POSITIVE CHARACTERISTIC MANIN-MUMFORD THEOREM

THOMAS SCANLON

Abstract. We present the details of a model theoretic proof of an analogue of the Manin-Mumford conjecture for semiabelian varieties in positive characteristic. As a by-product of the proof we reduce the general positive characteristic Mordell-Lang problem to a question about purely inseparable points on subvarieties of semiabelian varieties.

1. Introduction

The Manin-Mumford conjecture in its original form (whose proof is originally due to Raynaud [11]) asserts that if A is an abelian variety over a number field k and $X \subseteq A$ is an irreducible subvariety of A, then $X(k^{\mathrm{alg}})$ meets the torsion subgroup of $A(k^{\mathrm{alg}})$ in a finite union of cosets of sugroups of the torsion group. If one replaces k with a field of positive characteristic, then there are obvious counterexamples to the direct translation of this conjecture. However, by isolating groups defined over finite fields appropriately one can state and prove a positive characteristic version of this conjecture.

We should say a word or two about attributions for this theorem. The current author sketched the proof presented here in [12]. As the reader will see, given the dichotomy theorem for existentially closed difference fields [3] this proof follows Hrushovski's proof of the number field Manin-Mumford conjecture [6]. In fact, the difference equations are easier to find in the positive characteristic case and these equations are essentially the same as those used by the other authors mentioned below. The main obstruction to the positive characteristic Manin-Mumford theorem following immediately from the number field proof is the presence of infinitely many definable subfields of difference closed fields in positive characteristic.

Pink and Roessler gave an algebraic proof this theorem in [10]. While their proof avoids appeals to the model theory of difference fields, it too uses some sophisticated arguments (involving, for instance, the theory of Dieudonné modules). Pillay presented a very elementary proof of the function field Mordell-Lang conjecture using an analysis of algebraic D-groups [7] and then transposed this argument to the context of algebraic σ-groups to reprove the Manin-Mumford conjecture over number fields [8]. The student working group supervised by Pillay and Scanlon at the 2003 Arizona Winter School completed a very elementary proof of the main theorem of this note along the lines of Pillay's characteristic zero proof. Some details of this argument are available in a streaming video on the Southwestern Center's webpage and in a recent preprint of Pillay [9].

I thank Z. Chatzidakis for sharing her then unpublished work on the dichotomy theorem for ACFA_p in 1998. Any reader who compares this version to the paper

Date: 8 May 2003.

Partially supported by NSF Grant DMS-0303618 and an Alfred P. Sloan Fellowship.

posted on the arXiv preprint server will note that there were numerous inaccurasies in that note. I thank F. Oort for pointing out some of these, but, of course, any remaining mistakes are entirely my own.

2. Statement of the main theorem

In this section we state the main theorem of this note. Before doing so we recall a definition from [5].

By way of notation, if X is a scheme over the ring R and S is an R-algebra, then we write X_S for the base change $X \times_{\mathrm{Spec}(R)} \mathrm{Spec}(S)$. Also, if A is an abelian group, then by A_{tor} we mean the torsion subgroup: $\{x \in A \mid (\exists n \in \mathbb{Z}_+)\ nx = 0\}$.

Definition 2.1. Let K be an algebraically closed field of characteristic p. Let G be a commutative algebraic group over K and $X \subseteq G$ an irreducible subvariety. We say that X is *special* if there are

- H_0 an algebraic group defined over $\mathbb{F}_p^{\mathrm{alg}}$,
- a point $a \in G(K)$,
- a subvariety $X_0 \subseteq G_0$ defined over $\mathbb{F}_p^{\mathrm{alg}}$, and
- a morphism of algebraic groups $h : (H_0)_K \to G$

such that $X = a + h(X_0)_K$.

With the definition of *special* in place we can state the positive characteristic version of the Manin-Mumford conjecture.

Theorem 2.2. *Let K be an algebraically closed field of characteristic p. Let G be a semiabelian variety over K and $X \subseteq G$ a closed subvariety. Then the Zariski closure of $X(K) \cap G(K)_{\mathrm{tor}}$ is a finite union of special subvarieties.*

3. The proof

In this section we prove Theorem 2.2. The proof is broken into two separate parts. First, we analyze integral models of semiabelian varieties to show that with an appropriate choice of automorphism, we can force the torsion points to satisfy a nontrivial difference equation. Secondly, we analyze the structure of finite rank difference algebraic subgroups of semiabelian varieties. Combining these two parts, we prove Theorem 2.2. As mentioned in the introduction, finding the relevant difference equations is entirely standard. Most of the heavy lifting in the analysis of difference algebraic groups was carried out in [1, 2, 3, 6]. Our main innovation is the use of orthogonality between incomparable fixed fields to convert nonmodularity into strong essential algebraicity. What we mean by this comment should be clear by the end of this section.

3.1. Difference equations for the torsion.

In this subsection, we show that for a given semiabelian variety G over an algebraically closed field K of characteristic p, it is possible to find an automorphism σ of K and a polynomial $P(X) \in \mathbb{Z}[X]$ so that $G = G^\sigma$; $P(\sigma)$, considered as an endomorphism of the group $G(K)$, vanishes on $G(K)_{\mathrm{tor}}$; and no root of P in $\mathbb{C}$ is a root of unity. Such automorphisms and polynomials play an essential rôle in our proof of Theorem 2.2. As the reader undoubtedly already surmises, σ will arise from a suitable lifting of some Frobenius automorphism and P will be the minimal polynomial over $\mathbb{Z}$ of that Frobenius considered as an element of the endomorphism ring of some algebraic group over a finite field.

