manuscripta mathematica manuscript No.
(will be inserted by the editor)

Thomas Scanlon[1] · José Felipe Voloch[2]

Difference algebraic subgroups of commutative algebraic groups over finite fields

the date of receipt and acceptance should be inserted later

Abstract. We study the question of which torsion subgroups of commutative algebraic groups over finite fields are contained in modular difference algebraic groups for some choice of a field automorphism. We show that if G is a simple commutative algebraic group over a finite field of characteristic p, ℓ is a prime different from p, and for some difference closed field $(\mathcal{K}, \sigma)$ the ℓ-primary torsion of $G(\mathcal{K})$ is contained in a modular group definable in $(\mathcal{K}, \sigma)$, then it is contained in a group of the form $\{x \in G(\mathcal{K}) : \sigma(x) = [a](x)\}$ with $a \in \mathbb{N} \setminus p^{\mathbb{N}}$. We show that no such modular group can be found for many G of interest. In the cases that such equations may be found, we recover an effective version of a theorem of Boxall.

1. Introduction

The work of Chatzidakis and Hrushovski [CH] on the model theory of difference fields in characteristic zero showed that groups defined by difference equations have a very restricted structure. For instance, if G is a semi-abelian variety over a difference closed field (K, σ) of characteristic zero and $\Gamma \leq G(K)$ is a definable finite rank subgroup of "modular type," then for any subvariety $X \subseteq G$, the set $X(K) \cap \Gamma$ is a finite union of cosets of definable subgroups of Γ. Using such facts one can resolve some diophantine questions about special subgroups of $G(K)$ (for instance, the torsion subgroup [Hr]). Recent work of Chatzidakis, Hrushovski, and Peterzil extends the class of difference fields for which this sort of result is known to positive characteristic. In this note, we analyze which subgroups of the torsion points of simple commutative algebraic groups over finite fields can be captured by such equations. Surprisingly, we show that when the difference equations exist, they may be taken to have a very simple form so that while the Manin-Mumford style results follow from [CHP], direct arguments in the style of [Bog] or [Hi] are available. Moreover, we exhibit many cases where for a given simple abelian variety A over a

Mathematics Department, University of California at Berkeley, Evans Hall, Berkeley, California 94720 USA e-mail: scanlon@math.berkeley.edu

Department of Mathematics, University of Texas at Austin, Austin, Texas 78712 USA e-mail: voloch@math.utexas.edu

finite field k and a prime ℓ it is not possible to find a difference closed field $(\mathcal{K}, \sigma)$ and a modular definable group $\Gamma \leq G(\mathcal{K})$ containing the ℓ-power torsion. This contrasts sharply with the case where A has generic moduli when one can find $(\mathcal{K}, \sigma)$ and $\Gamma \leq A(\mathcal{K})$ modular so that Γ contains *all* the torsion of A [Sc2]. Under the assumption of the ℓ-adic four exponentials conjecture we give a precise criterion for the existence of modular difference algebraic groups containing the ℓ-primary torsion of a simple abelian variety A depending on the multiplicative group of $\mathrm{End}(A) \otimes \mathbb{Q}_\ell$.

In the cases where we establish the existence of modular difference algebraic groups containing the ℓ-primary torsion of some given algebraic group G, we recover part of a theorem of Boxall [Box] together with effective bounds (better than Boxall's in one sense and worse in another). Under the assumption of Artin's conjecture on the density of the set of primes p for which a given integer a is a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$ and a related conjecture on the density of $\{p$:prime and $a^{p-1} \not\equiv 1 \pmod{p^2}\}$ we show that modular difference algebraic subgroups of the multiplicative group may contain a very large subgroup of the roots of unity. For such groups we conclude a stronger (qualitative as well as quantitative) theorem than does Boxall.

The authors would like to thank MSRI for the hospitality during the period this work was carried out. The authors thank B. Conrad and the referee for their detailed comments on earlier versions of this paper. The first author is supported by an NSF Mathematical Sciences Postdoctoral Research Fellowship. The second author would like to thank the University of Texas' URI for financial support.

2. General set up

A difference field is a field K given together with a field endomorphism $\sigma : K \to K$. We define the fixed field of σ to be $\mathrm{Fix}(\sigma) := \{x \in K : \sigma(x) = x\}$. If X is a scheme over K, then we define $X^\sigma := X \times_{\mathrm{Spec}(K)} \mathrm{Spec}(K)$ where we take $\sigma^* : \mathrm{Spec}(K) \to \mathrm{Spec}(K)$ to form the fibre product. Concretely, if

$$X = \mathrm{Spec}(K[x_1, \ldots, x_n]/(f_1(\mathbf{a_1}; \mathbf{x}), \ldots, f_m(\mathbf{a_m}; \mathbf{x}))$$

where

$$f_i(y_1, \ldots, y_q; x_1, \ldots, x_n) \in \mathbb{Z}[y_1, \ldots, y_q; x_1, \ldots, x_n]$$

and $\mathbf{a_i} \in K^q$, then

$$X^\sigma = \mathrm{Spec}(K[x_1, \ldots, x_n]/(f_1(\boldsymbol{\sigma}(\mathbf{a_1}); \mathbf{x}), \ldots, f_m(\boldsymbol{\sigma}(\mathbf{a_m}); \mathbf{x})))$$

σ induces a map on points $\sigma : X(R) \to X^\sigma(R)$ which we continue to denote by σ. When $X \subseteq \mathbb{A}^n$ is given as a subscheme of affine space, then the map $\sigma : X(K) \to X^\sigma(K)$ is induced by $(x_1, \ldots, x_n) \mapsto (\sigma(x_1), \ldots, \sigma(x_n))$. When X is defined over $\mathrm{Fix}(\sigma)$, then we identify X with X^σ.

