A drastically oversimplified partial account of Hrushovski's approach to Manin-Mumford

Martin Bays

2023-05-17
Blockseminar "Model Theory meets Algebraic Geometry"
Landhaus Rothenberge, Universität Münster

Contents

1 Torsion

Definition 1. Let A be a commutative algebraic group.

- $A[n] := \{x : nx = 0\} \leq A$, the n-torsion subgroup
- $A[\infty] := \bigcup_{n\in\mathbb{N}} A[n]$, the torsion subgroup.
- For p prime,
$$A[p]' := \bigcup_{\{n:(n,p)=1\}} A[n],$$
the prime-to-p-torsion subgroup.
- Also $A[p^\infty] := \bigcup_n A_p^n$.

Fact 1. *If A is an abelian variety and n is prime to the characteristic, $A[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2\dim A}$.*

2 Manin-Mumford

Theorem ("Manin-Mumford Conjecture"; Raynaud 1983 (A abelian), Hindry 1987)**.**
*Let A be a commutative algebraic group over a number field K.
Let $\Gamma := A[\infty]$ be the torsion subgroup.
Let $X \subseteq A$ be a subvariety.
Then $X \cap \Gamma$ is a finite union of cosets of subgroups of A.*

Hrushovski gave (1996) a new proof of this theorem.
Very briefly, the proof proceeds as follows:

- Consider A as a definable group in a model of ACFA_0.
- Let p be a suitable prime (almost all primes will be suitable).
- We find a finite rank definable subgroup $B \leq A$ containing $A[p]'$.
- Using the trichotomy for ACFA_0, we show that B is a 1-based group.
- Then $X \cap B$ is a boolean combination of cosets.
- Hence $X \cap A[p]'$ is a finite union of cosets.
- Considering two different primes, conclude the same for $X \cap A[\infty]$.

Here, we sketch the broad outlines of the proof of this latter result,
with a number of drastic simplifying assumptions.

Definition 2. Let A be an abelian variety.

- A is **simple** if it has no infinite proper algebraic (i.e. Zariski closed, equiv. ACF-definable) subgroup.
- $\mathrm{End}(A)$ is the ring of algebraic endomorphisms (equiv. ACF-definable endomorphisms).
For $n \in \mathbb{Z}$, the multiplication-by-n map $[n] : x \to nx$ is an endomorphism,
so we consider $\mathbb{Z} \leq \mathrm{End}(A)$ embedded this way.
So $\mathrm{End}(A) = \mathbb{Z}$ means there are no other algebraic endomorphisms.

We sketch Hrushovski's strategy in the following special case:

Theorem 3. *Let A be a simple abelian variety over $\mathbb{Q}$ with $\mathrm{End}(A) = \mathbb{Z}$.
Then for any proper subvariety $X \subsetneq A$,
$X \cap A[\infty]$ is finite.*

3 Definable endomorphisms and subgroups

Let $(L, \sigma) \models \mathrm{ACFA}_0$ be a monster model. Identify A with $A(L)$.

Fact 2. *Let G be an algebraic group over L.
Any definable subgroup $H \leq G$ is of finite index in a subgroup of the form*
$$\{x : (x, \sigma x, \ldots, \sigma^{n-1}x) \in S\}$$
for some algebraic subgroup
$$S \leq G \times G^\sigma \times \ldots \times G^{\sigma^{n-1}}.$$

Using this and the structure of algebraic subgroups of abelian varieties,
we can understand definable subgroups of A as follows.
A is over $\mathbb{Q}$, so $A^\sigma = A$,
and σ induces a group automorphism of A.
Hence any Laurent polynomial $f(\sigma) \in \mathbb{Z}[\sigma, \sigma^{-1}]$ induces a group endomorphism of A;
e.g. $(\sigma^{-4} + 3 + 2\sigma^2)(x) = \sigma^{-4}(x) + 3x + 2\sigma^2(x)$.

Definition.

