THE BULLETIN OF SYMBOLIC LOGIC
Volume 7, Number 1, March 2001

DIOPHANTINE GEOMETRY FROM MODEL THEORY

THOMAS SCANLON

§1. Introduction. With Hrushovski's proof of the function field Mordell-Lang conjecture [16] the relevance of geometric stability theory to diophantine geometry first came to light. A gulf between logicians and number theorists allowed for contradictory reactions. It has been asserted that Hrushovski's proof was simply an algebraic argument masked in the language of model theory. Another camp held that this theorem was merely a clever one-off. Still others regarded the argument as magical and asked whether such sorcery could unlock the secrets of a wide coterie of number theoretic problems.

In the intervening years each of these prejudices has been revealed as false though such attitudes are still common. The methods pioneered in [16] have been extended and applied to a number of other problems. At their best, these methods have been integrated into the general methods for solving diophantine problems. Moreover, the newer work suggests limits to the application of model theory to diophantine geometry. For example, all such known applications are connected with commutative algebraic groups. This need not be an intrinsic restriction, but its removal requires serious advances in the model theory of fields.

The story of and the mathematics behind Hrushovski's proof have been explained well in many other fora (see, for example, [4, 17, 28]). I need to repeat parts of this material in order to tell the sequel, but the reader should consult these other sources for details. Mordell's conjecture has also been exposited well (see, for example [22]), but to ground the geometric problems described in this article in elementary algebra I repeat part of this story as well.

The plan of this article is as follows. I recall in section 2 some definitions from algebraic geometry and model theory. I recall in section 3 the Mordell-Lang conjecture. I recall in section 4 the theory of weakly normal groups and their relevance to Mordell-Lang-like problems. Also in this section I

Received August 31, 1998; revised October 17, 2000.
Partially supported by an NSF MSPRF.

1079-8986/01/0701-0002/$3.10

sketch a proof of the positive characteristic Manin-Mumford conjecture. I discuss in section 5 the theory of prolongations of definable sets in difference and differential fields indicating how this theory may be used to compute upper bounds for the number of solutions to various diophantine problems. I discuss in section 6 the theory of the semipluriminimal socle of a group of finite Morley rank and sketch how this theory has been used to prove some uniform finiteness theorems. I discuss in section 7 a general specialization argument which when combined with other methods may be used to prove results on diophantine approximations. I conclude in section 8 with some questions on extensions of these results and with some remarks on how these theorems have fed back into pure model theory.

I thank Daniel Lascar for soliciting this article. He requested it two years ago as a resume of my thesis [33]. I wrote a version of this article at that time, but I was unhappy with the result and hesitated to revise it. Daniel Lascar, through his gentle though persistent prodding, is largely responsible for this article finally being written. Of course, I alone am responsible for all errors of fact, style, taste, and judgment. I thank the referees and editors of this *Bulletin* for suggesting many improvements. I thank Ehud Hrushovski for correcting my history of the Mordell-Lang problem, but especially for his guidance during my graduate studies.

§**2. Background and notation.** In this section I recall some definitions and notation from algebraic geometry and model theory. The reader may wish to skim or skip this section and return only when encountering an unfamiliar term in the main text.

2.1. Background from algebraic geometry. The reader who desires more explanation could consult [11] or [12].

For the following definitions, I fix an uncountable algebraically closed field K and a subfield $k < K$. Denote by k^{alg} the algebraic closure of k. The definitions I give below would strike an algebraic geometer as too naïve, but they suffice for this article.

Definition 2.1. Let $N \in \mathbb{N}$ be a natural number. On $K^{N+1} \smallsetminus \{(0, \dots, 0)\}$ define an equivalence relation by

$$(x_0, \dots, x_N) \sim (y_0, \dots, y_N) \iff (\exists \lambda \in K^\times) \bigwedge_{i=0}^{N} \lambda x_i = y_i.$$

Projective N-space over K is defined as

$$\mathbb{P}^N(K) := (K^{N+1} \smallsetminus \{(0, \dots, 0)\})/\sim.$$

Denote by $[a_0 : \dots : a_N]$ the $\sim$-class of $(a_0, \dots, a_N) \in K^{N+1} \smallsetminus \{(0, \dots, 0)\}$. Define $\mathbb{P}^N(k)$ as the image of $k^{N+1} \smallsetminus \{(0, \dots, 0)\}$ under the quotient map.

Note that in the definition of the equivalence relation on $k^{N+1} \smallsetminus \{(0, \ldots, 0)\}$ it does not matter whether $\lambda \in K^\times$ or $\lambda \in k^\times$.

Definition 2.2. A polynomial $f(x_0, \ldots, x_N) \in K[x_0, \ldots, x_N]$ is *homogeneous of degree* $d \in \mathbb{N}$ if the identity $f(\lambda x_0, \ldots, \lambda x_N) = \lambda^d f(x_0, \ldots, x_N)$ holds in $K[x_0, \ldots, x_N, \lambda]$.

Note that the zero polynomial is homogeneous of every degree. Note also that while the value of a homogeneous polynomial is not constant on a $\sim$-class in general, if the value is zero at one point of the $\sim$-class, then it is zero at every point.

Definition 2.3. A *projective algebraic subvariety of* $\mathbb{P}^N(K)$ is a set $X(K) \subseteq \mathbb{P}^N(K)$ of the form

$$V(f_1, \ldots, f_m) := \left\{ [a_0 : \ldots : a_N] \in \mathbb{P}^N(K) : \bigwedge_{i=1}^{m} f_i(a_0, \ldots, a_N) = 0 \right\}$$

where $f_1, \ldots, f_m$ are homogeneous polynomials. The variety X is *defined over* k if the polynomials defining X may be chosen to have coefficients from k. We write $X(k) := X(K) \cap \mathbb{P}^N(k)$ for the k-rational points on X.

The notion of *defined over* given above is equivalent to the model theoretic version. There is a more refined algebro-geometric version involving the ideal of definition of X. This distinction can be important for positive characteristic fields.

Definition/Proposition 2.4. The projective algebraic subvarieties of $\mathbb{P}^N(K)$ are the closed sets of the *Zariski topology* on $\mathbb{P}^N(K)$. This topology is Noetherian and $\mathbb{P}^N(K)$ has dimension N. A connected projective algebraic variety of dimension one is called a projective algebraic curve.

Definition/Proposition 2.5. The *degree* of an irreducible projective variety $X(K) \subseteq \mathbb{P}^N(K)$ is defined to be $\deg(X)$, the maximal finite value of $|X(K) \cap L(K)|$ where L is defined by the simultaneous vanishing of $N - \dim(X)$ homogeneous polynomials of degree one.

If $X(K)$ is any projective variety, then its degree is defined to be the sum of the degrees of its irreducible components.

If X is defined by a single irreducible homogeneous polynomial, f, then $\deg(X) = \deg(f)$. More generally, if $X(K) = V(f_1, \ldots, f_n)$, $(f_1, \ldots, f_n) \subseteq K[x_0, \ldots, x_N]$ is prime, and $\dim(X) = N - n$, then $\deg(X) = \prod_{i=1}^{n} \deg(f_i)$.

Remark 2.6. When k is a topological field, $\mathbb{P}^N(k)$ carries another topology induced from the field topology on k via the quotient map. The Zariski topology is coarser than this other topology as long as the topology on k is T_1. When k is locally compact, $X(k)$ is compact whenever X is a projective algebraic variety.

Affine algebraic varieties, subsets of some Cartesian power of K defined by the simultaneous vanishing of a system of polynomial equations, may be more familiar to the reader. These varieties enter through the next definition.

DEFINITION 2.7. A *quasiprojective* variety is a (Zariski) relatively closed subset of some Zariski open subspace of a projective space.

The degree of a quasiprojective variety is defined to be the degree of its Zariski closure in the ambient projective space.

For example, affine N-space over K, $\mathbb{A}^N(K) := K^N$ may be identified with the quasiprojective variety $\mathbb{P}^N(K) \smallsetminus V(x_0)$ via $(a_1, \dots, a_N) \mapsto [1 : a_1 : \dots : a_N]$. More generally, if $X(K) \subseteq \mathbb{A}^N(K) \subseteq \mathbb{P}^N(K)$ is an affine algebraic variety, then it is a quasiprojective variety.