By a *difference closed field* we mean an algebraically closed difference field $(\mathcal{K}, \sigma)$ in which σ is surjective and the following condition holds: if X is an irreducible variety over $\mathcal{K}$, $Y \subseteq X \times X^\sigma$ is an irreducible subvariety of $X \times X^\sigma$ which dominates both X and X^σ via the first and the second projections, respectively, and $U \subseteq Y$ is a Zariski open subset, then there is a point $x \in X(\mathcal{K})$ with $(x, \sigma(x)) \in U(\mathcal{K})$. Such difference fields are also called models of ACFA.

If (K, σ) is a difference field and X a variety over K, then a difference subvariety $\widetilde{Y} \subseteq X$ of X over K is given by a variety $Y \subseteq X \times X^\sigma \times \cdots \times X^{\sigma^N}$ for some N. The points of $\widetilde{Y}$ are $\widetilde{Y}(K, \sigma) := \{x \in X(K) : (x, \sigma(x), \ldots, \sigma^N(x)) \in Y(K)\}$. If G is an algebraic group over K, then we say that the difference subvariety $\Gamma \subseteq G$ is a difference algebraic group if for all difference fields (L, ρ) extending (K, τ), $\Gamma(L, \rho)$ is a subgroup of $G(L)$. This can be checked with (L, ρ) a difference closed field. Note that if G is defined over $\mathrm{Fix}(\sigma)$, then $\sigma : G(K) \to G(K)$ is a group homomorphism. If $P(X) \in \mathrm{End}_K(G)[X]$ is a polynomial, of the form $P(X) = \sum_{i=0}^N \psi_i X^i$, then $P(\sigma) : G(K) \to G(K)$ defined by $x \mapsto \sum_{i=0}^N \psi_i(\sigma^i(x))$ is a group homomorphism. The kernel of $P(\sigma)$ is a difference algebraic subgroup of G where the corresponding variety is $\{(x_0, \ldots, x_N) \in G^{N+1} : \sum_{i=0}^N \psi_i(x_i) = 0\}$. For the purposes of this note we say that a difference algebraic subgroup Γ of an algebraic group G over a difference field (K, σ) is *modular* if for all difference fields (L, ρ) extending (K, s) and all subvarieties $X \subseteq G^N$ over L, the set $X(L) \cap \Gamma(L, \rho)$ is a finite union of cosets of subgroups of $\Gamma(L, \rho)$. The reader may notice that we have appropriated the word *modular* for a weaker property: for any difference closed field $(\mathcal{K}, \sigma)$ extending (K, σ) the group $\Gamma(\mathcal{K}, \sigma)$ is weakly normal for the structure induced by quantifier free formulas in the pure field language. The reader should consult [C] for a more thorough discussion of modularity in this context.

For the rest of this paper k will denote a finite field of characteristic p. $\tau \in \mathrm{Gal}(\bar{k}/k)$ denotes the Frobenius field automorphism relative to k. That is, if $k = \mathbb{F}_q$, then $\tau(x) = x^q$. Recall that $\mathrm{Gal}(\bar{k}/k)$ is topologically generated by τ and is isomorphic as a topological group to $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$ with τ corresponding to $1 \in \widehat{\mathbb{Z}}$. $\widehat{\mathbb{Z}}$ is isomorphic to $\prod_{\ell \text{ prime}} \mathbb{Z}_\ell$. If $a \in \widehat{Z}$ then we denote its image in $\mathbb{Z}_\ell$ by a_ℓ. If X is any

variety over k, then $F : X \to X$ denotes the Frobenius endomorphism of X (relative to k).

If G is a commutative algebraic group over k and $\Lambda \in \mathrm{End}_k(G)$ is an endomorphism then $G[\Lambda]$ denotes the kernel of Λ considered as a subgroup scheme of G. $T_\Lambda G$ denotes the Λ-Tate module of G, $\varprojlim G[\Lambda^n](\bar{k})$ where the transition maps are given by $\Lambda^{m-n} : G[\Lambda^m](\bar{k}) \to G[\Lambda^n](\bar{k})$. By $\mathrm{Aut}(T_\Lambda G)$ we mean the group of continuous automorphisms of $T_\Lambda G$. Likewise, $\mathrm{End}(T_\Lambda G)$ denotes the ring of continuous endomorphisms of $T_\Lambda G$. $\mathrm{Gal}(\bar{k}/k)$ acts continuously on $T_\Lambda G$. We denote the representation corresponding to this actions by $\rho_{G,\Lambda} : \mathrm{Gal}(\bar{k}/k) \to \mathrm{Aut}(T_\Lambda G)$.

