MODEL THEORY AND DIOPHANTINE GEOMETRY LECTURES 3, 4 AND 5

THOMAS SCANLON

Introduction

These notes continue the notes of Anand Pillay on model theory and diophantine geometry. In my lectures I describe a model theoretic approach to some analogues of the Mordell-Lang conjecture for Drinfeld modules. Many questions remain open and algebraic proofs along the lines of the proof of the Manin-Mumford conjecture described by Pillay may be possible. We discuss these questions and potential alternate approaches to these problems throughout these notes.

These notes are organized as follows. We begin in Section 1 with a discussion of the Mordell-Lang conjecture in its original form and some of its generalization. A discussion of Drinfeld modules and the Drinfeld module analogues of the the Mordell-Lang conjectures raised by Laurent Denis follows in Section 2. In Section 3 we discuss the general technique for proving Mordell-Lang type theorems by working with locally modular groups in enriched fields. In Section 5 we outline a weak solution to the the Drinfeld module Mordell-Lang conjecture proved using the model theory of separably closed fields. In Section 4 we prove the the Drinfeld module version of the Manin-Mumford conjecture using the model theory of difference fields. In Section 6 we end these notes with several open questions.

1. The Mordell-Lang conjecture

The Mordell-Lang conjecture and its proofs are the subject of several survey papers. The number theoretic approach to this conjecture is well exposed in the book [11] and the survey article [13]. The model theoretic approaches to these problems are described in the book [2] and the paper [19].

The Mordell-Lang conjecture concerns the structure induced on certain arithmetic subgroups of algebraic groups from the ambient algebraic variety.

As was pointed out in Pillay's notes [18], the model-theoretic approach to algebraic geometry tends to follow the Weil-style foundations in which varieties are identified with their set of points over a very large algebraically closed fields, morphisms are identified with the corresponding function on these sets points, *et cetera.* While there is much truth in this observation, we will not make such identifications in these notes. When we wish to apply facts about definable sets in certain enriched fields to prove results about varieties (or even schemes), we will explicitly describe the required interpretations.

Definition 1.1. The additive group scheme, $\mathbb{G}_a$, is the commutative group scheme whose corresponding functor of points $\mathbb{G}_a : \mathrm{Sch} \to \mathrm{Ab}$ is defined by $S \mapsto (\mathcal{O}_S, +)$.

Partially supported by NSF Grant DMS-0007190 and a Sloan Fellowship.

The additive group scheme, $\mathbb{G}_m$, is the commutative group scheme whose functor of points $\mathbb{G}_m : \mathrm{Sch} \to \mathrm{Ab}$ is given by $S \mapsto (\mathcal{O}_S^\times, \cdot)$.

Definition 1.2. Let K be a field. An *abelian variety* over K is a nontrivial, connected, complete algebraic group defined over K. An *algebraic torus* over K is an algebraic group T which when considered as an algebraic group over the algebraic closure K^{alg} of K is isomorphic to some Cartesian power of the multiplicative group. A *semi-abelian variety* over K is an algebraic group S which fits into an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & T \arrow[r] & S \arrow[r] & A \arrow[r] & 0 \end{tikzcd}$$

where T is an algebraic torus and A is an abelian variety.

The reader may wish to consult [16], [10], or [14] for more details about abelian varieties. We recall that every abelian variety admits a projective embedding. So, we could have defined an abelian variety to be a projective, connected algebraic group. If $K = \mathbb{C}$ and A is an algebraic group over K, then A is an abelian variety if and only if $A(\mathbb{C})$ is a compact, connected Lie group, or equivalently, isomorphic as a Lie group to a Cartesian power of circle groups.

Using the above isomorphism, it is easy to see that for a semiabelian variety S over $\mathbb{C}$ and a positive integer n, the n-torsion group

$$S[n](\mathbb{C}) := \{x \in S(\mathbb{C}) \mid [n]_S(x) = 0\}$$

is isomorphic (as a group) to $(\mathbb{Z}/n\mathbb{Z})^{t+2a}$ where $t = \dim T$ is the dimension of the toric part of S and $a = \dim A$ is the dimension of the abelian part. Moreover, the full torsion group

$$S(\mathbb{C})_{\mathrm{tor}} := \{x \in S(\mathbb{C}) \mid (\exists n \in \mathbb{Z}_+)[n]_S(x) = 0\}$$

is dense (in the Zariski as well as the archimedian topologies) in $S(\mathbb{C})$.

These properties of the torsion groups of semiabelian varieties hold over other algebraically closed fields of characteristic zero, and in a revised form, over all algebraically closed fields. In characteristic zero, one can use the fact that the theory of algebraically closed fields of characteristic zero is complete to pass from $\mathbb{C}$ to general algebraically closed fields of characteristic zero generally. Alternatively, one can develop a purely algebraic theory of abelian varieties which applies equally well to abelian varieties over fields of positive characteristic.

The arithmetic of abelian varieties is instrumental in understanding the diophantine geometry of curves and other higher dimensional varieties. Given an algebraic curve C over some field K, there is an associated abelian variety J (called the Jacobian of C). Given the additional datum of a K-rational point $P \in C(K)$, provided that the genus of C is positive, one obtains an embedding $C \hookrightarrow J$ defined over K. We denote the embedded curve by C as well. In this way, one may identify the set of K-rational points on C with the intersection of the K^{alg}-points on C with the group of K-rational points on J. This may not seem like much of a reduction until one sees that whenever K is a finitely generated field and A is an abelian variety over K, the group $A(K)$ is a finitely generated abelian group. Consequently, in order to understand the structure of rational points on curves over finitely generated fields, one need only understand intersections of finitely generated subgroups of abelian varieties with curves over algeraically closed fields.

The Mordell-Lang conjecture grew out of these considerations, but gives a stronger conclusion than merely what the structure of rational points on curves is. We recall that if Γ is an abelian group, then the *(rational) rank of* Γ is $\mathrm{rk}(\Gamma) := \dim_{\mathbb{Q}}(\Gamma \otimes \mathbb{Q})$.

Theorem 1.3 (Mordell-Lang conjecture)**.** *Let S be a semiabelian variety over $\mathbb{C}$ and let $\Gamma < S(\mathbb{C})$ be a subgroup of the $\mathbb{C}$-points of S having finite rational rank. If $X \subseteq S$ is a subvariety, then $X(\mathbb{C}) \cap \Gamma$ is a finite union of cosets of subgroups of Γ.*

Theorem 1.3 as stated above is due to McQuillan, though the main case of Γ finitely generated was proved by Faltings. Various other people (including, but not limited to, Vojta, Lang, and Raynaud) made deep contributions to its solution. The special case of $\mathrm{rk}\Gamma = 0$ goes by the name of the Manin-Mumford conjecture and its proof is the topic of Pillay's second lecture. Characteristic p versions of the Mordell-Lang conjecture are known, but in this case one must make allowances in some way for varieties defined over finite fields. Our aim is to transpose this problem to Drinfeld modules.

2. Drinfeld modules

In this section we introduce the theory of Drinfeld modules and Denis' Mordell-Lang-like conjectures for Drinfeld modules. The main reference for this section is [6]. We treat Drinfeld modules as analogues of elliptic curves, emphasizing their algebraic, as opposed to their analytic, theory.

If S is a semi-abelian variety over a field K, then the ring of algebraic endomorphisms of S defined over K, $\mathrm{End}_K(S)$, is a finitely generated ring. In particular, regardless of the size of K, the ring $\mathrm{End}_K(S)$ is countable. This fact does not hold for arbitrary commutative algebraic groups. For example, if R is any commutative ring, then for each $\lambda \in R$ scalar multiplication by λ defines an algebraic endomorphism of the additive group. If K is a field of characteristic zero, then one may identify $\mathrm{End}_K \mathbb{G}_a$ with K. This is not the case in positive characteristic.

If R is a commutative ring of characteristic $p > 0$, then the map $\tau : R \to R$ given by $x \mapsto x^p$ is a ring endomorphism of R. (We write τ for this p-power Frobenius morphism on all rings of characteristic p.) Moreover, this Frobenius map gives an algebraic endomorphism of the additive group over R. As such, polynomials in τ over R give algebraic endomorphisms of the additive group.

Definition 2.1. Let R be a ring and $\sigma : R \to R$ a ring endomorphism. We define the ring of linear σ-operators over R to be the simple ring extension $R\{\sigma\} = \{\sum_{i=0}^{d} a_i \tau^i : a_i \in R\}$ subject to the commutation conditions $\sigma a = \sigma(a)\sigma$ for $a \in R$.

While each element of $R\{\tau\}$ may be naturally regarded as an additive map on R, it is more than that. Each $\phi \in R\{\tau\}$ may be identified with a morphism of algebraic groups $\phi : \mathbb{G}_a \to \mathbb{G}_a$. As such, we have a map $R\{\tau\} \to \mathrm{End}(\mathbb{G}_{a/R})$ which is actually an isomorphism between the twisted polynomial ring in τ over R and the ring of algebraic endomorphisms of the additive group defined over R.

