# THE JET SPACE PROOF OF THE MORDELL-LANG CONJECTURE IN CHARACTERISTIC ZERO

PAUL BAGINSKI

## 1. Introduction

The branch of logic known as model theory has flourished for the last fifty years. Sprouting from several algebraic ideas, this subject uncovers abstract, universal properties of theories which imply concrete properties about models of these theories. Examples of such concrete properties are the number of non-isomorphic models of a given cardinality and the number of definable subsets of a model of the theory. These properties correspond intuitively to the algebraic notions of isomorphism and varieties, respectively. Many other fundamental concepts in model theory have similar analogues in algebra, and it is from these analogues that the deeper ideas and theorems in model theory have emerged. Thus it comes as a surprise that for several decades, the only applications of model theory to algebra derived from concepts based only on the original algebraic roots. The techniques involved in such applications used notions such as the Compactness Theorem, model completeness, and elimination of quantifiers, all of which are not far removed from ideas at the core of mathematics. Admittedly, there had been numerous, significant contributions to algebra due to these methods, but it seemed that the deeper developments of model theory such as stability theory were not having repercussions on this branch of applied model theory. To many, the deep innovations of model theory seemed to have diverged from their algebraic roots.

Though such thought had become prevalent, several model theorists persisted in investigating the applications of deep ideas in model theory to algebra. Their work paid off in 1996 when Ehud Hrushovski tied many burgeoning ideas into a coherent proof of the Mordell-Lang conjecture of algebraic geometry. Many skeptics dismissed Hrushovski's proof as generalized algebraic techniques masked behind model theoretic terminology. They felt that the use of deeper results of model theory could be bypassed and that they were not essential to the proof. Based on precedent, these allegations were not unjustified . Adding to the skepticism of the model-theoretic nature of the proof was the fact that Faltings [8] had exhibited an algebraic proof of the characteristic zero case just a few years prior. This leap forward had many mathematicians anticipating that an algebraic proof of the positive case was forthcoming. In their eyes, Hrushovski's unified proof for all characteristics fulfilled the prophecy, albeit being mislabelled as a model-theoretic proof. However, after numerous unsuccessful attempts at reducing the argument to algebraic techniques, the overall consensus became that Hrushovski's proof intrinsically displayed a deep application of model theory. His proof of the Mordell-Lang conjecture demonstrated that over the years the ties between algebra and model theory had not faded,

*Date*: April 28, 2003.

but strengthened. Hrushovski's result has precipitated the discovery of numerous theorems. A blossoming of applications has stemmed from Hrushovski's work as model theorists begin using the wealth of knowledge that had remained untapped for applications of model theory. The ensuing results from Hrushovski, Ziegler, Pillay and others further underlined the inherent connections between algebra and model theory.

In this dissertation, we present a portion of a proof of the Mordell-Lang conjecture for characteristic zero. A good part of this proof is one put forth by Anand Pillay and Martin Ziegler [24] which utilizes the idea of differential jet spaces. The proof modifies the original proof of Hrushovski by developing an alternate framework in which to obtain a key result for the theorem. We will present a complete, detailed exposition of topics in model theory and algebraic geometry needed to understand both the statement of the theorem and its proof. The next section provides the reader with a general history for the development of the Mordell-Lang conjecture and an intuition for its utility and significance. After this prelusive chapter, we devote the rest of the dissertation to the proof of the Mordell-Lang conjecture. We partition this part of the exposition into five components: foundational algebraic geometry; foundational model theory; model theory of algebraically closed fields; model theory of differentially closed fields; and proof for characteristic zero. Our exposition will usually take an algebro-geometric perspective, in that we will usually provide intuition using algebraic ideas.

After the subsequent motivational chapter the exposition will be broken up as follows. The third chapter will provide an overview of several ideas from algebraic geometry. These ideas will vary from the most fundamental, such as the concept of varieties, to very specialized, such as the concept of an algebraic jet space (the precursor to Pillay and Ziegler's differential jet spaces). The fourth section presents the necessary background in model theory. Again, the exposition will vary from the basic idea of types to the specialized ideas of local modularity and one-basedness. When they exist, any parallels to ideas from the algebraic geometry chapter will be noted in order to underline the close ties between model theory and algebra. After these ties have been highlighted, the fifth chapter will translate many of the ideas from the third chapter into a model theoretic framework. This chapter serves as the core of the dissertation, as many of the ideas put forth will be built upon in chapters six and seven. Moreover, this chapter accustoms the reader to placing a model-theoretic interpretation of algebraic ideas. This method will be key when we translate the algebraic statement of the Mordell-Lang conjecture of chapter two into one that is more tractable from model-theoretic standpoint. Chapter six describes the framework of differentially closed fields and lays the final groundwork for the proof of the characteristic zero case. In this section, the concept of differential jet spaces will be developed with great care. These jet spaces will be the final tool needed for the presentation of the proof for characteristic zero in chapter seven. In that final section, our focus will be the presentation of Pillay and Ziegler's proof [24]. During this section we will also be explaining many components of the original Hrushovski proof.

## 2. From Diophantus to Mordell-Lang

Though the wording of the Mordell-Lang conjecture lies in the realm of abstract concepts such as abelian varieties and algebraic groups, the historical motivation

draws from the concrete idea of diophantine problems. Since the times of Diophantus of Alexandria (and probably earlier), mathematicians have been interested in the solutions to equations. The simplest such equations involve polynomials over a given field, such as the field of rationals $\mathbb{Q}$. In the attempt to find solutions to such polynomial equations, mathematicians developed the field of complex numbers $\mathbb{C}$, as well as the general theory of algebraically closed fields, where every nonconstant polynomial equation has a solution.

These developments have been promising in that they show that every polynomial equation over $\mathbb{Q}$ has a solution in $\mathbb{C}$, however it is not immediately clear how one determines whether an equation has solutions in $\mathbb{Q}$ and if so how one can determine the set of solutions. This question of decidability lay so centrally to the development of number theory that David Hilbert selected it as the tenth problem of his famous 23 problems. Since then, Matiyasevich [20] proved that it is impossible to obtain a general algorithm for determining all the integer solutions to a polynomial over $\mathbb{Q}$. It remains unsolved whether one can obtain such an algorithm for the rational solutions, but it seems that it may be just as difficult. Thus, in order to have any success, we are forced to specialize to particular kinds of polynomial equations.

By the Fundamental Theorem of Algebra, we know that any polynomial equation in only one variable has only finitely many complex (and thus finitely many rational) solutions. Hence, we proceed to the next level of difficulty: a polynomial equation $P(x, y)$ in two variables. To ease our task, we will also loosen our demands; rather than require a description of all rational solutions of $P(x, y)$, we will only concern ourselves with whether there are an infinite number of rational solutions.

As we will see in the next section, the polynomial $P(x, y)$ defines the algebro-geometric structure of a variety $V$ (we sometimes will write $V(\mathbb{C})$). This variety can be decomposed uniquely into a finite union of irreducible varieties, which over the complex numbers correspond to affine algebraic curves $C_1(\mathbb{C}), \ldots, C_n(\mathbb{C})$. Rational solutions of $P$ correspond to $C_i(\mathbb{Q})$, the rational points on the curves. Thus $P$ has infinitely many rational solutions if and only if $C_i(\mathbb{Q})$ is infinite for some $1 \leq i \leq n$. In this manner we have transferred our original problem to the problem of determining whether an affine algebraic curve $C$ has infinitely many rational points.

At this point, the curve $C$ may not have many useful properties, but there are many powerful theorems in algebraic geometry that state that a curve is birationally isomorphic to another curve with additional structure. Thus, we would be significantly empowered if our problem transferred through under birational isomorphisms. Precisely, we wish to have the following: If $C$ and $C'$ are algebraic curves defined over $\mathbb{Q}$ which are birationally isomorphic (with the isomorphism defined over $\mathbb{Q}$ as well), then $C(\mathbb{Q})$ is infinite if and only if $C'(\mathbb{Q})$ is infinite. But since algebraic curves are connected and of dimension one, rational functions are defined on all but finitely many points of the curve. Thus, the infinitude of the rational points of either curve cannot be missed by a birational isomorphism.

Now we are free to replace the curve $C$ by more tractable curves which are birationally isomorphic to $C$. It is well-known that any algebraic curve $C$ is birationally isomorphic to a smooth projective curve $C'$, where $C'$ and the birational isomorphism are defined over the same field as $C$. Our motivation for transferring the problem to projective space can be seen through the following example. Let $n > 2$ be given and consider the Pythagorean equation $X^2+Y^2 = Z^2$ and Fermat equation

$X^n + Y^n = Z^n$. Since any rational solution to either equation can be rearranged into an integral solution, we shall only concern ourselves with integral solutions. The first equation has been known since Pythagoras to have infinitely many integer solutions. The second equation also has infinitely many integer solutions (simply take $X = 0$ and $Y = Z$, for instance). Thus, in this affine setting the equations seem to be on par. However, when we transfer to the projective setting the distinction becomes clear. Every integer multiple of the points (0,1,1) and (1,0,1) (and also (1,-1,0) when $n$ is odd) is a solution in affine space to the Fermat equation. Thus, the points (0,1,1), (1,0,1), and (depending on the parity of $n$) (1,-1,0) are solutions of the Fermat equation in projective space. However, as was proven by A. Wiles ([32] and [33], these are the only integral projective points which are a solution to the Fermat equation. Thus, in projective space, the Fermat equation has only finitely many rational solutions. On the contrary, the Pythagorean equation maintains an infinite number of rational solutions even in projective space, since there are an infinite number of solutions $(x, y, z)$ none of which is a scalar multiple of another. Thus, in the realm of projective space, the distinction between the number of rational solutions to the Fermat and Pythagorean equations can be realized.

At this point, we are considering a smooth projective curve $C$ defined over $\mathbb{Q}$. Such a curve is known to be a one-dimensional, connected, compact, complex manifold, and therefore a Riemann surface. As a result, the curve has a defined genus, $g$, which topologically represents the number of holes in the curve.

In the case when $C$ has genus 0, either $C(\mathbb{Q}) = \emptyset$ or all but finitely many rational solutions are parametrized by rational functions. That is, there are rational functions $x(t), y(t)$ such that all but a finite number of rational solutions have the form $(x(t), y(t))$. For example, if we consider the equation $X^2 + Y^2 = 1$, our curve $C$ in affine space is a circle. A rational parametrization for this curve is

$$(x(t), y(t)) = (\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1})$$

and the only omitted rational solution is $(0, 1)$. Thus, we need only inspect this rational parametrization to determine the set of rational solutions.

In the case where $C$ has genus greater than 0, we are once again able to transfer the problem into a richer setting. This time, the richer setting will be that of an abelian variety (essentially a variety with the additional structure of an abelian group). Any curve $C$ of genus $g \geq 1$ can be embedded into a torus $J$, called the Jacobian of $C$. It is a well-known theorem of Riemann that the Jacobian is always an abelian variety. Furthermore, the Jacobian and the embedding are both defined over the same field as $C$ (in this case $\mathbb{Q}$), so the image $C'$ of $C$ will have infinitely many rational points precisely if $C$ has infinitely many rational points. Thus, we have translated the problem to a curve of genus $g \geq 1$ embedded in its Jacobian. This has given us the additional structure of an ambient abelian variety, and so we are able to use the Mordell-Weil theorem, which states:

**Theorem 2.1** (Mordell-Weil)**.** *If $K$ is a finitely-generated field and $A$ is an abelian variety over $K$, then $A(K)$ is a finitely generated abelian group.*

Thus, taking $K = \mathbb{Q}$ and $A$ to be the Jacobian of $C$, we conclude that $J(\mathbb{Q})$ is finitely-generated (this is the Mordell part of the theorem). Though $C(\mathbb{Q})$ will

be a subgroup of $J(\mathbb{Q})$, it will only be guaranteed to be the whole group when $C$ has genus 1 (this is because $C$ is isomorphic to $J$ for genus 1). In this case, $C(\mathbb{Q})$ is infinite precisely if $C(\mathbb{Q})$ is nonempty and the Jacobian has a point of infinite order. This is due to the fact that $C$ would be a translate of an elliptic curve with one of its rational points as its origin. In the remaining case of when $g \geq 2$, $C(\mathbb{Q})$ is in general a proper subgroup of $J(\mathbb{Q})$. Moreover, because of considerations of whether $C$ can carry an algebraic group structure, one is led to surmise that $C(\mathbb{Q})$ is finite when $g \geq 2$ (this last assertion is known as the Mordell conjecture, and was proven by Faltings [6]). Thus when $g \geq 1$, we have the following setup: an abelian variety $J$, a curve $C$ inside $J$, and a finitely-generated group $J(\mathbb{Q})$. Our goal is to conclude that under these conditions $C(\mathbb{Q}) = C(\mathbb{C}) \cap J(\mathbb{Q})$ is finite, except when $C$ is a translate of an elliptic curve. Abstracting slightly from this setup, we yield the following conjecture:

**Conjecture 2.2** (Lang's conjecture for curves)**.** *Let $X$ be a complex curve of genus $g \geq 1$ lying inside a complex abelian variety $A$. Let $\Gamma$ be a finitely-generated subgroup of $A$. Then $X(\mathbb{C}) \cap \Gamma$ is finite unless $X$ is a translate of an elliptic curve.*

This conjecture generalized the Mordell conjecture, however, Lang observed that even this conjecture could be generalized further to arbitrary abelian varieties $A$ and subvarieties $X$ defined over an algebraically closed field $K$. He realized that although one is not likely to have $X(K) \cap \Gamma$ to be finite, it nonetheless possesses a finiteness structure. Specifically, his conjecture was:

**Conjecture 2.3** (Mordell-Lang conjecture)**.** *Let $K$ be an algebraically closed field and let $A$ be an abelian variety defined over $K$. Let $X$ be a subvariety of $A$ and let $\Gamma$ be a finitely-generated subgroup of $A$. Then there are $\gamma_1, \ldots, \gamma_m \in \Gamma$, abelian subvarieties $B_i, \ldots, B_n$ of $A$ such that $\gamma_i + B_i \subseteq X$ for each $1 \leq i \leq m$ and*

$$X(K) \cap \Gamma = \bigcup_{i=1}^{m} \gamma_i + (B_i(K) \cap \Gamma).$$

This conjecture subsumes Lang's conjecture for curves, for if a complex curve $X$ is a translate of an elliptic curve, then since an elliptic curve is an abelian variety the conclusion of the Mordell-Lang conjecture holds. Otherwise, Lang's conjecture says that $X(\mathbb{C}) \cap \Gamma$ is finite, say $\{\gamma_1, \ldots, \gamma_m\}$. But then since $\{0\}$ is an abelian variety, we have that $X(\mathbb{C}) \cap \Gamma = \cup_{i=1}^{m} \gamma_i + (\{0\} \cap \Gamma)$, and so the conclusion of Mordell-Lang holds in this case as well.

In this manner, we have come from the concrete problem of determining rational solutions to a polynomial in two variables to the abstract formulation of the Mordell-Lang conjecture. Thus, a proof of the Mordell-Lang conjecture not only has repercussions for the theory of abelian varieties, but also at a very basic level it affects the theory of diophantine problems.

This history of the Mordell-Lang conjecture combines the expositions of Thomas Scanlon [27] and Marc Hindry [10]. I would like to also take this opportunity to thank the first author for clarifying some points of the proof of the Mordell-Lang conjecture during my visit to Berkeley in the Spring of 2003.