We regard $\mathbb{Z}$ as a subring of $\mathrm{End}_k(G)$. If $S \subseteq \mathrm{End}_k(G)$ is a submonoid under composition, then we define $G_S := \bigcup_{s \in S} G[s](\bar{k})$. Our main goal is to describe which groups of the form G_S are subgroups of some modular difference algebraic group for some choice of $\sigma \in \mathrm{Gal}(\bar{k}/k)$. When S is generated by a single endomorphism Λ we may write $G[\Lambda^\infty]$ for G_S.

Before proceeding to analyze particular commutative algebraic groups, we observe that we may restrict our attention to difference algebraic groups defined as kernels of endomorphisms of the form $P(\sigma)$ with $P(X) \in \mathrm{End}_K[X]$.

Proposition 1 *If G is a simple commutative algebraic group over k, $(\mathcal{K}, \sigma)$ is a difference closed field extending $\bar{k}$, $\Xi \leq G(\bar{k})$ is an infinite $\mathrm{Gal}(\bar{k}/k)$-stable subgroup, and $\Gamma \leq G$ is a modular difference algebraic subgroup of G over L such that $\Xi \leq \Gamma(\mathcal{K}, \sigma)$, then there is some $P(X) \in \mathrm{End}_K(G)$ and $\rho \in \mathrm{Gal}(\bar{k}/k)$ such that $\ker P(\rho)$ is a modular group with $\Xi \leq \ker P(\rho)(\bar{k})$.*

Proof: Since k is finite, $k \subseteq \mathrm{Fix}(\sigma^m)$ for some $m \geq 1$. If we let Υ be the smallest difference algebraic group containing Γ definable in $(\mathcal{K}, \sigma^m)$, then Υ is also modular. So we may assume that $k \subseteq \mathrm{Fix}(\sigma)$.

Since the algebraic group G is not modular itself, $\Gamma_N :=$ the Zariski closure of $\{(x, \sigma(x), \ldots, \sigma^N(x)\}$ is not equal to G^{N+1} for some N. Take N minimal. Then for some $m \leq N$, $\Xi_m :=$ the Zariski closure of $\{(x, \ldots, \sigma^m(x)) : x \in \Xi\}$ is not equal to G^{m+1}. Since Ξ is a group, so is Ξ_m. As G is simple and m was chosen to be minimal so that $G^{m+1} \neq \Xi_m$, we have $\Xi_m = \{(x_0, \ldots, x_m) \in G^{m+1} : \sum_{i=0}^m \psi_i(x_i) = 0\}$ for some $\psi_i \in \mathrm{End}_\mathcal{K}(G)$. Since $\Xi \subseteq G(\bar{k})$, $\{(x, \ldots, \sigma^m(x)) : x \in \Xi\} \subseteq G^{m+1}(\bar{k})$. Thus, each ψ_i is defined over $\bar{k}$. Since Ξ is $\mathrm{Gal}(\bar{k}/k)$-stable, so is Ξ_m. As k is perfect, this implies that Ξ_m, and hence each ψ_i, is defined over k.

Set $P(X) := \sum_{i=0}^{m} \psi_i X^i \in \mathrm{End}_k(G)[X]$. So the difference algebraic subgroup $\ker P(\sigma) = \widetilde{\Xi_m}$ defined by Ξ_m is a difference algebraic subgroup of Γ (and is therefore modular) and $\widetilde{\Xi_m}(\bar{k}, \sigma)$ contains Ξ. $\diamondsuit$

3. The multiplicative group

In analyzing the case of the multiplicative group $\mathbb{G}_m(\bar{\mathbb{F}}_p)$ we will see that finding appropriate equations and automorphisms comes down to solving exponential equations ℓ-adically. These equations are easy to solve in the case of $\mathbb{G}_m$, but as the rank of the endomorphism ring of the algebraic group grows, so does the difficulty in finding these equations.

In this section $k = \mathbb{F}_p$.

Theorem 2 *For any prime $\ell \neq p$ there is some $\sigma \in \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ and $a \in \mathbb{Z}$ such that the difference algebraic group over $(\bar{\mathbb{F}}_p, \sigma)$ given as $\ker P(\sigma)$ where $P(X) = X - a \in \mathrm{End}\mathbb{G}_m[X]$ is modular and $\mathbb{G}_m[\ell^\infty] \leq \ker P(\sigma)(\bar{\mathbb{F}}_p)$.*

Proof: Let $\rho := \rho_{\mathbb{G}_m,\ell} : \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p) \to \mathbb{Z}_\ell^\times = \mathrm{Aut}(T_\ell \mathbb{G}_m)$ be the Galois representation corresponding to the action of $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ on $T_\ell \mathbb{G}_m$. $\rho(\tau) = p$ so that the image of ρ is the ℓ-adic closure of the group generated by p, which is an open subgroup of $\mathbb{Z}_\ell^\times$. As $\mathbb{N} \setminus p^{\mathbb{N}}$ is dense in $\mathbb{Z}_\ell$, we may find $a \in (\mathbb{N} \setminus p^{\mathbb{N}}) \cap \rho(\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p))$. Let $\sigma \in \rho^{-1}(a)$. Then, $\mathbb{G}_m[\ell^\infty] \leq \{x \in \mathbb{G}_m(\bar{\mathbb{F}}_p) : \sigma(x) = x^a\}$ by the choice of a and σ. The criterion following Theorem 5.4 of [CH] together with the main trichotomy theorem of [CHP] shows that the equation $\sigma(x) = x^a$ defines a modular group. We give a direct proof of this fact in the next proposition. $\diamondsuit$

