$ has the congruence subgroup property.*

Proof. Let H be a finitely generated subgroup of $A(\overline{K})$. Since H is finitely generated, there is a global function field L such that $H \leq A(L)$. By the preceding remark, this proposition follows from either Proposition 2 or Corollary 2 applied with K replaced by L. □

Lemma 6. *Suppose that G_1 and G_2 are topological abelian groups in which every finitely generated subgroup has the congruence subgroup property. Then*

every finitely generated subgroup of $G_1 \times G_2$ has the congruence subgroup property.

Proof. Let H be a finitely generated subgroup of $G_1 \times G_2$. For $i \in \{1, 2\}$, let H_i be the image of H under the projection $G_1 \times G_2 \to G_i$; hence H_i is finitely generated and has the congruence subgroup property. It follows that the subgroup $H_1 \times H_2$ of $G_1 \times G_2$ has the congruence subgroup property. Now Lemma 5 implies that H has the congruence subgroup property since H is a subgroup of the finitely generated abelian group $H_1 \times H_2$. □

Lemma 7. *Let A_1 and A_2 be semi-abelian varieties defined over K. Suppose that there exists a morphism $\phi : A_1(\overline{K}) \to A_2(\overline{K})$ between the two topological groups (each endowed with the product topology defined before Proposition 4) such that its kernel T is finite, and that every finitely generated product topological subgroup of $A_2(\overline{K})$ has the congruence subgroup property. Then every finitely generated product topological subgroup of $A_1(\overline{K})$ has the congruence subgroup property.*

Proof. Let H be a finitely generated product topological subgroup of $A_1(\overline{K})$. Fix a positive integer n. We only need to show that nH is open in H. Since T is finite, Lemma 2 implies the existence of an open subgroup U with a finite index m in H such that $U \cap T$ is trivial. Then we have $mH \leq U$. Since $\phi(H)$ is a finitely generated subgroup of $A_2(\overline{K})$, the subgroup $nm\phi(H)$ is open in the product topological group $\phi(H)$ by assuption. It follows that $nmH + T = \phi^{-1}(nm\phi(H))$ is open in the product topological group $H + T = \phi^{-1}(\phi(H))$,

and hence that $H \cap (nmH + T)$ is open in H. Since $nmH \leq mH \leq U$ and $U \cap T$ is trivial, we see that $U \cap (nmH + T) = nmH$. Therefore nmH and thus nH are open in H as desired. $\square$

Proposition 5. *Suppose that A is isotrivial. Then every finitely generated subgroup of the product topological group $A(\overline{K})$ has the congruence subgroup property.*

Proof. We claim that there exist a non-negative integer n_0 and an abelian variety B_0 defined over some finite subfield of $\overline{K}$ such that A and $\mathbb{G}_{\mathrm{m}}^{n_0} \times B_0$ are isogenous over $\overline{K}$. Note that B_0 is defined over some finite extension L over K. By Proposition 4 applied with K replaced by its finite extension L, any finitely generated subgroup of either the topological group $\mathbb{G}_{\mathrm{m}}(\overline{K})$ or the topological group $B_0(\overline{K})$ has the congruence subgroup property. Lemma 6 implies that every finitely generated subgroup of $(\mathbb{G}_{\mathrm{m}}^{n_0} \times B_0)(\overline{K})$ has the congruence subgroup property since $(\mathbb{G}_{\mathrm{m}}^{n_0} \times B_0)(\overline{K}) = \big(\mathbb{G}_{\mathrm{m}}(\overline{K})\big)^{n_0} \times B_0(\overline{K})$. By Lemma 7 applied with K replaced by its finite extension L, our claim proves this proposition, for it provides a morphism $A(\overline{K}) \to (\mathbb{G}_{\mathrm{m}}^{n_0} \times B_0)(\overline{K})$ with a finite kernel between the two product topological groups.

It remains to prove our claim. Since A is isotrivial, it is $\overline{K}$-isomorphic as algebraic groups to a semi-abelian variety A_0 defined over some finite subfield l of $\overline{K}$. Hence there exist a non-negative integer n_0, an abelian variety B_0, and a strictly exact sequence $1 \to \mathbb{G}_{\mathrm{m}}^{n_0} \to A_0 \to B_0 \to 0$ defined over l. Recall that, for any pair $(\mathbb{G}, T)$ of commutative algebraic groups, the set of

isomorphism classes of commutative algebraic groups E along with the strictly exact sequence $0 \to T \to E \to \mathbb{G} \to 0$ forms an abelian group $\mathrm{Ext}(\mathbb{G}, T)$ under the Baer sum. In fact, Ext is a bifunctor from the category of pairs of commutative algebraic groups to the category of abelian groups. It is not hard to see that, for any commutative algebraic groups E representing its class $[E] \in \mathrm{Ext}(\mathbb{G}, T)$, and any positive integer m, there is a natural exact sequence

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

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 $m[E] \in \mathrm{Ext}(\mathbb{G}, T)$. In our case, the isomorphism class $[A_0]$ of A_0 lies in $\mathrm{Ext}(B_0, \mathbb{G}_{\mathrm{m}}^{n_0}) = \mathrm{Ext}(B, \mathbb{G}_{\mathrm{m}})^{n_0}$. One knows (e.g., the comments following Theorem 6 of Chapter VII in [Ser88]) that $\mathrm{Ext}(B_0, \mathbb{G}_{\mathrm{m}})$ is isomorphic to the abelian group underlying the dual abelian variety B_0' of B_0. Since A_0 is defined over the finite field l, we see that $[A_0]$ lies in a subgroup of $\mathrm{Ext}(B_0, \mathbb{G}_{\mathrm{m}}^{n_0})$ which is isomorphic to the finite group $(B_0'(l))^{n_0}$. Therefore $[A_0]$ has a finite order m, that is, the commutative algebraic group $\mathbb{G}_{\mathrm{m}}^{n_0} \times B_0$ lies in $m[A_0] \in \mathrm{Ext}(B_0, \mathbb{G}_{\mathrm{m}}^{n_0})$. Hence we get a exact sequence $1 \to \mathbb{G}_{\mathrm{m}}^{n_0}[m] \to A_0 \to \mathbb{G}_{\mathrm{m}}^{n_0} \times B_0 \to 0$ defined over some finite subfield of $\overline{K}$. This concludes that A_0 and $\mathbb{G}_{\mathrm{m}}^{n_0} \times B_0$ are isogenous over $\overline{K}$ since $\mathbb{G}_{\mathrm{m}}^{n_0}[m]$ is finite. As A is $\overline{K}$-isomorphic as algebraic groups to A_0, it completes our proof. □

Corollary 3. *Let H be a finitely generated subgroup of $A(K)$. Suppose that A is isotrivial. Then for any subset J of $A(K)$, we have $J \cap \overline{H} = J \cap H$.*

Proof. Choose a finite subset S of Ω_K such that $H \leq A(O_S)$ and $S \cup \Omega = \Omega_K$. Since the product topological group $A(O_S)$ has the congruence subgroup property by Proposition 5, it follows that $A(O_S) \cap \overline{H} = H$. Also, since $S \cup \Omega = \Omega_K$, it is clear that $A(K) \cap \overline{A(O_S)} = A(O_S)$. Hence we have $J \cap \overline{H} = J \cap A(K) \cap \overline{A(O_S)} \cap \overline{H} = J \cap A(O_S) \cap \overline{H} = J \cap H$ for any subset J of $A(K)$. $\square$

For a Hausdorff topological abelian group G, its group law and underlying topology induce a natural structure of uniform space which is compatible with the topology of G. The notion of Cauchy sequences in G are defined using this uniform structure. By compatibility, the topological closure of a subspace H in G consists of exactly those points in G which are the limit of some sequence in H. In order to study the closure of a topological subgroup J in $\prod_{v \in \Omega} A(K_v)$, we prove the following result:

Lemma 8. *Let G be a Hausdorff topological abelian group with a topological subgroup J. Denote by $\overline{J}$ the topological closure of J in G. Suppose that the topology of G is generated by open subgroups. Then $\overline{J}$ is a subgroup of G. If we further assume that J is finitely generated and that every open subgroup of J has the congruence subgroup property, then every torsion element of $\overline{J}$ lies in J.*

Proof. To show that $\overline{J}$ is a subgroup of G, let $P, Q \in \overline{J}$. By the remark preceding this lemma, there are sequences $(P_i)_{i \geq 1}$ and $(Q_i)_{i \geq 1}$ of elements in J such that $P_i \to P$ and $Q_i \to Q$. Since the topology of G is generated by

open subgroups, it is easy to check that the sequence $(P_i - Q_i)_{i\geq 1}$ converges to $P - Q$, which shows $P - Q \in \overline{J}$. This concludes that $\overline{J}$ is a subgroup of G.

It remains to show that any torsion element of $\overline{J}$ lies in J under the additional hypotheses. First we note that since the topology of G is generated by open subgroups, any convergent sequence in G belongs to the set of all Cauchy sequences in G, which forms an abelian group under the termwise addition. Therefore, a torsion element P of $\overline{J}$ is the limit of a Cauchy sequence $(P_i)_{i\geq 1}$ of elements in J such that for some natural number s we have $sP_i \to O$, where O denotes the identity of G. By the fundamental theorem of finitely generated abelian groups, there is a finite subgroup T and a torsion-free subgroup F of J such that $J = T + F$. Hence for each i, we have $P_i = Q_i + R_i$ for some $Q_i \in T$ and $R_i \in F$. Let t be an integer such that $tT = \{O\}$. Our assumption that $(P_i)_{i\geq 1}$ is Cauchy clearly implies that $(tP_i)_{i\geq 1} = (tR_i)_{i\geq 1}$ is Cauchy. We claim that $(R_i)_{i\geq 1}$ is also Cauchy, that is, for any open subgroup U of J, there is a positive integer N such that $R_i - R_j \in U$ whenever $i \geq j \geq N$. To prove this claim, fix an open subgroup U of J. The finiteness of T implies that F is open in J by the congruence subgroup property of J; we may therefore assume that $U \leq F$. The congruence subgroup property of the open subgroup U of J implies that tU is open in J. Because $(tR_i)_{i\geq 1}$ is Cauchy, there is a positive integer N such that $tR_i - tR_j \in tU$ whenever $i \geq j \geq N$, which is equivalent to that $R_i - R_j \in U$ whenever $i \geq j \geq N$ since $(R_i)_{i\geq 1}$ is a sequence of elements in the torsion-free subgroup F which contains U. This proves our claim. We therefore see that $(Q_i)_{i\geq 1} = (P_i)_{i\geq 1} - (R_i)_{i\geq 1}$ is Cauchy. Hence there exist a

positive integer N_0 such that $i \geq j \geq N_0$ implies $Q_i - Q_j \in tF \cap T = \{O\}$, i.e. the sequence $(Q_i)_{i\geq 1}$ converges to Q_{N_0}. On the other hand, our assumption $sP_i \to O$ implies $stR_i = stP_i \to O$. A similar proof shows that this in turn implies that $R_i \to O$. We conclude that the limit P of the sequence $(P_i)_{i\geq 1}$ is Q_{N_0}, which lies in G. □

The following corollary generalizes Lemma 3.6 in [PV10].