We start with an algebraic lemma. Of course, this lemma, with the ring of formal power series over a finite field replaced by a general complete complete DVR with a finite residue field, holds for general finitely generated domains, but as we need only the positive characteristic version, we restrict to that case.

Lemma 3.1. *Let R be a finitely generated domain of characteristic $p > 0$. Then for some power q of p, there is an embedding $R \hookrightarrow \mathbb{F}_q[[\epsilon]]$.*

Proof. Write $R = \mathbb{F}_p[a_1, \ldots, a_n]$ for appropriate generators $a_1, \ldots, a_n$. Rearranging the generatots if need be, we may assume that $a_1, \ldots, a_m$ are algebraically independent and that R is algebraic over $R' := \mathbb{F}_p[a_1, \ldots, a_m]$. For each $i > m$ let $P_i(X) \in R'[X]$ be a minimal polynomial for a_i over R' (ie $P_i \not\equiv 0$, $P_i(a_i) = 0$, and P_i has minimal possible degree d_i). Let $Q_i(X_1, \ldots, X_m) \in \mathbb{F}_p[X_1, \ldots, X_n]$ be the polynomial for which $Q_i(a_1, \ldots, a_m)$ is the coefficient of X^{d_i} in $P_i(X)$. Let q be a high enough power of p so that the set $\mathbb{A}^m(\mathbb{F}_q) \smallsetminus \bigcup_{i=m+1}^n V(Q_i)(\mathbb{F}_q)$ is nonempty. Let $\langle b_1, \ldots, b_m \rangle$ be one such point. Then for any $i \leq n$ and any $\langle c_1, \ldots, c_m \rangle \in \mathbb{F}_q[[\epsilon]]$ we have $Q_i(b + \epsilon c) \in \mathbb{F}_q[[\epsilon]]^\times$. Choose $c = \langle c_1, \ldots, c_m \rangle$ algebraically independent (such exists as the transencendence degree of $\mathbb{F}_q((\epsilon))$ is $2^{\aleph_0}$) and define an embedding $R'' := \mathbb{F}_p[a_1, \ldots, a_m, Q_{m+1}(a)^{-1}, \ldots, Q_n(a)^{-1}] \hookrightarrow \mathbb{F}_q[[\epsilon]]$ via $a_i \mapsto b_i + \epsilon c_i$. 4 Now R is contained in finite integral extension of R'' and thus via the above embedding of $\mathbb{F}_q[[\epsilon]]$. Every such extension is contained in the ring of integers of some finite extension of $\mathbb{F}_q((\epsilon))$, each of which is isomorphic to $\mathbb{F}_{q^r}[[\eta]]$ for some positive integer r. □

Using Lemma 3.1 we show that every semiabelian variety over a field of characteristic $p > 0$ may be regarded as a base change of the generic fibre of some semiabelian scheme over a DVR whose special fibre has the same p-rank.

Lemma 3.2. *Let K be a field of characteristic p and G a semiabelian variety over K. Then there are a discrete valuation ring $R \subseteq K$ with a finite residue field $\mathbb{F}_q$ and a semiabelian scheme $\mathfrak{G}$ over R for which the p-rank of the special fibre of $\mathfrak{G}$ is equal to the p-rank of the generic fibre and $G \cong \mathfrak{G}_K$.*

Proof. Choose any finitely generated subring S over which we have a semiabelian scheme $\mathfrak{G}'$ with $(\mathfrak{G}')_K \cong G$. Let $S' := S(G[p](K^{\mathrm{alg}}))$. Let r be the p-rank of G $(= \dim_{\mathbb{F}_p} G[p](K^{\mathrm{alg}}))$. Let $\gamma_1, \ldots, \gamma_r \in G[p](K^{\mathrm{alg}}) = \mathfrak{G}[p](S')$ be a basis for the (physical) p-torsion on G. The set U of primes $\mathfrak{p} \in \mathrm{Spec}(S')$ such that the image of $\gamma_1, \ldots, \gamma_r$ remain linearly independent in $(\mathfrak{G} \otimes S'/\mathfrak{p})[p](S'/\mathfrak{p})$ is open in the Zariski topology. Let S'' be the coordinate ring of this set. By Lemma 3.1 we can embed S'' into a complete DVR T with a finite residue field. Let $R \subseteq K$ be the ring of integers of a maximal immediate (with respect to the valuation inherited from T) extension of S'' in K. □

With this next lemma we limit the rings in which we must search for torsion points.

Lemma 3.3. *Let R be a discrete valuation ring of characteristic p with residue field $\mathbb{F}_q$ and field of quotients K. Let S be the maximal unramified algebraic extension of R and let $S' := S^{p^{-\infty}} := \{y \in K^{\mathrm{alg}} \mid (\exists n \in \mathbb{N}) y^{p^n} \in S\}$ be the perfection of S. Then for any semiabelian scheme G over R, the natural map $G(S')_{\mathrm{tor}} \to G(K^{\mathrm{alg}})_{\mathrm{tor}}$ is an isomorphism.*

Proof. Of course, this map is an injection. So, we must show that it is a surjection. For any finite étale group scheme F over R, Hensel's lemma shows that $F(S) \hookrightarrow F(K^{\mathrm{alg}})$ is an isomorphism. For each $n \in \mathbb{Z}_+$, Consider the connected-étale sequence over S':

$$0 \longrightarrow G[n]^0 \longrightarrow G[n] \longrightarrow G[n]_{\acute{e}t} \longrightarrow 0$$

Over a perfect ring, this sequence splits and the group of rational points in a connected finite flat group scheme over a domain is trivial. Thus, $G[n](S') \cong G[n]_{\acute{e}t}(S') \cong G[n]_{\acute{e}t}(K^{\mathrm{alg}}) \cong G[n](K^{\mathrm{alg}})$.

