Compositio Math. 141 (2005) 1351–1364
doi:10.1112/S0010437X05001879

A 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 due to Raynaud [Ray83]) asserts that if A is an abelian variety over a number field k with an algebraic closure k^{alg} 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 subgroups 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 [Sca01]. As the reader will see, given the model-theoretic treatment of difference closed fields from [CHP02] this argument follows Hrushovski's proof of the number field Manin–Mumford conjecture [Hru01]. 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 of this theorem in [PR04]. While their proof avoids appeals to the model theory of difference fields, it also uses some sophisticated arguments (involving, for instance, the theory of Dieudonné modules). Pillay presented an elementary proof of the function field Mordell–Lang conjecture using an analysis of algebraic D-groups [Pil04] and then transposed this argument to the context of algebraic σ-groups to reprove the Manin–Mumford conjecture over number fields [Pil03a]. The student working group supervised by Pillay and Scanlon at the 2003 Arizona Winter School completed an elementary proof of the key lemma required to extend Pillay's argument for the Manin–Mumford conjecture to positive characteristic. Some details of this argument are available in a streaming video on the Southwestern Center's webpage and in a recent preprint of Pillay [Pil03b].

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 [Hru96].

Received 16 September 2003, accepted in final form 20 July 2005.
2000 Mathematics Subject Classification 03C60, 11G10, 12H10.
Keywords: semiabelian varieties, modular groups, torsion points, difference fields.
Partially supported by NSF Grant DMS-0303618 and an Alfred P. Sloan Fellowship.

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 $X \times_{\mathrm{Spec}(R)} \mathrm{Spec}(S)$. We write '$S$-point (of X)' and 'S-valued point (of X)' indiscriminately for the elements of $X_S(S)$. 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 $\mathbb{F}_p^{\mathrm{alg}}$;
- $H \leqslant G$ an algebraic subgroup of G;
- a point $a \in G(K)$;
- a subvariety $X_0 \subseteq H_0$ defined over $\mathbb{F}_p^{\mathrm{alg}}$; and
- a morphism of algebraic groups $h : H \to (H_0)_K$;

such that $X = a + h^{-1}(X_0)_K$.

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 split 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 [Cha97, CH99, CHP02, Hru01]. 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 section, 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: σ fixes a field of definition for G; $P(\sigma)$, 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 role 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 discrete valuation ring (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.

https://doi.org/10.1112/S0010437X05001879 Published online by Cambridge University Press

Lemma 3.1. *Let R be a finitely generated domain of characteristic $p > 0$. Then there is a Zariski dense and open set $U \subseteq \operatorname{Spec} R$ so that for any $\mathfrak{p} \in U$ for some power q of p, there is an embedding $\iota : R \hookrightarrow \mathbb{F}_q[[\epsilon]]$ with $\iota(\mathfrak{p}) \subseteq (\epsilon)$.*

Proof. Write $R = \mathbb{F}_p[a_1, \dots, a_n]$ for appropriate generators $a_1, \dots, a_n$. Rearranging the generators if need be, we may assume that $a_1, \dots, a_m$ are algebraically independent and that R is algebraic over $R' := \mathbb{F}_p[a_1, \dots, a_m]$. For each $i > m$, let $P_i(X) \in R'[X]$ be a minimal polynomial for a_i over R' (i.e. $P_i \not\equiv 0$, $P_i(a_i) = 0$, and P_i has minimal possible degree d_i). Let $Q_i(X_1, \dots, X_m) \in \mathbb{F}_p[X_1, \dots, X_n]$ be the polynomial for which $Q_i(a_1, \dots, a_m)$ is the coefficient of X^{d_i} in $P_i(X)$. Let $U := D(\prod_i Q_i(a)) = \{\mathfrak{q} \in \operatorname{Spec} R \mid \prod_i Q_i(a) \notin \mathfrak{q}\}$.

Now take $\mathfrak{p} \in U$ and let $\mathfrak{q} := \mathfrak{p} \cap R'$. Let q be a high enough power of p so that the set $V(\mathfrak{q})(\mathbb{F}_q) \smallsetminus \bigcup_{i=m+1}^{n} V(Q_i)(\mathbb{F}_q)$ is nonempty. Let $\langle b_1, \dots, b_m \rangle$ be one such point. Then for any $i \leqslant n$ and any $\langle c_1, \dots, c_m \rangle \in \mathbb{F}_q[[\epsilon]]$ we have $Q_i(b + \epsilon c) \in \mathbb{F}_q[[\epsilon]]^\times$. Choose $c = \langle c_1, \dots, c_m \rangle$ algebraically independent (such exists as the transcendence degree of $\mathbb{F}_q((\epsilon))$ is $2^{\aleph_0}$) and define an embedding $R'' := \mathbb{F}_p[a_1, \dots, a_m, Q_{m+1}(a)^{-1}, \dots, Q_n(a)^{-1}] \hookrightarrow \mathbb{F}_q[[\epsilon]]$ via $a_i \mapsto b_i + \epsilon c_i$. Now R is contained in a finite integral extension of R'' and, thus, via the above embedding, of $\mathbb{F}_q[[\epsilon]]$. Every such finite integral 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 DVR $R \subseteq K$ 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 $\gamma_1, \dots, \gamma_r \in G[p](K^{\mathrm{alg}}) = \mathfrak{G}[p](S')$ be a basis for the (physical) p-torsion on G. The set U of primes $\mathfrak{p} \in \operatorname{Spec}(S')$ such that the image of $\gamma_1, \dots, \gamma_r$ remain linearly independent in $(\mathfrak{G} \otimes S'/\mathfrak{p})[p](S'/\mathfrak{p})$ is open in the Zariski topology. Let $U'' \subseteq U$ be a dense affine open subset of U and let S'' be the coordinate ring of U''. 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 the following lemma we limit the rings in which we must search for torsion points.

