DIOPHANTINE GEOMETRY OF THE TORSION OF A DRINFELD MODULE

THOMAS SCANLON

Abstract. We prove an analogue of the Manin-Mumford conjecture for Drinfeld modules of generic characteristic.

1. Introduction

L. Denis proposed that the qualitative diophantine results known for certain subgroups of semi-abelian varieties should hold for Drinfeld modules. In particular, the Manin-Mumford conjecture which asserts that an irreducible subvariety of a semi-abelian variety containing a Zariski dense set of torsion points must itself be a translate of a sub algebraic group should be true with "semi-abelian variety" replaced by "power of the additive group considered as an $\mathbb{F}_p[t]$-module via a Drinfeld module." In [4], Denis permits finite extensions of $\mathbb{F}_p[t]$ but insists that the Drinfeld module have generic characteristic. The strengthening permits one to consider general Drinfeld modules while the restriction is necessary since every point of $\mathbb{G}_a(\mathbb{F}_p^{\mathrm{alg}})$ is a torsion point for every Drinfeld module of finite characteristic. The analogue of Boxall's theorem [1] may still be true for Drinfeld modules of finite characteristic for I-power torsion for some ideal I, but it is shown in [8] that the methods of this paper cannot apply to this case.

I thank J. F. Voloch for bringing this question to my attention, Z. Chatzidakis for explaining [3] to me and for comments on an earlier version of this paper, E. Hrushovski for comments on an earlier version, B. Poonen for discussions about Drinfeld modules, and MSRI for its hospitality during some of the research on this paper.

2. Set Up

In this section we establish the notation to be used throughout the rest of this paper and state the version of Denis' conjecture to be proven. The basic reference for this section is [6]. We follow the notation of [6] with the notable exception that we denote the number of elements in the constant field by q, a power of p, rather than r.

Denote by p a fixed prime number and by q a fixed power of p. Fix a smooth absolutely irreducible projective curve C over $\mathbb{F}_q$ and a closed point ∞. The ring $\mathbf{A}$ is $H^0(C \setminus \{\infty\}, \mathcal{O}_C)$, the ring of regular functions on $C \setminus \{\infty\}$ with field of fractions $\mathbf{k} := \mathbb{F}_q(C)$. As usual, $\mathbb{G}_a$ denotes the additive group scheme $\mathrm{Spec}\mathbb{Z}[\mathrm{X}]$ with comultiplication defined by $X \mapsto X \otimes 1 + 1 \otimes X$. For T any scheme $\mathrm{End}_{\mathrm{T}}\mathbb{G}_{\mathrm{a}}$

Date: 10 February 2000.

Partially supported by an NSF Post-Doctoral Fellowship. Some of the research for this paper took place while the author was a member of MSRI.

denotes the ring of endomorphisms of $\mathbb{G}_{a_{/T}}$ defined over T. In all the cases we consider T is the spectrum of an $\mathbb{F}_p$-algebra, R. In this case, the map $\tau : \mathbb{G}_a \to \mathbb{G}_a$ defined on points by $x \mapsto x^p$ belongs to $\mathrm{End}_{\mathrm{T}}(\mathbb{G}_{\mathrm{a}})$ and $\mathrm{End}_{\mathrm{T}}(\mathbb{G}_{\mathrm{a}})$ may be identified with the ring of twisted polynomials in τ over R, $R\{\tau\} := \{\sum_{i=0}^{N} a_i \tau^i : N \in \mathbf{N}, a_i \in R\}$ with the commutation rule $\tau a = a^p \tau$. We will drop the subscript from $\mathbb{G}_{a_{/T}}$ when the base is understood.

An $\mathbf{A}$ field is an $\mathbb{F}_q$ morphism $\iota : \mathbf{A} \to K$ from $\mathbf{A}$ to a field K. A *Drinfeld module* (over ι) is an $\mathbb{F}_q$-algebra homomorphism $\varphi : \mathbf{A} \to \mathrm{End}_{\mathrm{K}}\mathbb{G}_{\mathrm{a}}$ such that φ and ι (or really the composition of ι with the inclusion $\chi : K \hookrightarrow \mathrm{End}_{\mathrm{K}}\mathbb{G}_{\mathrm{a}}$ via $a \mapsto a\tau^0$) have the same differential and $\varphi(A)$ is not contained in $\chi(K)$. Concretely, for any $a \in \mathbf{A}$ if $\varphi(a) = \sum_{i=0}^{m} a_i \tau^i$, then $a_0 = \iota(a)$ but $\varphi(a) \neq \chi \circ \iota(a)$ for some $a \in \mathbf{A}$. We denote $\varphi(a)$ by φ_a. The *characteristic* of φ is the ideal $\ker \iota$. We say that φ has *generic characteristic* if its characteristic is (0). The endomorphism ring of φ over K is $\mathrm{End}_{\mathrm{K}}(\varphi) := \{\psi \in \mathrm{End}_{\mathrm{K}}\mathbb{G}_{\mathrm{a}} : (\forall \mathrm{a} \in \mathbf{A})\ \psi \circ \varphi_{\mathrm{a}} = \varphi_{\mathrm{a}} \circ \psi\}$ considered as a subring of $\mathrm{End}_{\mathrm{K}}\mathbb{G}_{\mathrm{a}}$. We note, and shall use, that $\mathrm{End}_{\mathrm{K}}(\varphi)$ is commutative whenever φ has generic characteristic (Proposition 4.7.6 of [6]). Moreover, there is a finite extension K' of K such that $\mathrm{End}_{\mathrm{K}'}(\varphi)$ is a finite rank $\mathbf{A}$-module and $\mathrm{End}_{\mathrm{L}}(\varphi) = \mathrm{End}_{\mathrm{K}'}(\varphi)$ for any field extension L/K' (Section 4.7 of [6]).

If $\varphi : \mathbf{A} \to K$ is a Drinfeld module, then for any positive integer N we can regard K^N as an $\mathbf{A}$-module via φ. Define the φ-torsion group of K^N to be $\varphi_{\mathrm{tor}}(K^N) := \{x \in K^N : (\exists a \in \mathbf{A}) a \neq 0 \text{ and } \varphi_{\mathrm{a}}(\mathrm{x}) = 0\}$. When K is understood, we may write φ_{tor}^N for $\varphi_{\mathrm{tor}}(K^N)$. For $a \in \mathbf{A} \setminus \{0\}$ we define the a-torsion of φ to be the subgroup scheme of $\mathbb{G}_a$ defined by $\varphi[a] := \ker \varphi_a$.

We call an algebraic subgroup $G \leq {\mathbb{G}_a}^g$ of a power of the additive group an algebraic $\mathbf{A}$-module if it is stable under the action of $\mathbf{A}$ on ${\mathbb{G}_a}^g$ via φ. An algebraic $\mathbf{A}$-module is nothing more nor less than a sub T-module of a power of φ.

We can now state our main theorem.

Theorem 1. *With the notation as above if $\varphi : \mathbf{A} \to \mathrm{End}_{\mathrm{K}}\mathbb{G}_{\mathrm{a}}$ is a Drinfeld of generic characteristic, $X \subseteq {\mathbb{G}_a}^N_K$ is an irreducible subvariety, and $X(K) \cap \varphi_{\mathrm{tor}}(K^N)$ is Zariski dense in X, then X is a translate of an algebraic $\mathbf{A}$-module.*

3. Background from the model theory difference fields

Theorem 1 is an analogue of the Manin-Mumford conjecture and our proof follows the lines of Hrushovski's proof of that theorem [5]. The main ingredient of Hrushovski's proof was the model theory of difference fields of characteristic zero. We use the model theory of positive characteristic difference fields. The main sources for this material are [2] and [3].

A difference field is a a field K given together with a field endomorphism $\sigma : K \to K$. If σ is an automorphism, then we say that (K, σ) is an inversive difference field. A difference closed field, or a model of ACFA, is a model complete difference field. Loosely speaking, a difference closed field is a difference field in which every consistent finite system of difference equations has a solution. The precise axioms are given in [2]. The theory of difference closed fields is supersimple in the sense of stability so that the ordinal valued foundation rank of forking, Lascar or SU-rank, is defined on all complete types and by extension to all definable sets. We use SU-rank mainly for groups of finite rank. We recall that if $H \leq G$ are definable groups with $\mathrm{SU}(G) < \omega$, then we have $\mathrm{SU}(H) + \mathrm{SU}(G/H) = \mathrm{SU}(G)$. In particular, if $\mathrm{SU}(H) = \mathrm{SU}(G)$, then H is of finite index in G.

