RESEARCH REPORTS

BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 34, Number 4, October 1997, Pages 405–422
S 0273-0979(97)00730-1

MODEL THEORY AND DIOPHANTINE GEOMETRY

ANAND PILLAY

ABSTRACT. I discuss some recent applications of model theory to diophantine-type problems in algebraic geometry. I give the required background, as well as a sketch of the proofs.

1. INTRODUCTION

In this report I will describe Hrushovski's work ([15], [16]) around the Mordell-Lang conjecture. This conjecture concerns properties of the intersection of a subvariety X of a semiabelian variety A with various kinds of "small" subgroups Γ of A. "Small" here means finitely generated, or more generally "finite rank", that is, contained in the prime-to-p divisible hull of a finitely generated subgroup, where p is the characteristic of the underlying field. The general content of the conjecture is that the Zariski closure of the intersection $X \cap \Gamma$ should be a finite union of translates of connected algebraic subgroups of A. One can then ask further questions concerning uniform bounds on the number of such translates, as a function of data such as the rank of Γ, dimension of A, degree of X etc. In the case where the characteristic is 0, A is an abelian variety and Γ is the group of torsion points of A, the conjecture is called the Manin-Mumford conjecture. The Mordell-Lang conjecture was originally stated in the characteristic 0 case, and this has been proved by McQuillan [29], following work of Faltings, Vojta, Raynaud, and Hindry. The characteristic p analogue is, in full generality, false.

The novelty of Hrushovski's work has various aspects: firstly a definitive new result is obtained for semiabelian varieties *over function fields*, in the positive characteristic case. Let me state a special case:
(*) Suppose $k < K$ are algebraically closed fields of any characteristic, A is an abelian variety over K with no nontrivial homomorphisms into any abelian variety defined over k, and Γ is a finite rank subgroup of A and X a closed subvariety of

1991 *Mathematics Subject Classification.* Primary 03C60, 14G05.
Partially supported by NSF grant DMS 96-96268.

A. Then the Zariski closure Y of $X \cap \Gamma$ is a finite union of translates of abelian subvarieties (namely algebraic subgroups) of A.

Secondly, quantitative results and better effective bounds are obtained in many cases; for example in the context of (*) above and in the presence of a discrete valuation v of K/k, the v-adic distance between any point $a \in \Gamma$ and Y is bounded by a fixed constant multiple of its v-adic distance to X. Also a new proof is given for the Manin-Mumford conjecture over number fields, yielding good bounds.

Thirdly, the methods come from model theory, a branch of mathematical logic.

Twentieth century logic has already made important contributions to diophantine geometry, one such being Matiyasevich's theorem on the undecidability of the problem of the existence of integral solutions to polynomial equations over the integers. Hrushovski's work represents a new level of interaction, in which it is at the qualitative or geometric level that the real action is taking place, although the methods often yield good quantitative results too. Model theory, in its pure aspect, operates at a fairly high level of generality. Its objects of study are "structures". A structure is, roughly speaking, simply a set X, equipped, for each n, with a distinguished family D_n of subsets of X^n satisfying various closure properties. These subsets are called *definable sets*. Building on and coming out of Shelah's work on classification theory, *geometric model theory* studies the behaviour and interaction of definable sets in a structure, under certain hypotheses on the structure. Definable groups play an important role in these analyses. The relevance of this to the subject under discussion is that from the data given: for example from an abelian variety A and a small subgroup Γ of A, a certain auxiliary model-theoretic/algebraic structure M is constructed. A key point is that the "arithmetic" object Γ is replaced by a, usually larger, subgroup B of A, which is *definable* in M but still somewhat small, and over which we have some more control. One then refers to various results in geometric model theory which apply to B and which yield information about the original "diophantine-geometric" situation. This general strategy was inspired by the work of Buium [2], who gave a proof of (*) above in the characteristic 0 case by embedding Γ into a suitable differential-algebraic group. In any case, this extremely brief outline will be fleshed out in the rest of the report.

In section 2, I state the Mordell-Lang and Manin-Mumford conjectures, together with a short historical background. In section 3, I describe the relevant model-theoretic machinery. In section 4, I discuss Hrushovski's proofs of the Mordell-Lang conjecture for function fields in all characteristics and of the Manin-Mumford conjecture.

The issue of uniform and effective bounds with respect to these problems is of great interest. For example Buium [3] obtains bounds in terms of stacks of exponentials for the number of translates required in (*). He obtains [4] similar bounds for the number of generic points of the intersection of a curve X in $\mathbf{C} \times \mathbf{C}$ with a finite rank subgroup of $\mathbf{C}^{*2}$, when X is defined over a number field. Both these results use an amalgam of intersection theoretic and differential field theoretic tools. Hrushovski obtains much better bounds for the Manin-Mumford conjecture over number fields. Model-theoretic methods *automatically* yield uniform bounds, essentially via the compactness theorem. To get "good" bounds however requires more work. We expect that bounds of a doubly exponential nature can be obtained for the Mordell-Lang conjecture over function fields, but discussion of these issues should be, in the interests of brevity, left for another time. So in this report we concentrate on the qualitative results.

2. The relevant conjectures and results from diophantine geometry

In the background to everything lies the Mordell conjecture, proved by Faltings. To begin we work over the field $\mathbf{C}$ of complex numbers. By a plane curve C we mean the solution set in $\mathbf{C}^2$ of an irreducible polynomial equation $F(X, Y) = 0$. The curve C is said to be defined over the subfield k of $\mathbf{C}$ if F can be chosen with coefficients from k. In this case, $C(k)$, the set of k-rational points of C, is simply the set of points on C whose coordinates lie in k. The Mordell conjecture states that if k is a number field, then for most curves C defined over k, namely for curves of genus greater than or equal to 2, $C(k)$ is finite. Let us say a word about genus. Given a plane curve C as above, we can adjoin points at infinity to obtain a projective curve C_1. This is done by adding another indeterminate Z, forming the associated homogeneous equation $G(X, Y, Z) = 0$ and considering the solutions of G in $P^2(\mathbf{C})$. C_1 will be called nonsingular (or smooth) if it sits in $P^2(\mathbf{C})$ as a complex submanifold. It will then be a compact Riemann surface and the genus of C_1 (and also C) will be the number of handles. $C_1(k)$ is the set of points P on C_1, such that for some choice $(x : y : z)$ of homogeneous coordinates for P, x, y, z are all in k. Finiteness of $C_1(k)$ is equivalent to finiteness of $C(k)$.

In order to state other more general conjectures and results one requires something of the language of algebraic geometry. The (naive) language of algebraic varieties (rather than schemes) will be enough for our purposes. In the next couple of paragraphs we work in an algebraically closed field K of arbitrary characteristic. There are three main points: (a) the category of algebraic varieties, (b) the Zariski topology on an algebraic variety, and (c) the notion of a variety or morphism being defined over a field k. The reader is referred to [32]. We will say a few words, mainly about (c), so as to fix notation. Let V be an affine variety, that is the solution set in some K^n of a (finite) set of polynomial equations $P_i(X_1, .., X_n) \in K[X_1, .., X_n]$. Let k be a subfield of K. V is said to be *defined over* k if the P_i can be chosen with coefficients in k, or more accurately, if the ideal $I(V)$ of all polynomials over K vanishing on V is generated by polynomials over k. A *morphism* between affine varieties $V \subset K^n$ and $W \subset K^m$ is said to be *defined over* k if the m polynomials which define the morphism can be chosen with coefficients in k. An abstract variety is something modelled locally on affine varieties; namely it is obtained by piecing together finitely many irreducible affine varieties, suitable Zariski open subsets of which are identified via *isomorphisms*. An example is projective space P^n. An abstract variety comes equipped with its own Zariski topology. The abstract variety V is said to be defined over k if all the data entering into the definition of V are defined over k. Similarly we have the notion of a morphism between abstract varieties being defined over k. If V is a variety defined over k, then $V(k)$ denotes the set of k-rational points of V, namely those points of V all of whose coordinates are in k (when read in some suitable chart). If K_1 is a field *containing* K, then it makes sense to speak of $V(K_1)$ too. For example if V is affine, then $V(K_1)$ is the set of points in K_1^n which are zeros of all polynomials over K vanishing on V. Usually when we speak of a variety V defined over k we identify V with its set of K-rational points for some algebraically closed field K containing k.