Lemma 3.3. *Let R be a DVR 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':

$$0 \longrightarrow G[n]^0 \longrightarrow G[n] \longrightarrow G[n]_{\text{ét}} \longrightarrow 0.$$

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, $G[n](S') \cong G[n]_{\text{ét}}(S') \cong G[n]_{\text{ét}}(K^{\mathrm{alg}}) \cong G[n](K^{\mathrm{alg}})$.

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

https://doi.org/10.1112/S0010437X05001879 Published online by Cambridge University Press

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 DVR 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

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

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 the 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 of the results of this section, 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 $G(K)_{\mathrm{tor}}$.*

Moreover, if $R \subseteq K$ is a finitely generated subring over which G is defined, then for any maximal ideal $\mathfrak{m}$ of R outside a proper Zariski closed set if $\sigma : K \to K$ is a relative Frobenius at $\mathfrak{m}$, then there is a polynomial $P(X) \in \mathbb{Z}[X]$ with no roots of unity amongst its complex roots for which $P(\sigma)$ 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 the 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.

For the 'moreover' clause, note that in Lemma 3.2 it suffices to take $\mathfrak{m}$ in the intersection of the open set U of Lemma 3.1 and the open set of primes for which the p-rank does not change upon reduction. □

3.2 Background from the model theory of difference fields

In this section we recall some of the main results on the model theory of difference fields (taken mostly from [CH99, CHP02, Hru01]) which we shall employ for our proofs. For the purposes of this paper we eschew the formalism of logic.

https://doi.org/10.1112/S0010437X05001879 Published online by Cambridge University Press

A difference field is simply a field K given together with a distinguished endomorphism $\sigma : K \to K$. A morphism of difference field $\psi : (K, \sigma) \to (L, \rho)$ is a homomorphism of fields $\psi : K \to K$ for which $\rho \circ \psi = \psi \circ \sigma$. If V is a variety over the difference field (K, σ), then we set $V^\sigma := V \times_{\mathrm{Spec}(K)} \mathrm{Spec}(K)$ where the second K obtains its K-algebra structure via σ.

Definition 3.6. A *difference closed field* is a difference field (K, σ) satisfying:

- K is algebraically closed;
- $\sigma : K \to K$ is an automorphism; and
- for any irreducible affine variety V over K and irreducible subvariety $W \subseteq V \times V^\sigma$ which dominates each factor via projection there is a K-rational point $a \in V(K)$ with $\langle a, \sigma(a)\rangle \in W(K)$.

In the literature, difference closed fields are called 'existentially closed difference fields' or 'models of ACFA'. In some sense, difference closed fields may be regarded as analogous to algebraically closed fields. For example, every difference field embeds into a difference closed field and if some finite system of difference equations and inequations is satisfiable in some extension of a difference closed field (K, σ), then it is already satisfiable in (K, σ) (see [CH99, p. 3007]).

For the remainder of this section (K, σ) refers to a difference closed field.

If (K, σ) is a difference closed field and X is an algebraic variety over K, then a *difference subvariety* $Y \subseteq X$ of X is given by an algebraic subvariety $\widetilde{Y} \subseteq X \times X^\sigma \times \cdots \times X^{\sigma^n}$ for some natural number n. The set of (K, σ)-rational points of Y is $Y(K, \sigma) := \{a \in X(K) \mid \langle a, \sigma(a), \ldots, \sigma^n(a)\rangle \in \widetilde{Y}(K)\}$. If $A \subseteq X(K)$ is any set of points and n is a natural number, then we define the nth prolongation of A, $\nabla_n(A)$, to be the Zariski closure in $X \times \cdots \times X^{\sigma^n}$ of the set $\{\langle a, \ldots, \sigma^n(a)\rangle \mid a \in A\}$. We consider two difference subvarieties of X to be the same if they have the same set of (K, σ)-rational points. Equivalently, two difference subvarieties are the same if they have identical prolongations. A finite Boolean combination of difference subvarieties is called a *difference constructible set*. If $\pi : X \to X'$ is a morphism of algebraic varieties and $C \subseteq X$ is a difference constructible subset, then $\pi(C(K, \sigma)) := \{y \in X'(K) \mid (\exists x \in C(K, \sigma))\ \pi(x) = y\}$ is called a *definable set*. Unlike the case of ordinary constructible sets in algebraic geometry, it is not the case that every definable set is constructible. However, every definable set may be expressed as the image of a constructible set under a map which is generically finite [CH99, Corollary 1.5].