## 3. Foundational Algebraic Geometry

In this section, we will work through the basic ideas from algebraic geometry which will be needed for the proof. These ideas will also be the source for examples and intuitive explanations. For the entirety of this exposition, all our fields will have characteristic zero, though we remark that many results hold for fields of any characteristic. For this section, the field $K$ will furthermore be algebraically closed.

The most fundamental concept to algebraic geometry is the notion of a variety. There are two fundamental kinds of varieties, affine and projective; the idea of an abstract variety provides a unification of these similar concepts under one encompassing notion. In order to avoid too much deviation, we will not provide a lengthy discussion of projective varieties and projective space, but rather concentrate on affine varieties for the main source of intuition. An affine variety represents the set of simultaneous solutions to a system of polynomial equations over affine space (analagously, a projective variety will be the set of simultaneous solutions to a system of polynomial equations over projective space, but more on this later). Precisely, we have the following definition of an affine variety.

**Definition 3.1.** Given a set $I$ of polynomials in $K[x_1, \ldots, x_n]$, we denote by $V(I)$ the subset of $K^n$ each of whose points is a simultaneous zero for all the polynomials in $I$. Explicitly, $V(I) = \{a \in K^n \,|\, P(a) = 0 \ \forall P \in I\}$. An **affine variety** is a set $V \subseteq K^n$ which is $V(I)$ for some $I \subseteq K[x_1, \ldots, x_n]$. Given an affine variety $V \subseteq K^n$, we define $I(V) = \{P \in K[x_1, \ldots, x_n] \,|\, P(a) = 0 \ \forall a \in V\}$.

There are several immediate consequences of the definition that are worthy of enumeration:

(1) $I(V)$ is an ideal,
(2) $V(I(V)) = V$,
(3) $I(V(I)) \supseteq I$,
(4) $I_1 \subseteq I_2 \Rightarrow V(I_1) \supseteq V(I_2)$,
(5) $V_1 \subseteq V_2 \Rightarrow I(V_1) \supseteq I(V_2)$.

The first two consequences indicate that we need only consider subsets $I \subseteq K[x_1, \ldots, x_n]$ which are ideals in order to define varieties. The second and third consequences further illustrate that the functions $V$ and $I$ are nearly inverse to each other. The following celebrated theorem of Hilbert gives a precise characterization of the case when $V$ and $I$ are inverse.

**Theorem 3.2** (Hilbert's Nullstellensatz)**.** *For any ideal $I$ of $K[x_1, \ldots, x_n]$,*

$$I(V(I)) = \sqrt{I}$$

*where $\sqrt{I} = \{P \in K[x_1, \ldots, x_n] \,|\, \exists n \ P^n \in I\}$ denotes the radical of $I$.*

*Proof.* see any standard commutative algebra text, such as page 412 of [12]. □

Thus, the Nullstellensatz indicates that $V$ and $I$ are order-reversing bijections between the set of affine varieties of $K^n$ and the set of radical ideals in $K[x_1, \ldots, x_n]$.

The intersection of any family $(V_j | j \in J)$ of affine varieties is also an affine variety given by $\bigcap_{j \in J} V_j = V(\bigcup_{j \in J} I(V_j))$. The union of any two affine varieties $V_1$ and $V_2$ is itself an affine variety: namely $V_1 \cup V_2 = V(\{P_1 P_2 \,|\, P_1 \in I(V_1),\ P_2 \in I(V_2)\})$. Since the empty set and the whole space are affine varieties ($\emptyset = V(K[x_1, \ldots, x_n])$

and $K^n = V(\emptyset)$), we have just shown that the affine varieties on $K^n$ are the closed sets of a topology called the **Zariski topology**.

The Zariski topology has some unusual topological properties. Any two open sets have a nonempty intersection; thus the Zariski topology is not Hausdorff. In fact every open set is dense. Though the Zariski topology possesses these properties which seem to indicate that it is not "well-behaved", the following proposition shows that the topology exhibits a powerful property.

**Proposition 3.3.** *The Zariski topology on $K^n$ is Noetherian (every intersection of closed sets is equal to a finite subintersection).*

*Proof.* Let $V = \cap_{\beta<\alpha} V_\beta$ be given and without loss of generality, assume the $V_\beta$ form a decreasing chain. Then $(I(V_\beta) \mid \beta < \alpha)$ forms an increasing chain of ideals in $K[x_1, \ldots, x_n]$. Since $K[x_1, \ldots, x_n]$ is a Noetherian ring, there is an $n < \omega$ such that $I(V_\beta) = I(V_n)$ for all $n \leq \beta < \alpha$. But $V = V(\bigcup_{\beta<\alpha} I(V_\beta)) = V(I(V_n)) = V_n$. □

The "finiteness" afforded by the Noetherian nature of the Zariski topology will be of vital importance for definability considerations in section 5.

A natural topological question to ask at this point (whose answer will be of importance to us when we define completeness) is whether the Zariski topology on a product is equal to the product of the Zariski topologies. The answer is no, however we have the following relationship:

**Proposition 3.4.** *The Zariski topology on $K^{2n}$ is strictly finer than the product of the Zariski topologies on $K^n$.*

*Proof.* Affine varieties in $K^{2n}$ are defined by ideals of polynomials $P(\bar{x}, \bar{y})$, where $\bar{x}$ and $\bar{y}$ each denote $n$ free variables. If $V$ and $W$ are varieties in $K^n$, then $V \times W$ is a variety in $K^{2n}$ with $I(V \times W) = (I(V)_{\bar{x}}, I(W)_{\bar{y}})$. Here $I(V)_{\bar{x}}$ denotes that the polynomials in $I(V)$ are written in terms of the free variables $\bar{x}$ and $I(W)_{\bar{y}}$ are the polynomials of $I(W)$ written using the free variables $\bar{y}$. Then $I(V \times W)$ is the ideal in $K[\bar{x}, \bar{y}]$ generated by the two ideals $I(V)_{\bar{x}}$ and $I(W)_{\bar{y}}$. Thus, we have shown that every product of varieties is a variety, and since varieties are closed under finite unions and arbitrary intersections, we have that the Zariski topology on $K^{2n}$ is finer than the product topology.

To show that it is strictly finer, consider the diagonal $\Delta = \{(\bar{a}, \bar{b}) \in K^{2n} \mid a = b\}$. The diagonal is clearly a variety since it is defined by ideal of the polynomial $\bar{x} - \bar{y} = 0$. However the diagonal is never in the product topology. Since any two open sets $U$ and $U'$ in $K^n$ have a nonempty intersection, there is an $\bar{a} \in K^n$ such that $(\bar{a}, \bar{a}) \in U \times U'$. Since every open set in the product topology must contain $U \times U'$ for some open sets $U, U'$ in $K^n$, we conclude that every open set in the product topology must intersect $\Delta$. Thus $\Delta$ cannot be closed. □

Thus, the Zariski topology on the product $V \times W$ of two varieties $V$ and $W$ is finer than the product topology on $V \times W$ (simply find an $n$ such that both $V$ and $W$ are embeddable into $K^n$; the Zariski topology on $V \times W$ is a subspace topology for the Zariski topology on $K^{2n}$).

In addition to yielding a topology, affine varieties also possess a well-behaved factorization theory. That is, there is a subclass of varieties which can be considered

"irreducible" such that there is a unique (modulo some considerations) decomposition of any affine variety into irreducible varieties. The exact nature of these notions is elucidated through the next series of definitions and theorems.

**Definition 3.5.** An affine variety $V$ is **irreducible** if whenever $V_1$ and $V_2$ are affine varieties such that $V_1 \cup V_2 = V$ then $V_1 = V$ or $V_2 = V$.

**Proposition 3.6.** *An affine variety $V$ is irreducible if and only if $I(V)$ is prime.*

*Proof.* Suppose $I(V)$ is prime, and $V = V_1 \cup V_2$ for some varieties $V_1$ and $V_2$. Then $I(V) \supseteq \{P_1P_2 \,|\, P_1 \in I(V_1),\ P_2 \in I(V_2)\}$. Either $I(V) \supseteq I(V_1)$, or else we may choose $P \in I(V_1)\backslash I(V)$. Since $PP' \in I(V)$ for every $P' \in I(V_2)$, by primality of $I(V)$ we have that $I(V_2) \subseteq I(V)$. Thus $V \subseteq V_1$ or $V \subseteq V_2$ and so $V$ is irreducible.

Conversely, if $I(V)$ is not prime, then we may choose $P_1, P_2 \notin I(V)$ such that $P_1P_2 \in I(V)$. Set $V_1 = V(I(V) \cup \{P_1\})$ and $V_2 = V(I(V) \cup \{P_2\})$. Then $V_1, V_2 \subset V$, but

$$\begin{aligned} V_1 \cup V_2 &= V(\{P_1P_2\} \cup \{P_1P \,|\, P \in I(V)\} \cup \{P_2P \,|\, P \in I(V)\} \cup I(V)) \\ &= V(I(V)) \\ &= V \end{aligned}$$

so $V$ is not irreducible. □

Since $K[x_1, \ldots, x_n]$ is a Noetherian ring, ideals are finitely-generated, and moreover prime ideals are finitely-generated by irreducible polynomials. Thus even though our definition of irreducibility was purely topological (it was simply a statement about closed sets), it precisely links the algebraic notion of irreducibility to the topology. Since $K[x_1, \ldots, x_n]$ is a Unique Factorization Domain, every polynomial can be factored into a product of irreducible polynomials. Translating this statement to a topological analogue, we would ideally desire every variety to be equal to a "product" of irreducible varieties. As the next important theorem shows, the analogue transfers to the topological context when we consider "product" to mean union.

**Theorem 3.7.** *[Decomposition Theorem] Every affine variety $V$ is equal to a finite union of irreducible varieties $W_i$, $1 \leq i \leq n$. This decomposition is unique if we do not consider decompositions where $W_i \subseteq \bigcup_{j \neq i} W_j$ for some $1 \leq i \leq n$.*

*Proof.* Since we are dealing with a Noetherian topology, the collection of all subvarieties of a given variety $V$ (ordered by inclusion) is a well-founded partially ordered set. Consequently we may prove this theorem by induction on $V$: if $V$ is reducible, then $V = V_1 \cup V_2$ for some proper subvarieties $V_1$ and $V_2$. By induction $V_1$ and $V_2$ have unique decompositions into irreducible subvarieties. These two decompositions combine to give a decomposition of $V$ (we must be a little careful in which varieties to omit in order to satisfy the condition that no variety is contained in the union of the rest, but this is not difficult). Suppose now that $V$ has decompositions $W_1, \ldots, W_n$ and $W_1', \ldots, W_m'$, where $n \leq m$. Then

$$W_1 = V \cap W_1 = \bigcup_{j=1}^{m} (W_j' \cap W_1).$$

As each $W_j' \cap W_1$ is closed and $W_1$ is irreducible, it must be that $W_1 = W_j' \cap W_1$ for some $1 \leq j \leq m$, say $j = 1$. Using the same argument with $W_1'$ in place of $W_1$,

we are forced to conclude by irreducibility that $W_1' = W_1' \cap W_1$, whence we have $W_1 = W_1'$. Repeat this process to show that (after rearranging) $W_i = W_i'$ for all $1 \leq i \leq n$. Because our decompositions do not allow for proper subvarieties, we finally conclude that $n = m$. □

We will now quickly remark on projective space and projective varieties. Given affine $n+1$ space $A^{n+1} = K^{n+1}$ we will define the **projective space** $\mathbb{P}^n$ to be the set of all equivalence classes $[\bar{a}]_\sim$, where $\bar{a} \sim \bar{b} \Leftrightarrow \exists \alpha \in K\ \bar{a} = \alpha \bar{b}$. Thus, the equivalence class of $\bar{a}$ is the line in $K^{n+1}$ through $\bar{a}$ and the origin. One easily checks that one can define field operations on $P^n$ by $[\bar{a}]+[\bar{b}] = [a \bar{+} b]$ and $[\bar{a}][\bar{b}] = [\bar{ab}]$. This will yield that the additive identity is $[\bar{0}]$ and the multiplicative identity is $[\bar{1}]$. One can further transfer over affine polynomials so that they are interpretable in projective space via a process called homogenization. A polynomial is called homogeneous if every term has the same degree (sum of the exponents of all the variables). For instance $X_1X_2^3 + X_3^4$ is homogeneous, whereas $X_1X_2^3 + X_2^3$ is not. Given a polynomial equation $P(X_1, \ldots, X_n) = 0$, we obtain a homogeneous polynomial equation $Q(X_1, \ldots, X_n, Z) = 0$ by multiplying terms of $P$ by powers of $Z$. For instance, the homogenization of $X_1X_2^3 + X_2^3 + a = 0$ is $X_1X_2^3 + X_2^3Z + aZ^4 = 0$. Homogenization is also invertible by substituting $Z = 1$; this is called dehomogenization. If $P(\bar{X})$ is a homogeneous polynomial, then $P(\bar{a}) = 0$ if and only if $P(\alpha\bar{a}) = 0$ for every $\alpha \in K$. Hence, we may say that $[\bar{a}]$ is a solution of $P$ when $P(\bar{a}) = 0$. With this notational groundwork, we now may analagously define **projective varieties** as sets of solutions to *homogeneous* polynomials in projective space. All our results for affine varieties, including having a Noetherian Zariski topology and the Decomposition theorem transfer to the projective setting.

We would now like to define the concept of an abstract variety, which subsumes the concepts of affine and projective varieties. We would also like to define this notion so that we may enjoy a Noetherian Zariski topology on abstract varieties, and also possess a decomposition theorem. But in order to provide such a notion, we must first consider morphisms between varieties.

**Definition 3.8.** A **morphism** from an affine variety $V \subseteq K^n$ to an affine variety $W \subseteq K^m$ is a map $f = (f_1, \ldots, f_m) : V \to W$ where each $f_i \in K[x_1, \ldots, x_n]$ is a polynomial map. An **isomorphism** is a bijective morphism whose inverse is also a morphism. A function $f$ from $V$ to $K$ is said to be **regular at** $a \in V$ if there is a Zariski open neighborhood $U$ of $a$ and there are polynomials $P, Q \in K[x_1, \ldots, x_n]$ such that $Q$ is everywhere nonzero on $U$ and $f = P/Q$ on $U$. A function $f$ from a Zariski open set $U$ to $K$ is **regular** if it is regular at each of its points.

*Remark* 3.9. *The correct definition of morphism requires that each $f_i \in K[V] = K[x_1, \ldots, x_n]/I(V)$, however, we can content ourselves in only considering representatives of these equivalence classes to be our functions. A concise explanation of the validity of this consideration follows Definition 3.15.*

**Definition 3.10.** A **quasi-affine variety** is a Zariski open set $U$ possessing the induced subspace topology.

With this set of definitions in hand, we are now able to define an abstract variety and also morphisms between abstract varieties.

**Definition 3.11.** An **(abstract) variety** is a set $V$ equipped with a finite open covering by subsets $V_1, \ldots, V_n$ and with maps $f_i : V_i \to U_i$, such that for each $1 \leq i, j \leq m$

(1) $f_i$ is a bijection and $U_i$ is an affine variety.
(2) $U_{ij} = f_i(V_i \cap V_j)$ is an open subset of $U_i$.
(3) $f_j \circ f_i^{-1}$ is an isomorphism between the quasi-affine varieties $U_{ij}$ and $U_{ji}$.

We say that $(V, V_i, f_i)$ is defined over a field $k$ if all the $U_i$ and the maps $f_j \circ f_i^{-1}$ are all defined over $k$.