Corollary 4. *Let H be a subgroup of $A(K)$. Then $\overline{H}$ is a subgroup of $\prod_{v\in\Omega} A(K_v)$. If we further assume that A is isotrivial and that H is finitely generated, then every torsion element of $\overline{H}$ lies in the image of H under the diagonal embedding $A(K) \to \prod_{v\in\Omega} A(K_v)$.*

Proof. Since $\prod_{v\in\Omega} A(K_v)$ is a Hausdorff topological abelian group with its topology generated by open subgroups, the first conclusion follows from the first part of Lemma 8. For the second part, we identify H with its image under the diagonal embedding $A(K) \to \prod_{v\in\Omega} A(K_v)$. By the assumption that A is isotrivial and that H is finitely generated, Proposition 5 shows that every topological subgroup of H, which is a topological subgroup of $\prod_{v\in\Omega} A(K_v)$, has the congruence subgroup property; hence the second part of Lemma 8 yields the desired conclusion. □

Proof of Theorem 1 in the case where $\dim X = 0$.

We denote X by Z to reflect this zero-dimensional case. As Z is zero-dimensional, it follows that $Z(K)$ is finite, and that the second conclusion

holds automatically once we have the first. In view of Subsection 2.2.3, we assume that A is defined over some finite subfield of K. Let Frob : $A \to A$ be a Frobenius endomorphism. All points of the K-variety Z is contained in $Z(L)$ for some fixed finite extension L over K. Again by Subsection 2.2.3, it suffices to establish (2.1) with K replaced by L. Hence we also assume that all points of Z is contained in $Z(K)$, i.e. for any extension K' of K we have $Z(K') = Z(K)$.

Since $\prod_{v\in\Omega} Z(K_v) \cap \overline{H} \supset Z(K) \cap H$ holds trivially, Corollary 3 implies that we only have to show $\prod_{v\in\Omega} Z(K_v) \cap \overline{H} \subset Z(K)$. Let $(Q_v)_{v\in\Omega} \in \prod_{v\in\Omega} Z(K_v) \cap \overline{H}$ with each $Q_v \in Z(K)$. Then there is a sequence $(P_n)_{n\geq 1}$ in H such that for each $v \in \Omega$, we have $P_n \to Q_v$ in the topological group $A(K_v)$. Since all the Q_v's lie in $A(K)$, we form the subgroup J of $A(K)$ generated by elements of H and all the Q_v's. As there are only finitely many distinct Q_v's, the subgroup J is still finitely generated. Now we have $P_n - Q_v \to 0$ in the v-adic topological group J. By Proposition 1, for each $v \in \Omega$ and each $r \geq 1$, there exists an N such that $P_n - Q_v \in \mathrm{Frob}^r(A(K))$ for any $n \geq N$. It follows that for any $v, w \in \Omega$, the element $Q_v - Q_w$ belongs to $\cap_{r\geq 1} \mathrm{Frob}^r(A(K))$. Since $\mathrm{Frob}(A(K)) \leq A(K^p)$, it is clear that $\cap_{r\geq 1} \mathrm{Frob}^r(A(K))$ is contained in the subgroup $A(\cap_{r\geq 1} K^{p^r})$, which is finite as $\cap_{r\geq 1} K^{p^r}$ is. Now we let $w_0 \in \Omega$ be fixed. Since $Q_v - Q_{w_0}$ belongs a fixed finite group for all $v \in \Omega$, we conclude that $(Q_v - Q_{w_0})_{v\in\Omega} = (Q_v)_{v\in\Omega} - Q_{w_0} \in \prod_{v\in\Omega} A(K_v)$ is a torsion point in $\overline{J}$. Now Corollary 4 implies that it lies in the image of J under the diagonal embedding $A(K) \to \prod_{v\in\Omega} A(K_v)$, and therefore $(Q_v)_{v\in\Omega} = Q_{w_0} \in Z(K)$. $\square$

Example 1. The following example shows that 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. Let K be a purely transcendental extension of a finite field k with transcendence degree 1. Fix a place v_0 of K. For any $\alpha, \beta \in K$, I will construct a sequence $(x_n)_{n\geq 1}$ in K such that $x_n \to \alpha$ under the v_0-adic topology while $x_n \to \beta$ under all other v-adic topology where $v \neq v_0$. In the case where $v_0 \in \Omega$, and α, β are distinct nonzero elements of K, the limit of the sequence $(x_n)_{n\geq 1}$ is an element in $\prod_{v\in\Omega} Z(K_v) \cap \overline{\mathbb{G}_{\mathrm{m}}(K)} \setminus Z(K)$, where Z is the zero-dimensional K-subvariety $\{\alpha, \beta\}$ of $\mathbb{G}_{\mathrm{m}}$. Choose a transcendence basis $\{t\}$ of K over k such that $t \notin O_{v_0}$. Therefore we have $K = k(t)$ and the place $v_0 \in \Omega_K$ comes from the degree map in the polynomial ring $k[t]$, and the set $\Omega_K \setminus \{v_0\}$ is in one-to-one correspondence with the set of monic irreducibles in $k[t]$. Write $\beta - \alpha = \frac{a}{b}$, where $a, b \in k[t]$. Enumerate all irreducibles in $k[t]$ as $p_1, p_2, p_3, \ldots$. Let $x_n = \frac{(\prod_{i=1}^n p_i)^n + a}{(\prod_{i=1}^n p_i)^{2n} + b} + \alpha$. It is clear that $x_n \to \alpha$ under the v_0-adic topology. On the other hand,

$$x_n - \beta = \frac{(\prod_{i=1}^n p_i^n)\,(b - a\prod_{i=1}^n p_i^n)}{b\,(\prod_{i=1}^n p_i^{2n} + b)}.$$

In this expression, note that, for each j, the numerator is divisible by p_j^n as $n \geq j$, while the denominator is not divisible by $p_j^{e_j+1}$ as $n \geq \max\{j, e_j + 1\}$, where $b = \prod_{i=1}^n p_i^{e_i}$ is the prime factorization. Therefore we see that $x_n \to \beta$ under the v-adic topology for any $v \neq v_0$.

Example 2. For any irreducible zero-dimensional K-subvariety Z of A and any subset H of $A(K)$, the equality $\prod_{v\in\Omega} Z(K_v) \cap \overline{H} = Z(K) \cap \overline{H}$ holds trivially;

however, even if H is a subgroup, it is still possible that the unique point of $Z(K) \cap \overline{H}$ does not lie in H, as the following example shows. Take $A = \mathbb{G}_{\mathrm{m}}$. Let $K = k(t)$ be a purely transcendental extension of a finite field k with transcendence degree 1. Enumerate all irreducibles in $k[t]$ as $p_1, p_2, p_3, \ldots$. Choose an element $\alpha \in K \setminus \{0, 1\}$. For every $n \geq 1$, let $x_n = \frac{(\prod_{i=1}^{n} p_i)^n}{(\prod_{i=1}^{n} p_i)^{2n}+1} + \alpha$. As in Example 1, we see that $x_n \to \alpha$ under the v-adic topology for all $v \in \Omega_K$. Write $\alpha = \frac{c}{d}$, where c and d are relatively prime elements in $k[t]$. Choose a natural number N such that every p_n with $n \geq N$ does not divide either c or d in $k[t]$. Since

$$x_n = \frac{d \prod_{i=1}^{n} p_i^n + c\,(\prod_{i=1}^{n} p_i^{2n} + 1)}{d\,(\prod_{i=1}^{n} p_i^{2n} + 1)}, \tag{2.10}$$

it follows that for any $n \geq N$, there is an irreducible in $k[t]$ other than $p_1, p_2, \ldots, p_n$ such that it divides the denominator but not the numerator in (2.10). Now we construct a sequence $(n_m)_{m \geq 1}$ inductively as follows. Take $n_1 = N$. Having defined $n_1, \ldots, n_{m-1}$ for some $m \geq 2$, we let n_m be the smallest natural number s such that every irreducible in $k[t]$ dividing either the denominator or the numerator in (2.10) with n replaced by any of $n_1, \ldots, n_{m-1}$ lies in the set $\{p_1, p_2, \ldots, p_s\}$. Now let H be the subgroup of $\mathbb{G}_{\mathrm{m}}(K)$ generated by $\{x_{n_m} : m \geq 1\}$. Note that $\alpha \in \overline{H}$ since $(x_{n_m})_{m \geq 1}$ is a subsequence of $(x_n)_{n \geq 1}$, which converges to α under the v-adic topology for every $v \in \Omega_K$. On the other hand, our construction shows that, for each $m \geq 2$, when the nonzero element x_{n_m} in $K = k(t)$ is written as the quotient of two relatively prime elements in $k[t]$, the denominator has an irreducible in $k[t]$ not dividing either the denominator or the numerator of any of $\alpha, x_{n_1}, x_{n_2}, \ldots, x_{n_{m-1}}$. Since

$\alpha \neq 1$, we therefore conclude that $\alpha \notin H$.

Note that the above two examples can be easily modified to similar ones in the setting with K replaced by the field $\mathbb{Q}$ of rational numbers.

2.4 Inductive Step

Consider the following purely algebraic question: Let N be a non-negative integer. Suppose that, for each $v \in \Omega$, we have an ideal I_v of the polynomial ring $K_v[X_0, \ldots, X_N]$, which is generated by elements of $K_v^{p^m}[X_0, \ldots, X_N]$ for some positive integer m. Does it follow that $\bigcap_{v\in\Omega} (I_v \cap K[X_0, \ldots, X_N])$ is generated by elements of $K^{p^m}[X_0, \ldots, X_N]$? We will provide a positive answer, which will play a key role in the inductive step of the proof of Theorem 1.