For definable sets there are various notions of dimension or rank. The simplest of these is the σ-dimension. If $A \subseteq X(K)$ is a subset of the (K-rational points of the) variety X, then we define the σ-dimension of A to be $\sup \dim \nabla_n(A) \in \mathbb{N} \cup \{\infty\}$. Many of the theorems we cite are stated in terms of S1-rank or SU-rank, which we decline to define here. In the case of difference closed fields, finiteness of any of these ranks (or dimensions) implies the finiteness of all the others (although they need not be equal to each other).

If the characteristic of K is $p > 0$, then the Frobenius map $\tau : K \to K$ given by $x \mapsto x^p$ is an automorphism. For the sake of unifying the statement, let τ be the identity map for K of characteristic zero. In general, if L is an algebraically closed field and $\rho : L \to L$ is an automorphism, then $\mathrm{Fix}(\rho)$ is perfect and $\mathrm{Fix}(\rho)^{\mathrm{alg}} = \bigcup_{n=1}^{\infty} \mathrm{Fix}(\rho^n)$. If $\langle n, m\rangle$ is a pair of integers with $n \neq 0$, then the automorphism $\rho := \sigma^n \tau^m$ has a fixed field $\mathrm{Fix}(\rho)$ which is pseudofinite [CH99, pp. 3007, 3013]. That is:

- $\mathrm{Fix}(\rho)$ is perfect;
- the Galois group of $\mathrm{Fix}(\rho)$ is isomorphic to $\widehat{\mathbb{Z}}$ and its topological generator is the restriction of ρ to $\mathrm{Fix}(\rho)^{\mathrm{alg}}$; and
- $\mathrm{Fix}(\rho)$ is pseudo-algebraically closed (every absolutely irreducible variety over $\mathrm{Fix}(\rho)$ has a $\mathrm{Fix}(\rho)$-rational point).

https://doi.org/10.1112/S0010437X05001879 Published online by Cambridge University Press

Every definable automorphism of K (meaning every automorphism whose graph is a definable set) takes the form $\sigma^n\tau^m$ for some $\langle n, m\rangle \in \mathbb{Z}^2$.

As noted in the introduction to this section, the notion of *orthogonality* is crucial to our proof.

Definition 3.7. If $D \subseteq X(K)$ is a definable subset of the variety X and $E \subseteq Y(K)$ is a definable subset of the variety Y, then we say that D and E are *orthogonal*, written $D \perp E$, if for every pair of natural numbers $\langle n, m\rangle$ every definable subset of $D^n \times E^m$ is a finite Boolean combination of sets of the form $A \times B$ with $A \subseteq D$ and $B \subseteq E$.

What we call here 'orthogonal' might be better termed 'fully orthogonal', but the distinction is irrelevant for our purposes. In the special case that D and E are difference varieties and $D \perp E$, then every difference subvariety of $D \times E$ is a finite union of difference varieties of the form $A \times B$ where $A \subseteq D$ and $B \subseteq E$ are difference subvarieties. If ρ and ρ' are two definable automorphisms for which $\mathrm{Fix}(\rho) \cap \mathrm{Fix}(\rho')$ is finite, then $\mathrm{Fix}(\rho) \perp \mathrm{Fix}(\rho')$. In particular, we have the following.

Fact 3.8. $\mathrm{Fix}(\rho)^{\mathrm{alg}}$ and $\mathrm{Fix}(\rho')^{\mathrm{alg}}$ are algebraically independent.

Definition 3.9. If G is an algebraic group over K and $\Gamma \leqslant G(K)$ is a definable subgroup (meaning that it is a definable subset which is the universe of a subgroup), then we say that Γ is *modular* if every difference constructible subset of any prolongation of Γ is a finite Boolean combination of cosets of difference constructible subgroups.

This term is somewhat better motivated in a more abstract context dealing with combinatorial geometries. Perhaps it would be better to call such groups *module-like*, but for historical reasons we stick with modular. The term 'one-based' is used for a condition applying beyond the context of groups. In the case of groups definable in difference closed fields, modularity and one-basedness are equivalent. In [Hru01] the terms 'locally modular, stably embedded (LMS)' and 'algebraically locally modular (ALM)' are used for related concepts.

The following result is not immediately obvious from the definitions, but holds nonetheless. In [Hru01, Proposition 3.4.1] it is proved under the additional hypothesis of stable embeddedness, but [Wag04, Corollary 12] shows that it holds in general.

Fact 3.10. If G is a definable group having a definable normal subgroup $N \lhd G$ such that N and G/N are both modular, then so is G. In particular, if G is abelian and is the sum of finitely many modular groups, then it is modular itself.

If $\rho : K \to K$ is a definable automorphism and G is an algebraic group over $\mathrm{Fix}(\rho)$, then $G(\mathrm{Fix}(\rho))$ is not modular (unless it is finite). Indeed, if $X \subseteq G^2$ is a sufficiently general curve (not a translate of an algebraic subgroup), then using the fact that $\mathrm{Fix}(\rho)$ is pseudo-algebraically closed one sees that $X(\mathrm{Fix}(\rho)) = X(K) \cap G(\mathrm{Fix}(\rho))^2$ is not expressible as a finite Boolean combination of difference constructible cosets. More generally, if H is any other algebraic group over K and $\psi : G_K \to H$ is a map of algebraic groups with $\psi(G(\mathrm{Fix}(\rho)))$ infinite, then the definable group $\psi(G(\mathrm{Fix}(\rho)))$ is not modular.