As the torsion group is the direct limit of the n-torsion groups, we conclude $G(S')_{\mathrm{tor}} \cong G(K^{\mathrm{alg}})_{\mathrm{tor}}$. □

It follows now that we can capture the torsion group of semiabelian varieties having good models over DVRs by difference equations.

Lemma 3.4. *Let R be a discrete valuation ring of characteristic p with residue field $\mathbb{F}_q$ and field of quotients K. Let G be a semiabelian scheme over R for which the p-rank of the generic fibre is equal to the p-rank of the special fibre. There is a polynomial $P(X) \in \mathbb{Z}[X]$ and an automorphism σ of K^{alg} fixing K such that $P(\sigma)$ vanishes on $G(K^{\mathrm{alg}})_{\mathrm{tor}}$ and no root of P in $\mathbb{C}$ is a root of unity.*

Proof. On the special fibre $\overline{G}$ of G the q-power Frobenius induces an endomorphism $F : \overline{G} \to \overline{G}$. As such, the subring of $\mathrm{End}(\overline{G})$ generated by F is a finite product of finite integral extensions of $\mathbb{Z}$. Let $P(X) \in \mathbb{Z}[X]$ be the minimal monic polynomial of F over $\mathbb{Z}$. By the Weil conjectures for $\overline{G}$, no complex root of P is a root of unity.

The completion of R is isomorphic to $\mathbb{F}_q[[\epsilon]]$. Let $\rho : \mathbb{F}_q^{\mathrm{alg}}[[\epsilon]] \to \mathbb{F}_q^{\mathrm{alg}}[[\epsilon]]$ be defined by

$$\sum_{i \geq 0} x_i \epsilon^i \to \sum_{i \geq 0} x_i^q \epsilon^i$$

Extend ρ to $\widetilde{\rho} : \mathbb{F}_q^{\mathrm{alg}}((\epsilon))^{\mathrm{alg}} \to \mathbb{F}_q^{\mathrm{alg}}((\epsilon))^{\mathrm{alg}}$ and let $\sigma := \widetilde{\rho} \restriction_{K^{\mathrm{alg}}}$ be the restriction of $\widetilde{\rho}$ to K^{alg}. Noting that ρ restricts to the identity on R, we see that σ is an automorphism of K^{alg}.

This choice of P and σ works. By Lemma 3.3 every torsion point in $G(K^{\mathrm{alg}})$ lives in $G(S')$ where S' is the perfection of the maximal algebraic unramified extension of R. Our hypothesis on the p-rank implies that for each $n \in \mathbb{Z}_+$ the reduction map induces an isomorphism $G[n](S') \cong \overline{G}[n](\mathbb{F}_q^{\mathrm{alg}})$. Moreover, as we have chosen σ to lift F, if we regard $G(S')$ as a $\mathbb{Z}[X]$-module with the generator X acting as σ and $\overline{G}(\mathbb{F}_q^{\mathrm{alg}})$ as a $\mathbb{Z}[X]$-module with the generator acting as F, then isomorphism $G(S')_{\mathrm{tor}} \to \overline{G}(\mathbb{F}_q^{\mathrm{alg}})$ is an isomorphism of $\mathbb{Z}[X]$-modules. P is defined so that $P(F) \equiv 0$ on $\overline{G}(\mathbb{F}_q^{\mathrm{alg}})$. Thus, $P(\sigma)$ vanishes on $G(S')_{\mathrm{tor}} = G(K^{\mathrm{alg}})_{\mathrm{tor}}$. □

Putting together all the results of this subsection, we find the polynomial and automorphism mentioned in the introduction.

Corollary 3.5. *Let $K = K^{\mathrm{alg}}$ be an algebraically closed field of characteristic $p > 0$ and G a semiabelian variety over K. There is a polynomial $P(X) \in \mathbb{Z}[X]$ having no roots of unity amongst its complex roots and an automorphism $\sigma : K \to K$ such that G is defined over the fixed field of σ and $P(\sigma)$ vanishes on $G(K)_{\mathrm{tor}}$.*

Proof. By Lemma 3.2 we may find a model of G over a DVR with a finite residue field so that p-rank of the generic and special fibres agree. Applying Lemma 3.4 to this model we obtain the requisite polynomial P and automorphism σ. $\square$

3.2. **Finite rank σ-algebraic groups.** In this subsection, we analyze the structure of subgroups of semiabelian varieties defined by difference equations.

Definition 3.6. Let $K = K^{\mathrm{alg}}$ be an algebraically closed field and $k \leq K$ the algebraic closure of the prime field in K. We say that the semiabelian variety G defined over K is *weakly isotrivial* if there is a semiabelian variety G_0 defined over k and a purely inseparable isogeny $\psi : G \to (G_0)_K$ defined over K. (Equivalently, there is a purely inseparable isogeny $\vartheta : (G_0)_K \to G$ defined over K.)

It is worth remarking that if G is isogenous to a semiabelian variety defined over a finite field, then, in fact, G is weakly isotrivial. Indeed, (in the notation of the definition) if $\psi : (G_0)_K \to G$ is an isogeny where G_0 is defined over k, then because every torsion point of G_0 is defined over k, we have that $(G_0)_K[\psi](K) \leq G_0(k)$. So, the quotient H of G_0 by the contant group scheme $(G_0)_K[\psi]_{\mathrm{red}}$ is defined over k and the induced isogeny $\vartheta : H_K \to G$ is bijective on K-points.