DEFINITION 2.8. An irreducible projective variety $X(K)$ which is given as the common zero set of the prime ideal $(f_1, \dots, f_m)$ generated by the homogeneous polynomials $f_1, \dots, f_m \in K[x_0, \dots, x_n]$ is *smooth at a point* $[a_0 : \dots : a_n] \in X(K)$ if the rank of the Jacobian matrix

$$\left\{ \frac{\partial f_i}{\partial x_j}(a_0, \dots, a_n) \right\}_{1 \le i \le m, 0 \le j \le n}$$

is $n - \dim(X)$. The variety $X(K)$ is *smooth* if it is smooth at every point.

While Definition 2.8 involves a choice of defining equations for X, smoothness is an intrinsic property of a variety and does not depend upon the choice of defining equations.

In the case that $K = \mathbb{C}$, a variety is smooth in the sense of algebraic geometry if and only if it is a complex analytic submanifold of the ambient projective space.

DEFINITION 2.9. A *rational function* $f : \mathbb{P}^N(K) \to \mathbb{P}^M(K)$ is a partial function of the form $[a_0 : \dots : a_N] \mapsto [f_0(a_0, \dots, a_N) : \dots : f_M(a_0, \dots, a_N)]$ where $f_0, \dots, f_M$ are homogeneous polynomials of the same degree and at least one of the polynomials is not the zero polynomial. If $X(K) \subseteq \mathbb{P}^N(K)$ and $Y(K) \subseteq \mathbb{P}^M(K)$ are quasiprojective subvarieties, then a rational function $f : X \to Y$ is a partial function which is the restriction of a rational function $\tilde{f}$ on $\mathbb{P}^N$ to X for which $\tilde{f}$ is defined at some point of each component of X and the image of $\tilde{f}$ on $X(K)$ is contained in $Y(K)$. The function f is called *regular* if it is defined at every point of $X(K)$.

DEFINITION 2.10. The connected varieties X and Y are *birationally equivalent* (or *birational*) if there are rational functions $f : X \to Y$ and $g : Y \to X$ so that $f \circ g$ and $g \circ f$ are defined and equal to the identity everywhere except possibly on a proper subvariety. These varieties are *biregularly equivalent* (or *biregular*) if f and g may be taken to be regular.

REMARK 2.11. What I have called "quasiprojective varieties" should properly be called "quasiprojective subvarieties of a projective space." One ought to regard biregular varieties as being the same variety.

REMARK 2.12. While it is not obvious from the definitions, the class of quasiprojective varieties is closed under products in that there is a natural way to regard the product of two projective spaces as a projective variety.

DEFINITION 2.13. An *algebraic group* is a group whose universe is a quasiprojective variety and whose group operations are given by regular functions. An *abelian variety* is a connected projective algebraic group.

2.2. Background from model theory. Most of the model theoretic terms used in this article are defined as they are introduced. In this section, I lay out my conventions and definitions of some peripheral terms.

NOTATION 2.14. If $\mathcal{M}$ is an $\mathcal{L}$-structure for some language $\mathcal{L}$, then I usually denote the universe of $\mathcal{M}$ by M. If $A \subseteq M$, then $\mathcal{L}_A$ denotes the expansion of $\mathcal{L}$ by constant symbols $\underline{a}$ for each $a \in A$. We regard $\mathcal{M}$ as an $\mathcal{L}_A$-structure by interpreting $\underline{a}$ as a. If $\Sigma(x_1, \dots, x_n) \subseteq \mathcal{L}_A(x_1, \dots, x_n)$ is a partial type (equivalently, consistent set of formulas) with free variables among $x_1, \dots, x_n$ then

$$\Sigma(\mathcal{M}) := \{ (a_1, \dots, a_n) \in M^n : \mathcal{M} \models \Sigma(a_1, \dots, a_n) \}.$$

Usually, I write a tuple as a single element. If $\Sigma = \{\varphi\}$ is a single formula, then $\varphi(\mathcal{M}) := \Sigma(\mathcal{M})$ is called an A-definable set. By a definable set, we mean an M-definable set.

DEFINITION 2.15. Let $\mathcal{M}$ be an $\mathcal{L}$-structure for some first-order language $\mathcal{L}$. If $A \subseteq M$ is a subset, then the *algebraic closure* of A is

$$\mathrm{acl}(A) := \{ b \in M : \exists \varphi(x) \in \mathcal{L}_A(x) \text{ with } \mathcal{M} \models \varphi(b) \text{ and } |\varphi(\mathcal{M})| < \aleph_0 \}.$$

Let me recall the definition of Morley rank.

DEFINITION 2.16. Let $\mathcal{M}$ be an $\mathcal{L}$-structure which is $\|\mathcal{L}\|^+$-saturated. For X a definable set in $\mathcal{M}$ we define the Morley rank of X, $\mathrm{RM}(X)$, to be the minimal ordinal (or $\pm\infty$) satisfying

- $\mathrm{RM}(\varnothing) = -\infty$.
- $\mathrm{RM}(X) \geq 0 \Leftrightarrow X \neq \varnothing$.
- $\mathrm{RM}(X) \geq \alpha + 1$ if and only if for every $n \in \mathbb{N}$ there are n disjoint definable subsets $X_i \subseteq X$ with $\mathrm{RM}(X_i) \geq \alpha$.
- $\mathrm{RM}(X) \geq \lambda$ for λ a limit ordinal if and only $\mathrm{RM}(X) \geq \alpha$ for all $\alpha < \lambda$.

The Morley degree of X, $\mathrm{dM}(X)$, is the maximal n such that there are n disjoint definable subsets of X each having the same Morley rank as X.

If $\mathcal{M}$ is a general $\mathcal{L}$-structure and X is a definable set defined by some formula $\varphi(x) \in \mathcal{L}_M(x)$, then we define $\mathrm{RM}(X) := \mathrm{RM}(\varphi(\mathcal{N}))$ and $\mathrm{dM}(X) := \mathrm{dM}(\varphi(\mathcal{N}))$ for $\mathcal{N} \succeq \mathcal{M}$ a sufficiently saturated elementary extension.

A definable set of Morley rank and Morley degree one is called *strongly minimal*.

We say that $\mathcal{M}$ *has finite rank* if $\mathrm{RM}(M) < \omega$.

DEFINITION 2.17. A group G considered as an $\mathcal{L}$-structure for some language $\mathcal{L}$ extending the language of groups is *connected* if it has no proper definable subgroup of finite index.

§3. From algebra to geometry: the Mordell-Lang conjecture. The problems and theorems described in this paper start with the Mordell-Lang conjecture. In principle, one could understand and, perhaps, even appreciate these problems without knowing the genesis of this line of mathematics, but someone ignorant of their connection to humbler algebraic problems might wrongly regard these problems as contrived. The Mordell-Lang conjecture proposes an elegant geometric solution to some of the most elementary and ancient of algebraic problems. The Mordell-Lang conjecture itself arose from the study of rational solutions to polynomial equations in two variables, but developed into a range of geometric questions.

By a diophantine problem one usually means something like

PROBLEM 3.1. *Given a system of algebraic equations* $\bigwedge_{i=1}^{m} f_i(x_1, \dots, x_n) = 0$ *with* $f_1, \dots, f_m \in \mathbb{Q}[x_1, \dots, x_n]$, *find all the solutions in* $\mathbb{Q}^n$.

A number of changes to the basic template of Problem 3.1 are allowed. For instance, $\mathbb{Q}$ might be replaced by some other commutative ring. The goal of "find all the solutions" may be replaced with a weaker desideratum such as a qualitative description of the set of solutions. The equations themselves might be replaced with some kind of inequality.

While these problems carry the name of Diophantus of Alexandria who first (among the authors of extant texts) systematically studied similar problems, it should be noted that, at least in the surviving portion of his *Arithmetica*, he dealt only with specific systems of equations of degree at most six and he contented himself with finding a solution rather than all of them.