A Drinfeld module may be regarded as a choice of a finitely generated subring of exotic algebraic endomorphisms of the additive group.

Definition 2.2. Let K be a field of characteristic p. A Drinfeld module over K (for $\mathbb{F}_p[t]$) is a homomorphism $\varphi : \mathbb{F}_p[t] \to \mathrm{End}_K(\mathbb{G}_a) = K\{\tau\}$ for which $\varphi(t)$ is not a scalar. That is, if we write $\varphi(t) = \sum_{i=0}^{d} a_i \tau^i$, then $a_i \neq 0$ for some $i > 0$.

For many purposes, one requires a more general definition of a Drinfeld module than what we have in Definition 2.2. There are technical advantages to working with more general rings than just $\mathbb{F}_p[t]$ in our proof of the Drinfeld module version of the Manin-Mumford conjecture. The applications of Drinfeld modules to positive characteristic class field theory rely heavily upon these generalizations.

Notation 2.3. Let q be a power of the prime p. Let C be an absolutely irreducible curve over $\mathbb{F}_q$. Let $\infty \in C$ be a closed point on C. Let $C' := C \setminus \{\infty\}$ be the open curve obtained by removing ∞ from C. We denote by $\mathbf{A}$ the ring of regular functions on C'. We denote by $\mathbf{K}$ the field of rational functions on C, the field of fractions of $\mathbf{A}$.

Taking $q = p$, $C := \mathbb{P}^1$ the projective line over $\mathbb{F}_p$, and $\infty \in C$ the point at infinity on $\mathbb{P}^1$, we obtain $C' = \mathbb{A}^1_{/\mathbb{F}_p}$ and $\mathbf{A} \cong \mathbb{F}_p[t]$.

With $\mathbf{A}$ fixed, we have our general notion of a Drinfeld module.

Definition 2.4. Let K be a field of characteristic p. A Drinfeld module over K (for $\mathbf{A}$) is a ring homomorphism $\varphi : \mathbf{A} \to \mathrm{End}_K \mathbb{G}_a$ whose image is not contained in the ring of scalars. That is, there is some $a \in \mathbf{A}$ for which if we write $\varphi(a) = \sum_{i=0}^d \alpha_i \tau^i \in K\{\tau\}$, then $\alpha_i \neq 0$ for some $i > 0$.

For $a \in \mathbf{A}$ we write φ_a for $\varphi(a)$ considered as an endomorphism of $\mathbb{G}_a$.

A Drinfeld module gives the additive group an exotic $\mathbf{A}$-module structure. That is, if R is a K-algebra, then we may regard R as an $\mathbf{A}$-module via $a * x := \varphi_a(x)$ for $a \in \mathbf{A}$ and $x \in R$. Via the diagonal action, we may regard any Cartesian power ${\mathbb{G}_a}^g$ of the additive group as an $\mathbf{A}$-module.

We define now the notion of a morphism between Drinfeld modules.

Definition 2.5. If φ and ψ are two Drinfeld modules over the field K, then the group of homomorphisms from φ to ψ over K is

$$\mathrm{Hom}_K(\varphi, \psi) := \{\alpha \in \mathrm{End}_K \mathbb{G}_a \mid (\forall a \in \mathbf{A}) \alpha \circ \varphi_a = \psi_a\}$$

If $\psi = \varphi$, then we write

$$\mathrm{End}_K(\varphi) = \mathrm{Hom}_K(\varphi, \varphi)$$

for the endomorphism ring of φ.

For a general Drinfeld module φ, the endomorphism $\mathrm{End}_K(\varphi)$ is a finitely generated ring. The endomorphism ring $\mathrm{End}_K(\varphi)$ is commutative for φ of *generic characteristic.*

Definition 2.6. Let $\varphi : \mathbf{A} \to K\{\tau\}$ be a Drinfeld module. Let $\pi : K\{\tau\} \to K\{\tau\}/(\tau) \cong K$ be the quotient map modulo the two-sided ideal generated by τ. Set $\iota := \pi \circ \varphi : \mathbf{A} \to K$. We define the *characteristic* of φ to be the ideal $\ker \iota$. We say that φ has *generic characteristic* when the characteristic is (0) and that φ has *finite characteristic* otherwise.

When $\varphi : \mathbf{A} \to \mathbb{F}_{p^n}\{\tau\}$ is a Drinfeld module over a finite field, then necessarily φ has finite characteristic $\mathfrak{p}$ (as the image of ι is a subring of $\mathbb{F}_{p^n}$). Moreover, as τ^n commutes with every element of $\mathbb{F}_{p^n}\{\tau\}$ we see that $\tau^n \in \mathrm{End}_{\mathbb{F}_{p^n}}(\varphi)$. As the endomorphism ring is integral over $\mathbf{A}$, we see that τ^n satisfies an integral equation over $\mathbf{A}$. Write the minimal polynomial of τ^n over $\mathbf{A}$ as $P_n(X) \in \mathbf{A}[X]$. An analogue of Weil conjectures is known for the roots of P_n.

Suppose that the image of the Drinfeld module $\varphi : \mathbf{A} \to K\{\tau\}$ is actually contained in $R\{\tau\}$ for some subring $R \subseteq K$ of K. If $\nu : R \to R'$ is any homomorphism, then ν extends to a map $R\{\tau\} \to R'\{\tau\}$. Composing φ with this map we obtain a morphism $\overline{\varphi} : \mathbf{A} \to R'\{\tau\}$. In the case that R' is a field, we actually have a new Drinfeld module.

Suppose now that R' is a domain. Let $\mathfrak{P} := \ker \nu$ be the kernel of ν. Let $\mathfrak{p}$ be the characteristic of $\overline{\varphi}$. Then we say that φ has *good reduction* at $\mathfrak{P}$ if for each $a \in \mathbf{A}$ the degree of φ_a as a polynomial in τ is the same as that of $\overline{\varphi}_a$. The set of primes of good reduction is a dense Zariski open subset of the spectrum of R.

Definition 2.7. Let $\varphi : \mathbf{A} \to K\{\tau\}$ be a Drinfeld module. For $a \in \mathbf{A}$ we define $\varphi[a] := \ker \varphi_a$. For $I \subseteq \mathbf{A}$ an ideal we define the *prime-to-I torsion of φ in R* to be $\varphi_{I'-\mathrm{tor}}(R) := \bigcup_{a \in \mathbf{A} \setminus I} \varphi[a](R)$.

The map $\nu : R \to R'$ induces a natural map $\varphi_{\mathfrak{p}'-\mathrm{tor}}(R) \to \overline{\varphi}_{\mathfrak{p}'-\mathrm{tor}}(R')$. Under the hypothesis that φ has good reduction at $\mathfrak{p}$, this map must be injective.

The analytic theory of Drinfeld modules is developed in analogy with the analytic theory of elliptic curve. Let $\mathbf{K}_\infty$ be the completion with respect to the ∞-adic topology of $\mathbf{K}$. Let $\mathbb{C}_\infty$ be the completion of the algebraic closure of $\mathbf{K}_\infty$. The valued field $\mathbb{C}_\infty$ plays the rôle of $\mathbb{C}$. If $\varphi : \mathbf{A} \to \mathbb{C}_\infty\{\tau\}$ is a Drinfeld module over $\mathbb{C}_\infty$ of generic characteristic, then one can find a power series $f \in \mathbb{C}_\infty[[X]]$ such that $f(x)$ converges for every $x \in \mathbb{C}_\infty$, f defines a surjective additive function from $\mathbb{C}_\infty$ to itself, and $f(ax) = \varphi_a(f(x))$ for all $a \in \mathbf{A}$ and $x \in \mathbb{C}_\infty$.

Building on the analogy between Drinfeld modules and elliptic curves, L. Denis raised a conjecture for Drinfeld modules based on the Mordell-Lang conjecture.

Conjecture 2.8 (Denis)**.** *Let K be an algebraically closed field of characteristic p. Let $\varphi : \mathbf{A} \to \mathrm{End}_K \mathbb{G}_a$ be a Drinfeld module of generic characteristic. Let $\Gamma \leq \mathbb{G}_a(K)$ be an $\mathbf{A}$-submodule of $\mathbb{G}_a(K)$ with $\dim_{\mathbf{K}}(\Gamma \otimes_{\mathbf{A}} \mathbf{K}) < \infty$. If $X \subseteq {\mathbb{G}_a}^g$ is a subvariety of some Cartesian power of the additive group, then $X(K) \cap \Gamma^g$ is a finite union of cosets of $\mathbf{A}$-submodules of Γ^g.*

Conjecture 2.8 is still open, but we shall outline proofs of a special case (the analogue of the Manin-Mumford conjecture) and of a slightly different version of the case for finitely generated $\mathbf{A}$-modules.