As mentioned in the course of the last proof one can prove directly, ie without recourse to the extensive theory of difference closed fields developed in [CH] and [CHP], that a difference algebraic subgroup of $\mathbb{G}_m$ defined by $\sigma(x) = x^a$ with $a \in \mathbb{N} \setminus p^{\mathbb{N}}$ is modular. Modularity of this group implies effective bounds on the degree of the Zariski closure of sets of the form $\{(x_1, \ldots, x_m) \in X : \sigma(x_i) = x_i^a \text{ for } 1 \leq i \leq m\}$ with X a variety (see section 2 of [Hr]). In the next proposition we show how modularity may be deduced via a calculation of these bounds.

Proposition 3 *Let $a \in \mathbb{N} \setminus p^{\mathbb{N}}$. Let $\alpha := \frac{a}{(a,p)}$. For $n \in \mathbb{N}$ define $d_n := \sum_1^n i 2^{i-1}$. Let (L, σ) be a difference closed field of characteristic*

p. Let $X \subseteq \mathbb{G}_m{}^g$ be a subvariety of $\mathbb{G}_m{}^g$ defined over L. Let $\Gamma_a \leq \mathbb{G}_m$ be the difference algebraic group defined by $\sigma(x) = x^a$. The set $\Gamma_a(L,\sigma)^g \cap X(L)$ is a finite union of cosets of subgroups $\mathbb{G}_m{}^g(L)$. Its Zariski closure has degree at most $\deg(X)^{2^{\dim(X)}}\alpha^{d_{\dim(X)}}$ *where* deg *is computed with respect to the usual inclusion of $\mathbb{G}_m{}^g$ in $\mathbb{P}^g$.*

Proof: To ease notation, we write X for $X(L)$ and Γ_a for $\Gamma_a(L,\sigma)$. By $X^{[a]}$ we mean the image of X under the map $(x_1,\dots,x_g) \mapsto (x_1^a,\dots,x_g^a)$.

We prove this proposition by Noetherian induction on X. When $\dim(X) = 0$, the result is trivial. So from now on we take $\dim(X) > 0$. If $X = \bigcup_{i=1}^m X_i$ is the decomposition of X into its irreducible components and $m > 1$, then by induction we have

$$\begin{aligned}
\deg(\overline{X \cap \Gamma_a^g}) &= \deg(\overline{\Gamma_a^g \cap \bigcup_{i=1}^m X_i}) \\
&\leq \sum_{i=1}^m \deg(\overline{X_i \cap \Gamma_a^g}) \\
&\leq \sum_{i=1}^m \deg(X_i)^{2^{\dim(X)}}\alpha^{d_{\dim(X)}} \\
&\leq (\sum_{i=1}^m \deg(X_i))^{2^{\dim(X)}}\alpha^{d_{\dim(X)}} \\
&= \deg(X)^{2^{\dim(X)}}\alpha^{d_{\dim(X)}}
\end{aligned}$$

So, we are left with considering X irreducible and positive dimensional. If X is of the form ζT where $T \leq \mathbb{G}_m{}^g$ is an algebraic subgroup and $\zeta \in \Gamma_a^g$, then $X = \overline{X \cap \Gamma_a^g}$ so that the result is certainly true in this case. Otherwise, $X^\sigma \neq X^{[a]}$ (see Lemme 2 of [Hi] - the lemma there is stated for abelian varieties and without σ but the proof goes through for any isogeny of commutative algebraic groups with nontrivial kernel). We compute now

$$\begin{aligned}
\deg(\overline{X \cap \Gamma_a^g}) &= \deg(\overline{(X^\sigma \cap X^{[a]})^{\sigma^{-1}} \cap \Gamma_a^g}) \\
&\leq (\deg((X^\sigma \cap X^{[a]})^{\sigma^{-1}}))^{2^{\dim(X)-1}}\alpha^{d_{\dim(X)-1}} \\
&\leq (\deg(X)^2\alpha^{\dim(X)})^{2^{\dim(X)-1}}\alpha^{d_{\dim(X)-1}} \\
&\leq \deg(X)^{2^{\dim(X)}}\alpha^{d_{\dim(X)}}
\end{aligned}$$