As is well-known to the readers of this *Bulletin*, the general solution to Problem 3.1 with $\mathbb{Z}$ in place of $\mathbb{Q}$ is impossible to solve [23] and the problem with $\mathbb{Q}$ itself may be just as difficult. Thus, one cannot hope for a good solution to a diophantine problem unless the class of equations has been restricted or the meaning of "find" has been weakened.

The Mordell-Lang conjecture developed from the following diophantine problem.

PROBLEM 3.2. *Given a nonzero polynomial* $f(x, y) \in \mathbb{Q}[x, y]$ *in two variables with rational coefficients determine whether the set of rational solutions,* $\{ (a, b) \in \mathbb{Q}^2 : f(a, b) = 0 \}$ *is infinite.*

REMARK 3.3. There are a couple of minor issues (concerning elliptic curves) obstructing the proof of the decidability of Problem 3.2. If the question is changed to: *Is there a field K which is a finite algebraic extension of $\mathbb{Q}$ (a* number field*) and for which the set of K-rational solutions,* $\{(a,b) \in K^2 : f(a,b) = 0\}$, *is infinite?*, then Faltings' theorem [9] gives an easy decision procedure.

As observed by Dedekind and Weber as early as the 1880s, Problem 3.2 may be expressed algebro-geometrically. The equation $f(x,y) = 0$ defines a finite union of affine algebraic curves $C_1(\mathbb{C}), \dots, C_m(\mathbb{C})$ and a rational solution to $f(a,b) = 0$ defines a $\mathbb{Q}$-rational point on one of these curves. Thus, if there were infinitely many rational solutions to $f(a,b) = 0$, then $C_i(\mathbb{Q})$ would be infinite for some i. It follows on general grounds that such a curve must be defined over $\mathbb{Q}$.

Since an algebraic curve is connected and of dimension one, any rational function on a curve is defined at all but finitely many points. Thus, if C and C' are two birational curves both defined over $\mathbb{Q}$ with the rational transformations witnessing birationality also defined over $\mathbb{Q}$, then $C(\mathbb{Q})$ is infinite if and only if $C'(\mathbb{Q})$ is infinite. As a general principle, for any algebraic curve C, there is some birational smooth projective curve C' for which C' and the rational functions witnessing birationality are defined over the same field where C is defined. Thus, Problem 3.2 has the following algebro-geometric form.

PROBLEM 3.4. *Given a smooth projective curve C defined over $\mathbb{Q}$, determine whether $C(\mathbb{Q})$ is infinite.*

While Problem 3.4 is now phrased in the language of algebraic geometry it does not yet qualify as a geometric problem.

Poincaré observed that Problem 3.4 might be better posed in terms of curves embedded in abelian varieties rather than in arbitrary projective spaces. I remark that a smooth projective curve over $\mathbb{C}$ is a one-dimensional, connected, compact, complex manifold. That is, it is a Riemann surface. Such a space is topologically classified by its genus (the number of holes, or if you prefer a prefer a more rigorous definition, half of its first Betti number).

REMARK 3.5. There is a well-defined notion of geometric genus for a smooth projective curve over an arbitrary algebraically closed field, but the definition requires a foray into the theory of divisors or sheaf cohomology which I would prefer to avoid.

REMARK 3.6. The genus of a curve may be computed quite easily from the defining equations of the curve.

To a curve C of genus $g \geq 1$ there is a naturally associated g-dimensional abelian variety, J_C, called the Jacobian of C. Given any point $P_0 \in C(K)$ there is a regular function $\varphi_{P_0} \colon C(K) \to J_C(K)$ which is biregular onto its image and sends P_0 to 0. Moreover, if C and P_0 are defined over k, then so are J_C, the group structure on J_C, and the map φ_{P_0}.

Take now C as in the statement of Problem 3.4. If the genus of C is zero, then Poincaré's observation tells us nothing, but a decision procedure based on the decidability of real and p-adic fields and the so-called Hasse principle handles this case [22]. So we may now assume that the genus of C is at least one. If $C(\mathbb{Q})$ is infinite, then, in particular, it is not empty. Take $P_0 \in C(\mathbb{Q})$ and set $C'(\mathbb{C}) := \varphi_{P_0}(C(\mathbb{C}))$. Then $C(\mathbb{Q})$ is infinite if and only if $C'(\mathbb{Q}) = C'(\mathbb{C}) \cap J_C(\mathbb{Q})$ is infinite. Poincaré's observation yields the following reduction of Problem 3.4.

PROBLEM 3.7. *Given a smooth projective curve C of genus at least one embedded in its Jacobian over $\mathbb{Q}$, determine whether $C(\mathbb{Q})$ is infinite.*

The solution to Problem 3.7 seems to depend on an understanding of the group $J_C(\mathbb{Q})$. As a point of fact, neither Faltings' original proof nor Vojta's refined proof [40] of the Mordell conjecture actually used information about the group $J_C(\mathbb{Q})$. However, the line of reasoning I am developing here is essential for the theorems proved by model theoretic methods.

In his thesis [25], Mordell proved that for any Jacobian J_C over $\mathbb{Q}$, the abelian group $J_C(\mathbb{Q})$ is finitely generated. Weil generalized Mordell's theorem showing that for any finitely generated field k and any abelian variety A defined over k, the abelian group $A(k)$ is finitely generated.

These theorems bring us close to a resolution of Problem 3.7 for genus one curves and suggest the solution for higher genus curves.

A smooth curve of genus one embedded in its Jacobian J_C may be identified with that Jacobian. Thus, a curve of genus one has infinitely many rational points if and only if it has at least one rational point and its Jacobian has a rational point of infinite order. To my knowledge, these questions are not known to be decidable, but there are methods based on the widely believed Birch-Swinnerton-Dyer conjecture for answering them.

A curve of genus greater than one cannot carry the structure of an algebraic group. There are a number of ways to prove this fact. For example, a Riemann surface of genus greater than one has a nonabelian fundamental group. When working over an arbitrary field, this fact follows from universality properties of the Jacobian. However one proves this fact, it together with Weil's theorem strongly suggest that a curve C of genus greater than one over a finitely generated field k can have only finitely many k-rational points. This suggestion is wrong in positive characteristic, but it is correct for k of characteristic zero. Mordell's conjecture, slightly generalized beyond $\mathbb{Q}$, is the following.

CONJECTURE 3.8 (Theorem of Faltings [9]). *If C is a smooth projective curve of genus greater than one over a finitely generated field k of characteristic zero, then $C(k)$ is finite.*

Using Weil's theorem, Conjecture 3.8 may be reformulated without any reference to arithmetic fields.

CONJECTURE 3.9. *Let $A(\mathbb{C})$ be an abelian variety over the complex numbers. Let $X(\mathbb{C}) \subseteq A(\mathbb{C})$ be a smooth curve of genus greater than one. Let $\Gamma < A(\mathbb{C})$ be a finitely generated subgroup. Then, $X(\mathbb{C}) \cap \Gamma$ is finite.*

To put Conjecture 3.9 in a form amenable to model theory we need to generalize it beyond curves. Lang, observing that groups seem to be the only obstruction to the finiteness of the set of rational points on a variety, generalized Mordell's conjecture to the following form.

CONJECTURE 3.10. *Let $A(\mathbb{C})$ be an abelian variety over the complex numbers. Let $\Gamma < A(\mathbb{C})$ be a finitely generated group. If $X(\mathbb{C}) \subseteq A(\mathbb{C})$ is a subvariety of A, then the Zariski closure of $X(\mathbb{C}) \cap \Gamma$ is a finite union of translates of abelian subvarieties of A.*

This conjecture is also a theorem of Faltings' [10].

While there is no known model theoretic proof of 3.10, it is now stated in a form closely connected to current preoccupations in model theory. Coincidentally, one of the original model theorists, Thoralf Skolem, proved Conjecture 3.9 under the hypothesis that $\mathrm{rk}(\Gamma) < \dim A$ [38].

§4. From geometry to model theory: weakly normal groups. Conjecture 3.10 may be expressed in terms of the structure induced on the finitely generated group Γ. With the next definition I say precisely what is meant by induced structure.