We discuss the Drinfeld module version of the Manin-Mumford conjecture in Section 4.

Theorem 2.9 (Drinfeld module Manin-Mumford)**.** *Let K be an algebraically closed field of characteristic p. Let $\varphi : \mathbf{A} \to \mathrm{End}_K \mathbb{G}_a$ be a Drinfeld module of generic characteristic. Let $\Gamma := \varphi_{\mathrm{tor}} := \{x \in \mathbb{G}_a(K) \mid (\exists a \in \mathbf{A} \setminus \{0\}) \varphi_a(x) = 0\}$ be the module of $\mathbf{A}$-torsion. Let $X \subseteq {\mathbb{G}_a}^g$ be a subvariety of some Cartesian power of the additive group. Then $X(K) \cap \Gamma^g$ is a finite union of cosets of $\mathbf{A}$-submodules of Γ^g.*

We had proposed a version of Conjecture 2.8 as a project for this Winter School, but as Dragos Ghioca has pointed out, what I had thought was the missing algebraic lemma is actually contained in the Ph.D. thesis of Thomas Blossier [1]. We outline a proof of this version of the conjecture in Section 5. This proof leaves open even the case of Conjecture 2.8 for Γ a finitely generated $\mathbf{A}$-module. We discuss the open problems and the revised project in Section 6. In any case, let us state the main theorem to be proved there.

Theorem 2.10. *Let K be an algebraically closed field of characteristic p. Let $\varphi : \mathbf{A} \to \mathrm{End}_K \mathbb{G}_a$ be a Drinfeld module of* finite *characteristic. Suppose, moreover, that φ has generic moduli in the sense that for no $\lambda \in K^\times$ does $\lambda \varphi \lambda^{-1}$ take values in $\mathrm{End}_{\mathbb{F}_p^{\mathrm{alg}}} \mathbb{G}_a$. Let $\Gamma \leq \mathbb{G}_a(K)$ be a finitely generated $\mathbf{A}$-module. Then, if $X \subseteq {\mathbb{G}_a}^g$ is a subvariety of some Cartesian power of the additive group, $X(K) \cap \Gamma^g$ is a finite union of cosets of subgroups of Γ^g.*

3. General strategy via locally modular groups

Our proofs of Theorems 2.9 and 2.10 follow the methods developed by Hrushovski in his proofs of the Manin-Mumford conjecture [8] and the function field Mordell-Lang conjecture [9]. We find some expansion of the theory of fields and definable groups in those expansions for which the induced structure on these definable groups reflects the induced structure on the arithemtically defined group Γ. The auxilliary theories differ (ACFA for Theorem 2.9 and SCF for 2.10), but the general ideas are the same.

Suppose that we wish to prove something like Theorem 2.10. The group Γ itself may not lend itself to direct geometric arguments. However, by working in some field $\mathbb{U}$ extending K and some expansion of the language of rings, we might find some definable group $\widetilde{\Gamma} \leq S(\mathbb{U})$ with $\Gamma \leq \widetilde{\Gamma}$ with the property that for any variety X the intersection $X(\mathbb{U}) \cap \widetilde{\Gamma}$ is a finite union of cosets of subgroups of Γ. It would then follow that Γ has the same property.

The truth of Theorem 2.10 implies that one could take $K = \mathbb{U}$ and expand the language of rings by a predicate for Γ taking $\widetilde{\Gamma} = \Gamma$. Of course, such an argument would be circular. So, if one wishes to apply this technique to prove a nontrivial theorem, one must find appropriate enriched fields and groups $\widetilde{\Gamma}$ definable in these expansions for which one can prove the characteristic property (that $X(\mathbb{U}) \cap \widetilde{\Gamma}$ is a finite union of cosets of subgroups of $\widetilde{\Gamma}$ for each variety X).

The specific expansions that have been used in such proofs all fit under the rubric of $\mathcal{D}$-fields.

3.1. $\mathcal{D}$-rings.

The abstract notion of a $\mathcal{D}$-ring subsumes the notions of difference and differential rings while including some exotic structures. The notion of a $\mathcal{D}$-ring is associated to that of a $\mathcal{D}$-functor.

Definition 3.1. Fix a commutative ring k. A $\mathcal{D}$-functor over k is a projective system of ring schemes $\{\pi_{\ell,n} : \mathcal{D}_\ell \to \mathcal{D}_n\}_{0 \leq n \leq \ell}$ over k whose additive groups $\{\mathbb{G}_a(\pi_{\ell,n}) : \mathbb{G}_a \circ \mathcal{D}_\ell \to \mathbb{G}_a \circ \mathcal{D}_n\}$ form a projective system of unipotent algebraic groups over k and such that $\mathcal{D}_0$ is the identity fuctor.

We denote the pro-ring scheme $\varprojlim \mathcal{D}_n$ by $\widehat{\mathcal{D}}$.

Our defintion of a $\mathcal{D}$-functor is a bit abstract. Let us instantiate with our basic examples.

Example 3.2. Define $\mathcal{D}_n : \mathrm{Ring} \to \mathrm{Ring}$ by $\mathcal{D}_n(R) := R^{n+1}$ with $\pi_{\ell,n} : \mathcal{D}_\ell \to \mathcal{D}_n$ defined to be the projection onto the first $n+1$ coordinates.

Example 3.3. Let $e > 0$ be a positive integer. Define $\mathcal{D}_n : \mathrm{Ring} \to \mathrm{Ring}$ by $\mathcal{D}_n(R) := R[\epsilon_1, \ldots, \epsilon_e]/(\epsilon_1, \ldots, \epsilon_e)^{n+1}$ and $\pi_{\ell,n} : \mathcal{D}_\ell \to \mathcal{D}_n$ as the reduction modulo $(\epsilon_1, \ldots, \epsilon_e)^{n+1}$ map. Taking $\{\prod_{i=1}^e \epsilon_i^{j_i} : 0 \leq j_i \leq n\}$ as a basis for $\mathcal{D}_n(R)$ over R, we obtain an isomorphism $\nu_n : \mathbb{G}_a \circ \mathcal{D}_n \to {\mathbb{G}_a}^{e(n+1)}$.

In the above examples one may work over $\mathbb{Z}$. In the next example, we work over a polynomial ring in positive characteristic.

Example 3.4. Let $e > 0$ be a positive integer. Let $k := \mathbb{F}_p[t_1, \ldots, t_e]$ be the polynomial ring in e indeterminates over the field of p elements. For $n \in \mathbb{N}$ a natural number and R a k-algebra, we set $\mathcal{D}_n(R) := R \otimes_k \mathbb{F}_p[t_1^{p^{-n}}, \ldots, t_e^{p^{-n}}]$. We take the maps $\pi_{n+\ell,n} : \mathcal{D}_{n+\ell} \to \mathcal{D}_n$ in the projective system to be τ^ℓ.

Given a $\mathcal{D}$-functor we has an associated notion of a $\mathcal{D}$-ring.

Definition 3.5. Fix k a commutative ring and $\{\mathcal{D}_n\}_{n=0}^\infty$ a $\mathcal{D}$-functor over k. A *$\mathcal{D}$-ring* is a k-algebra R given together with a section $D : R \to \widehat{\mathcal{D}}(R)$ of the projection map $\pi : \widehat{\mathcal{D}}(R) \to \mathcal{D}_0(R) = R$.

Given a natural transformation $\Psi : \mathcal{D} \to \mathcal{D} \circ \mathcal{D}$, we say that the the $\mathcal{D}$-ring (R, D) is *(Ψ)-iterative* if the following diagram is commutative.

$$\begin{tikzcd}
R \arrow[r, "D"] \arrow[d, "D"'] & \widehat{\mathcal{D}}(R) \arrow[d, "\widehat{\mathcal{D}}(D)"] \\
\widehat{\mathcal{D}}(R) \arrow[r, "\Psi"'] & \widehat{\mathcal{D}}(\widehat{\mathcal{D}}(R))
\end{tikzcd}$$

As each $\mathbb{G}_a \circ \mathcal{D}_n$ is unipotent, we may choose coordinates identifying the underlying scheme of $\mathcal{D}_n$ with some affine space $\mathbb{A}^{m_n}$. We may thus express D as a sequence $\langle D_{n,i} : 0 \leq n, 1 \leq i \leq m_n \rangle$ of function $D_{n,i} : R \to R$. Likewise, the natural transformation $\Psi : \mathcal{D} \to \mathcal{D} \circ \mathcal{D}$ may be expressed in terms of a coherent system of additive polynomials. The condition that $D = \langle D_{n,i} \rangle$ defines a the structure of a $\mathcal{D}$-ring on R then translates into equations of the form

- $D_{n,i}(1) = c_{n,i}$ for appropriate constants $c_{n,i}$,
- $D_{n,i}(x+y) = A_{n,i}(D_{n,1}(x), \ldots, D_{n,m_n}(x); D_{n,1}(y), \ldots, D_{n,m_n}(y))$ for some polynomial $A_{n,i}$, and
- $D_{n,i}(x \cdot y) = P_{n,i}(\vec{D(x)}, \vec{D(y)})$ for an appropriate polynomial P_i, and
- $D_{n,i}(x) = \pi_{\ell,n;i}(D_{\ell,1}(x), \ldots, D_{\ell,m_\ell}(x))$ where $\pi_{\ell,n;i}$ is the i^{th} coordinate of map $\pi_{\ell,n} : \mathcal{D}_\ell \to \mathcal{D}_n$ considered in coordinates.

