Difference subgroups of commutative algebraic groups over finite fields

Thomas Scanlon and José Felipe Voloch

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 field of characteristic zero and $\Gamma \subset G$ is a subgroup of "modular type", then for any subvariety $X \subset G$, $X \cap \Gamma$ is a finite union of cosets of subgroups of Γ (see [Ch]). Using such facts once can resolve diophantine questions about special subgroups of G (for instance, the torsion subgroup [Hr]). Recent work of Chatzidakis, Hrushovski and Peterzil [CHP] extends the class of difference fields for which this sort of result is known to positive characteristic. In this note, we analyze the subgroups of the torsion points of simple commutative algebraic groups over finite fields that can be constructed by such difference equations. Our results are reasonably complete modulo some well-known conjectures in Number Theory. In one case, we need the p-adic version of the four exponentials conjecture and in another we need a version of Artin's conjecture on primitive roots.

We recover part of a theorem of Boxall [Bo] on the intersection of varieties with the group of m-power torsion points, but in general this theorem does *not* follow from the model-theoretic analysis, because there may be no field automorphism σ so that the m-power torsion group is contained in a modular group definable with σ. On the other hand, some of the groups defined by modular difference equations are much larger than the group of m-power torsion points, so our results are stronger in another direction. In some ways, the model theoretic approach extends the approach of Bogomolov and the original one of Lang.

1. General set up

A difference ring (R, σ) is a commutative ring R with unity, together with an endomorphism σ of R. We define $\mathrm{Fix}(\sigma) = \{x \in R \mid \sigma(x) = x\}$, the subring of R fixed by σ. If X is a scheme over R we define X^σ to be $X \times_{\mathrm{Spec}\, R} \mathrm{Spec}\, R$, where we take $\sigma^* : \mathrm{Spec}\, R \to \mathrm{Spec}\, R$ to form the fiber product. Then σ induces a map on points $X(R) \to X^\sigma(R)$ again denoted by σ. If X is a group scheme then this map is a group homomorphism. If X is defined over $\mathrm{Fix}(\sigma)$ then we can identify X^σ with X.

When $G/\mathrm{Fix}(\sigma)$ is a commutative group scheme we let $\mathrm{End}_\sigma(G)$ denote the ring generated by $\sigma : G \to G$ and $\mathrm{End}(G)$, as a subgroup of the endomorphism ring of the functor that assigns to each difference ring containing $\mathrm{Fix}(\sigma), (R', \sigma)$, the group $G(R')$.

There is a homomorphism $\mathbf{Z}[T] \to \mathrm{End}_\sigma(G)$ sending T to σ. We denote by $P(\sigma)$ the image of $P(T) \in \mathbf{Z}[T]$ by this map.

Let p be a prime number. A p-Weil number is an algebraic number α all of whose archimedian absolute values are all equal to p^r for some rational number r. We usually omit the p, when it is clear from the context. A polynomial $P(T) \in \mathbf{Z}[T]$ will be called *modular* if none of its roots is a Weil number. The name modular is chosen to conform with the results of [CHP] asserting that when $P(T) \in \mathbf{Z}[T]$ is modular, then for any semiabelian variety $G/\mathrm{Fix}(\sigma)$, $\ker P(\sigma)$ is a group of modular type. On the other hand, if $P(T)$ has a Weil number as root, then $\ker P(\sigma)$ contains an infinite group commensurable with a group of the form $G(\mathrm{Fix}(\sigma^n F^m))$, for some n, m integers, where F is the Frobenius endomorphism $x \mapsto x^p$. The results of [CH] show that every commutative subgroup of a commutative algebraic group defined over a finite field definable in an existentially closed difference field is commensurable with a group of the form $\ker \Lambda$ where $\Lambda \in \mathrm{End}_\sigma(G)$. If G is a semi-abelian variety, then the groups $\ker \Lambda$ are contained in $\ker P(\sigma)$ for some non-zero $P(T) \in \mathbf{Z}[T]$.

Our main goal is to describe the groups of the form $\ker \Lambda(\bar{k}, \sigma)$, where G is a commutative algebraic group over a finite field k of characteristic p, σ is an element of the absolute Galois group of k, $\Lambda \in \mathrm{End}_\sigma(G)$, and $\ker \Lambda$ is of modular type over an existentially closed difference field. A slightly lower target is to characterize which "natural" subgroups of $G(\bar{k})$ are contained in some modular group. Here, "natural" means defined by some simple group-theoretic condition. In particular we will deal with the l-primary torsion of $G(\bar{k})$ for any prime l, or more generally, groups of the form $G_S = \{x \in G(\bar{k}) \mid mx = 0, m = \prod_{p \in S} p^{c_p}\}$, where S is some set of prime numbers. When S consists of a single prime, our results are complete.

