ACFA Seminar

David Marker
University of Illinois, Chicago
Fall 1997

My goal this semester is to survey the work of Hrushovski and Chatzidakis on the model theory of ACFA and its application in Hrushovski's proof of the Manin-Mumford conjecture for number fields. The references for the seminar are the following preprints:

Z. Chatzidakis & E. Hrushovski, Model theory of difference fields

Z. Chatzidakis, Groups definable in ACFA

A. Pillay, ACFA and the Manin Mumford Conjecture

The later two papers will appear in the proceedings of the NATO Workshop in Algebraic Model Theory. I am also using notes from a course Pillay gave at Notre Dame.

§1 Model Completeness and Quantifier Elimination

Let $\mathcal{L}^-$ be the language of rings $\{+,-,\cdot,0,1\}$ and let $\mathcal{L}$ be $\mathcal{L}^- \cup \{\sigma\}$ where σ is a unary function symbol.

Definition (K,σ) is a model of ACFA, the theory of algebraically closed fields with a generic automorphism if and only if

1) K is an algebraically closed field,

2) σ is an automorphism of K, and

3) If $U \subset K^n$ is an irreducible variety, V is an irreducible subvariety of $U \times \sigma(U)$ that projects generically onto U and $\sigma(U)$ and W is a proper subvariety of V, then there is $a \in U(K)$ such that $(a,\sigma(a)) \in V \setminus W$.

Remarks It takes a bit of work to show that 3) is first order. Recall that if $\phi(\bar{x},\bar{y})$ is an $\mathcal{L}^-$ formula, then $\{\bar{b} : \{\bar{a} : \phi(\bar{a},\bar{b})\}$ has dimension $k\}$, is definable by an $\mathcal{L}^-$ formula for any k. Indeed this is true for Morely rank in any strongly minimal set. Thus "projects generically onto" can be expressed in a first order way.

One can show that "irreducibility" is first order using the following observations.

a) Suppose $V \subset K^n$ is a Zariski closed set of dimension d and $n > d+1$. Then V is irreducible iff for all $p \in K^n \setminus V$ and all hyperplanes H, the projection of V to H via p is irreducible.

b) Suppose $\phi(x,y,b)$ defines an $n-1$ dimensional subset of the K^n for all b. For each b there is a nonzero polynomial $p(\bar{x})$ such that $\{\bar{x} : \phi(\bar{x},b) \wedge p(\bar{x}) \neq 0\}$ has dimension at most $n-2$. By compactness there is a number d such that we can choose a p of degree at most d. Then $\phi(\bar{x},b)$ is irreducible iff there is a polynomial p of degree at most d such that $\{\bar{x} : \phi(\bar{x},b) \wedge p(\bar{x}) \neq 0\} = \emptyset$ and p does not factor. This is first order.

The definability of "irreducibility" is intimately related to the fact that in algebraically closed fields Morely degree is definable (ie. ACF has the *definable multiplicity property*). Indeed one can give a different characterization of ACFA using the conclusion of the lemma below instead of 3). Using the definable multiplicity property one can see that this has a first order axiomatization. Indeed much of the basic theory generalizes to strongly minimal sets with the definable multiplicty property and elimination of imaginaries.

Lemma 1.1 Suppose $K \models$ ACFA, $\mathbf{K} \supset K$ is an algebraically closed field, $a, b \in \mathbf{K}^n$ and $\mathrm{tp}^-(b/K) = \sigma(\mathrm{tp}(a/K))$, and $\phi(x, y)$ is an $\mathcal{L}^-$ formula over K such that $\phi(a, b)$. There is $c \in K^n$ such that $\phi(c, \sigma(c))$.

Proof

Let U be the locus of a over K (i.e. the smallest Zariski closed set defined over K containing a). Let V be the locus of (a, b) over K. By assumption, the locus of b over K is $\sigma(U)$. By quantifier elimination in algebraically closed fields, there is a proper Zariski closed set W such that $(x, y) \in V \setminus W \to \phi(x, y)$. Since $K \models$ ACFA, there is $c \in U(K)$ such that $(c, \sigma(c)) \in V \setminus W$.