If the ground ring k has characteristic zero, then the condition that D be Ψ-iterative translates into the additional assertion that $D_{n,i} \circ D_{\ell,j}(x)$ is some particular k-linear combination of $\langle D_{s,t}(x) \rangle$. When k has characteristic p, one might have to allow for a $k\{\tau\}$-linear combination.

Let us consider now what the associated notions of $\mathcal{D}$-rings are for our above examples.

Example 3.6. In Example 3.2, a $\mathcal{D}$-ring is just a ring R given together with a sequence of endomorphisms $D_i : R \to R$. If we define $\Psi : \widehat{\mathcal{D}} \to \widehat{\mathcal{D}} \circ \widehat{\mathcal{D}}$ by $\langle x_i \rangle_{i=0}^\infty \mapsto \langle \langle x_{i+j} \rangle_{i=0}^\infty \rangle_{j=0}^\infty$, then this $\mathcal{D}$ structure is iterative if and only if $D_i = D_1^i$ for every i.

Example 3.7. In Example 3.3, a $\mathcal{D}$-ring is just a ring R given together with e stacks of commuting Hasse derivations. If R is a $\mathbb{Q}$-algebra, then such a structure is determined by specifying e commuting derivations $\partial_i : R \to R$ and defining $D : R \to \widehat{\mathcal{D}}(R) = R[[\epsilon_1, \ldots, \epsilon_e]]$ by

$$r \mapsto \sum_{\alpha_1,\ldots,\alpha_e=0}^{\infty} \frac{1}{\alpha_1! \cdots \alpha_e!} \partial_1^{\alpha_1} \cdots \partial_e^{\alpha_e}(r) \epsilon_1^{\alpha_1} \cdots \epsilon_e^{\alpha_e}$$

In any case, we write $D_\alpha(x)$ for the coefficient of ϵ^α in $D(x)$.

If we regard $\widehat{\mathcal{D}} \circ \widehat{\mathcal{D}}(R)$ as $R[[\epsilon_1, \ldots, \epsilon_e]][[\delta_1, \ldots, \delta_e]]$, then we may define $\Psi : \widehat{\mathcal{D}} \to \widehat{\mathcal{D}} \circ \widehat{\mathcal{D}}$ via the continuous map of R-algebras $R[[\eta_1, \ldots, \eta_e]] \to R[[\epsilon_1, \ldots, \epsilon_e; \delta_1, \ldots, \delta_e]]$ which sends η_i to $(\epsilon_i + \delta_i)$. Then, the $\mathcal{D}$-ring is iterative just in case $D_\alpha \circ D_\beta = \binom{\alpha+\beta}{\alpha} D_{\alpha+\beta}$ for all multi-indices α and β.

Example 3.8. Consider now Example 3.4. We may write $\mathcal{D}_n(R)$ as

$$\oplus_{j_1,\ldots,j_e=0}^{p^n-1} R(1 \otimes \prod_{i=0}^{p^n-1} t_i^{j_i p^{-n}})$$

Let (R, D) be a $\mathcal{D}$-ring. Write $D_n(x) = \sum_I D_{n,I}(x)(\sqrt[p^n]{t})^I$. As $D_n : R \to \mathcal{D}_n(R)$ is a section of $\tau^n : \mathcal{D}_n(R) \to R$, we have $x = \sum_I [D_{n,I}(x)]^{p^n} t^I$. We obtain a map $\Psi : \widehat{\mathcal{D}} \to \widehat{\mathcal{D}} \circ \widehat{\mathcal{D}}$ from the k-linear maps $k^{p^{-(n+m)}} \to k^{p^{-n}} \otimes_k k^{p^{-m}}$ defined on the basis element $\prod t_i^{j_i p^{-(n+m)}}$ as $(\prod t_i^{j_i p^{-n}}) \otimes (\prod t_i^{j_i p^{-m}})$.

Associated to each of these notions of a $\mathcal{D}$-ring, there is a theory of $\mathcal{D}$-rings.

Fix a $\mathcal{D}$-functor $\langle \mathcal{D}_n \rangle_{n=0}^{\infty}$ (over some ring k). Fix also isomorphisms $\mathcal{D}_n \cong \mathbb{A}^{m_n}$ and a natural trasformation $\Psi : \widehat{\mathcal{D}} \to \widehat{\mathcal{D}} \circ \widehat{\mathcal{D}}$. The language of $\mathcal{D}$-rings, $\mathcal{L}_{\mathcal{D}}$, is the language of rings $\mathcal{L}(+, \times, 0, 1)$ augmented by unary function symbols $\alpha \cdot$ (scalar multiplication by α for each $\alpha \in k$) and $D_{n,i}$ for each $n \in \mathbb{N}$ and $i \leq m_n$. Given a $\mathcal{D}$-ring (R, D), there is a natural way to put a $\mathcal{L}_{\mathcal{D}}$-structure on R. The theory of $\mathcal{D}$-fields, $T_{\mathcal{D}}$, is the the first-order theory of the class of interative $\mathcal{D}$-fields (K, D) in the language $\mathcal{L}_{\mathcal{D}}$.

We say that the $\mathcal{D}$-field (K, D) is $\mathcal{D}$-closed if it is existentially closed in the class of iterative $\mathcal{D}$-fields as an $\mathcal{L}_{\mathcal{D}}$-structure. In two of the cases considered above (provided that we take $k = \mathbb{Q}$), the class of $\mathcal{D}$-closed iterative $\mathcal{D}$-fields is first order axiomatizable, and has been intensively studied.

If $\mathcal{D}$ comes from Example 3.2, then the model companion of $T_{\mathcal{D}}$ is the theory of existentially closed diffence fields, ACFA, described in Pillay's lectures. Recall that a difference field (K, σ) is exististentially closed if and only if $K = K^{\mathrm{alg}}$, σ is an automorphism, and for any irreducible variety X over K, any irreducible subvariety $V \subseteq X \times X^\sigma$, and any dense Zariski open $U \subseteq V$, there is a point $a \in X(K)$ with $\langle a, \sigma(a) \rangle \in U(K)$.

If $\mathcal{D}$ comes from Example 3.3 (and $k = \mathbb{Q}$), then the model completion of $T_{\mathcal{D}}$ is (a definitional expansion of) the theory of differentially closed fields of characteristic zero with e commuting derivations. While this theory is central in algebraic model theory, it does not play a rôle in our work here.

If $\mathcal{D}$ comes from Example 3.4, then the framework of $\mathcal{D}$-fields is still valuable, but the most reasonable model complete theory in $\mathcal{L}_{\mathcal{D}}$ is that of separably closed fields having $t_1, \ldots, t_e$ as a p-basis (*ie* $[K : K^p] = p^e$ and $K = K^p(t_1, \ldots, t_e)$). We denote this theory by $\mathrm{SCF}_{p,e}$.

Associated to any iterative $\mathcal{D}$-ring (R, D) we have a $\mathcal{D}$-ring $R\langle X \rangle_{\mathcal{D}}$ of $\mathcal{D}$-polynomials over R. This ring is the universal simple iterative $\mathcal{D}$-ring extension of R and may be expressed as a quotient of the ordinary polynomial ring over R in the variables $D_{n,i}X$ for $n > 0$ and $0 < i \leq m_n$. Iterating this process, we obtain the $\mathcal{D}$-ring $R\langle X_1, \ldots, X_d\rangle_{\mathcal{D}}$ of $\mathcal{D}$-polynomials over R in d indeterminates. Each $f \in R\langle X_1, \ldots, X_d\rangle_{\mathcal{D}}$ may be expressed as an ordinary polynomial F in the variables $D_{n,i}X_j$ ($i \leq m_n$, $1 \leq j \leq d$) for an approproiate $n \geq 0$. If (R, D) is an iterative $\mathcal{D}$-field, then every quantifier-free formula in $\mathcal{L}_{\mathcal{D},R}$ is equivalent to a finite Boolean combination of $\mathcal{D}$-polynomial equations.

If $(R, D) \to (R', D)$ is a map of $\mathcal{D}$-rings and $a = \langle a_1, \ldots, a_n\rangle \in (R')^n$ is an n-tuple from R', then the the $\mathcal{D}$-ideal of a over R', $I(a/R')$, is the set $\{f \in R\langle X_1, \ldots, X_n\rangle : f(a) = 0\}$.