In order to answer this question, we shall make use of the iterative derivation. Let L be a field of characteristic p. An iterative derivation on 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 any $i \geq 0$ and $x, y \in L$.

iii) $D^{(i)}D^{(j)} = \binom{i+j}{i} D^{(i+j)}$ for any $i, j \geq 0$, 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

Note that the property (iii) implies the composition of operators in $\{D^{(i)}\}_{i\geq 0}$ is commutative. For each $i \geq 0$, let $i = \sum_{n=0}^{d} i_n p^n$ be its base p expansion, that is, each i_n is a nonnegative integer less than p. Repeated applications of the property (iii) gives

$$\prod_{n=0}^{d} \left(D^{(p^n)}\right)^{i_n} = c_i D^{(i)}, \qquad \text{where } c_i = \prod_{n=0}^{d} \left[\binom{\sum_{s=0}^{n} i_s p^s}{i_n p^n} \prod_{a=1}^{i_n} \binom{ap^n}{p^n} \right].$$

The following result, known as Lucas's lemma (e.g., [Sch39]), shows that $c_i \in L^*$; therefore we have an explicit formula which expresses $D^{(i)}$ in terms of $\{D^{(p^n)}\}_{n\geq 0}$.

Lemma 9. *Let $i = \sum_{n\geq 0} i_n p^n$ and $j = \sum_{n\geq 0} j_n p^n$ be the base p expansions of the nonnegative integers i and j. Then $\binom{i}{j}$ is not divisible by p if and only if $i_n \geq j_n$ for all n.* □

For any positive integer m, the preceding remark implies that the subset $L_m = \{x \in L : D^{(l)}(x) = 0 \text{ if } 1 \leq l < p^m\}$ is a subfield of L. Inspired by the proof of Claim 2.2.3 in [Ogu78], we consider the additive endomorphism $\sum_{i=0}^{p^m-1} (-t)^i D^{(i)}$ on L and prove the following lemma.

Lemma 10. *Suppose there exists $t \in L$ such that $D^{(i)}\left((-t)^j\right) = (-1)^i \binom{j}{i} t^{j-i}$ for any $i \geq 0$. Then for any $c \in L$ and any $m \geq 0$, the element $\sum_{i=0}^{p^m-1} (-t)^i D^{(i)}(c)$ lies in L_m.*

Proof. In view of the remark preceding Lemma 9, it suffices to show that for every natural number s less than m we have

$$D^{(p^s)}\left(\sum_{i=0}^{p^m-1}(-t)^i D^{(i)}(c)\right)=0.$$

Fix such a natural number s and put $j=p^s$. By the property (iii) of iterative derivations and the assumption $D^{(i)}\left((-t)^j\right)=(-1)^i\binom{j}{i}t^{j-i}$, we get

$$D^{(j)}\left(\sum_{i=0}^{p^m-1}(-t)^i D^{(i)}(c)\right)=\sum_{i=0}^{p^m-1}\sum_{l=0}^{j}(-1)^l\binom{i}{l}\binom{i+j-l}{i}(-t)^{i-l}D^{(i+j-l)}(c).$$

Consider the base p expansions $i=\sum_{n\geq 0}i_n p^n$, $j=\sum_{n\geq 0}j_n p^n$ and $l=\sum_{n\geq 0}l_n p^n$ of i, j and l. Lemma 9 shows that $\binom{i}{l}\binom{i+j-l}{i}$ 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

$$\begin{array}{rl} & D^{(j)}\left(\sum_{i=0}^{p^m-1}(-t)^i D^{(i)}(c)\right)\\ = & \sum_{i=0}^{p^m-1}\binom{i+j}{i}(-t)^i D^{(i+j)}(c)+\sum_{i=0}^{p^m-1}(-1)^j\binom{i}{j}(-t)^{i-j}D^{(i)}(c)\\ = & \sum_{i=j}^{j+p^m-1}\binom{i}{j}(-t)^{i-j}D^{(i)}(c)+\sum_{i=j}^{p^m-1}(-1)^j\binom{i}{j}(-t)^{i-j}D^{(i)}(c)\\ = & \sum_{i=p^m}^{p^m+p^s-1}\binom{i}{p^s}(-t)^{i-p^s}D^{(i)}(c), \end{array}$$

where the last equality holds because $1+(-1)^j=1+(-1)^p=0$ in K. Finally, since $s<m$, the s-th digit of the p-adic expension of natural numbers between p^m and p^m+p^s-1 is always zero, it then follows from Lemma 9 that each term in the last sum vanishes. This finishes the proof. □

We extend $\{D^{(i)}\}_{i\geq 0}$ to operators 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 after

the extensions, $\{D^{(i)}\}_{i\geq 0}$ still forms an iterative derivation on $L[X_0,\ldots,X_N]$ with $L_m[X_0,\ldots,X_N] = \{g \in K[X_0,\ldots,X_N] : D^{(l)}(g) = 0 \text{ if } 1 \leq l < p^m\}$ for any $m \geq 0$. Now we are able to give a criterion which determines if an ideal of the polynomial ring $L[X_0,\ldots,X_N]$ is generated by a collection of polynomials with coefficients in the subfield L_m.

Lemma 11. *Suppose there exists $t \in L$ such that $D^{(i)}\left((-t)^j\right) = (-1)^i\binom{j}{i}t^{j-i}$ for any $i \geq 0$. Let m be a positive integer, and I be an ideal of $L[X_0,\ldots,X_N]$. Then I is generated by elements of $L_m[X_0,\ldots,X_N]$ if and only if the conditions $D^{(i)}(I) \subset I$ hold for all $1 \leq i < p^m$.*

Proof. Suppose that I is generated by elements of $L_m[X_0,\ldots,X_N]$. Then each $g \in I$ may be expressed as $g = \sum_{j=1}^{s} g_j h_j$ with $g_j \in I \cap L_m[X_0,\ldots,X_N]$ and $h_j \in L[X_0,\ldots,X_N]$; for each $1 \leq i < p^m$ and $1 \leq j \leq s$, we have $D^{(i)}(g_j) = 0$ therefore conclude that $D^{(i)}(g) = \sum_{j=1}^{s}\sum_{l=0}^{i} D^{(l)}(g_j)D^{(i-l)}(h_j) = \sum_{j=1}^{s} g_j D^{(i)}(h_j) \in I$. Hence the conditions $D^{(i)}(I) \subset I$ hold for all $1 \leq i < p^m$

For the other implication, suppose that I is an ideal of $L[X_0,\ldots,X_N]$ satisfying $D^{(i)}(I) \subset I$ for all $1 \leq i < p^m$. Let J be the ideal of $L[X_0,\ldots,X_N]$ generated by $I \cap L_m[X_0,\ldots,X_N]$. It is clear that $J \subset I$. Now we show that in fact $I = J$, which will complete the proof. For the sake of contradiction, suppose that $I \setminus J$ is non-empty. Choose a lexicographic order on the set of monomials in $X_0,\ldots,X_N$. With respect to this order, for any non-zero element 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 non-zero coefficient. Now let f be an

element in $I \setminus J$ with the smallest degree. Since I and J are ideals, we may assume that in the expression of f, the nonzero coefficient of the unique term involving the degree of f is 1. For any positive integer i, since $D^{(i)}(1) = 0$, we note that $D^{(i)}(f)$ has a smaller degree than f, and hence conclude that $D^{(i)}(f) \notin I \setminus J$ by the choice of f. For every $1 \leq i < p^m$, since $D^{(i)}(f) \in D^{(i)}(I) \subset I$, we see that $D^{(i)}(f)$ is in I and therefore in J. Consider the element $g = f + \sum_{i=1}^{p^m-1}(-t)^i D^{(i)}(f)$ in $L[X_0, \ldots, X_N]$, which is in I since $D^{(i)}(f) \subset I$ for every $0 \leq i < p^m$. Lemma 10 shows that g is in $L_m[X_0, \ldots, X_N]$, and hence it is by definition in J. The contradiction $f = g - \sum_{i=1}^{p^m-1}(-t)^i D^{(i)}(f)) \in J$ finishes the proof. $\square$

In order to use iterative derivation to the question proposed in the beginning of this section, we first construct an iterative derivation on K. From field theory, there exists $t \in K$ such that K is a finite separable extension of the function field $\mathbf{F}_p(t)$ of one variable over the prime field. Choose a place $v \in \Omega_K$ which restricts to a place $w \in \Omega_{\mathbf{F}_p(t)}$ corresponding to a separable irreducible polynomial in $\mathbf{F}_p[t]$ such that $\mathbf{F}_p(t)_w = K_v$. Let α be a root of this polynomial. Then $\mathbf{F}_p(t)_w$ is a natural subfield of $\mathbf{F}_p(\alpha)((t-\alpha))$ and we have a tower $\mathbf{F}_p(\alpha)(t) \subset K(\alpha) \subset \mathbf{F}_p(\alpha)((t-\alpha))$ of fields. By Remark 1 in [GV87], there exists an iterative derivation $\{D^{(i)}\}_{i \geq 0}$ on $K(\alpha)$ such that $D^{(j)}((t-\alpha)^i) = \binom{i}{j}(t-\alpha)^{i-j}$ and $(K(\alpha))^{p^m} = \{x \in K(\alpha) : D^{(l)}(x) = 0 \text{ if } 1 \leq l < p^m\}$ for any $i, j, m \geq 0$. It is not hard to check that $D^{(j)}(t^i) = \binom{i}{j}(t)^{i-j}$, and by separability assumptions that $K^{p^m} = K_m = \{x \in K : D^{(l)}(x) = 0 \text{ if } 1 \leq$

$l < p^m\}$ for any $i, j, m \geq 0$. One easily verifies $D^{(i)}\left((-t)^j\right) = (-1)^i\binom{j}{i}t^{j-i}$ for any $i \geq 0$.