One obtains a Zariski topology on $V$ by defining $U \subseteq V$ to be open precisely if $f_i(U \cap V_i)$ is open in $U_i$ for each $i$. It is clear that this topology is Noetherian as well since the topologies on the $U_i$ are all Noetherian. One can now define topological concepts such as irreducibility and the like in a similar manner to before. One can quickly verify that both affine varieties and projective varieties are abstract varieties.

**Definition 3.12.** Let $(V, V_i, f_i)$ be an irreducible variety. A **rational function** $f : V \to K$ is a regular function from some open subset $U$ of $V$ to $K$. A function $f : V \to W$ is a **birational isomorphism** if it is an isomorphism between open subsets of $V$ and $W$. In this case, we say $V$ and $W$ are **birationally isomorphic**.

*Remark* 3.13. *One can use morphisms to perform a so-called* **change of coordinates***, that is, given a point $x$ of $K^n$ we can find an isomorphism of $K^n$ with itself that maps $x$ to* 0*.*

The general definition of an algebraic variety can be interpreted as follows: at any point, there is a neighborhood around that point which is isomorphic to an affine variety. That is, the algebraic variety resembles an affine variety locally at every point. This definition resembles the definition for a differential manifold, namely that at any point of the manifold, there is a neighborhood around that point resembling a Euclidean subspace. Due to this similarity in structure, one is encouraged to try to transfer some basic notions from differential geometry to algebraic geometry. The simplest of these is the tangent space at a point, which is usually constructed by considering a neighborhood which is locally Euclidean and taking a tangent space to this Euclidean subspace. Thus, our definition will also be based on the local behavior, i.e. we only need to construct the tangent space at a point of an *affine* variety. Intuitively, if a line in the plane intersects a convex (or concave) piece of a one-dimensional smooth curve it will do so in two points, unless it is tangent to the curve. In this case, the line intersects the piece in only one point, but we may say intuitively that this intersection has "multiplicity" two. We will now formalize this idea of intersection multiplicity in order to aid in the construction of a tangent space.

Let a point $x$ of an affine variety $X \subseteq K^n$ be given, and perform a change of coordinates such that $x$ is the origin $0 = (0, 0, \ldots, 0)$. Then given any other point $a \in K^n$, the unique line connecting $a$ and $x$ is given by $L_a = \{ta \,|\, t \in K\}$. If $I(X) = \{F_1, \ldots, F_r\}$, then the line $L_a$ intersects $X$ for all values of $t \in K$ such that $F_1(ta) = F_2(ta) = \ldots = F_r(ta) = 0$. Thus, our points of intersection are completely determined by the functions $F_1(ta), \ldots, F_r(ta)$ of the single variable $t$. Namely, if $f(t)$ is the greatest common divisor of $F_1(ta), \ldots, F_r(ta)$, then each zero

of $f$ is a value of $t$ for which $ta$ is an intersection point. Furthermore, $f$ precisely defines our notion of multiplicity of the intersection. The number of times $t$ appears as a root of $f$ is defined to be the **multiplicity** of the intersection of the line $L_a$ with the variety $X$ at the point $ta$. Since $L_a$ and $X$ by construction intersect at $x$, this intersection has multiplicity at least one. We define the **tangent space** $\mathcal{T}_x(X)$ of $X$ at $x$ to be the union of all lines $L_a$ whose intersection with $X$ at $x$ has multiplicity greater than 1. In other words, if $m_x(a)$ denotes the multiplicity of the intersection of $L_a$ and $X$ at $x$, then

$$\mathcal{T}_x(X) = \bigcup \{L_a \mid a \in K^n,\ a \neq x,\ m_x(a) > 1\}.$$

**Proposition 3.14.** *$\mathcal{T}_x(X)$ is a $K$-linear subspace of $k^n$.*

*Proof.* Since $x = 0$ is a root of each $F_i$, we have that the constant terms of all the $F_i$ are zero. Thus, each can be broken up as $F_i = G_i + H_i$, where $G_i$ is the linear part of $F_i$ and $H_i$ is the remaining part. The intersection at $x$ of the line $L_a$ has multiplicity greater than 1 if and only if $t^2$ divides $f(t)$, which occurs precisely when $t^2$ divides each $F_i(ta)$. Since $t^2$ already divides $H_i(ta)$, we have that $t^2$ divides $F_i(ta)$ if and only if $G_i(a) = 0$. Thus, $a \neq x$ is in $\mathcal{T}_x(X)$ precisely when $G_1(a) = \ldots = G_r(a) = 0$. Since these constraints are $K$-linear, the resulting space $\mathcal{T}_x(X)$ is also clearly $K$-linear. □

In particular, we have that $\mathcal{T}_x(X)$ is finite-dimensional. Furthermore, this dimension is independent of the choice of the representative $F_i$ and is invariant (preserved under isomorphisms of $X$). For further information on tangent spaces, as well as a proof of the invariance of the tangent space, the reader is advised to consult [28].

We will now proceed with the construction of algebraic jet spaces. This construction will be mimicked to a significant extent in chapter five, where we construct differential jet spaces. We will also show that algebraic jet spaces are a generalization of tangent spaces, or more precisely, characterizations of weaker notions of tangent spaces.

**Definition 3.15.** Let $X \subseteq K^n$ be an irreducible affine variety. The **coordinate ring** $K[X]$ of $X$ over $K$ is defined to be $K[X] = K[x_1, \ldots, x_n]/I(X)$. The **function field** $K(X)$ of $X$ over $K$ is the field of fractions of the coordinate ring $K[X]$.

We will write elements of $K[X]$ as $[f]_X$, where $f \in K[x_1, \ldots, x_n]$, and just simply $f$ when $X = K^n$. Given any point $a \in X$, we define a ring

$$\mathcal{M}_a(X) = \{[f]_X \in K[X] \mid f(a) = 0\}.$$

Since $f(a) = 0$ for each $f \in I[X]$, we conclude that for any $f, g \in K[x_1, \ldots, x_n]$, if $f - g \in I[X]$ then $f(a) = g(a)$. Thus, $\mathcal{M}_a(X)$ is indeed well-defined. Furthermore, we have that $\mathcal{M}_a(X)$ is a Noetherian ring, being a subring of the Noetherian ring $K[X]$. We also may view $\mathcal{M}_a(X)$ as a (proper) ideal of $K[X]$, and consequently use Corollary 10.18 of [1] to conclude $\bigcap_n \mathcal{M}_a(X)^n = (0)$. Since $\mathcal{M}_a(X)$ is Noetherian, we have the stronger conclusion that $\mathcal{M}_a(X)^n = (0)$ for some $n$, however we will not need this fact.

For each $m \geq 2$, we may consider the $k$-vector space $\mathcal{M}_a(X)/\mathcal{M}_a(X)^m$. This vector space is finite dimensional since $\mathcal{M}_a(X)$ is a finitely-generated ideal.

**Definition 3.16.** The dual space of $\mathcal{M}_a(X)/\mathcal{M}_a(X)^m$ is called the $(m-1)$st **jet space** of $X$ at $a$. We denote the $(m-1)$st jet space of $X$ at $a$ by $J_a^{m-1}(X)$.

Another common name for $J_a^m(X)$ is the $m$-jet of $X$ at $a$. When $X = K^n$ we shall simply write $J_a^m$ and $\mathcal{M}_a$. The jet space for $X = K^n$ acts as a universal jet space in the sense of the following proposition.

**Proposition 3.17.** *Let an irreducible affine variety $X \subseteq K^n$ be given. There is a canonical linear embedding from $J_a^m(X)$ into $J_a^m$.*

*Proof.* $M_a$ maps naturally (via the quotient map) onto $M_a(X)$ and so there are also natural mappings of $M_a/M_a^m$ onto $M_a(X)/M_a(X)^m$. By duality, we get an embedding in the reverse direction, namely from $J_a^{m+1}(X)$ into $J_a^{m+1}$. □

From this point on, we shall identify $J_a^m(X)$ with its image in $J_a^m$.

According to Corollary 1 of Chapter II, Section 1.3 of [28], the first jet space $J_a^1(X)$ is isomorphic to the tangent space $\mathcal{T}_a(X)$ of $X$ at $a$.

Now that we have a picture of jet spaces, we may consider how jet spaces over different affine varieties interact. Namely, we will prove the following fundamental result:

**Proposition 3.18.** *Let $X, Y$ be irreducible subvarieties of $k^n$ and $a \in X \cap Y$ be given. Then $J_a^m(X) = J_a^m(Y)$ for all $m \geq 1$ iff $X = Y$.*

*Proof.* Let $f \in I_X$ be given and fix $m \geq 2$. Then $f/\mathcal{M}_a^m$ is mapped to $[f]_X/\mathcal{M}_a^m(X)$ under the canonical linear embedding. But since $f \in I_X$, $[f]_X = [0]_X$ and so $[f]_X \in \mathcal{M}_a(X)^m$ is mapped to 0 by $J_a^{m-1}(X)$. Transferring the statement back to $J_a^{m-1}$ via the canonical embedding, we see that $J_a^{m-1}(X)$ (now considered as a subspace of $J_a^{m-1}$) maps $f/\mathcal{M}_a^m$ to 0. But as subspaces of $J_a^{m-1}$, $J_a^{m-1}(X) = J_a^{m-1}(Y)$, so $J_a^{m-1}(Y)$ maps $f/\mathcal{M}_a^m$ to 0. Consequently, transferring again under the canonical embedding, $J_a^{m-1}(Y)$ maps $[f]_Y/\mathcal{M}_a^m(Y)$ to 0, and so $[f]_Y \in \mathcal{M}_a^m(Y)$. Since $m \geq 2$ was arbitrary, we have $[f]_Y \in \bigcap_{m<\omega} \mathcal{M}_a^m(Y) = \{[0]_Y\}$. Thus $f$ must be in $I_Y$. Reversing roles of $X$ and $Y$ in the proof yields that $I_X = I_Y$ and so $X = Y$. □

Since every affine variety has a unique decomposition into irreducible components, we may extend the notion of jet space to arbitrary affine varieties by defining the jet space at each point to be the jet space at that point for the corresponding irreducible component. Jet spaces can also be defined for $K$-rational points $a$ of arbitrary varieties $X$. Around each point $a \in X(K)$, there is a minimal affine neighborhood $Y_a$. Indeed we need only take $Y_a$ to be the intersection of all neighborhoods of $a$ which are affine; this is equal to a finite intersection of such neighborhoods by the Noetherianness of the Zariski topology. Consequently $Y_a$ is itself an affine neighborhood of $a$. Now we define the jet space at $a$ for $X$ to simply be the jet space at $a$ for the affine variety $Y_a$. The above theorem holds for arbitrary varieties as well.

If $f$ is a morphism over $K$ from the variety $X$ to the variety $Y$ and $a \in X(K)$, then $f$ induces a canonical linear map $J_a(f) : J_a^m(X) \to J_{f(a)}^m(Y)$. In fact, $J$ is a functor.

These facts about algebraic jet spaces will be utilized again when we deal with differential jet spaces, but for now we set aside our consideration of algebraic jet spaces.

For the remainder of this section we will develop the theory of varieties that also have additional algebraic structure, such as that of a group.

**Definition 3.19.** An **algebraic group** is a variety $V$ together with morphisms $\mu : V \times V \to V$ and $\iota : V \to V$ such that $\mu$ gives a group operation on $V$, and $\iota$ is the map $x \mapsto x^{-1}$. We say that the algebraic group $(V, \mu, \iota)$ is defined over the field $k$ if $V, \mu, \iota$ are all defined over $k$. In general, we will just write $V$ when referring to an algebraic group.

There are a few standard examples of algebraic groups. Of course, the additive group structure of $K^n$ defines an algebraic group.

A second example is the group $SL_n(K)$ considered as a subset of $K^{n^2}$. It is a variety since it is defined by the polynomial equation $det(M) = 1$, and matrix multiplication gives it a group structure such that the group operations are morphisms. One also has that $GL_n(K)$ is an algebraic group, though with a slightly more complicated construction of the underlying variety. We cannot use the method we employed for $SL_n(K)$ since we would have that $GL_n(K)$ is defined by the equation $det(M) \neq 0$. This defines a Zariski open set, rather than a Zariski closed set. Indeed, this is the case when we consider $GL_n(K)$ as a subset of $K^{n^2}$. Instead we shall consider the set

$$\{(M, \gamma) \in GL_n(K) \times K \mid \gamma det(M) - 1 = 0\},$$

which is clearly a variety in $K^{n^2+1}$. The group operation is easily defined in terms of matrix multiplication, which yields that this set is isomorphic as a group to $GL_n(K)$. Consequently we may consider $GL_n(K)$ as an algebraic group.

*Remark* 3.20. *In this last example we began with the group $GL_n(K)$ and found an isomorphic group which was an algebraic group. This is an occurrence of a more general phenomenon predicted by a result known as Weil's Theorem (Theorem 7.10). We will speak more on this theorem later in our discussion, but suffice it to say that we were able to find such an isomorphic group because $GL_n(K)$ was a "definable" group.*

Another example of an algebraic group is that of an elliptic curve. An **elliptic curve** is a projective curve given by the homogenization of a polynomial of the form

$$Y^2 = X^3 + aX + b,$$

where $a, b \in K$. For example, the projective curve given by $ZY^2 = X^3 + a^2XZ^2$ is an elliptic curve, where $a \in K$. A powerful result of algebraic geometry is that every elliptic curve has an associated group structure (see section 1.7 of [13] or section 1.4 of [29] for the construction). Thus, every elliptic curve is an algebraic group (in fact it is even an abelian variety).

**Definition 3.21.** A variety $V$ is **complete** if for any variety $Y$ the projection $\pi : V \times Y \to Y$ is a closed map, where both spaces are in the respective Zariski topologies. As a reminder, a closed map by definition maps closed sets to closed sets.

**Proposition 3.22.** *A closed subset $W$ of a complete variety $V$ is complete.*

*Proof.* Let $Y$ be a variety and consider the Zariski topology on $V \times Y$. Proposition 3.4 indicates that this Zariski topology is finer than the product topology. Therefore $W \times Y$ is closed in the Zariski topology since $W$ is closed and so $W \times Y$ is closed in the product topology. Consequently, any closed subset of $W \times Y$ is a closed subset of $V \times Y$ and hence is mapped to a closed subset of $Y$ under projection by the completeness of $V$. So $W$ is complete. □

**Definition 3.23.** An algebraic group is **connected** if it contains no proper algebraic subgroup of finite index.

**Proposition 3.24.** *Every algebraic group $G$ has a subgroup $G'$ of finite index which is connected.*

*Proof.* Take the intersection $G'$ of all algebraic subgroups of $G$ which have finite index. Since every algebraic subgroup of $G$ is a variety, $G'$ is an intersection of varieties. Since the Zariski topology is Noetherian, it must be that $G'$ is equal to a finite intersection of algebraic subgroups of $G$ with finite index. Thus $G'$ itself must be an algebraic subgroup of $G$ with finite index; in fact it is the algebraic subgroup of $G$ with greatest finite index. □

**Definition 3.25.** An **abelian variety** is a complete connected algebraic group.

*Remark* 3.26. *When we use the phrase "$B$ is an abelian subvariety of $A$" we will always mean that $B$ is an abelian variety which is a subvariety of $A$ and $B$'s group structure is a subgroup of $A$. That is, we wish that the abelian variety $B$ be both a subgroup and a subvariety.*

As one might expect from the name, an abelian variety is guaranteed to be an abelian group. Though the proof is short and sweet, we shall omit it and instead refer the reader to Example 4.6 in [23] for a proof.