3.2. **Stability and simplicity.** Many of the model-theoretic tools used in our proofs of Theorems 2.9 and 2.10 come from the study of stable, and more generally simple, theories and the auxilliary theories we use, namely ACFA and SCF, are simple. In this section we survey some of the basic properties of and concepts for stable and simple theories. This treatment is by necessity very brief. You may wish to consult [12] or [22] for more details.

We start by recalling the notion of a type.

Definition 3.9. Let $\mathcal{L}$ be a first-order language, $\mathfrak{M}$ an $\mathcal{L}$-structure, $A \subseteq M$ a subset of the universe of $\mathfrak{M}$, and $b \in M^n$ an tuple of elements of M. Recall that $\mathcal{L}_A$ is the expansion of the language $\mathcal{L}$ by new constant symbols $\underline{a}$ for each $a \in A$. We regard $\mathfrak{M}$ as an $\mathcal{L}_A$-structure by interpreting $\underline{a}^{\mathfrak{M}} = a$. An *$n$-type over A* is a complete, consistent extension of the $\mathcal{L}_A$-theory of $\mathfrak{M}$ in the language $\mathcal{L}_A(x_1, \ldots, x_n)$. The set of all n-types over A is denoted by $S_n(A)$. The *type of b over A* is the set $\mathrm{tp}(b/A) := \{\phi(x_1, \ldots, x_n) \in \mathcal{L}_A(x_1, \ldots, x_n) : \mathfrak{M} \models \phi(b)\}$.

With the definition of type in place, we can give a quick definition of stability. However, the definition we present here is more useful for set theoretic problems (*ie* counting the number of models), than for the algebraic problems to which we wish to apply stability.

Definition 3.10. Let $\mathcal{L}$ be a first-order language, T an $\mathcal{L}$-theory, and κ an infinite cardinal. We say that T is κ-stable if for every model $\mathfrak{M} \models T$ with $|M| \leq \kappa$, we have $|S_1(M)| \leq \kappa$. We say that T is *stable* if it is κ-stable for some κ.

Example 3.11. Using quantifier elimination in the language of rings for algebraically closed fields, one shows that for $K = K^{\mathrm{alg}}$ an algebraically closed field there is a natural bijection between $S_n(K)$ and $\mathrm{Spec}(K[x_1, \ldots, x_n])$. In particular, as $\mathrm{Spec}(K[x]) = \{(0)\} \cup \{(x - a) : a \in K\}$, we have $|S_1(K)| = |K|$. That is, the theory of algebraically closed fields if κ-stable for every $\kappa \geq \aleph_0$.

Besides the set-theoretic aspect of stability, there are two key features of stable theories. First, in a stable theory, every type over a model is definable (formally: if $\mathfrak{M}$ is a model of a stable theory, $p(x) \in S_n(M)$ is a type over M, and $\phi(x_1, \ldots, x_n; y_1, \ldots, y_m)$ is an $\mathcal{L}$-formula, then the set $\{b \in M^m : \phi(x; b) \in p\}$ is definable by a formula in $\mathcal{L}_M$). Secondly, in a stable theory one can develop a good notion of independence generalizing linear independence in vector spaces and algebraic independence in fields. The definability of types is equivalent to stability, and to date, no good substitute for it is known in more general theories. If one gives too strong a definition of *good notion of independence*, then this aspect is also equivalent to stability. However, there are many other theories which possess an indepedence notion naturally generalizing the independence notion of stable theories. Simple theories fall into this class. We give the formal definition of simplicity and of independence now.

Definition 3.12. Let $\mathfrak{M}$ be an $\mathcal{L}$-structure for some first-order language $\mathcal{L}$. Let $A \subseteq M$ be a subset of the universe of $\mathfrak{M}$. Let $\phi(x_1, \ldots, x_n; y_1, \ldots, y_m)$ be an $\mathcal{L}$-formula and $b \in M^m$ an m-tuple from $\mathfrak{M}$. We say that $\phi(x; b)$ *divides over* A if there are a natural number k and an infinite sequence $\langle b_i \rangle_{i=0}^{\infty}$ of realizations of $\mathrm{tp}(b/A)$ (in some elementary extension $\mathfrak{N} \succeq \mathfrak{M}$) such that for any k-sequence $j_1 < \cdots < j_k$ of natural numbers we have $\mathfrak{N} \not\models (\exists x) \bigwedge_{i=1}^{k} \phi(x; b_{j_i})$.

We say that the partial type $\Sigma(x)$ *forks over* A if it implies a finite disjunction of formulas each of which divides over A.

Example 3.13. If $\phi(x_1, x_2; y)$ is the formula $x_2 = x_1 + y$ (in the language of abelian groups), $\mathfrak{M} = (\mathbb{Q}, +, 0)$ is the field of rational numbers considered as an additive group, and b is any nonzero element of $\mathbb{Q}$, then $\phi(x; b)$ divides over $\varnothing$.

Our independence notion is taken from forking.

Definition 3.14. Let $\mathfrak{M}$ be an $\mathcal{L}$-structure for some first-order language $\mathcal{L}$. Let $B \subseteq C \subseteq M$ and $B \subseteq A \subseteq M$ be subsets of the universe of $\mathfrak{M}$. We say that A *is free from* C *over* B if $\mathrm{tp}(A/C)$ does not fork over B.

We say that the $\mathcal{L}$-theory T is *simple* if for any model $\mathfrak{M} \models T$ and sets $B \subseteq A \subseteq M$ and $B \subseteq C \subseteq M$, if A is free from C over B, then C is free from A over B.

While it is not immediately obvious from the defintions we have given here, every stable theory is simple. Forking has a natural algebraic interpretation in the theories ACFA, DCF$_0$, and SCF. Let K be a model of one of these theories. For $B \subseteq A \subseteq K$ and $B \subseteq C \subseteq K$, A is free from C over B if and only if the algebraic closure of the $\mathcal{D}$-field generated by A is algebraically independent from the algebraic closure of the $\mathcal{D}$-field generated by C over the algebraic closure of the $\mathcal{D}$-field generated by B.

Simple theories come equipped with many dimension functions. We make particular use of Lascar (or U or SU) rank. This rank is defined as follows. Work inside a very saturated model of some theory. Take a a tuple and A a small subset. We always have $U(a/A) \geq 0$. For λ a limit ordinal we have $U(a/A) \geq \lambda \Leftrightarrow (\forall \alpha < \lambda) U(a/A) \geq \alpha$. Finally, $U(a/A) \geq \alpha + 1$ if and only if there is some set $B \supseteq A$ such that $\mathrm{tp}(a/B)$ forks over A and $U(a/B) \geq \alpha$.

In our applications, we work in cases where the U-rank is finite. In a $\mathcal{D}$-field, if $A = K$ is a $\mathcal{D}$-subfield, then $U(a/K) \leq \mathrm{tr.deg}_K(K\langle a \rangle)$ where $K\langle a \rangle$ is the $\mathcal{D}$-field generated by K and a.

We use U-rank to analyze groups. If $H \leq G$ is a definable subgroup of G and $U(H) = U(G) < \infty$, then H is of finite index in G. When G is a group of finite U-rank and $N \trianglelefteq G$ is a normal subgroup, then $U(G) = U(N) + U(G/N)$.

3.3. **Modular groups.** The relevance of stability theory to Mordell-Lang-type problems is seen through the theory of modular groups.

Definition 3.15. Let $\mathfrak{M}$ be an $\mathcal{L}$-structure for some first-order language $\mathcal{L}$. Let $G \subseteq M^n$ be a group living as a definable subset of some Cartesian power of M and having a definable group operation. Let $\Gamma \leq G$ be a subgroup of G (not necessarily definable!). We say that Γ is *modular* if for every natural number m

and every quantifier-free $\mathcal{L}_M$-definable subset of $X \subseteq G^m$ there is another set $Y \subseteq G^m$ which is a finite Boolean combination of definable subgroups of G^m such that $X \cap \Gamma^m = Y \cap \Gamma^m$.

Note that the set $Y \cap \Gamma^n$ of the above definition is itself a finite Boolean combination of cosets of subgroups of Γ^n.

Remark 3.16. Our use of the term *modular* is not standard. First, the term is usually reserved for definable, or at worst type-definable, groups. By expanding $\mathcal{L}$ with a predicate for Γ, we may regard Γ as definable. The second more serious difference is that we are considering only quantifier-free formulas while one usually asks that every definable subset of Γ^m be a finite Boolean combination of cosets. Thirdly, we work in a fixed structure $\mathfrak{M}$ rather than in the class of all elementarily equivalent structures. This distinction is relevant to issues of uniformity. Finally, the correct historical term would be *weakly normal group.* The term *modular* is derived from the theory of combinatorial geometries. In the case that G is a strongly minimal group, it is modular in the above sense if and only if its associated combinatorial pre-geometry is modular.