If (K, σ) is a difference field and $L \subseteq K$ is a subfield closed under σ and σ^{-1}, then for $x \in K$, the σ-degree of x over L, $\deg_\sigma(x/L)$, is $\mathrm{tr.deg}(L(\{\sigma^n(x)\}_{n\in\omega})/L)$. We note that $\mathrm{SU}(x/L) \leq \deg_\sigma(x/L)$.

For $A \subseteq K$, K a difference closed field, $\mathrm{acl}(A)$, the model theoretic algebraic closure of A is by definition the set of $x \in K$ satisfying some formula over A which has only finitely many solution in K. Concretely, $\mathrm{acl}(A)$ is the field theoretic algebraic closure of the inversive difference field generated by A.

Following [3] a group G quantifier-free definable in a difference closed field is called *modular* if every quantifier-free definable subset of any power of G is a finite Boolean combination of cosets of definable subgroups. This use of the word "modular" conflicts with earlier model theoretic uses of the word.

4. Proof of the main theorem

Our proof of Theorem 1 proceeds in several steps. First, we recall some of the theory of reductions of Drinfeld modules and use this to find difference equations for a large submodule of the torsion. Secondly, we analyze these equations in light of the dichotomy theorem of [3] to see that they define modular groups so that the conclusion of Theorem 1 under the stronger hypothesis that $X(K)$ contains a Zariski dense set of points from the submodule found in the first step follows from the general theory of quantifier-free modularity. Finally, we show how to work with two primes of $\mathbf{A}$ to cover all the torsion points.

Since $\mathbf{A}$, and, in fact, $\mathrm{End}_{K^{\mathrm{alg}}}(\varphi)$, is a finitely generated $\mathbb{F}_p$-algebra, we may find a finitely generated subalgebra $B \subseteq K^{\mathrm{alg}}$ such that the image of $\varphi : \mathbf{A} \to \mathrm{End}_K\mathbb{G}_a$ is contained in $\mathrm{End}_B\mathbb{G}_a$ and every endomorphism of φ is defined over B. Let L be the field of fractions of B. For $\mathfrak{p} \in \mathrm{Spec(B)}$ we obtain another ring homomorphism $\varphi^{\mathfrak{p}} : \mathbf{A} \to \mathrm{End}_{k(\mathfrak{p})}\mathbb{G}_a$ over $\iota^{\mathfrak{p}}$ by composing φ with the reduction map $\pi^{\mathfrak{p}} : B \to k(\mathfrak{p})$ where $k(\mathfrak{p})$ is the quotient field of $B/\mathfrak{p}$ and $\iota^{\mathfrak{p}} := \pi^{\mathfrak{p}} \circ \iota$. We say that φ has *good reduction* at $\mathfrak{p}$ if φ_a and $\varphi^{\mathfrak{p}}_a$ have the same degree for each $a \in \mathbf{A}$. The scheme Spec(B) contains an open set of primes at which φ has good reduction (Lemma 4.13.11 of [6]).

For $\mathfrak{p} \in \mathrm{Spec(B)}$ a smooth closed point let

- $\widehat{L^{\mathrm{unr}}_{\mathfrak{p}}}$ be the completion of the maximal unramified extension of the completion of L at p,
- $q_{\mathfrak{p}} := p^n = \#k(\mathfrak{p})$ (written "q" when $\mathfrak{p}$ is clear from the context) and
- $\sigma_p : \widehat{L^{\mathrm{unr}}_{\mathfrak{p}}} \to \widehat{L^{\mathrm{unr}}_{\mathfrak{p}}}$ be a relative Frobenius lifting τ^n to a continuous automorphism of $\widehat{L^{\mathrm{unr}}_{\mathfrak{p}}}$.

When $\mathfrak{p}$ is also a point of good reduction for φ, then τ^n is integral over $\mathbf{A}$ in $\mathrm{End}_{k(\mathfrak{p})}(\varphi^{\mathfrak{p}})$. Let $P_{\mathfrak{p}}(t) \in \mathrm{End_L}(\varphi)[\mathrm{t}]$ be the minimal monic polynomial for τ^n. We define $P^{(m)}_{\mathfrak{p}}(t) \in \mathrm{End_L}(\varphi)[\mathrm{t}]$ to be the minimal monic polynomial for τ^{mn}.

Until noted otherwise, we fix $\mathfrak{p} \in \mathrm{Spec(B)}$ a smooth closed point of good reduction for φ and an extension $(\mathcal{K}, \sigma)$ of $(\widehat{L^{\mathrm{unr}}_{\mathfrak{p}}}, \sigma_{\mathfrak{p}})$ to an $\aleph_1$-saturated difference closed field. We denote by $\mathcal{L}$ the language of inversive difference rings $\mathcal{L}(+, \cdot, -, \sigma, \sigma^{-1}, 0, 1)$ while for $m \in \mathbb{Z}_+$, $\mathcal{L}[m]$ refers to the sublanguage of $\mathcal{L}$ in which every instance of σ occurs as σ^{mn} for some $n \in \mathbb{Z}$.

Lemma 2. *The* $\mathbf{A}$*-module* $\ker P_{\mathfrak{p}}(\sigma)(\mathcal{K}) := \{x \in \mathcal{K} : P_{\mathfrak{p}}(\sigma)(x) = 0\}$ *contains* $\varphi[a](K)$ *for each* $a \in \mathbf{A} \setminus \mathfrak{p}$.

Proof: Let $a \in \mathbf{A} \setminus \mathfrak{p}$ be given. Since $a \notin \mathfrak{p}$, $\iota^{\mathfrak{p}}(a) \neq 0$. Thus, $\varphi_a^{\mathfrak{p}}$ is a separable polynomial. Since φ has good reduction at $\mathfrak{p}$, $\deg \varphi_a^{\mathfrak{p}} = \deg \varphi_a$. Therefore, $\varphi[a]$ is an étale group scheme over Spec(B). In particular,

- $\varphi[a](B_{\mathfrak{p}}^{sh}) = \varphi[a](\widehat{L_{\mathfrak{p}}^{\mathrm{unr}}}) = \varphi[a](K)$ where $B_{\mathfrak{p}}^{sh}$ is the strict henselization of B localized at $\mathfrak{p}$ and
- the intersection of $\varphi[a](B_{\mathfrak{p}}^{sh})$ with the kernel of reduction $\pi^{\mathfrak{p}} : \mathbb{G}_a(B_{\mathfrak{p}}^{sh}) \to \mathbb{G}_a(k(\mathfrak{p})^{\mathrm{alg}})$ is trivial.

The first remark means that it suffices to show that $\ker P_{\mathfrak{p}}(B_{\mathfrak{p}}^{sh}, \sigma_{\mathfrak{p}})$ contains $\varphi[a](B_{\mathfrak{p}}^{sh})$. Since $\sigma_{\mathfrak{p}}$ fixes B, the operator $P_{\mathfrak{p}}(\sigma_{\mathfrak{p}})$ maps $\varphi[a](B_{\mathfrak{p}}^{sh})$ back to itself. Since the operator $P_{\mathfrak{p}}(\sigma_{\mathfrak{p}})$ reduces to the zero operator on $\mathbb{G}_a(k(\mathfrak{p})^{\mathrm{alg}})$, it must map all of $\mathbb{G}_a(B_{\mathfrak{p}}^{sh})$ to the kernel of reduction. By the second remark above, this means that it annihilates $\varphi[a](B_{\mathfrak{p}}^{sh})$. ♠

The next few lemmata show that the $\mathbf{A}$-module $\ker P_{\mathfrak{p}}(\sigma)(\mathcal{K})$ is modular.