Proposition 3.22 indicates that any connected algebraic group in an abelian variety must be an abelian variety as well.

We conclude this section with a statement on quotients of abelian varieties:

**Proposition 3.27.** *Let $B \subseteq A$ be abelian varieties such that $B$ is an abelian subvariety of $A$. Then the quotient group $A' = A/B$ is an abelian variety and the canonical projection $\pi : A \to A'$ is a morphism.*

*Proof.* Left to the reader.

The results regarding tangent spaces followed the exposition in [28]. The development of algebraic jet spaces mimicked that in [24].

## 4. Foundational Model Theory

Since the proof of the Mordell-Lang conjecture we wish to present involves heavy model-theoretic machinery, we must prepare the reader with his arsenal. These tools from model theory will be employed heavily in the subsequent chapters. In the next chapter, we will interpret ideas in algebraic geometry from a model theoretic

standpoint, while in later chapters we will introduce new ideas with model-theoretic considerations frequently interspersed.

Define types, stationary types, saturated models, monster model, Morley rank, $\aleph_0$-stability,

**Theorem 4.1.** *In $\aleph_0$-stable theory types are definable.*

*Proof.* see any standard introductory text on model theory, such as [9] or [19].

strongly minimal sets, canonical basis, local modularity, one-basedness, genericity, orthogonality.

**Definition 4.2.** Given sets $A$ and $B$ and a tuple $c$, we say that $tp(c/A)$ is **internal** to $B$ if there is a $d$ independent from $c$ over $A$ and there is a tuple $b \in B$ such that $c$ is definable over $A, d, b$.

Let us develop an intuitive grasp of the concept of internality. Assume $c$ is definable over $A, d, b$, and consider $p = tp(c/A)$. The set $A$ is already necessary to the definition of $p$. Internality states that the only additional "information" we need is $d$ and some tuple $b \in B$. But since $c$ and $d$ are independent over $A$, $d$ does not really add much information about the type $p$. Consequently, the core of the "extra" information needed to define $p$ comes from $b$, i.e. from parameters inside $B$.

## 5. Model Theory of Algebraically Closed Fields

Since algebraically closed fields form the underlying framework of the proof, this section will present a general model theoretic view of several facts from the theory of algebraically closed fields. The developments in this section will also prime the reader before he encounters the specialization in the more complicated setting of differentially closed fields.

Interpret ideas from section 3 from a model-theoretic point of view. Show how closed sets in the Zariski topology are definable and how a definable map on a set $S$ can be definably extended to a definable map on the closure of $S$ (uses finiteness of the closure). Definability of varieties in field-theoretic sense and model-theoretic sense and how they agree (Page 68, Corollary 2.7 of Pillay in Bous). Show that being an abelian variety is a first order property and that the group operation on an abelian variety is definable.

The theory of algebraically closed fields of characteristic zero, $\mathbf{ACF}_0$, is given by the following set of axioms in the language of fields:

(1) The field axioms,
(2) For each $0 < n < \omega$, an axiom which states that
$$\underbrace{1 + \ldots + 1}_{n \text{ times}} \neq 0,$$
(3) For each $0 < n < \omega$ an axiom of the form
$$\forall c_0 \forall c_1 \ldots \forall c_n \exists a \sum_{i=0}^{n} x_i a^i = 0.$$

**Theorem 5.1.** *The theory $\mathbf{ACF}_0$ is $\aleph_0$-stable.*

*Proof.* This result is well known both to model theorists, and to algebraists (Steinitz's theorem). □

**Theorem 5.2.** *Algebraically closed fields are strongly minimal.*

*Proof.* .

Page 70 of Bous, remark 3.1 links Morley rank of irreducible varieties to algebraic notion (via genericity).

One of the more important facts about jet spaces is the following:

**Proposition 5.3.** *If $X$ is an affine subvariety of $K^n$ definable over a field $k \leq K$ then $J_a^m(X)$ is definable over $k$ for every $m$ and every $a$.*

*Proof.* Fix $m \geq 1$. Let $\mathcal{D}$ be the set of differential operators of the form

$$\frac{\partial^s}{\partial x_{i_1}^{s_1} \partial x_{i_2}^{s_2} \cdots \partial x_{i_r}^{s_r}}$$

where $0 < s \leq m$, $1 \leq i_1 < i_2 < \ldots < i_r \leq n$, $0 < s_i$ and $\sum_{i=1}^r s_i = s$. Let $d = |\mathcal{D}|$. Then $J_a^m(X)$ is isomorphic to the following subspace of $K^d$:

$$\{(u_D)_{D \in \mathcal{D}} \mid \forall P \in I_X \cap k[x_1, \ldots, x_n] \sum_{D \in \mathcal{D}} DP(a) u_D = 0\}.$$

The isomorphism for $m = 1$ is constructed on page 59 of [17], and the generalization to arbitrary $m \geq 1$ is left to the reader. It is clear that the above space is definable since $I_X \cap k[x_1, \ldots, x_n]$ is finitely generated, $\mathcal{D}$ is finite and the polynomial $DP$ can be easily defined from $P$ for each $D \in \mathcal{D}$. □

**Theorem 5.4.** *Let $G$ be an algebraic group.*

1. *If $H$ is a subgroup of $G$ then the Zariski closure of $H$ in $G$ is also a subgroup of $G$.*
2. *If $H$ is a definable subgroup of $G$ then $H$ is closed in $G$ (and thus an algebraic subgroup).*

*Proof.* Lemma 4.3 in Pillay's section (page 75).

**Definition 5.5.** A group is **connected** if it contains no proper definable subgroup of finite index.

Reexamining Definition 3.23 in light the second part of Theorem 5.4, we see that the two definitions of "connected" coincide for algebraic groups. Thus, there is no confusion about which definition we mean. In general, we will use the above definition since it is more tractable from a model-theoretic perspective and it is not limited to only algebraic groups.

Using some of the theory of $\omega$-stable groups, one is able to characterize the connected component of an algebraic group $G$, as predicted by Proposition 3.24. Namely, we have the following:

**Proposition 5.6.** *Let $G$ be an algebraic group. If we decompose the variety $G$ into irreducible components (as in Theorem 3.7), then the component containing the identity is an algebraic group. Furthermore, it is connected and has finite index in $G$, thus it is the connected component of $G$ predicted by Proposition 3.24.*

*Proof.* see [23] for a proof.

## 6. Model Theory of Differentially Closed Fields

Here we will develop ideas central to the characteristic zero proof of the Mordell-Lang conjecture. The topic which will garner the most focus in this section is the notion of the jet space at a point of a differentially closed field. This idea generalizes the better-known concepts of a tangent space to a differential curve or manifold and of a jet space for an algebraically closed field. Our presentation will, in part, follow that in [24]. The fundamentals of differential fields which we present here can be found in a number of sources, such as [17] and [35].

First, we will construct the basic setting for the theory of differentially closed fields. For this, we define some basic notions for differential algebra.

**Definition 6.1.** A **derivation** on a ring $\mathcal{R}$ is an additive function $\partial : \mathcal{R} \to \mathcal{R}$ satisfying the equation $\partial(fg) = \partial(f)g + f\partial(g)$ for all $f, g \in \mathcal{R}$.

A **differential ring** $(\mathcal{R}, +, \cdot, \partial, 0, 1)$ is a commutative ring with identity equipped with a derivation map. A **differential ideal** of a differential ring is an ideal $I$ of the ring closed under the derivation map, that is $\partial(f) \in I$ for all $f \in I$. A **differential field** $(\mathcal{U}, +, \cdot, \partial, 0, 1)$ is a field equipped with a derivation.

For our purposes, all our fields will have characteristic zero, though it is worthwhile to note that the theory of differential fields of positive characteristic has also been developed (see [34]). Unfortunately, in the positive characteristic case, the theory of differential fields of does not behave nearly as well. Fundamentally, this is due to the fact that the theory of differentially closed fields of characteristic $p$ is only stable, and not $\aleph_0$-stable like in characteristic zero (we talk more about the stability of differentially closed fields of characteristic zero later in this section).

*Remark* 6.2. *Since we will frequently be switching back and forth between model-theoretic notions interpreted over fields and interpreted over differential fields, we must have a convention for distinguishing between the two. Whenever we speak of a notion in terms of differential fields, we will precede the term with "∂-". We shall leave the unaltered terms to denote the field theoretic interpretation of the notion. For example, "∂-definable" will signify that an object is definable in the language of differential fields, whereas "definable" will denote that an object is definable in the language of fields. The difference is noteworthy since in the case of differential fields we have additional the unary function ∂ at our disposal for the definitions of objects.*

For each differential ring, we have a distinguished subring called the **ring of constants** $\mathcal{C}_\mathcal{U}$. Precisely, $\mathcal{C}_\mathcal{U} = \{c \in U \mid \partial(c) = 0\}$. When the ring $\mathcal{U}$ is understood, we shall omit the subscript. It is easy to verify that if $\mathcal{U}$ is a field, then the ring of constants is also a field which furthermore contains the prime field, $\mathbb{Q}$. It is also clear from the definition that the ring(field) of constants is definable. Furthermore, in the context of fields, we have the following relationship between constancy and algebraicity:

**Proposition 6.3.** *If $\mathcal{T} \supseteq \mathcal{U}$ are differential fields and $a \in \mathcal{T}$ is algebraic over $\mathcal{C}_\mathcal{U}$, then $a \in \mathcal{C}_\mathcal{T}$.*

*Proof.* Let $f = \sum_{i=0}^{n} c_i x^i$ be the minimal polynomial of $a$ over $\mathcal{C}_\mathcal{U}$. Then

$$0 = \partial(f(a)) = \sum_{i=1}^{n} i c_i \partial(a) a^{i-1} = \partial(a) g(a),$$

where $g(x) = \sum_{i=0}^{n-1}(i+1)c_{i+1}x^i$. Since $g$ is a polynomial over $\mathcal{C}_\mathcal{U}$ of order less than $f$, we have that $g(a) \neq 0$ and so $\partial(a) = 0$. □

A natural question to ask at this point is if any field can be the field of constants for some differential field. As the next lemma and theorem show, the answer for algebraically closed fields is yes. But first we need to define two key technical concepts.

**Definition 6.4.** Let $\mathcal{U}$ be a differential ring and let $\mathcal{U}[x]$ be the ring of polynomials over $\mathcal{U}$ in one variable (in the field-theoretic sense). Then, given $P \in \mathcal{U}[x]$, with $P = \sum_{i=0}^{n} c_i x^i$, we define $P^\partial$ to be the polynomial $\sum_{i=0}^{n} \partial(c_i)x^i$ and we define $P'$ to be the polynomial $\sum_{i=1}^{n} ic_i x^{i-1}$.

For a polynomial $Q \in \mathcal{U}[x_1, \ldots, x_n]$, we define $\partial Q/\partial x_i$ to be $Q'$, when $Q'$ is considered as a polynomial of the one variable $x_i$, i.e. $Q$ is considered as a polynomial in $\mathcal{U}[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n][x_i]$.

**Lemma 6.5.** *Let $(K, +, \cdot, \partial, 0, 1)$ be a differential field with an algebraically closed constant field $k$. If $a$ is algebraic over $K$, then there is a derivation $D$ on $K(a)$ extending $\partial$ such that $k$ is the field of constants of $(K(a), +, \cdot, D, 0, 1)$.*

*Proof.* Let $K, k, a, \partial$ as above be given and assume that $a \notin K$. Choose the minimal polynomial $P$ of $a$ over $K$. We define the derivative of $a$ to be

$$D(a) = -\frac{P^\partial(a)}{P'(a)}.$$

Since $P'$ has positive degree less than $P$, we know that $P'(a) \neq 0$, so $D(a)$ is defined. Furthermore, since $a$ is not algebraic over $k$, $P^\partial \neq 0$. Combine this with the fact that $P^\partial$ has degree less than $P$ (because the term of highest order is annihilated), and we see that $P^\partial(a) \neq 0$ and so $D(a) \neq 0$ and $a$ is not a constant in $K(a)$.

Since $\{1, a, \ldots, a^{n-1}\}$ forms a basis for $K(a)$ as a vector space over $K$, the following definition of $D$ is well-defined on all of $K(a)$: for all $d_0, \ldots, d_{n-1} \in K$,

$$D\left(\sum_{i=0}^{n-1} d_i a^i\right) = \sum_{i=0}^{n-1}(\partial(d_i)a^i + id_i a^{i-1}D(a))$$

That $D$ is a derivation follows directly from this definition. Furthermore, for each $c \in K$, $D(c) = \partial(c)$. Since $a$ is not a constant, no element of $K(a)\backslash K$ can be constant either. For if $b \in K(a)\backslash K$ were constant, then $k(b)$ would be contained in the field of constants of $K(a)$. Since $a$ is algebraic over $k(b)$, Proposition 6.3 (with $\mathcal{T} = \mathcal{U} = K(a)$) shows that $a$ is in the field of constants of $K(a)$. But this contradicts that $a$ is not constant in $K(a)$. Thus $k$ remains the field of constants in $K(a)$. □

We will denote the field $(K(a), +, \cdot, D, 0, 1)$ by $K < a >$; it is the **differential field generated by $a$ over $K$.**

**Theorem 6.6.** *Let $k \leq K$ be fields of characteristic zero with $k$ algebraically closed. There is a derivation $\partial$ on $K$ such that $k$ is the field of constants.*

*Proof.* Let $G \subset K$ be a transcendence basis for $K$ over $k$. By Corollary VI.1.6 of [12], $K$ is algebraic over $k(G)$, the field of fractions for the ring of polynomials of $k$ over $G$. Thus, if we are given a derivation $\partial$ on $k(G)$ which has $k$ as the field of

constants, we may extend it to a desired derivation on $K$ by repeated use of the previous lemma. Explicitly, set $k(G) = F_0$ and $\partial = \partial_0$. We will define differential fields $(F_\alpha, +, \cdot, \partial_\alpha, 0, 1)$ recursively such that $k(G) \leq F_\alpha \leq K$, $\partial_\alpha$ extends $\partial$, and $k$ is the field of constants of $\partial_\alpha$. If $F_\alpha \neq K$, choose $a \in K \backslash F_\alpha$, take $F_{\alpha+1} = F_\alpha < a >$ and set $\partial_{\alpha+1}$ to be the derivation on $F_{\alpha+1}$. When $\beta$ is a limit ordinal, define $F_\beta = \bigcup_{\alpha<\beta} F_\alpha$ and $\partial_\beta = \bigcup_{\alpha<\beta} \partial_\alpha$. The recursion will terminate in at most $|k(G)| \cdot \aleph_0$ steps since this is the maximum number of algebraic elements over $k(G)$. At the end of the recursion we will have the desired derivation on $K$.

Thus we are reduced to the task of obtaining a derivation on $k(G)$ such that $k$ is the field of constants. Enumerate $G$ as $\{g_\beta \mid \beta < \alpha\}$ and label $G_\beta = \{g_\gamma \mid \gamma < \beta\}$. We recursively construct a chain of derivations $\partial_\beta$ such that

(1) $\partial_\beta$ is a derivation on $k(G_\beta)$ with $k$ as the constant field,
(2) $\partial_\beta \subset \partial_{\beta+1}$,
(3) for $\beta$ limit, $\partial_\beta = \bigcup_{\gamma<\beta} \partial_\gamma$.