The following lemma is essentially tautological if one knows that a minimal algebraically closed field of moduli exists for the isogeny class of the algebraic group A (described in the statement). Our proof uses basic stability theory. Certainly, a direct algebraic proof is possible, but we feel that as issues of canonical parameters and representability are directly implicated by the statement, they should naturally appear in the proof.

Lemma 3.7. *Let M be an algebraically closed field and $K_1, K_2 \leq M$ algebraically closed subfields which are algebraically independent over their intersection $K_1 \cap K_2$. Suppose that A is an algebraic group defined over K_1 and that there are an algebraic group B defined over K_2 and a surjective map of algebraic groups $g : A_M \to B_M$ with $(\ker g)_{\mathrm{red}}$ defined over K_1. Then there is an algebraic group B_0 defined over $K_1 \cap K_2$ and a surjective morphism $h : A \to (B_0)_{K_1}$ defined over K_1 with $((\ker g)_{\mathrm{red}}) = ((\ker h)_{\mathrm{red}})_M$.*

Proof. Choosing a presentation of A over K_1, B over K_2, and g over M, we may express the assertion "g is a surjective map of algebraic groups from A to B" as a sentence in the language of fields with parameters from M. As the theory of algebraically closed fields is model complete, we may assume that all of the necessary parameters come from the algebraic closure of the compositum of K_1 and K_2. Separating the parameters and using quantifiers to speak about algebraic extensions, we may write this sentence as $\varphi(a; b)$ where a is a tuple from K_1, b is a tuple from K_2, and $\varphi(x; y)$ is a formula of the language of rings having no extra parameters. The formula $\varphi(x; y)$ asserts "A_x is an algebraic group, B_y is an algebraic group, $C_x \leq A_x$ is an algebraic subgroup of A_x, there are parameters z satisfying a particular algebraic relation over x and y such that $g_z : A_x \to B_y$ is surjective and (on points) $\ker g_z = C_x$."

The formula $\varphi(x; y)$ is represented in $\mathrm{tp}(a/K_2)$, but K_1 and K_2 are free over $K_1 \cap K_2$. Thus, $\varphi(x; y)$ is represented in $\mathrm{tp}(a/K_1 \cap K_2)$. That is, we can find a tuple c from $K_1 \cap K_2$ for which $\varphi(a; c)$ holds. This gives the result. $\square$

Until further notice is given $(\mathbb{U}, +, \times, \sigma, 0, 1)$ denotes a fixed existentially closed difference field of characteristic $p > 0$. We denote by τ the p-power Frobenius automorphism of $\mathbb{U}$. All fields considered will be regarded as subfields of $\mathbb{U}$. In the final application to the Manin-Mumford problem, we shall require a special choice of σ.

We now apply Lemma 3.7 to the special of algebraic closures of incomparable fixed fields in existentially closed difference fields.

Lemma 3.8. *Let A be a semiabelian variety defined over* $\mathrm{Fix}(\sigma)$. *Suppose that there there are nonzero integers m and n such that A is isogenous to a semiabelian variety defined over* $\mathrm{Fix}(\sigma^n\tau^m)$, *then A is isogenous to a semiabelian variety defined over a finite field.*

Proof. The fields $\mathrm{Fix}(\sigma)$ and $\mathrm{Fix}(\sigma^n\tau^m)$ are orthogonal, and in particular, algebraically independent. We have $\mathrm{Fix}(\sigma)^{\mathrm{alg}} = \bigcup_{N\geq 0}\mathrm{Fix}(\sigma^N)$ and $\mathrm{Fix}(\sigma^n\tau^m)^{\mathrm{alg}} = \bigcup_{M\geq 0}\mathrm{Fix}(\sigma^{nM}\tau^{mM})$ so that $\mathrm{Fix}(\sigma)^{\mathrm{alg}}\cap\mathrm{Fix}(\sigma^n\tau^m)^{\mathrm{alg}} = \mathbb{F}_p^{\mathrm{alg}}$. Thus, using the fact that every algebraic subgroup of A is defined over $\mathrm{Fix}(\sigma)^{\mathrm{alg}}$ by Lemma 3.7 we see that A is isogenous to a semiabelian variety defined over $\mathbb{F}_p^{\mathrm{alg}}$. □

We recall also the definition of (quantifier-free) modularity in existentially closed difference fields.

Definition 3.9. Let G be an algebraic group over $\mathbb{U}$. A subgroup $\Gamma \leq G(\mathbb{U})$ is said to be *modular* if for every pair of natural numbers $\langle n, m\rangle$ and every algebraic subvariety $X \subseteq G^n \times (G^\sigma)^n \times \cdots \times (G^{\sigma^m})^n$ the set

$$\{\langle\gamma_1,\ldots,\gamma_n\rangle \in \Gamma^n \mid \langle\gamma_1,\ldots,\gamma_n;\sigma(\gamma_1),\ldots,\sigma(\gamma_n);\ldots;\sigma^m(\gamma_1),\ldots,\sigma^m(\gamma_n)\rangle \in X(\mathbb{U})\}$$

is a finite union of cosets of subgroups of Γ^n.

Remark 3.10. While it is not immediately clear from the definition, if Γ is a *definable* extension of a modular group by a modular group, then it is modular itself (see Proposition 3.4.1 of [6]).

If $k \leq \mathbb{U}$ is a subfield and G is an algebraic group over k having infinitely many k-points, then the group $G(k)$ is not modular. Within the class of groups definable in existentially closed difference fields only these groups obstruct modularity.