If G is an algebraic group over a finite field k, then $G(\bar{k})$ is locally finite. So it is impossible that $G(\bar{k}) = \Gamma_1 \cdot \ldots \cdot \Gamma_n$, with each Γ_i modular, because $G(\bar{k})$ contains many subvarieties other than groups subvarieties while $\Gamma_1 \cdot \ldots \cdot \Gamma_n$ would be modular if each Γ_i were. This puts a restriction on S. In particular, if $S \cup S'$ is the set of all primes then one of $G_S, G_{S'}$ will not be contained in a modular group.

2. The multiplicative group

In analyzing the case of the multiplicative group $\mathbf{G}_m$ 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 $\mathbf{G}_m$, but as the rank of the endomorphism group of the algebraic group grows, so does the difficulty in solving these equations.

Theorem 1. *For any prime $\ell \neq p$, there exists $\sigma \in \mathrm{Gal}(\bar{\mathbf{F}}_p/\mathbf{F}_p)$ and $P(T) \in \mathbf{Z}[T]$ modular such that the ℓ-primary torsion subgroup of $\mathbf{G}_m$ is contained in $\ker P(\sigma)$.*

Proof: Consider the action of $\mathrm{Gal}(\bar{\mathbf{F}}_p/\mathbf{F}_p)$ on $T_\ell \mathbf{G}_m \cong \mathbf{Z}_\ell$. The image of $\mathrm{Gal}(\bar{\mathbf{F}}_p/\mathbf{F}_p)$ on $\mathrm{Aut}(T_\ell \mathbf{G}_m) \cong \mathbf{Z}_\ell^\times$ is the ℓ-adic closure of the group generated by p. If a is an integer in the ℓ-adic closure of the group generated by p, is not a Weil number (that is, is not an integral power of p), we take σ in the Galois group mapping to a and $P(T) = T - a$ and we will be done. Thus it is enough to show that such a exists. This is immediate. Since the ℓ-adic closure of the group generated by p is open, we can take a sufficiently close to 1 ℓ-adically, not a power of p and it will serve our purpose.

Let us investigate now for which sets S of primes, G_S is contained in $\ker \sigma - a$, for suitable σ and a. As in the proof of the theorem, for $\ell \in S$ we need to know if a is in the ℓ-adic closure of the group generated by p in $\mathbf{Z}_\ell$. According to Artin's conjecture on primitive roots, p should be a primitive root $\bmod \ell$ for a positive proportion of primes ℓ. Also, one expects that $p^{\ell-1} \not\equiv 1 (\bmod \ell^2)$ for most primes ℓ, therefore one expects that, for a positive proportion of primes ℓ the ℓ-adic closure of the group generated by p in $\mathbf{Z}_\ell$ is $\mathbf{Z}_\ell^\times$ and thus S can be taken to be a set of primes of positive density. Unfortunately, to prove this seems beyond the power of current techniques.

3. Simple Abelian Varieties

If A is a simple abelian variety over a finite field k then $\operatorname{End} A$ contains $\mathbf{Z}[F]$ as a subring where $F : A \to A$ is the Frobenius unless $A = 0$, which we tacitly exclude in the following. For each rational prime ℓ, we let $T_\ell A$ denote the Tate module of A and $\rho_\ell : \operatorname{Gal}(\bar{k}/k) \to \operatorname{Aut}_{\mathbf{Z}_\ell}(T_\ell A)$ the Galois action on the Tate module. Let $\iota_\ell : \operatorname{End}(A) \otimes \mathbf{Z}_\ell \to \operatorname{End}_{\mathbf{Z}_\ell}(T_\ell A)$ be the natural inclusion. When $\ell \neq p$, ι_ℓ is an isomorphism. If we let $f \in \operatorname{Gal}(\bar{k}/k)$ denote the Frobenius, then $\rho_\ell(F) = \iota_\ell(f \otimes 1)$. We will simply denote this common image by f.