Lemma 12. *Let N be a non-negative integer. For each $v \in \Omega$, let I_v be an ideal of $K_v[X_0, \ldots, X_N]$. Let m be a positive integer. Suppose that for each $v \in \Omega$, I_v is generated by elements of $K_v^{p^m}[X_0, \ldots, X_N]$. Then $\bigcap_{v\in\Omega}\left(I_v \cap K[X_0, \ldots, X_N]\right)$ is generated by elements of $K^{p^m}[X_0, \ldots, X_N]$.*

Proof. For every nonnegative integer i, it is a fact that the endomorphism $D^{(i)}$ on K is continuous with respect to any place of K. Therefore, for each place $v \in \Omega$, we have an iterative derivation $\{D_v^{(i)}\}_{i\geq 0}$ on K_v which extend $\{D^{(i)}\}_{i\geq 0}$. By continuity, all elements in $K_v^{p^m}$ are mapped to zero by those $D_v^{(i)}$ with $1 \leq i < p^m$. Extend $\{D_v^{(i)}\}_{i\geq 0}$ to an iterative derivation on the polynomial ring $K_v[X_0, \ldots, X_N]$ by sending X_i to 0 for every $i \in \{0, 1, \ldots, N\}$. Since I_v is generated by elements of $K_v^{p^m}[X_0, \ldots, X_N]$, which are mapped to zero by those $D_v^{(i)}$ with $1 \leq i < p^m$, it follows that for these i we have $D_v^{(i)}(I_v) \subset I_v$ for each $v \in \Omega$. But then

$$\begin{array}{rl} & D^{(i)}\left(\bigcap_{v\in\Omega}\left(I_v \cap K[X_0, \ldots, X_N]\right)\right) \\ \subset & \bigcap_{v\in\Omega}\left(D_v^{(i)}\left(I_v \cap K[X_0, \ldots, X_N]\right)\right) \\ \subset & \bigcap_{v\in\Omega}\left(D_v^{(i)}(I_v) \cap K[X_0, \ldots, X_N]\right) \\ \subset & \bigcap_{v\in\Omega}\left(I_v \cap K[X_0, \ldots, X_N]\right) \end{array}$$

for all $1 \leq i < p^m$. Now Lemma 11 completes the proof. □

We now shift our attention back to Theorem 1. In view of Subsection 2.2.3 shows, we will assume that A is defined over a finite subfield of K, In

this case, there is a Frobenius endomorphism Frob : $A \to A$, which induces an injective group homomorphism Frob : $A(K) \to A(K)$. For each positive integer m, note that $\overline{\mathrm{Frob}^m(A(K))} \subset \prod_{v\in\Omega} A(K_v^{p^m})$. This motivates us to prove the following result, which is crucial for the inductive step of the proof of Theorem 1.

Proposition 6. *Let X be a closed K-subvariety of A. Let m be a positive integer. Suppose that A is defined over a finite subfield of K, and that X is not defined over K^{p^m}. Then there is a proper closed K-subvariety Y of X such that $X(K_v) \cap A(K_v^{p^m}) \subset Y(K_v)$ for all $v \in \Omega$.*

Proof. Since any finite subfield of K is contained in K^{p^m}, we may embed A into some projective space $\mathbb{P}^N$ so that its underlying variety is expressed in the form (2.2), where I and J are homogeneous ideals in the polynomial ring $K^{p^m}[X_0, \ldots, X_N]$. Since X is a closed K-subvariety of A, it is described by the same expression as the underlying variety of A except I is replaced by a homogeneous ideal $\tilde{I}$ in the polynomial ring $K[X_0, \ldots, X_N]$ such that $I \subset \tilde{I} \cap K^{p^m}[X_0, \ldots, X_N]$. Fix a place $v \in \Omega$. Consider the ideal $\tilde{I}_v$ in $K_v[X_0, \ldots, X_N]$ generated by homogeneous polynomials which vanish on the subset $X(K_v) \cap A(K_v^{p^m})$ of $\mathbb{P}^N(K_v)$. Let Y be the variety in $\mathbb{P}^N$ given by (2.2) with I replaced by $\left(\bigcap_{v\in\Omega}(\tilde{I}_v \cap K[X_0, \ldots, X_N])\right) \cap K^{p^m}[X_0, \ldots, X_N]$, which is a homogeneous ideal in $K^{p^m}[X_0, \ldots, X_N]$. By construction, we see that Y is defined over K^{p^m}, and that $X(K_v) \cap A(K_v^{p^n}) \subset Y(K_v)$ for all $v \in \Omega$ To see

that Y is a closed subvariety of X, we need to show that

$$\tilde{I} \subset \left\{ \left(\bigcap_{v \in \Omega} (\tilde{I}_v \cap K[X_0, \ldots, X_N]) \right) \cap K^{p^m}[X_0, \ldots, X_N] \right\} K[X_0, \ldots, X_N]. \tag{2.11}$$

We claim that $\tilde{I}_v$ is generated by elements in $K_v^{p^m}[X_0, \ldots, X_N]$ for each $v \in \Omega$. Then Lemma 12 gives that $\bigcap_{v \in \Omega}(\tilde{I}_v \cap K[X_0, \ldots, X_N])$ is generated by elements in $K^{p^m}[X_0, \ldots, X_N]$. Therefore the ideal in the right side of (2.11) is just equal to $\left(\bigcap_{v \in \Omega}(\tilde{I}_v \cap K[X_0, \ldots, X_N])\right)$, which clearly contains I by construction. Note that $Y \neq X$ since Y is defined over K^{p^m} while X is not.

It remains to prove our claim. By noting that $X(K_v) \cap A(K_v^{p^m}) \subset \mathbb{P}^N(K_v^{p^m})$, our claim follows from the a general result, which states that for a subfield F of a field L, the ideal generated by those homogeneous polynomials in $L[X_0, \ldots, X_N]$ vanishing on a subset of $\mathbb{P}^N(F)$ is generated by elements in $F[X_0, \ldots, X_N]$. We also give an alternative proof in our case as follows. Recall the iterative derivation $\{D_v^{(i)}\}_{i \geq 0}$ on $K_v[X_0, \ldots, X_N]$ in the proof of Lemma 12. Let $f \in I_v$ be a homogeneous polynomial and $P \in X(K_v) \cap A(K_v^{p^m})$. By definition, we have $f(P) = 0$. For each $1 \leq i < p^m$, we also have $D_v^{(i)}(f(P)) = D_v^{(i)}(f)(P)$ since $f \in K_v[X_0, \ldots, X_N]$ and $P \in \mathbb{P}^N(K_v^{p^m})$ as well as $D_v^{(i)}$ which vanishes on $K_v^{p^m}$, acts on a polynomial in $K_v[X_0, \ldots, X_N]$ by acting only on its coefficients. This shows $D_v^{(i)}(I_v) \subset I_v$ for all $1 \leq i < p^m$, which proves our claim according to Lemma 11 applied to the case $L = K_v$. $\square$

We note that if A is defined over a finite subfield k of K, them a single point of A is defined over K^{p^m} for any $m > 0$, for it is isomorphic to the

distinguished point in A, where the isomorphism and the distinguished point are both defined over k which is contained in K^{p^m}. Therefore Proposition 6 does not apply in the case where X is a singleton, and the inductive step of the proof of Theorem 1, namely Proposition 7 below, does not apply in the case where X has dimension zero.

One more lemma is needed before we may carry out the inductive step. For any subgroup H of $A(K)$, Lemma 4 implies that $\overline{H}$ is a subgroup of $\prod_{v\in\Omega} A(K_v)$. Hence $\overline{H}$ is a subgroup of $\overline{J}$ for any subgroups $H \leq J$ of $A(K)$; in particular, the diagonal embedding $J \to \overline{J}$ canonically induces a group homomorphism $J/H \to \overline{J}/\overline{H}$.

Lemma 13. *Let $H \leq J$ be subgroups of $A(K)$. Consider the group homomorphism*

$$J/H \to \overline{J}/\overline{H} \tag{2.12}$$

induced by the diagonal embedding $J \to \overline{J}$. Suppose that A is isotrivial. If H is finitely generated, then (2.12) is injective. If we further assume that the index $[J : H]$ is finite, then (2.12) is actually an isomorphism.

Proof. If H is finitely generated, then Corollary 3 gives $J \cap \overline{H} = H$, which exactly means that (2.12) is injective. Now assume further that $[J : H]$ is finite. We have to show that (2.12) is surjective. Let $y \in \overline{J}$ be the limit in the topological group $\prod_{v\in\Omega} A(K_v)$ of a sequence (y_i) in J. Since H is open in the product topological group J by Proposition 5, there is an i_0 such that the sequence $(y_i - y_{i_0})$ will eventually lie in H. Hence the limit $y - y_{i_0}$ of this

sequence lies in $\overline{H}$, that is, the coset $y+\overline{H}$ contains the element $y_{i_0} \in J$, which is the surjectivity as desired. $\square$

Proposition 7. *Let H be a finitely generated subgroup of $A(K)$, and X be a positive-dimensional closed K-subvariety of A. Suppose that A is defined over a finite subfield of K, and that any irreducible component of X with the largest dimension is not isotrivial. Then there is a closed K-subvariety Y of X with a smaller dimension, satisfying $\prod_{v\in\Omega} X(K_v) \cap \overline{H} \subset \prod_{v\in\Omega} Y(K_v)$.*

Proof. Fix a Frobenius endomorphism $\mathrm{Frob} : A \to A$. Note that there is a finitely generated subgroup H_0 of $A(K)$ such that $H \leq H_0$ and $\mathrm{Frob}(H_0) \leq H_0$; for example, we may take $H_0 = A(O_S)$ for some finite subset S of Ω_K. Since $\prod_{v\in\Omega} X(K_v) \cap \overline{H} \subset \prod_{v\in\Omega} X(K_v) \cap \overline{H_0}$, it is enough to prove the desired result under the additional hypothesis that $\mathrm{Frob}(H) \leq H$.

Assume that X is irreducible. First we show that there is a positive integer N such that for any $\gamma \in H$ the variety $X - \gamma$ is not defined over K^{p^N}. Indeed, if for every positive integer n there was a $\gamma_n \in H$ such that $X - \gamma_n$ was defined over K^{p^n}, then the argument in the proof of Theorem A. Part 1 in [AV92] using Hilbert schemes would conclude that a translate of X by some point in $A(\overline{K})$ is defined over a finite subfield of $\overline{K}$, contradicting to the hypothesis that X is not isotrivial. Therefore we have a positive integer N such that for any fixed $\gamma \in H$ the variety $X - \gamma$ is not defined over K^{p^N} and hence Proposition 6 implies that there is a proper closed K-subvariety Y of $X - \gamma$ such that $(X - \gamma)(K_v) \cap A(K_v^{p^N}) \subset Y(K_v)$ for all $v \in \Omega$.