Definition 3.11. Let G be a commutative algebraic group defined over $\mathbb{U}$ and $\Gamma \leq G(\mathbb{U})$ a definable subgroup. We say that Γ is *essentially algebraic* if there is group H of the form $\sum_{i=1}^m \psi_i(H_i(\mathrm{Fix}(\sigma^{n_i}\tau^{m_i}))$ where $n_i > 0$, $m_i \in \mathbb{Z}$, H_i is an algebraic group over $\mathrm{Fix}(\sigma^{n_i}\tau^{m_i})$, and $\psi_i : (H_i)_{\mathbb{U}} \to G$ is a map of algebraic groups with finite kernel such that $\Gamma/(H\cap\Gamma)$ is finite.

We say that Γ is *strongly essentially algebraic* if each H_i may be taken to be defined over a finite field.

Proposition 3.6.2 of [6] was included in that paper merely to round out the theory of groups of finite S1-rank. It played no part in the proof of the number field version of the Manin-Mumford conjecture, but it plays an important rôle here. We recall the specific form that we use.

Lemma 3.12. *Let G be a semiabelian variety over $\mathbb{U}$ and $\Gamma \leq G(\mathbb{U})$ a definable subgroup of finite order. Let $\Xi \leq \Gamma$ be an essentially algebraic subgroup. We presume that if $\Psi \leq \Gamma$ is an essentially algebraic subgroup of Γ, then $\Psi\cap\Xi$ is of finite index in Ψ. Then if $X \subseteq G$ is an irreducible subvariety with a trivial stabilizer and $X(\mathbb{U})\cap\Gamma$ Zariski dense in X, X must be contained in a single translate of the Zariski closure of Ξ.*

Proof. Let $M \leq \Gamma$ be a modular subgroup of maximal possible order. Set $\Phi := M + \Xi$. There are only countably many definable subgroups of Φ and the main dichotomy theorem of [3] shows that if $\Upsilon \leq \Gamma$ is contained in the model theoretic algebraic closure of a rank one set, $\Phi \cap \Upsilon$ has finite index in Υ. So, Proposition 3.6.2 of [6] shows that $X(\mathbb{U}) \cap \Gamma$ is contained in finitely many translates of Φ.

Let $s : G \times G \to G$ be the summation map $\langle x, y\rangle \mapsto x + y$. Let $\widetilde{X} := s^{-1}X \subseteq G \times G$. Then $X(\mathbb{U}) \cap \Phi = s(\widetilde{X}(\mathbb{U}) \cap (M \times \Xi))$. As $M \perp \Xi$, the set $\widetilde{X}(\mathbb{U}) \cap (M \times \Xi)$ is a finite union of sets of the form $a + (\Delta \times Y)$ where $Y \subseteq \Xi$ and $\Delta \leq M$. As X is irreducible, is equal to the Zariski closure of $X(\mathbb{U}) \cap \Gamma$, and has a trivial stabilizer; we see that there is only one such set in the union and Δ is trivial. □

For our ultimate application of Lemma 3.12 we need a complete description of the essentially algebraic groups which intervene. With the following lemma we see that they are all strongly essentially algebraic.

Lemma 3.13. *Let G be a semiabelian variety defined over $\mathrm{Fix}(\sigma)$. We presume that every connected algebraic subgroup of $G_{\mathbb{U}}$ and every endomorphism of $G_{\mathbb{U}}$ is already defined over $\mathrm{Fix}(\sigma)$. Let $P(X) \in \mathbb{Z}[X]$ be a polynomial with integer coefficients having no roots of unity amongst its complex roots. If $E \leq \ker P(\sigma) < G(\mathbb{U})$ is an essentially algebraic subgroup of the kernel of $P(\sigma)$ on $G(\mathbb{U})$, then E is strongly essentially algebraic.*

Proof. It suffices to consider the case that E is a subgroup of a group of the form $\psi(H(k))$ where $k = \mathrm{Fix}(\sigma^n \tau^m)$ for a pair of integers with $n \neq 0$, H is an algebraic group over k, and $\psi : H_{\mathbb{U}} \to G$ is a morphism of algebraic groups having a finite kernel. We consider the cases of $m = 0$ and $m \neq 0$ separateley.

Consider the case that $m = 0$. Let N be a multiple of n so that ψ is defined over $\mathrm{Fix}(\sigma^N)$. Factor $P(X) = \beta \prod(X - \alpha_i)$ and set $Q(X) = \beta \prod(X - \alpha_i^N)$. Then $\ker P(\sigma) \leq \ker Q(\sigma^N)$ and $Q(X)$ is a polynomial with integer coefficients having no roots of unity amongst its complex roots. Now, $\psi(H(\mathrm{Fix}(\sigma^N)))$ is a subgroup of $G(\mathrm{Fix}(\sigma^N))$. Thus, $G(\mathrm{Fix}(\sigma^N))$ meets $\ker Q(\sigma^N)$ in an infinite group. It follows that $Q(1) = 0$ contrary to our hypothesis on Q.

Consider now the case of $m \neq 0$. Let $G' \leq G$ be the image of ψ (as an algebraic group). By our hypotheses, G' is defined over $\mathrm{Fix}(\sigma)$. By Lemma 3.8 there is an algebraic group H_0 defined over $\mathbb{F}_p^{\mathrm{alg}}$ and an isogeny $\vartheta : (H_0)_{\mathbb{U}} \to H_{\mathbb{U}}$. Taking N large enough, we see that ϑ is defined over $k' := \mathrm{Fix}(\sigma^{nN} \tau^{mN})$. The group $\vartheta(H_0(k'))$ is a subgroup of finite index in $H(k')$. It follows that $(\psi \circ \vartheta)(H_0(k'))$ meets E in a group of finite index so that E is strongly essentially algebraic. □

Before we can finish the proof of Theorem 2.2, we need to understand the structure of subvarieties of semiabelian varieties which meet the torsion of essentially algebraic groups in a Zariski dense set.