We assume familiarity with the notions of *dimension* of a variety, *smooth (or nonsingular)* variety, and *birational isomorphism* between varieties. A curve is an irreducible variety of dimension 1. Any irreducible variety will be birationally

isomorphic to a smooth projective variety (namely a smooth closed subvariety of some projective space). Taking K to be the field of complex numbers, a smooth projective curve will be a compact Riemann surface and will have an associated genus, the number of handles or holes. In general (namely for K an arbitrary algebraically closed field) the genus g of a smooth projective curve V can be defined algebraically as the K-dimension of the space of regular differential 1-forms on V.

Diophantine or arithmetic geometry is largely concerned with the qualitative and quantitative features of sets of the form $V(k)$ where k is a number field, and V is a variety defined over k. In more down to earth language one is looking at solutions sets in a number field k of systems of polynomial equations over k. The geometric aspect of the subject comes from actual or conjectured relationships between properties of $V(k)$ and algebraic-geometric properties of V. By a function field, we will mean (here), a finitely generated extension K of an algebraically closed field k (we say K is a function field over k). There are many analogies between number fields and function fields. So the subject also deals with sets $V(K)$ where K is a function field and V is defined over K. In fact it is this function field situation which we will be most concerned with in this article.

We can now state formally:

Mordell conjecture. If C is a curve of genus greater than or equal to 2 which is defined over a number field k, then $C(k)$ is finite.

As remarked above this was proved by Faltings [11]. Historically the Mordell conjecture was first proved by Manin [24] in the function field case:

Theorem (characteristic 0)**.** *Let K be a function field over k (k algebraically closed). Let C be a curve of genus ≥ 2 which is defined over K. Then either*

(i) $C(K)$ is finite, or

(ii) C is isomorphic to some curve C_1 defined over k, and moreover all but finitely many points of $C(K)$ come from points of $C_1(k)$ under this isomorphism.

The conclusion of part (ii) of the theorem is due to de Franchis. In fact Manin's proof of the above had a mistake, found 20 years later by Coleman. But a revised proof was given by Coleman [8], and the mistake patched up by Chai [10]. In any case, the key point of Manin's approach was that a function field supports a nontrivial derivation. The consequent use of differential algebra turns out to be also pertinent in the work of both Buium and Hrushovski.

We want now to state Lang's generalization of the Mordell conjecture. In order to make sense of the generalization, a couple of things have to be said. Firstly, an algebraic group is an algebraic variety G with a group operation $*$ which is a morphism from $G \times G$ to G. An *abelian variety* is an irreducible (or as is normally said, connected) algebraic group which is also a projective variety. Over the complex numbers an abelian variety is a complex torus. In any case, an abelian variety is commutative and prime to p-divisible (where p is the characteristic), and for any prime l different from p, the points of order a power of l are Zariski dense in A. An abelian subvariety of A is precisely a connected closed subgroup of A. The point is that any smooth projective curve C of genus $g \geq 1$ defined over a field k embeds in an abelian variety A of dimension g also defined over k. A is called the *Jacobian variety* of C, $J(C)$. Over the complex numbers this Jacobian construction is quite classical: A point P is chosen on C, and an analytic map from C^g onto $\mathbf{C}^g/L$ is defined, for a suitable lattice L, by integrating differential forms on C between P and

points $P_1, .., P_g$. A group structure is induced on C^g/E for a suitable equivalence relation E, and this group turns out to be an abelian variety. The second point is the Mordell-Weil theorem, which states that if A is an abelian variety defined over a number field K, then $A(K)$ is a finitely generated group. (See [33] for more on the Mordell-Weil Theorem and diophantine geometry.)

Mordell-Lang conjecture, first approximation. Assume characteristic to be 0. Let A be an abelian variety, X a closed subvariety, and Γ a finitely generated subgroup of A. Then $X \cap \Gamma$ is a finite union of translates of subgroups of A. Equivalently, the Zariski closure of $X \cap \Gamma$ is a finite union of translates of abelian subvarieties of A.

The Mordell-Lang conjecture implies the Mordell conjecture, for let C be a curve of genus ≥ 2 defined over a number field K. Let A be its Jacobian variety, also defined over K. By the Mordell-Weil theorem $A(K)$ is finitely generated. Clearly $C(K) = C \cap A(K)$, so the Mordell-Lang conjecture implies that the Zariski closure of $C(K)$ is a finite union of translates of abelian subvarieties of A. If all of these abelian subvarieties are trivial, then $C(K)$ is finite, as required. Otherwise, as $dim(C) = 1$, $C(K)$ itself must be a translate of an abelian subvariety of A, but as is well-known, this implies that C has genus 1, contradiction.

The above first version of the Mordell-Lang conjecture was proved by Faltings [12].

The full Mordell-Lang conjecture, appearing first in [21], will be a generalization in two ways: first A is replaced by a *semi-abelian variety*, and secondly, Γ is replaced by a "finite rank" subgroup of A. By a semi-abelian variety we mean a (commutative) connected algebraic group S which contains a closed subgroup T such that T is isomorphic to some finite power of the multiplicative group, and S/T is an abelian variety. S will also be divisible. By a finite rank subgroup of S we mean (at least in the characteristic 0 case) a subgroup Γ which is contained in the divisible hull of a finitely generated subgroup.

Mordell-Lang conjecture (characteristic 0)**.** Let S be a semiabelian variety, X a subvariety, and Γ a finite rank subgroup of S. Then $X \cap \Gamma$ is a finite union of translates of subgroups of S.

The Mordell-Lang conjecture was proved in its entirety by McQuillan [29], using the work of Faltings and others. In the special case where A is an abelian variety and Γ its group of torsion points, the Mordell-Lang conjecture reduces to what is called the Manin -Mumford conjecture. This was proved by Raynaud [30] and then generalized by Hindry [14] to all commutative algebraic groups. See [22] for more background on this.

The question arises as to what one can say along the lines of the Mordell-Lang conjecture in positive characteristic. The first thing to remark is that the Mordell-Lang conjecture (even in its first approximation) and the Mordell conjecture for function fields (as proved by Manin) fail in positive characteristic: let X be a curve of genus $g \geq 2$ defined over $\mathbf{F}_p$, say, and let A be its Jacobian variety. Let k be the algebraic closure of $\mathbf{F}_p$, let t be a generic point of X over k, let $K = k(t)$, and let Γ be the subgroup of $A(K)$ generated by $\{Fr^n(t) : n \in \mathbf{N}\}$ (where Fr is the Frobenius endomorphism $x \to x^p$). Γ is finitely generated (by the Lang-Neron theorem), and $X \cap \Gamma$ could not be a finite union of translates of subgroups. Similarly $X(K) - X(k)$ is infinite.

