§6 Where we are going and why: number theoretic applications

Before continuing our analysis of types and forking in ACFA, I would like to give some glimpse of where we are heading and why.

Our main goal will be the Chatzidakis-Hrushovski Dichotemy theorem. We now restrict our attention to characteristic zero (we call this ACFA_0). We begin by recalling two definitions from stability theory.

Definition Suppose $p \in S(A)$ and $q \in S(B)$. We say that p and q are *orthogonal* if for any $C \supseteq A \cup B$ if p' and q' are non-forking extensions of p and q to C and a and b realize p' and q', then $a \mathop{\smile\!\!\!\!\!\!|}_C b$. We write $p \perp q$. If $p \in S(A)$ and ϕ is a formula, we say p is orthogonal to ϕ if for $p \perp q$ for any complete type q with $\phi \in q$

We say that $p \in S(E)$ is *1-based* if A_0 and B_0 are independent over $\text{acl}_\sigma(EA_0) \cap \text{acl}_\sigma(EB_0)$ for any A_0 and B_0 finite sets of realizations of p.

Theorem 6.1 (The Dichotemy Theorem for ACFA_0) If $\text{SU}(p) = 1$, then either p is stable and locally modular or $p \not\perp \sigma(x) = x$.

In particular, if G is a definable group, then either G is stable and 1-based, or $G \not\perp \sigma(x) = x$.

Once we know G is stable and 1-based, we can use the Hrushovski-Pillay result that definable subsets are Boolean combinations of cosets of definable subgroups. The following theorem gives an important algebraic tool for deciding if a subgroup is orthogonal to the fixed field.

Theorem 6.2 Let K be a model of ACFA of characteristic zero. Let A be a commutative algebraic group defined over the fixed field. Suppose $P(X)$ is a polynomial and view $P(\sigma)$ as an endomorphism of A. The group $B = ker(P(\sigma))$ is of finite SU-rank and B is stable and 1-based if and only if P has no cyclotomic factors (ie. no root of unity is a root of p).

In the remainder of the semester I will discuss aspects of the proofs of 6.1 and 6.2. But for the rest of this section we will look at applications of 6.2. As a warm up we give an easy application of 6.2. The following lemma was used by Falting's in his proof of the Mordell-Lang Conjecture.

Proposition 6.3 Suppose A is an abelian variety and X is a subvariety of A such that $2X = X$ (ie. the homomorphsim $x \mapsto x + x$ sends X onto X). Then X is a coset of an abelian subvariety of A.

Proof

Suppose A and X are defined over an algebraically closed field K of chatacteristic zero. Let x be a generic point of X. Then $2x$ is also a generic point of X. Let σ be an automorphism of the algebraic closure of $K(x)$ sending x to $2x$ and fixing K. Extend σ to $L \supset K(x)$ such that $L \models$ ACFA. View σ as an automorphism of A. Let $P(X) = X - 2$. Then $P(\sigma)$ is an endomorphism of A and $x \in ker(P(\sigma)) \cap X$. By 6.3 $ker(P(\sigma))$ is 1-based, thus $X \cap P(\sigma)$ is a Boolean combination of cosets of definable subgroups. Let $B + b$ be such a coset containg x. If C is the Zariski closure of B, then C is an algebraic subgroup of A and $C + b$ is contained in X. Since $C + b$ contains a generic point of X, $C + b = X$.

The premier application of 6.2 is Hrushovksi's proof of the Manin-Mumford conjecture.

Theorem 6.4 Let A be a connected commutative algebraic group and X a subvaritey of A defined over a number field K. Then $X \cap Tor(A)$ is a finite union of cosets $Tor(B) + b$ where B is a connected algebraic subgroup of A and $b \in A$.

Theorem 6.4 was proved for abelian varieties by Raynaud and for commutative algebraic groups by Hindry. Aside from giving a new proof Hrushovski's proof (with more work) gives better bounds on the number of cosets needed.

Hrushovski's proof to 6.4 is in two steps. The first is to show that for most primes p, the conclusion holds with $T'_p(A)$ replacing $Tor(A)$, where T'_p is the set of torsion points with order prime to p. The harder step is to show that once we know this for two primes we know it for all $Tor(A)$. In fact this step was know to number theorists, but Hrushovski must give a new proof to get his bounds to work.

We will illustrate the first case (making a few simplifying assumptions).

Suppose A is an abelian varitey, $X \subset A$ is a curve and both A and X are defined over $\mathbf{Q}$. Suppose X is not a coset of a subgroup of A. We will show $T'_p(A) \cap X$ is finite for most primes p.

We may assume all the polynomials used to define A (and the graph of its group law) have coefficents in $\mathbf{Z}$. It makes sense to look at A_p the object defined by reducing the equations mod p. We say that p is a prime of *good reduction* if A_p is an abelian variety of dimension $2\dim(A)$. By compactness, all but finitely primes are primes of good reduction. We will assume p is a prime of good reduction.

