Lectures 1 and 2 of “Model Theory and Diophantine Geometry”, Arizona Winter School, 2003

Anand Pillay
University of Illinois at Urbana-Champaign

February 24, 2003

1 Introduction

These notes are for the first two lectures of the lecture series ”Model Theory and Diophantine Geometry” by Thomas Scanlon and myself. The full series of lectures will be on the Manin-Mumford conjecture and variants. As is well-known, model-theoretic ideas, specifically definability theory in difference fields of characteristic zero, were used by Hrushovski [2] to give another proof of the Manin-Mumford conjecture concerning the intersection of subvarieties of a (semi)-abelian variety A with the group of torsion points of A. Subsequently Scanlon [7] used the positive characteristic difference field theory to prove Denis' conjecture, a version of Manin-Mumford for Drinfeld modules (and this is the only known proof). Scanlon will present his proof (in lectures 3-5), which will use the whole model-theoretic machinery. I will give a self-contained “new” proof (in lecture 2) of Manin-Mumford, avoiding model theory other than some elementary properties of existentially closed difference fields.

I would like to thank Piotr Kowalski for many comments and suggestions which helped me considerably in preparing these notes.

2 Difference fields and differential fields

The main purpose of this section is to introduce existentially closed difference fields which will play a central role in most of the lectures in our series.

I will use freely basic notions of first order logic: theories, complete theories, formulas, definable sets, the notion of being definable *over* a given set of parameters, quantifier-elimination, and sometimes saturated models.

The main first order theories which we shall consider here are $ACFA$, the theory of existentially closed fields with an automorphism, and its completions.

As a motivating and somewhat "easier" example, we will also discuss DCF_0, the theory of differentially closed fields of characteristic zero.

In the background is the theory ACF of algebraically closed fields. The language of ACF is that of rings $(+, -, \cdot, 0, 1)$, and ACF has quantifier elimination in this language. The completions are obtained by fixing the characteristic. It is often convenient to regard the objects of algebraic geometry (varieties, morphisms,..) as definable sets and functions in an algebraically closed field. This is not so much due to ignorance of the scheme-theoretic point of view, but is rather because this presentation is directly amenable to current model-theoretic methods. The point of view essentially coincides with that of Weil's Foundations. That is, we work in an algebraically closed field K of uncountable transcendence degree. An affine variety V is a subset of K^n defined by finitely many polyomial equations. If k is a countable subfield over which V is defined, then a generic point of V over k is a point $a \in V$ such that $tr.deg(k(a)/k) = dim(V)$. The assumptions on K ensure that such generic points exist. For irreducible V defined over k, any given k-constructible property will hold on a Zariski open subset of V if and only if it holds at a generic point of V over k. This formalism passes over to abstract varieties in the sense of Weil.

The notion of an existentially closed structure in a given class of structures is rather central: Let T be a $\forall\exists$ theory in a language L. An ec structure for T is an L-structure M which is a substructure of a model of T and such that whenever $M \subseteq N \models T$, and $\phi(x_1, .., x_n)$ is a quantifier-free firmula with parameters from M which has a solution in N, then $\phi(x_1, .., x_n)$ has a solution in M. An ec structure for T will actually be itself a model of T.

In many cases, the class of ec structures for T is axiomatizable, namely is the class of models of a first order L-theory T' containing T. In that case we say that T' is the model companion of T. T' has the feature of being model-complete (any L-formula is equivalent mod T to both an existential and universal formula). Again in many situations T' has outright quantifier-elimination. In any case, saturated models of T' will be "universal domains" for studying models of the original theory T.

Let us start by briefly describing DCF_0, as here the relationship between definability and geometry is clearest. A derivation ∂ on a field K is an additive homomorphism such that $\partial(x \cdot y) = \partial(x) \cdot y + x \cdot \partial(y)$. A differential field is a field equipped with a derivation. If (K, ∂) is such, then a differential polynomial over K in indeterminates $x_1, .., x_n$ is a polynomial over K in indeterminates $x_1, .., x_n, \partial(x_1), .., \partial(x_n), \partial^2(x_1), .., \partial^2(x_n), ...$ If $P(x)$ is a differential polynomial over K in the single indeterminate x then the order of P is the greatest n such that $\partial^n(x)$ appears nontrivially in P. An (affine) differential algebraic variety is the zero set of a finite number of differential polynomials. There are associated notions of differential polynomial map and differential rational map.