♢

We observe that if $\ell_1, \ldots, \ell_s$ is a finite set of primes and S is the submonoid of $\mathbb{Z}$ generated by these primes, then one may effectively find $a \in \mathbb{N} \setminus p^{\mathbb{N}}$ such that there is some $\sigma \in \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ with $\mathbb{G}_{mS} \leq \{\zeta \in \mathbb{G}_m(\bar{\mathbb{F}}_p) : \sigma(\zeta) = \zeta^a\}$. Let $\mu := \prod_{i=1}^{s}(\ell_i - 1)$. Let $q := p^\mu$. Let $\omega = \tau^\mu \in \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$. Let n_i be the ℓ-adic valuation of $q-1$. Let a be the smallest natural number which is not a rational power of p satisfying the congruences $a \equiv 1 \pmod{\ell_i^{n_i}}$. Let $\alpha_i := \frac{\log_{\ell_i}(a)}{\log_{\ell_i}(q)}$ where $\log_{\ell_i}(x)$ is the ℓ_i-adic logarithm. Let $\sigma_i \in \mathrm{Gal}(\mathbb{F}_p(\mathbb{G}_m[\ell_i^\infty])/\mathbb{F}_p)$ be ω^{α_i}. Then σ_i acts as $\zeta \mapsto \zeta^a$ on $\mathbb{G}_m[\ell^\infty]$. The various σ_i amalgamate to give an element of $\mathrm{Gal}(\mathbb{F}_p(\mathbb{G}_{mS})/\mathbb{F}_p)$ as they agree on generators of each of the common subfields. Take $\sigma \in \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ to be a common extension of these σ_i's.

The above method of finding a and σ does not necessarily minimize a since we only looked for a close to 1 ℓ_i-adically. If, for instance, p is a generator of $\mathbb{F}_{\ell_i}^\times$ and we have $p^{\ell_i - 1} \not\equiv 1 \pmod{\ell_i^2}$ for each i, then we can take a to be the least positive integer not equal to a power of p and relatively prime to $\prod_i^m \ell_i$. This observation shows how under the assumption of two widely believed conjectures we can find a non-finitely generated submonoid S of $\mathbb{N}$, $a \in \mathbb{N} \setminus p^{\mathbb{N}}$, and $\sigma \in \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ such that $\mathbb{G}_{mS} \leq \{\zeta \in \bar{\mathbb{F}}_p^\times : \sigma(\zeta) = \zeta^a\}$.

Theorem 4 *Assume the following two conjectures:*

Artin's Conjecture: *The set of primes $\{\ell : p$ generates $\mathbb{F}_\ell^\times\}$ has positive density in the set of all primes.*

Conjecture on the Zeros of the the Derivative of p: *The set of primes $\{\ell : p^{\ell-1} \not\equiv 1 \pmod{\ell^2}\}$ has density one in the set of all primes.*

Then there is a non-finitely generated submonoid $S \subseteq \mathbb{N}$, natural number a not equal to a power of p, and a field automorphism $\sigma \in \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ such that $\mathbb{G}_{mS} \leq \{\zeta \in \bar{\mathbb{F}}_p^\times : \sigma(\zeta) = \zeta^a\}$.

Proof: The conjunction of the two conjectures we assume implies that $S_0 := \{\ell : \ell$ prime,$p^{\ell-1} \not\equiv 1 \pmod{\ell^2}$, and p generates $\mathbb{F}_\ell^\times\}$ has positive density in the set of all primes. In particular, S_0 is infinite. Let S be the submonoid of $\mathbb{N}$ generated by S_0. Let a be the least natural number not equal to a power of p and relatively prime to all $\ell \in S_0$. (Note that there are natural numbers satisfying both of these requirements as the complement of $S_0 \cup \{p\}$ in the set of all primes is non-empty.) For each $\ell \in S_0$, we can find $\sigma_\ell \in \mathrm{Gal}(\mathbb{F}_p(\mathbb{G}_m[\ell^\infty])/\mathbb{F}_p)$ which acts as $\zeta \mapsto \zeta^a$ on $\mathbb{G}_m[\ell^\infty]$. As noted above in the case of a finitely generated S, these automorphisms amalgamate and may be extended to a common $\sigma \in \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$. $\diamondsuit$

The conclusion of the previous theorem does not directly imply either of the assumed conjectures, but it does imply weak forms of each of them.

4. Simple abelian varieties

In this section, we revert to the notion of the set up where k denotes an arbitrary finite field of characteristic p. Let ℓ be a rational prime and A a simple abelian variety over k. Let $\iota_{A,\ell} : \mathrm{End}_k(A) \otimes \mathbb{Z}_\ell \to \mathrm{End}(T_\ell A)$ be the natural map. Then $\rho_{A,\ell}(\tau) = \iota_{A,\ell}(F \otimes 1)$. We denote this common image by f. Except in the case that $\ell = p$ and A has p-rank zero, $\mathrm{End}(T_\ell A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is a central simple division algebra of finite dimension over $\mathbb{Q}_\ell$, identified with $\iota_{A,\ell}(\mathrm{id}_A \otimes \mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. (In the exceptional case this ring is the zero ring.) Assume for now that $A[\ell](\bar{k}) \neq 0$. Then let $K_\ell := \mathbb{Q}_\ell(f) \subseteq \mathrm{End}(T_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. Let M_ℓ be a normal closure of K_ℓ. We define the *multiplicative rank of A at ℓ* to be zero if $\ell = p$ and $A[p](\bar{k}) = 0$ and the rank of the multiplicative subgroup of $M_\ell^\times$ generated by the conjugates of f over $\mathbb{Q}_\ell$ otherwise. Note that except in the case of $\ell = p$ and $A[p](\bar{k}) = 0$, the multiplicative rank is at least one since every eigenvalue of f has absolute value a positive power of p for each Euclidean norm so that f cannot be a root of unity.