- Let $\mathrm{End}^*(A)$ be the ring of definable group endomorphisms of A.
- Let $E^*(A) := \mathbb{Q} \otimes \mathrm{End}^*(A)$.

Fact 3.

(I) $E^*(A)$ is the Laurent polynomial ring $\mathbb{Q}[\sigma, \sigma^{-1}]$.

*(II) Any definable subgroup $H \leq A$ is a finite index subgroup of the kernel of a definable endomorphism,
i.e. $H \leq \ker(f)$ and $[\ker(f) : H] < \infty$ for some $f \in \mathrm{End}^*(A)$.*

(III) Any proper definable subgroup $H < A$ has finite rank.

*(IV) Let $f, g \in \mathrm{End}^*(A)$.
Then $\ker(f) \cap \ker(g)$ has finite index in $\ker(f)$ iff $f|g$ in $E^*(A)$
(and $\ker(f) \leq \ker(g)$ iff $f|g$ in $\mathrm{End}^*(A)$).*

4 Good reduction

Definition. $f(T) \in \mathbb{Z}[T]$ has **no cyclotomic factors** if no cyclotomic polynomial divides f;
equivalently, no root of unity $\zeta \in \mathbb{C}$ satisfies $f(\zeta) = 0$.

Proposition 1. *For all but finitely many primes p,
there is $f(T) \in \mathbb{Z}[T]$ with no cyclotomic factors and $\sigma \in \mathrm{Aut}(\bar{\mathbb{Q}})$
such that $A[p]' \leq \ker(f(\sigma))$.*

Proof. Let $p \in \mathbb{N}$ be prime, let $\psi : \mathbb{Z} \to \mathbb{F}_p$ be the reduction map.
Reducing the coefficients of the defining polynomials over $\mathbb{Z}$,
we obtain a reduced variety A_p over $\mathbb{F}_p$,
and a reduced "addition" $+_p : (A_p)^2 \to A_p$ (possibly ill-defined).
Say p is **of good reduction** for A if $(A_p, +_p)$ is an abelian variety of the same dimension as A.

Fact. *All but finitely many p are of good reduction.*

Proof. Write above conditions as an $\mathcal{L}_{\mathrm{ring}}$-sentence which holds in ACF_0,
and hence by compactness in ACF_p for all large enough p. □

Fact (Weil)**.** *Let p be of good reduction.
Let $\phi_p \in \mathrm{Aut}(\mathbb{F}_p^{\mathrm{alg}})$ be Frobenius $x \mapsto x^p$.
Then there is $f(T) \in \mathbb{Z}[T]$ with no cyclotomic factors such that $f(\phi_p)$ vanishes on A_p.*

Sketch proof. Let $l \neq p$ be prime.
Let $T_l := \varprojlim_n A_p[l^n]$ as a $\mathbb{Z}_l$-module (the l-adic Tate module).
Let $V_l := \mathbb{Q}_l \otimes_{\mathbb{Z}_l} T_l$, a finite-dimensional $\mathbb{Q}_l$-vector space.
Then ϕ_p acts on T_l and hence on V_l as a linear endomorphism.
Let $f(T) := \det(TI - \phi_p|_{V_l})$ be the characteristic polynomial of this action.
A priori $f(T) \in \mathbb{Q}_l[T]$, but it turns out that $f(T) \in \mathbb{Z}[T]$.
Now if ζ is an nth root of unity and $f(\zeta) = 0$,
then ζ is an eigenvalue of $\phi_p|_{V_l}$,
and hence 1 is an eigenvalue of $\phi_p^n|_{V_l}$.
Then ϕ_p^n has infinitely many fixed points in $A_p[\infty]$,
contradicting the fact that the fixed field of ϕ_p^n is the finite field $\mathbb{F}_{p^n}$.
Finally, $f(\phi_p|_{V_l}) = 0$ (Cayley-Hamilton),
so $f(\phi_p)$ is zero on $A_p[l^\infty]$,
and hence on A_p, since (Fact) $A_p[l^\infty]$ is Zariski dense in A_p. □

Now by some valuation theory we'll omit:

- ϕ_p lifts to an automorphism σ of $\bar{\mathbb{Q}}$.
- If m is coprime to p, any m-torsion point of A_p lifts to an m-torsion point of A.