Lemma 1.2 If (F, σ) is a field with an automorphism, then there is $(K, \sigma^*) \supseteq (F, \sigma)$ with $K \models$ ACFA.

Proof

Since we can always extend a field automorphism to the algebraic closure we may assume F is algebraically closed. The lemma will then follow by iterated applications of the following claim.

claim If F is an algebraically closed field, U, V and W are as in 3) and all are defined over F, then there is (F_1, σ_1) extending (F, σ) and $a \in U(F_1)$ such that $(a, \sigma_1(a)) \in V \setminus W$.

Let F_1 be a big algebraically closed field. Let (a, b) be a generic point of V. Then $(a, b) \notin W$, a is a generic point of U and b is a generic point of $\sigma(U)$. Thus $\mathrm{tp}^-(a/F) = \sigma(\mathrm{tp}^-(a/F))$. Thus we can extend σ to F_1 sending a to b.

Remark Suppose F is an $\aleph_0$-saturated algebraically closed field. Topologize $Aut(F)$ by taking basic open sets $N_f = \{\tau : \tau \supset f\}$ where f is a finite partial automorphism. The above argument shows that for any U, V, W as in 3), the set of automorphisms σ where there is no solution $(a, \sigma(a)) \in V \setminus W$ is nowhere dense in $Aut(F)$ and hence should be avoided by a "generic" automorphism (i.e. if we build an automorphism by Cohen forcing, that automorphism will satisfy ACFA).

Theorem 1.3 ACFA is model complete.

Proof

Suppose $K \subset L$ are models of ACFA, $\phi(x_1, \ldots, x_n)$ is a quantifier free $\mathcal{L}$ formula with parameters from K, $\bar{b} \in L$ and $L \models \phi(\bar{b})$. There is a quantifier free $\mathcal{L}^-$ formula ψ such that $\phi(\bar{x}) \leftrightarrow \psi(\bar{x}, \sigma(\bar{x}), \sigma^2(\bar{x}), \ldots, \sigma^m(\bar{x}))$.

Let $c = (\bar{b}, \sigma(\bar{b}), \ldots, \sigma^{m-1}(\bar{b}))$ and $d = \sigma(c) = (\sigma(\bar{b}), \ldots, \sigma^m(\bar{b}))$. Let $\theta(\bar{u}_1, \ldots, \bar{u}_m, \bar{v}_1, \ldots, \bar{v}_m)$ be the $\mathcal{L}^-$ formula

$$\psi(\bar{u}_1, \ldots, \bar{u}_m, \bar{v}_m) \wedge \bar{v}_1 = \bar{u}_2 \wedge \bar{v}_2 = \bar{u}_3 \wedge \ldots \bar{v}_{m-1} = \bar{u}_m.$$

By 1.1 there is $e = (\bar{e}_1, \ldots, \bar{e}_m)$ in K with $\theta(e, \sigma(e))$. But then $\bar{e}_{j+1} = \sigma^j(\bar{e}_1)$ for $j = 1, \ldots, m-1$ and $\phi(\bar{e}_1)$.

Suppose E, F and K are fields with $E \subset F$ and $E \subset K$. Recall that F and K are *linearly (algebraically) disjoint* over E if whenever $c_1, \ldots, c_n \in F$ are linearly (algebraically) dependent over K, then they are linearly (algebraically) dependent over E. We summarize some standard facts about linear and algebraic disjointness.

Lemma 1.4 a) F and K are linearly disjoint over E iff the homomorphism $a \otimes_E b \mapsto ab$ gives an embedding of $F \otimes_E K$.

b) Suppose F and K are linearly disjoint over E, $\sigma \in Aut(F)$, $\tau \in Aut(K)$ and $\sigma|E = \tau|E$. There is an automorphism μ of the composite FK such $\mu|F = \sigma$ and $\mu|K = \tau$.

c) If F and K are linearly disjoint over E, then they are algebraically disjoint over E.

d) If F and K are algebraically disjoint over E and E is algebraically closed, then F and K are linearly disjoint over K.