The key to a correct formulation of say the Mordell conjecture for function fields in positive characteristic is to say nothing about the case in which C is isomorphic to a curve defined over k. This version was proved by Samuel [31] and Grauert [13]: If k is algebraically closed of characteristic $p > 0$, K is a finitely generated extension of k, and C is a curve of genus ≥ 2 defined over k which is not weakly isomorphic to a curve defined over k, then $C(K)$ is finite.

We are now almost in a position to state Hrushovski's theorem. The statement in full generality requires some additional definitions. For now $k < K$ are algebraically closed fields (of any characteristic) and A is a semi-abelian variety defined over K. We will say that a closed subvariety X of A is *special* if there are a connected algebraic subgroup (i.e. semiabelian subvariety) A_1 of A, a semi-abelian variety A_0 defined over k and a subvariety X_0 of A_0 also defined over k, and a surjective homomorphism of algebraic groups $h : A_1 \to A_0$ such that $X = h^{-1}(X_0) + c$ for some $c \in A$. Note that if there is no homomorphism from any algebraic subgroup of A onto a positive-dimensional algebraic group defined over k (in other words A is an abelian variety with k-trace 0), then to be a special subvariety of A means simply to be a translate of a semi-abelian subvariety of A. Finally by a finite rank subgroup of the semi-abelian variety A in the characteristic p case, we will mean a subgroup which is contained in the prime-to-p divisible hull of a finitely generated subgroup.

Here now is Hrushovski's main result (with above notation and conventions still in place).

Theorem 2.1. *(Mordell-Lang conjecture for function fields in all characteristics.) Suppose Γ is a finite rank subgroup of A, and X is a closed subvariety of A. Then there is a finite set $X_1, .., X_n$ of special subvarieties of A such that $X \cap \Gamma \subseteq X_1 \cup ... \cup X_n \subseteq X$.*

So if A is an abelian variety with k-trace 0, then the conclusion can be restated as: $X \cap \Gamma$ is a finite union of translates of subgroups of A. Buium [2] gives a proof of this special case for characteristic 0, using differential algebraic geometry and complex analysis. Hrushovski's proof of the theorem (inspired by Buium's work) uses some general model-theoretic results, together with the model theory of differential fields in the characteristic 0 case and the model theory of separably closed fields in the positive characteristic case. The positive characteristic case is a new result. Abramovich and Voloch [1] had earlier obtained several special cases, which do not suffice for the general result (even for the special case where A has k-trace 0).

We complete this section by stating Hrushovski's good bounds for the Manin-Mumford conjecture over number fields. Let us fix an abelian variety A defined over a number field K. We also fix a projective embedding of A, so any subvariety X of A has a certain "degree". $Tor(A)$ denotes the group of torsion points of A.

Theorem 2.2. *Let A be an abelian variety defined over a number field K and X a closed subvariety defined over the algebraic closure of K. Then there are a finite number M of translates $A_i + a_i$ of abelian subvarieties A_i of A, such that $Tor(A) \cap X = \bigcup\{Tor(A_i) + a_i : i = 1, .., M\}$. Moreover there are constants c, e depending only on A (so not on K or X) such that $M \leq cdeg(X)^e$.*

The proof makes use of the model theory of difference fields, that is fields equipped with an automorphism, as worked out by Chatzidakis and Hrushovski [7].

As remarked in the introduction, the proofs of these theorems have a common overall strategy. The situation at hand is embedded into a suitable auxiliary model-theoretic/algebraic situation, in which deep model theoretic results are shown to be applicable. The information gathered feeds back into the original situation to yield the desired conclusions. Among the model-theoretic notions and results used are (i) the general theory of *orthogonality*, coming from [34], (ii) the theory of 1-based or modular groups [17], and (iii) the theory of Zariski structures [19]. We will try to convey the flavour of these results, as well as the model-theoretic analysis of differential fields and difference fields in the next section.

3. Model theory, stability theory, and model-theoretic algebra

We begin by giving some background on the basics of first order logic and model theory. We also recommend [20] for a modern introduction to model theory.

A structure, in the sense of model theory (or predicate logic), will be a set X equipped with, for each n, a certain distinguished family D_n of subsets of X^n satisfying various closure properties (where X^n denotes the Cartesian product $X \times ... \times X$, n times). We will specify shortly these closure conditions on the families D_n, but for the moment one should note that from a structure (X, D_n) we obtain a certain *category*, the category of *definable sets* and *definable maps*. A definable set will be a set in some D_n and a definable map will be a function whose graph is a definable set. The conditions we require of the definable sets consist essentially of closure under the first order logical operations of finite intersection, finite union, Cartesian product, complementation, projection, and taking fibres. Closure under projection means that if $Y \in D_{n+1}$, then the projection of Y on the first n-coordinates is in D_n. Closure under taking fibres means that if $Y \in D_{n+m}$, and $a \in X^n$, then $\{b \in X^m : (a, b) \in Y\} \in D_m$. We also require that for each n, $X^n \in D_n$, and that the diagonal $\Delta \in D_2$. As an example let X be an algebraically closed field k and D_n the family of constructible subsets of k^n, where by a constructible set we mean a finite Boolean combination of Zariski closed sets. The fact that the closure conditions are satisfied comes from Chevalley's theorem that the projection of a constructible set is also constructible.

It is sometimes convenient to take instead of the single set X a family $(X_i : i \in I)$ of sets and for each $i_1, .., i_s \in I$ and $n_1, .., n_s \in \mathbf{N}$ a distingushed family of subsets of $X_{i_1}^{n_1} \times ... \times X_{i_s}^{n_s}$. This is called a many sorted structure. For now however we stick with the one-sorted situation.

A structure $(X, D_n)_n$ is usually denoted by M (for model) and usually the underlying set X is confused notationally with M (so one may speak of $a \in M$ rather than $a \in X$).

An important part of the general theory is to be able to talk of a definable set being *defined over* a subset of M. Also in concrete examples one wants to consider the family of definable sets generated by certain primitives. So we slightly refine our notion of a structure as follows:

Definition 3.1. (i) By a structure M we mean a set X equipped with a family $L = (L_n : n = 1, 2, ..)$ where each L_n is a (possibly empty) family of subsets of X^n, and where the diagonal $\Delta = \{(a, b) \in X^2 : a = b\}$ is a member of L_2.

(ii) Let M be a structure as in (i). We define the class $D^0(M)$ of 0-definable sets in M to be the smallest class of subsets of X^n for various n which contains $\bigcup\{L_n : n = 1, ..\}$ and is closed under finite intersections, finite unions, complementation, Cartesian products and projection. $D^0_n(M)$ will be those members of $D^0(M)$ which are subsets of X^n. The class $D(M)$ of definable sets in M is obtained from the class $D^0(M)$ by further closing under taking fibres. ($D(M)$ is clearly closed under the other operations too.) $D_n(M)$ is those members of $D(M)$ which are subsets of X^n.

(iii) Let M be a structure, and let $Y \in D_n(M)$. Let A be an arbitrary subset of X. We say that Y is A-definable if there is some $m \in \mathbf{N}$, some $Z \in D^0_{m+n}(M)$ and some $a \in X^m$ all of whose coordinates are from A, such that $Y = \{b \in X^n : (a, b) \in Z\}$.

As remarked above, given a structure M we will identify notationally M with its underlying set. The symbol X will from now on be reserved for definable sets (or an indeterminate in a polynomial).