DEFINITION 4.1. Let $\mathcal{M}$ be an $\mathcal{L}$-structure in some first-order language $\mathcal{L}$. Let $X \subseteq M^N$ be a (not necessarily definable) non-empty subset of some Cartesian power of M. The induced structure on X is the $\mathcal{L}'$-structure $\mathcal{X}$ defined by:

- The universe of $\mathcal{X}$ is X.
- For each formula $\varphi(x_1^1, \dots, x_1^N; \dots; x_m^1, \dots, x_m^N) \in \mathcal{L}\Big(\{x_i^j\}_{1 \le i \le m}^{1 \le j \le N}\Big)$ there is a basic m-ary relation $R_\varphi(y_1, \dots, y_m)$ in $\mathcal{L}'$ interpreted in $\mathcal{X}$ by $R_\varphi(\mathcal{X}) = X^m \cap \varphi(\mathcal{M})$.

REMARK 4.2. What I have called *induced structure* might more properly be termed *full induced structure*. One might prefer to fix some family of formulas $\Sigma \subseteq \mathcal{L}(\{x_i\}_{i \in \omega})$ and take for $\mathcal{L}'$ only those formulas R_φ with $\varphi \in \Sigma$.

Using quantifier elimination for $(\mathbb{C}, +, \cdot, 0, 1)$, Conjecture 3.10 may be expressed as "Every quantifier-free definable set for the induced structure on Γ is a finite Boolean combination of cosets of definable groups." Groups satisfying the hypothesis that all definable subsets of any Cartesian power are finite Boolean combinations of cosets of definable groups are called *weakly normal*. Using a quantifier elimination theorem for modules proven independently by Baur [2] and Monk [24] we have the following transformation of Conjecture 3.10.

CONJECTURE 4.3. *If $A(\mathbb{C})$ is a complex abelian variety and $\Gamma < A(\mathbb{C})$ is a finitely generated group, then the induced structure (from the language $\mathcal{L}_{\mathbb{C}}(+,\cdot)$) on Γ is weakly normal.*

We now have the Mordell-Lang conjecture in a model theoretic form, but how does this help? As I have oft mentioned, there is no known model-theoretic proof of Conjecture 4.3. Moreover, if one could show directly that the induced structure on Γ is weakly normal, then there would be little point in dressing up the argument in the robes of stability theory. The point is: there are a number of related questions for which an indirect stability theoretic analysis of auxiliary structures produces coherent solutions.

I note a simple observation which transports the goal of proving that Γ has weakly normal induced structure to the realm of possibility. If G is a weakly normal group, then the induced structure on any subgroup is also weakly normal. Thus, to prove that Γ in the statement of Conjecture 4.3 is weakly normal it suffices to find some intermediate group $\Gamma \leq \bar{\Gamma} < A(\mathbb{C})$ with $\bar{\Gamma}$ having weakly normal induced structure. In practice, one searches for $\bar{\Gamma}$ as a group definable in some expansion of the theory of fields in which there are transparent criteria for detecting the weak normality of definable groups. Alas, also in practice, the search for $\bar{\Gamma}$ seldom reveals such a group, but partial success together with some trickery sometimes suffices.

To illustrate this technique in a case not complicated by the failure mentioned in the previous sentence, let me sketch the proof of the positive characteristic Manin-Mumford conjecture. The Manin-Mumford conjecture proper deals with abelian varieties over fields of characteristic zero and was first proven by Raynaud [30]. A model-theoretic proof yielding better effective bounds is due to Hrushovski [15]. Taking the basic results of [7] as given, the proof of the positive characteristic Manin-Mumford conjecture is much easier than all the other theorems described in this paper.

PROPOSITION 4.4. *Let K be an algebraically closed field of positive characteristic. Let $A(K)$ be a sufficiently general abelian variety defined over K. Let $\Gamma := A(K)_{\text{tor}} := \{ a \in A(K) : \exists n \in \mathbb{Z}_{+} na = 0 \}$ be the torsion subgroup. Then the induced (from $\mathcal{L}_K(+,\cdot)$) structure on Γ is weakly normal.*

In the statement of Proposition 4.4 the phrase "sufficiently general" means that there is no positive dimensional abelian variety B defined over a finite field and a nonzero morphism of algebraic groups $\psi\colon B \to A$.

SKETCH OF PROOF. Using a bit of number theory, namely, the theories of very good reduction and of relative Frobenii, we make a good choice of a field automorphism $\sigma\colon K \to K$ and a polynomial $P(X) \in \mathbb{Z}[X]$ so that $P(\sigma)$ defines a group homomorphism $P(\sigma)\colon A(K) \to A(K)$ with $\ker P(\sigma) \supseteq \Gamma$. Of course, one could achieve the explicit requirements by setting $\sigma := \mathrm{id}_K$ and $P(X) = X - 1$. This would get you nowhere. The phrase about very good reduction and the relative Frobenius is important.

The next step is to extend $(K, +, \cdot, \sigma)$ to an existentially closed model $(\mathcal{K}, +, \cdot, \sigma)$ of the theory of difference fields (a field given together with a distinguished automorphism) and to set $\bar{\Gamma} := \ker P(\sigma) \colon A(\mathcal{K}) \to A(\mathcal{K})$.

There are strong criteria for deciding whether a group definable in an existentially closed difference field has weakly normal induced (from $\mathcal{L}_{\mathcal{K}}(+, \cdot)$) structure and it is routine to check these criteria for $\bar{\Gamma}$. Applying the observation about subgroups of weakly normal groups, we see that Γ has weakly normal induced structure. $\dashv$

I left three black boxes in the above sketch. First, what are σ and P? Second, what are the criteria for checking weak normality? Third, how are these criteria proven? I indicated obliquely the answer to the first question and because of its number theoretic content, I decline to give more details here. The interested reader can consult [31] for a detailed explanation. As a full answer to the other questions would fill hundreds of pages, I indicate a partial answer.

As one might guess from the fact that the definition of weakly normal groups has nothing to do with normal subgroups, weak normality is actually a property which may be predicated of an abstract theory and the above definition of a weakly normal group merely lays out the consequence of this abstract version of weak normality for a group. Weak normality is tied up with a bevy of conditions; one-basedness, nonexistence of a type definable pseudoplane, local modularity, linearity, pseudolinearity, nonexistence of an interpretable field, etc; which are equivalent under appropriate hypotheses but are otherwise subtly different. These conditions have markedly different characters: stability theoretic, dimension theoretic, combinatorial geometric, algebraic, etc. So, even when these conditions are equivalent, one avatar or another may be easier to recognize and apply.

The class of weakly normal groups definable in a given structure of finite rank is closed under taking definable subgroups, definable quotients, and definable extensions. Thus, to prove that a group is weakly normal, it suffices to prove that each subquotient in some definable composition series is weakly normal. Using a theorem proven independently by Hrushovski and Pillay [20], it suffices to show that the group is in the model theoretic algebraic closure of some set which is abstractly weakly normal. In many cases, this transforms the problem to an analysis of strongly minimal sets.

Weak normality has many equivalent formulations for strongly minimal sets with linearity being the most relevant here.

Definition 4.5. Let X be a strongly minimal set. A family of plane curves on X is a definable set $\mathcal{C} \subseteq X^2 \times B$ where

- For any $b \in B$ the set $\mathcal{C}_b := \{ (x, y) \in X^2 : (x, y, b) \in \mathcal{C} \}$ is strongly minimal and

- for any $b \in B$ there are only finitely many $b' \in B$ for which $\mathcal{C}_b \cap \mathcal{C}_{b'}$ is infinite.

The dimension of the family is $\mathrm{RM}(B)$.

DEFINITION 4.6. The strongly minimal set is *linear* if every family of plane curves on X has dimension at most one. It is *k-pseudolinear* if there is some $k \in \omega$ for which every family of plane curves on X has dimension at most k.

The following theorem of Hrushovski [13] may be used to define weak normality for strongly minimal sets.