DF_0 denotes the theory of differential fields (fields equipped with a derivation) of characteristic 0 in the language of rings together with a symbol ∂ for the derivation. DF_0 *does* have a model companion, and this is the (complete) theory DCF_0, the theory of differentially closed fields of characteristic zero. The easiest to state axioms for DCF_0 are those found by L. Blum, and concern differential polynomial equations in a single differential indeterminate x: if f, g are differential polynomials over K and the order of f is strictly greater than the order of g then the system $f(x) = 0, g(x) \neq 0$ has a solution in K. An important fact is that DCF_0 has quantifier-elimination in the given language. So definable subsets of K^n are Boolean combinations of "differential algebraic varieties", and definable maps are piecewise differential rational functions. Although this will not play a role in these first lectures, it is worth mentioning another important model-theoretic property of DCF_0: it is ω-stable. This means that if K is a countable differentially closed field, then the number of complete n-types over K is countable. The ω-stability of a theory gives rise to an intrinsic ordinal valued dimension, called Morley rank, which can be assigned to formulas or definable sets in models of the theory. Roughly speaking, a definable set X has Morley rank 0 if it is finite, and Morley rank $\geq \alpha + 1$ if there are pairwise disjoint definable subsets X_i

of X for $i = 1, 2, ...$ such that each X_i has Morley rank $\geq \alpha$.

Let us fix $K = (K, +, \cdot, \partial)$ a saturated differentially closed field, which note is also an algebraically closed field. Let $X \subset K^n$ be definable over a differential subfield k. We call X finite-dimensional if there is a finite bound on $tr.deg.(k(a, \partial(a), \partial^2(a)...)/k)$. for $a \in X$. The "category" of finite-dimensional definable sets in K and definable maps between them, is what was relevant and useful for issues such as the geometric version of Mordell-Lang. X is finite-dimensional if and only if the Morley rank of X, $RM(X)$ is finite. Among such sets is the field $\mathcal{C}$ of constants of K, another algebraically closed field. The structure induced on $\mathcal{C}$ from living in $(K, +, \cdot, \partial)$ is just the field structure. So our category of finite Morley rank sets includes "algebraic geometry", but is much richer.

It is worth mentioning a rather more geometric way of interpreting finite Morley rank sets in DCF_0. Let $V \subseteq K^n$ be an irreducible algebraic variety. The first prolongation $\tau(V)$ of V will be the subvariety of K^{2n} given by the defining equations for V (in the first n coordinates), as well as the equations
$\sum_{i=1,..,n}(\partial P/\partial x_i)(x_1, .., x_n)v_i + P^{\partial}(x_1, .., x_n)$.
as P ranges over generators of the ideal of V.
Here P^{∂} is the result of hitting the coefficients of P with the derivation ∂.
If V is defined over the constants, then $\tau(V)$ is precisely the tangent bundle of V. In any case $\tau(V)$ comes with a canonical projection $\pi : \tau(V) \to V$. Let $s : V \to \tau(V)$ be a map (in the algebraic-geometric sense) which is also a section of π. Pairs of the form (V, s) are precisely the "algebraic D-varieties" of Buium, and belong to algebraic geometry.

An important fact about differentially closed fields, is that in the above situation, $(V, s)^{\sharp} =_{def} \{a \in V(K) : s(a) = (a, \partial(a))\}$ is *Zariski-dense* in V. Moreover, up to finite Boolean combination, every definable set of finite Morley rank in K is of the form $(V, s)^{\sharp}$.

Let us now turn to difference fields. Fix a language L_σ consisting of the language of rings $L = \{+, \cdot, -, 0, 1\}$ together with a unary function symbol σ. ACF_σ is the $\forall\exists$ L_σ-theory expressing that K is an algebraically closed field and σ is an automorphism. (K being a ring and σ being an endomorphism would also be enough.) We call a model (K, σ) of ACF_σ a difference field.

It turns out that ACF_σ does have a model companion, namely the class of existentially closed difference fields is axiomatizable. In fact the additional axioms are precisely:

(*) for any irreducible variety V over K, and any irreducible variety $W \subset V \times \sigma(V)$ defined over K which projects dominantly onto both V and $\sigma(V)$, there is $a \in V(K)$ such that $(a, \sigma(a)) \in W$.

To actually write down the axioms requires quantifying over the coefficients in the defining polyomials of V and W as well as knowing that things such as "irreducibility" are constructible conditions.

In any case the resulting theory is usually called $ACFA$. $ACFA$ is not complete, even after fixing the characteristic. The completions are determined by the isomorphism type of the algebraic closure of the prime field considered as a difference field with the retriction of σ.