An algebraically closed field k say can be viewed as a structure as follows. Let the underlying set of M be k, and take L_2 to be the diagonal, and L_3 to consist of the graphs of addition and multiplication. Owing to Chevalley's theorem mentioned earlier, the definable sets in M will be precisely the constructible sets. In particular any affine variety $V \subset k^n$ will be definable, and moreover if k_0 is a subfield of k, V will be k_0 definable in the model-theoretic sense if and only if V is defined over k_0 in the algebraic-geometrical sense (although the last statement should be slightly modified in the positive characteristic case). In fact we could start with any field k and do the same thing. However if k is not algebraically closed, one will always obtain nonconstructible sets among the definable sets. In model-theoretic parlance the only infinite quantifier-eliminable fields are algebraically closed [23]. For example if $k = \mathbf{R}$, the ordering on $\mathbf{R}$ will be 0-definable (as the projection of $\{(x, y) : x = y^2\}$ on the first coordinate). If $k = \mathbf{Q}$, the ring of integers will even be definable, as was proved by Julia Robinson (see 5.5.4 and 5.5.5 in [20]).

In the example above we identified the *operations* of $+$ and $\cdot$ with their graphs, in order to make sense of a field as a structure. We could also modify our definition of a structure by allowing, for each n a set F_n of functions from M^n to M, and expanding our notion of definable set. For example, if $Y \in D_1(M)$ and $f \in F_n$, then $\{(a_1, .., a_n) \in M^n : f(a_1, .., a_n) \in Y\}$ should be a definable set. So in the case of fields, this presentation makes it clear why the solution set of a finite set of polynomials should be a definable set. In any case, we assume the reader understands what we mean when we consider a set equipped with functions (for example addition, multiplication, derivation, etc.) as a structure.

Given a structure $M = (M, L_n)_n$ we can formulate "first order sentences" built up from symbols for the primitives in the various L_n, and we can ask whether such sentences are true or false in M. (The main point in establishing the truth or falsity of such a sentence in M is that the quantifiers "there exists", "for all" should be interpreted as ranging over elements of M.) The symbols for the primitives in the L_n's are said to comprise the vocabulary or signature of M. So in the case of fields, we give ourselves symbols $+$ and $\cdot$ for addition and multiplication, and we can formulate, using the logical connectives "and", "or", "not", "there exists", "for all" sentences built up from these primitives. These are called first order sentences in the vocabulary of M. As a trivial example the commutativity of addition is expressible

by such a sentence. As a less trivial (but still easy) example the property (for fixed d) that any nonzero polynomial of degree d in one indeterminate X has a solution will be expressible by a certain first order sentence. The theory of M, $Th(M)$ is by definition the set of all first order sentences in the vocabulary of M which are true in M. If two structures M and N have the same vocabulary (for example they are both groups, or they are both fields), we can ask whether $Th(M) = Th(N)$, namely whether the same first order sentences are true in M as are true in N. If this is the case, we say M and N are *elementarily equivalent*. If Σ is a set of first order sentences formulated in a certain vocabulary, then if M is a structure with the same vocabulary, M will be called a *model* of Σ if every sentence $\sigma \in \Sigma$ is true in M.

The compactness theorem of first order logic yields, for any structure M whose underlying set has infinite cardinality, structures of any infinite cardinality which are elementarily equivalent to M. An important and convenient notion is that of a saturated structure. Working in an ω-saturated structure is akin to working in an algebraically closed field of infinite transcendence degree over the prime field. The latter gives the existence of generic points of varieties over finitely generated subfields. This is essentially what the former gives too.

Definition 3.2. The structure M is said to be ω-saturated if for any finite subset A of M and any n, if $\{Y_i : i \in I\}$ is a set of A-definable subsets of M^n such that $\bigcap\{Y_i : i \in I'\} \neq \emptyset$ for all finite subsets I' of I, then $\bigcap\{Y_i : i \in I\} \neq \emptyset$.

Fact 3.3. *For any structure M there is a structure M' elementarily equivalent to M which is ω-saturated.*

In place of ω we could take any infinite cardinal κ and define κ-saturation just as in Definition 3.2, except that A can be any subset of M of cardinality strictly less than κ. Fact 3.3 remains true with κ in place of ω. The field of complex numbers is c-saturated, where c is the size of the continuum (equivalently the size of $\mathbf{C}$). (As the definable sets here are precisely the constructible sets, this amounts to saying that any variety V defined over a subfield k of $\mathbf{C}$ of cardinality strictly less than c has a generic point over k in $\mathbf{C}$.)

In model theory there are various combinatorially defined notions of dimension for definable sets. The original reason for introducing these notions was to help in counting and classifying models of first order theories. These notions and corresponding notions of independence (akin to algebraic independence in fields) play an important role in the subject currently under discussion. We will call a set $\{X_i : i \in \omega\}$ of definable sets uniformly definable if there is some definable set $Y \subset M^{n+m}$ such that each X_i is of the form $\{a \in M^n : (a, b) \in Y\}$ for some $b \in M^m$.

Definition 3.4. Let M be an ω-saturated structure. Let X be a definable set.

(i) We first define the Morley dimension of X, $Mdim(X)$ as follows: $Mdim(X) = -1$ if X is empty, $Mdim(X) = 0$ if X is finite, $Mdim(X) \geq n + 1$ if there is an infinite set $\{X_i : i < \omega\}$ of pairwise disjoint definable sets, each a subset of X such that $Mdim(X) \geq n$ for all i. We put $Mdim(X) = n$ if $Mdim(X) \geq n$ but not $\geq n + 1$. If $Mdim(X) =$ n, then there will be a greatest natural number d such that X can be partioned into d definable subsets, each of Morley dimension n. d is called the Morley degree of X.

(ii) Now we define the Shelah dimension $Shdim(X)$. The first two clauses ($Shdim(X) = -1$, $Shdim(X) = 0$) are as in (i). The inductive clause is: $Shdim(X) \geq n + 1$ if there is a uniformly definable family $\{X_i : i < \omega\}$ of definable sets, each X_i a subset of X, and there is some $k < \omega$ such that the intersection of any k of the X_i's is empty, and $Shdim(X_i) \geq n$ for all i.

It is natural to extend both Morley and Shelah dimension so as to have possibly infinite ordinal values. (For example, to have dimension $\geq \alpha + 1$ is defined analogously to the above, and for δ a limit ordinal, to have dimension $\geq \delta$ is to have dimension $\geq \alpha$ for each $\alpha < \delta$.) In the algebraic contexts which will be analysing, definable sets of infinite ordinal-valued dimensions will be present, but the finite-dimensional sets will play a more important role.

We will usually assume M to be an ω-saturated structure, or even a κ-saturated structure for some uncountable κ. Fact 3.3 tells us that for most purposes there is no harm in making this assumption.

If M is an algebraically closed field, then for any definable set X, both $Mdim(X)$ and $Shdim(X)$ are well-defined, equal, and correspond to the algebraic-geometric dimension of the constructible set X. If moreover X is a possibly reducible variety, then the Morley degree of X is equal to the number of irreducible components of X of maximal dimension. An interesting situation where Shelah dimension is defined but Morley dimension is not is in the case of pseudofinite fields. A pseudofinite field is an infinite field in which all sentences which are true in all finite fields hold. If F is such, then definable sets in F need not be constructible. However for any definable set X, $Shdim(X)$ is well-defined and equal to the algebraic-geometrical dimension of the Zariski closure of X. In general if $Mdim(X)$ is finite, then so is $Shdim(X)$ (but they may not have the same value).