Theorem 5 *Let A be a simple abelian variety defined over a finite field k of characteristic p. Let ℓ be a rational prime. Let r be the multiplicative rank of A at ℓ. If $r = 1$, then there is some $a \in \mathbb{N}$ and a field automorphism $\sigma \in \mathrm{Gal}(\bar{k}/k)$ such that the equation $\sigma(x) = [a]_A(x)$ defines a modular difference algebraic subgroup of A whose $(\bar{k}, \sigma)$-points contain $A[\ell^\infty]$. If $r > 2$, then there is no modular difference algebraic subgroup of A whose points include $A[\ell^\infty]$. If the ℓ-adic four exponentials conjecture holds, there is no such modular difference group in the case of $r = 2$ either.*

Proof: If $r = 1$, then for any conjugate f' of f over $\mathbb{Q}_\ell$ we have $f^n = (f')^m$ for some non-zero integers n and m, Since all the Euclidean absolute values of f are equal, we must have $n = m$. Thus, $f^n \in \mathbb{Q}_\ell$ for some $n \in \mathbb{Z}_+$. As f is integral over $\mathbb{Z}$, and thus *a fortiori* over $\mathbb{Z}_\ell$, actually $f^n \in \mathbb{Z}_\ell$. Arguing as in the proof of Theorem 2 we can find $\sigma \in \mathrm{Gal}(\bar{k}/k)$ and $a \in \mathbb{N} \setminus p$ such that σ acts as $x \mapsto [a]_A(x)$ on $A[\ell^\infty]$. We deduce modularity of the group defined by $\sigma(x) = [a]_A(x)$ either directly as in the proof of Proposition 3 replacing "α" in the bounds with the separable degree of $[a]_A$ or by the criterion of [C]: by the main theorem of [CHP] if this difference algebraic group were

not modular then it would be non-orthogonal to some fixed field of the form $\mathrm{Fix}(\sigma^\alpha\tau^\beta)$ with $\alpha > 0$. The analysis of [C] shows that for definable subgroups of abelian varieties this is only possible if over a difference closed field $(\mathcal{K},\sigma)$ the group $\{x \in A(\mathcal{K}) : \sigma(x) = [a]_A(x)$ and $\sigma^\alpha(x) = \tau^{-\beta}(x)\}$ is infinite. This group is contained in $A[F^\beta a^\alpha - 1](\bar{k})$ or $A[a^\alpha - F^{-\beta}](\bar{k})$ depending on whether or not $\beta \geq 0$. In either case, because a is not a power of p (and hence not a power of F in $\mathrm{End}_k(A)$), these groups are finite.

Now consider the case of $r \geq 2$. If there were some $\sigma \in \mathrm{Gal}(\bar{k}/k)$ and difference algebraic subgroup $\Gamma \leq A$ over $(\bar{k},\sigma)$ with $A[\ell^\infty] \leq \Gamma(\bar{k},\sigma)$, then by Proposition 1 we could find $P(X) \in \mathrm{End}_k(A)[X]$ such that $\ker P(\sigma)$ is modular and $A[\ell^\infty] \subseteq \ker P(\sigma)(\bar{k},\sigma)$. This implies that $\beta := \rho_{A,\ell}(\sigma)$ would have all algebraic eigenvalues on $T_\ell A$ and so would be an algebraic number when considered as an element of M_ℓ. Write $\sigma = \tau^\alpha$ for appropriate $\alpha \in \widehat{\mathbb{Z}}$. Then $\beta = f^{\alpha_\ell}$. Replacing f, σ, β with f^N, σ^N, and β^N for an appropriate $N \in \mathbb{Z}_+$ we may assume that f is ℓ-adically close to 1. Let $\omega_1, \ldots, \omega_r \in \mathrm{Gal}(M_\ell/\mathbb{Q}_\ell)$ such that $\omega_1(f), \ldots, \omega_r(f)$ are multiplicatively independent. Let $x_i := \log_\ell(\omega_i(f))$. Let $y_1 = 1$ and $y_2 := \alpha_\ell$. y_1 and y_2 are linearly independent over $\mathbb{Q}$ as long as $\alpha_\ell \notin \mathbb{Q}$ and by the choice of the ω_i's the x_i's are linearly independent over $\mathbb{Q}$. When $r > 2$, the ℓ-adic six exponentials theorem asserts that at least one of $\exp_\ell(x_i y_j)$ is transcendental over $\mathbb{Q}$ [La]. When $r = 2$, this assertion is the as yet unproven ℓ-adic four exponentials conjecture. Note that $\exp_\ell(x_i y_1) = \omega_i(f)$ is algebraic and because each ω_i is ℓ-adically continuous $\exp_\ell(x_i y_2) = \exp_\ell(\log_\ell(\omega_i(f))\alpha_\ell) = \omega_i(\exp_\ell(\log_\ell(f)\alpha_\ell)) = \omega_i(\beta)$ is also algebraic. So we must have $\alpha_\ell \in \mathbb{Q}$ (or $r = 2$ and the ℓ-adic four exponentials conjecture fails), say $\alpha_\ell = \frac{c}{d}$ with $c, d \in \mathbb{Z}$. Then the group $\{x \in A(\bar{k}) : \sigma^d(x) = F^c(x)\} = A(\mathrm{Fix}(\sigma^d\tau^{-c}))$ contains $A[\ell^\infty]$. As noted in the proof of Theorem 2, the group of points of a positive dimensional algebraic group over a fixed field can never be modular and a modular group can never have infinite intersection with a non-modular group so the assertion that $\ker P(\sigma)$ defines a modular group must be false. $\diamondsuit$