Theorem 2. *Let A be a simple abelian variety defined over a finite field of characteristic p. Let ℓ be a rational prime and let r be the rank of the multiplicative subgroup of $\operatorname{Aut}_{\mathbf{Z}_\ell}(T_\ell)$ generated by the Galois conjugates of f over $\mathbf{Q}_\ell$. If $r \leq 1$ then the ℓ-primary torsion of A is contained in $\ker P(\sigma)$, for some $\sigma \in \operatorname{Gal}(\bar{\mathbf{F}}_p/\mathbf{F}_p)$ and $P(T) \in \mathbf{Z}[T]$ modular. If $r > 2$, then the ℓ-primary torsion of A is not contained in any such group and if $r = 2$ the same happens assuming the l-adic four-exponentials conjecture.*

Proof: The case of $r = 0$ is trivial. The case $r = 1$ is the same as the proof of Theorem 1, replacing p there by f. Assume now that $r \geq 2$. If there were some $\sigma \in \operatorname{Gal}(\bar{k}/k)$ and modular $P(T) \in \mathbf{Z}[T]$ with $\ker P(\sigma) \supseteq A(\bar{k})[\ell^\infty]$, then $\beta := \rho_\ell(\sigma)$ would have all algebraic eigenvalues on $T_\ell A$ and so would be an algebraic number when considered as an element of $\operatorname{End}(T_\ell A) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$. Write $\sigma = f^a$ where $a \in \hat{\mathbf{Z}}$. Then $\beta = f^{a_\ell}$ where a_ℓ is the image of a under the natural map $\hat{\mathbf{Z}} \to \mathbf{Z}_\ell$. Replacing f with f^N for an appropriate integer N, we may assume that f is ℓ-adically closed to 1. Let $\tau_1, \ldots, \tau_r$ be continuous ring automorphisms of $\mathrm{End}_{\mathbf{Z}_\ell}(T_\ell A) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$ such that $\tau_1(f), \ldots, \tau_r(f)$ are multiplicatively independent. Let $x_i := \log_\ell(\tau_i(f))$. Let $y_1 = 1$ and $y_2 = a_\ell$. If $a_\ell \notin \mathbf{Q}$, then y_1 and y_2 are linearly independent over $\mathbf{Q}$ and by the definition of r, the x_i's are linearly independent over $\mathbf{Q}$. When $r > 2$, the ℓ-adic six exponential theorem asserts that at least one of $\exp(x_i y_j)$ is transcendental [La]. When $r = 2$, this assertion is the ℓ-adic four exponentials conjecture. Note that $\exp(x_i y_1) = \tau_i(f)$ is algebraic and $\exp(x_i y_2) = \tau_i(\beta)$ is also algebraic, so if σ is to satisfy any nontrivial integral equation on the ℓ-primary torsion, it must be a rational power of the Frobenius, but then its eigenvalues must be p-Weil numbers, so it cannot satisfy a modular equation.

4. The additive group

While for semiabelian varieties, the torsion groups are all contained in nontrivial m-torsion groups for some rational integer m, on the additive group, $\mathbf{G}_a(\bar{k})[m] = 0$ or $\mathbf{G}_a(\bar{k})$ depending whether $(p, m) = 1$ or not. However, $\mathrm{End}_k \mathbf{G}_a$ is a very large ring being the ring of twisted polynomials over k in one variable: $k\{F\} := \{\sum_{i=0}^n a_i F : a_i \in k, n \in \mathbf{N}\}$ with the commutation rule $Fa = a^p F$. Let $\Lambda \in \mathrm{End}_k \mathbf{G}_a$. By the Λ-power torsion we mean the group $\mathbf{G}_a(\bar{k})[\Lambda^\infty] := \{x \in \mathbf{G}_a(\bar{k}) : \Lambda^n(x) = 0 \text{ for some } n \in \mathbf{Z}_+\}$.

Theorem 3. *Let k be a finite field and $\Lambda \in \mathrm{End}_k \mathbf{G}_a$ be an endomorphism of $\mathbf{G}_a$ over k with nontrivial kernel over $\bar{k}$. There is no field automorphism $\sigma \in \mathrm{Gal}(\bar{k}/k)$ and modular group defined by a difference equation involving σ containing the Λ-power torsion.*

Proof: It suffices to consider the case that Λ is irreducible over $\bar{k}$. The Λ-Tate module is a finite rank free $k[[\Lambda]]$-module and its continuous automorphism group is an order in a possibly skew finite extension of $k((\Lambda))$. Let f denote the image of the Frobenius in $\mathrm{End}_{cont} T_\Lambda \mathbf{G}_a$. If $\sigma \in \mathrm{Gal}(\bar{k}/k)$ satisfies any non-trivial equation over $\mathrm{End}\, \mathbf{G}_a$ on $\mathbf{G}_a(\bar{k})[\Lambda^\infty]$, then the image β of σ in $\mathrm{End}_{cont} T_\Lambda \mathbf{G}_a \otimes_{k[[\Lambda]]} k((\Lambda))$ would be algebraic over f and hence over $k((\Lambda))$. Write $\sigma = F^a$ with $a \in \hat{\mathbf{Z}}$. Then, $\beta = f^{a_p}$. If $a \in \mathbf{Q}$, then σ cannot satisfy a modular equation as on the maximal p extension of $\mathbf{F}_p$ some power of