Again we have the notion of a difference polynomial over a difference field (K, σ): a polynomial over K in indeterminates $x_1, .., x_n, \sigma(x_1), ..., \sigma(x_n), \sigma^2(x_1), ...$ A difference-algebraic variety is a subset of K^n defined by finitely many difference polynomial equations. So the quantifier-free definable sets in difference fields are Boolean combinations of difference-algebraic varieties. $ACFA$ does *not* have quantifier-elimination, but as for pseudofinite fields, it is rather close. Any L_σ-formula $\phi(x_1, .., x_n)$ is equivalent, modulo $ACFA$ to a formula of the form $\exists y(\theta(\bar{\sigma}(x_1.., x_n), \bar{\sigma}(y))$ where $\bar{\sigma}(\bar{x})$ denotes $(\bar{x}, \sigma(\bar{x}), .., \sigma^m(\bar{x}))$ for some m, θ is a quantifier-free L-formula (that is a formula in the language of rings) and $\theta(\bar{z}, \bar{w})$ implies that $\bar{w}$ is (field-theoretically) algebraic over $\bar{z}$.

If (K, σ) is a model of $ACFA$, the fixed field $Fix(\sigma)$ of σ in K is a pseudofinite field (namely an infinite model of the theory of finite fields). In fact the structure $(Fix(\sigma), +, \cdot)$ is *strongly stably embedded* in the structure $(K, +, \cdot, \sigma)$. Namely, if $X \subset Fix(\sigma)^n$ is definable with parameters in the structure $(K, +, \cdot, \sigma)$, then X is definable in the structure $(Fix(\sigma), +, \cdot)$ with parameters.

$ACFA$ (or rather its completions) are not ω-stable. They have a somewhat weaker model-theoretic property, *supersimplicity*, which will appear in later lectures. On the other hand $ACFA$ *is* quantifier-free ω-stable, meaning that over any countable model there are only countably many complete quantifier-free types. This yields an ordinal-valued Morley rank for quantifier-free formulas, defined as above, but restricted to quantifier-free formulas.

Let us now fix a (saturated) model $(K, +, \cdot, \sigma)$ of $ACFA$, and definability will mean definablity in this structure (with parameters). Let X be definable over a difference subfield k. We say that X is finite-dimensional if there is a finite bound on $tr.deg(k(a, \sigma(a), \sigma^2(a), ..)/k)$ for $a \in X$. If X is quantifier-free definable (for example a difference-algebraic variety), then X will be finite-dimensional if and only X has finite quantifier-free Morley rank.

The interesting category for us will be that of finite rank difference-algebraic varieties. Among the sets here are the fixed fields $Fix(\sigma^n)$ in characteristic zero, and more generally $Fix(\sigma^r \circ Fr^m)$ in positive characteristic where Fr is the Frobenius automorphism.

As in the DCF_0 case, quantifier-free definable sets of finite rank have canonical representations up to Boolean combination. Let V be an irreducible variety, and let W be a correspondence between V and the variety $\sigma(V)$. This means that W is an irreducible algebraic subvariety of $V \times \sigma(V)$ inducing a generic finite-to-finite correspondence between V and $\sigma(V)$. Given such data V and W, let $(V, W)^\sharp$ denote $\{a \in V(K) : (a, \sigma(a)) \in W\}$. Then the finite rank difference-algebraic varieties are essentially sets of the form $(V, W)^\sharp$. The axioms for $ACFA$ imply that $(V, W)^\sharp$ is Zariski-dense in V. Note the following special case of (V, W): V is defined over $Fix(\sigma)$ (so $\sigma(V) = V$), and W is the graph of a dominant morphism $\phi : V \to V$. So the classification of finite rank difference varieties in a sense subsumes the algebraic geometrical classification of such pairs (V, ϕ).

Let us elaborate on this latter category somewhat, and state and prove an easy result which will be used later. (K, σ) is as before a (saturated) model of $ACFA$, in particular a universal domain for algebraic geometry. By a "algebraic σ-variety" we will mean, for now, an irreducible algebraic variety V equipped with a dominant morphism $\phi : V \to \sigma(V)$. (Note this is an object of algebraic geometry, and is not the same thing formally as a finite rank difference-algebraic variety.) By a σ-morphism between (V, ϕ) and (W, ψ) we mean a morphism $f : V \to W$ (in the sense of algebraic geometry) such that $\sigma(f) \circ \phi = \psi \circ f$ on V. By a σ-rational map between (V, ϕ) and (W, ψ) we mean a rational (not everywhere defined) map from V to W such that for generic $a \in V$, $\sigma(f)(\phi(a)) = \psi(f(a))$. By an algebraic σ-group we mean a connected algebraic group G, equipped with an isogeny $\phi : G \to \sigma(G)$. (Note that the group operation will then by a σ-morphism.) Finally we will call an algebraic σ-variety (V, ϕ) *trivial* if V is defined over $Fix(\sigma)$ and ϕ is the identity. So note that our objects are algebraic varieties with additional structure and the morphisms are just algebraic morphisms respecting this additional structure. On the other hand, note that if f is a σ-(iso)-morphism between (V, ϕ) and (W, ψ), then f induces a map (bijection) between $(V, \phi)^\sharp$