Proof

a) and c) are standard. b) follows easily from i) as we can extend σ and τ to $F \otimes_E K$. d) can be found in Lang's *Algebra*. Here is a model theoretic proof. Let $\bar{\alpha} \in F$ be linearly dependent over K. Let U be the locus of $\bar{\alpha}$ over the algebraic closure of K and let V be the locus of $\bar{\alpha}$ over E. Since "irreducibility" is definable, U and V are irreducible over the algebraic closure of K. Since $\bar{\alpha}$ has the same transcendence degree over E and K, U and V have the same dimension and hence are equal. Since U is contained in a hyperplane, by model completeness there is a hyperplane H defined over E such that $\bar{\alpha} \in H$. Thus $\bar{\alpha}$ is linearly dependent over E. [Another model theoretic proof uses the fact that $\mathrm{tp}(\bar{\alpha}/K)$ is the heir of $\mathrm{tp}(\bar{\alpha}/E)$.]

For any $A \subset K$ we let $\langle A \rangle_\sigma$ denote the smallest subset of K containing A and closed under σ and σ^{-1} and let $\mathrm{acl}_\sigma(A)$ denote the algebraic closure of $\langle A \rangle_\sigma$.

Proposition 1.5 If $E \subset K$ and $E = \mathrm{acl}_\sigma(E)$, then ACFA + Diag($E$) is complete.

Proof

Suppose $(L, \tilde{\tau}) \models$ ACFA and $(L, \tilde{\tau}) \supset (E, \sigma)$. We want to show that $K \equiv L$. Work inside a large saturated algebraically closed field $\mathbf{K}$ and find copies of L and K that are algebraically disjoint over E. By 1.4 we can extend σ and τ to an automorphsim μ of $\mathbf{K}$ as in 1.1 we can also insure $(\mathbf{K}, \mu) \models$ ACFA. Since ACFA is model complete, $K \equiv L$.

Corollary 1.6 The theory of a model of ACFA is determined by the action of σ on the algebraic closure of the prime field.

Corollary 1.7 $\mathrm{tp}(a/A) = \mathrm{tp}(b/A)$ if an only if there is an isomorphism between $\mathrm{acl}_\sigma(A, a)$ and $\mathrm{acl}_\sigma(A, b)$ fixing A and sending a to b.

While quantifier elimination fails in ACFA (for example $\exists y\ y^2 = x$ is not equivalent to a quantifier free formula). We can eliminate quantifiers down to very special existential formulas.

Let Σ be the collection of all formulas of the form $\exists y_1, \ldots, \exists y_n\ \phi(\bar{x}, \bar{y})$ where $\phi(\bar{x}, \bar{y})$ is quantifier free and if $\phi(\bar{a}, \bar{b})$, then $\bar{b} \in \mathrm{acl}_\sigma(\bar{a})$. The conjunction or disjunction of Σ formulas is equivalent to a Σ formula.

Lemma 1.8 Suppose $\phi(\bar{a}) \to \phi(\bar{b})$ for all Σ-formulas ϕ, then $\mathrm{tp}(\bar{a}) = \mathrm{tp}(\bar{b})$.

Proof

Since $\psi(\bar{a}) \leftrightarrow \psi(\bar{b})$ for all quantifier free formulas, $\langle \bar{a} \rangle_\sigma \cong \langle \bar{b} \rangle_\sigma$. Suppose $c \in \mathrm{acl}_\sigma(\bar{a})$. Let $p(X, \bar{a})$ be a polynomial in X such that $p(c, \bar{a}) = 0$.