Coming out of each of these notions of dimension is a notion of *independence*, which we describe briefly. Suppose that M is structure, A is a subset of M and X is an A-definable set of finite Morley dimension. Let $a \in X$ and let B be a subset of M including A. We define the Morley rank of a over B, $Mrk(a/B)$ to be the least n such that there is a B definable set Y of Morley dimension n with $a \in Y$. If $B \subset C \subset M$, we say that a is independent from C over B if $Mrk(a/C) = Mrk(a/B)$. Similarly we can define $Shrk$ and independence in that context. Usually A, B, etc. will denote finite subsets of the ω-saturated structure M (or subsets of cardinality strictly less than κ if M is assumed to be κ-saturated). For the next few definitions, *dim* can be interpreted as either $Mdim$ or $Shdim$ and similarly with rk and independence.

Definition 3.5. Let M be a structure, and X, Y definable subsets, both defined over A say. We will say that X and Y are orthogonal if for all $B \supset A$, for all $a \in X$ and for all $b \in Y$, a is independent from b over B.

In the case where M is an algebraically closed field, any two infinite definable sets will be nonorthogonal. It will be in structures such as differentially closed fields or separably closed fields that we will be able to find and exploit orthogonality. As an explanation of nonorthogonality in a special case we have:

Fact 3.6. *Suppose (in a structure M) that X and Y are definable sets, each of Morley dimension 1. Then X is nonorthogonal to Y if there is a definable finite-to-finite relation R between infinite definable subsets of X and Y.*

Geometric stability theory studies the fine structure of independence and the implications for, among other things, definable groups. The general subject is expounded in [28]. A fundamental notion is *modularity*, or *1-basedness*. Because of the centrality of this notion in the work being discussed, I will give the definition. First we need to mention the model-theoretic notion of algebraic closure. Suppose M is a structure, and A a subset of X. By $acl(A)$, the *algebraic closure* of A in M, we mean the union of all finite A-definable subsets X of M. If M is an algebraically closed field, and A is a subfield k of M, then $acl(k)$ reduces to the usual field-theoretic algebraic closure of k.

Definition 3.7. Let M be a structure, and X a definable set of finite dimension, defined over A say. We will say that X is modular if for any finite tuple a of elements in X and for any $B \supset A$, a is independent from $acl(B)$ over $acl(A \cup a) \cap acl(B)$.

Again in the special case where X is a definable set of Morley dimension and Morley degree 1, modularity has a more geometric description: There should be no infinite definable family of definable subsets of $X \times X$, each of Morley dimension and Morley degree 1 and with pairwise intersections finite.

A typical example of a structure in which all definable sets are modular (with finite Morley dimension) is a vector space V over a field F, where the primitives consist of the addition operation of V and for each $\lambda \in F$, scalar multiplication by λ. On the other hand an algebraically closed field yields a situation where modularity fails drastically.

We can now give the consequences of modularity for definable groups. By a definable group in a structure we mean a group G such that both the underlying set of G and the group operation are definable sets. The following is from [17].

Proposition 3.8. *Suppose G is a definable group of finite Morley dimension in the structure M. Suppose moreover that G is modular. Then every subset of G definable in M is a finite Boolean combination of translates of definable subgroups of G. Also G must be abelian-by-finite.*

Proposition 3.8 is not strictly true for groups of finite Shelah dimension. However it is true if we assume *stability* of G. The notion of stability is again central to model theory. A definable set X will be called *stable* if there do not exist a definable relation R, elements $a_i \in X$ for $i < \omega$ and tuples b_j from M for $j < \omega$, such that $(a_i, b_j) \in R$ iff $i < j$. Any definable set of finite Morley dimension will be stable.

Proposition 3.9. *Suppose M is a structure, and G is a stable definable group of finite Shelah dimension. Suppose also that G is modular. Then any definable subset of G is a finite Boolean combination of translates of definable subgroups of G.*

Boris Zilber conjectured some time ago that a fundamental dichotomy holds: if M is a structure, and X is a definable set in M, of finite Morley dimension, then either X is modular or there is some infinite field k definable in M, also of finite Morley dimension, which is nonorthogonal to X. This conjecture was refuted by Hrushovski. However the conjecture was shown to be true if additional assumptions, with an algebraic-geometric flavour, are made about X. The important notion here is that of a Zariski structure or Zariski set. Before giving the definition, let me mention that the notion of a definable set does not a priori have any geometric content. In the example of algebraically closed fields, among the definable sets are some *privileged* ones, the Zariski closed sets. However the general model-theoretic

notions such as Morley dimension do not make this distinction; an irreducible curve and the same curve with a point removed both have Morley dimension and degree 1. So at this level of generality, one does not expect any model-theoretic interpretation of intersection theory. The notion of a Zariski structure brings into the picture such geometric notions.

Definition 3.10. Let M be a structure, and X a definable set in M of Morley dimension 1 and Morley degree 1. X will be called a Zariski set if for each n, X^n is equipped with a Noetherian topology, satisfying various conditions:

(i) every closed set is definable (in M) and conversely any subset of X^n definable in M is a finite Boolean combination of closed sets,

(ii) the diagonal is a closed subset of X^2, and if Y is a closed subset of X^{n+m}, then for each $a \in X^n$ the fibre $Y_a = \{b \in X^m : (a, b) \in Y\}$ is a closed subset of X^m.

(iii) if Y, Z are irreducible closed subsets of X^n, then every irreducible component of $Y \cap Z$ has Morley dimension at least $Mdim(Y) + Mdim(Z) - n$.

Hrushovski and Zilber proved, in a long and deep paper [19], that the Zilber conjecture holds for Zariski sets:

Proposition 3.11. *Let M be a structure, and let X be a definable set in M which is Zariski. Then either X is modular, or there is some algebraically closed field k definable in M such that k has Morley dimension 1 and is nonorthogonal to X.*

In fact Hrushovski and Zilber prove that if X is a nonmodular Zariski set, then X equipped with the family of Noetherian topologies on the various X^n is very close to being an algebraic curve over k.

The above results are applied to various fields with or without additional operators. The model-theoretic analysis of various algebraic structures begins with attempting to describe the definable sets. This procedure usually goes under the name of "quantifier-eimination". The first we mention is the case of differentially closed fields of characteristic zero. The interested reader is advised to look at [25] for a comprehensive account of the model theory of differentially closed fields, as well as for further references and historical background. By a differential field we mean here a field F of characteristic zero equipped with a derivation D. (That is, D is an additive homomorphism from F to F and satisfies the Leibniz rule, $D(ab) = D(a)b + aD(b)$.) An example is $\mathbf{C}(x)$ with the derivation d/dx. Differential fields serve as an algebraic context for studying (algebraic) differential equations. In the same way as algebraically closed fields are ones in which any system of polynomial equations with a solution in a larger field has already a solution, differentially closed fields are those differential fields in which differential polynomial equations have solutions. The basic axiom for differentially closed fields is that whenever f, g are differential polynomials in a single differential indeterminate x, and the order of f is strictly greater than the order of g, then $f = 0$, $g \neq 0$ has a solution. We consider a differential field F as a structure, where the primitives are the operations $+$, $\cdot$ and D. It turns out that any two differentially closed fields are elementarily equivalent. Differentially closed fields are stable, and any definable set is a finite Boolean combination of zero-sets of differential polynomials. In fact all definable sets have Morley dimension, but possibly with infinite ordinal value. Independence, as defined above, has a natural meaning: Let k be a differential subfield of the differentially closed field (F, D), and let a, b be finite

tuples from F. Let $k < a >$ be the differential field generated by k and a and similarly for $k < b >$; then a is independent from b over k if the fields $k < a >$ and $k < b >$ are free over k. The structure of the definable sets of finite Morley dimension play an important role below. It is easy to characterise such sets. Let us fix a saturated differentially closed field (K, D). Let X be a definable set, defined over the small differential subfield k of K. Then $RM(X)$ is finite just if there is a finite bound on $tr.deg(k(a, D(a), D^2(a), .)/k)$. An example is the field of constants $\mathcal{C} = \{x \in K : D(x) = 0\}$ of K. In [18] it was shown that if X is a definable set in K of Morley dimension 1 and Morley degree 1, then after taking away finitely many points, X is a Zariski structure. On the other hand, it follows from work of Cassidy [9] that any field of finite Morley dimension definable in K is definably isomorphic to $\mathcal{C}$. Proposition 3.11 applies, to show that any definable set X in K of Morley dimension and degree 1 is either modular or nonorthogonal to the field $\mathcal{C}$. Definable sets of finite Morley dimension are controlled in some technical sense by sets of Morley dimension 1. Applying this to definable groups, we obtain, using Proposition 3.8:

Lemma 3.12. *Let G be a group of finite Morley dimension definable in the differentially closed field K. Then either G is modular or G is nonorthogonal to the field of constants $\mathcal{C}$.*

Consider now a simple abelian variety A over K. A will be definable in (K, D), but of infinite Morley dimension. It follows from work of Buium [5] that A will have a unique smallest infinite definable subgroup, A^*, which moreover has finite Morley dimension. If it so happens that A is defined over $\mathcal{C}$, then A^* is precisely $A(\mathcal{C})$, the group of $\mathcal{C}$ rational points of A. In this case A^* is clearly nonorthogonal to $\mathcal{C}$. Conversely, if A^* is nonorthogonal to $\mathcal{C}$, then it can be shown, using minimality of A^* together with simplicity of A and some model theory, that A is rationally isomorphic to some abelian variety defined over $\mathcal{C}$ (that is, A descends to $\mathcal{C}$). We conclude:

Proposition 3.13. *((K, D) a differentially closed field, $\mathcal{C}$ its field of constants, and A a simple abelian variety over K.) Either A is rationally isomorphic (namely isomorphic as an algebraic group) to an abelian variety defined over $\mathcal{C}$ or A^* is modular.*

Another proof of this proposition was obtained by the author and A. Buium [6], using complex analysis and algebraic geometry, in place of Proposition 3.11.

There is one more model-theoretic ingredient needed for the Mordell-Lang conjecture for function fields. It actually rests on a general result about commutative groups of finite Morley dimension, but we state it in the special case of definable subgroups of abelian varieties in differentially closed fields. Let A be an arbitrary abelian variety over K. By the definable socle of A we mean the group generated by the minimal infinite definable subgroups of A. A will be an (almost direct) sum of simple abelian varieties A_i. Clearly the definable socle of A will be the product of the A_i^*. We let A^* denote the definable socle of A (with no ambiguity). If B is a definable subgroup of A of finite Morley dimension, and X is a definable subset of B of Morley degree 1, then by $Stab_B(X)$ (the model-theoretic stabilizer of X in B) we mean $\{b \in B : Mdim(X \cap (b + X) = Mdim(X)\}$. This will be a definable subgroup of B.

Proposition 3.14. *Let A be an abelian variety over K. Let B be a definable subgroup of A which has finite Morley dimension and contains A^*. Let X be a definable subset of B of Morley degree 1 and with $Stab_B(X)$ finite. Then X is, up to a set of smaller Morley dimension, contained in a translate of A^*.*

We should say that an analogous result holds for algebraic tori in place of abelian varieties.

The second kind of structures which will concern us are separably closed fields. An account of the model theory of these structures is contained in [26]. Let K be a field of characteristic $p > 0$. If K has dimension p^e over its subfield of *pth* powers, we say that K has Ershov invariant e. Let K be such. Fixing a basis $m_1, .., m_{p^e}$ for K over K^p (the field of *pth* powers) gives rise to natural functions λ_i on K for $i < p^e$: for any $a \in F$, $a = (\lambda_1(a))^p m_1 + ...(\lambda_{p^e}(a))^p m_{p^e}$. These functions are definable in the structure $(K, +, \cdot, m_1, .., m_{p^e})$. K is said to be separably closed if K has no proper separably algebraic extension. Any two separably closed fields of Ershov invariant e are elementarily equivalent. The theory of such fields (in a language with primitives for $+, \cdot, m_1, .., m_{p^e}, \lambda_1, .., \lambda_{p^e}$) is called SCF_e. It turns out that any definable set is a finite Boolean combination of zero sets of λ-polynomials, namely polynomials in various interates of the λ_i applied to the variables. Let K be a saturated separably closed field of Ershov invariant e. K will be stable, but strictly speaking has NO infinite definable sets of finite Morley dimension. However in place of definable sets, one can consider infinitely-definable sets, that is sets X which are a countable intersection of definable sets. An example is $k = \bigcap_n K^{p^n} = K^{p^\infty}$. One can reformulate Morley dimension for infinitely-definable sets, and k will have Morley dimension 1. The notion of a Zariski set can again be reformulated to make sense for infinitely-definable sets. Hrushovski shows that any infinitely definable set (in K) of Morley dimension 1 is a Zariski set. He also explains how Proposition 3.11 holds for infinitely definable Zariski sets. On the other hand, results of Messmer [27] show that any infinitely definable field of finite Morley dimension must be definably isomorphic to k. Let now A be a simple abelian variety defined over K. Let us define A^* to be $\bigcap_n p^n(A(K))$. A^* is clearly infinitely-definable in K, and Hrushovski shows it has finite Morley dimension and moreover is minimal among infinitely-definable subgroups of A. The conclusion is:

Proposition 3.15. *(K a separably closed field, $k = K^{p^\infty}$ and A a simple abelian variety defined over K.) Either there is a bijective rational homomorphism between A and a simple abelian variety defined over k, or A^* is modular.*

The third and final class of structures we will consider are fields of characteristic 0 with a *generic* automorphism. What does this mean? Let F be a field, and σ an automorphism of F. We can form *difference equations* over F. Let $x_1, .., x_n$ be indeterminates. By a difference polynomial $P(x_1, .., x_n)$ over F we mean an ordinary polynomial over F in indeterminates $\sigma^j(x_i)$, for $i = 1, 2, \ldots, n$ and $j = 0, 1, 2, \ldots$. σ is said to be generic if any finite set of difference equations and inequations over F which is satisfied in some difference field extending (F, σ) is already satisfied in (F, σ). (We could have defined differentially closed fields and separably closed fields in an analogous fashion.) We consider difference fields as structures where the primitives are $+$, $\cdot$ and σ. The class of fields with a generic automorphism turns out to be axiomatisable; the axioms (which we will not explicitly mention) are known as $ACFA$. Let (K, σ) be a saturated model of $ACFA$. K will be algebraically closed. Any definable set will have Shelah dimension, possibly infinite.