We note that Theorem 2.10 may be interpreted as asserting the modularity of Γ.

Proposition 3.17. *Let K be a field. Let G be an algebraic group over K. Let $\Gamma \leq G(K)$ be a subgroup of the K-rational points of G. Then Γ is modular if and only if for any variety $X \subseteq G^m$ defined over K the set $X(K) \cap \Gamma^m$ is a finite union of cosets of subgroups of Γ^m.*

Proof. The right-to-left implication is immediate.

The left-to-right implication is only slightly less immediate. Let $X \subseteq G^m$ be a subvariety of G^m. Noting that $X(K) \cap \Gamma^m = \overline{X(K) \cap \Gamma^m}(K) \cap \Gamma^m$, we may assume that X meets Γ^m in a Zariski dense set. Moreover, writing X as a finite union of its irreducible components, we may assume that X is irreducible.

Now, $X(K) \cap \Gamma^m$ is a quantifier-free definable subset of Γ^m so that by modularity of Γ, this set is a finite Boolean combination of subgroups of Γ^m. Write

$$X(K) \cap \Gamma^m = \bigcup_{j=1}^{d} [(a_j + H_j) \setminus (\bigcup_{i=1}^{m_j} b_{i,j} + M_{i,j})]$$

where for each j we have $H_j = \overline{H_j}(K) \cap \Gamma^n$, $\overline{H_j}$ is connected as an algebraic group, $\overline{M_{i,j}} < \overline{H_j}$ for each $i \leq m_n$, and $b_{i,j} + M_{i,j} \subseteq a_j + H_j$.

Let

$$Y_j := \overline{(a_j + H_j) \setminus (\bigcup_{i=1}^{m_j} b_{i,j} + M_{i,j})}$$

We claim that $Y_j = a_j + \overline{H_j}$ is a translate of an algebraic subgroup of G^n. To see this, choose any

$$h \in H_j \setminus \bigcup_{i,\ell=1}^{m_j} (a_i - a_\ell) + \sum_{k=1}^{m_j} M_{i,j}$$

Then

$$a_j + H_j = [(a_j + H_j) \setminus (\bigcup_{i=1}^{m_j} b_{i,j} + M_{i,j})] \cup h + [(a_j + H_j) \setminus (\bigcup_{i=1}^{m_j} b_{i,j} + M_{i,j})]$$

Thus, $a_j + \overline{H_j} = Y_j \cup (h + Y_j)$. As $\overline{H_j}$ is connected, either $Y_j = a_j + \overline{H_j}$ (as we claimed) or $Y_j = (a_j - h) + \overline{H_j} = a_j + [(-h) + \overline{H_j}] = a_j + \overline{H_j}$, again as we claimed.

As X is irreducible, we have $X = Y_j$ for some j. We compute $X(K) \cap \Gamma^m = Y_j(K) \cap \Gamma^m = (a_j + \overline{H_j}(K)) \cap \Gamma^m = a_j + (\overline{H_j}(K) \cap \Gamma^m)$ which is a coset of a subgroup of Γ^m. □

Remark 3.18. Using definablity of types in stable theories, one can derive a stronger version of Proposition 3.17 which itself implies automatic uniformity in such Mordell-Lang-type theorems (see [17, 8, 21]).

We are left with proving that the group Γ is modular. To do so we prove that some supergroup is modular.

Proposition 3.19. *Let $\Gamma \leq \widetilde{\Gamma} \leq G$ be subgroups of some definable group G. If $\widetilde{\Gamma}$ is modular, then Γ is also quantifier-free modular.*

Proof. Let $X \subseteq G^m$ be a quantifier-free definable set. By hypothesis, there is a set $Y \subseteq G^m$ which is a finite Boolean combination of cosets of definable subgroups such that $Y \cap \widetilde{\Gamma} = X \cap \widetilde{\Gamma}$. But then $X \cap \Gamma = (X \cap \widetilde{\Gamma}) \cap \Gamma = (Y \cap \widetilde{\Gamma}) \cap \Gamma = Y \cap \Gamma$. □

In our proofs of Theorems 2.9 and 2.10, we take $\widetilde{\Gamma}$ to be an appropriately chosen group definable in either ACFA or SCF. For these theories (and some others) there are tractable criteria for recognizing modular definable groups. These criteria are derived from the positive answer to Zilber's conjecture for these theories.

We state Zilber's conjecture in a form directly applicable to our problems. Before doing so we need another definition.

Definition 3.20. We say that the group G (type-definable in some some sufficiently saturated structure) is *c-minimal* if G is infinite, but every type-definable subgroup $H < G$ of infinite index must be finite.

Definition 3.21. Let T be a first-order theory. We say that the Zilber dichotomy holds for T if for every non-modular c-minimal group G type-definable in some (sufficiently saturated) model of T there is a type-definable field k, an algebraic group H over k, and a definable subgroup $\Psi \leq H(k) \times G$ for which the projection map (to either factor) restricted to Ψ has finite kernel and image of finite index.

Remark 3.22. The Zilber dichotomy is usually stated as a trichotomy for strongly minimal sets. Recall that a definable set X (in some sufficiently saturated structure) is *strongly minimal* if X is infinite but every definable subset of X is either finite or cofinite. Zilber had conjectured that every strongly minimal set falls into one of three mutually exclusive classes: trivial (every definable relation on X^n is reducible to binary relations), non-trivial locally modular (there is an interpretable modular group G and a definable finite-to-finite correspondence between G and X), or field-like (there is an interpretable algebraically closed field K and a finite-to-finite correspondence between K and X). The Zilber trichotomy fails in general, but (properly understood) it holds in the theories we consider here. Nevertheless, even in these cases this statement of the trichotomy is not immediately meaningful as there are no strongly minimal sets in either ACFA or SCF.

So, to prove that a group definable in some theory in which the Zilber dichotomy holds is modular, we show that the group has a decomposition series in terms of c-minimal groups each of which cannot be put into a finite-to-finite correspondence with the k-rational points of an algebraic group. That this suffices requires an extra argument and facts about the ambient theory (simplicity and weak elimination of quantifiers). The specific groups we consider are actually c-minimal so that this issue does not arise in our proofs, but you should be aware of it before attempting to generalize these arguments.

Conjecture 2.8 asserts more than merely the modularity of the group Γ. Specifically, it is conjectured that the quantifier-free definable sets in Γ^g must be translates of $\mathbf{A}$-modules. In general, one cannot recognize this property in the combinatorial geometry of the enveloping definable groups. However, we can reduce the issue to the study of subgroups of $\Gamma \times \Gamma$.

Proposition 3.23. *Let G be a c-minimal modular group. Assume that G has the property that every definable subgroup of some Cartesian power of G is of finite index in a quantifier-free definable group. Suppose that R is a (not necessarily commutative) subring of the ring of quantifier-free definable endomorphisms of G. Suppose, moreover, that every definable subgroup of G is commensurable with a R-module (in the sense that for every definable $H \leq G \times G$ there is some R-submodule $M \leq G \times G$ with $|H/(M \cap H)| < \aleph_0$ and $|M/(H \cap M)| < \aleph_0$), then every definable subgroup of every Cartesian power of G is commensurable with an R-module.*

4. Difference closed fields and the Drinfeld module Manin-Mumford conjecture

In this section we outline a proof of Theorem 2.9. Details of this proof are given in [20].

The proof breaks into several distinct parts. First, we find an existentially closed difference field $(\mathbb{U}, \sigma)$ with $K \leq \mathbb{U}$ and a definable group $\Gamma \leq \mathbb{G}_a(\mathbb{U})$ containing the torsion module and which stands a good chance of being modular. We then establish the modularity of Γ by mixing the main dichotomy theorem of [4] with results of Gekeler on Drinfeld modules over finite fields. If we were satisfied to show that every variety meets the torsion on ${\mathbb{G}_a}^g$ in a finite union of cosets, then we could stop here, but we wish to show that the cosets are actually translates of modules. To establish this, we mix some difference algebra with the analytic theory of Drinfeld modules to show that every quasi-endomorphism is a module, and then prove a general result on rank one groups to conclude the full result.

As Pillay suggests in his lectures, the techniques in his proof of Manin-Mumford probably apply to the case of this Drinfeld module version.

The proof of Theorem 2.9 begins very much like the proof of usual Manin-Mumford conjecture. We find a finitely generated ring $R \leq K$ for which the Drinfeld module $\varphi : \mathbf{A} \to K\{\tau\}$ factors through $R\{\tau\} \hookrightarrow K\{\tau\}$. We then find two maximal ideals $\mathfrak{P}, \mathfrak{Q} \subseteq R$ of good reduction for φ with $\mathfrak{p} := \iota^{-1}\mathfrak{P}$ and $\mathfrak{q} := \iota^{-1}\mathfrak{Q}$ coprime in $\mathbf{A}$. Write $\varphi_{\mathfrak{P}}$ for the reduction of φ at $\mathfrak{P}$ and $\varphi_{\mathfrak{Q}}$ for the reduction of φ at $\mathfrak{Q}$.