THEOREM 4.7. *The following are equivalent for a strongly minimal set X.*

- *The theory of X is weakly normal.*
- *X is linear.*
- *X is k-pseudolinear for some $k \in \mathbb{N}$.*

The proof of the implication from pseudolinearity to linearity involves the interpretation, from the hypothesis of pseudolinearity but the failure of linearity, of an infinite field. The presence of an infinite field is incompatible with k-pseudolinearity as one sees, for instance, by considering the family of graphs of monic polynomials of degree $k+1$.

One might wonder whether, and Zilber conjectured that, a nonlinear strongly minimal set always interprets a field. The conjecture is false [14], but under the hypothesis that the strongly minimal set is a *Zariski geometry*, then Zilber's conjecture is true [21].

DEFINITION 4.8. Let $\mathcal{L}$ be a relational language. A *Zariski geometry* $\mathcal{X}$ is a strongly minimal $\mathcal{L}$-structure for which

- $\mathcal{X}$ eliminates quantifiers in $\mathcal{L}$,
- for each $n \in \omega$, the $\mathcal{L}_X$-atomic relations on X^n are the closed sets for a Noetherian topology, and
- if $Y \subseteq X^n$ is an irreducible closed set, $\Delta_{i,j} = \{ (a_1, \dots, a_n) \in X^n : a_i = a_j \}$, and $Z \subseteq Y \cap \Delta_{i,j}$ is a nonempty irreducible component of the intersection, then $\dim Z + 1 \geq \dim Y$.

Recall that a topological space X is *irreducible* there are no proper closed sets $Y, Z \subsetneq X$ with $X = Y \cup Z$. In Definition 4.8, one may replace dim with RM.

Heuristically, the condition on the dimension of a component of an intersection reflects the smoothness of the underlying Zariski geometry. If the Zariski geometry X is not linear, then one recovers an infinite field by using a high dimensional family of curves to define something like a tangent space to X with an action of the field.

How does the theory of Zariski geometries give criteria for recognizing the weakly normal groups definable in existentially closed difference fields? First, one must extend the basic work on Zariski geometries so that it applies to difference fields. As these theories are not stable, this requires a very substantial technical effort [7]. Next, one classifies the fields which are interpretable in existentially closed difference fields and finds that they are simply the fixed fields of automorphisms of the form $\sigma^n \tau^m$ where σ is the distinguished automorphism, τ is either the Frobenius in positive characteristic or the identity in characteristic zero, and $m, n \in \mathbb{Z}$ are integers. From these steps one concludes that a definable group which is not weakly normal must have an infinite subquotient which admits a definable homomorphism with a finite kernel to the k-rational points of an algebraic group over one of the fixed fields, k. To put this observation to use one needs to know something about the theory of algebraic groups. In the case of Proposition 4.4 the algebraic work is routine. In some other cases, the algebra used at this point can be somewhat more involved.

§5. From enriched fields back to pure fields: prolongations. In many of the auxiliary theories of enriched fields used in the proofs of diophantine theorems the analysis of definable sets may be reduced to the study of definable sets in pure fields through the systematic use of prolongations. These prolongations are also used to prove effective finiteness results which would not otherwise be apparent.

Let me introduce prolongations for differential fields first. Recall that a differential field is a field K given together with a derivation, a function $\partial\colon K \to K$ satisfying $\partial(x + y) = \partial(x) + \partial(y)$ and $\partial(x \cdot y) = x \cdot \partial(y) + \partial(x) \cdot y$ universally, and that an existentially closed differential field is called a differentially closed field. If $(K, +, \cdot, \partial)$ is a differentially closed field, $X \subseteq K^N$ is a definable set, and $m \in \mathbb{N}$ is a natural number, then the m-th prolongation space, or m-th jet space, of X is $\nabla_m X$, the Zariski closure in $K^{N(m+1)}$ of $\{ (a, \dots, \partial^m a) : a \in X \}$. I note that there are natural algebraic maps $\pi_{m,n}\colon \nabla_{m+n} X \to \nabla_n X$ and differentially defined maps $\nabla_m\colon X \to \nabla_m X$ given by $a \mapsto (a, \dots, \partial^m a)$. The quantifier elimination theorem for differentially closed fields of characteristic zero asserts that for any definable set X, there is a natural number $m \in \mathbb{N}$ and a set $\tilde{X} \subseteq \nabla_m X$ definable in the language of pure fields such that $X = \nabla_m^{-1}(\tilde{X})$. The construction of the jet space works also for subsets of quasiprojective varieties. However, the higher jet spaces of a projective variety are not projective. This curiosity is related to the existence of some weakly normal groups definable in differentially closed fields.

For a difference field K, we define the prolongation spaces in analogy to the jet spaces in differentially closed fields replacing ∂ with σ, the distinguished automorphism. In this case, the m-th prolongation space of a definable set $X \subseteq K^N$ is the Zariski closure in $K^{N(m+1)}$ of $\{ (x, \sigma(x), \dots, \sigma^m(x)) : x \in X \}$.

Effective bounds were first calculated using prolongation spaces in an argument used in Hrushovski's proof of the Manin-Mumford conjecture [15].

PROPOSITION 5.1 (Proposition 2.5 of [15]). *Let* $(\mathcal{K}, +, \cdot, \sigma)$ *be an existentially closed difference field. Let* $n, N \in \mathbb{N}$ *be natural numbers and* $\Upsilon \subseteq \mathbb{A}^{N(n+1)}(\mathcal{K}) = \nabla_n \mathbb{A}^N(\mathcal{K})$ *an affine variety. Then the degree of the Zariski closure of* $\nabla_n^{-1}(\Upsilon(\mathcal{K}))$ *is at most* $\deg(\Upsilon)^{2^{\dim(\Upsilon)}}$.

The proof of Proposition 5.1 is a routine induction using Bezout's theorem that $\deg(X \cap Y) \leq \deg(X) \cdot \deg(Y)$ for varieties X and Y and the observation that if $X \subseteq \mathcal{K}^N$ and $Y(\mathcal{K}) \subseteq \mathbb{A}^{N(n+1)}$ is the Zariski closure of $\nabla_n(X)$, then $\sigma(\pi(Y(\mathcal{K}))) = \nu(Y(\mathcal{K}))$ where π (respectively, ν) is the projection onto the first (respectively, last) Nn coordinates.

As mentioned before the statement of Proposition 5.1, this proposition is instrumental in the proof of an effective Manin-Mumford conjecture. As surveys of this theorem are available in other sources (see for example [3, 27]), I expound this technique through the proof of the Drinfeld module version of the Manin-Mumford conjecture [36].

We start with some notation.

NOTATION 5.2. Let $p > 0$ be a prime number. Let $A := \mathbb{F}_p[t]$ be the polynomial ring in one variable over the field of p elements. Let K be an algebraically closed field of characteristic p. By $\mathrm{End}(K, +)$ I mean the ring of group endomorphisms of $(K, +)$ given by regular functions. A Drinfeld module is a ring homomorphism $\varphi \colon A \to \mathrm{End}(K, +)$ for which $\varphi(t)$ is not simply scalar multiplication. Put another way, a Drinfeld module is a way to regard K as an A-module with the action being given by polynomial functions, not all of which are linear. The Drinfeld module φ is said to have generic characteristic if writing $\varphi(t) = [x \mapsto \sum_{i=0}^N a_i x^{p^i}]$ we have $a_0 \notin \mathbb{F}_p{}^{\mathrm{alg}}$.

The Manin-Mumford conjecture for Drinfeld modules (proposed by Denis [8]) is the following.

THEOREM 5.3. *Let* $\varphi \colon A \to \mathrm{End}(K, +)$ *be a Drinfeld module of generic characteristic. Let* $\Gamma := \{ y \in K : (\exists a \in A \smallsetminus \{0\})\ \varphi(a)(y) = 0 \}$ *be the torsion module of* φ. *Then,* Γ *has weakly normal induced structure. Moreover, for every definable subgroup* $H \leq \Gamma^n$ *of some Cartesian power of* Γ *there is a definable* A*-module* $\tilde{H} \leq H$ *of finite index.*

One could add some more conclusions to Theorem 5.3 concerning uniformities.