Lemma 3. *Any $\mathcal{L}[m]$-definable $\mathbf{A}$-submodule of $\ker P_{\mathfrak{p}}^{(m)}(\sigma^m)(\mathcal{K})$ is commensurable with an $\mathbf{A}$-module of the form $\ker R(\sigma^m)(\mathcal{K})$ for some $R(X) \in \mathrm{End}_{\mathcal{K}}(\varphi)[\mathrm{X}]$ dividing $P_{\mathfrak{p}}^{(m)}(X)$ in $(\mathrm{End}_{\mathcal{K}}(\varphi) \otimes_{\mathbf{A}} \mathbf{k})[\mathrm{X}]$.*

Proof: Let $M \leq \ker P_{\mathfrak{p}}^{(m)}(\sigma^m)(\mathcal{K}))$ be an $\mathcal{L}[m]$-definable $\mathbf{A}$-submodule over the small inverssive difference field $\mathcal{M} \subset \mathcal{K}$. Let $n = \max\{\deg_{\sigma^m}(a/\mathcal{M}) : a \in M\}$. Let $W \leq {\mathbb{G}_a}^{n+1}$ be the zero component of algebraic locus of $\{(a, \sigma^m(a), \sigma^{2m}(a), \ldots, \sigma^{nm}(a)) : a \in M\}$. Since M is an $\mathbf{A}$-module, W is an algebraic $\mathbf{A}$-module. Moreover, by the definition of n, W is of dimension n and is thus a hypersurface defined by some $Q(x_0, x_1, \ldots, x_n) = \sum_{i=0}^n q_i(x_i) = 0$ where each $q_i \in \mathrm{End}_{\mathcal{M}}(\mathbb{G}_{\mathrm{a}})$ and at least one of the q_i's is separable. Let $Q(\sigma^m) := \sum_{i=0}^n q_i \sigma^{mi} \in \mathrm{End}_{\mathcal{K}}(\mathbb{G}_{\mathrm{a}})[\sigma^{\mathrm{m}}]$. Let $M' := \{a \in \mathbb{G}_a(\mathcal{K}) : P_{\mathfrak{p}}^{(m)}(\sigma^m)(a) = 0 \text{ and } \mathrm{Q}(\sigma^{\mathrm{m}})(\mathrm{x}) = 0\}$. M' is commensurable with M. We aim to show that Q is actually in $\mathrm{End}_{\mathcal{K}}(\varphi)[\sigma^{\mathrm{m}}]$. It then follows that M' is of finite index in $\ker Q(\sigma^m)$.

Let $t \in \mathbf{A}$ such that $\mathbf{A}$ is a finite integral extension of $\mathbb{F}_p[t]$. Let $\varphi|_{\mathbb{F}_p[t]} : \mathbb{F}_p[t] \to \mathrm{End}_{\mathrm{K}}\mathbb{G}_{\mathrm{a}}$ denote the restriction of φ to $\mathbb{F}_q[t]$. Note that $\mathrm{End}_{\mathcal{K}}(\varphi) = \mathrm{End}_{\mathcal{K}}(\varphi|_{\mathbb{F}_{\mathrm{p}}[\mathrm{t}]})$ as each such ring is commutative.

Because W is an $\mathbf{A}$-module, $\varphi_t(W) \subseteq W$ (image taken as an algebraic group, or if you like, on the $\mathcal{K}$-points). Since φ_t is a finite map, $\dim W = \dim \varphi_t(W)$. As W is connected, this implies $\varphi_t(W) = W$. So, $\varphi_t^* W = W + \varphi[t]^{n+1}$. This means that the ideals $(Q(\varphi_t(x_0), \varphi_t(x_1), \ldots, \varphi_t(x_n))$ and $(\prod_{\alpha \in Q(\varphi[t]^{n+1}(\mathcal{K}))}(Q(x_0, \ldots, x_n) - \alpha))$ are equal. We may rewrite the product defining the second ideal as $\psi_t \circ Q$ where $\psi_t \in \mathrm{End}_{\mathcal{K}}(\mathbb{G}_{\mathrm{a}})$ with $\ker \psi_t = Q(\varphi[t](\mathcal{K})^{n+1})$.

Specializing all the x_j's to be zero except for x_i, we see that $q_i \circ \varphi_t = \psi_t \circ q_i$. Taking i so that q_i is separable, we see that $\varphi_t = \psi \pmod{\tau}$ and that $\deg \varphi_t = \deg \psi_t$. Hence, ψ_t also defines a Drinfeld module ψ over $\iota|_{\mathbb{F}_p[t]}$ by sending t to ψ_t. Moreover, the equation $q_i \circ \varphi_t = \psi_t \circ q_i$ implies that $q_i \circ \varphi = \psi \circ q_i$ so that q_i is an isogeny from φ to ψ. Let h be any isogeny from ψ to φ. (h exists by Proposition 4.7.13 of [6].) Then for any j we have the equality $(h \circ q_j) \circ \varphi_t = h \circ (q_j \circ \varphi_t) = h \circ (\psi_t \circ q_j) = (h \circ \psi_t) \circ q_j = (\varphi_t \circ h) \circ q_j = \varphi_t \circ (h \circ q_j)$. Therefore, $r_j := h \circ q_j \in \mathrm{End}_{\mathcal{K}}(\varphi)$. Set $R(X) := \sum_{i=0}^n r_j X^j$. Then $\ker R(\sigma^m)(\mathcal{K})$ is commensurable with M' and hence with M.

Since $\ker R(\sigma^m)$ is commensurable with a subgroup of $\ker P_{\mathfrak{p}}(\sigma^m)(\mathcal{K})$ and $(\mathrm{End}_{\mathcal{K}}(\varphi)\otimes_{\mathbf{A}} \mathbf{k})[X]$ is a PID, R divides $P_{\mathfrak{p}}(\sigma^m)$ in this ring. ♠

Lemma 4. *There are no infinite $\mathcal{L}[m]$-definable $\mathbf{A}$-submodules of $\ker P_{\mathfrak{p}}^{(m)}(\sigma^m)(\mathcal{K})$ of infinite index.*

Proof: $P_{\mathfrak{p}}^{(m)}(X)$ is irreducible in $\mathrm{End}_{\mathcal{K}}(\varphi)[X]$ by its very definition. By Gauß' lemma, it remains irreducible in $(\mathrm{End}_{\mathcal{K}} \otimes_{\mathbf{A}} \mathbf{k})[X]$. ♠

Lemma 5. $\ker P_{\mathfrak{p}}^{(m)}(\sigma^m)(\mathcal{K})$ *is almost minimal in $(\mathcal{K}, \sigma^m)$ in the sense that there is an SU-rank 1 $\mathcal{L}[m]$-definable set X and a finite set F such that* $\ker P_{\mathfrak{p}}^{(m)}(\sigma^m)(\mathcal{K}) \subset \mathrm{acl}_{\sigma^m}(X, F)$.

Proof: Let $X \subseteq \ker P_{\mathfrak{p}}^{(m)}(\sigma^m)(\mathcal{K})$ be any definable subset of SU-rank one which contains the origin. Let N be any definable subgroup of $\ker P_{\mathfrak{p}}^{(m)}(\sigma^m)(\mathcal{K})$ which is commensurable with the group generated by X. As $\ker P_{\mathfrak{p}}^{(m)}(\sigma^m)(\mathcal{K})$ has finite rank, such a group exists. Let $G \leq N$ be an infinite $\mathcal{L}[m]$-definable group defined over a small inversive difference field B of minimal SU-rank. Let $n = \max\{\deg_{\sigma^m}(a/B) : a \in G\}$. Let W be the connected component of the algebraic locus of $\{(a, \sigma^m(a), \ldots, \sigma^{nm}(a)) : a \in G\}$. Then the group $H := \{a \in \mathbb{G}_a(\mathcal{K}) : (a, \sigma^n(a), \ldots, \sigma^{nm}(a)) \in W\}$ is of finite index in G and hence also minimal. Let $V = \sum_{a\in\mathbf{A}} \varphi_a W$ where φ_a acts diagonally and the image is taken as an algebraic group. Since W is connected, each $\varphi_a W$ is connected. V may be realized as the direct limit of the image of $\bigoplus_{a\in\mathbf{A}, v_\infty(a)\leq m} \varphi_a W$ in ${\mathbb{G}_a}^{n+1}$ under the sum morphism. As the dimensions cannot increase indefinitely, eventually they must stabilize. As each of these groups is connected, the direct limit reduces to a finite sum so that V is an algebraic group. Let $M = \{a \in \mathbb{G}_a(\mathcal{K}) : P_{\mathfrak{p}}^{(m)}(\sigma^m)(a) = 0 \text{ and } (\mathrm{a}, \sigma^{\mathrm{m}}(\mathrm{a}), \ldots, \sigma^{\mathrm{mn}}(\mathrm{a})) \in \mathrm{V}\}$. Since V is an $\mathbf{A}$-module, so is M. Observe that M is commensurable with a finite sum of groups of the form $\varphi_a H$ for some $a \in \mathbf{A}$. Since M is infinite, by the above corollary, it is commensurable with $\ker P_{\mathfrak{p}}^{(m)}(\sigma^m)(\mathcal{K})$. Hence, $\ker P_{\mathfrak{p}}^{(m)}(\sigma^m)(\mathcal{K})$ is contained in the σ^m-algebraic closure of X together with the co-efficients of finitely many elements of $\varphi(\mathbf{A})$ and a finite set of coset representative of M in $\ker P_{\mathfrak{p}}^{(m)}(\sigma^m)(\mathcal{K})$. ♠