and $(W,\psi)^\sharp$. Moreover, for such f and g, if $f|(V,\phi)^\sharp = g|(V,\phi)^\sharp$ then $f = g$ (by Zariski-denseness).

Fact 2.1 *Suppose that (G,ϕ) is an algebraic σ-group, X is an irreducible σ-subvariety of G containing the identity, X generates G, and $(X,\phi|X)$ is σ-birationally isomorphic to a trivial σ-variety. Then (G,ϕ) is σ-isomorphic (as an algebraic σ-group) to a trivial algebraic σ-group.*

Proof. Let $f : X \to Y$ be the σ-birational map between $(X,\phi|X)$ and (Y,id) where Y is defined over $Fix(\sigma)$. As X generates G, multiplication induces a surjective morphism $\pi : X^d \to G$ (for some d) and this is clearly a σ-morphism. On the other hand, f^{-1} induces a σ-birational isomorphism between Y^d and X^d. Composing, we obtain a dominant σ-rational map h from (Y^d,id) to (G,ϕ). We would like to obtain from this a trivial σ-variety Z, and a σ-birational isomorphism between (Z,id) and $G(\phi)$. Consider the equivalence relation E on generic points of Y^d: $E(a,b)$ iff $h(a) = h(b)$. As h is a σ-rational map, we see that $h(a) = h(b)$ implies $\sigma(h)(a) = \sigma(h)(b)$, so E is σ-invariant, as is its Zariski-closure, which is therefore defined over $Fix(\sigma)$. This yields a rational dominant map h' defined over $Fix(\sigma)$ from Y^d to some variety Z defined over $Fix(\sigma)$ such that for generic points a, b of Y^d, $h'(a) = h'(b)$ iff $E(a,b)$ iff $h(a) = h(b)$. Composing h'^{-1} with h yields a σ-birational isomorphism h'' between (Z,id) and (G,ϕ). The group operation on G induces, via h''^{-1}, a generically associative operation $Z \times Z \to Z$, which is σ-invariant, hence defined over $Fix(\sigma)$. Weil's theorem then yields an algebraic group H defined over k, and h'' extends to a (σ)-isomorphism between (H,id) and (G,ϕ).

3 The Manin-Mumford conjecture: statement and background

The setting of the theorem will be characteristic zero. We will prove:

Theorem 3.1 *Let k be a number field, A a semiabelian variety defined over k, and X an irreducible subvariety of A also defined over k. Let $Tor(A)$ denote the group of torsion elements of A, a subgroup of $A(\bar{k})$. Then the Zariski closure of $X \cap Tor(A)$ is a finite union of translates of abelian subvarieties of A.*

Some words of explanation: An abelian variety is a connected algebraic group whose underlying variety is projective (or complete). An algebraic torus is an algebraic group isomorphic to some finite power of $\mathbf{G}_m$ the multiplicative group. A semiabelian variety is a commutative algebraic group which, as an algebraic group, is an extension of an abelian variety by an algebraic torus. A semiabelian variety is divisible. The torsion elements of a semiabelian variety form a Zariski-dense subgroup. Also there are only finitely many elements of order r for any given r. In fact if A is an abelian variety then $T_p(A)$ the group of elements of A with order a power of p is $\mathbf{Z}_{p^\infty}^{2dim(A)}$, and if A is an algebraic torus then this is $\mathbf{Z}_{p^\infty}^{dim(A)}$.

We will refer to the statement of the theorem as the Manin-Mumford conjecture although this was first stated in the case where X is a curve of genus ≥ 2 embedded in its Jacobian A. In this case the conclusion can be restated as $X \cap Tor(A)$ is finite. (For otherwise some X will already be the Zariski closure of its intersection with $Tor(A)$ and as X is irreducible, the conclusion of the theorem forces X to be an abelian subvariety of A, up to translation, hence an elliptic curve, contradicting genus being ≥ 2.)