Now
$$|A[m]| = m^{2\dim A} = |A_p[m]|$$
for m coprime to p,
so the homomorphism
$$\psi : A[p]' \to A_p[p]'$$
is an isomorphism.

Claim 1. $A[p]' \leq \ker(f(\sigma))$.

Proof. Let $\xi \in A[p]'$. Then
$$\psi(f(\sigma)(\xi)) = f(\phi_p)(\psi(\xi)) = 0,$$
so
$$f(\sigma)(\xi) = 0.$$
□

□*Proposition 1*

Now embed $(\bar{\mathbb{Q}}, \sigma)$ into a monster model $(L, \sigma) \models \mathrm{ACFA}$.
From now on, we work in (L, σ), and identify A with $A(L)$.
Let $B := \ker(f(\sigma)) \leq A$, a definable subgroup of A.
We have
$$A[p]' \leq B \leq A.$$

5 Modularity

Proposition 2. *$B \leq A(L)$ is modular:
if $a, b \in B^{<\omega}$ are tuples, then $\mathrm{Cb}(a/b) \subseteq \mathrm{acl}(a)$.*

Proof. Assume for now that f is irreducible in $E^*(A)$.
B is infinite since $A[p]'$ is,
so there exists an SU-rank 1 type $p(x)$ containing $x \in B$.
Suppose p is not modular.
By trichotomy, for some C,
replacing p with a non-forking extension to C,
$p(L) \subseteq \mathrm{acl}(C, k)$ where $k = \mathrm{Fix}(\sigma)$.

Fact (Zilber indecomposability theorem)**.** *For some n, $B' := (p(L)p(L)^{-1})^n$ is a subgroup.*

Hence $B' \subseteq \mathrm{acl}(C, k)$.

Fact. *B' is the intersection of a countable chain of definable subgroups of B.*

Lemma. *Any definable infinite subgroup H of B has finite index in B.*

Proof. By Fact 3(II,IV):
H has finite index in $\ker(g)$ say,
and so $\ker(g) \cap \ker(f)$ has finite index in $\ker(g)$,
so $g|f$ in $E^*(A)$, so by irreducibility of f also $f|g$,
so $\ker(g) \cap \ker(f)$ has finite index in $\ker(f) = B$,
hence so does H. □

So B/B' is profinite, of cardinality $\leq 2^{\aleph_0}$.
Hence, enlarging C by representatives of the cosets of B', we have $B \subseteq \mathrm{acl}(C, k)$.

Fact. *It follows that for some finite normal $K \leq B$,*
$$B/K \subseteq \mathrm{dcl}(C, k).$$

So, since k eliminate imaginaries and is stably embedded,
B/K is definably isomorphic over C to a definable group in the pseudofinite field k.
A **virtual isogeny** between groups G and H is a homomorphism $h : G' \to H'$ where

- G' is a finite index subgroup of G,
- H' is a finite index subgroup of H,
- $\ker(h)$ is finite.

Fact (Hrushovski-Pillay)**.** *Any definable group in k is definably virtually isogenous with a group $H(k)$ where H is an algebraic group over k.*

Let $H(k_1)$ be minimal such that:

- $k_1 \geq k$ is a finite extension of k,
- H is an algebraic group over k_1, and
- there is a definable virtual isogeny h of B with a subgroup of $H(k_1)$.

Fact. *H is an abelian variety.*

Now the graph of h is a definable subgroup of $A \times H$.