Proposition 6. $\ker P_{\mathfrak{p}}(\sigma)(\mathcal{K})$ *is modular.*

Proof: By the main theorem of [3], if this proposition were false, then $\ker P_{\mathfrak{p}}(\sigma)$ would be non-orthogonal to some fixed field k of the form $\{x : \sigma^m(x) = \tau^n(x)\}$ for appropriate integers m and n. This implies that $\ker P_{\mathfrak{p}}^{(m)}(\sigma^m)(\mathcal{K})$ is non-orthogonal to k in $\mathcal{L}[m]$. Since $\ker P_{\mathfrak{p}}^{(m)}(\sigma^m)(\mathcal{K})$ is almost minimal in $\mathcal{L}[m]$, this would imply that $\ker P_{\mathfrak{p}}(\sigma)(\mathcal{K})$ contains a minimal group non-orthogonal to k in $\mathcal{L}[m]$. This minimal group is definably isogenous to the group of k-points of a k-algebraic group. Since k is perfect and $\ker P_{\mathfrak{p}}(\sigma)(\mathcal{K})$ has exponent p, it follows that there are $\psi, \theta \in \mathrm{End}_{\mathcal{K}}\mathbb{G}_{\mathrm{a}}$ such that the intersection $\psi(\mathbb{G}_a(k)) \cap \theta(\ker P_{\mathfrak{p}}^{(m)}(\sigma^m)(\mathcal{K}))$ is infinite. Since k is perfect, we may arrange that ψ is separable. Likewise, since only $\ker \theta(\mathcal{K})$ matters, we may arrange that θ is separable.

Let R be the quotient skew-field of $\mathrm{End}_{\mathcal{K}}\mathbb{G}_{\mathrm{a}}$. Every element of R may be regarded as a multi-valued homomorphism from $\mathbb{G}_a$ to itself. As such, every non-zero element of R has finite kernel. So, the above intersection being infinite means that if we write $P_{\mathfrak{p}}^{(m)}(X) = \sum_{i=0}^{N} p_i X^i$ with $N = \deg P_{\mathfrak{p}}^{(m)}(X)$, then $\Xi := \sum_{i=0}^{N} p_i(\theta^{-1}\psi)^{\sigma^{mi}}\tau^{ni}$ is zero in R.

We see that this cannot be by working in three different cases.

Case 1 $n < 0$**:** Let v_τ be the valuation on R induced by $v_\tau(\tau) = 1$. Since each nonzero p_i is separable, θ is separable, and ψ is separable, for each i either $v_\tau(p_i(\theta^{-1}\psi)^{\sigma^{mi}}) = 0$ or $p_i = 0$. As $P_{\mathfrak{p}}^{(m)}(X)$ is monic, $p_N = 1 \neq 0$. Hence, the term $p_N(\theta^{-1}\psi)^{\sigma^{mN}}\tau^{nN}$ has valuation nN which is strictly less than the valuations of all the other terms. That is, $\Xi \neq 0$.

Case 2 $n = 0$**:** This time we work with a different valuation on R, namely with respect to the valuation $v_\infty(\gamma) = -\deg_\tau \gamma$. By a theorem of Gekeler (Theorem 4.12.8 of [6]), if M is a splitting field of $P_{\mathfrak{p}}^{(m)}(X)$ over $\mathrm{End}_{\mathcal{K}}(\varphi) \otimes_{\mathbf{A}} \mathbf{k}$ and w is an extension of v_∞ to M, then all roots to $P_{\mathfrak{p}}^{(m)}$ have the same non-zero w-valuation. This means, in particular, that $v_\infty(p_0) < v_\infty(p_i)$ for $i > 0$ and $p_i \neq 0$. Thus, if $p_i \neq 0$ and $i > 0$, then $v_\infty(p_i(\theta^{-1}\psi)^{\sigma^{mi}}) = v_\infty(p_i) + v_\infty(\psi) - v_\infty(\theta) > v_\infty(p_0) + v_\infty(\psi) - v_\infty(\theta) = v_\infty(p_0\theta^{-1}\psi)$. Thus, $v_\infty(\Xi) = v_\infty(p_0) + v_\infty(\psi) - v_\infty(\theta) \neq \infty$. In particular, $\Xi \neq 0$.

Case 3 $n > 0$**:** We return to the calculation of **Case 1**. $v_\tau(p_0\theta^{-1}\psi) = 0$ while every other term is either zero or has $v_\tau(p_i(\theta^{-1}\psi)^{\sigma^{mi}}\tau^{ni}) = ni > 0$. Therefore, $\Xi \neq 0$.

♠

Proposition 7. *If $X \subseteq {\mathbb{G}_a}^n$ is an irreducible variety containing a Zariski dense set of $\mathbf{A}$-torsion points which are unramified at $\mathfrak{p}$, then X is a coset of an algebraic group.*

Proof: Since $\Gamma := \ker P_{\mathfrak{p}}(\sigma)(\mathcal{K})^n$ contains all the $\mathfrak{p}$-unramified torsion, $X(\mathcal{K})$ meets Γ in a Zariski dense set. Since Γ is modular Theorem A of [3] shows that every quantifier free definable subset is a finite Boolean combination of definable groups. Thus, $X(\mathcal{K}) \cap \Gamma$ is a finite Boolean combination of cosets definable subgroups of ${\mathbb{G}_a}^n$. As this set is Zariski dense in X, we see that generically in ACF, the function $(x, y, z) \mapsto x - y + z$ maps X^3 to X so that X is a coset of an algebraic group. ♠

The following lemmata complete the proof that the definable subgroups of $\ker P_{\mathfrak{p}}(\sigma)(\mathcal{K})$ are commensurable with $\mathbf{A}$-modules.

We follow the notation already established with the exception that by Γ we mean $\ker P_{\mathfrak{p}}(\sigma)(\mathcal{K})$. We let $n := \deg P_{\mathfrak{p}}$.

Proposition 8. *Let $m \in \mathbb{Z}_+$ be a positive integer. If $X \leq \Gamma^m$ is a definable subgroup, then X is commensurable with an $\mathbf{A}$-module.*

The proof of Proposition 8 proceeds by induction. The cases of $m = 1$, $m = 2$, and $m > 2$ require substantially different proofs. For the case of $m = 1$ we prove the stronger result that $\mathrm{SU}(\Gamma) = 1$. For the case of $m = 2$ we use an analytic argument. The case of $m > 2$, given the case $m = 2$, follows from a general result about finite rank definable groups in ACFA possessing a module structure.

Before setting out for the proof proper we begin with some lemmata about the arithmetic of the ring $K\{\tau\}[\sigma]$.

We denote by $\pi : K\{\tau\}[\sigma] \to K[\sigma]$ the reduction map induced by $\tau \mapsto 0$.

Lemma 9. *Let $A, B \in K\{\tau\}[\sigma]$ be separable (ie $\pi(A) \neq 0$ and $\pi(B) \neq 0$) with $\deg \pi(A) = \deg \pi(B)$. Let $j := \max\{s : (\exists \alpha \in K\{\tau\})\alpha A \equiv B \pmod{\tau^s}\}$. Let $\tilde{A}, \tilde{B} \in K\{\tau\}[\sigma]$ so that $\tilde{A}B = \tilde{B}A$. Then either $j = \infty$ or there is a nontrivial factor f of A for which $f^{(\tau^j)}$ is a factor of $\tilde{A}$.*

Proof: If $j = 0$, then from the equation $\pi(\tilde{A})\pi(B) = \pi(\tilde{B})\pi(A)$ and the fact that $\pi(B)$ is not a multiple of $\pi(A)$ one sees that $\pi(\tilde{A})$ must share a factor with $\pi(A)$.