If ρ is a (nontrivial) definable automorphism and A is modular, then $A \perp \mathrm{Fix}(\rho)$. (Even, if $\rho_1, \ldots, \rho_m$ is a finite sequence of nontrivial definable automorphisms, then $A \perp (\bigcup_{i=1}^m \mathrm{Fix}(\rho_i))$.) In the case of groups, [CHP02, Theorem A, p. 305] is a converse of sorts. Specifically, if G is a commutative algebraic group over K and $\Gamma \leqslant G(K)$ is a finite σ-dimensional definable subgroup having no infinite definable subgroup of infinite index, then Γ is modular if and only if $\Gamma \perp \mathrm{Fix}(\rho)$ for every nontrivial definable automorphism $\rho : K \to K$.

Recall that if $A, B \leqslant C$ are two subgroups of the group C, then we say that A and B are *commensurable* if $A/(A \cap B)$ and $B/(A \cap B)$ are both finite.

https://doi.org/10.1112/S0010437X05001879 Published online by Cambridge University Press

With the next definition we introduce (strongly) essentially algebraic groups. This notion is implicit, although not explicit, in the literature.

Definition 3.11. Let G be a commutative algebraic group defined over K. The group $\Gamma < G(K)$ is a *basic essentially algebraic subgroup* of $G(K)$ if it is an infinite group of the form $\psi(H(\mathrm{Fix}(\rho)))$ where $\rho : K \to K$ is a nontrivial definable endomorphism, H is an algebraic group defined over $\mathrm{Fix}(\rho)$ and $\psi : H_K \to G$ is a morphism of algebraic groups. If the group H may be taken to be defined over a finite field, then we say that Γ is a *basic strongly essentially algebraic subgroup* of $G(K)$. A definable subgroup of $G(K)$ which is commensurable with a finite sum of basic essentially algebraic (respectively, basic strongly essentially algebraic) subgroups is said to be *essentially algebraic* (respectively, *strongly essentially algebraic*).

The dichotomy theorem for definable subgroups of commutative algebraic groups may be strengthened as follows.

Fact 3.12. Let G be a semiabelian variety over K. Suppose that $\Gamma < G(K)$ is an infinite definable subgroup of finite σ-dimension having no infinite definable subgroup of infinite index. Then Γ is either modular or essentially algebraic.

This result is not explicitly stated in our references. So, we explain how to derive it from the published theorems.

Proof. By [CHP02, Theorem A], if Γ is not modular, then it is nonorthogonal to the fixed field, $\mathrm{Fix}(\rho)$, of some nontrivial definable field endomorphism ρ. Let $Y \subseteq \Gamma$ be a minimal difference subvariety (Y is infinite but every proper difference subvariety is finite). By the analogue of Zilber's indecomposability theorem [Hru01, Lemma 3.2.2], Y generates a definable subgroup of Γ which by our hypothesis must have finite index in Γ. As $\Gamma \not\subset \mathrm{Fix}(\rho)$, it follows that $Y \not\subset \mathrm{Fix}(\rho)$. One sees easily that possibly after naming some parameters, a witness to this nonorthogonality gives a finite-to-finite correspondence between Y and $\mathrm{Fix}(\rho)$. Thus, the hypotheses of [Hru01, Lemma 4.0.2] hold and we obtain an algebraic group H defined over $\mathrm{Fix}(\rho)$ and a definable homomorphism $\gamma : \Gamma \to H(\mathrm{Fix}(\rho))$ having a finite kernel and a finite cokernel. If n is the exponent of $\ker \gamma$, then the map $\delta : y \mapsto [n](\gamma^{-1}(y))$ is a well-defined homomorphism on $\gamma(\Gamma)$ having a finite kernel. It follows that δ, possibly restricted to a subgroup of finite index, is the restriction of an isogeny $\widetilde{\delta} : H_K \to G$ which witnesses the essential algebraicity of Γ. □

Proposition 3.6.2 of [Hru01] 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 role here. Unfortunately, the statement of [Hru01, Proposition 3.6.2] contains some very technical hypotheses, all of which are satisfied in our intended application, but they are technical nonetheless. We recall this proposition specialized slightly to the case of definable subgroups of algebraic groups.

Fact 3.13. Let $k \leqslant K$ be a countable algebraically closed difference subfield. We are given

- G, a commutative algebraic group over k;
- $\Gamma < G(K)$, a difference constructible subgroup of finite σ-dimension defined over k;
- $X \subseteq \Gamma$, an irreducible difference subvariety of Γ; and
- $\Xi \leqslant \Gamma$, a difference constructible subgroup defined over k

such that:

- every difference constructible subgroup of Γ/Ξ is defined over k;

https://doi.org/10.1112/S0010437X05001879 Published online by Cambridge University Press

- it is not possible to find a definable group $\Xi < \Upsilon \leqslant \Gamma$, a minimal difference variety Y (in the sense that $Y(K,\sigma)$ is infinite but any proper difference subvariety of Y is finite), difference subvariety $W \subseteq \Upsilon \times Y^n$ for which the first projection is surjective and the second projection is generically finite over its image, and Υ/Ξ infinite; and
- the stabilizer of X in Ξ is trivial.