Since the injective group homomorphism Frob : $A(K) \to A(K)$ preserves the finitely generated subgroup H, the index $[H : \mathrm{Frob}^N(H)]$ is finite. Hence Lemma 13 implies that there are finitely many α_i's in H such that $\overline{H} = \bigcup_i \left(\alpha_i + \overline{\mathrm{Frob}^N(H)}\right)$. By what has been just shown, for each i there is a proper closed K-subvariety Y_i of $X - \alpha_i$ such that $(X - \alpha_i)(K_v) \cap A(K_v^{p^N}) \subset Y_i(K_v)$ for all $v \in \Omega$. Therefore $Y_i + \alpha_i$ is a proper closed K-subvariety of X such that $X(K_v) \cap \left(\alpha_i + A(K_v^{p^N})\right) \subset (Y_i + \alpha_i)(K_v)$ for all $v \in \Omega$. Since X is irreducible, the dimension of $Y_i + \alpha_i$ is smaller than that of X. Let $Y = \bigcup_i (Y_i + \alpha_i)$. Then Y is a closed K-subvariety of X with a smaller dimension, satisfying that for all $v \in \Omega$,

$$\begin{array}{rl} & X(K_v) \cap \left(\bigcup_i \left(\alpha_i + A(K_v^{p^N})\right)\right) \\ = & \bigcup_i \left(X(K_v) \cap \left(\alpha_i + A(K_v^{p^N})\right)\right) \\ \subset & \bigcup_i (Y_i + \alpha_i)(K_v) \\ = & Y(K_v). \end{array}$$

Now we remove the assumption that X is irreducible. Let $X = \bigcup_j X_j$ be a decomposition of X of finitely many irreducible components. For those j's which X_j has its dimension equal to that of X and hence is not isotrivial, we have just shown that there is a closed K-subvariety Y_j of X_j with a smaller dimension, satisfying $X_j(K_v) \cap \left(\bigcup_i \left(\alpha_i + \mathrm{Frob}^N(A(K_v))\right)\right) \subset Y_j(K_v)$ for all $v \in \Omega$. For the remaining j's, we simply put $Y_j = X_j$. Let $Y = \bigcup_j Y_j$. Then Y is a closed K-subvariety of X with a smaller dimension. Note that

$\overline{\mathrm{Frob}^N(H)} \subset \overline{\mathrm{Frob}^N(A(K))} \subset \prod_{v\in\Omega} A(K_v^{p^N})$. Then we have

$$\begin{aligned}
& \textstyle\prod_{v\in\Omega} X(K_v) \cap \overline{H} \\
= \; & \textstyle\prod_{v\in\Omega} X(K_v) \cap \bigcup_i \left(\alpha_i + \overline{\mathrm{Frob}^N(H)}\right) \\
\subset \; & \left(\textstyle\prod_{v\in\Omega} X(K_v)\right) \cap \prod_{v\in\Omega} \bigcup_i \left(\alpha_i + A(K_v^{p^N})\right) \\
\subset \; & \textstyle\prod_{v\in\Omega} \left(X(K_v) \cap \bigcup_i \left(\alpha_i + A(K_v^{p^N})\right)\right) \\
\subset \; & \textstyle\prod_{v\in\Omega} \left(\left(\bigcup_j X_j(K_v)\right) \cap \bigcup_i \left(\alpha_i + A(K_v^{p^N})\right)\right) \\
\subset \; & \textstyle\prod_{v\in\Omega} \bigcup_j \left(X_j(K_v) \cap \bigcup_i \left(\alpha_i + A(K_v^{p^N})\right)\right) \\
\subset \; & \textstyle\prod_{v\in\Omega} \bigcup_j Y_j(K_v) \\
= \; & \textstyle\prod_{v\in\Omega} Y(K_v).
\end{aligned}$$

□

Proof of Theorem 1. In view of Subsection 2.2.3, we assume that A is defined over some finite subfield of K. We prove the desired conclusions by induction on the dimension of X. The base case where the dimension of X is zero has been proved in the end of Section 2.3. For the inductive step, by the assumption on X in Theorem 1, Proposition 7 concludes the existence of a closed K-subvariety Y of X with smaller dimension such that $\prod_{v\in\Omega} X(K_v) \cap \overline{H} \subset \prod_{v\in\Omega} Y(K_v)$. The assumption on X also ensures that Y has no positive-dimensional isotrivial closed K-subvarieties; hence the inductive hypothesis implies that $\prod_{v\in\Omega} Y(K_v) \cap \overline{H} = Y(K) \cap H$ and the common set is finite. It follows that

$$\prod_{v\in\Omega} X(K_v) \cap \overline{H} \subset \prod_{v\in\Omega} Y(K_v) \cap \overline{H} = Y(K) \cap H \subset X(K) \cap H. \tag{2.13}$$

Since the inclusion $X(K) \cap H \subset \prod_{v\in\Omega} X(K_v) \cap \overline{H}$ is trivial, we conclude that (2.13) is indeed a chain of equalities, in which the common set is finite. □

Example 3. The following example shows that the conclusion in Theorem 1 would fail, even in the case where $\dim X = 1$, if we removed the hypothesis that X has no positive-dimensional isotrivial $\overline{K}$-subvarieties. Let $K = k(t)$ be a purely transcendental extension of a finite field k with transcendence degree 1. Take $H = \langle t \rangle$ be the cyclic subgroup of $\mathbb{G}_{\mathrm{m}}(K)$ generated by t, and a cofinite subset Ω of Ω_K such that $t \in O_v^*$ for every $v \in \Omega$. I will construct a point $(\alpha_v)_{v\in\Omega} \in \overline{H} \setminus \mathbb{G}_{\mathrm{m}}(K)$, and therefore conclude that $\prod_{v\in\Omega} \mathbb{G}_{\mathrm{m}}(K_v) \cap \overline{H} = \overline{H} \neq \mathbb{G}_{\mathrm{m}}(K) \cap H$. Consider the sequence $(t^{q^{n!}})_{n\geq 1}$ in H, where $q = |k|$. Note that for any $m \geq n$, we have

$$t^{q^{m!}} - t^{q^{n!}} = \left(t^{q^{n!(\frac{m!}{n!}-1)}} - t \right)^{q^{n!}},$$

in which we see that $t^{q^{n!(\frac{m!}{n!}-1)}} - t$ will be divisible by an arbitrary irreducible in $k[t]$ provided that n is large enough, hence $t^{q^{m!}} - t^{q^{n!}} \to 0$ in every place of K which corresponds to an irreducible in $k[t]$. Since $t \in O_v^*$ for every $v \in \Omega$, the above observation shows that $(t^{q^{n!}})_{n\geq 1}$ is a Cauchy sequence in the product topological group H. Since $\prod_{v\in\Omega} \mathbb{G}_{\mathrm{m}}(K_v)$ is complete, there is a unique $(\alpha_v)_{v\in\Omega} \in \overline{H} \subset \prod_{v\in\Omega} \mathbb{G}_{\mathrm{m}}(K_v)$ such that for any $v \in \Omega$ we have $t^{q^{n!}} \to \alpha_v$ in $\mathbb{G}_{\mathrm{m}}(K_v)$. Note that $t^{q^{n!}} - 1 = (t-1)^{q^{n!}} \to 0$ in the place v_{t-1} of K which corresponds to the irreducible $t - 1$ in $k[t]$; while $(t-1)^{q^{n!}}$ does not converge to zero in any $v \in \Omega \setminus \{v_{t-1}\}$. Therefore we see that $\alpha_{v_{t-1}} = 1 \neq \alpha_v$ for any $v \in \Omega \setminus \{v_{t-1}\}$, and conclude that $(\alpha_v)_{v\in\Omega} \notin \mathbb{G}_{\mathrm{m}}(K)$. Also we note that $\mathbb{G}_{\mathrm{m}}(K) \cap H = H$ is clearly an infinite set. Since $\mathbb{G}_{\mathrm{m}}$ is irreducible with dimension one, this example also shows that the conclusion in Proposition 7

would fail if we removed the hypothesis that any irreducible component of X with the largest dimension is not isotrivial.

Chapter 3

Hyperplanes inside an Algebraic Torus and a Conjecture of Skolem over a Global Function Field

3.1 Introduction

We keep the notations of Chapter 2, which are briefly recalled as follows. Let K be a global field of positive characteristic p. We fix a co-finite subset Ω of the set Ω_K of all places of K. For each $v \in \Omega$, we denote by K_v the completion of K at v, by O_v the valuation ring in K_v, and by m_v the maximal ideal in O_v. For a finite subset S of Ω, the subring of S-integers in K is denoted by

$$O_S = \{x \in K : x \in O_v \text{ for each } v \notin S\}.$$

Fix a natural number N and consider the split algebraic torus $\mathbb{G}_{\mathrm{m}}^N$. In Subsection 2.2.2 of Chapter 2, we see that there is a natural topology on $\prod_{v\in\Omega} \mathbb{G}_{\mathrm{m}}^N(K_v)$ making it a complete topological group. For any subgroup H of $\mathbb{G}_{\mathrm{m}}^N(K)$, we denote by $\overline{H}$ the topological closure of the image of H in $\prod_{v\in\Omega} \mathbb{G}_{\mathrm{m}}^N(K_v)$ under the diagonal embedding $\mathbb{G}_{\mathrm{m}}^N(K) \to \prod_{v\in\Omega} \mathbb{G}_{\mathrm{m}}^N(K_v)$.

Let X be a K-subvariety of $\mathbb{G}_{\mathrm{m}}^N$ and H be a subgroup of $\mathbb{G}_{\mathrm{m}}^N(K)$. The subset $\prod_{v\in\Omega} X(K_v) \cap \overline{H}$ is clearly an obstruction to the existence of points

in $X(K) \cap H$. In [HV10], Harari and Voloch notice that this obstruction is closed related to an old conjecture proposed by Skolem in [Sko37], which seems to have been largely ignored in the recent literature. Indeed, this conjecture, about which very little is know, predicts that, in the case where K were a number field, X is a subvariety of $\mathbb{G}_{\mathrm{m}}^N$ cut by a K-hyperplane in the affine space $\mathbb{A}^N$, and H is the subgroup Γ^N of $\mathbb{G}_{\mathrm{m}}^N(K)$ for a finitely generated subgroup Γ of $\mathbb{G}_{\mathrm{m}}(K)$ satisfying $H \subset \prod_{v\in\Omega} \mathbb{G}_{\mathrm{m}}^N(O_v)$, the condition $\prod_{v\in\Omega} X(K_v) \cap \overline{H} \neq \emptyset$ is sufficient to ensure that $X(K) \cap H \neq \emptyset$; we will explain this carefully in Section 3.2. While the main result in Chapter 2 shows that $\prod_{v\in\Omega} X(K_v) \cap \overline{H} = X(K) \cap H$ if H is finitely generated and X satisfies some hypothesis, the subvarieties (except the zero-dimensional one) associated to Skolem's conjecture does not satisfy this hypothesis. In this chapter, we adopt different arguments to establish the conclusion of the main result in Chapter 2 for those cases relevant to Skolem's conjecture. In Section 3.2, we reformulate Skolem's conjecture in terms of adelic intersections, and deduce some results about its function field analog our main result, which itself is proved in Section 3.3.