So, we may assume that $j > 0$. Let $\alpha \in K\{\tau\}$ so that $\alpha A \equiv B \pmod{\tau^j}$. Observe that necessarily $\tilde{B} \equiv \tilde{A}\alpha \pmod{\tau^j}$. We write $B = \alpha A + C\tau^j$ and $\tilde{B} = \tilde{A}\alpha + \tilde{C}\tau^j$. The equation $\tilde{A}B = \tilde{B}A$ yields $\tilde{A}C\tau^j = \tilde{C}A^{\tau^j}\tau^j$. Canceling τ^j and applying π, we see that $\pi(\tilde{A})\pi(C) = \pi(\tilde{C})\pi(A)^{\tau^j}$. If $\pi(\tilde{A})$ and $\pi(A)^{\tau^j}$ are coprime, then there is some $\gamma \in K^\times$ for which $\pi(C) = \gamma\pi(A)^{\tau^j}$. Observe then that $B \equiv (\alpha + \gamma\tau^j)A \pmod{\tau^{j+1}}$ contradicting the maximality of j. ♠

Lemma 10. *If $Q = \sum_{j=0}^{\ell} q_j(x_j)$ with $q_j \in \mathcal{K}\{\tau\}$, $t \in \mathbf{A}$ is nonconstant, and for some nonzero $\alpha, \beta \in \mathcal{K}\{\tau\}$ we have $\alpha Q\varphi_t = \beta Q$, then the group $\{(x_0, \ldots, x_\ell) \in \mathcal{K}^{\ell+1} : Q(x) = 0\}$ is commensurable with an $\mathbf{A}$-module.*

Proof: Let $X \leq {\mathbb{G}_a}^{\ell+1}$ be the group defined by $Q(x) = 0$. Our hypothesis is that X and $\varphi_t^{-1}X$ are commensurable. By Denis' Lemme 4 of [4], this implies that X^0 is an $\mathbf{A}$-module. ♠

Proposition 11. $\mathrm{SU}(\Gamma) = 1$. *Thus, $X \leq \Gamma$ is a definable subgroup, then X is commensurable with an $\mathbf{A}$-module.*

Proof: As Γ is modular, it suffices to show that if $X \leq \Gamma$ is a subgroup of SU-rank one, then X is of finite index in Γ.

X is commensurable with a quantifier-free definable group, so we may assume that X itself has a quantifier-free definition of the form $\sum_{j=0}^{\ell} q_j \circ \sigma^j(x) = 0$ where $q_j \in \mathcal{K}\{\tau\}$ and $\ell \leq n$.

As Γ is modular, X is actually definable over $\mathrm{acl}(K) = K^{alg}$ which is contained in the union of the fixed fields of the powers of σ. Replacing σ with a power, we may assume that X is definable over the fixed field of σ on K^{alg}. To keep the notation simple, we take a finite extension and write K for a field of definition for X.

Let $t \in \mathbf{A}$ be nonconstant. By Denis' Lemme 4 of [4], if $X \cap \varphi_t^{-1}(X)$ is commensurable with X, then X is commensurable with an $\mathbf{A}$-module and is therefore commensurable with Γ by Lemma 4. Thus, we may assume that $X \cap \varphi_t^{-1}(X)$ is finite.

By additivity of SU-rank, we see that $\mathrm{SU}(X + \varphi_t^{-1}(X)) = 2$ so that $\deg_\sigma(X + \varphi_t^{-1}(X)) = 2\deg(X)$.

Let $\tilde{A}, \tilde{B} \in K^{per}\{\tau\}[\sigma]$ so that $\deg_\sigma(\tilde{A}) = \deg_\sigma(\tilde{B}) = \deg_\sigma(Q)$, $\tilde{A}$ and $\tilde{B}$ are separable, and $\ker \tilde{A} \circ Q \geq \ker(Q \circ \varphi_t)$ and $\ker \tilde{B} \circ Q \circ \varphi_t \geq \ker Q$. As the σ-degree of $X + \varphi_t^{-1}(X)$ is twice the σ-degree of X, the groups $\ker \tilde{A} \circ Q$ and $\ker \tilde{B} \circ Q \circ \varphi_t$ are commensurable with $X + \varphi_t^{-1}(X)$. Hence, there exist separable $\alpha, \beta \in K^{per}\{\tau\}$ such that $\alpha\tilde{A}Q = \beta\tilde{B}Q\varphi_t$. As $\pi(Q\varphi_t) = t\pi(Q)$, the greatest j for which we can find $\gamma \in K^{per}\{\tau\}$ with $\gamma Q \equiv Q\varphi_t \pmod{\tau^j}$ is at least one. However, by Lemma 10, j

is not equal to ∞. Hence, by Lemma 9, there is a nontrivial factor f of $\pi(Q)$ for which $f^{(\tau^j)}$ is a factor of $\tilde{B}$.

By Lemma 5, there is an integer $r \geq 2$ so that Γ is commensurable with $\sum_{s=0}^{r} \varphi_{t^s}(\varphi_t^{-1}(X))$. Let $C \in K^{per}\{\tau\}[\sigma]$ be separable and have minimal degree in σ so that $\ker C \circ \tilde{B} \circ Q \circ \varphi_t \geq \sum_{s=2}^{r} \varphi_{t^{s-1}}(X)$. Then, as $\ker(C\tilde{B}Q\varphi_t)$ and Γ are commensurable and the prolongation of Γ is irreducible, there is some separable $\delta \in K^{per}\{\tau\}$ such that $C\tilde{B}Q\varphi_t = \delta P_{\mathfrak{p}}$. Applying π, we see that f and $f^{(\tau^j)}$ are both factors of $\pi(P)$. Note that $\pi(P)$ is the polynomial P considered over $\mathbf{k}$ embedded in $\mathcal{K}$ via ι. By Gekeler's theorem , the roots of P all have the same non-zero ∞-valuation (or really, the unique extension of ∞ to the splitting field of P). If a is a root of f, then a^{p^j} is a root of $f^{(\tau^j)}$. Of course, if $v_\infty(a) \neq 0$, then $v_\infty(a^{p^j}) = p^j v_\infty(a) \neq v_\infty(a)$. With this contradiction we conclude that X and $\varphi_t^{-1}(X)$ are commensurable so that X is commensurable with an $\mathbf{A}$-module and hence with Γ itself. ♠

Lemma 12. *If $X \leq \Gamma$ is an infinite definable subgroup, then there is a nonzero element $a \in \mathbf{A}$ for which $\varphi_a(X) \geq \varphi_a(\Gamma_{\mathrm{tor}})$.*

Proof: As X is an infinite definable subgroup of Γ, the group Γ/X is finite by Proposition 11. Hence, the group $\Gamma_{\mathrm{tor}}/(\Gamma_{\mathrm{tor}} \cap X)$ is also finite. Let $a \in \mathbf{A} \setminus 0$ so that $\varphi[a](\mathcal{K}) \cap \Gamma$ contains a set of coset representatives for $X \cap \Gamma_{\mathrm{tor}}$ in Γ_{tor}. Then, $\varphi_a(\Gamma_{\mathrm{tor}}) = \varphi_a((\varphi[a](\mathcal{K}) \cap \Gamma_{\mathrm{tor}}) + (X \cap \Gamma_{\mathrm{tor}})) \leq \varphi_a(X)$. ♠

Lemma 13. *The groups Γ_{tor} and $\varphi_{\mathrm{tor}}(K_{\mathfrak{p}}^{unr})$ are commensurable.*

Proof: If this lemma were false, then Γ would contain infinitely many torsion points in the kernel of reduction at $\mathfrak{p}$. We show that this is not possible.

Let R the ring of $\mathfrak{p}$-integers in the completion of K^{alg}.

The exact sequence $0 \to \mathfrak{m}_R \to R \to k \to 0$ gives rise to an exact sequence of Galois modules $0 \to T_{\mathfrak{p}}(\varphi(\mathfrak{m}_R)) \to T_{\mathfrak{p}}(\varphi(R)) \to T_{\mathfrak{p}}(\varphi(k)) \to 0$. Let $Q(X) \in \mathrm{End}(\varphi)[X]$ be the characteristic polynomial of the reduction of σ on $T_{\mathfrak{p}}(\varphi(k))$ and let $S(X) \in \mathrm{End}(\varphi)[X]$ be the characteristic polynomial of σ on $T_{\mathfrak{p}}(\varphi(\mathfrak{m}_R))$. Of course, $Q(X)$ divides $P_{\mathfrak{p}}(X)$. Thus, if $\Gamma \cap \mathfrak{m}_R$ is infinite, then S and $\frac{P_{\mathfrak{p}}}{Q}$ must have a common factor. Note that any root of S is a unit in R (as it is an eigenvalue of an automorphism). We show now that no root of $\frac{P_{\mathfrak{p}}}{Q}$ is a $\mathfrak{p}$-unit.

As the endomorphism ring of φ is commutative, we may assume that $\mathbf{A}$ is equal to the endomorphism ring of φ, losing only the condition that $\mathbf{A}$ is normal. For what follows, this is not a serious problem.