Then X is contained in a single coset of Ξ.

In our intended application, G is a semiabelian variety. In this case, the algebraic groups $\nabla_n(G) = G \times \cdots \times G^{\sigma^n}$ are themselves semiabelian varieties and every algebraic subgroup of $\nabla_n(G)$ is defined over k. It follows that every difference constructible subgroup of Γ is defined over k. It follows from Facts 3.10 and 3.12 that if Ξ is the sum of E, an essentially algebraic subgroup of maximal possible σ-dimension, and M, a modular subgroup of maximal possible σ-dimension, then the hypothesis on the nonexistence of Υ holds.

3.3 σ-algebraic groups of finite σ-dimension

In this section, we analyze the structure of subgroups of semiabelian varieties defined by difference equations.

Definition 3.14. Let $K = K^{\mathrm{alg}}$ be an algebraically closed field and $k \leqslant K$ 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 $(G_0)_K[\psi](K) \leqslant G_0(k)$. So, the quotient H of G_0 by the constant group scheme $(G_0)_K[\psi]_{\mathrm{red}}$ is defined over k and the induced isogeny $\vartheta : H_K \to G$ is bijective on the K-rational points.

Slicker proofs of the following lemma are certainly possible. For instance, it follows from the existence of a minimal algebraically closed field of moduli for the isogeny class of an algebraic group. While we expect that the existence of such fields is well known, we were unable to find published proofs for the case of semiabelian varieties. We present an algebraic reformulation using the language of Weil-style algebraic geometry of an argument from basic stability theory.

Lemma 3.15. *Let M be an algebraically closed field and K_1 and K_2 algebraically closed subfields which are algebraically independent over $L := K_1 \cap K_2$. Suppose that A is an algebraic group over K_1, B is an algebraic group over K_2 and that there is a surjective morphism of algebraic groups $g : A_M \to B_M$ with $\Upsilon := (\ker g)_{\mathrm{red}}$ defined over K_1. Then there is an algebraic group B' defined over L and a morphism of algebraic groups $g' : A \to (B')_M$ with $\Upsilon = (\ker g')_{\mathrm{red}}$.*

Proof. Choosing equations for A, B, and g, we may express A as a fibre $A = \mathcal{A}_a$ of a group scheme $\mathcal{A} \to V_1$ and $B = \mathcal{B}_b$ as a generic fibre of a group scheme $\mathcal{B} \to V_2$ where V_1 and V_2 are irreducible varieties over L, $a \in V_1(K_1)$, and $b \in V_2(K_2)$. Moreover, we may assume that a is Weil generic in V_1 over L and b is Weil generic in V_2 over L. Likewise, identifying g with its graph, we may find a map $\pi : W \to V_1 \times V_2$, a subvariety $G \subseteq (\mathcal{A} \times \mathcal{B}) \times_{(V_1 \times V_2)} W$, and an M-rational point $c \in W(M)$ for which $\pi(c) = \langle a, b \rangle$ and G_c is the graph of g. The condition on $z \in W(M)$ that G_z is the graph of a surjective morphism of algebraic groups is constructible. Hence, possibly at the cost of shrinking G, we may assume that it holds for general $z \in W(M)$.

Using Chevalley's theorem, one sees that the set

$$C := \{y \in V_2(M) \mid (\exists z \in W(M))\ G_z \text{ is the graph of a surjective map from } \mathcal{A}_a \text{ to } \mathcal{B}_y \text{ with kernel } \Upsilon\}$$

https://doi.org/10.1112/S0010437X05001879 Published online by Cambridge University Press

is K_1-constructible. By hypothesis, $b \in C$. As K_1 and K_2 are algebraically independent, b is still Weil generic in V_2 over K_1. Hence, outside of a proper closed subset, every point in $V_2(M)$ lies in C. In particular, we can find some point $b' \in V_2(L) \cap C$. □

Until further notice is given $(\mathbb{U}, \sigma)$ denotes a fixed difference closed 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 3.15 to the special case of algebraic closures of incomparable fixed fields in difference closed fields.

Lemma 3.16. *Let A be a semiabelian variety defined over $\mathrm{Fix}(\sigma)$. Suppose that 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. By Fact 3.8 the fields $\mathrm{Fix}(\sigma)^{\mathrm{alg}}$ and $\mathrm{Fix}(\sigma^n\tau^m)^{\mathrm{alg}}$ are algebraically independent over their common intersection. We know that

$$\mathrm{Fix}(\sigma)^{\mathrm{alg}} = \bigcup_{N \geqslant 0} \mathrm{Fix}(\sigma^N) \quad \text{and} \quad \mathrm{Fix}(\sigma^n\tau^m)^{\mathrm{alg}} = \bigcup_{M \geqslant 0} \mathrm{Fix}(\sigma^{nM}\tau^{mM})$$

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 3.15 we see that A is isogenous to a semiabelian variety defined over $\mathbb{F}_p^{\mathrm{alg}}$. □

As promised, we specialize Fact 3.13 to the case of definable subgroups of semiabelian varieties.