Let v be a valuation of K extending the $\mathfrak{P}$-adic valuation on the field of fractions of R and w a valuation extending the $\mathfrak{Q}$-adic valuation. Then it is not hard to see that prime-to-$\mathfrak{p}$ torsion submodule of the full torsion module consists entirely of v-unramified points. Moreover, as the w-unramified torsion contains the $\mathfrak{p}$-torsion, the full torsion group is contained in the sum of the v-unramified torsion and the w-unramified torsion.

Let $n := [R/\mathfrak{P} : \mathbb{F}_p]$ and $m := [R/\mathfrak{Q} : \mathbb{F}_p]$. Let $P(X) \in \mathbf{A}[X]$ be the minimal polynomial of τ^n considered as an element of $\mathrm{End}(\varphi_{\mathfrak{P}})$ and $Q(X) \in \mathbf{A}[X]$ the minimal polynomial of τ^m considered as an element of $\mathrm{End}(\varphi_{\mathfrak{Q}})$. If $\sigma \in \mathrm{Aut}(K/R)$ extends the relative (p^n-power) Frobenius on the maximal v-unramified extension of R, then $P(\sigma)$ vanishes on the v-unramified torsion. Likewise, if ρ extends the relative (p^m-power) Frobenius on the maximal w-unramified extension of R, then $Q(\rho)$ vanishes on the w-unramified torsion. Possibly at the cost of replacing R by a finite extension (and therefore n and m by some powers), we may find a single automorphism $\sigma : K \to K$ so that $P(\sigma) \circ Q(\sigma)$ vanishes on all of the torsion. We fix $(\mathbb{U}, \sigma)$ an extension of (K, σ) to a sufficiently saturated model of ACFA. We take $\widetilde{\Gamma} := \ker P(\sigma) \circ Q(\sigma) : \mathbb{G}_a(\mathbb{U}) \to \mathbb{G}_a(\mathbb{U})$.

We note that $\widetilde{\Gamma} = \ker P(\sigma)(\mathbb{U}) + \ker Q(\sigma)(\mathbb{U})$ so that it suffices to show that each summand is modular, c-minimal, and that every definable subgroup of its square is commensurable with an $\mathbf{A}$-module. The arguments that follow are insensitive to the differences between P and Q. We work with P, but everything follows *mutatis mutandis* for Q. To ease notation, write $\Xi := \ker P(\sigma)(\mathbb{U})$.

To prove modularity of Ξ, one first shows that Ξ has no proper infinite $\mathbf{A}$-submodules of infinite index. This fact is itself proved in steps. Working with prolongations, one shows that every definable $\mathbf{A}$-submodule of Ξ must be commensurable with a module defined by an equation of the form $R(\sigma) = 0$ for some $R \in \mathbf{A}[X]$. So, because P is irreducible, Ξ satisfies the conditions of c-minimality for $\mathbf{A}$-modules. To prove that Ξ is c-minimal it suffices to show that every infinite definable subgroup of Ξ is commensurable with an $\mathbf{A}$-module. For this one needs to work out the arithemetic of the ring $\mathbb{U}\{\tau\}[\sigma]$ and then apply some facts about the roots of P.

If Ξ is not modular, then the non-modularity of G is witnessed by a finite-to-finite definable correspondence between Ξ and the k-rational points of some algebraic group over some definable field k. Such fields are completely classified; they must take the form $\mathrm{Fix}(\sigma^i \tau^j) := \{x \in \mathbb{U} : \sigma^i(x^{p^j}) = x\}$ for some $i \in \mathbb{Z}_+$ and $j \in \mathbb{Z}$. Using this fact and the structure theorem for algebraic groups, one converts the existence of such a correspondence into a specific equation in the skew-field of quotients of $\mathbb{U}\{\tau\}$. Using facts about the roots of $P(X)$, one shows that such an equation cannot hold. Thus, Ξ is modular.

Using our general result about modular c-minimal groups, to finish the proof of the theorem, it suffices to show that every infinite quantifier-free definable subgroup of $\Upsilon \leq \Xi \times \Xi$ for which the projection in either direction has finite kernel is commensurable with an $\mathbf{A}$-module. This is done in several steps. First, one notes that any such group must be defined over algebraic closure of the fixed field of σ. Next, one notes that the algebraic points on Ξ are exactly the torsion points. Thus, after massaging Υ a bit, we see that Υ restricts to give a finite-to-finite correspondence on the torsion module. Working analytically, one sees that the commutator of Υ with φ_a (for $a \in \mathbf{A}$) (or of its converse relation) defines a contraction mapping ∞-adically close to the origin which takes torsion to torsion. For Galois-theoretic reasons this is seen to be impossible.

5. Separably closed fields and the Drinfeld module Mordell-Lang conjecture

In this section we outline a proof of Theorem 2.10. As we noted in the introduction, we had intended for theorem to be addressed as our associated project, but what we had thought was the missing algebraic lemma had actually been included in Thomas Blossier's thesis [1]. At the end of this section we discuss a revised version of the project.

Our proof of Theorem 2.10 follows along the lines of Hrushovski's proof of the positive characteristic function field Mordell-Lang theorem in [9].

We start by finding a finitely generated field $L \leq K$ be a finitely generated field for which the image of φ is contained in $\mathrm{End}_L \mathbb{G}_a$ and $\Gamma \leq \mathbb{G}_a(L)$.

Fix some $t \in \mathbf{A} \setminus \mathbb{F}_p^{\mathrm{alg}}$. We take $\mathbb{U}$ to be a saturated elementary extension of L^{sep} and define $\varphi^\sharp(\mathbb{U}) := \bigcap_{n \geq 0} \varphi_{t^n}(\mathbb{U})$.

Claim 5.1. *If $\varphi^\sharp(\mathbb{U})$ is modular, then Theorem 2.10 follows.*

Proof. It suffices to show that if X is an irreducible variety and $X(\mathbb{U}) \cap \Gamma^g$ is Zariski dense in X, then X is a translate of an algebraic group. Let X be a potential counterexample to this assertion. If $\varphi^\sharp(\mathbb{U})$ is modular, then it follows by the compactness theorem that there is a natural number n such that for any $a \in {\mathbb{G}_a}^g(\mathbb{U})$ the set $(X + a)(\mathbb{U}) \cap \varphi_{t^n}(\mathbb{U})^g$ is a finite union of cosets of subgroups of $\varphi_{t^n}(\mathbb{U})^g$. However, group Γ^g is contained in finitely cosets $C_1, \ldots, C_s$ of $\varphi_{t^n}(\mathbb{U})^g$. But then, $X(\mathbb{U}) \cap \Gamma^g = \bigcup (X(\mathbb{U}) \cap C_i) \cap \Gamma^g$. Each of the sets $X(\mathbb{U}) \cap C_i$ is a finite union of cosets. It follows that intersection with Γ^g has the same form. □

We wish to prove that $\varphi^\sharp(\mathbb{U})$ is modular by using an algebraic test for modularity. Such tests exist for *minimal* groups and we check now that $\varphi^\sharp(\mathbb{U})$ is minimal.

Claim 5.2. *$\varphi^\sharp(\mathbb{U})$ is a minimal group.*

Proof. Visibly, $\varphi^\sharp(\mathbb{U})$ is infinite, so it suffices to show that $U(\varphi^\sharp(\mathbb{U})) \leq 1$. Let $a \in \varphi^\sharp(\mathbb{U})$ be any point. Then, as a general result $U(a/L) \leq \mathrm{tr.deg}_L L\langle a \rangle$ where $L\langle a \rangle$ is the $\mathcal{D}$-field generated by a over L. By Lemma 2.15 of [9] (slightly modified) this last transcendence degree is bounded by one. □

The main result of [3] shows that if $G \leq \mathbb{G}_a(\mathbb{U})$ is a definable subgroup of the additive group, then either G is modular, or there is a definable isogeny $\alpha : G \to \mathbb{G}_a(\mathbb{U}^{p^\infty})$. Lemme 3.4.27 of [1] shows that if $\theta \in \tau\mathbb{U}\{\tau\}$ is an inseparable twisted polynomial in the Frobenius over $\mathbb{U}$ and $\theta^\sharp(\mathbb{U}) := \bigcap_{n \geq 0} \theta^n(\mathbb{U})$ is minimal, then either $\theta^\sharp(\mathbb{U})$ is modular, or there is some $\lambda \in \mathbb{U}^\times$ such that $\lambda\theta\lambda^{-1} \in \mathbb{U}^p\{\tau\}$. Using the saturation of $\mathbb{U}$, we may conclude from Blossier's lemma that either $\theta^\sharp(\mathbb{U})$ is modular or there is some $\lambda \in \mathbb{U}^\times$ such that $\lambda\theta\lambda^{-1} \in \mathbb{U}^{p^\infty}\{\tau\}$. Thus, if $\varphi^\sharp(\mathbb{U})$ is not modular, we may find some $\lambda \in \mathbb{U}^\times$ such that $\lambda\varphi_t\lambda^{-1} \in \mathbb{U}^{p^\infty}\{\tau\}$.