Lemma 3.14. *Let G be a semiabelian variety over $\mathbb{U}$. Suppose that G is weakly isotrivial and that $X \subseteq G$ is an irreducible subvariety with $X(\mathbb{U}) \cap G(\mathbb{U})_{\mathrm{tor}}$ Zariski dense in X. Then X is special.*

Proof. Let H be a semiabelian variety defined over a finite field and $\psi : H_{\mathbb{U}} \to G$ a purely inseparable isogeny witnessing the weak isotriviality of G. Let $X_0 := \psi^{-1}X \subseteq H_{\mathbb{U}}$ As ψ is purely inseparable, $X(\mathbb{U}) = \psi X_0(\mathbb{U})$. As $G(\mathbb{U})_{\mathrm{tor}}$ is dense in X, we see that $H(\mathbb{U})_{\mathrm{tor}} = H(\mathbb{F}_p^{\mathrm{alg}})$ is dense in X_0. Hence, X_0 is defined over $\mathbb{F}_p^{\mathrm{alg}}$. □

We are now in a position now to prove Theorem 2.2. The symbol $\mathbb{U}$ no longer refers to a fixed existentially closed difference field. The other notation refers to the statement of Theorem 2.2.

Proof. Working by noetherian induction on X, we may assume that X is irreducible and that $X(K) \cap G(K)_{\mathrm{tor}}$ is Zariski dense in X. Passing to the quotient by the stabilizer of X, we may assume that X has a trivial stabilizer.

Let $(\mathbb{U}, +, \times, 0, 1, \sigma) \models$ ACFA be an existentially closed difference field with $K \leq \mathbb{U}$, $\sigma(G) = G$, $P(X) \in \mathbb{Z}[X]$ a polynomial over the integers with no roots of unity amongst its complex roots and $P(\sigma)$ vanishing on $G(K)_{\mathrm{tor}}$, and every connected algebraic subgroup of any power of G is already defined over $\mathrm{Fix}(\sigma)$. Let $E \leq \ker P(\sigma) =: \Gamma$ be an essentially algebraic subgroup of maximal dimension. By lemma 3.12, $X(K)$ is contained in a translate of the Zariski closure of E. Translating, we may assume that X is a subvariety of the Zariski closure, H, of E. By Lemma 3.13 E is strongly essentially algebraic so that H is isogenous to a semiabelian variety defined over a finite field. Now, X meets the torsion of H in a Zariski dense set so by Lemma 3.14 X is special. □

4. Towards the full positive characteristic Mordell-Lang conjecture

The full Mordell-Lang conjecture over $\mathbb{C}$ asserts that if S is a semiabelian variety over $\mathbb{C}$, $\Gamma \leq S(\mathbb{C})$ is a finite dimensional subgroup of the complex points (in the sense that $\dim_{\mathbb{Q}}(\Gamma \otimes \mathbb{Q}) < \infty$), and $X \subseteq S$ is a closed subvariety, then $X(\mathbb{C}) \cap \Gamma$ is a finite union of cosets of subgroups of Γ. Of course, the direct translation of this statement to positive characteristic is false, but with the requisite allowances for special varieties it may be true. Hrushovski proved such a version with the restriction that $\mathrm{rk}_{\mathbb{Z}_{(p)}}(\Gamma \otimes \mathbb{Z}_{(p)})$ be finite. In this section we note that the full version (with $\mathbb{Q}$ in place of $\mathbb{Z}_{(p)}$) would follow from the restricted case where Γ is assumed to lie in $S(K)$ where K is the perfection of a finitely generated field.

At this point, let us state precisely the conjectures to be proven.

Conjecture 4.1. *Let K be an algebraically closed field of positive characteristic, S a semiabelian variety over K, $\Gamma < S(K)$ a finite dimensional (in the sense that $\dim_{\mathbb{Q}}(\Gamma \otimes \mathbb{Q}) < \infty$) subgroup of the K points, and $X \subseteq S$ a closed irreducible subvariety for which $X(K) \cap \Gamma$ is Zariski dense in X. Then X is special.*

An ostensible weakening of Conjecture 4.1 takes the following form.

Conjecture 4.2. *Let K be a finitely generated field of characteristic $p > 0$ and $K^{\mathrm{alg}} > K$ an algebraic closure of K. Let $L := K^{\mathrm{per}} := \{x \in K^{\mathrm{alg}} \mid (\exists n \in \mathbb{Z}_+)\ x^{p^n} \in K\}$ be the perfection of K. Let S be a semiabelian variety over L and $\Gamma \leq S(L)$ a finite dimensional subgroup of the L-points of S. If $X \subseteq S$ is an irreducible subvariety for which $X(L) \cap \Gamma$ is Zariski dense in X, then X is special.*

Using the methods of the previous section, we show that there two conjectures are equivalent.

Theorem 4.3. *Conjecture 4.1 and Conjecture 4.2 are equivalent.*

Proof. As each instance of Conjecture 4.2 is an instance of Conjecture 4.1, the left-to-right implication is immediate. We concentrate on proving the other direction.