Lemma 3.17. *Let G be a semiabelian variety over $\mathbb{U}$ and $\Gamma \leqslant G(\mathbb{U})$ a definable subgroup of finite σ-dimension. Let $E \leqslant \Gamma$ be an essentially algebraic subgroup of maximal σ-dimension. 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 E.*

Proof. Let $M \leqslant \Gamma$ be a modular subgroup of maximal possible σ-dimension. Set $\Xi := M + E$. As we noted in the discussion following Fact 3.13, this fact applies to Ξ so that $X(\mathbb{U}) \cap \Gamma$ is contained in a single coset of Ξ. Translating, we may assume that $X(\mathbb{U}) \cap \Gamma \subseteq \Xi$.

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 $X(\mathbb{U}) \cap \Xi = s(\widetilde{X}(\mathbb{U}) \cap (M \times \Xi))$. As $M \perp E$, the set $\widetilde{X}(\mathbb{U}) \cap (M \times E)$ is a finite union of sets of the form $(\Delta \times Y)$ where $Y \subseteq E$ and $\Delta \subseteq M$ are definable sets. As M is modular and X is closed, we may take Δ to be a translate of a definable subgroup of M. As X is irreducible and is equal to the Zariski closure of $X(\mathbb{U}) \cap \Gamma$, it is equal to $s(\overline{\Delta} \times \overline{Y})$ for one of the sets $\Delta \times Y$ in the decomposition of $\widetilde{X}(\mathbb{U}) \cap (M \times E)$. As X has a trivial stabilizer, Δ must be a single point, a. That is, $X = a + \overline{Y}$ for some definable subset $Y \subseteq E$. *A fortiori*, $X \subseteq a + \overline{E}$. □

For our ultimate application of Lemma 3.17 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 3.18. *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 $E \leqslant \ker P(\sigma) < G(\mathbb{U})$ is an essentially algebraic subgroup of the kernel of $P(\sigma)$ on $G(\mathbb{U})$, then E is strongly essentially algebraic.*

https://doi.org/10.1112/S0010437X05001879 Published online by Cambridge University Press

Proof. It suffices to consider the case that E is a subgroup of a group of the form $\psi(H(F))$ where $F = \mathrm{Fix}(\sigma^n\tau^m)$ for a pair of integers with $n \neq 0$, H is an algebraic group over F, 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 $m \neq 0$ separately.

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 $\ker P(\sigma) \leqslant \ker Q(\sigma^N)$ 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 $G' \leqslant G$ be the image of ψ (as an algebraic group). By our hypotheses, G' is defined over $\mathrm{Fix}(\sigma)$. By Lemma 3.16 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 $F' := \mathrm{Fix}(\sigma^{nN}\tau^{mN})$. The group $\vartheta(H_0(F'))$ is a subgroup of finite index in $H(F')$. It follows that $(\psi \circ \vartheta)(H_0(F'))$ 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 3.19. *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 to prove Theorem 2.2. The symbol $\mathbb{U}$ no longer refers to a fixed difference closed 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.

By Corollary 3.5 we may find an automorphism $\sigma : K \to K$ and a polynomial $P(X) \in \mathbb{Z}[X]$ having no roots of unity amongst its complex roots so that $P(\sigma)$ vanishes on $G(K)_{\mathrm{tor}}$. Every connected algebraic subgroup of G is defined over a finite extension of $\mathrm{Fix}(\sigma)$. In particular, taking $n \geqslant 1$ sufficiently divisible, every connected algebraic subgroup of G is defined over $\mathrm{Fix}(\sigma)$. If $P(X)$ factors as $\prod(X - \alpha_i)$, then the polynomial $Q(X) = \prod(X - \alpha_i^n)$ also has integral coefficients, no roots of unity amongst its complex roots, and $Q(\sigma^n)$ vanishes on $G(K)_{\mathrm{tor}}$. Thus, replacing σ with σ^n and P with Q we may assume that every connected algebraic subgroup of G is already defined over $\mathrm{Fix}(\sigma)$.

Let $(\mathbb{U}, \sigma)$ be a difference closed field extending (K, σ). Let $E \leqslant \ker P(\sigma) =: \Gamma$ be an essentially algebraic subgroup of maximal σ-dimension. By Lemma 3.17, $X(K)$ 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 3.18, 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 3.19, X is special. □

https://doi.org/10.1112/S0010437X05001879 Published online by Cambridge University Press

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 $\mathbb{C}$, $\Gamma \leqslant S(\mathbb{C})$ is a finite rank 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. Generalizing results of Abramovich and Voloch [AV92], 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 rank (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 $\Gamma \leqslant S(L)$ a finite rank 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.

It should be noted that the groups in Conjecture 4.2 are much smaller than those in Conjecture 4.1. For instance, using the notation above, $S(L)$ always has a finite torsion group, and unless finite itself, is never n-divisible for n coprime to p. Neither of these properties need hold for Γ of Conjecture 4.1. We reduce Conjecture 4.1 to Conjecture 4.2 by choosing an automorphism so as to split the group Γ into a subgroup of a modular group and a subgroup of an orthogonal group and then analyzing the situation along the lines of our work from the last section. A single choice of an automorphism might not suffice, but through an appropriate induction we complete the reduction.