σ would agree with a Frobenius and groups defined with a Frobenius are definable in the field language so are either finite or all of the additive group, but if $a \notin \mathbf{Q}$, then by a theorem of Mendès France and van der Poorten [MFvdP], β is transcendental.

5. Semiabelian varieties over the ring of Witt vectors

We wish to point out some consequences of our methods and results to semiabelian varieties over the ring of Witt vectors. Before doing that, we need to remain in the situation we had before and study difference equations on the additive group $\mathbf{G}_a$ over a finite field. Consider $\Gamma = \ker P(\sigma) \subset \mathbf{G}_a$, for some $\sigma \in \mathrm{Gal}(\bar{\mathbf{F}}_p/\mathbf{F}_p)$ and $P(T) \in \mathbf{F}_p[T]$. We may assume that $P(0) \neq 0$ and that $P(T)|(T^n - 1)$ for some n. Then, $\Gamma \subset \mathrm{Fix}(\sigma^n)$, and Γ is a vector space over $\mathrm{Fix}(\sigma)$. We thus conclude that Γ is finite if $\mathrm{Fix}(\sigma)$ is finite and is either 0 or infinite, otherwise.

Now let $W(\bar{\mathbf{F}}_p)$ be the ring of infinite Witt vectors over $\bar{\mathbf{F}}_p$ and $G/W(\bar{\mathbf{F}}_p)$ a semiabelian scheme. If $\sigma \in \mathrm{Gal}(\bar{\mathbf{F}}_p/\mathbf{F}_p)$ then σ acts on $W(\bar{\mathbf{F}}_p)$ and we consider $R = (W(\bar{\mathbf{F}}_p), \sigma)$ as our difference ring. Consider $\Gamma = \ker P(\sigma) \subset G$, for some $P(T) \in \mathbf{Z}[T]$. The exact sequence $0 \to \hat{G} \to G \to \bar{G} \to 0$, where $\hat{G}$ is the formal group of G and $\bar{G}$ is the special fibre of G, reduces the study of the properties of Γ to those of the image of $\Gamma, \bar{\Gamma}$ in $\bar{G}$ and of $\hat{\Gamma} = \Gamma \cap \hat{G}$. The group $\bar{\Gamma}$ is a group defined by a difference equation in a semiabelian variety over a finite field and thus the results of the previous sections apply. The group $\hat{\Gamma}$ is filtered by groups defined by difference equations on additive groups over a finite field, so the above remarks apply. In particular we get

Theorem 4. *Notation as above. If the fixed field of σ in $\bar{\mathbf{F}}_p$ is finite then $\hat{\Gamma}$ is a finitely generated $\mathbf{Z}_p$ module. If $P(T)$ reduces to a monomial modulo p, then $\hat{\Gamma} = 0$ and Γ is discrete.*

This follows easily from the above discussion. We point out the case of $\hat{\Gamma} = 0$ since the methods of [Sc] then yield that for any subvariety X of G, there exists $c > 0$ such that for any $g \in \Gamma$, either $g \in X$ or the p-adic distance from g to X is bounded below by c.

Acknowledgements: The authors would like to thank MSRI for the hospitality during the period that this work was carried out. The first author is supported by an NSF Postdoctoral Fellowship. The second author would like to thank the University of Texas's URI for financial support.

References.

[Bo] 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 Univ. Press, Cambridge, 1995.

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

[CH] Z. Chatzidakis and E. Hrushovski, *The model theory of difference fields*, preprint Universite Paris VII, July 1996.

[CHP] Z. Chatzidakis, E. Hrushovski, and Y. Peterzil, ACFA_p, in preparation, 1998.

[Hr] E. Hrushovski, *The Manin-Mumford conjecture and the model theory of difference fields*, manuscript, 1996.

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

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

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

MSRI, 1000 Centennial Drive, Berkeley, CA 94720, USA

email: `scanlon@msri.org`

Dept. of Mathematics, Univ. of Texas, Austin, TX 78712, USA

e-mail: `voloch@math.utexas.edu`