Let S be a semiabelian variety over the algebraically closed field K, $\Gamma < S(K)$ a finite dimensional subgroup of the K-points of S and $X \subseteq S$ a closed irreducible subvariety containing a Zariski dense set of Γ points. We work by noetherian induction on X and pass to quotients when need be so that we may assume that X has a trivial stabilizer.

Let $B \subseteq \Gamma$ be a subset of Γ for which $|B| = |\{b \otimes 1_{\mathbb{Q}} \mid b \in B\}|$ and $\{b \otimes 1_{\mathbb{Q}} \mid b \in B\}$ is a basis for $\Gamma \otimes \mathbb{Q}$. Let $k < K$ be a finitely generated subring for which S and X are defined over k (More precisely, there is a group scheme S' over k and a closed subscheme $X' \subseteq S'$ also over k so that $S = S'_K$, $X = X'_K$, and the inclusion of X in S is also given by base change. We ignore these niceties for the remainder of this argument.) and $B \subseteq S(k)$. Then the group $S(k)$ is finitely generated and Γ is a subgroup of the division hull $S(k)^{\mathrm{div}}$ of $S(k)$ in $S(K)$: $\{\xi \in S(K) \mid (\exists n \in \mathbb{Z}_+)\, n\xi \in S(k)\}$. Thus, we may, and do, assume that $\Gamma = S(k)^{\mathrm{div}}$.

Choose, as in the proof of Theorem 2.2, a relative Frobenius σ on K fixing k and a polynomial $P(X) \in \mathbb{Z}[X]$ having no roots of unity amongst its roots for which $P(\sigma)$ vanishes on the torsion subgroup of $S(K)$.

Let $(\mathbb{U}, \sigma)$ be an existentially closed difference field extending (K, σ). Let $T = \ker P(\sigma)(\mathbb{U})$ and $F := S(\mathrm{Fix}(\sigma))$. Note that the operator $x \mapsto P(\sigma) \circ (\sigma - 1)(x)$ vanishes on Γ. Thus, $\Gamma \leq T + F$. More importantantly for us, since the group $T \cap F \leq S[P(1)](k^{\mathrm{per}})$ is finite, the group $(\Gamma \cap T) + (\Gamma \cap F)$ is of finite index in Γ. Thus, the result for Γ follows from the corresponding statement for $(\Gamma \cap T) + (\Gamma \cap F)$. So, we may, and do, assume that $\Gamma = (\Gamma \cap T) + (\Gamma \cap F)$.

Let $s : S \times S \to S$ be the addition map $(x, y) \mapsto x + y$. Let $\widetilde{X} := s^{-1}X$. We have

$$\begin{aligned} X(K) \cap \Gamma &= X(\mathbb{U}) \cap \Gamma \\ &= s(\widetilde{X}(\mathbb{U}) \cap [(T \cap \Gamma) \times (F \cap \Gamma)]) \\ &= s([\widetilde{X}(\mathbb{U}) \cap (T \times F)] \cap [(T \cap \Gamma) \times (F \times \Gamma)] \end{aligned}$$

So it suffices to understand the intersection on the right.

As $P(X)$ has no roots of unity amongst its complex roots, the groups $\ker P(\sigma)(\mathbb{U})$ and $S(\mathrm{Fix}(\sigma))$ are orthogonal. Thus, there are (σ-)closed sets $Y_1, \ldots, Y_n \subseteq T$ and $Z_1, \ldots, Z_n \subseteq F$ such that

$$\widetilde{X}(\mathbb{U}) \cap (T \cap F) = \bigcup_{i=1}^{n} Y_i \times Z_i$$

Let $\mathfrak{Y}_i := \overline{Y_i \cap \Gamma}$ and $\mathfrak{Z}_i := \overline{Z_i \cap \Gamma}$. Then we have,

$$\begin{aligned} X(K) \cap \Gamma &= s([\widetilde{X}(\mathbb{U}) \cap (T \times F)] \cap [(T \cap \Gamma) \times (F \cap \Gamma)] \\ &= \bigcup_{i=1}^{n} (Y_i \times Z_i) \cap [(T \cap \Gamma) \times (F \cap \Gamma)] \\ &= \bigcup_{i=1}^{n} [\mathfrak{Y}_i(\mathbb{U}) \cap (T \cap \Gamma)] \times [\mathfrak{Z}_i(\mathbb{U}) \cap (F \cap \Gamma)] \end{aligned}$$

Decomposing further, we may assume that each $\mathfrak{Y}_i$ and $\mathfrak{Z}_i$ is irreducible.

As Γ is Zariski dense in X, we see that $X = \mathfrak{Y}_i + \mathfrak{Z}_i$ for some i.

From the proof of Theorem 2.2 we see that each of the $\mathfrak{Y}_i$ is a special variety. The sum of two special varieties is still special, so it suffices to show that $\mathfrak{Z}_i$ is special.

As $X = \mathfrak{Z}_i + \mathfrak{Y}_i$, we have $\dim \mathfrak{Z}_i \leq \dim X$. If we have a strict inequality, then by induction we know that $\mathfrak{Z}_i$ is special. If $\dim \mathfrak{Z}_i = \dim X$, then as X is irreducible we conclude that $X = \gamma + \mathfrak{Z}_i$ for some $\gamma \in \Gamma$. Thus, $X(K) \cap \Gamma = \gamma + (\mathfrak{Z}_i(\mathbb{U}) \cap F \cap \Gamma)$. So, it suffices to consider intersections of varieties with groups of the form $F \cap \Gamma$. As the torsion group of F is finite (contained in $S[P(1)](\mathbb{U})$), we see that $P(1)(F \cap \Gamma)$ is of finite index in $F \cap \Gamma$ and is torsion free. Thus, it suffices to show the following claim.