The fixed field of σ will be a pseudofinite field and will have Shelah dimension 1. A deep model-theoretic study of the models of $ACFA$ was carried out by Chatzidakis and Hrushovski [7]. A kind of Zilber dichotomy was proved in the characteristic 0 case: sets of Shelah dimension 1 are either nonorthogonal to the fixed field, or are stable and modular. Emanating from this is the following result of Hrushovski on definable subgroups of commutative algebraic groups:

Proposition 3.16. *Let (K, σ) be a model of $ACFA$. Let A be a commutative algebraic group defined over $Fix(\sigma)$. Let $p(T)$ be a nonzero polynomial over the integers. View $p(\sigma)$ as an endomorphism of A, and let $B = Ker(p(\sigma))$. Then B is a definable subgroup of A of finite Shelah dimension. Moreover, if $p(T)$ has no complex roots of unity among its roots, then B is stable and modular.*

4. A sketch of the proofs

In all cases the group Γ (whether it is an arbitrary finite-rank subgroup of A in the Mordell-Lang conjecture case, or the group of torsion points of A in the Manin-Mumford conjecture case) will be replaced by an essentially larger group B which is definable and finite-dimensional in a suitable differentially closed field, separably closed field, or model of $ACFA$.

We begin with the Mordell-Lang conjecture for function fields (Theorem 2.1). We have a pair $k < K$ of algebraically closed fields, a semi-abelian variety A over K, an irreducible subvariety X of A also over K, and a finite rank subgroup Γ of $A(K)$. We want to show that the Zariski closure of $X \cap \Gamma$ is a finite union of special subvarieties of A. So as to simplify somewhat the proof, we will assume that A is an *abelian variety* (although much of the power and simplicity of the model-theoretic approach makes itself felt in the more general semi-abelian case). We make some preliminary reductions. First we may assume, by considering separately the irreducible components of the Zariski closure of $X \cap \Gamma$, that

Assumption I. $X \cap \Gamma$ is Zariski-dense in X.
Let $Stab(X) = \{a \in A : a + X = X\}$, the algebraic-geometric stabilizer of X in A, which will be a closed subgroup of A. There is no harm in quotienting A by the connected component of $Stab(X)$, so we assume:

Assumption II. $Stab(X)$ is finite.
Under assumptions I and II, we will prove that X is special, in fact we aim for:

III. There are an abelian subvariety A' of A, an abelian variety A'' defined over k, and a subvariety X'' of A'' also defined over k, and a bijective rational homomorphism h between A' and A'' such that $h^{-1}(X'')$ is a translate of X.

From this point on, mainly for notational convenience, we will treat separately the characteristic 0 and characteristic p cases. Just note that the set-up allows us at any time to replace X by a translate of X in A.

The characteristic 0 case. We can assume K has infinite transcendence degree over k, and thus we can adjoin a derivation D to K such that (K, D) is differentially closed and k is the field of constants of A. Suppose $dim(A) = d$ (as an algebraic variety). The theory of differential algebraic groups (see [5]) enables us to find a definable homomorphism f from A onto $(K, +)^d$ whose kernel is precisely A^*. (Homomorphisms of this kind were first defined by Manin in [24] and related work.) The image of Γ under f is a finite-dimensional vector space over the rationals.

Tensoring with k yields a finite dimensional vector space H over k. Let $B = f^{-1}(H)$. Then B is a definable subgroup of A which has finite Morley dimension and contains both Γ and A^*.

We now undertake a rather canonical decomposition of A. First A is an almost direct sum of finitely many simple abelian subvarieties $A_1, .., A_r$ say. By 3.13, for each i exactly one of the following holds: (a) A_i^* is modular, or (b) A_i descends to k. Let C be the sum of those A_i satisfying (a) and D the sum of those A_i satisfying (b). Then A^* is the almost direct sum of C^* and D^*. Moreover C^* is modular and orthogonal to D^*. Also D is isomorphic to an abelian variety defined over k.

Now, let $Y = X \cap B$, a definable set in (K, D) (even a so-called "differential algebraic" set). Then Y is Zariski-dense in X. We may assume that Y has Morley degree 1. As $Stab(X)$ is finite, it is not difficult to conclude that $Stab_B(Y)$, the model-theoretic stabilizer of Y in B, is also finite. By Proposition 3.14, replacing Y and X by a suitable translate, we may assume that Y is contained in A^*. The orthogonality of C^* and D^* implies that $Y = (Y \cap C^*) + (Y \cap D^*)$. The modularity of C^*, together with Proposition 3.8, implies that $Y \cap C^*$ is essentially a coset in C^*; if this intersection is infinite, then the orthogonality of C^* to D^* implies that $Stab_{A^*}(Y)$ is infinite, a contradiction. So $Y \cap C^*$ is finite, which implies it must be at most one point. Thus replacing, if need be, Y and X by suitable translates, we may assume that Y is contained in D^*.

Let h be a rational isomorphism between D and an abelian variety A'' defined over k. From the discussion before 3.13, we see that $h(D^*) = A''(k)$. In particular, $h(Y) \subset A''(k)$. Let $X'' = h(X)$. Then X'' is the Zariski closure of $h(Y)$, so defined over k. Taking A' to be D we have obtained III.

The characteristic p case. The proof will be much like the above. However there is some difference in setting things up. Also (as we restrict ourselves to abelian varieties), Proposition 3.14 (or a suitable version for separably closed fields) will not be required. Let Γ_0 be a finitely generated subgroup of $A(K)$ whose prime-to-p division points contains Γ. Let K_0 be a finitely generated extension of k containing the generators of Γ_0. Let K_1 be the separable closure of K_0. Then (as K_0 is finitely generated over k), K_1 has finite Ersov invariant and moreover $k = K_1^{p^\infty}$. Also Γ can be seen to be contained in $A(K_1)$. For notational convenience we use K to denote this separably closed field K_1 in place of the original algebraically closed field. Some rather subtle transfer arguments allow us to assume that K is ω-saturated. Let $B_n = p^n(A(K))$, and $B = \bigcap_n B_n$. B is an infinitely-definable group. For any n, $p^n\Gamma$ has finite index in Γ, and thus meets only finitely many translates of B_n. Thus for some translate, say C_n of B_n, $X \cap C_n$ is Zariski-dense in X. We may assume that the C_n's form a descending chain, whereby it is not difficult to see that for $C = \bigcap_n C_n$, $X \cap C$ is Zariski-dense in X. Translating X we may assume that $X \cap B$ is Zariski-dense in X.

As in the characteristic 0 case, above, but now using Proposition 3.15, we write A as a sum of abelian subvarieties C and D (both defined over K), such that C^* $(= \bigcap_n p^n(C(K)))$ is modular and orthogonal to D^* and where D is weakly isomorphic to an abelian variety defined over k, and moreover $B = C^* + D^*$. Let $Y = X \cap B$. As in the characteristic 0 case, we conclude, after translating Y and X, that Y is contained in D^*. Conclusion III follows as before.

The Manin-Mumford conjecture. We will describe Hrushovski's proof, without worrying about the good bounds. Let K be a *number field*, A an abelian variety defined over K and X a subvariety of A. Let $\tilde{K}$ be the algebraic closure of K (which note is also the algebraic closure of $\mathbf{Q}$). We identify X, A with their sets of $\tilde{K}$ rational points. Let $Tor(A)$ be the group of torsion elements of A. For any prime p let $T_{p'}(A)$ be the group of torsion points whose order is prime to p. We first show that for infinitely many primes p, $X \cap T_{p'}$ is a finite union of cosets. The key point is to adjoin an automorphism σ to $\tilde{K}$, extend to an automorphism (which we also call σ) of a larger field F such that (F, σ) is a model of ACFA, and find some definable stable modular subgroup B of A of finite Shelah dimension, which contains $T_{p'}(A)$.