For $\beta = 0$, $\partial_\beta$ is simply the zero map on $k$. For $\beta$ limit, simply take the union of the derivations $\partial_\gamma$ for $\gamma < \beta$. Finally, if $\beta = \gamma + 1$ then $k(G_\beta) \cong k(G_\gamma)(g_\beta)$, so we can obtain a derivation $\partial_\beta$ by simply modifying the standard derivative on $F(x)$, the field of rational functions over a field $F$. Namely, if we are given $c_0, \ldots, c_m \in k(G_\gamma)$ and a polynomial $f = \sum_{i=0}^m c_i g_\beta^i$, define

$$\partial_\beta(f) = \sum_{i=0}^m \partial_\gamma(c_i) g_\beta^i + \sum_{i=0}^m i c_i g_\beta^{i-1}.$$

Due to the unique representation of polynomials, this equation defines a derivation $\partial_\beta$ on the ring $k(G_\gamma)[g_\beta]$. Moreover, it is clear by the linear independence of the $g_\beta^i$ in $k(G_\gamma)[g_\beta]$ that $\partial(f) = 0$ if and only if $f \in k$. Consequently $k$ is the ring of constants of this derivation.

We may further extend $\partial_\beta$ to the field $k(G_\gamma)(g_\beta)$ by defining

$$\partial_\beta \left( \frac{f}{h} \right) = \frac{h\partial_\beta(f) - f\partial_\beta(h)}{h^2}$$

whenever $f$ and $h$ are coprime. It is easy to check that this is a well-defined derivation that extends the original derivation on $k(G_\gamma)[g_\beta]$. To see that $k$ is still the field of constants, consider $f \neq 0$ and $h \neq 0$ coprime such that $\partial_\beta(f/h) = 0$. Without loss of generality, we may assume $f$ is monic. Since $\partial(f/h) = 0$, we have $h\partial(f) = f\partial(h)$ and therefore, since $f$ and $h$ are coprime, we find that $f|\partial(f)$. But since $f$ is monic, $\partial(f)$ has degree less than $f$, thus $\partial(f) = 0$ and so $f \in k$. But $\partial(f) = 0$ also implies that $\partial(h) = 0$ and consequently $h \in k$ as well. So $f/h \in k$ and $k$ is the field of constants of the derivation $\partial_\beta$ on $k(G_\beta)$. □

It is worthwhile to note that the derivation depended on the choice of $G$, as well as the elements of $K$ chosen for the application of the lemma and the order in which these elements were chosen. These considerations indicate that there are potentially many derivations on $K$ which have $k$ as the field of constants. However, extensions of derivations are not quite so arbitrary. To help convince the reader of this fact, we sketch a proof of a simple proposition that presents an explicit expression for the derivation of an element in terms of polynomials. As a straightforward corollary, we conclude that there is a unique way to extend a derivation on a field to an algebraic extension of the field.

**Proposition 6.7.** *Let $K$ be a differential field and let $a \in K$ be given. If $P$ is a polynomial over $K$ such that $P(a) = 0$, then*

$$\partial(a) = -\frac{P^{\partial}(a)}{P'(a)}.$$

*Proof.* If $P = x^n + \sum_{i=0}^{n-1} c_i x^i$, then $0 = P(a) = \partial(P(a))$. Rearranging the terms of this last equation yields the desired expression. □

**Corollary 6.8.** *Let $K$ be differential field and let $a$ be algebraic over $K$. Then there is a unique way to extend the derivation on $K$ to a derivation on $K(a)$.*

*Proof.* Let $\partial$ be extended to $K(a)$ and let $b \in K(a)$ be given. If $P$ is the minimal polynomial of $b$ over $K$, then by the previous proposition

$$\partial(b) = -\frac{P^{\partial}(b)}{P'(b)}.$$

Since the term on the right is fixed regardless of how we extend $\partial$, it must be that there is only one way to extend $\partial$ to $K(a)$. □

*Remark* 6.9. *The above proposition can be generalized to $a \in K^n$ and polynomials $P \in K[x_1, \ldots, x_n]$ such that $P(a) = 0$. In this case, we obtain that*

$$P^{\delta}(a) = -\sum_{i=1}^{n} \frac{\partial P}{\partial x_i}(a)\partial(a_i).$$

In the case of fields, we have the powerful notion of being algebraically closed, and we shall have the analogous notion of differentially closed in the case of differential fields. First we construct the ring $\mathcal{U}\{x\} = \mathcal{U}[x, \partial x, \partial^2 x, \ldots]$ of differential polynomials over $\mathcal{U}$ and endow it with a natural derivation extending the one on $\mathcal{U}$. We define $\mathbf{ord}(f)$, the **order** of $f$, to be the greatest $n \geq 0$ for which $\partial^n x$ appears in $f$ with a nonzero coefficient.

**Definition 6.10.** A **differentially closed field** is a differential field $\mathcal{U}$ such that given $f, g \in \mathcal{U}\{x\}$ with $\mathrm{ord}(f) > \mathrm{ord}(g)$, there is an $a \in \mathcal{U}$ with $f(a) = 0$ and $g(a) \neq 0$.

We first note that the notion of being differentially closed is expressible in the language of differentially closed fields (via an infinite family of sentences). Furthermore, $\mathcal{U}\{x\}$ is automatically algebraically closed. Indeed, given $f(x) \in \mathcal{U}[x]$, we may consider the polynomial $f(\partial(x)) \in \mathcal{U}$. Since $f(\partial(x))$ has order 1, by differential closedness there is an $a \in \mathcal{U}$ such that $f(\partial(a)) = 0$, and thus $\partial(a)$ is a root for our original polynomial $f \in \mathcal{U}[x]$. An easy consequence of the algebraic closedness of $\mathcal{U}$ and Proposition 6.3 is that the field of constants of a differentially closed field is also algebraically closed.

The richness of differentially closed fields ranks on par with that of algebraically closed fields. There is a Basis Theorem (though not as general as Hilbert's Basis Theorem) and a Nullstellensatz. Additionally, for every differential field there is a least differentially closed field containing it, called the differential closure. Lastly, we mention that the theory of differentially closed fields (**DCF**) is $\omega$-stable. With these results in hand, we have the groundwork for developing a differential algebraic

geometry. Indeed, many useful ideas from algebraic geometry and commutative algebra transfer without much difficulty to the differential setting. As Pillay and Ziegler [24] observed, even the concept of jet space possessed a useful analogue in the differential setting, with the construction mimicking the one in the case of algebraically closed fields.

**Theorem 6.11.** *Every differential field $\mathcal{U}$ has an extension $\mathcal{T}$ which is differentially closed.*

*Proof.* see Lemma 2.2 of [17].

With this theorem in hand, we would like to define the differential closure of a field $\mathcal{U}$ to be the least differentially closed field containing $\mathcal{U}$. However, we cannot at this point be certain that there is precisely one minimal differentially closed field containing $\mathcal{U}$. That result will follow from model theoretic considerations once we have the following theorem:

**Theorem 6.12. DCF** *is $\aleph_0$-stable.*

*Proof.* See Lemma 2.8 of [17].

**Corollary 6.13.** *For every differential field $\mathcal{U}$, there is least differentially closed field $\mathcal{T}$ containing $\mathcal{U}$. We call $\mathcal{T}$ the* **differential closure** *of $\mathcal{U}$.*

*Proof.* Due to the previous theorem and a standard result of Morley on $\aleph_0$-stable theories, there is an atomic prime model $\mathcal{T}$ of **DCF** over $\mathcal{U}$. A prime model $M$ over $A$ in a theory $T$ is by definition a model $M$ of $T$ containing $A$ as a substructure, such that for any model $N$ of $T$, if $A \subseteq N$ then there is an elementary embedding $\sigma : M \to N$ fixing $A$. Thus, $\mathcal{T}$ is differentially closed, being a model of **DCF**. Furthermore, $\mathcal{T}$ is minimal among differentially closed fields containing $A$, and is elementarily equivalent to every other minimal differentially closed field containing $A$ (such a field must be a prime model as well). By a standard result of Shelah on $\aleph_0$-stable theories, any two prime models over the same set are isomorphic. Thus $\mathcal{T}$ is the sole minimal differentially closed field containing $A$ (up to isomorphism). Morley's result also stated that $\mathcal{T}$ is atomic over $\mathcal{U}$, that is every $a \in \mathcal{T}^n$ realizes an isolated $\partial$-type in $\partial$-$S^n(\mathcal{U})$. For $n = 1$ this implies each $a \in \mathcal{T}$ must simultaneously satisfy all the polynomials in a differential ideal $I$ of $\mathcal{U}\{x\}$ and $a$ is the only possible simultaneous solution for all the polynomials in $I$. As we shall see later, this states that $a$ is differentially algebraic over $\mathcal{U}$. Thus, atomicity implies that the differential closure $\mathcal{T}$ acts precisely as we would expect: it contains a nontrivial root to every polynomial in $\mathcal{U}\{x\}$. As we will see later, a concise way to state this is $\mathcal{T} = \partial\text{-}acl(\mathcal{U})$. □

The next theorem is an important result from a model-theoretic perspective, however we will omit the proof due to its technical nature. The interested reader should consult Theorem 2.4 and Corollary 2.5 of [17].

**Theorem 6.14.** The theory **DCF** of differentially closed fields admits elimination of quantifiers and is complete and model complete.

Elimination of quantifiers has significant repercussions on our model-theoretic knowledge of the field of constants $\mathcal{C}$. Namely, we have the following important result:

**Theorem 6.15.** *Let $\mathcal{U}$ be a differentially closed field. Then the field of constants $\mathcal{C}$ has no additional structure other than being an algebraically closed field. That is, a subset of $\mathcal{C}^n$ is $\partial$-definable over $\mathcal{U}$ if and only if it is definable over $\mathcal{C}$. Consequently, $\mathcal{C}$ is strongly $\partial$-minimal.*

*Proof.* We reproduce the proof of Corollary 1.10 of [35]. Let $D \subseteq \mathcal{C}^n$ be a $\partial$-definable over $\mathcal{U}$. Since **DCF** has quantifier elimination, it must be that $D$ is defined by a finite boolean combination of formulas $f_i = 0$, where $f \in \mathcal{U}\{x_1, \ldots, x_n\}$. But since $D \subseteq \mathcal{C}^n$, $f_i(x_1, \ldots, x_n, \partial x_1, \ldots, \partial x_n, \ldots) = f_i(x_1, \ldots, x_n, 0, \ldots, 0, \ldots)$ on $D$. Taking $\bar{f}_i = f_i(x_1, \ldots, x_n, 0, \ldots, 0, \ldots)$ we have that $\bar{f}_i \in \mathcal{U}[x_1, \ldots, x_n]$. Take $D'$ to be the *definable* subset of $\mathcal{U}^n$ given by replacing the $f_i$ in the definition of $D$ with $\bar{f}_i$. Then $D = D' \cap \mathcal{C}^n$. However, since $\mathcal{U}$ and $\mathcal{C}$ are models of the $\aleph_0$-stable theory **ACF**, we have that types are definable (Theorem 4.1). Therefore, since $D'$ is definable in $K$ we must have $D' \cap \mathcal{C}^n = D$ definable in $\mathcal{C}$.

This first part of the proof has shown that for the field of constants being strongly $\partial$-minimal is equivalent to being strongly minimal. But since $\mathcal{C}$ is algebraically closed, by Theorem 5.2 we have that $\mathcal{C}$ is strongly minimal. □

*Remark* 6.16. *This theorem will be of vital importance to us in the proof of the Mordell-Lang conjecture. During the proof we will encounter algebraically closed fields $k < K$. Since there are in general more $\partial$-definable sets than definable sets, it will be advantageous for us to transfer the setting to differential fields by defining an appropriate derivation $\partial$ on $K$. This way, interesting sets which previously may not have been definable will turn out to be $\partial$-definable. However, to proceed with this transformation, we must have some way to return to the setting of just algebraically closed fields and definability. Our tool for achieving this step will be the above theorem: we will reveal that our "useful" sets are $\partial$-definable over the field of constants, whereby they will be definable over the field of constants.*

We now quickly mention the interpretations of some model-theoretic concepts in the setting of differential fields. In algebraically closed fields we have that $MR(tp(a/K))$ is the transcendence degree of $K(a)$ over $K$. Similarly, it is easy to deduce that the differential Morley rank $\partial MR(\partial\text{-tp}(a/\mathcal{U}))$ is the transcendence degree of the field of fractions of $\mathcal{U}\{a\}$ over $\mathcal{U}$. We always have $MR(tp(a/\mathcal{U})) \leq \partial MR(tp(a/\mathcal{U}))$ because a set is definable only if it is $\partial$-definable.

For any subset $A \subseteq \mathcal{U}$ we define $I^\partial(A) = \{P \in \mathcal{U}\{x\} \mid P(a, \partial a, \partial^2 a, \ldots) = 0\}$. We will always have that $I^\partial(A)$ is a differential ideal. Given a subset $S \subseteq K$, $\partial\text{-}acl(S)$ is the set of all elements of $K$ which are differentially algebraic over (the differential field generated by) $S$. Assume $S$ is a differential subfield of $K$. Then $a$ is **differentially algebraic** over $S$ if and only if $I^\partial(\{a\}) \cap S\{x\}$ is nontrivial. Elements $a_1, \ldots, a_m \in K$ are **differentially algebraically independent** over $S$ if $I^\partial(\{a_1, \ldots, a_n\}) \cap S\{x_1, \ldots, x_n\} = \{0\}$. Otherwise, they are **differentially algebraically dependent**.

Just as in the case of algebraically closed fields, we have the concepts of a variety, a "Zariski" topology, and a jet space. Furthermore, the derivation will allow us to obtain an alternate formulation of tangent spaces (one would naturally expect that tangency has a connection to the derivative). By modification of the concept of a tangent space, we will obtain the fruitful concepts of a prolongation space and differential jet space; the rest of the section will be devoted to developing these concepts.

**Definition 6.17.** An **(affine) differential algebraic variety** $V \subseteq \mathcal{U}^n$ is the set of simultaneous zeros for the differential polynomials in a subset $I$ of $\mathcal{U}\{x_1, \ldots, x_n\}$.

Each such set $I$ of differential polynomials has a corresponding affine differential algebraic variety $V^\partial(I)$ which contains all the simultaneous zeros. As with algebraic varieties, we will have that $I^\partial(V)$ satisfies $V = V^\partial(I^\partial(V))$ for every differential algebraic variety $V$.

*Remark* 6.18. *If $V \subseteq \mathcal{U}^n$ is an affine algebraic variety, then we will continue to use $I(V)$ to denote the appropriate ideal of $\mathcal{U}[x_1, \ldots, x_n]$, and use $I^\partial(V)$ to denote the differential ideal in $\mathcal{U}\{x_1, \ldots, x_n\}$. Note that generators for the algebraic ideal $I(V)$ will generate the differential ideal $I^\partial(V)$.*

As in the algebraic fields case, if we define differential algebraic varieties to be basic closed sets we yield a topology on $\mathcal{U}^n$ known as the **$\partial$-topology** or the **Kolchin topology**. The Kolchin topology represents a Zariski-like topology on $\mathcal{U}^n$ and many of the properties of the Zariski topology transfer over. Most importantly we have the two following facts:

**Theorem 6.19** (Differential Basis Theorem)**.** *The Kolchin topology is Noetherian. That is, there are no infinite descending chains of Kolchin closed sets in $K^n$.*

**Theorem 6.20** (Kolchin's Irreducibility Theorem)**.** *If $V \subseteq \mathcal{U}^n$ is an irreducible affine algebraic variety then it is irreducible in the Kolchin topology.*

Proofs of these theorems can be found in [14] and [17]. Since the Zariski geometry is coarser than the Kolchin topology, one would probably expect that some Zariski irreducible sets are not Kolchin irreducible. However, the last theorem indicates that the extra closed sets in the Kolchin topology are added in a way that does not tamper with irreducibility considerations. This theorem evidences the deeper interactions between Zariski and Kolchin topologies which will be of use to us.