Claim 4.4. *If $\Psi \leq S(k)^{\mathrm{div}}$ is torsion free, $Z \subseteq S$ is an irreducible closed subvariety, and $Z(K) \cap \Psi$ is Zariski dense in Z, then Z is special.*

Proof of Claim: For the purposes of this argument, we define the rank of Ψ to be the minimal integer d for which there is a finite group G and an embedding $\mu : \Psi/(\Psi \cap S(k^{\mathrm{per}})) \hookrightarrow G \oplus (\mathbb{Q}/\mathbb{Z})^d$.

We prove the claim by induction on d. When $d = 0$, the claim is an immediate consequence of our hypothesis that Conjecture 4.2 holds.

Consider now the case that $d > 0$. Let $\gamma \in \Psi$ be some element for which the projection to $(\mathbb{Q}/\mathbb{Z})^d$ of $\mu(\gamma)$ is not zero. Then there is a conjugate ρ of σ for which $\rho(\gamma) \neq \gamma$. Extend ρ to $\mathbb{U}$ so that $(\mathbb{U}, \rho)$ is an existentially closed difference field.

Possibly passing to a subgroup of finite index, we see that $\ker P(\rho) \circ (\rho - 1)(\mathbb{U})$ is a direct sum of $S(\mathrm{Fix}(\rho))$ and $\ker P(\rho)$. Let $\pi : \ker P(\rho) \circ (\rho - 1)(\mathbb{U}) \to S(\mathrm{Fix}(\rho))$ and $\nu : \ker P(\rho) \circ (\rho - 1)(\mathbb{U}) \to \ker P(\rho)$ be the projections expressing $\ker P(\rho) \circ (\rho - 1)(\mathbb{U})$ as a direct sum. Then $\Gamma = \pi(\Gamma) + \nu(\Gamma)$. Note that the rank of $\pi(\Gamma) < d$ but (using the orthogonality of $\ker P(\rho)$ and $S(\mathrm{Fix}(\rho))$ as above) we have $Z(K) \cap \Gamma = a + [(Z - a)(K) \cap \pi(\Gamma)]$ for some $a \in \nu(\Gamma)$. By induction, $Z - a$, and hence Z also, are special.

With this claim established the theorem follows. ☐

Conjecture 4.2 remains open, but there are some nontrivial cases in which it is known. Dragos Ghioca has shown that if E is a non-isotrivial elliptic curve over a finitely generated field k of characteristic $p > 0$, then there is a natural number n such that $E(K^{\mathrm{per}}) = E(K^{p^{-n}})$ [4]. Consequently, if A is a product of non-isotrivial elliptic curves over the finitely generated field K and $\Gamma \leq A(K^{\mathrm{per}})$ is a finite dimensional subgroup, then Γ is actually finitely generated. So, by reducing to Hrushovski's theorem one sees that Conjecture 4.2 holds for A isogenous to a product of (not necessarily ordinary, not necessarily non-isotrivial) elliptic curves. Such a reduction cannot be achieved in every case. For instance, there are non-weakly isotrivial abelian varieties A of p-rank zero. If A is defined over K and $A(K)$ is infinite, the $A(K^{\mathrm{per}})$ cannot be finitely generated. However, the reduction might succeed for sufficiently general ordinary abelian varieties.

References

[1] Z. Chatzidakis, Groups definable in ACFA, in **Algebraic Model Theory**, (B. Hart, A. Lachlan, and M. Valeriote eds.) NATO ASI Series C: Mathematical and Physical Sciences **496**, Kluwer Academic Publishers (Dordecht, The Netherlands), 1997, 25 – 52.

[2] Z. Chatzidakis and E. Hrushovski, *Trans. Amer. Math. Soc.* **351** (1999), no. 8, 2997–3071.

[3] Z. Chatzidakis, E. Hrushovski, and Y. Peterzil, Model theory of difference fields. II. Periodic ideals and the trichotomy in all characteristics, *Proc. LMS* (3) **85** (2002), no. 2, 257–311.
[4] D. Ghioca, Elliptic curves over the perfect closure of a function field, preprint, 2003.
[5] E. Hrushovski, The Mordell-Lang conjecture for function fields, *JAMS* **9** (1996), no. 3, 667–690.
[6] E. Hrushovski, The Manin-Mumford conjecture and the model theory of difference fields, *APAL* **112** (2001), no. 1, 43–115.
[7] A. Pillay, Mordell-Lang for functions fields in characteristic zero, revisited, pre-print 2002.
[8] A. Pillay, Lectures 1 & 2 of "Model Theory and Differential Geometry," Arizona Winter School 2003, `http://swc.math.arizona.edu/~swcenter/notes/files/03PillayNotes1.pdf`
[9] A. Pillay, On the Manin-Mumford conjecture, preprint, 2003.
[10] R. Pink and D. Roessler, On ψ-invariant subvarieties of semiabelian varieties and the Manin-Mumford conjecture, preprint, 2002.
[11] M. Raynaud, Around the Mordell conjecture for function fields and a conjecture of Serge Lang, in: Proc. Algebraic Geometry of Tokyo, Lecture Notes, vol. **1016**, Springer, Berlin, 1982.
[12] T. Scanlon, Diophantine geometry from model theory, *BSL* **7** (2001), no. 1, 37–57.

E-mail address: `scanlon@math.berkeley.edu`

University of California, Berkeley, Department of Mathematics, Evans Hall, Berkeley, CA 94720-3480, USA