Let R be the ring of integers of K. We may assume A to be defined over R. Let $\mathbf{p}$ be a prime of R and let k be the residue field (a finite field of characteristic p, where $\mathbf{p}$ lives above p). Reducing the equations defining A mod $\mathbf{p}$ yields a variety $A_{\mathbf{p}}$ defined over k and living in $\tilde{k}$. $\mathbf{p}$ is said to be a prime of good reduction for A if $A_{\mathbf{p}}$ is an abelian variety of the same dimension as A. There are infinitely many primes of good reduction. Pick one, $\mathbf{p}$. Let $K_{\mathbf{p}}$ be the completion of K at $\mathbf{p}$ and let L be the algebraic closure of $K_{\mathbf{p}}$. The valuation on $K_{\mathbf{p}}$ extends to one on L, with residue field $\tilde{k}$. There is a natural map π from $A(L)$ to $A_{\mathbf{p}}(\tilde{k})$. The main point here is that π induces an *isomorphism* between the groups of prime-to-p torsion points $T_{p'}(A)$ and $T_{p'}(A_{\mathbf{p}})$. Now suppose that q is the cardinality of k, and let τ be the Frobenius automorphism $x \to x^q$ of $\tilde{k}$. Weil's theory of endomorphisms of abelian varieties yields an integral polynomial $P(T)$ such that $P(\tau)$ is 0 on $A_{\mathbf{p}}(\tilde{k})$, and $P(T)$ has no roots of unity among its roots. ($P(T)$ is just the characteristic polynomial of τ acting on some Tate module of $A_{\mathbf{p}}$.) Let ρ be a lift of τ to an element of $Gal(L/K_{\mathbf{p}})$. Then, by virtue of the aforementioned isomorphism between $T_{p'}(A)$ and $T_{p'}(A_{\mathbf{p}})$, $P(\rho)$ will vanish on $T_{p'}(A)$. Embed L in a field F and extend ρ to an automorphism σ of F in such a way that (F, σ) is a model of $ACFA$. So $T_{p'}(A)$ is contained in $B = Ker(P(\sigma))$. By Proposition 3.16, B is a definable (in (F, σ)) subgroup of $A(F)$ which is stable, modular, and with finite Shelah dimension. By Proposition 3.9, $X \cap B$ is a finite union of translates of subgroups. Thus also $X \cap T_{p'}(A)$ is a finite union of translates of subgroups.

As far as the qualitative result is concerned, it is apparently standard to deduce the desired result for *all* torsion points, making use of facts about the action of Galois on torsion, a result by Kawamata on the so-called *special set of* X and using also another prime l.

References

[1] D. Abramovich and J. Voloch, Toward a proof of the Mordell-Lang conjecture in characteristic p, International Math. Res. Notices 5 (1992), 103-115. MR **94f:**11051

[2] A. Buium, Intersections in jet spaces and a conjecture of S. Lang, Annals of Math. 136 (1992), 557-567. MR **93j:**14055

[3] A. Buium, Effective bound for the geometric Lang conjecture, Duke Math. Journal 71 (1993), 475-499. MR **95c:**14055

[4] A. Buium, Uniform bound for generic points of curves in tori, J. reine angew. Math. 469 (1995), 211-219. MR **96k:**12012

[5] A. Buium, Differential algebraic groups of finite dimension, Springer Lecture Notes 1506, 1992. MR **93i:**12010

[6] A. Buium and A. Pillay, A gap theorem for abelian varieties over differential fields, Math. Research Letters 4 (1997), 211-219.

[7] Z. Chatzidakis and E. Hrushovski, Model theory of difference fields, preprint 1995.
[8] R. Coleman, Manin's proof of the Mordell conjecture over function fields, L'enseignment Mathematique 36 (1990), 393-427. MR **92e:**11069
[9] Ph. J. Cassidy, The classification of the semisimple differential algebraic groups, Journal of Algebra 121 (1989), 169–238. MR **90g:**12007
[10] Ching-Li Chai, A note on Manin's theorem of the kernel, Amer. J. Math. 113 (1991), 387-389. MR **93b:**14036
[11] G. Faltings, Endlichkeitssatze fur abelsche Varietaten uber Zahlkorpern, Inventiones Math. 73 (1983), 349-366. MR **85g:**11026a
[12] G. Faltings, The general case of S. Lang's conjecture, in Barsotti Symposium in Algebraic Geometry, Academic Press, 1994. MR **95m:**11061
[13] H. Grauert, Mordell's Vermutung über rationale Punkte auf algebraischen Kurven und Funktionenkörper, Publ. Math. IHES 25 (1965), 131-149. MR **36:**5139
[14] M. Hindry, Autour d'une conjecture de Serge Lang, Inventiones Math. 94 (1988), 575-603. MR **89k:**11046
[15] E. Hrushovski, The Mordell-Lang conjecture for function fields, Journal of AMS 9 (1996), 667-690. MR **97h:**11154
[16] E. Hrushovski, Difference fields and the Manin-Mumford conjecture, preprint 1996.
[17] E. Hrushovski and A. Pillay, Weakly normal groups, in Logic Colloquium '85, North-Holland, 1987.
[18] E. Hrushovski and Z. Sokolovic, Minimal sets in differentially closed fields, to appear in Trans. AMS.
[19] E. Hrushovski and B. Zilber, Zariski geometries, Journal of AMS 9 (1996), 1-56. MR **96c:**03077
[20] W.A. Hodges, Model Theory, Cambridge University Press, 1993. MR **94e:**03002
[21] S. Lang, Division points on curves, Ann. Mat. Pura Appl. LXX (1965), 229-234. MR **32:**7560
[22] S. Lang, Number Theory III: Diophantine Geometry, Encyclopedia of Math. Sciences vol. 60, Springer-Verlag, 1991. MR **93a:**11048
[23] A. J. Macintyre, K. McKenna and L. van den Dries, Elimination of quantifiers in algebraic structures, Advances in Mathematics 47 (1983), 74-87. MR **84f:**03028
[24] Yu. Manin, Rational points of algebraic curves over function fields, AMS Translations Ser. II 59 (1966), 189-234.
[25] D. Marker, Model theory of differential fields, in Model Theory of Fields, D. Marker, M. Messmer and A. Pillay, Lecture Notes in Logic 5, Springer, 1996.
[26] M. Messmer, Some model theory of separably closed fields, in Model Theory of Fields, D. Marker, M. Messmer and A. Pillay, Lecture Notes in Logic 5, Springer 1996.
[27] M. Messmer, Groups and fields interpretable in separably closed fields, Transactions of AMS 344 (1994), 361–377. MR **95c:**03086
[28] A. Pillay, Geometric Stability Theory, Oxford University Press, 1996. CMP 97:07
[29] M. McQuillan, Division points on semi-abelian varieties, Inventiones Math. 120 (1995), 143-159. MR **96b:**14020
[30] M. Raynaud, Sous-variétés d'une variété abélienne et points de torsion, in Arithmetic and Geometry, Vol I, Birkhauser, 1983. MR **85k:**14022
[31] P. Samuel, Compléments à un article de Hans Grauert sur la conjecture de Mordell, Pbl. Math. IHES 29 (1966), 55-62. MR **34:**4272
[32] I. R. Shafarevich, Basic Algebraic Geometry I, Springer-Verlag, 1994. MR **95m:**14001
[33] J-P. Serre, Lectures on the Mordell-Weil Theorem, Vieweg, 1989. MR **90e:**11086
[34] S. Shelah, Classification Theory, North-Holland, 1990. MR **91k:**03085

Department of Mathematics, University of Illinois at Urbana-Champaign, Urbana, Illinois 61801

E-mail address: pillay@math.uiuc.edu