Theorem 4.3. *Conjectures 4.1 and 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 rank subgroup of the K-rational points of S, and $X \subseteq S$ a closed irreducible subvariety containing a Zariski dense set of points from Γ. 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 finite subset of Γ for which $\{b \otimes 1_{\mathbb{Q}} \mid b \in B\}$ is a basis for $\Gamma \otimes \mathbb{Q}$. Let $M < K$ be a finitely generated subring for which S and X are defined over M and $B \subseteq S(M)$. Denote the fraction field of M by L. More precisely, there is a group scheme S' over M and a closed subscheme $X' \subseteq S'$ also over M 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. As M is a finitely generated ring, it follows from the Lang–Néron theorem that $S(M)$ is a finitely generated group. The group Γ is a subgroup of the division hull of $S(M)$,

$$S(M)^{\mathrm{div}} := \{\xi \in S(K) \mid (\exists n \in \mathbb{Z}_+)\ n\xi \in S(M)\}.$$

For the purposes of this argument, we say that (σ, P) is a *good pair* if $\sigma : K \to K$ is a field automorphism and $P(X) \in \mathbb{Z}[X]$ is an integral polynomial for which $P(\sigma)$ vanishes on $S(K)_{\mathrm{tor}}$ and

https://doi.org/10.1112/S0010437X05001879 Published online by Cambridge University Press

$P(X)$ has no roots of unity amongst its complex roots. By Corollary 3.5 for almost any relative Frobenius σ there is a polynomial P so that (σ, P) is a good pair. In particular, for any point $\xi \in \Gamma \smallsetminus S(L^{\mathrm{per}})$ there are good pairs (σ, P) with $\sigma(\xi) \neq \xi$.

For the moment, fix one good pair (σ, P). Let $(\mathbb{U}, \sigma)$ be a difference closed field extending (K, σ). Let $T = \ker P(\sigma)(\mathbb{U})$ and $F := S(\mathrm{Fix}(\sigma))$. We note that $\Gamma = (\Gamma \cap T) + (\Gamma \cap F)$. Indeed, as $P(X)$ and $(X-1)$ are coprime in $\mathbb{Q}[X]$ there are polynomials $Q, R \in \mathbb{Z}[X]$ and a positive integer $m \in \mathbb{Z}_+$ for which $Q(X)P(X) + R(X)(X-1) = m$. We have reduced to the case that $\Gamma = S(M)^{\mathrm{div}}$, so, in particular, $m\Gamma = \Gamma$ and $\sigma(\Gamma) \subseteq \Gamma$. Thus,

$$\begin{aligned}
\Gamma &= m\Gamma \\
&= (Q(\sigma) \circ P(\sigma) + R(\sigma) \circ (\sigma - 1))(\Gamma) \\
&\subseteq Q(\sigma) \circ P(\sigma)(\Gamma) + R(\sigma) \circ (\sigma - 1)(\Gamma) \\
&\subseteq Q(\sigma)(\Gamma \cap F) + R(\sigma)(\Gamma \cap T) \\
&\subseteq (\Gamma \cap F) + (\Gamma \cap T) \\
&\subseteq \Gamma.
\end{aligned}$$

Hence, $\Gamma = (\Gamma \cap F) + (\Gamma \cap T)$.

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

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

So it suffices to understand the intersection on the right.

As $P(X)$ has no roots of unity amongst its complex roots, the groups T and F are orthogonal. Indeed, if T were nonorthogonal to $\mathrm{Fix}(\sigma)$, then it would contain an essentially algebraic subgroup nonorthogonal to $\mathrm{Fix}(\sigma)$, but as was shown in the second paragraph of the proof of Lemma 3.18, this is impossible.

Thus, there are (σ-)closed sets $Y_1, \dots, Y_n \subseteq T$ and $Z_1, \dots, Z_n \subseteq F$ such that

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

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

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

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

By modularity of T, $\mathfrak{Y}_i$ must be a translate of a connected algebraic group. Thus, if $\dim \mathfrak{Y}_i > 0$, then $\mathfrak{Y}_i + \mathfrak{Z}_i$ is a subvariety of the Ueno locus of X, $\mathrm{Ueno}(X)(\mathbb{U}) := \{x \in X(\mathbb{U}) \mid x + B \subseteq X \text{ for some infinite algebraic group } B \leqslant S\}$, which by our hypothesis that X has no stabilizer is a proper subvariety of X (see [Hru98, Lemma 11]).

If $\mathfrak{Y}_i$ is zero dimensional, then as $\mathfrak{Y}_i(\mathbb{U}) \cap (\Gamma \cap T)$ is dense, $\mathfrak{Y}_i = \{\gamma\}$ for some $\gamma \in \Gamma \cap T$ and $\mathfrak{Z}_i = X - \gamma$. As the $\mathrm{Fix}(\sigma)$-rational points are dense in $\mathfrak{Z}_i$, we see that $\mathfrak{Z}_i$ is defined over $\mathrm{Fix}(\sigma)$.

https://doi.org/10.1112/S0010437X05001879 Published online by Cambridge University Press

As X has a trivial stabilizer and is itself defined over $\mathrm{Fix}(\sigma)$, it follows that if $X - \gamma$ is also defined over $\mathrm{Fix}(\sigma)$, then $\gamma \in F$.