If $\phi_1(x, \bar{a}), \ldots, \phi_n(x, \bar{a})$ are Σ formulas such that $\phi(c, \bar{a})$, then there is a d such that $p(d, \bar{b}) = 0$ and $\phi_1(d, \bar{b}) \wedge \ldots \wedge \phi_n(d, \bar{b})$. Since there are only finitely many solutions to $p(X, \bar{b}) = 0$, by a pigeon hole argument we can find d such that $p(d, \bar{b}) = 0$ and $\phi(d, \bar{b})$ for any Σ formula ϕ such that $\phi(c, \bar{a})$. We extend our isomorphism by sending c to d and continuing inductively.

Thus $\mathrm{acl}_\sigma(\bar{a}) \cong \mathrm{acl}_\sigma(\bar{b})$, and $\mathrm{tp}(\bar{a}) = \mathrm{tp}(\bar{b})$.

Theorem 1.9 (Quantifier Elimination) Every formula $\phi(\bar{v})$ is equivalent to a Σ formula.

Proof

If $\phi(\bar{a})$, then by the lemma and compactness there is a Σ formula $\psi(\bar{v})$ such that $\psi(\bar{a})$ and $\psi(\bar{v}) \to \phi(\bar{v})$. By compactness of the Stone space there are Σ formulas $\psi_1(\bar{v}), \ldots, \psi_m(\bar{v})$ such that $\psi_i(\bar{v}) \to \phi(\bar{v})$ and $\phi(\bar{v}) \to \bigvee \psi_i(v)$. Thus $\phi(\bar{v}) \leftrightarrow \bigvee \psi_i(v)$.

In characteristic zero we can say a bit more. Let Σ_1 be the collection of Σ formulas with a single existential quantifier. A disjunction of Σ_1 formulas is easily seen equivalent to a Σ_1 formula. In fact every Σ formula is equivalent to a Σ_1 formula. Suppose $\exists y_1 \ldots \exists y_n$ $\phi(\bar{x}, \bar{y})$ is a Σ formula. If $\phi(\bar{a}, \bar{b})$ then, by the primitive element theorem, the extension of $\langle \bar{a} \rangle_\sigma$ generated by $b_1, \ldots, b_n$ is generated by a single element c. By compactness we can find d, m and l such that $\exists \bar{y}\ \phi(\bar{x}, \bar{y})$ iff there is a z satisfying a polynomial of degree at most d and rational functions over the integers $r_1, \ldots, r_n$ of degree at most l such that if $w_i = r_i(\bar{x}, \sigma(\bar{x}), \ldots, \sigma^m(\bar{x}), z)$, then $\phi(\bar{x}, w_1, \ldots, w_n)$. The right hand side can be expressed as a disjunction of Σ_1 formulas and is hence equivalent to a Σ_1 formula.

We give a second useful consequnece of our description of types.

Lemma 1.10 a is model theoretically algebraic over A if and only if $a \in \mathrm{acl}_\sigma(A)$.

Proof

Let $E = \mathrm{acl}_\sigma(A)$ and suppose $a \in K \setminus E$. We want to show that a is not model theoretically algebraic over E. Working in a large algebraically closed field $\mathbf{K} \supset K$. Find $K_1, K_2, \ldots$ isomorphic to K over E and algebraically disjoint over E. Let a_i denote the image of a. Let σ_i be the automorphism of K_i induced by σ via the isomorphism. As in 1.4 we can extend σ to an automorphsim of $\mathbf{K}$ such that $\sigma | K_i = \sigma_i$ and we may assume $(\mathbf{K}, \sigma) \models \mathrm{ACFA}$. By 1.7 all of the a_i have the same type as a over E, so a is not model theoretically algebraic over E.

Clearly every element of $\mathrm{acl}_\sigma(A)$ is model theoretically algebraic over A.

In these notes, $\mathrm{acl}(A)$ will usually denote the field theoretic algberaic closure.

§2 The Fixed Field

Let $K \models$ ACFA and let $F = \{x \in K : \sigma(x) = x\}$ be the fixed field of σ. The field F plays an essential role in the model theory of ACFA.