3.2 Main Result and its Consequence on a Conjecture of Skolem

As a motivation of the main result in this chapter, we introduce an old conjecture proposed in the number field case by Skolem in [Sko37]. Following [HV10], Skolem's conjecture may be rephrased as follows. Let $\beta_1, \ldots, \beta_M \in$

$\mathbb{G}_{\mathrm{m}}(K)$, and Γ be a finitely generated subgroup of $\mathbb{G}_{\mathrm{m}}(K)$. Let S be a finite set of places of K containing all Archimedean ones such that $\{\beta_1, \ldots, \beta_M\} \cup \Gamma \subset \mathbb{G}_{\mathrm{m}}(O_S)$. Consider the following two statements:

(L) For every nonzero ideal I of O_S, there exists $(x_1, \ldots, x_M) \in \Gamma^M$ such that $\sum_{i=1}^{M} \beta_i x_i \in I$.

(G) There exists $(x_1, \ldots, x_M) \in \Gamma^M$ such that $\sum_{i=1}^{M} \beta_i x_i = 0$.

We will see that shortly the first statement is equivalent to a certain local solvability. For this reason, we use the labels (L) and (G), where (L) stands for "local" and (G) stands for "global."

Note that (G) implies (L). In [Sko37], Skolem asserts that in the case where K were a number field, (L) and (G) would be equivalent; in that paper, he also shows that this assertion holds in the case where $M = 2$.

It is noticed in [HV10] that Skolem's conjecture is related to the intersection considered in Chapter 2. Below we describe the connection explicitly. Note that the fact that K is a global field is enough for this connection to hold.

Consider the finitely generated subgroup Γ^M of $\mathbb{G}_{\mathrm{m}}^M(K)$. Let V be the subvariety of $\mathbb{G}_{\mathrm{m}}^M = (\mathbb{A}^1 \setminus \{0\})^M$ cut by the hyperplane $\sum_{i=1}^{M} \beta_i x_i = 0$ in $\mathbb{A}^M$. Then V is a subvariety of $\mathbb{G}_{\mathrm{m}}^M$, and $V(K) \cap \Gamma^M$ consists of exactly those $(x_1, \ldots, x_M) \in \Gamma^M$ such that $\sum_{i=1}^{M} \beta_i x_i = 0$; in particular, (G) is equivalent to $V(K) \cap \Gamma^M \neq \emptyset$. On the other hand, every nonzero ideal I of O_S is a product of nonnegative powers of prime ideals of O_S; each prime ideal is equal

to $m_v \cap O_S$ for some $v \in \Omega_K \setminus S$. Taking $\Omega = \Omega_K \setminus S$, it is easy to see that (L) can be translated into the equivalent condition of $\prod_{v\in\Omega} V(K_v) \cap \overline{\Gamma^M} \neq \emptyset$, discussed in the second-to-last paragraph in Section 2.1 of Chapter 2. Under this reformulation, Skolem's conjecture asserts that $\prod_{v\in\Omega} V(K_v) \cap \overline{\Gamma^M} \neq \emptyset$ if and only if $V(K) \cap \Gamma^M \neq \emptyset$.

In view of the main result in Chapter 2, it is natural to try to establish $\prod_{v\in\Omega} V(K_v) \cap \overline{\Gamma^M} = V(K) \cap H$, which clearly implies Skolem's conjecture. The first observation is that in the case where K is a global function field, the main result in Chapter 2 cannot be applied in this case since V is isotrivial; it is isomorphic to the subvariety of $\mathbb{G}_{\mathrm{m}}^M = (\mathbb{A}^1 \setminus \{0\})^M$ cut by the hyperplane $\sum_{i=1}^M x_i = 0$ in $\mathbb{A}^M$, via the translation of the element $(\beta_1, \ldots, \beta_M)$ in $\mathbb{G}_{\mathrm{m}}^M(K)$. This breaks down the dimension-reducing step in the proof of the main result in Chapter 2. The work in this chapter is therefore motivated.

Before stating the main result in this chapter, let me connect Skolem's conjecture with another adelic intersection slightly different from above. As we will see, this formulation is more useful when we deduce consequences about the function field analog of Skolem's conjecture from our main result.

Fix an element β_i from $\{\beta_1, \ldots, \beta_M\}$. Since the roles of β_i's in (L) and (G) are symmetric, after a re-indexing we may assume that $i = M$, which

make the notation easier. Consider the following two statements:

(L') For every nonzero ideal I of O_S, there exists $(x_1, \ldots, x_{M-1}) \in \Gamma^{M-1}$ such that $\sum_{i=1}^{M-1}(-\beta_M^{-1}\beta_i)x_i - 1 \in I$.

(G') There exists $(x_1, \ldots, x_M) \in \Gamma^{M-1}$ such that $\sum_{i=1}^{M-1}(-\beta_M^{-1}\beta_i)x_i - 1 = 0$.

It is easy to see that (L) is equivalent to (L') while (G) is equivalent to (G'). We denote by V' the subvariety of $\mathbb{G}_{\mathrm{m}}^{M-1} = (\mathbb{A}^1 \setminus \{0\})^{M-1}$ cut by the hyperplane $\sum_{i=1}^{M-1}(-\beta_M^{-1}\beta_i)x_i - 1 = 0$ in $\mathbb{A}^{M-1}$, then the same analysis as to the last formulation shows that (L') is equivalent to $\prod_{v\in\Omega} V'(K_v) \cap \overline{\Gamma^{M-1}} \neq \emptyset$, and (G') is equivalent to $V'(K) \cap \Gamma^{M-1} \neq \emptyset$. Hence Skolem's conjecture asserts that $\prod_{v\in\Omega} V'(K_v) \cap \overline{\Gamma^{M-1}} \neq \emptyset$ if and only if $V'(K) \cap \Gamma^{M-1} \neq \emptyset$.

Motivated by these two reformulations of Skolem's conjecture, our main result in this chapter is the following

Theorem 2. *Let N be a natural number. Let H be a subgroup of $\mathbb{G}_m^N(K)$. Let W (resp. W') be the subvariety of $\mathbb{G}_m^N = (\mathbb{A}^1 \setminus \{0\})^N$ cut by the hyperplane $\sum_{i=1}^N b_i x_i = 0$ (resp. $\sum_{i=1}^M b_i x_i = 1$) in $\mathbb{A}^N$, where $(b_1, \ldots, b_N) \in \mathbb{G}_m^N(K)$. For each $h = (h_1, \ldots, h_N) \in H$, consider the following sequence of N elements in K:*

$$b_1 h_1, \ldots, b_N h_N. \tag{3.1}$$

Suppose that H is finitely generated.

1. *Suppose that there exists a natural number m such that for any $h \in H$, the sequence (3.1) is linearly independent over K^{p^m}. Then we have $\prod_{v\in\Omega} W(K_v) \cap \overline{H} = \emptyset$.*

2. *Suppose that there exists a natural number m such that for any $h \in H$, one of the following holds:*

   (a) *there is some $j \in \{1, \ldots, N\}$ such that the sequence (3.1) with $b_j h_j$ replaced by 1 is linearly independent over K^{p^m}.*

   (b) *The sequence (3.1) is linearly independent over K^{p^m} while there is some $j \in \{1, \ldots, N\}$ such that the sequence (3.1) with $b_j h_j$ replaced by 1 is linearly dependent over K^{p^m}.*

   (c) *The sequence (3.1) is linearly dependent over K^{p^m} while there is some $j \in \{1, \ldots, N\}$ such that the sequence (3.1) with $b_j h_j$ replaced by 1 is linearly independent over K^{p^m}.*

   Then we have $\prod_{v \in \Omega} W'(K_v) \cap \overline{H} = W'(K) \cap H$. Moreover, this common set is finite with its size at most the size of the image in H/H^{p^m} of those $h \in H$ satisfying the assumption (2a).

In this theorem, note that the assumptions on a particular $h \in H$ are really properties on the associated element in the finite set H/H^{p^m}. Those assumptions are exactly the ones which makes Proposition 8 works when W (resp. W') is replaced by its translation $h^{-1}W$ (resp. $h^{-1}W'$) by $h^{-1} \in \mathbb{G}_{\mathrm{m}}^N(K)$.

Example 4. Although the assumptions about linear dependence in Theorem 2 appear to be artificial, one cannot expect the conclusion of this theorem hold without imposing any hypothesis on W and W' as the following example shows. Let k be the finite field with q elements, and $K = k(t)$ be a purely

transcendental extension of k with transcendence degree 1. Take $\Gamma = \langle t, -t, 1-t\rangle$ be the subgroup of $\mathbb{G}_{\mathrm{m}}(K)$ generated by t, $-t$, and $1-t$. Let S be a finite set of places of K such that $\Gamma \subset \mathbb{G}_{\mathrm{m}}(O_S)$, and take $\Omega = \Omega_K \setminus S$. Consider the case where $N = 2$ and $b_1 = b_2 = 1$ in the statement of Theorem 2. It is clear that $\{(t^{q^m}, -t^{q^m}) : m \geq 0\} \subset W(K) \cap \Gamma^2$ and $\{(t^{q^m}, 1-t^{q^m}) : m \geq 0\} \subset W'(K) \cap \Gamma^2$. In Example 3 of Chapter 2, we see that, under the topology of $\prod_{v\in\Omega} \mathbb{G}_{\mathrm{m}}(K_v)$ the sequence $(t^{q^{n!}})_{n\geq 1}$ in Γ converges to an element $\alpha \in \prod_{v\in\Omega} \mathbb{G}_{\mathrm{m}}(K_v) \setminus \mathbb{G}_{\mathrm{m}}(K)$; hence the sequence $(-t^{q^{n!}})_{n\geq 1}$ in Γ converges to $-\alpha$, and the sequence $(1-t^{q^{n!}})_{n\geq 1}$ in Γ converges to $1-\alpha$. Therefore we conclude that $(\alpha, -\alpha) \in \prod_{v\in\Omega} W(K_v) \cap \overline{\Gamma^2} \setminus W(K)$ and similarly $(\alpha, 1-\alpha) \in \prod_{v\in\Omega} W'(K_v) \cap \overline{\Gamma^2} \setminus W'(K)$. We also see that the conclusion in Theorem 2, in the case where $H = \Gamma^N$ for some finitely generated subgroup Γ of $\mathbb{G}_{\mathrm{m}}(K)$, is strictly stronger than the function field analog of Skolem's conjecture.