So, we have shown that for any good pair (σ, P),

$$X(\mathbb{U}) \cap \Gamma = (\mathrm{Ueno}(X)(\mathbb{U}) \cap \Gamma) \cup (X(\mathbb{U}) \cap \Gamma \cap F).$$

As observed above, if $\gamma \in \Gamma \smallsetminus S(L^{\mathrm{per}})$, then we can find a good pair (ρ, Q) with $\rho(\gamma) \neq \gamma$. If, in addition, $\gamma \notin \mathrm{Ueno}(X)(\mathbb{U})$, then from the above equation we see that $\gamma \notin X(\mathbb{U})$. Hence, $X(\mathbb{U}) \cap \Gamma = (\mathrm{Ueno}(X)(\mathbb{U}) \cap \Gamma) \cup (X(L^{\mathrm{per}}) \cap \Gamma)$ whose Zariski closure is a finite union of special varieties, by induction in the case of $\mathrm{Ueno}(X)$ and by the hypothesis that Conjecture 4.2 holds in the latter case. □

Conjecture 4.2 remains open, but there are some nontrivial cases in which it is known. Ghioca has shown that if E is a nonisotrivial elliptic curve over a finitely generated field k of characteristic $p > 0$, then there is a natural number n such that $E(K^{\mathrm{per}}) = E(K^{p^{-n}})$ (see [Ghi05]). Consequently, if A is a product of non-isotrivial elliptic curves over the finitely generated field K and $\Gamma \leqslant A(K^{\mathrm{per}})$ is a finite rank 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) elliptic curves. Such a reduction cannot be achieved in every case. For instance, there are nonweakly isotrivial abelian varieties A of p-rank zero. If A is defined over K and $A(K)$ is infinite, then the group $A(K^{\mathrm{per}})$ cannot be finitely generated. However, the reduction might succeed for sufficiently general ordinary abelian varieties.

Acknowledgements

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 posted on the arXiv preprint server will note that there were numerous inaccuracies in that note. I thank F. Oort for pointing out some of these, one anonymous referee for catching other errors and suggesting improvements, especially the correct argument for the equality $\Gamma = (\Gamma \cap F) + (\Gamma \cap T)$ in the proof of Theorem 4.3, and another anonymous referee for suggesting numerous improvements and especially for suggesting a way to bridge the divide between logicians and geometers.

References

AV92 D. Abramovich and J. F. Voloch, *Toward a proof of the Mordell–Lang conjecture in characteristic p*, Internat. Math. Res. Notices **5** (1992), 103–115.

Cha97 Z. Chatzidakis, *Groups definable in ACFA*, in *Algebraic model theory*, eds B. Hart, A. Lachlan and M. Valeriote, NATO ASI Series C: Mathematical and Physical Sciences, vol. 496 (Kluwer Academic, Dordrecht, 1997), 25–52.

CH99 Z. Chatzidakis and E. Hrushovski, *Model theory of difference fields*, Trans. Amer. Math. Soc. **351** (1999), 2997–3071.

CHP02 Z. Chatzidakis, E. Hrushovski and Y. Peterzil, *Model theory of difference fields. II. Periodic ideals and the trichotomy in all characteristics*, Proc. London Math. Soc. (3) **85** (2002), 257–311.

Ghi05 D. Ghioca, *Elliptic curves over the perfect closure of a function field*, PhD thesis, UC Berkeley, 2005.

Hru96 E. Hrushovski, *The Mordell–Lang conjecture for function fields*, J. Amer. Math. Soc. **9** (1996), 667–690.

Hru01 E. Hrushovski, *The Manin–Mumford conjecture and the model theory of difference fields*, Ann. Pure Appl. Logic **112** (2001), 43–115.

Hru98 E. Hrushovski, *Proof of Manin's theorem by reduction to positive characteristic*, in *Model theory and algebraic geometry: an introduction to E. Hrushovski's proof of the geometric Mordell–Lang conjecture*, ed. E. Bouscaren, Lecture Notes in Mathematics, vol. 1696 (Springer, Berlin 1998), 197–205.

Pil04 A. Pillay, *Mordell–Lang conjecture for function fields in characteristic zero, revisited*, Compositio Math. **140** (2004), 64–68.

Pil03a A. Pillay, *Lectures 1 and 2 of 'Model theory and differential geometry'*, Arizona Winter School, 2003, http://swc.math.arizona.edu/∼swcenter/notes/files/03PillayNotes1.pdf.

Pil03b A. Pillay, *On the Manin–Mumford conjecture*, Preprint (2003).

PR04 R. Pink and D. Roessler, *On ψ-invariant subvarieties of semiabelian varieties and the Manin–Mumford conjecture*, J. Algebraic Geom. **13** (2004), 771–798.

Ray83 M. Raynaud, *Sous-variétés d'une variété abélienne et points de torsion*, in *Arithmetic and Geometry*, vol. I, Progress in Mathematics, vol. 35 (Birkhäuser, Boston, MA, 1983), 327–352.

Sca01 T. Scanlon, *Diophantine geometry from model theory*, Bull. Symbolic Logic **7** (2001), 37–57.

Wag04 F. Wagner, *Some remarks on one-basedness*, J. Symbolic Logic **69** (2004), 34–38.

Thomas Scanlon scanlon@math.berkeley.edu
Department of Mathematics, University of California, Berkeley, Evans Hall, Berkeley, CA 94720-3840, USA

https://doi.org/10.1112/S0010437X05001879 Published online by Cambridge University Press