Before defining the concepts of differential tangent space and prolongation space, we will need the following technical lemma, which will be central for our analysis of the ($\partial$-)definability of those spaces.

**Lemma 6.21.** *Let $V \subseteq \mathcal{U}^n$ be a differential variety and let $I' \subseteq I(V)$ generate the ideal $I(V)$. Suppose $F : \mathcal{U}[x_1, \ldots, x_n] \to \mathcal{U}[x_1, \ldots, x_n]$ is an additive map which also satisfies*

$$F(QP)(a) = Q(a) \cdot F(P)(a)$$

*for all $P \in I$, $Q \in \mathcal{U}[x_1, \ldots, x_n]$ and $a \in V$.*

*Then for each $u \in \mathcal{U}^n$, $u$ satisfies*

$$\sum_{i=1}^{n} \frac{\partial P}{\partial x_i}(a) u_i + F(P)(a) = 0. \tag{6.1}$$

*for all $P \in I(V)$ and all $a \in V$ if and only if $u$ satisfies the above equation for all $P \in I'$ and all $a \in V$.*

*Proof.* Since $F$ and $\partial/\partial x_i$ for each $i$ are additive maps, we are reduced to showing that if $u$ satisfies 6.1 for a polynomial $P \in I(V)$, then it will satisfy the corresponding equation for $QP$ for any $Q \in \mathcal{U}[x_1, \ldots, x_n]$. Once we have shown this, both directions of the implication are proven since $I' \subseteq I(V)$ and $I'$ generates $I(V)$. But equation 6.1 for $QP$ is proven easily via the following simplification: for each $a \in V$

$$\begin{aligned}\sum_{i=1}^{n} \frac{\partial(QP)}{\partial x_i}(a)u_i + F(QP)(a) &= \sum_{i=1}^{n}(Q(a)\frac{\partial P}{\partial x_i}(a)u_i + P(a)\frac{\partial Q}{\partial x_i}(a)u_i) + F(QP)(a) \\ &= Q(a)\left(\sum_{i=1}^{n}\frac{\partial P}{\partial x_i}(a)u_i\right) + F(QP)(a) \\ &= Q(a)\left(\sum_{i=1}^{n}\frac{\partial P}{\partial x_i}(a)u_i + F(P)(a)\right)\end{aligned}$$

□

Let $V$ be an irreducible affine algebraic variety and fix $a \in V$. We propose the following alternate definition of $\mathcal{T}_a(V)$, the **tangent space** of $V$ at $a$:

$$\mathcal{T}_a(V) = \{u \in \mathcal{U}^n \mid \sum_{i=1}^{n}\frac{\partial P}{\partial x_i}(a)u_i = 0 \ \forall P \in I(V)\}.$$

It is shown on page 59 of [17] that the space defined above is the tangent space $\mathcal{T}_a(V)$. This can be done by showing that the above definition is isomorphic to the first jet space (exhibited in the proof of Proposition 5.3) which in turn is isomorphic to the tangent space (appeared in the Foundational Algebraic Geometry section near the beginning of the discussion on jet spaces). Thus, we have this new description of the tangent space to a variety using the language of differential fields. Since $I(V)$ is finitely generated, we may use Lemma 6.21 (with $F$ just being the zero map) to conclude that $\mathcal{T}_a(V)$ can be equivalently defined using just a finite set of polynomials which generate $I(V)$. Clearly then, the tangent space $\mathcal{T}_a(V)$ is a $\partial$-definable affine differential algebraic variety. Actually, one can bypass the usage of the symbol $\partial$ and define the polynomials $\frac{\partial P}{\partial x_i}$ in terms of the polynomials $P$ and thus obtain that the tangent space is a definable affine algebraic variety. Furthermore, we now have a simple way to consider all the tangents spaces simultaneously in the form of a tangent bundle.

**Definition 6.22.** Given an irreducible affine algebraic variety $V$ we define the **tangent bundle** to be:

$$\mathcal{T}(V) = \{(a, u) \in \mathcal{U}^{2n} \mid a \in V, \ \sum_{i=1}^{n}\frac{\partial P}{\partial x_i}(a)u_i = 0 \ \forall P \in I(V)\}.$$

We can easily see that the tangent bundle also is a definable affine algebraic variety. A slight variation on the definitions of tangent spaces yields the notion of the valuable concept of a prolongation of a variety.

**Definition 6.23.** The **prolongation** of a variety $V$ is

$$\tau(V) = \{(a,u) \in \mathcal{U}^{2n} \mid a \in V,\ \sum_{i=1}^{n} \frac{\partial P}{\partial x_i}(a)u_i + P^{\partial}(a) = 0\ \forall P \in I(V)\}.$$

The **prolongation** of a variety $V$ at a point $a \in V$ is the set:

$$\tau_a(V) = \{u \in \mathcal{U}^n \mid (a,u) \in \tau(V)\}.$$

Since $(QP)^{\partial} = Q^{\partial}P + QP^{\partial}$, we have that $F : P \to P^{\partial}$ meets the requirements for Lemma 6.21. Thus, it is equivalent to define $\tau(V)$ simply using polynomials from a finite generating set for $I(V)$. As with $\mathcal{T}(V)$, this has shown that $\tau(V)$ is a $\partial$-definable differential variety. Again, we may formally define $\frac{\partial P}{\partial x_i}$ and $P^{\partial}$ in terms of $P$ without the use of the symbol $\partial$ and thus see that $\tau(V)$ is simply a definable algebraic variety. Similarly, $\tau_a(V)$ is a definable algebraic variety for every $a \in V$. The prolongation and the tangent bundle are intimately related: if $V$ is defined over $\mathcal{C}$ then $P^{\delta} = 0$ for every $P \in I(V)$ and thus $\tau(V) = \mathcal{T}(V)$. Even if $V$ is not definable over the field of constants, we still have a strong relationship between the two spaces. Namely, the map $(a,u) \mapsto (a, u + \partial(a))$ is a $\partial$-definable isomorphism between $\mathcal{T}(V)$ and $\tau(V)$. The key step in proving that this map is an isomorphism is given to us by Remark 6.9. When the map is restricted to those elements of $\mathcal{T}(V)$ whose first coordinate is $a$, we obtain a $\partial$-definable isomorphism between $\mathcal{T}_a(V)$ and $\tau_a(V)$.

There are natural maps $\pi : \tau(V) \to V$ and $t : \mathcal{T}(V) \to V$ given by projection onto the first $n$ coordinates. These maps have natural sections $\nabla : V \to \tau(V)$ and $z : V \to \mathcal{T}(V)$, respectively, so that $\pi \circ \nabla = id_V = t \circ z$. The map $\nabla$ is given by $\nabla(a) = (a, \partial(a))$ (we have that $\nabla$ maps into $\tau(V)$ by another application of Remark 6.9). The zero map $z(a) = (a, 0)$ gives a section for the tangent space projection.

We will not go into full detail here, but we can consider both $\mathcal{T}$ and $\tau$ as functors from the category of irreducible affine varieties with morphisms to itself. For a more detailed proof of this fact, consult [18]. We will just mention that if $V \subseteq \mathcal{U}^n$ and $W \subseteq \mathcal{U}^m$ are affine varieties and $\phi = (\phi_1, \ldots, \phi_m)$ is a morphism from $V$ to $W$, then we may define $\mathcal{T}(\phi) : \mathcal{T}(V) \to \mathcal{T}(W)$ and $\tau(\phi) : \tau(V) \to \tau(W)$ as follows:

$$\begin{aligned} \mathcal{T}(\phi)(a,u) &= (\phi(a), d\phi_a(u)) \\ \tau(\phi)(a,u) &= (\phi(a), d\phi_a(u) + \phi^{\partial}(a)), \end{aligned}$$

where

$$d\phi_a(u) = \left( \sum_{i=1}^{n} \frac{\partial \phi_1(a)}{\partial x_i} u_i, \ldots, \sum_{i=1}^{n} \frac{\partial \phi_m(a)}{\partial x_i} u_i \right)$$

and $\phi^{\partial}(a) = (\phi_1^{\partial}(a), \ldots, \phi_m^{\partial}(a))$.

We now will restrict our considerations of tangent spaces and prolongation spaces to those of algebraic groups. If $G$ is an algebraic group with morphisms $m$ and $\iota$ giving multiplication and inverse, respectively, then $\mathcal{T}(G)$ is an algebraic group with multiplication given by $\mathcal{T}(m)$ and inversion given by $\mathcal{T}(\iota)$. Similarly $\tau(G)$ is an algebraic group with multiplication given by $\tau(m)$ and inversion given by $\tau(\iota)$. To see this, simply apply the functors $\mathcal{T}$ and $\tau$ to the appropriate commutative diagrams.

Consider the case when $\pi$ has an additional $\partial$-definable section $j$; then it is of interest to determine the set where $j$ and $\nabla$ agree. Define a homomorphism $\phi : \tau(X) \to \ker\pi$ by $\phi(x) = x - j(\pi(x))$, and define $\psi_j : X \to \ker\pi$ to be $\phi \circ \nabla$. As $\nabla$ is a section for $\pi$ we see that $\psi_j(x) = \nabla(x) - j(x)$ and so ker $\psi_j$ is precisely the set of $a \in X$ for which $j(a) = \nabla(a)$.

**Lemma 6.24.** *Ker $\psi_j$ is Zariski dense in $X$.*

*Proof.* This proof requires alternate formulation of **DCF** provided by Pierce and Pillay [21]. Namely, a field $\mathcal{U}$ is differentially closed if and only if for every algebraic variety $V$ defined over $\mathcal{U}$ and every $\partial$-definable $W \subseteq \tau(V)$, if $W$ projects generically onto $V$ then there is $a \in V$ such that $\nabla(a) \in W$.

Now we proceed with proving density. Let $Y \subseteq X$ be Zariski open in $X$ and consider the $\partial$-definable set $j(Y) \subseteq \tau(X)$. Then $\pi$ projects $j(Y)$ generically onto $Y$ since $j$ is a section of $\pi$. By the above characterization, there is an $a \in Y$ such that $\nabla(a) \in j(Y)$. So $\nabla(a) = j(b)$ for some $b \in Y$. But since $\nabla$ is also a section of $\pi$, we see that $a = b$, and thus $a \in ker\psi_j$. □

In general, we will not have an additional $\partial$-definable section $j$ of $\pi$, however, using abelian varieties, we will be able to determine a class of varieties for which such sections must exist. Recall that if $A$ is an abelian variety, then $\tau(A)$ is an algebraic group. The section $\nabla : \tau(A) \to A$ is definable if $A$ is defined over $\mathcal{C}$, the field of constants. Otherwise, it is generally just $\partial$-definable. Our goal is to find an extension $A'$ of $A$ such that $\pi : A' \to \tau(A')$ has a *definable* section $j$. We acquire such a group extension $A'$ by considering objects known as vector group extensions.

**Definition 6.25.** A **vector group** is a group $G$ which is the additive group of a vector space. Given an algebraic group $G$, $H$ is an **extension of $G$ by a vector group** if there is a surjective homomorphism $p : H \to G$ such that $ker(p)$ is isomorphic to a vector group.

Examples of extensions of $G$ by vector groups are $\mathcal{T}(G)$ with the homomorphism $t$ and $\tau(G)$ with the homomorphism $\pi$.

For our discussion, we will need the following result on vector group extensions of abelian varieties due to Rosenlicht [26].

**Theorem 6.26.** There exists an extension $\hat{A}$ of $A$ by a vector group with surjective homomorphism $p : \hat{A} \to A$ satisfying the following universal mapping property: If $q : B \to A$ is an extension of $A$ by a vector group, then there is a unique homomorphism $j : \hat{A} \to B$ such that $p = q \circ j$.

**Definition 6.27.** The algebraic group $\hat{A}$ described in the previous theorem is known as the **universal extension of $A$ by a vector group**.

From the universal mapping property, it is clear that $\hat{A}$ is unique up to isomorphism. Furthermore, it is proven in [26] that if $A$ has dimension $d$ then $\hat{A}$ has dimension $2d$.

Consider the prolongation $\hat{\pi} : \tau(\hat{A}) \to \hat{A}$. We have a section for $\hat{\pi}$, namely the corresponding $\hat{\nabla} : \hat{A} \to \tau(\hat{A})$, but as was mentioned earlier $\hat{\nabla}$ is $\partial$-definable. It is not immediately obvious that $\hat{\pi}$ has a definable section, however, the universal mapping property of $\hat{A}$ and $p$ will yield our desired definable section $j : \hat{A} \to \tau(\hat{A})$.

For any algebraic group $G$, it is clear that $\pi : \tau(G) \to G$ and $t : \mathcal{T}(G) \to G$ are extensions of $G$ by vector groups. Consequently $p \circ \hat{\pi} : \tau(\hat{A}) \to A$ is an extension of $A$ by a vector group. By the universal mapping property of $\hat{A}$, there is a unique homomorphism $j : \hat{A} \to \tau(\hat{A})$ such that $p = (p \circ \hat{\pi}) \circ j$. But since $p \circ \mathrm{id} = p$ as well, we have that $\mathrm{id} = \hat{\pi} \circ j$ by the universal mapping property of $p$. Thus $j$ is a section of $\hat{\pi}$ and this construction has shown that $j$ is definable.

These mappings and algebraic groups will be the basis of our construction of the Manin Kernel in Step 3 of the proof of the Mordell-Lang conjecture. We now switch directions to develop the theory of differential jet spaces.

Given an irreducible affine algebraic variety $X$ in our differentially closed field $\mathcal{U}$ we would like a concept of jet space which reflects the differential nature of the field. We already constructed $J_a^M(X)$, the algebraic jet space of $X$ at a point $a \in X$, however this vector space is unsatisfactory since it lacks compatibility with the derivation $\partial$. Instead, we will restrict ourselves to a Zariski dense subspace which we will be able to describe after the next series of definitions.

*Remark* 6.28. *To simplify the proofs of certain facts (and to utilize results from our discussion on prolongation spaces), we will assume that $X$ is an algebraic group, however we note that the construction of differential jet spaces works for arbitrary $X$.*

Let $s_1, \ldots, s_n$ be polynomials in $\mathcal{U}[x]$ and let $s = (s_1, \ldots, s_n)$. We may consider $s$ as a mapping from $X$ to $\mathcal{U}^n$ and examine the set $X_s^\sharp = \{x \in X \mid s(x) = \partial(x)\}$.