Postponing the proof of Theorem 2 until Section 3.3, we conclude this section by giving some results on the function field analog of Skolem's conjecture as immediate corollaries. From the first reformulation, we have the following

Corollary 5. *Let $\beta_1, \ldots, \beta_M \in \mathbb{G}_m(K)$, and Γ be a finitely generated subgroup of $\mathbb{G}_m(K)$. Let S be a finite set of places of K such that $\{\beta_1, \ldots, \beta_M\} \cup \Gamma \subset \mathbb{G}_m(O_S)$. For each $(\gamma_1, \ldots, \gamma_M) \in \Gamma^M$, consider the following sequence of M elements in K:*

$$\beta_1\gamma_1, \ldots, \beta_M\gamma_M. \tag{3.2}$$

Suppose that there exists a natural number m such that for any $(\gamma_1, \ldots, \gamma_M) \in \Gamma^M$, the sequence (3.2) is linearly independent over K^{p^m}. Then (L) does not hold. In particular, the function field analog of Skolem's conjecture holds.

Taking into account the fact that the roles of β_i's in (L) and (G) are symmetric, we also obtain the following result on the function field analog of Skolem's conjecture from the second reformulation.

Corollary 6. *In the same notation as in Corollary 5, suppose that there exists a natural number m and $M_0 \in \{1, \ldots, M\}$ such that for any $(\gamma_i)_{i \in \{1,\ldots,M\} \setminus \{M_0\}} \in \Gamma^{M-1}$, one of the following holds:*

1. *there is some $j \in \{1, \ldots, M\} \setminus \{M_0\}$ such that the sequence (3.2) with $\beta_{M_0}\gamma_{M_0}$ replaced by β_{M_0} and $\beta_j\gamma_j$ deleted is linearly independent over K^{p^m}.*

2. *The sequence (3.2) with $\beta_{M_0}\gamma_{M_0}$ deleted is linearly independent over K^{p^m} while there is some $j \in \{1, \ldots, M\} \setminus \{M_0\}$ such that the sequence (3.2) with $\beta_{M_0}\gamma_{M_0}$ replaced by β_{M_0} and $\beta_j\gamma_j$ deleted is linearly dependent over K^{p^m}.*

3. *The sequence (3.2) with $\beta_n M_0 \gamma_{M_0}$ deleted is linearly dependent over K^{p^m} while there is some $j \in \{1, \ldots, M\} \setminus \{M_0\}$ such that the sequence (3.2) with $\beta_{M_0}\gamma_{M_0}$ replaced by β_{M_0} and $\beta_j\gamma_j$ deleted is linearly independent over K^{p^m}.*

Then the function field analog of Skolem's conjecture holds. Moreover, if there is no $(\gamma_i)_{i\in\{1,\dots,M\}\setminus\{M_0\}} \in \Gamma^{M-1}$ *satisfying (1), then (L) does not hold.*

An elements in $\mathbb{G}_{\mathrm{m}}(K)$ is always linearly independent over any subfield of K; two elements in $\mathbb{G}_{\mathrm{m}}(K)$ is linearly dependent over a subfield of K if and only if their quotient belongs to this subfield. These observations leads to the following much simpler form of Corollary 6 in case where $M \in \{2, 3\}$.

Corollary 7. *In the same notation as in Corollary 5, the function field analog of Skolem's conjecture holds in either of the following two situations:*

1. $M = 2$.
2. $M = 3$ *and there are two indices* $i_0 < j_0$ *such that every power of* $\beta_{i_0}^{-1}\beta_{j_0}$ *does not lie in* Γ.

Proof. For $M = 2$, the assumption (1) in Corollary 6 is always satisfied, hence the conclusion follows. For $M = 3$, if every power of $\beta_{i_0}^{-1}\beta_{j_0}$ does not lie in Γ for some $1 \leq i_0 < j_0 \leq 3$, then Lemma 3 in [Vol98] implies that $\beta_n {i_0}^{-1}\beta_{j_0} \notin \bigcap_{m\geq 1} \mathbb{G}_{\mathrm{m}}(K)^{p^m}\Gamma$. Therefore there exists a natural number m_0 such that for any $\gamma \in \Gamma$ the set $\{\beta_{j_0}, \beta_i\gamma\}$ is linearly independent over K^{p^m}. i.e. the assumption (1) in Corollary 6 always holds with $M_0 = j_0$. This completes the proof. □

Note that the unconditional result for the case $M = 2$ in Corollary 7 really comes from the conclusion about W' in the case where $N = 1$ in

Theorem 2, where assumption is satisfied trivially. In this simple case, W' is an irreducible zero-dimensional subvariety of $\mathbb{G}_{\mathrm{m}}$ and hence the equality $\prod_{v\in\Omega} W'(K_v)\cap\overline{H} = W'(K)\cap\overline{H}$ hold trivially. The only content in Theorem 2 in this case is therefore the statement $W'(K)\cap\overline{H} = W'(K)\cap H$, which is really a special case of Corollary 3 in Chapter 2. This special case of the corollary follows solely from Proposition 2 in Chapter 2. As remarked before Lemma 3, the number field analogue of Proposition 2 is just a reformulation of Theorem 1 in [Che51]. Hence the case $M = 2$ of the *original* Skolem's conjecture may be also proved in our framework.

3.3 Proof of the Main Result

In view of the statement of Theorem 2 we aim to prove in this section, we fix a natural number N and $b_1,\ldots,b_N\in\mathbb{G}_{\mathrm{m}}(K)$ as well as a subgroup H of $\mathbb{G}_{\mathrm{m}}^N(K)$ throughout this section. We denote by W (resp. W') the subvariety of $\mathbb{G}_{\mathrm{m}}^N = (\mathbb{A}^1\setminus\{0\})^N$ cut by the hyperplane $\sum_{i=1}^N b_i x_i = 0$ (resp. $\sum_{i=1}^M b_i x_i = 1$) in $\mathbb{A}^N$. As noted in Section 3.2, the dimension-reducing step of the proof of the main result in Chapter 2 is not applicable for Theorem 2; indeed, the crucial result in that step is Proposition 4. We give the following replacement of this proposition, and then prove Theorem 2 in the same vein as for the main result in Chapter 2.

Proposition 8. *Consider the following sequence of N elements in K:*

$$b_1,\ldots,b_N. \tag{3.3}$$

Let m be a natural number.

a) *Suppose that the sequence (3.3) is linearly independent over K^{p^m}. Then we have $W(K_v) \cap \mathbb{G}_m^N(K_v^{p^m}) = \emptyset$ for all $v \in \Omega$.*

b) *Suppose that there is some $j \in \{1, \ldots, N\}$ such that the sequence (3.3) with b_j replaced by 1 is linearly independent over K^{p^m}. Then there exists a singleton J, which is a subset of $W'(K)$, such that we have $W'(K_v) \cap \mathbb{G}_m^N(K_v^{p^m}) \subset J$ for all $v \in \Omega$.*

c) *Suppose that one of the following holds:*

- *There is some $j \in \{1, \ldots, N\}$ such that the sequence (3.3) with b_j replaced by 1 is linearly dependent over K^{p^m} while the sequence (3.3) is linearly independent over K^{p^m}.*
- *There is some $j \in \{1, \ldots, N\}$ such that the sequence (3.3) with b_j replaced by 1 is linearly independent over K^{p^m} while the sequence (3.3) is linearly dependent over K^{p^m}.*

Then we have $W'(K_v) \cap \mathbb{G}_m^N(K_v^{p^m}) = \emptyset$ for all $v \in \Omega$.

Proof. As shown in Chapter 2, there exists an iterative derivation $\{D^{(i)} : i \geq 0\}$ on K which extends to an iterative derivation $\{D_v^{(i)} : i \geq 0\}$ on K_v for each $v \in \Omega$ such that $K^{p^n} = \{x \in K : D^{(i)}(x) = 0 \text{ for } 1 \leq i < p^n\}$ and $K_v^{p^n} = \{x \in K : D_v^{(i)}(x) = 0 \text{ for } 1 \leq i < p^n\}$ for each natural number n and each $v \in \Omega$. Fix some $v \in \Omega$ and some $(c_1, \ldots, c_N) \in W(K_v) \cap \mathbb{G}_{\mathrm{m}}^N(K_v^{p^m})$, i.e. $c_j \in \mathbb{G}_{\mathrm{m}}(K_v^{p^m})$ for

$1 \leq j \leq N$ such that $\sum_{j=1}^{N} b_j c_j = 0$. By the defining property of the iterative derivation $\{D_v^{(i)}\}$ and the assumption $c_j \in K_v^{p^m}$, we have $\sum_{j=1}^{N} D^{(i)}(b_j) c_j^{(l)} = D_v^{(i)} \left(\sum_{j=1}^{N} b_j c_j^{(l)} \right) = 0$ for $0 \leq i < p^m$. Similarly, for any $v \in \Omega$ and any $(c_1, \ldots, c_N) \in W'(K_v) \cap \mathbb{G}_{\mathrm{m}}^N(K_v^{p^m})$, we have $\sum_{j=1}^{N} D^{(i)}(b_j) c_j^{(l)} = D^{(i)}(1)$ for $0 \leq i < p^m$.

For an increasing sequence $\{\epsilon_i\}_{1 \leq i \leq N}$ of integers such that $\epsilon_1 = 0$ and $\epsilon_N < p^m$, consider the following system of equalities:

$$\sum_{j=1}^{N} D^{(\epsilon_i)}(b_j) c_j = D^{(\epsilon_i)}(e), \quad 1 \leq i \leq N,$$

where $e \in \{0, 1\}$. in the other case where $e = 1$, it holds for any $(c_1, \ldots, c_N) \in W'(K_v) \cap \mathbb{G}_{\mathrm{m}}^N(K_v^{p^m})$. Denote by $\mathbf{B}$ the matrix with $D^{(\epsilon_i)}(b_j)$ being its entry at the i-th row and j-th column, by $\mathbf{c}$ the column vector with its j-th component being c_j, by $\mathbf{e}$ the column vector with its i-th component being $D^{(i)}(e)$. With these notation, we write the above system of equalities as $\mathbf{Bc} = \mathbf{e}$, which implies

$$(\det \mathbf{B})\mathbf{c} = \mathbf{B}^* \mathbf{e}, \tag{3.4}$$

where $\mathbf{B}^*$ denotes the adjoint matrix of $\mathbf{B}$.