Let h be the height of $\varphi_{\mathfrak{p}}$. Write $P_{\mathfrak{p}} = \sum p_j X^j$. Let ℓ be minimal so that $v_{\mathfrak{p}}(p_\ell) = 0$. Observe that if $\ell < h$, then $\sum \varphi_{\mathfrak{p}}(p_j)\tau_q^j \equiv \iota_{\mathfrak{p}}(p_\ell)\tau_q^\ell + \pmod{\tau_q^{\ell+1}}$ contradicting the fact that $\varphi^{\mathfrak{p}}(P_{\mathfrak{p}})$ vanishes on τ_q. Thus, $\ell \geq h$. Factor $P = \prod(X - \alpha_j)$ and observe that ℓ is equal to the number of roots α_j which are not $\mathfrak{p}$-units. Hence, P has at least h roots (counting multiplicity) which are not units at $\mathfrak{p}$. Note that the rank of $T_{\mathfrak{p}}(k)$ is equal to rank of φ (which is the degree of P) minus h so that no root of $\frac{P_{\mathfrak{p}}}{Q}$ is a $\mathfrak{p}$-unit. ♠

Lemma 14. $\mathrm{acl}(K) \cap \Gamma = \Gamma_{\mathrm{tor}}$

Proof: We have the inclusion $\ker P_{\mathfrak{p}}(\sigma)(\mathcal{K}) \cap \mathrm{Fix}(\sigma^m) \leq \ker P_{\mathfrak{p}}^{(m)}(\sigma^m)(\mathcal{K}) \cap \mathrm{Fix}(\sigma^m) \leq \varphi[P_{\mathfrak{p}}^{(m)}(1)](\mathcal{K}) \leq \Gamma_{\mathrm{tor}}$. As $\mathrm{acl}(K) = \bigcup_{m=0}^{\infty} \mathrm{Fix}(\sigma^m)$, we have $\mathrm{acl}(K) \cap \Gamma \leq \Gamma_{\mathrm{tor}}$. The reverse inclusion is clear. ♠

We deal now with the case of $m = 2$.

Proposition 15. *If $X \leq \Gamma^2$ is a definable subgroup, then X is commensurable with an $\mathbf{A}$-module.*

Proof: As X is commensurable with a quantifier-free group, we may suppose that X is already quantifier-free definable. In fact, we may assume that X is defined as a subgroup of Γ^2 by an equation of the form $Q(x) = R(y)$ where $R, Q \in \mathcal{K}\{\tau, \sigma\}$ have degree $\ell < n$ in σ and at least one of Q and R is separable. By swapping x and y if need be, we will assume that R is separable. As Γ is modular, we may actually take the defining equations to have coefficients algebraic over K and by replacing σ with a power and K with a finite extension we may take $R, Q \in K\{\tau\}[\sigma]$.

Let $\tilde{X} \leq ({\mathbb{G}_a}^2)^{\ell+1}$ be the prolongation of X.

We denote by $\pi_1 : \Gamma^2 \to \Gamma$ the projection onto the first factor and by $\pi_2 : \Gamma^2 \to \Gamma$ the projection onto the second factor. We abuse notation somewhat and continue to denote by π_1 and π_2 the restrictions of these maps to X.

If either $\pi_1(X)$ or $\pi_2(X)$ is finite, then the result follows from Proposition 11. If $\mathrm{SU}(X) > 1$, then as $\mathrm{SU}(\Gamma^2) = 2$ by Proposition 11 and Γ is modular, we conclude that X is commensurable with Γ^2 itself. Hence, we may assume that $\mathrm{SU}(X) = 1$ and both $\pi_1(X)$ and $\pi_2(X)$ are infinite. By Lemma 12, we may find some $a \in \mathbf{A}$ so that $\varphi_a(\pi_1(X)) \geq \Gamma_{\mathrm{tor}}$ and $\varphi_a(\pi_2(X)) \geq \Gamma_{\mathrm{tor}}$. As X is commensurable with $\{(x, y) \in \Gamma^2 : \varphi_a(x, \sigma(x), \ldots, \sigma^\ell(x); y, \ldots, \sigma^\ell(y)) \in \varphi_a(\tilde{X})\}$, we may assume that $\pi_1(X) \geq \Gamma_{\mathrm{tor}}$ and $\pi_2(X) \geq \Gamma_{\mathrm{tor}}$.

If $(x, y) \in X$, then $y \in \mathrm{acl}(K, x) = K(x, \sigma(x), \ldots, \sigma^{n-1}(x))^{alg}$. Hence, in the equation for X we may assume that $R \in K\{\tau\}$. As noted above, we have already reduced to the case that R is separable. By Lemma 14 we know that $\Gamma \cap \mathrm{acl}(K) = \Gamma_{\mathrm{tor}}$. Hence, if $(x, y) \in X$ and $x \in \Gamma_{\mathrm{tor}}$, then y is torsion as well. Thus, we may take $b \in \mathbf{A} \setminus \{0\}$ so that $X \cap 0 \times \Gamma \leq 0 \times \varphi[b]$. So if $(\xi, \zeta) \in X$ and $\xi \in \Gamma_{\mathrm{tor}}$, then $\varphi_b(\zeta) \in \varphi_{\mathrm{tor}}(K(\xi))$.

By Lemma 13 the group Γ_{tor} is commensurable with $\varphi_{\mathrm{tor}}(K_{\mathfrak{p}}^{unr})$. Replacing σ with a power and K with a finite extension, we may assume that $\Gamma_{\mathrm{tor}} = \varphi_{\mathrm{tor}}(K_{\mathfrak{p}}^{unr})$. Thus, the extension $K(\Gamma_{\mathrm{tor}})/K$ is Galois and its Galois group is topologically generated by σ.

Let $\Xi := \{(\xi, \sigma(\xi), \ldots, \sigma^{n-1}(\xi)) : \xi \in \Gamma_{\mathrm{tor}}\}$. Let

$$\hat{X} := \overline{(\xi, \ldots, \sigma^{n-1}(\xi); \zeta, \ldots, \sigma^{n-1}(\zeta)) : (\xi, \zeta) \in X\}}$$

Write $Q = \sum_{j=0}^{n-1} q_j \sigma^j$ where $q_j \in K\{\tau\}$. Let $\tilde{Q} := \sum_{j=0}^{\ell} q_j(x_j)$. The variety $\hat{X}$ is a subvariety of the prolongation of X and may be described by the equations $\tilde{Q}(x_0, \ldots, x_{n-1}) = R(y_0)$, $\tilde{Q}^\sigma(x_1, \ldots, x_{n-1}, S_n(x_0, \ldots, x_{n-1}) = R^\sigma(x_1)$, …, $\tilde{Q}^{\sigma^{n-1}}(x_{n-1}, S_n(x_0, \ldots, x_{n-1}), \ldots, S_{2n-1}(x_0, \ldots, x_{n-1})) = R^{\sigma^{n-1}}(x_{n-1})$ where

$$S_{n+j}(x, \sigma(x), \ldots, \sigma^{n-1}(x)) = \sigma^{n+j}(x)$$

for $x \in \Gamma$. Our goal is to show that X is commensurable with an $\mathbf{A}$-module. To do this, we show that $\hat{X}$ is commensurable with an $\mathbf{A}$-module.

We work now in the ∞-adic topology. Near zero in the ∞-adic topology we may invert R (and hence R^{σ^j} for any integer j) as an analytic function since R is separable. Let $\mathcal{U}$ be a small enough neighborhood of zero in ${\mathbb{G}_a}^n(\mathbb{C}_\infty)$ in which the compositional inverse to $(R, R^\sigma, \dots, R^{\sigma^{n-1}})$ is given by a convergent analytic function. In $\mathcal{U}^2$, $\hat{X}$ is the graph of a (partial) analytic function. Set $g_j := (R^{\sigma^j})^{-1} \circ \tilde{Q}^{\sigma^j}(x_j, \dots, x_{n-1}, S_n(x_0, \dots, x_{n-1}), \dots, S_{n+j-1}(x_0, \dots, x_{n-1}))$. Then, $\hat{X} \cap \mathcal{U}^2$ is defined by $y = (y_0, \dots, y_{n-1}) = (g_0(x), \dots, g_{n-1}(x)) = g(x)$. If we show that $\varphi_b \circ g$ commutes with the action of $\mathbf{A}$, then the same is true of g which would imply that $\hat{X}$ is commensurable with an $\mathbf{A}$-module.