5. The additive group

While for semi-abelian varieties the torsion groups are all contained in m-torsion groups for some rational integer m, on the additive group $\mathbb{G}_a[m](\bar{k}) = 0$ or $\mathbb{G}_a(\bar{k})$ depending on whether or not $(p, m) = 1$. However, $\mathrm{End}_k(\mathbb{G}_a)$ is a very large ring being the ring of twisted

polynomials in F: $k\{F\} := \{\sum_{i=0}^{n} a_i F^i : a_i \in k, n \in \mathbb{N}\}$ where $Fa = a^p F$.

Theorem 6 *Let k be a finite field of characteristic p. Let Λ be a non-zero endomorphisms of $\mathbb{G}_a$ over k. For no field automorphism $\sigma \in \mathrm{Gal}(\bar{k}/k)$ and modular difference algebraic group $\Gamma \leq \mathbb{G}_a$ over $(\bar{k}, \sigma)$ does one have $\mathbb{G}_a[\Lambda^\infty] \leq \Gamma(\bar{k}, \sigma)$.*

Proof: $T_\Lambda \mathbb{G}_a$ is a finite rank module over $\mathbb{F}_p[[t]]$ where we allow t to act as Λ. So $\mathrm{Aut}(T_\Lambda \mathbb{G}_a)$ may be regarded as a subgroup of $\mathrm{GL}_r(\mathbb{F}_p[[t]])$ for $r = \mathrm{rk}_{\mathbb{F}_p[[t]]}(T_\Lambda \mathbb{G}_a)$. If $\sigma \in \mathrm{Gal}(\bar{k}/k)$ and $\Gamma \leq \mathbb{G}_a$ is a modular difference algebraic group whose $(\bar{k}, \sigma)$-points contain $\mathbb{G}_a[\Lambda^\infty]$, then σ satisfies a non-trivial equation on $T_\Lambda \mathbb{G}_a$ with co-efficients from $\mathrm{End}_k \mathbb{G}_a$ by Proposition 1. This implies that $\beta := \rho_{\mathbb{G}_a, \Lambda}(\sigma)$ (and also $\det(\beta) \in \mathbb{F}_p[[t]]$) would be algebraic over $\mathbb{F}_p[F]$ and hence over $\mathbb{F}_p(t)$. Write $\sigma = \tau^a$ for some $a \in \widehat{\mathbb{Z}}$. Then we have $\beta = F^{a_p}$. If $a_p \in \mathbb{Q}$, then Γ cannot be modular and contain $\mathbb{G}_a[\Lambda^\infty]$ for as in the case of abelian varieties some positive integral power, say c, of σ would agree with a Frobenius, say F^d, on $\mathbb{G}_a[\Lambda^\infty]$ so that $\Gamma(\bar{k}, \sigma) \cap \mathbb{G}_a(\mathrm{Fix}(\sigma^c \tau^{-d}))$ would be infinite contradicting modularity of Γ. However, if $a_p \notin \mathbb{Q}$, then by a theorem of Mendès France and van der Poorten [MFP], $\det(\beta)$ is transcendental over $F_p(t)$. ♢

6. Semi-abelian schemes over the Witt vectors

We wish to point out some consequences of our methods for semi-abelian schemes over the Witt vectors. If K is a field of characteristic $p > 0$, we denote by $W(K)$ the ring of (infinite length p-) Witt vectors over K, which has maximal ideal $pW(K)$ and residue field $W(K)/pW(K) \cong K$. We write $\bar{a}$ for the image in K of some $a \in W(K)$ under the quotient map. The group of continuous automorphisms of $W(K)$ is isomorphic to $\mathrm{Aut}(K)$ via the reduction map: $\sigma \mapsto \bar{\sigma} := (x \mapsto \bar{\sigma}(\widetilde{x}))$ where $\widetilde{x}$ is any lifting of x.

Theorem 7 *Let K be algebraically closed field of characteristic $p > 0$. Let $\sigma : W(K) \to W(K)$ be a continuous automorphism. Let G be a semi-abelian scheme over $W(K)$. Let $\widehat{G}$ denote the group of $pW(K)$-points of the formal group of G. Let $P(X) \in \mathbb{Z}[X]$ be a non-zero polynomial over $\mathbb{Z}$. Let $\Xi := \ker P(\sigma)(W(K), \sigma) \leq G(W(K))$ and let $\widehat{\Xi} := \Xi \cap \widehat{G}$. If $\mathrm{Fix}(\bar{\sigma})$ is finite, then Ξ is a finite rank $\mathbb{Z}_p$-module. If P reduces to a monomial modulo p, then Ξ is discrete.*

Proof: Since every non-zero integer acts as an isogeny of G, replacing P by P divided by the greatest common divisor of its co-efficients does not change the truth value of the statement of the theorem. So we assume from now on that the co-efficients of P have 1 as their greatest common divisor.