First consider the case where $e = 0$. In this case, we see from the construction that (3.4) holds for any $(c_1, \ldots, c_N) \in W(K_v) \cap \mathbb{G}_{\mathrm{m}}^N(K_v^{p^m})$. Since the right hand side of (3.4) is the zero vector but each component of $\mathbf{c}$ cannot be zero, a contradiction occurs when $\det \mathbf{B} \neq 0$, which holds for some choice of $\{\epsilon_i\}_{1 \leq i \leq N}$ by Theorem 1 of [GV87], provided that the sequence (3.3) is linearly independent over K^{p^m}. The contradiction proves (a).

Now we consider the case where $e = 1$ and therefore (3.4) holds for any $(c_1, \ldots, c_N) \in W'(K_v) \cap \mathbb{G}_{\mathrm{m}}^N(K_v^{p^m})$. Note that for any $j \in \{1, \ldots, N\}$, the j-th component of $\mathbf{B}^*\mathbf{e}$ is just the determinant of the matrix obtained by replacing the j-th column of $\mathbf{B}$ with $\mathbf{e}$; in the same manner which $\mathbf{B}$ is constructed from the sequence (3.3), this matrix may be also constructed from the sequence (3.3) with b_j replaced by 1. By Theorem 1 of [GV87], since every component of $\mathbf{c}$ is nonzero, the assumption in (c) ensure the existence of a choice of $\{\epsilon_i\}_{1 \le i \le N}$ for which exactly one of the two sides of (3.4) is equal to zero; this contradiction proves (c). On the other hand, the assumption in (b) implies there is a choice of $\{\epsilon_i\}_{1 \le i \le N}$ for which the right hand side of (3.4) is not zero. If the left hand side is zero, we conclude $W'(K_v) \cap \mathbb{G}_{\mathrm{m}}^N(K_v^{p^m}) = \emptyset$ and just take J to be any subset $W'(K)$ with exactly one element; otherwise we conclude $\mathbf{c} = \mathbf{B}^{-1}\mathbf{e}$ and take J to be singleton consisting of the point $(c_1, \ldots, c_N)$, which is in fact in $W'(K)$ since entries of $\mathbf{B}$ and components of $\mathbf{e}$ are all in K. This completes the proof. □

Note that Proposition 8 leads to a stronger result than that of the dimension-reducing step of the proof of the main result in Chapter 2. It descends local points from W or W' to *global points* (rather than just local ones) of zero-dimensional subvarieties of $\mathbb{G}_{\mathrm{m}}^N$. Having this, we only need Corollary 3 in Chapter 2 to finish the proof of Theorem 2.

Proof of Theorem 2. Since H is finitely generated, Lemma 13 in Chapter 2 implies that there are finitely many η_i's in H such that $\overline{H} = \bigcup_i \left(\eta_i \overline{H^{p^m}}\right)$.

Since $\overline{H^{p^m}} \subset \prod_{v\in\Omega} \mathbb{G}_{\mathrm{m}}^N(K_v^{p^m})$, we obtain $\overline{H} \subset \prod_{v\in\Omega} \bigcup_i \left(\eta_i \mathbb{G}_{\mathrm{m}}^N(K_v^{p^m})\right)$. Note that for each $v \in \Omega$ we have

$$\begin{array}{rl} & W(K_v) \cap \bigcup_i \left(\eta_i \mathbb{G}_{\mathrm{m}}^N(K_v^{p^m})\right) \\ = & \bigcup_i \left(W(K_v) \cap \eta_i \mathbb{G}_{\mathrm{m}}^N(K_v^{p^m})\right) \\ = & \bigcup_i \eta_i \left((\eta_i^{-1}W)(K_v) \cap \mathbb{G}_{\mathrm{m}}^N(K_v^{p^m})\right); \end{array}$$

these equalities also hold with W replaced by W'. For any $g = (g_1, \ldots, g_N) \in \mathbb{G}_{\mathrm{m}}^N(K)$, the variety gW (resp. gW') is just subvariety of $\mathbb{G}_{\mathrm{m}}^N = (\mathbb{A}^1 \subset \{0\})^N$ cut by the hyperplane $\sum_{j=1}^N b_j g_j^{-1} x_j = 0$ (resp. $\sum_{j=1}^N b_j g_j^{-1} x_j = 1$) in $\mathbb{A}^N$. Since $\eta_i \in H$, the assumption of (1) and part (a) of Proposition 8 implies $(\eta_i^{-1}W)(K_v) \cap \mathbb{G}_{\mathrm{m}}^N(K_v^{p^m}) = \emptyset$ for each i; therefore we have $\prod_{v\in\Omega} W(K_v) \cap \overline{H} \subset \prod_{v\in\Omega} W(K_v) \cap \bigcup_i \left(\eta_i \mathbb{G}_{\mathrm{m}}^N(K_v^{p^m})\right) = \bigcup_i \eta_i \left((\eta_i^{-1}W)(K_v) \cap \mathbb{G}_{\mathrm{m}}^N(K_v^{p^m})\right) = \emptyset$. Similarly, the assumption of (2) and part (b) and (c) of Proposition 8 implies that for each i, we have either $(\eta_i^{-1}W')(K_v) \cap \mathbb{G}_{\mathrm{m}}^N(K_v^{p^m}) = \emptyset$ or a singleton J_i, which is a subset of $(\eta_i^{-1}W')(K)$, such that $(\eta_i^{-1}W')(K_v) \cap \mathbb{G}_{\mathrm{m}}^N(K_v^{p^m}) \subset J_i$; since $\eta_i \in \mathbb{G}_{\mathrm{m}}^N(K)$ and J_i is a subset of $(\eta_i^{-1}W')(K)$ for each i, we take $J = \bigcup_i \eta_i J_i$ and see that it is a subset of $W'(K)$ satisfying $\prod_{v\in\Omega} W'(K_v) \cap \overline{H} \subset \prod_{v\in\Omega} \bigcup_i \eta_i \left((\eta_i^{-1}W')(K_v) \cap \mathbb{G}_{\mathrm{m}}^N(K_v^{p^m})\right) \subset \prod_{v\in\Omega} \bigcup_i \eta_i J_i = J$. Therefore $\prod_{v\in\Omega} W'(K_v) \cap \overline{H} \subset \left(\prod_{v\in\Omega} W'(K_v) \cap \mathbb{G}_{\mathrm{m}}^N(K)\right) \cap J \cap \overline{H} \subset J \cap \overline{H}$. By Corollary 3 in Chapter 2, we have $J \cap \overline{H} = J \cap H$ and conclude that $\prod_{v\in\Omega} W'(K_v) \cap \overline{H} \subset J \cap H \subset W'(K) \cap H \subset \prod_{v\in\Omega} W'(K_v) \cap \overline{H}$, which must be therefore a chain of equalities. In the construction of J, note that each occurrence of a term $\eta_i \mathfrak{J}_i$, which is a singleton, corresponds to an element $\eta_i \in H$ of a complete set of coset representatives of H^{p^m} in H; therefore J has exactly its size equal to that of the image in H/H^{p^m} of those $(h_1, \ldots, h_N) \in H$ satisfying the assumption

(2a), and the last part of the conclusion follows. □

Bibliography

[AV92] Dan Abramovich and José Felipe Voloch. Toward a proof of the Mordell-Lang conjecture in characteristic p. *Internat. Math. Res. Notices*, (5):103–115, 1992.

[Che51] Claude Chevalley. Deux théorèmes d'arithmétique. *J. Math. Soc. Japan*, 3:36–44, 1951.

[Fal83] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[GV87] Arnaldo García and J. F. Voloch. Wronskians and linear independence in fields of prime characteristic. *Manuscripta Math.*, 59(4):457–469, 1987.

[HR79] Edwin Hewitt and Kenneth A. Ross. *Abstract harmonic analysis*, volume 1. Springer-Verlag, New York, 1979.

[HV10] David Harari and José Felipe Voloch. The Brauer-Manin obstruction for integral points on curves. *Math. Proc. Cambridge Philos. Soc.*, 149(3):413–421, 2010.

[Mil72] James Stuart Milne. Congruence subgroups of abelian varieties. *Bull. Sci. Math. (2)*, 96:333–338, 1972.

[Ogu78] Arthur Ogus. F-crystals and Griffiths transversality. In *Proceedings of the International Symposium on Algebraic Geometry (Kyoto Univ., Kyoto, 1977)*, pages 15–44, Tokyo, 1978. Kinokuniya Book Store.

[PV10] Bjorn Poonen and José Felipe Voloch. The Brauer-Manin obstruction for subvarieties of abelian varieties over function fields. *Ann. of Math. (2)*, 171(1):511–532, 2010.

[Ray83] M. Raynaud. Courbes sur une variété abélienne et points de torsion. *Invent. Math.*, 71(1):207–233, 1983.

[Sch39] Friedrich Karl Schmidt. Die Wronskische Determinante in beliebigen differenzierbaren Funktionenkörpern. *Math. Z.*, 45(1):62–74, 1939.

[Sch99] Victor Scharaschkin. *Local-global problems and the Brauer-Manin obstruction*. ProQuest LLC, Ann Arbor, MI, 1999. Thesis (Ph.D.)–University of Michigan.

[Ser71] Jean-Pierre Serre. Sur les groupes de congruence des variétés abéliennes. II. *Izv. Akad. Nauk SSSR Ser. Mat.*, 35:731–737, 1971.

[Ser88] Jean-Pierre Serre. *Algebraic groups and class fields*, volume 117 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1988. Translated from the French.

[Sko37] Thoralf Skolem. Anwendung exponentieller kongruenzen zum beweis der unlösbarkeit gewisser diophantischer gleichungen. *Avhdl. Norske Vid. Akad. Oslo I*, 12:1–16, 1937.

[Vol98] José Felipe Voloch. The equation $ax + by = 1$ in characteristic p. *J. Number Theory*, 73(2):195–200, 1998.