The proof of Theorem 5.3 starts as does the proof of Proposition 4.4 in that we use the theory of reductions of Drinfeld modules and of the relative Frobenius to find a good choice $\sigma \colon K \to K$ of an automorphism and a polynomial $P(X) \in A[X]$ so that $\ker P(\sigma)$ captures (most of) the torsion module. The qualification "most of" reflects that it is in general impossible to find such σ and P with $\Gamma \leq \ker P(\sigma)$. We ignore this obstruction for now. Set $\Xi_\sigma := \ker P(\sigma) \colon \mathcal{K} \to \mathcal{K}$ where $(\mathcal{K}, \sigma)$ is an existentially closed difference field extending (K, σ). We then prove Theorem 5.3 with Ξ_σ in place of Γ using the main theorem of [7] to prove weak normality and a hybrid of analytic, algebraic, and model theoretic arguments to prove that the definable groups are commensurable with A-modules.

At this point the uniformities accorded by prolongations enter the story. The first part of the argument shows that for any affine algebraic variety $X(\mathcal{K}) \subseteq \mathcal{K}^N$ the intersection $X(\mathcal{K}) \cap \Xi_\sigma^N$ is a finite union of cosets of definable A-modules. Compactness alone would give the existence of bounds on the numbers of cosets one needs, but using Proposition 5.1 one can explicitly bound the number of such cosets in terms of $\deg(X)$, N, $\dim(X)$, and the degrees of the coefficients of P.

Once one finds these bounds, a second good choice of an automorphism $\rho\colon \mathcal{K} \to \mathcal{K}$ and polynomial $Q(X) \in A[X]$ are chosen with $\Xi_\rho := \ker Q(\rho)\colon \mathcal{K} \to \mathcal{K}$ and $\Gamma \leq \Xi_\sigma + \Xi_\rho$. The uniform bounds for $\overline{X(\mathcal{K}) \cap \Xi_\sigma}$ as X varies through a family are used to transfer the problem of understanding $X(\mathcal{K}) \cap \Gamma$ into an analysis of $\tilde{X}(\mathcal{K}) \cap \Xi_\rho$ for some variety $\tilde{X}$ explicitly computed from X.

§**6. The socle.** While we have a full description of the structure of groups of finite Morley rank for which all the associated strongly minimal sets are linear, there are groups in which both linear and non-linear components reside. There are even groups which are in no way weakly normal, but because they may be expressed as non-trivial extensions, in some geometric arguments they behave like weakly normal groups. The analysis of these situations uses the theories of orthogonality and of the infelicitously named *semipluriminimal socle*. In this section, I concentrate on the socle and its use in some proofs.

Definition/Proposition 6.1. If G is a sufficiently saturated group of finite Morley rank, then the *semipluriminimal socle* of G is the maximal connected group $G^\sharp \leq G$ for which there is a definable set Y of Morley rank at most one with $G^\sharp \subseteq \mathrm{acl}(Y)$.

It is a routine matter to understand the structure of $G^\sharp$ in terms of Y. The point of $G^\sharp$ is that we can understand the definable sets in G just in terms of the definable sets in $G^\sharp$ and $G/G^\sharp$.

Proposition 6.2. *If G is a group of finite Morley rank and $G^\sharp$ is rigid* (*every definable subgroup of $G^\sharp$ is definable over* $\mathrm{acl}(\varnothing)$), *then every every definable set in G is a finite Boolean combination of sets of the form $a + T + \pi_H^{-1}(S)$ where $a \in G$, $T \subseteq G^\sharp$ is a definable set, $H \leq G$ is a definable subgroup, $\pi_H\colon H \to H/(H \cap G^\sharp) \hookrightarrow G/G^\sharp$ is the quotient map, and $S \subseteq G/G^\sharp$ is a definable set*.

Proposition 6.2 has been applied to prove a number of theorems in diophantine geometry. It first appeared in [16] in the proof of the Mordell-Lang conjecture for semi-abelian varieties (commutative connected quasi-projective algebraic groups which are extensions of abelian varieties by products of multiplicative groups) and again in a slightly different form in [15] to extend the Manin-Mumford conjecture to general commutative algebraic groups. It leads to easy (that is, without any recourse to the theory of Zariski geometries) proofs of some other theorems.

In [19], Hrushovski and Pillay use Proposition 6.2 together with the theory of prolongations to compute effective bounds on the number of generic points on subvarieties of complex abelian varieties.

THEOREM 6.3. *Let $A(\mathbb{C})$ be a complex abelian variety and $X(\mathbb{C}) \subseteq A(\mathbb{C})$ a subvariety both defined over $\mathbb{Q}^{\mathrm{alg}}$. Let $\Gamma < A(\mathbb{C})$ be a finitely generated group. We assume that X does not contain any subvariety of the form $X_1 + X_2$ where X_1 and X_2 are positive dimensional subvarieties of A.*

Then $|(X(\mathbb{C}) \cap \Gamma) \smallsetminus X(\mathbb{Q}^{\mathrm{alg}})|$ is finite and bounded by an explicit doubly exponential function of the rank of Γ, $\deg(X)$, and geometric data associated to A.

SKETCH OF PROOF. Endow $\mathbb{C}$ with a derivation $\partial\colon \mathbb{C} \to \mathbb{C}$ so that $\mathbb{Q}^{\mathrm{alg}}$ is the constant field of ∂. Using ∂ we define $\partial \log_A\colon A(\mathbb{C}) \to \mathbb{C}^g$ where $g = \dim A$ via $a \mapsto$ "$\nabla_1(a) - (a, 0)$." Here I have identified the fiber above the origin of $A(\mathbb{C})$ of $\pi_{1,0}\colon \nabla_1 A \to A$ with $\mathbb{C}^g$ and I have written the zero section as $a \mapsto (a, 0)$. Perhaps, the logarithmic derivative is more familiar on the multiplicative group: $\partial \log\colon \mathbb{C}^\times \to \mathbb{C}$ is given by

$$x \mapsto \frac{\nabla_1(x)}{(x,0)} = \frac{(x, \partial x)}{(x,0)} = \left(1, \frac{\partial x}{x}\right)$$

which we identify with $\frac{\partial x}{x}$.

As the map $\partial \log_A$ is a group homomorphism, $\partial \log_A(\Gamma) < \mathbb{C}^g$ is a finite rank subgroup of $\mathbb{C}^g$. As such, it is contained in a finite dimensional $\mathbb{Q}^{\mathrm{alg}}$-vector space. Every such vector space is the kernel of some linear differential operator. So, we find a linear differential operator $L\colon \mathbb{C}^g \to \mathbb{C}$ with $\ker L = \partial \log_A(\Gamma) \otimes \mathbb{Q}^{\mathrm{alg}}$. Set $\bar{\Gamma} := \ker L \circ \partial \log_A$.

One shows easily that $\bar{\Gamma}^\sharp = A(\mathbb{Q}^{\mathrm{alg}})$ is rigid and then uses Proposition 6.2 to show that $(\bar{\Gamma} \smallsetminus A(\mathbb{Q}^{\mathrm{alg}})) \cap X(\mathbb{C})$ is finite. A differential version of Proposition 5.1 finishes the argument. ⊣

In another curious development, Proposition 6.2 has been used to prove the Mordell-Lang conjecture for complex tori. I should mention that the model theoretic proof of this result is only one of many proofs.

PROPOSITION 6.4. *If T is a complex torus (a compact, connected, complex Lie group), $\Gamma < T$ is a finitely generated subgroup, and $X \subseteq T$ is a closed analytic submanifold, then $X \cap \Gamma$ is a finite union of cosets of subgroups of Γ.*

The proof of Proposition 6.4 as presented in [29] proceeds by reduction to Faltings' theorem by using Proposition 6.2. One can find other proofs using basic results about complex analysis in [1].

§7. From exact solutions to approximations: specializations. The theorems described in the previous sections have dealt with exact solutions to equations. In this section I discuss a family of problems dealing with approximate solutions to diophantine equations.

Let me remind you of the definition of a valuation.

DEFINITION 7.1. Let K be a field. A valuation v on K is a function $v\colon K \to \Gamma \cup \{\infty\}$ where $(\Gamma, +, <)$ is an ordered abelian group and ∞ is new symbol defined to be greater than every element of Γ subject to the addition rules $\infty + \gamma = \infty = \gamma + \infty = \infty + \infty$. Moreover, the function v is assumed to satisfy $v(x \cdot y) = v(x) + v(y)$ and $v(x+y) \geq \min\{v(x), v(y)\}$ universally and $v(0) = \infty$.