We fix some notation $\mathbf{F}_p$ will be the field with p elements, $\mathbf{Q}_p$ is the field of p-adic numbers and $\mathbf{Z}_p$ be the ring of p-adic integers. We let K be the algebraic closure of $\mathbf{Q}_p$ and k be the algebraic closure of $\mathbf{F}_p$. K is itself a henselian valued field with valuation ring R and reduction map $\pi : R \to k$.

If $x \in A(K)$, then since A is a projective variety we can think of x as having homogeneous coordinates in R and $\pi(x) \in A_p(k)$. The following lemma is proved by careful applications of Hensel's lemma

Lemma 6.5 i) $\pi : A(K) \to A_p(k)$ is surjective.

ii) If $x \in A(K)$ is a torsion point of order l, where l is prime to p, then $\pi(x) \neq 0$.

iii) There is an automorphsim σ of K such that $\sigma|\mathbf{Q}_p$ is the identity and $\pi(\sigma(x)) = \sigma(x)^p$ for $x \in R$. We call σ a lifting of Frobenius.

Corollary 6.6 $\pi : T'_p(A) \to T'_p(A_p)$ is an isomorphism.

Proof

By 6.4 ii) π is an embedding. For any m there are $m^{2\dim(A)}$ points of order m in both A and A_p, thus π is surjective.

We work in generality. Let B be an abelian variety. Let l be a prime which is not equal to the characteristic of the field of definition of B. Let $B[l^n]$ denote the Torsion points of B of order l^n. Then $|B[l^n]| = l^{2n\dim(B)}$ and $B[l^n]$ is a free $\mathbf{Z}/l^n\mathbf{Z}$-module of dimension $2\dim(B)$. The map $x \mapsto lx$ is a homomorphism from $B[l^{n+1}]$ to $B[l^n]$ and the module structure commutes with the homomorphsim $m \mapsto m (\mathrm{mod}\ l^n)$ from $\mathbf{Z}/l^{n+1}\mathbf{Z}$ to $\mathbf{Z}/l^n\mathbf{Z}$. The *Tate Module* $T^l(B)$ is defined to be $\lim\limits_{\leftarrow} A[l^n]$. Thus $T^l(B) = \{(a_1, a_2, \dots) : a_i \in B[l^i]$ and $la_{i+1} = l_i\}$. Clearly $T^l(B)$ is a free $\mathbf{Z}_l$-module of dimension $2\dim(B)$.

Lemma 6.7 Suppose B is an abelian variety defined over $\mathbf{F}_q$ where $q = p^n$. The automorphism $\tau(x) = x^q$ determines an automorphsim of B. There is a polynomial $P(X)$ with integer coefficients such that $P(\tau) = 0$ and P has no cyclotomic factors.

Proof (sketch)

Let $l \neq p$ be a prime. Any automorphsim of B determines an automorphsim of the Tate module $T^l(B)$. As $T^l(B)$ is a finite dimensional free $\mathbf{Z}_l$-module, we can find a characteristic polynomial $P(X) \in \mathbf{Z}_l[X] \setminus \{0\}$ such $P(\tau) = 0$ on $T^l(B)$. The hard part (that we will skip) is that $P(X) \in \mathbf{Z}[X]$.

Since $\{x : l^n x = 0 \text{ for some } n\}$ is Zariski-dense in B, $P(\tau) = 0$ on B. Suppose λ is an n-th root of unity and $P(\lambda) = 0$. (ie. λ is an eigenvalue of τ). It follows that $1 = \lambda^n$ is an eigenvalue of τ^n. But then there is a non-zero $v = (a_1, a_2, \dots) \in T^l(B)$ with $\tau^n(v) = v$ and τ fixes infinitely many elements of A, a contradiction since $\mathrm{Fix}(\tau^n)$ is finite.

Let $(L, \sigma) \models$ ACFA with $L \supset K$ and $\sigma|K$ a lifting of Frobenius. Clearly σ induces an automorphsim of $T'_p(A)$ and the reduction map π is an isomorphism between $(T'_p(A), +, \sigma)$ and $(T'_p(A_p), +, \tau)$ (where $\tau(x) = x^p$). Let $P(X)$ be the polynomial we get by applying 6.7 to A_p. Then $P(T'_p(A)) = 0$. Thus $T'_p(A) \subseteq B = \{x \in A(L) : P(x) = 0\}$. By theorem 6.2, B is a stable 1-based group of finite SU rank. By Hrushovski-Pillay $B \cap X$ is a finite union of cosets of definable subgroups of A. If $C + b$ is such a coset then it's Zariski closure is a coset of an algberaic subgroup of A. Since the Zariski closure is contained in the curve X and X is not a coset of a subgroup, $C + b$ is finite. Since $T'(A) \cap X \subseteq B \cap X$, $T'(A) \cap X$ is finite.

This explains the prime-to-p case. We refer the reader to Pillay's article *ACFA and the Manin-Mumford Conjecture* for details on how to do the general case (and to Hrushovski's article to see how to get the bounds).