Let $a \in \mathbf{A}$. Let $f := \varphi_b \circ (g \circ \varphi_a - \varphi_a \circ g)$. Observe that $f \equiv 0 \mod (x_0, \dots, x_{n-1})^2$. Thus, provided that $\mathcal{U} \subseteq \mathfrak{m}^n_{\mathbb{C}_\infty}$, we have $f(\mathcal{U}) \subseteq \mathcal{U}$ and more importantly, if $x \in \mathcal{U}$ and is not zero, then $|f(x)|_\infty < |x|_\infty$.

We note that either $f \equiv 0$ or there is an integer N such that for any x if $f(x) = 0$, then $[K(x) : K] \leq N$. In the latter case we see that if $\overbrace{f \circ \cdots \circ f}^{\ell \text{ times}}(x) = 0$, then the extension of fields $[K(x) : K]$ decomposes into ℓ subextensions each of degree at most N. Since the Galois groups $\mathrm{Gal}(K^{unr}_{\mathfrak{p}}/K)$ and $\mathrm{Gal}(\mathbb{F}_q^{alg}/\mathbb{F}_q)$ are isomorphic via the reduction map, we see that there are torsion points $\zeta \in \Gamma_{\mathrm{tor}}$ with $[K(\zeta) : K]$ prime and arbitrarily large. Thus, we can find $\zeta \in \Gamma_{\mathrm{tor}}$ so that $\xi := (\zeta, \sigma(\zeta), \dots, \sigma^{n-1}(\zeta)) \in \Xi$ and for all positive integers ℓ we have $f^{(\ell)}(\xi) \neq 0$. By the above comment on rationality, we see that $f^{(\ell)}(\xi) \in K(\xi)$. By the fact that f is a contraction mapping, we see that the set $\{f^{(\ell)}(\xi) : \ell \in \mathbb{Z}_+\}$ is infinite. However, no finitely generated field can contain infinitely many φ-torsion points. Hence, we must have $f \equiv 0$. As $f \equiv 0$ for any choice of $a \in \mathbf{A}$, we see that g commutes with φ so that $\hat{X}$ and hence X are commensurable with $\mathbf{A}$-modules. ♠

Remark 16. The reader may recognize Tamagawa's proof of Poonen's theorem on the rigidity of Drinfeld modules in parts of the last proof.

We now finish the proof of Proposition 8. The remaining case applies more generally than the groups considered in this paper.

Proof: We are now in the case of $m > 2$.

If $\mathrm{SU}(X) = m$, then X is commensurable Γ^m and we are done. Thus, after reordering the coordinates we see that if $\nu : \Gamma^m \to \Gamma^{m-1}$ is the projection onto the first $m-1$ coordinates, then ν is finite on X. Let $Y := \nu(X)$. By induction, we know that Y is commensurable with an $\mathbf{A}$-module. Passing to that commensurate $\mathbf{A}$-module Z and replacing X with $\nu^{-1}(Z)$, we may assume that Y itself is an $\mathbf{A}$-module. Let $\vartheta : \Gamma^{m-1} \to \Gamma^g$ be a projection so that $\vartheta(Y)$ is commensurable with Γ^g and $g = \mathrm{SU}(Y)$. Let $a \in \mathbf{A} \setminus \{0\}$ so that $\varphi[a]^{m-1}$ contains the kernel of ϑ. Define $\psi : \vartheta(Y) \to \Gamma^{m-1}$ by $x \mapsto \varphi_a(\vartheta^{-1}(x))$. Let $\hat{X} := \{(x, y) \in \Gamma^g \times \Gamma : (\psi(x), y) \in X\}$. Since ψ is a map of $\mathbf{A}$-modules, if $\hat{X}$ is commensurable with an $\mathbf{A}$-module, so is X.

If $g < m-1$, then we are done by induction. Thus, we have reduced to the case that $\mathrm{SU}(X) = m-1$ and $\pi(X) = Y$ is commensurable with Γ^{m-1}. As has become standard by now, we may also assume that X is quantifier-free definable and that its defining equations correspond to a connected algebraic group. Let ℓ be large enough and $\tilde{X} \leq ({\mathbb{G}_a}^m)^\ell$ so that $X = \{x \in {\mathbb{G}_a}^m(\mathcal{K}) : (x, \sigma(x), \dots, \sigma^{\ell-1}(x)) \in \tilde{X}\}$. Note that because the eventual σ-degree of Γ is one, $\ell = n+1$ suffices.

As $m > 2$, $m - 1 \geq 2$. Thus, there are infinitely many distinct connected algebraic $\mathbf{A}$-submodules of ${\mathbb{G}_a}^{m-1}$ of codimension one. Let $\{M_j\}_{j\in\omega}$ enumerate these. Observe that $(M_j(\mathcal{K}) \times \Gamma) \cap X$ has SU-rank $m-2$ but that for $j \neq j'$ we have $\mathrm{SU}([(M_j(\mathcal{K}) \times \Gamma) \cap X] \cap [(M_{j'}(\mathcal{K}) \times \Gamma) \cap X]) = m - 3$. By the case of the previous paragraph we see that each of the groups $(M_j(\mathcal{K})\times\Gamma)\cap X$ is commensurable with an $\mathbf{A}$-module K_j. Replacing K_j with its quantifier-free connected component, we may assume that $K_j \leq X$. The above phrase means that we assume that $K_j = \{x \in {\mathbb{G}_a}^m(\mathcal{K}) : (x, \ldots, \sigma^{\ell-1}(x)) \in \tilde{K}_j\}$ with $\tilde{K}_j = \tilde{K}_j^0$. Note also that K_j is not commensurable with $K_{j'}$ for distinct j and j'.

If $a \in \mathbf{A}$ is nonzero, then for any index j we have $\tilde{K}_j = \varphi_a(\tilde{K}_j)$. Thus, $\varphi_a(\tilde{X})$ contains $\bigcup_{j=0}^{\infty} \tilde{K}_j$ as does $\tilde{X}$. If $\tilde{X} \neq \varphi_a(\tilde{X})$, then $Z := \{x \in {\mathbb{G}_a}^m(\mathcal{K}) : (x, \ldots, \sigma^{\ell-1}) \in \tilde{X} \cap \varphi_a(\tilde{X})\}$ is a proper quantifier-free definable subgroup of X (and hence has SU-rank less than $m-1$) which contains infinitely many pairwise incommensurable subgroups of SU-rank $m-2$ (and hence has SU-rank at least $m-1$). This is impossible. Therefore, $\tilde{X} = \varphi_a(\tilde{X})$ and this holds for any $a \in \mathbf{A}$. So, the original X is commensurable with an $\mathbf{A}$-module. ♠

Our task now is to extend this result to all the torsion points. We accomplish this by showing that the proof of Proposition 7 yields uniform estimates on the number and degrees of the components of the Zariski closures of the intersections of varieties with $\ker P_{\mathfrak{p}}(\sigma)(\mathcal{K})$. Combining this estimate with a similar estimate at another prime of good reduction will prove Theorem 1. This technique is modification of the quantitative version Hrushovski's proof of the Manin-Mumford conjecture in [5].

Lemma 17. *Let* $r := \mathrm{rank}(\varphi)$. *Let* $d := [\mathbf{k}(\tau^n) : \mathbf{k}]$ *where* $q_{\mathfrak{p}} = p^n$ *and the extension takes place inside* $\mathrm{End}(\varphi^{\mathfrak{p}}) \otimes_{\mathbf{A}} \mathbf{k}$.

Then, $\deg(S_{\mathfrak{p}}) = q_{\mathfrak{p}}^d$ *and* $\deg_X P_{\mathfrak{p}} = d$.

Proof: That the degree of $P_{\mathfrak{p}}$ is d is immediate from its definition. The calculation of the degree of the hypersurface $S_{\mathfrak{p}}$ is based on Gekeler's theorem (Theorem 4.12.8 of [6]) that the roots of $P_{\mathfrak{p}}$ all have normalized $|\cdot|_\infty$ absolute value of $q_{\mathfrak{p}}^{\frac{1}{r}}$ so that the absolute value of any co-efficient of $P_{\mathfrak{p}}$ is at most $q_{\mathfrak{p}}^{\frac{d}{r}}$ with the constant term actually achieving this. By the definition of the rank of φ, this means that the co-efficients of $P_{\mathfrak{p}}$ have degree (as polynomials in τ^n) of at most d (again, being achieved for the co-efficent of τ^0). So, the degree of $S_{\mathfrak{p}}$ is $q_{\mathfrak{p}}^d$. ♠

The above Lemma implies a uniform bound on the degree of the Zariski closure of the intersection of a variety X with the kernel of $P_{\mathfrak{p}}(\sigma)$.