**Proposition 6.29.** *$X_s^\sharp$ is an algebraic variety over $\mathcal{U}$.*

*Proof.* For each $a \in X_s^\sharp$, each $m \geq 2$, and each $1 \leq j \leq n$, $\partial^m(a_j) = \partial^{m-1}(s_j(a_j))$. This is the $m-1$st derivation of a polynomial evaluated at $a_j$; consequently it is of the form $y + \sum_{i=1}^{r} c_i a_j^{i-1} \partial(a_j)$ for some $r \geq 0$ and $y, c_i \in \mathcal{U}$. Since $\partial(a_j) = s_j(a_j)$, we have that $\partial^m(a_j)$ is simply a polynomial in $U[x]$ evaluated at $a_j$. Thus, in each coordinate, $\partial^m(a)$ is just an evaluation of a polynomial at $a$. Consequently, given any differential polynomial $P$ in $\mathcal{U}\{x_1, \ldots, x_n\}$, we are able to obtain a polynomial $P^\sharp \in U[x_1, \ldots, x_n]$ such that $P^\sharp(a) = P(a)$ for all $a \in X_s^\sharp$. $P^\sharp$ is simply constructed by resolving occurrences of $\partial$ with $s$ in the manner described above. As a result, we have a definite way for constructing $P^\sharp$ from $P$ such that $P \mapsto P^\sharp$ defines a ring homomorphism from $U\{x_1, \ldots, x_n\}$ to $U[x_1, \ldots, x_n]$. Consequently $I = \{P^\sharp \mid P \in I^\partial(X)\}$ is an ideal in $\mathcal{U}[x_1, \ldots, x_n]$ and $X_s^\sharp = V(I)$. □

**Proposition 6.30.** *If $(a, s(a)) \in \tau(X)$ for every $a \in X$, then $X_s^\sharp$ is Zariski dense in $X$.*

*Proof.* The map $j : X \to \tau(X)$ given by $j(a) = (a, s(a))$ is a section of $\pi$. Thus $ker\psi_j$ is dense in $X$ by Lemma 6.24, and it is clear that $ker\psi_j$ is simply $X_s^\sharp$. □

*Remark* 6.31. *From this point forth, we will assume that $s$ and $X$ satisfy the hypothesis of the previous proposition.*

In order to properly develop the concept of differential jet spaces, we need the notion of a $\partial$-module, which can be thought of as a differential analogue to a vector space.

**Definition 6.32.** A **$\partial$-module** over $\mathcal{U}$ is a finite-dimensional vector space $V$ over $\mathcal{U}$ equipped with an additive endomorphism $D_V$ such that for all $c \in \mathcal{U}$ and $v \in V$,

$$D_V(cv) = \partial(c)v + cD_V(v).$$

Given two $\partial$-modules $(V, D_V)$, $(W, D_W)$ over $\mathcal{U}$, a **$\partial$-module homomorphism** is a linear transformation $f : V \to W$ such that $f(D_V(v)) = D_W(f(v))$ for every $v \in V$. Together, these definitions yield the category $\mathcal{U}[\partial]$ of $\partial$-modules over $\mathcal{U}$.

A useful example of a $\partial$-module is illustrated in the next proposition.

**Proposition 6.33.** *For any point $a \in X$ and all $m \geq 1$, $\mathcal{M}_a(X)/\mathcal{M}_a^{m+1}(X)$ is a $\partial$-module.*

*Proof.* We have a derivation $D$ on $\mathcal{U}[x_1, \ldots, x_n]$ given by:

$$Df = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i} s_i + f^{\partial}.$$

Since $(a, s(a)) \in \tau(X)$ for every $a \in X$, we have $Df(a) = 0$ for every $f \in I(X)$ and every $a \in X$, i.e. $Df \in I(X)$. Thus $D$ naturally becomes a derivation on $\mathcal{U}[X] = \mathcal{U}[x_1, \ldots, x_n]/I(X)$. Indeed, if $f - g \in I(X)$, then $Df - Dg = D(f - g) \in I(X)$. Under the derivation $D$, $\mathcal{M}_a^m(X)$ is a differential ideal of $\mathcal{U}[X]$ for every $a \in X$ and every $m \geq 1$. Consequently, the derivation $D$ can be extended to $\mathcal{M}_a(X)/\mathcal{M}_a^m(X)$ for every $m \geq 2$ yielding a $\partial$-module structure on this finite-dimensional vector space. □

A vector space over a field $F$ is a module which respects the field structure of $F$ as the set of scalars. Analogously, a $\partial$-module over a differential field $F$ is a module which respects the differential field structure of $F$ as the set of scalars. Recalling the construction of algebraic jet spaces over $F$, the $m$th jet space of $X$ at the point $a$ was defined to be $\mathrm{Hom}(\mathcal{M}_a(X)/\mathcal{M}_a^{m+1}(X),\ F)$ in the category of $F$-vector spaces. Extrapolating to the differential case yields the following definition:

**Definition 6.34.** Given an irreducible differential variety $X$ over the differential field $\mathcal{U}$ and a point $a \in X$, we define the **mth differential jet space** of $X$ at $a$ to be

$$Hom_{\mathcal{U}[\partial]}(\mathcal{M}_a(X)/\mathcal{M}_a^{m+1}(X),\ \mathcal{U})$$

the set of all $\partial$-module homomorphisms from $\mathcal{M}_a(X)/\mathcal{M}_a^{m+1}(X)$ to $\mathcal{U}$.

From this definition we see that the $m$th differential jet space of $X$ at $a$ is the set of all $f \in J_a^m(X)$ which commute with the derivations, i.e. $f(D(v)) = \partial(f(v))$ for all $v \in \mathcal{M}_a(X)/\mathcal{M}_a^{m+1}(X)$. What is not immediate is that the differential jet space has a more explicit form. As we will show, the differential jet space is an algebraic jet space; in particular,

$$J_a^m(X_s^\sharp) = Hom_{\mathcal{U}[\partial]}(\mathcal{M}_a(X)/\mathcal{M}_a^{m+1}(X),\ \mathcal{U}).$$

Prove Lemma 2.2 and indicate the consequences of this theorem for $J_a^m(X^\sharp)$ and $J_a^m(X)$. Prove Lemma 2.4.

Much of the discussion on the model theoretic properties of **DCF** derived from the expositions in [17] and [35]. The discussion on tangent spaces and prolongations is sampled from [18]. Lastly, the discussion on differential jet spaces comes from [24].

## 7. Proof for Characteristic Zero

7.1. **Overview.** In this section, we pull together all the ideas from the previous chapters to provide a proof of the Mordell-Lang Conjecture for function fields of characteristic zero. The theorem we present will not be as general as the original proof of Hrushovski–his result holds for all characteristics and for semi-abelian varieties (as opposed to the abelian varieties in our proof). His proof also works for groups $\Gamma$ of finite rational rank (a group has finite rational rank if there is a finitely-generated subgroup $\Gamma_0$ of $\Gamma$ such that for every nonzero $\gamma \in \Gamma$ there is an $n$ such that $n\gamma \in \Gamma_0$ and $n\gamma \neq 0$. This is not related to the Morley rank). We shall content ourselves with $\Gamma$ that are just finitely-generated. The jet-spaces proof of Pillay and Ziegler also works in full generality (semi-abelian varieties and finite rational rank groups) in characteristic zero, and for abelian varieties and finite rational rank groups in positive characteristic. For a complete exposition on these general proofs, the reader is advised to consult [11] for Hrushovski's proof and [24] for Pillay and Ziegler's result.

We chose a restricted statement of the theorem so that the entire exposition could be streamlined. We felt that the complications encountered when handling semi-abelian varieties, finite rank groups, and a positive characteristic would break the flow of the exposition. Thus, to convey the general techniques more clearly, we elided the full generality. Our main theorem (which implies the Mordell-Lang conjecture) is the following:

**Theorem 7.1.** *Let $k < K$ be algebraically closed fields of characteristic zero. Let $A$ be an abelian variety defined over $K$ and let $X$ be an irreducible subvariety of $A$ defined over $K$ as well. Let $\Gamma$ be a finitely-generated rank subgroup of $A(K)$ and suppose that $X \cap \Gamma$ is Zariski dense in $X$.* THEN *there is an $\gamma \in \Gamma$, an abelian subvariety $B$ of $A$ containing $\gamma + X$, an abelian variety $A'$ defined over $k$, an subvariety $X'$ of $A'$ defined over $k$, and a rational homomorphism $f$ from $B$ to $A'$ defined over $k$ such that $\gamma + X = f^{-1}(X')$.*

This theorem is usually what is known as the "relative form of the Mordell-Lang conjecture." It is reduction result, in that it allows us to reduce the problem from objects definable over $K$ to objects defined over the subfield $k$. In particular then, we are always able to reduce the problem to the least possible algebraically closed subfield $k$, which will be a number field. Since Faltings [8] proved the Mordell-Lang conjecture for number fields, the Mordell-Lang Conjecture is proven for all fields of characteristic zero.

Beyond having the reduction, the above theorem allows us to prove the Mordell-Lang conjecture in the special case when $A$ has $K/k$ image 0.

**Definition 7.2.** Given an abelian variety $A$ defined over $K$, the $K/k$ **image** of $A$ is an abelian variety $A'$ defined over $k$ with the following universal mapping property: there is a surjective homomorphism $\pi : A \to A'$ and for any surjective homomorphism $\pi' : A \to B$ into an abelian variety $B$ defined over $k$, there is a

unique morphism $f : A' \to B$ such that $\pi' = f \circ \pi$.

The $K/k$ image always exists (see [15]), and from the universal mapping property it is apparent that the $K/k$ image of $A$ is unique up to isomorphism. It can be thought of as the largest quotient of $A$ defined over $k$. With this definition in hand, we may now proceed with the proof of the special case of the Mordell-Lang Conjecture.

**Corollary 7.3** (Mordell-Lang Conjecture)**.** *Let $k < K$ be algebraically closed fields of characteristic zero, $A$ be an abelian variety defined over $K$ with $K/k$ image 0, $X$ a subvariety of $A$ defined over $K$, and $\Gamma$ a finitely-generated subgroup of $A$. Then there are $\gamma_1, \ldots, \gamma_m \in \Gamma$, abelian subvarieties $B_1, \ldots, B_n$ of $A$ such that $\gamma_i + B_i \subseteq X$ for each $1 \leq i \leq m$ and*

$$X(K) \cap \Gamma = \bigcup_{i=1}^{m} \gamma_i + (B_i(K) \cap \Gamma).$$

*Proof.* Let $W_1, \ldots, W_n$ be the unique decomposition of $Z = \overline{X \cap \Gamma}$ into irreducible varieties (per Theorem 3.7). As each $W_i$ is irreducible, $W_i \cap \Gamma$ is dense in $W_i$. Indeed, we have

$$Z = \overline{Z \cap \Gamma} = \bigcup_{i=1}^{n} \overline{W_i \cap \Gamma}.$$

Thus for each $i$, we have $W_i = \overline{W_i \cap \Gamma} \cup (W_i \cap \bigcup_{j \neq i} \overline{W_j \cap \Gamma})$. By irreducibility of $W_i$, either $W_i = W_i \cap \bigcup_{j \neq i} \overline{W_j \cap \Gamma}$ or $W_i = \overline{W_i \cap \Gamma}$. The former cannot be the case, since it implies $W_i \subseteq \bigcup_{j \neq i} W_j$ which is a contradiction to the choice of the $W$'s in the decomposition. Therefore we have $W_i = \overline{W_i \cap \Gamma}$ for every $1 \leq i \leq n$.

Since $Z$ is definable over $K$, each $W_i$ is definable over $K$ (this falls out from the proof of Theorem 3.7). Thus, we may apply Theorem 7.1 for each $W_i$ in the role of $X$ to choose $\gamma_i \in \Gamma$, varieties $W_i'$ defined over $k$, and rational homomorphisms $f_i$ such that $W_i = \gamma_i + f^{-1}(W_i')$. Label the variety $f^{-1}(W_i')$ by $B_i$ for each $i$. Thus, $Z = \cup_{i=1}^{n} \gamma_i + B_i$ and so

$$X(K) \cap \Gamma = Z(K) \cap \Gamma = \bigcup_{i=1}^{n} \gamma_i + (B_i(K) \cap \Gamma).$$

□

The proof of Theorem 7.1 will occur in 8 steps:

- **Step 1:** Reduce to the case where $X$ has finite stabilizer in $A$.
- **Step 2:** Transfer the problem to the context of differentially closed fields by replacing $K$ with a differentially closed field $L$ and replacing $k$ with the field of constants of $L$. Furthermore, we will require $L$ to be an $\aleph_0$-saturated model of **DCF**.
- **Step 3:** Enlarge $\Gamma$ to a finite Morley $\partial$-rank algebraic subgroup $H$ of $A$.
- **Step 4:** Choose a generic element $a \in X \cap H$.
- **Step 5:** Show that $p = tp(a/K)$ is internal to $k$.
- **Step 6:** Prove that the set of realizations of $p$ generates a connected definable subgroup $H_1$ of $H$ and call $A_1$ the closure of $H_1$. $A_1$ is an abelian subvariety of $A$.

**Step 7:** Using internality, choose a commutative algebraic group $A_2$ defined over $k$ and a $\partial$-definable isomorphism $f : H_2 \to H_1$, where $H_2 = A_2(k)$.

**Step 8:** Extend $f$ to a rational homomorphism $F : A_2 \to A_1$ and show that $F$ is in fact an isomorphism.

Of course, in steps 1, 2 and 3, we must show that a proof of the Mordell-Lang conjecture in these stronger settings implies that Mordell-Lang conjecture holds in the original, weaker setting.

I would like to thank Javier Moreno for providing me an initial version of the above outline. During my early investigations into the proof, it was an invaluable beacon, and I hope that it will serve to guide the reader equally well.

7.2. **Step 1.** Assume Theorem 7.1 holds when $X$ has finite stabilizer. Let arbitrary $X$, $A$ and $\Gamma$ be given per the hypotheses of Theorem 7.1. Let $Stab_X = \{a \in A \,|\, a + X = X\}$. $Stab_X$ is a subgroup of $A$, furthermore it is definable in terms of $X$ and $A$, both of which are definable over $K$. Thus $Stab_X$ is definable over $K$, so by Theorem 5.4, $Stab_X$ is an algebraic subgroup of $A$. By Proposition 3.24, there is a connected algebraic subgroup $S$ of $Stab_X$, which is also complete by Proposition 3.22, and thus an abelian variety. Consequently we may consider the quotient abelian variety $A_1 = A/S$ and the canonical projection $\pi : A \to A_1$. Call the image of $X$ under $\pi$, $X_1$, and label the image of $\Gamma$ by $\Gamma_1$ . $Stab_{X_1}$ is finite since $S$ had finite index and furthermore $X_1 \cap \Gamma_1$ is dense in $X_1$. Is $X_1 \cap \Gamma_1$ dense in $X_1$? Consequently we may apply Theorem 7.1 to $A_1$, $X_1$ and $\Gamma_1$ which yields an abelian variety

7.3. **Step 2.** Let $\partial$ be a derivation on $K$ such that $k$ is the field of constants (such a derivation exists by Theorem 6.6). Let $L$ be the differential closure of $K$, which is guaranteed to exist by Corollary 6.13. Since $k$ is algebraically closed, $k$ must be the field of constants of $L$ by Proposition 6.3. Consequently, $k$ is definable in $L$. Examining the statement of the Mordell-Lang conjecture, we see that $A$ and $X$ will be defined over $L$, and that $\Gamma$ will be a subgroup of $A(L) = A(K)$. Furthermore, there is no alteration to the conclusion of the conjecture. Thus, enlarging $K$ to a larger field such as $L$ does not cause a loss in generality.

We would now like to further reduce the problem to the case where $L$ is an $\aleph_0$-saturated model of **DCF**. Let $L'$ be an $\aleph_0$-saturated model of **DCF** elementarily extending $L$. Then $L'$ has a field of constants $k'$ and $k' \supseteq k$. Assuming we have proven the Mordell-Lang conjecture for $L', k', A, X, \Gamma$, we may choose $a \in A$; an abelian subvariety $B'$ of $A$ defined over $L'$ containing $a + X$, and an isomorphism $f'$ of $B'$ with an abelian variety $A'$ defined over $k'$ such that $f'(a + X)$ is defined over $k'$. Thus, $B'$ is a definable subset of $A$; $B'$ and $A'$ are abelian varieties (a first-order object in the language of **ACF**); $f'$ and $f'(a + X)$ are definable over $k'$, a definable subset of $L'$; and $f'$ is an isomorphism (a first order property). Thus, the statement of Mordell-Lang is a first order existential formula in the language of **DCF** with the parameters $A, X$, and $\Gamma$. If Mordell-Lang is satisfied by the model $L'$ of **DCF** then since $L$ is an elementary submodel, we have that Mordell-Lang holds for $L, k, A, X, \Gamma$.