Since $\widehat{\Xi}$ is p-adically closed, preserved by $\mathbb{Z}$, and $\lim_{n\to\infty}[p^n]_G(x) = 0$ for any $x \in \widehat{\Xi}$, $\widehat{\Xi}$ is naturally a $\mathbb{Z}_p$-module. The issue is to calculate its rank

Let $\log_G : \widehat{G} \to \widehat{\mathbb{G}_a}^g(pW(K))$ be the formal logarithm of G (which converges on $\widehat{G}$) where $g = \dim G$. Let $\widehat{G}_n := \log_G^{-1}(p^nW(K))$. Then $\{\widehat{G}_n\}_{n=1}^{\infty}$ is an $\mathrm{Aut}(K)$-invariant filtration of $\widehat{G}$ and each quotient $\widehat{G}_n/\widehat{G}_{n+1}$ is naturally isomorphic to $\mathbb{G}_a(K)^g$.

Write $P(X) = \sum_{i=0}^n a_iX^i$. Then the equation $P(\sigma)(x) \in \widehat{G}_{n+1}$ on $\widehat{G}_n$ corresponds to the system of equations $\sum_{i=0}^n \bar{a}_i\bar{\sigma}^i(x_1) = 0, \ldots, \sum_{i=0}^n \bar{a}_i\bar{\sigma}(x_g) = 0$ on $\mathbb{G}_a(K)^g$. Since p does not divide all the co-efficients a_i, the equations $\sum_{i=0}^n \bar{a}_i\bar{\sigma}^i(x) = 0$ is a non-trivial linear difference equation over K. As such, its set of solutions is a vector space of dimension $d := \max\{i : \bar{a}_i \neq 0\} - \min\{i : \bar{a}_i \neq 0\} \leq n$ over $\mathrm{Fix}(\bar{\sigma})$. In particular, if $\mathrm{Fix}(\bar{\sigma})$ is finite, then the set of solutions to $\sum_{i=0}^n \bar{a}_i\bar{\sigma}^i(x) = 0$ is a vector space over $\mathbb{F}_p$ of dimension $r := d[\mathrm{Fix}(\bar{\sigma}) : \mathbb{F}_p]$.

We can realize $\widehat{\Xi}$ as $\varprojlim_{n\to\infty} \widehat{\Xi}/(\widehat{\Xi} \cap \widehat{G}_n)$ which by the above considerations is an inverse limit of groups expressible as iterated extensions of $(\mathbb{Z}/p\mathbb{Z})^{rg}$. From this it follows that $\widehat{\Xi}$ is a $\mathbb{Z}_p$ module of rank rg. ♢

We point out the special case when $\ker P(\sigma)$ is a modular group, for in that case the methods of [Sc1] (notably, Theorem 2.3 - the Hypotheses 1 and 3 there are included to ensure discreteness and Hypothesis 2 is equivalent to modularity) show that if $\Upsilon \leq \Xi$ is a discrete subgroup, then for any subvariety X of G there is a constant $c > 0$ such that for any $\xi \in \Upsilon$ either $\xi \in X$ or the p-adic distance from g to X is bounded below by c. Under the additional hypothesis that P reduces to a monomial modulo p we may take $\Upsilon = \Xi$.

References

[Bog] F. Bogomolov, Points of finite order on abelian varieties, *Izvestiya Akademii Nauk SSSR. Seriya Matematicheskaya* **44** (1980), no. 4, 782 – 804.

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

[C] Z. Chatzidakis, Groups definable in ACFA, **Algebraic Model Theory** (Toronto, 1996), Kluwer Acad. Publ., Dodrecht, 1997, pp. 25 – 52.

[CDM] Z. Chatzidakis, L. van den Dries, and A. Macintyre, Definable sets over finite fields, *Journal für die reine und angewandte Mathematik* **427** (1992), 107 – 135.

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

[CHP] Z. Chatzidakis, E. Hrushovski, and Y. Peterzil, The model theory of difference fields II, manuscript, 1998.

[Hi] M. Hindry, Points de torsion sur les sous-variétés de variétés abèliennes, *Comptes Rendus des Séances de l'Académie des Sciences. Série I. Mathématique*, **304** (1987), no. 12, 311 – 314.

[Hr] E. Hrushovski, The Manin-Mumford conjecture and the model theory of difference fields, manuscript, 1995.

[La] S. Lang, **Introduction to Transcendental Numbers**, Addison-Wesley, Reading, MA, 1966.

[MFP] M. Mendès France, A. J. van der Poorten, Automata and the arithmetic of formal power series, *Acta Arithmetica* **XLVI** (1986), pp. 211 – 214.

[Sc1] T. Scanlon, p-adic distance from torsion points of semi-abelian varieties, *Journal für die reine und angewandte Mathematik* **499** (1998), 225 – 236.

[Sc2] T. Scanlon, The absolute Mordell-Lang conjecture in positive characteristic, in preparation.