A field given together with a valuation is called a valued field.

The valuation topology on a valued field is the weakest topology making v continuous for the order topology on Γ.

One of the most basic examples of a valued field is the field of p-adic numbers. Take $p \in \mathbb{N}$ a prime number. Define a valuation $v_p\colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ on $\mathbb{Q}$ by $v_p(0) = \infty$ and $v_p(p^r \frac{a}{b}) = r$ where $a, b \in \mathbb{Z}$ are prime to p. The field of p-adic numbers, $\mathbb{Q}_p$, is the completion of $\mathbb{Q}$ with respect to the valuation topology. The valuation v_p extends uniquely to $\mathbb{Q}_p$, and, in fact, even to $\mathbb{Q}_p^{\mathrm{alg}}$. The field $\mathbb{Q}_p^{\mathrm{alg}}$ is not complete. Its completion is the algebraically closed field $\mathbb{C}_p$, on which there is a unique extension of the valuation v_p having values in $\mathbb{Q} \cup \{\infty\}$.

The Tate-Voloch conjecture is a p-adic diophantine approximation version of the Manin-Mumford conjecture. The conjecture arose from a theorem of Tate and Voloch on forms in p-adic roots of unity [39].

THEOREM 7.2 (Tate, Voloch). *Let $f(x_1, \dots, x_n) \in \mathbb{C}_p[x_1, \dots, x_n]$ be a polynomial in n variables over $\mathbb{C}_p$.*

There is a rational number $r \in \mathbb{Q}$ such that for any n-tuple of roots of unity $\zeta_1, \dots, \zeta_n \in \mathbb{C}_p^{\times}$ either $f(\zeta_1, \dots, \zeta_n) = 0$ or $v_p(f(\zeta_1, \dots, \zeta_n)) < r$.

The geometrization of Theorem 7.2 takes the following form.

CONJECTURE 7.3. *Let $G(\mathbb{C}_p)$ be a semi-abelian variety over $\mathbb{C}_p$. Let $\Gamma := G(\mathbb{C}_p)_{\mathrm{tor}}$ be the torsion subgroup. Let $X(\mathbb{C}_p) \subseteq G(\mathbb{C}_p)$ be a closed subvariety. Then there is a rational number $r \in \mathbb{Q}$ such that for any $\zeta \in \Gamma$ either $\zeta \in X(\mathbb{C}_p)$ or the p-adic proximity of ζ to X, $\lambda_p(\zeta, X)$, is less than r.*

I will not give a precise definition of $\lambda_p(\cdot, X)$ here but note simply that if G is affine and X is defined as $\{\, a \in G(\mathbb{C}_p) : \bigwedge_{i=1}^{m} f_i(a) = 0 \,\}$ then we can define $\lambda_p(a, X) := \min\{\, v(f_i(a)) : 1 \leq i \leq m \,\}$.

Conjecture 7.3 in its full form is still open, but we have the following theorem [34, 35].

THEOREM 7.4. *Conjecture 7.3 is true under the hypothesis that G is defined over $\mathbb{Q}_p^{\mathrm{alg}}$.*

The proof of Theorem 7.4 makes use of the weakly normal groups employed in [15] together with a few other ideas. First, some p-adic nonstandard analysis is used to convert theorems on the finiteness of the number of torsion points on a variety into proximity bounds. Secondly, since we are forced to work with a single prime, it is necessary to use definable groups which are not weakly normal. The theory of orthogonality together with some Galois theory controls the nonweakly normal parts of these groups. Finally, more sophisticated results on Galois representations are needed in order to find enough difference equations.

The key to converting finiteness theorems on numbers of exact solutions into bounds on proximity is (a slight elaboration of) the next lemma.

LEMMA 7.5. *Let (K, v) be an algebraically closed valued field with value group Γ_K. Let $\sigma\colon K \to K$ be a field automorphism satisfying $(\forall x \in K)\ v(x) = v(\sigma(x))$. Let $\mathcal{O}_{K,v} := \{ x \in K : v(x) \geq 0 \}$ be the ring of v-integers in K.*

Let $X(K) \subseteq \mathbb{A}^n(K)$ be an affine algebraic variety. Let $\tilde{\Upsilon}(K) \subseteq \mathbb{A}^{n(m+1)}(K)$ be an affine algebraic variety and set $\Upsilon(K) := \nabla_m^{-1}(\tilde{\Upsilon}(K))$.

Suppose that for every difference field $(\mathcal{K}, \sigma)$ extending (K, σ) the set $X(\mathcal{K}) \cap \Upsilon(\mathcal{K})$ is finite.

Then, there is a value $\gamma \in \Gamma_K$ such that for any $\zeta \in \Upsilon(\mathcal{O}_{K,v})$ either $\zeta \in X(\mathcal{O}_{K,v})$ or $\lambda_v(\zeta, X) \leq \gamma$.

To prove Lemma 7.5 one takes a Γ-sequence of counter-examples to each $\gamma \in \Gamma$ serving as the requisite bound and then produces an element of Υ in some ultrapower of K which is infinitesimally close to X but is not itself in X. By applying a standard part mapping, a new element of X is created but a compactness argument shows that there can be no such new element.

With Lemma 7.5 in place, to prove Theorem 7.4 one needs to find the right σ and the right Υ. If, for instance, one could find $\sigma\colon \mathbb{C}_p \to \mathbb{C}_p$ preserving the value group and some weakly normal group Υ containing $G(\mathbb{C}_p)_{\mathrm{tor}}$ defined by a σ-equation, then for varieties X containing no translates of groups, Lemma 7.5 immediately implies the desired result. In practice, a single choice of σ and Υ does not suffice and the full argument is more delicate.

An approximation lemma for valued differential fields analogous to Lemma 7.5 holds. Using this analogue, the conclusion of [16], and some basic model theory of separably closed fields one can prove a positive characteristic version of the so-called *abc*-theorem for commutative algebraic groups [32] generalizing the characteristic zero theorem of Buium [6].

§8. Concluding remarks.

The main theorem on Zariski geometries often goes by the name of the Zilber trichotomy. When dealing with groups, one sees only a dichotomy, between weakly normal and algebraic groups. The other dichotomy actually holds for all weakly normal strongly minimal sets. Recall that a sufficiently saturated strongly minimal set X is *trivial* if given any finite subset $A \subseteq X$ and an element $a \in X$, if $a \in \operatorname{acl}(A)$, then there is some $b \in A$ such that $a \in \operatorname{acl}(\{b\})$. A trivial strongly minimal set is necessarily weakly normal. As one can see by taking $a = b + c$ and $A := \{b, c\}$ with b and c generic, if X is a strongly minimal group, then X cannot be trivial. The converse, at least among weakly normal strongly minimal sets is true: if X is weakly normal, strongly minimal, and not trivial; then X is bi-interpretable with a weakly normal group.

All of the theorems described in this article have harnessed only the dichotomy within the class of groups. However, it is expected (and has been proven in some cases [18]) that most strongly minimal sets in existentially closed difference and differential fields are trivial. Since these trivial sets are present, we should see them reflected in arithmetic.

Since triviality does not in and of itself give a complete description of the class of definable sets, as does weak normality for a group, knowing that some set definable in a difference or differential field is trivial might not give much information. To extract the arithmetic content of triviality in these theories we need a classification of the possible structures on trivial sets. In [18] it is shown that any strongly minimal set in a certain class of sets definable in differentially closed field has essentially no structure. However, even for this class, there is no known interpretation of this amorphousness in terms of finiteness for solutions to algebraic (as opposed to differential) equations.

Even restricted to diophantine questions concerning algebraic groups, there are limits to the model theoretic methods. It is impossible to find a weakly normal group definable in an existentially closed differential or difference field containing an infinite set of points rational over a number field. Thus, there can be no new proof of the Mordell-Lang conjecture using the model theory of fields as currently understood. There are subgroups of abelian varieties over finite fields which are known to have weakly normal induced structure [5] which cannot be embedded into a weakly normal group definable in an existentially closed difference field [37].