Thus we have shown that without loss of generality, we may assume that $K$ is an $\aleph_0$-saturated model of **DCF** with field of constants $k$.

7.4. **Step 3.** At this point, it would be ideal if $\Gamma \subseteq A \subseteq K^n$ were a group of finite Morley $\partial$-rank; unfortunately, it may be the case that $\Gamma$ is not $\partial$-definable and hence

has no Morley $\partial$-rank. However, this scenario is the only possibility for failure, i.e. if $\Gamma$ is $\partial$-definable then its Morley $\partial$-rank must be finite. Indeed, regardless of the $\partial$-definability of $\Gamma$, we will always be able to find a $\partial$-definable group $H$ containing $\Gamma$ which will have finite Morley $\partial$-rank. Thus, if $\Gamma$ were $\partial$-definable, then by monotonicity of the rank, $\Gamma$ would also have finite $\partial$-rank. Consequently, the case when $\Gamma$ is not $\partial$-definable is the only time when we will actually need to replace $\Gamma$ with the larger group $H$. To find such $\partial$-definable group $H$ containing $\Gamma$ we consider a structure known as the Manin kernel. In this construction, we will work specifically with the abelian variety $A$ and its subgroups, however many parts of the construction work in greater generality. The interested reader is advised to consult [18] for a detailed exposition of the Manin kernel.

Before developing the tools necessary to construct the Manin kernel, we quickly remark that replacing $\Gamma$ does not lead to any loss of generality. Indeed, let us assume that $\Gamma \leq H \leq A$ as groups and the Mordell-Lang conjecture holds for $K, k, X, A$ and $H$. If $\Gamma \cap X$ is dense in $X$ then trivially $H \cap X$ is dense in $X$. Thus, the hypothesis of Mordell-Lang for $K, k, X, A$ and $\Gamma$ implies the hypothesis for $K, k, X, A$ and $H$ and thus also yields its conclusion.

Recall the setup constructed in the chapter on differentially closed fields. We are given the abelian variety $A$ (defined over $K$), the universal extension $\hat{A}$ of $A$ by a vector group, as well as the surjective homomorphism $p : \hat{A} \to A$. We are also given a homomorphism $\hat{\pi}$ from the prolongation $\tau(\hat{A})$ of $\hat{A}$ to $\hat{A}$. This map has a definable section $j : \hat{A} \to \tau(\hat{A})$. We also have the $\partial$-definable section $\hat{\nabla}$ for $\hat{\pi}$. Thus we may consider $\psi = \psi_j : \hat{A} \to \tau(\hat{A})$ whose kernel is the points of $\hat{A}$ on which $j$ and $\hat{\nabla}$ agree. Lemma 6.24 indicates that $ker\psi$ is dense in $\hat{A}$.

Consider the group $G = ker\hat{\pi}/\psi(ker(p))$. Since $t(\hat{A})$ is an extension of $\hat{A}$ by a vector group, we have that $ker\hat{\pi}$ is a vector space, specifically it will be a $k$-vector space. Similarly, since $\hat{A}$ is a vector group extension of $A$, we have that $kerp$ is a vector space, and thus $\psi$ is also a vector space. Particularly, $\psi(ker(p))$ contains the infinite set $\mathbb{Z}$ and thus by the strong minimality of the field of constants $k$ (c.f. Theorem 6.15), $\psi(ker(p))$ contains $k$ is a $k$-vector space. Therefore, $G$ is a quotient of $k$-vector spaces and has the structure of a $k$-vector space as well.

We would now like to construct a $\partial$-definable homomorphism $\mu : A \to G$. We already have the homomorphisms $p : \hat{A} \to A$ and $\psi : \hat{A} \to ker\hat{\pi}$, and there is a natural quotient homomorphism $q : ker\hat{\pi} \to G = ker\hat{\pi}/\psi(kerp)$.

**Definition 7.4.** The homomorphism $\mu : A \to G$ is defined for each $a \in A$ by $\mu(a) \in (q \circ \psi)(p^{-1}(a))$.

We first remark that $\mu$ is well-defined, that is, for every $a \in A$, $(q \circ \psi)(p^{-1}(a))$ is a singleton. Indeed, if $b, c \in \hat{A}$ and $p(b) = p(c)$ then $b - c \in kerp$ and so $\psi(b - c) \in \psi(kerp)$. But since $\psi$ is a homomorphism, $\psi(b - c) = \psi(b) - \psi(c)$ and so $q \circ \psi(b) = q \circ \psi(c)$, whence we have our desired result. We also can see that $\mu$ is surjective. From this analysis we are able to conclude that $G$ has the further structure of an algebraic group due to the following theorem of Cassidy [5]:

**Theorem 7.5.** If $A$ is an algebraic vector group and $\mu : A \to G$ is a surjective $\partial$-definable group homomorphism, then $G$ is $\partial$-definably isomorphic to an algebraic vector group.

An interesting and important question to ask is what the kernel of $\mu$ could be. As we will see in the next theorem, the kernel has a very desirable form.

**Theorem 7.6.** *Let $Tor(A)$ denote the torsion points of the group structure on $A$. Let $A^\sharp$ be the Kolchin closure of $Tor(A)$. Then if $A$ has Morley rank $d$, $A^\sharp$ has Morley $\partial$-rank $2d$. Furthermore, $ker\mu = A^\sharp$.*

*Proof.* □

Now that we have the $\partial$-definable (over $K$) $k$-vector space $G$ and $\partial$-definable (over $K$) homomorphism $\mu$, we are able to construct our finite Morley $\partial$-rank group $H$ containing $\Gamma$.

**Theorem 7.7.** *Let $\Gamma_0$ be a finitely generated subgroup of an abelian variety $A$. Then there is a finite $\partial$-dimensional algebraic subgroup $H$ containing $\Gamma_0$. Furthermore, $H \supseteq \{a \in A \,|\, \exists m \geq 0 \; ma \in \Gamma_0\}$.*

*Proof.* Let $\gamma_1, \ldots, \gamma_n$ generate $\Gamma_0$. Let $G_0 \subseteq G$ be the vector space generated by $\mu(\gamma_1), \ldots, \mu(\gamma_n)$ and consider the $\partial$-definable algebraic group $H = \mu^{-1}(G_0)$. Given an $a \in A$, if there is an $m$ such that $ma \in \Gamma_0$, then $ma = \sum_{i=1}^n s_i\gamma_i$ for some $s_i \in \mathbb{Z}$. Thus, $\mu(a) = \frac{1}{m}\sum_{i=1}^n s_i\mu(\gamma_i)$ and $\mu(a) \in G_0$. Hence, $H$ contains $\{a \in A \,|\, \exists m \geq 0 \; ma \in \Gamma_0\}$.

$H$ is finite $\partial$-dimensional since

$$\begin{aligned} \partial MR(H) &\leq \partial MR(\mu(H)) + \partial MR(ker(\mu)) \\ &= \partial MR(G_0) + \partial MR(A^\sharp) \\ &= n + 2d, \end{aligned}$$

where the pertinent information on $ker(\mu)$ is provided in Theorem 7.6. □

Thus, if we take $\Gamma_0$ to be a finitely-generated group witnessing $\Gamma$'s finite rational rank, by the last sentence of the previous theorem we have that $H$ will also contain $\Gamma$.

7.5. **Step 4.** Since $H$ is an algebraic group and $X$ is closed

Remark 1.54 (b) of Pillay lecture notes gives the existence of a unique $\partial$-generic point, which will have maximal rank.

7.6. **Step 5.** For this section, let $K'$ be a proper differential subfield of $K$.

**Theorem 7.8.** *Suppose $tp(a/K')$ has finite Morley $\partial$-rank. Let $b$ be a tuple such that $tp(a/K'b)$ is stationary. Let $c = Cb(tp(a/K'b))$. Then $tp(c/K'a)$ is internal to $k$, the field of constants.*

*Proof.* Pillay Ziegler

**Corollary 7.9.** *Let $G$ be a connected finite-$\partial$-dimensional $K'$-definable differential algebraic group. Let $a \in G$ be given with $p = tp(a/K')$ stationary. Let $H < G$ be the left-stabilizer of $p$. Then $tp(Ha/K')$ is internal to $k$, the field of constants.*

*Proof.* Pillay Ziegler

7.7. **Step 6.** Zilber's Indecomposables Theorem (see Poizat's Stable Groups book) [25]

7.8. **Step 7.** Since $\partial$-definable over $k$ (the field of constants) is the same as definable over $k$ (by Theorem 6.15), we are allowed to use Weil's theorem to construct our connected algebraic group and homomorphism defined over $k$. (commutativity of the group follows from the fact that its preimage in $A$ must be commutative, being a subgroup of the abelian group $A$). This is all Corollary 1.11 part 1) in Wood.

We now employ the following theorem of A. Weil [31]:

**Theorem 7.10** (Weil)**.** Let $V$ be an irreducible variety defined over a field $F$. Let $f : V \times V \to V$ be a rational function defined over $F$ which satisfies the following two properties:

(1) For any $x, y \in V$ generic and independent over $F$, $F(x, y) = F(x, f(x, y)) = F(y, f(x, y))$.
(2) For any $x, y, z \in V$ generic and independent over $F$, $f(f(x, y), z) = f(x, f(y, z))$.

Then there is a connected algebraic group $H$ defined over $F$, and a birational isomorphism $h$ from $V$ to $H$ defined over $F$, such that for all $x, y \in V$ generic and independent over $F$, $h(f(x, y)) = h(x) \cdot h(y)$.

So we obtain our connected commutative algebraic group defined over $k$, the field of constants. Its preimage must also be a connected algebraic group, and thus an abelian variety by Proposition 3.22.

7.9. **Step 8.** Extend naturally using Noetherianness of the Zariski topology.

## References


[1] M. F. Atiyah, I. G. McDonald, **Introduction to Commutative Algebra**, Perseus Books Publishing, 1969.

[2] E. Bouscaren, *Proof of the Mordell-Lang Conjecture for Function Fields*, **Model Theory and Algebraic Geometry: An introduction to E. Hrushovski's proof of the geometric Mordell-Lang conjecture**, E. Bouscaren (Ed.), Lecture Notes in Mathematics 1696, Springer, 1999.

[3] E. Bouscaren (Ed.), **Model Theory and Algebraic Geometry: An introduction to E. Hrushovski's proof of the geometric Mordell-Lang conjecture**, Lecture Notes in Mathematics 1696, Springer, 1999.

[4] E. Bouscaren, *An Introduction to Independence and Local Modularity*, **Algebraic Model Theory**, B.T. Hart et al., Kluwer 1997.

[5] P. Cassidy, *Unipotent Differential Algebraic Groups*, **Contributions to Algebra**, ed. H. Bass, P. Cassidy and J. Kovacic, Academic Press, 1977.

[6] G. Faltings, *Endlichkeits Sätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. 73 (1983), no. 3, 349-366.

[7] G. Faltings, *Diophantine approximation on abelian varieties*, Annals of Math. 133 (1991), 549-576.

[8] G. Faltings, *The general case of Lang's conjecture*, **Barsotti's Symposium in Algebraic Geometry**, Acad. Press, 1994, 175-182.

[9] R. Grossberg, **A Course in Model Theory**, in preparation.

[10] M. Hindry, *Introduction to abelian varieties and the Mordell-Lang conjecture*, **Model Theory and Algebraic Geometry: An introduction to E. Hrushovski's proof of the geometric Mordell-Lang conjecture**, E. Bouscaren (Ed.), Lecture Notes in Mathematics 1696, Springer, 1999.

[11] E. Hrushovski, *The Mordell-Lang Conjecture for Function Fields*, Journal of the American Mathematical Society 9 (1996), 667-690.

[12] T. Hungerford, **Algebra**, Springer, 1974.

[13] N. Koblitz, **Introduction to Elliptic Curves and Modular Forms**, Springer-Verlag, 1984.

[14] E. Kolchin, **Differential Algebra and Algebraic Groups**, Academic Press, 1973.

[15] S. Lang, **Abelian Varieties**, Interscience, 1959.
[16] D. Lascar, *Omega-stable groups*, **Model Theory and Algebraic Geometry: An introduction to E. Hrushovski's proof of the geometric Mordell-Lang conjecture**, E. Bouscaren (Ed.), Lecture Notes in Mathematics 1696, Springer, 1999.
[17] D. Marker, *Model Theory of Differential Fields*, **Model Theory of Fields**, Lecture Notes in Logic 5, Springer, 1996.
[18] D. Marker, *Manin Kernels*, **Connections betweeen Model Theory and Algebraic and Analytic Geometry**, quaderni di matematica vol. 6 (2000), 1-21.
[19] D. Marker, **Model Theory: An Introduction**, Springer Verlag, 2002.
[20] Y. Matiyasevich, *Enumerable sets are diophantine*, Dokl. Akalt. Nauk. SSSR 191 (1970), 279-282 (Russian); Sov. Math. Dokl. 11 (1970), 354-357 (English translation).
[21] D. Pierce, A. Pillay, *A note on the axioms for differentially closed fields of characteristic zero*, Journal of Algebra, 204 (1998), 108-115.
[22] A. Pillay, *Mordell-Lang for function fields in characteristic zero, revisited*, to appear in Compositio Math.
[23] A. Pillay, *Algebraically Closed Fields*, **Model Theory and Algebraic Geometry: An introduction to E. Hrushovski's proof of the geometric Mordell-Lang conjecture**, E. Bouscaren (Ed.), Lecture Notes in Mathematics 1696, Springer, 1999.
[24] A. Pillay, M. Ziegler, *Jet spaces of varieties over differential and difference fields*, to appear in Selecta Math.
[25] B. Poizat, **Stable Groups**, American Mathematical Society, 2001.
[26] M. Rosenlicht, *Extensions of vector groups by abelian varieties*, Am. J. Math 80 (1958).
[27] T. Scanlon, *Diophantine Geometry from Model Theory*, Bulletin of Symbolic Logic, 7 , no. 1, March 2001, 37-57.
[28] I. R. Shafarevich, **Basic Algebraic Geometry**, Springer-Verlag, 1970.
[29] J. H. Silverman, J. Tate, **Rational Points on Elliptic Curves**, Springer, 1992.
[30] K. E. Smith, L. Kahanpää, P. Kekäläinen, W. Traves, **An Invitation to Algebraic Geometry**, Springer, 2000.
[31] A. Weil, *On algebraic groups of transformations*, American Journal of Math. 77 (1955).
[32] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. Math. 141 (1995), 443-551.
[33] A. Wiles, R. Taylor, *Ring-theoretic properties of certain Hecke algebras*, Ann. Math. 141 (1995), 553-572.
[34] C. Wood, *The model theory of differential fields*, Israel J. Mathematics vol. 16, 1973.
[35] C. Wood, *Differentially Closed Fields*, **Model Theory and Algebraic Geometry: An introduction to E. Hrushovski's proof of the geometric Mordell-Lang conjecture**, E. Bouscaren (Ed.), Lecture Notes in Mathematics 1696, Springer, 1999.

*E-mail address*: paulb2@andrew.cmu.edu