Claim 5.3. *We may find $\mu \in (L^{\mathrm{sep}})^\times$ so that $\mu\varphi_t\mu^{-1} \in \mathbb{F}_p^{\mathrm{alg}}\{\tau\}$.*

Proof. The main point is that if we expand the language of fields by a predicate for a subfield, then $(L^{\mathrm{alg}}, \mathbb{F}_p^{\mathrm{alg}}) \preceq (\mathbb{U}^{\mathrm{alg}}, \mathbb{U}^{p^\infty})$ is an elementary extension (see Proposition 7.7 of [15]). Writing $\varphi_t = \sum_{j=1}^d a_j \tau^j$ we have

$$(\mathbb{U}^{\mathrm{alg}}, \mathbb{U}^{p^\infty}) \models (\exists \lambda \neq 0) \lambda\varphi_t \bigwedge_{j=1}^{d} S(\lambda^{p^j - 1} a_j)$$

It follows that $(L^{\mathrm{alg}}, \mathbb{F}_p^{\mathrm{alg}})$ is a model of the same sentence witnessed by some $\mu \in L^{\mathrm{alg}}$. Choose $j \leq d$ with $a_j \neq 0$. Let $\mu_j := \mu^{p^j - 1} a_j \in (\mathbb{F}_p^{\mathrm{alg}})^\times$. The polynomial $X^{p^j - 1} - \mu_j a_j^{-1} \in L^{\mathrm{sep}}[X]$ is separable, so we actually have $\mu \in L^{\mathrm{sep}}$. □

With this claim we finish the proof as we had assumed that φ could not be conjugated to a Drinfeld module over a finite field.

6. Questions

Theorem 2.10 is related to Denis' conjecture, but it is incomplete in at least two ways. First, we have not shown that the groups which arise as intersections with varieties must be **A**-modules. Secondly, we have not directly addressed the problem raised in Denis' conjecture: the case of Drinfeld modules of generic characteristic. Our revised project concerns these extensions.

The issue of whether the exceptional groups must be **A**-modules is related to the more general question of the structure of the quasi-endomorphism rings of modular minimal groups in separably closed fields.

Question 6.1. *Let $K = K^{\mathrm{sep}}$ be a saturated separably closed field of characteristic p. Let $\phi \in \tau K\{\tau\} \setminus \{0\}$ be an inseparable polynomial in the Frobenius over K.) Let $\phi^\sharp(K) := \bigcap_{n \geq 0} \phi^n(K)$. Suppose that $\alpha \leq \phi^\sharp(K) \times \phi^\sharp(K)$ is a connected definable subgroup. Must there exist a positive integer n such that α commutes with ϕ^n?*

A positive answer to the following question could be instrumental in resolving Question 6.1.

Question 6.2. *Let K be a finitely generated field of characteristic p. Let $\varphi : \mathbf{A} \to K\{\tau\}$ be a Drinfeld module over K of finite characteristic. Let $a \in \mathbf{A}$ with $\varphi_a \in \tau K\{\tau\}$. Let $L := K^{\mathrm{sep}}$ be the separable closure of K. Suppose that $x \in \bigcap_{n \geq 0} \varphi_{a^n}(L)$. Is x necessarily an **A**-torsion point?*

Denis' Drinfeld module version of the Mordell-Lang conjecture remains open. However, Theorem 2.10 should imply a weak function-field version of Denis' conjecture.

Conjecture 6.3. *Let $K = K^{\mathrm{alg}}$ be an algebraically closed field of characteristic p. Let $\varphi : \mathbf{A} \to K\{\tau\}$ be a Drinfeld module over K. We assume that there does not exist $\lambda \in K^\times$ and $L \leq K$ a subfield of absolute transcendence degree ≤ 1 such that $\lambda^{-1}\varphi\lambda : \mathbf{A} \to L\{\tau\}$. Let $\Gamma \leq \mathbb{G}_a(K)$ be a finitely generate **A**-module. If $X \subseteq {\mathbb{G}_a}^g$ is a subvariety of some Cartesian power of the additive group, then $X(K) \cap \Gamma^g$ is a finite union of cosets of subgroups of Γ^g.*

I have in mind a reduction of Conjecture 6.3 to Theorem 2.10 based on a specialization of φ to a Drinfeld module of finite characteristic which does not descend to a finite field. Provided that one chooses the specialization so that it is injective on Γ, the conclusion should follow.

While the theories of specific kinds of $\mathcal{D}$-fields (difference fields, differential fields, separably closed fields, *et cetera*) have been studied extensively, the general theory has not been worked out.

Problem 6.4. *Study the model theory of $\mathcal{D}$-rings. Specifically,*

- *For which $\mathcal{D}$-functors does a model companion of the theory of $\mathcal{D}$-domains exist?*
- *Which of these theories are simple? stable?*
- *Describe the definable groups in these theories.*

References

[1] T. Blossier, Ensesmbles minimaux localement modulaires, PhD thesis, Paris VII, 2001.

[2] E. Bouscaren, Proof of the Mordell-Lang conjecture for function fields, **Model theory and algebraic geometry**, 177–196, Lecture Notes in Math., 1696, Springer, Berlin, 1998.

[3] E. Bouscaren and F. Delon, Minimal groups in separably closed fields, *J. Symbolic Logic* **67** (2002), no. 1, 239–259.

[4] Z. Chatzidakis, E. Hrushovski, and Y. Peterzil, Model theory of difference fields. II. Periodic ideals and the trichotomy in all characteristics, *Proc. London Math. Soc.* (3) **85** (2002), no. 2, 257–311.

[5] L. Denis, Géométrie diophantienne sur les modules de Drinfeld, **The arithmetic of function fields** (Columbus, OH, 1991), 285–302, Ohio State Univ. Math. Res. Inst. Publ., **2**, de Gruyter, Berlin, 1992.

[6] D. Goss, **Basic Structures of Function Field Arithmetic**, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), **35**, Springer-Verlag, Berlin, 1996.

[7] R. Hartshorne, **Algebraic Geometry**, Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.

[8] E. Hrushovski, The Mordell-Lang conjecture for function fields, *JAMS* **9** (1996), no. 3, 667–690.

[9] E. Hrushovski, The Manin-Mumford conjecture and the model theory of difference fields, *APAL* **112** (2001), no. 1, 43–115.

[10] S. Lang, **Abelian Varieties**, Interscience Tracts in Pure and Applied Mathematics, No. 7, Interscience Publishers, Inc., New York; Interscience Publishers Ltd., London, 1959.

[11] S. Lang, **Number Theory III: Diophantine geometry**, Encyclopaedia of Mathematical Sciences, **60**, Springer-Verlag, Berlin, 1991.

[12] D. Marker, **Model Theory: An introduction**, Graduate Texts in Mathematics, **217**, Springer-Verlag, New York, 2002.

[13] B. Mazur, Abelian varieties and the Mordell-Lang conjecture. **Model theory, algebra, and geometry**, 199–227, MSRI Publ., **39**, Cambridge Univ. Press, Cambridge, 2000.

[14] Milne, Abelian varieties, in **Arithmetic Geometry** (G. Cornell and J. Silverman, eds.) Springer-Verlag, New York, 1986.

[15] R. Moosa and T. Scanlon, *F*-structures and integral points on semiabelian varieties over finite fields, preprint, 2002.

[16] D. Mumford, **Abelian Varieties**, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research, Bombay; Oxford University Press, London, 1970.

[17] A. Pillay A. Pillay, The model theoretic content of the Lang's conjecture, in **Model Theory and Algebraic Geometry**, LNL **12**, (E. Bouscaren, ed.), 101–106, Springer, Berlin, 1998.

[18] A. Pillay, Lectures 1 and 2 of “Model Theory and Diophantine Geometry,” Arizona Winter School 2003.

[19] T. Scanlon, Diophantine geometry from model theory, *Bulletin of Symbolic Logic*, **7** (2001), no. 1, 37–57.

[20] T. Scanlon, Diophantine geometry of the torsion of a Drinfeld module, *J. Number Theory*, **97** (2002), no. 1, 10–25.

[21] T. Scanlon, Uniformity in the Mordell-Lang conjecture, e-print `math.LO/0105238`, 2001.

[22] F. Wagner, **Simple Theories**, Mathematics and its Applications, **503**, Kluwer Academic Publishers, Dordrecht, 2000.

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

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