Various versions of this conjecture were proved by Raynaud, Hindry, McQuillan, Bogomolv, Ullmo-Zhang, Buium (some with explicit bounds). Hrushovski [2] gave a proof of Theorem 3.1, using the model theory of difference fields of characteristic zero. The first step involved essentially capturing $Tor(A)$ by a finite rank difference equation of a special kind. The second step involved showing that the resulting finite-dimensional difference-algebraic group is "modular". This second step proceeded via an analysis of orthogonality and definable groups in $ACFA_0$, using results from [1]. In our proof below, the first step is identical, but we give what amounts to a different and direct proof of the second step, in the language of algebraic σ-groups, following ideas in [4]. Closely related things were done in the papers [5] and [6] of Pink and Roessler. In fact it was after seeing these papers that I realized that various easy reductions allow a direct application of the jet-map methods from [4]. Jet maps, following Abramovich, also appear in Pink-Roessler's second paper [6], but our formalism, working in existentially closed difference fields and considering linear difference equations on jets, seems to have some advantages.

4 The proof.

Let A, X, k be as in the assumptions of the theorem 3.1. First some notation. We write the group operation on A as + and so also 0 for the identity. If K is an extension field of k (such as $\bar{k}$ for example), σ is an automorphism of K over k, and $P(T) \in \mathbf{Z}(T)$, say $P(T) = a_nT^n + ...a_1T + a_0$, then $P(\sigma)$ denotes the following (non algebraic) endomorphism of $A(K)$: $P(\sigma)(x) = a_n\sigma^n(x) + ... + a_1\sigma(x) + a_0x$.

First note that by replacing X by an irreducible component of the Zariski closure of $X \cap Tor(A)$, we may assume that $X \cap Tor(A)$ is Zariski-dense in X. (The new X will be defined over a finite extension of k, still a number field.) Replacing X by a $X - a$ for some $a \in X \cap Tor(A)$, we may assume in addition that $0 \in X$. We now have to prove that X is a semiabelian subvariety (that is, a connected algebraic subgroup) of A.

Lemma 4.1 *After possibly replacing k by a finite extension, there is an automorphism σ of $\bar{k}$ over k, and a monic polynomial $P(T) \in \mathbf{Z}(T)$ which has no complex roots of unity among its roots, such that $Tor(A) \subseteq Ker(P(\sigma))$.*

Proof. The argument, following Hrushovski, is purely algebraic. Pink-Roessler reproduce the argument too. I have nothing new to say here, but will give a sketch for the sake of completeness. Let $\mathbf{p}$ be a prime of good reduction for A. This means that $\mathbf{p}$ is a prime ideal of the ring of integers of the number field k, and that after reducing the equations defining A mod $\mathbf{p}$ one obtains a semiabelian variety $A_{\mathbf{p}}$ over $\mathbf{F}_q$ (for a suitable prime power $q = p^r$) whose abelian and linear parts have the same dimensions as those of A. In particular if $L, \bar{A}$ are the linear, abelian parts of A then $L_{\mathbf{p}}$, $\bar{A}_{\mathbf{p}}$ are the linear and abelian parts of $A_{\mathbf{p}}$. Let $T'_p(-)$ denote prime-to-p torsion points. So we have an exact sequence:
$0 \to T'_p(L_{\mathbf{p}}) \to T'_p(A_{\mathbf{p}}) \to T'_p(\bar{A}_{\mathbf{p}}) \to 0$. Let σ be the automorphism $x \to x^q$ of the algebraic closure of $\mathbf{F}_q$. A result of Weil [8] yields a monic integral polynomial $F_1(T) \in \mathbf{Z}(T)$ without complex roots of unity among its roots such that $F(\sigma) = 0$ on $T'_p(\bar{A}_{\mathbf{p}})$. On the other hand, if $L_{\mathbf{p}}$ is isomorphic to a power of the multiplicative group over $\mathbf{F}_{q^l}$ then taking $F_2(T)$ to be $T^l - q^l$, $F_2(\sigma)$ will vanish on $T'_p(L_{\mathbf{p}})$. Thus, if $F(T)$ is the product of F_2 and F_1 then $F(\sigma)$ vanishes on $T'_p(A_{\mathbf{p}})$.

Now, if L is the maximal unramified extension of the completion $k_{\mathbf{p}}$ of k at $\mathbf{p}$, then σ lifts to an automorphism σ' of L, $T'_p(L) \subseteq A(L)$, and the reduction map yields a bijection between $T'_p(A)$ and $T'_p(A_{\mathbf{p}})$, and thus an abstract isomorphism between $(T'_p(A), +, \sigma')$ and $T'_p(A_{\mathbf{p}}), +, \sigma)$. Hence $F(\sigma')$ vanishes on $T'_p(A)$.