Proposition 18. *With the notation as above, for any variety* $X \subseteq {\mathbb{G}_a}^m$ *if* S *is the kernel of* $P_{\mathfrak{p}}(\sigma)$, *then the Zariski closure of* $X \cap S$ *is a union of at most* $(q_{\mathfrak{p}}^{rm} \deg(X)^{d+1})^{2^{(d+1)\dim(X)}}$ *translates of algebraic* $\mathbf{A}$*-modules. In fact, the degree of this Zariski closure is bounded by this number.*

Proof: This is an immediate application of Corollary 2.6 of [5] using the calculation of Lemma 17. ♠

We fix now a second prime $\mathfrak{q}$ of good reduction with ρ an extension of $\mathcal{K}$ of a relative Frobenius at $\mathfrak{q}$ so that $(\mathcal{K}, \rho) \models \mathrm{ACFA}$. Working first with σ and then with ρ we complete the proof of Theorem 1 following the argument of Section 5 of [5].

Proof of Main Theorem: We fix some more notation. $U_{\mathfrak{p}}$ is the $\mathbf{A}$-module of φ-torsion points unramified at $\mathfrak{p}$. $F_{\mathfrak{p}}$ is the $\mathbf{A}$-module of φ-torsion points in the kernel of reduction at $\mathfrak{p}$. We let $d := \deg_X P_{\mathfrak{q}}$ and write $P_{\mathfrak{p}}(X) = \sum_{i=0}^{d} a_i X^i$. We write φ for the composite of φ with the diagonal inclusion of $\mathrm{End}_{\mathrm{K}}(\mathbb{G}_{\mathrm{a}})$ in $\mathrm{End}_{\mathrm{K}}(\mathbb{G}_{\mathrm{a}}{}^{\nu})$ for any given ν.

Since $\ker P_{\mathfrak{p}}(\sigma)(\mathcal{K})$ is modular, up to commensurability there are only $\aleph_0$ definable subgroups of any of its Cartesian powers. It folows by compactness that for X given as in the statement of the theorem, there is a finite set $\mathcal{T}(X)$ of connected algebraic $\mathbf{A}$-modules such that the components of the Zariski closures of $a + X(\mathcal{K}) \cap \ker P_{\mathfrak{p}}(\sigma)(\mathcal{K})^m$ are of the form $b + N$ for appropriate $b \in {\mathbb{G}_a}^m(\mathcal{K})$ and $N \in \mathcal{T}(X)$.

Let $\Gamma := \{x = (x_0, \dots, x_d) \in ({\mathbb{G}_a}^m)^{dm+1} : \bigwedge_{i=0}^{d(m-1)+1} \sum_{j=0}^{d} \varphi_{a_j}(x_{j+i}) = 0\}$. Γ is the dm-th prolongation of $\ker P_{\mathfrak{q}}(\rho)(\mathcal{K})^m$. That is, it is the Zariski closure of $\{(x, \rho(x), \dots, \rho^{dm}(x)) : x \in {\mathbb{G}_a}^m(\mathcal{K}) \text{ and } P_{\mathfrak{q}}(\rho)(x) = 0\}$. Notice that $\dim \Gamma = dm$.

For each $N \in \mathcal{T}(X)$, let $\Sigma_N := \{(x, y) \in ({\mathbb{G}_a}^m)^{dm+1} \times ({\mathbb{G}_a}^m)^{dm+1} : x \in \Gamma \text{ and } \bigwedge_{i=0}^{dm+1} x_i + y_i + N \subseteq X$, but for any $M \in \mathcal{T}(X)$ one has $\dim(x_i + y_i + M \cap X) \leq \dim N\}$.

Let $\pi_2 : ({\mathbb{G}_a}^m)^{dm+1} \times ({\mathbb{G}_a}^m)^{dm+1} \to ({\mathbb{G}_a}^m)^{dm+1}$ be the projection $(x, y) \mapsto y$. Let Υ_N be the Zariski closure of $(\ker P_{\mathfrak{p}}(\sigma)(\mathcal{K})^m)^{dm+1} \cap \pi_2(\Sigma_N)$. Then by Proposition 7, Υ_N is a finite union of translates of algebraic $\mathbf{A}$-modules.

Let $\pi_N : ({\mathbb{G}_a}^m)^{dm+1} \to ({\mathbb{G}_a}^m/N)^{dm+1}$ be the quotient map. Let $\Xi_N := \pi_N(\Upsilon_N)$. So, Ξ_N is a finite union of translates of $\mathbf{A}$-modules. Note that $\dim \Xi_N = \dim \Gamma = dm < dm + 1$.

By Lemma 5.12 of [5] it follows that

$$\tilde{\Xi}_N := \{(x, y) \in {\mathbb{G}_a}^m \times {\mathbb{G}_a}^m(\mathcal{K}) : (x, \rho(x), \dots, \rho^{dm}(x); \pi_N(y), \rho(\pi_N(y)), \cdots, \rho^{dm}(\pi_N(y))) \in \Xi_N\}$$

is a finite boolean combination of cosets of $\mathbf{A}$-modules. Moreover, by the definition of Υ_N, if $(x, y) \in \tilde{\Xi}_N$, then $x_0 + y_0 + N \subseteq X$.

Let $\hat{X} := \{(x, y) \in {\mathbb{G}_a}^m \times {\mathbb{G}_a}^m : x + y \in X\}$. Then

$$\begin{aligned}
\overline{X \cap \varphi_{\mathrm{tor}}^m} &= \{x + y : (x, y) \in \overline{\hat{X} \cap U_{\mathfrak{p}}^m \times F_{\mathfrak{p}}^m}\} \\
&=: +(\overline{\hat{X} \cap U_{\mathfrak{p}}^m \times F_{\mathfrak{p}}^m}) \\
&\subseteq +(\overline{\hat{X} \cap \cup_{N \in \mathcal{T}(X)} \tilde{\Xi}_N}) \\
&\subseteq X
\end{aligned}$$

The set on the penultimate line is a finite union of cosets of $\mathbf{A}$-modules. So we find that $X \cap \varphi_{\mathrm{tor}}^m$ is contained in a finite union of of translates of $\mathbf{A}$-modules each of which is contained in X. Thus, the Zariski closure of $X \cap \varphi_{\mathrm{tor}}^m$ is a finite union of translates of algebraic $\mathbf{A}$-modules. ♠

Remark 19. The proof given here certainly generalizes to give a stronger theorem. For instance, it applies immediately to T-modules obtained as subquotients of products of Drinfeld modules of generic characteristic. One obtains uniform bounds on the degrees of the Zariski closures of the intersection of a variety $X \subseteq {\mathbb{G}_a}^m$ with φ_{tor}^n depending only on $m, \deg(X), q_{\mathfrak{p}}$, and $q_{\mathfrak{q}}$ from the above proof as in Hrushovski's version of the Manin-Mumford conjecture [5]. This proof also yields uniform $\mathfrak{p}$-adic estimates on the distance from torsion points to varieties as in [7].

References

[1] J. Boxall, Sous-variétés algébriques de variétés semi-abéliennes sur un corps fini, **Number Theory** (Paris 1992 - 1993), pp. 69–80, LMS Lecture Note Ser. (**215**), Cambridge University Press, Cambridge, 1995.

[2] Z. Chatzidakis and E. Hrushovski, The model theory of difference fields, *Transactions of the AMS*, (to appear).

[3] Z. Chatzidakis, E. Hrushovski, and Y. Peterzil, The Model Theory of Difference Fields II, preprint, 1999.

[4] L. Denis, Géométrie diophantienne sur les modules de Drinfeld, in: **The Arihmetic of Function Fields** (eds. D. Goss *et al*) (1992), 285 – 302.

[5] E. Hrushovski, The Manin-Mumford conjecture and the model theory of difference fields, preprint, 1996.

[6] D. Goss, **Basic Structures of Function Field Arithmetic**, Ergebniße der Mathematik und ihrer Grenzgebiete **35**, Springer, Berlin, 1996.

[7] T. Scanlon, p-adic distance from torsion points of semi-abelian varieties, *Journal für die Reine und Angewandte Mathematik* **499** (1998), 225–236.

[8] T. Scanlon and J. F. Voloch, Difference subgroups of commutative algebraic groups over finite fields, *Manuscripta Mathematica***99** (1999) 3, 329 – 339.

University of California, Berkeley, Mathematics Department, Evans Hall, Berkeley, California 94720, USA

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