We say that a field F is *pseudofinite* iff

a) F is perfect,

b) F is pseudoalgebraically closed (PAC) (ie. if V is an absolutely irreducible variety defined over F, then $V(F) \neq \emptyset$), and

c) F has a unique extension of degree d for each $d > 1$.

In deep and beautiful work Ax proved that pseudofinite fields are exactly the infinite models of the theory of finite fields.

Theorem 2.1 (van den Dries) F is pseudofinite.

Proof

If K has characteristic $p > 0$, and $\sigma(a) = a$, then a has a unique p^{th} root b in K and b must also be fixed by σ. Thus F is closed under p^{th} roots and hence perfect.

Suppose U is an absolutely irreducible variety defined over F. Then $\sigma(U) = U$. Let $V = \{(x, y) \in U \times U : x = y\}$. Since $K \models ACFA$, there is $a \in U(K)$ such that $(a, \sigma(a)) \in V$. Clearly $a \in U(F)$, so F is PAC.

Fix $d > 1$. Let $t_1, \ldots, t_n$ be algebraically independent over K. Extend σ to $K(t_1, \ldots, t_n)$ by $\sigma(t_i) = t_{i+1}$ for $i < d$ and $\sigma(t_d) = t_1$. By lemma 1.2 we can find $L \models$ ACFA, with $L \supset K(t_1, \ldots, t_n)$. Thus by model completeness there are $a_1, \ldots, a_n \in K$ such that $\sigma(a_i) = a_{i+1}$ for $i < d$ and $\sigma(a_d) = a_1$. Then $(X - a_1) \cdots (X - a_d) \in F[X]$ is the minimal polynomial of a_i/F for each i and $F(a_i)$ is an extension of degree d.

Suppose $F \subset L_1, L_2 \subset K$ are two distinct extensions of F of degree $d > 1$. Let L be a finite Galois extension of F such that $L \supset L_1, L_2$. We claim that L is a cylcic extension of F. Let G be the Galois group of L/F. Since L is Galois, $\sigma|L \in G$. We claim $\sigma|L$ generates G. If not, then by the fundamental theorem of Galois theory there is a proper extension E/F, such that $E = \{x \in L : \sigma^m(x) = x \text{ for all } m\}$. But then $E \subseteq F$, a contradiction. Thus G is cyclic.

There are $G_1, G_2 \subset G$ such that $L_i = \{x \in L : \forall \tau \in G_i \ \tau(x) = x\}$ and $[L : G_i] = d$. But, since G is cylcic, there is only one subgroup of index d, a contradiction.

Lemma 2.2 (Duret) Pseudofinite fields have the independence property.

Proof

Let F be a pseudofinite field. Let $d \in F \setminus F^2$. Suppose $a_1, \ldots, a_n, b_1, \ldots, b_m \in F$ are distinct.

We claim that there is $x \in F$ such that $(x - a_i) \in F^2$ for $i = 1, \ldots, n$ and $(x - b_j) \notin F^2$ for $j = 1, \ldots, m$.

Consider $V = \{(x, y_1, \ldots, y_n, z_1, \ldots, z_m, w_1, \ldots, w_m) : \bigwedge y_i^2 = x - a_i \wedge \bigwedge z_i = d(x - b_i) \wedge \bigwedge z_i(u - b_i) = 1\}$. V is absolutely irreducible and thus there is $(x, \bar{y}, \bar{z}, \bar{w}) \in V(F)$. Clearly $(x - a_i)$ and $d(x - b_j)$ is a square for all i and j. Since $x - b_j \neq 0$ and $d \notin F^2$, $(x - b_j) \notin F^2$.

Corollary 2.3 ACFA has the independence property and is hence unstable.

Alternatively one could note that the sqaures form a subgroup of the multiplicative subgroup of index 2. By results of Poizat the multiplicative subgroup of a stable field is connected. So F is unstable.