We then easily obtain an automorphism σ' of $\bar{k}$ which vanishes on $T'_p(A)$. We can do exactly the same thing with any other prime of good reduction of A. Now a result of Serre implies, that after passing to a finite extension k_1 of k, and if $\mathbf{p}$ is a prime of k_1 of good reduction for A, then $k_1(T_p(A))$ and $k_1(T'_p(A))$ are linearly disjoint over k_1. We assume that $k_1 = k$, and pick two primes $\mathbf{p}$, $\mathbf{l}$ of good reduction for A. By the previous paragraph, we find automorphisms σ, τ of $\bar{k}$ over k and monic integer polynomials $P_p(T)$, $P_l(T)$ without complex roots of unity among their roots such that $P_p(\sigma)$ vanishes on $T'_p(A)$ and $P_l(\tau)$ vanishes on $T'_l(A)$. In particular $F_l(\tau)$ vanishes on $T_p(A)$. By linear disjointness, $\sigma|k(T'_p(A))$ and $\tau|k(T_p(A))$ extend to a common automorphism σ' of $\bar{k}$ over k. As $Tor(A) = T_p(A) + T'_p(A)$, taking $P = P_pP_l$, $P(\sigma')$ vanishes on $Tor(A)$, and the lemma is proved.

We now perform an elementary reduction to get to the context of "algebraic groups equipped with an isogeny". Let $H = Ker(P(\sigma)) \subset A(\bar{k})$. Note that H is Zariski-dense in A, as $Tor(A)$ is. Assume that $P(T) = T^n + a_{n-1}T^{n-1} + .. + a_1T + a_0$ (with $a_i \in \mathbf{Z}$). Let $A^n = A \times A \times .. \times A$ (n times), and likewise for X^n. Let $H_1 = \{(x, \sigma(x), .., \sigma^{n-1}(x)) : x \in H\}$. Let ϕ be the (algebraic) endomorphism of A^n defined by: $\phi(x_0, .., x_{n-1}) = (x_1, x_2, .., x_{n-2}, -a_0x_0 - a_1x_1 - .. - a_{n-1}x_{n-1})$. Let $\pi : A^n \to A$ be the projection onto the first coordinate.

Remark 4.2 *For each $r \geq 1$ $\phi^r - id$ is an isogeny of A^n.*

Proof. Note first that $P(\phi) = 0$. We leave it as an exercise to show that for each r there is an integral polynomial $P_r(T)$ with no complex roots of unity amng its roots such that $P_r(\phi^r) = 0$. Now if $\phi^r - id$ is not an isogeny, then there is a connected positive-dimensional semiabelian subvariety B of A^n on which ϕ^r acts as the identity. As there are only finitely many elements of B of any given order it follows that $P_r(1) = 0$, a contradiction.

Lemma 4.3 *There are a semiabelian variety B of A^n (defined over k) and an irreducible subvariety X' of B (defined over a finite extension of k) such*

that
(i) $\pi|B : B \to A$ *is surjective,*
(ii) $\phi|B$ *is an isogeny of* B *with itself,*
(iii) for some $m \geq 1$, $\phi^m(X') \subseteq X'$.
(iv) $\pi(X')$ *is a Zariski-dense subset of* X.

Proof. Note first that
(*) H_1 is precisely $\{x \in A^n(\bar{k}) : \sigma(x) = \phi(x)\}$.
Let B_1 be the Zariski closure of H_1 in A^n, and B the connected component of B_1. B_1 and B are defined over k. Because $\pi(H_1) = H$ and H is Zariski-dense in A, it follows that π maps B_1 onto A and thus π maps B onto A yielding (i).
As B_1 is defined over k, and σ fixes k pointwise, for any $b \in H_1$, $\phi(b) \in B_1$, hence $\phi(B_1) \subseteq B_1$. For any Zariski open subset U of B_1 defined over k, U meets H_1, hence $\phi(B_1)$ meets U. So $\phi(B_1) = B_1$. Hence also $\phi(B) = B$, giving (ii).
Let us now write π for $\pi|B$. Let $B^\sharp$ denote $B \cap H_1$. Then $\pi(B^\sharp)$ has finite index in H hence, as $0 \in X$, $\pi(B^\sharp \cap X)$ is Zariski-dense in X. Let Y be the Zariski closure of $\pi^{-1}(X) \cap B^\sharp$ in B. As in the proof of (ii), Y is defined over k and $\phi(Y) \subseteq Y$. Also $\pi(Y)$ is Zariski-dense in X. So clearly there is an irreducible component X' of Y say, which contains 0 and such that $\pi(X')$ is Zariski-dense in X. X' is defined over some finite extension of k. Moreover, as ϕ will permute the irreducible commponents of Y, $\phi^m(X') \subseteq X'$ for some $m \geq 1$. This proves (iii) and (iv).