One might conclude from this article that the work on applications of stability theory to diophantine geometry has yielded results in only one direction: number theoretic theorems proven using stability theoretic techniques. However, there has been some feedback at several levels. Of course, strong results on Zariski geometries and the model theory of fields and groups have been proven in the service of diophantine theorems. However, the connection goes deeper than this. Zilber has raised a diophantine conjecture, what he calls the conjecture on intersections with tori, which generalizes the Mordell-Lang conjecture and is essential for his quest for an axiomatization of the theory of the complex exponential function and the program of Baldwin and Holland to build a bad field [42].

REFERENCES

[1] D. Abramovich, *Subvarieties of Abelian varieties and Jacobians of curves*, ***Ph. D. Thesis***, Harvard University, 1991.

[2] W. Baur, *Elimination of quantifiers for modules*, ***Israel Journal of Mathematics***, vol. 25 (1976), pp. 64–70.

[3] E. Bouscaren, *Théorie des modèles et conjecture de Manin-Mumford [d'après Ehud Hrushovski]*, ***Séminaire Bourbaki***, vol. 52, Exposé 870, March 2000.

[4] E. Bouscaren (editor), ***Model theory and algebraic geometry: An introduction to E. Hrushovski's proof of the geometric Mordell-Lang conjecture***, Lecture Notes in Mathematics, vol. 1696, Springer-Verlag, New York, 1998.

[5] J. Boxall, *Sous-variétés algébriques de variétés semi-abéliennes sur un corps fini*, ***Number theory (Paris, 1992–1993)***, London Mathematical Society Lecture Note Series, vol. 215, Cambridge University Press, Cambridge, 1995, pp. 69–80.

[6] A. Buium, *The abc theorem for abelian varieties*, ***International Mathematical Research Notices***, vol. 5 (1994), p. 219 ff.

[7] Z. Chatzidakis, E. Hrushovski, and Y. Peterzil, *Model theory of difference fields II: periodic ideals and the trichotomy in all characteristics*, ***Journal of the London Mathematical Society***, to appear.

[8] L. Denis, *Géométrie diophantienne sur les modules de Drinfeld*, ***The arithmetic of function fields (Columbus, Ohio 1991)*** (D. Goss, editor), 1992, pp. 285–302.

[9] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpen*, ***Inventiones Mathematicae***, vol. 73 (1983), no. 3, pp. 349–366.

[10] ———, *The general case of S. Lang's conjecture*, ***Barsotti symposium in algebraic geometry (Abano Terme, 1991)***, Perspectives in Mathematics, vol. 15, Academic Press, San Diego, California, 1994, pp. 175–182.

[11] J. Harris, ***Algebraic geometry: A first course***, Graduate Texts in Mathematics, vol. 133, Springer-Verlag, New York, 1995.

[12] R. Hartshorne, ***Algebraic geometry***, Graduate Texts in Mathematics, vol. 52, Springer-Verlag, New York, 1977.

[13] E. Hrushovski, *Unimodular minimal structures*, ***Journal of the London Mathematical Society***, vol. 46 (1992), no. 3, pp. 385–396.

[14] ———, *A new strongly minimal set. stability in model theory, III (Trento, 1991)*, ***Annals of Pure and Applied Logic***, vol. 62 (1993), no. 2, pp. 147–166.

[15] ———, *The Manin-Mumford conjecture and the model theory of difference fields*, preprint, 1996.

[16] ———, *The Mordell-Lang conjecture for function fields*, ***Journal of the American Mathematical Society***, vol. 9 (1996), no. 3, pp. 667–690.

[17] ———, *Stability and its uses*, ***Current developments in mathematics, 1996 (cambridge, massachusetts)***, International Press, Boston, Massachusetts, 1997, pp. 61–103.

[18] E. Hrushovski and M. Itai, *On model complete differential fields*, preprint, 1997.

[19] E. Hrushovski and A. Pillay, *Transcendental points on subvarieties of abelian varieties*, to appear in ***American Journal of Mathematics***.

[20] ———, *Weakly normal groups*, ***Logic colloquium '85 (Orsay 1985)***, Studies in Logic and the Foundations of Mathematics, vol. 122, North-Holland Publishing Co., Amersterdam-New York, 1987, pp. 233–244.

[21] E. Hrushovski and B. Zilber, *Zariski geometries*, ***Journal of the American Mathematical Society***, vol. 9 (1996), no. 1, pp. 1–56.

[22] S. Lang, ***Number theory III***, Encyclopedia of Mathematics, vol. 60, Springer-Verlag, New York, 1991.

[23] Y. MATIYASEVICH, *Enumerable sets are diophantine*, ***Dokl. Akalt. Nauk. SSSR***, vol. 191 (1970), pp. 279–282, in Russian; see ***Sov. Math. Dokl.***, vol. 11 (1970), pp. 354–357 for an English translation.

[24] MONK, ***Ph. D. Thesis***, University of California at Berkeley, 1976.

[25] MORDELL, *On the rational solutions of the indeterminate equation of the third and fourth degrees*, ***Mathematical Proceedings of the Cambridge Philosophical Society***, vol. 21 (1922), pp. 179–192.

[26] A. PILLAY, ***Geometric stability theory***, Oxford Logic Guides, vol. 32, Oxford University Press, New York, 1996.

[27] ———, *ACFA and the Manin-Mumford conjecture*, ***Algebraic model theory (Toronto, Ontario, 1996)***, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., vol. 496, Kluwer Academic Publishers, Dordrecht, 1997, pp. 195–205.

[28] ———, *Model theory and diophantine geometry*, ***Bulletin of the American Mathematical Society***, vol. 34 (1997), no. 4, pp. 405–422.

[29] ———, *Mordell-Lang for complex tori*, preprint, 1999.

[30] M. RAYNAUD, *Sous-variétés d'une variété abélienne et points de torsion*, ***Arithmetic and geometry, I***, Progress in Mathematics, vol. 35, Birkhäuser Boston, Boston, Massachusetts, 1983, pp. 327–352.

[31] T. SCANLON, *Diophantine consequences of dichotomy theorems in difference and differential fields*, 1998, `http://www.msri.org/publications/ln/msri/1998/mtf/scanlon/1/index.html`.

[32] ———, *The abc theorem for commutative algebraic groups in characteristic p*, ***International Mathematical Research Notices***, vol. 18 (1997), pp. 881–898.

[33] ———, *The model theory of valued D-fields*, ***Ph. D. Thesis***, Harvard University, May 1997.

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

[35] ———, *The conjecture of Tate and Voloch on p-adic proximity to torsion*, ***International Mathematical Research Notices***, (1999), no. 17, pp. 909–914.

[36] ———, *Diophantine geometry of the torsion of a Drinfeld module*, preprint, 1999.

[37] T. SCANLON and J. F. VOLOCH, *Difference algebraic subgroups of commutative algebraic groups over finite fields*, ***Manuscripta Mathematicae***, vol. 99 (1999), no. 3, pp. 329–339.

[38] T. SKOLEM, *Einige Sätze über p-adische Potenzreihen mit Anwendung auf gewisse exponentielle Gleichungen*, ***Mathematische Annalen***, vol. 111 (1935), no. 3, pp. 399–424.

[39] J. TATE and J. F. VOLOCH, *Linear forms in p-adic roots of unity*, ***International Mathematical Research Notices***, vol. 12 (1996), pp. 589–601.

[40] P. VOJTA, *Mordell's conjecture over function fields*, ***Inventiones Mathematicae***, vol. 98 (1989), no. 1, pp. 115–138.

[41] A. WEIL, *L'arithmétique sur les courbes algébriques*, ***Acta Mathematicae***, vol. 52 (1928), pp. 281–315.

[42] B. ZILBER, *Intersecting varieties with tori*, preprint, 2000, `http://www.maths.ox.ac.uk/~zilber`.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF CALIFORNIA, BERKELEY
BERKELEY, CALIFORNIA 94720-3840, USA
E-mail: scanlon@math.berkeley.edu