With the data given by the lemma, we have two cases.
CASE I. X' is a semiabelian subvariety of B.
But then $\pi(X') = X$ will be a semiabelian subvariety of A, and the theorem is proved.

CASE II. Otherwise.
We seek a contradiction. Let S be the stabilizer of X' in B, namely $\{b \in B : b + X = X\}$. Then S is ϕ^m-invariant, and $X'/S \subseteq B/S$ is positive-dimensional, with trivial stabilizer. Moreover ϕ^m is an isogeny of B/S with itself, X'/S is ϕ^m-invariant, and, by Remark 4.2, $\phi^{rm} - 1$ is an isogeny of B/S with itself, for all $r \geq 1$. So, changing notation, the contradiction will follow from the next general proposition. This is essentially 7.1 in [6], and can be considered as as an endomorphism analogue of the result 2.1 in [3] on

algebraic D-groups. Our proof follows closely the latter.

Proposition 4.4 *Let A be a semiabelian variety, $\phi : A \to A$ a separable isogeny, and $X \subseteq A$ a subvariety of X containing 0. Suppose that $\phi(X) \subseteq X$ and that $Stab_A(X) = \{0\}$. Then for some $r \geq 1$, $\phi^r | A_X =$ identity, where A_X is the semiabelian subvariety of A generated by X.*

Proof. It is convenient to work in a saturated existentially closed difference field (K, σ) such that all the data is defined over $k = Fix(\sigma)$. We will identify A and X with their sets $A(K), X(K)$ of K-points. Let $A^\sharp = \{a \in A : \sigma(a) = \phi(a)\}$ and likewise for $X^\sharp$. As $(K, \sigma) \models ACFA$, $A^\sharp$ is Zariski-dense in A and $X^\sharp$ is Zariski-dense in X.

Let $\mathcal{M}$ be the maximal ideal of the local ring of A at 0. For $p \geq 1$, let $j_p(A)_0$ be the p-jet of A at 0, namely the dual space to $\mathcal{M}/\mathcal{M}^{p+1}$. $j_p(A)_0$ is a finite-dimensional K-vector space (defined over k). For any subvariety Y of A passing through 0 we obtain likewise $j_p(Y)_0$ as a subspace of $j_p(A)_0$. If Z varies in an algebraic family of subvarieties of A all passing through 0, then there is sufficiently large p such that Z is determined within this family by $J_p(Z)_0 \subseteq j_p(A)_0$. We will apply this to the family $\{X - t : t \in X\}$ of translates of X by elements of X. For suitably large p and for some r, we have a rational map $f : X \to Gr_r(L)$, defined over k, where $L = j_p(A)_0$, $Gr_r(L)$ is the variety of r-dimensional subspaces of L, and $f(t) = j_p(X - t)_0$. Moreover, as X has trivial stabilizer in A, f is a birational isomorphism of X with the Zariski closure of its image, Y say. For $t \in X$ write $f(t) = L_t < L$.

By separability, ϕ induces a linear automorphism ϕ' of L, defined over k. Moreover as L is defined over k, $\sigma(L) = L$, hence $L^\sharp = \{v \in L(K) : \sigma(v) = \phi'(v)\}$ is Zariski-dense in L.

Now suppose $t \in X^\sharp$. Then $\sigma(X - t) = \phi(X - t)$. Hence $\sigma(L_t) = \phi'(L_t)$, whereby $L_t^\sharp = \{v \in L_t : \sigma(t) = \phi'(t)\}$ is again Zariski-dense in L_t. Note that $L_t^\sharp$ is precisely $L_t \cap L^\sharp$.

L is a K-vector space of dimension m say, and $L^\sharp$ is a k-vector subspace of the same dimension. Moreover a basis b can be found for $L^\sharp$ over k which is simultaneously a basis for L over K. With respect to the basis b, L identifies with K^n (hence $Gr_r(L)$ with $Gr_r(K^n)$), and $L^\sharp$ identifies with k^n. For $t \in X^\sharp$, $L_t^\sharp$ is then a subspace of k^n. As this is Zariski-dense in L_t it implies that L_t is defined over k, namely $L(t) \in Gr(K^n)(k)$. As $X^\sharp$ is Zariski-dense in X, it follows that a Zariski-dense set of points of $Y = f(X)$ are defined over k, hence so is Y.

So we have so far proved:

Claim 1. There is a birational map f between X and a variety Y, such that Y is defined over k and for $t \in X^\sharp$, $f(t) \in Y(k)$.

Now we consider the semiabelian subvariety A_X of A generated by X. Note that $\phi(A_X) = A_X$. So by Fact 2.1, we have:

Claim 2. There is an algebraic group B defined over k and an (algebraic) isomorphism h between A_X and B such that $h(A_X^\sharp) = B(k)$.

The graph of f is a semiabelian subvariety of $A_X \times B$. As $A_X \times B$ is defined over k, h (and so also h^{-1}) is defined over a finite extension k_1 of k. It follows that $A_X^\sharp$ is contained in $A_X(k_1)$. For some n, k_1 is contained in $Fix(\sigma^n)$. So ϕ^n is the identity on $A_X^\sharp$. By Zariski-denseness, ϕ^n is the identity on A_X. This completes the proof of Proposition 4.4, and thus also the proof of Theorem 3.1.

Remark 4.5 *From the proof above, one can deduce Corollary 4.1.13 of [2], at least in its quantifier-free version: Work in $(K, \sigma) \models ACFA_0$ as above. Let A be a semiabelian variety defined over $Fix(\sigma)$. Let $P(T)$ be a a polynomial over the integers with no complex roots of unity among its roots. Then $B = Ker(P(\sigma)) < A(K)$ is "quantifier-free modular", namely every quantifier-free definable subset of B^n is a Boolean combination of translates of quantifier-free definable subgroups.*

5 Project/ Exercise

In Pink and Roessler's paper [6], the following is proved (Proposition 7.3 in that paper).

Proposition 5.1 *(char. $p > 0$.) Let A be a semiabelian variety, and $\phi : A \to A$ an isogeny. Assume that r, s are postive integers, and that there is a separable isogeny λ from $Fr^r(A)$ to A such that $\phi^s = \lambda \circ Fr^r$. Let X be an irreducible subvariety of A containing 0 such that $\phi(X) \subseteq X$, $Stab_A(X)$ is trivial, and X generates A. Show that there is an isomorphism f of A with a semiabelian variety A_0 defined over $\mathbf{F}_{p^r}$ such that $(f(\phi))^s = Fr^r$ on A_0.*

Some words of explanation. Fr denotes the Frobenius automorphism $x \to x^p$. This, as well as its powers, act on varieties, as well on points of varieties. So Fr^r is a bijective morphism between X and $Fr^r(X)$. $f(\phi)$ in the last line of the proposition denotes the isogeny $f \circ \phi \circ f^{-1}$ of A_0. $\mathbf{F}_{p^r}$ is the finite field with p^r elements. The proof of the proposition in [6] seems somewhat involved.

The project is to find a simple proof of Proposition 6.1 along the lines of our proof of 4.4, and using a suitable modification of Fact 2.1.

Another general question relating these lectures to those of Scanlon, is whether the methods above apply to the Drinfeld modules version of Manin-Mumford.

References

[1] Z. Chatzidakis and E. Hrushovski, Model theory of difference fields, Transactions AMS, 351 (1999), 2997-3071.

[2] E. Hrushovski, The Manin-Mumford conjecture and the model theory of difference fields, Annals of Pure and Applied Logic, 112 (20001), 43-115.

[3] A. Pillay, Mordell-Lang for function fields in characteristic zero, revisited, to appear in Compositio Math. (See “recent preprints” at http://www.math.uiuc.edu/People/pillay.html)

[4] A. Pillay and M. Ziegler, Jet spaces of varieties over differential and difference fields. (See “recent preprints” at http://www.math.uiuc.edu/People/pillay.html)

[5] R. Pink and D. Roessler, On Hrushovski’s proof of the Manin-Mumford conjecture. (See “recent preprints” at http://www.math.ethz.ch/ pink/preprints.html)

[6] R. Pink and D. Roessler, On ψ-invariant subvarieties of semiabelian varieties and the Manin-Mumford conjecture (See “recent preprints” at http://www.math.ethz.ch/ pink/preprints.html)

[7] T. Scanlon, Diophantine geometry of the torsion of a Drinfeld module, Journal of Number Theory, vol. 97, Number 1, (2002), 10-25.

[8] Andre Weil, *Varieties abeliennes et courbes algebrique*, Hermann, Paris 1948.