Lemma. *An abelian variety over L has only countably many definable subgroups.*

Proof. An abelian variety has only countably many algebraic subgroups.
So by Fact 2, every definable subgroup has finite index in one of countably many definable subgroups.
So STS: a definable subgroup H has only finitely many subgroups H' of index n.
But indeed, $[n] : H \to H$ has finite kernel, so $\mathrm{SU}(nH) = \mathrm{SU}(H)$,
so $[H : nH] < \infty$.
But $nH \leq H'$ since $n(H/H') = 0$,
so H' is a union of cosets of nH. □

Hence h has only finitely many conjugates over k_1.
So say $\tau := \sigma^t$ is a power of σ such that $h^\tau = h$ and $k_1 \subseteq \mathrm{Fix}(\tau)$.
Then for $x \in B$,
$$h(\tau(x)) = \tau(h(x)) = h(x),$$
so
$$\zeta_x := \tau(x) - x \in \ker h.$$

Now $\ker h$ is finite and preserved by τ,
so say N is such that $\tau^N|_{\ker h} = id$,
and say $M \ker h = 0$.
Then for $x \in \mathrm{dom}(h)$,
$$\tau^{NM}(x) - x = \sum_{i<NM} \tau^{i+1}(x) - \tau(x) = \sum_{i<NM} \tau^i(\zeta_x) = M \sum_{i<N} \tau^i(\zeta_x) = 0.$$

Let $n := tNM$.
Then $\mathrm{dom}(h) \leq \ker(f(\sigma)) \cap \ker(\sigma^n - 1)$,
so $\ker(f(\sigma)) \cap \ker(\sigma^n - 1)$ has finite index in $\ker(f(\sigma)) = B$,
so by Fact 3(IV), $f(\sigma)|(\sigma^n - 1)$ in $E^*(A)$,
contradicting f having no cyclotomic factors.
So X is modular.
Hence $B' = (XX^{-1})^n$ is modular.
Hence also B is modular.
Indeed: let C be representatives of the cosets of B' in B;
adding parameters for C, any $a \in B^n$ is interalgebraic with some $a+c \in (B')^n$, so B is modular,
hence B is modular also without C,
since (as in Addick's talk) modularity is preserved by "deleting parameters".
This concludes the case that f is irreducible.
The general case proceeds roughly as follows:
If $f = gh$, then $h(\sigma)$ induces a short exact sequence
$$0 \to \ker(h(\sigma)) \to \ker(f(\sigma)) \to \ker(g(\sigma)) \to 0.$$

Now the CBP can be read as saying:
a finite-rank set B is modular iff it is orthogonal to k,
i.e. $b \perp_E c$ for any $b \in B$, $c \in k$, and small E.
So if $\ker(f(\sigma))$ is non-modular,
then $\ker(f(\sigma))$ is non-orthogonal to k,
hence either $\ker(h(\sigma))$ or $\ker(g(\sigma))$ is non-orthogonal to k and hence non-modular.
So we conclude inductively from the irreducible case.

□*Proposition 2*

6 $V \cap A[p]'$

By an argument analagous to the case of stable 1-based groups [Cha00, Proposition 4.7],
qf-definable subsets of B are boolean combinations of cosets of definable subgroups.
(In fact, by the trichotomy result of Chatzidakis-Hrushovski, B is stable stably embedded,
so any definable subset is a boolean combination of cosets of $\mathrm{acl}^{\mathrm{eq}}(\emptyset)$-definable subgroups.
But I don't know how to obtain this from the jet spaces approach.)
Now let $V \subsetneq A$ be a proper subvariety.
We want to show that $V \cap A[p]'$ is finite.

Fact. *The Zariski closure of a boolean combination of cosets of subgroups of A is a finite union of cosets.*

Let $V' := \overline{V \cap A[p]'}^{\mathrm{Zar}}$.
Then $V' = \overline{V' \cap B}^{\mathrm{Zar}}$ is, by the above, a finite union of cosets of algebraic subgroups.
Since A is simple, those algebraic subgroups are finite,
so V' and hence $V \cap A[p']$ is finite.

7 $V \cap A[\infty]$

Finally, we sketch how to deduce that $V \cap A[\infty]$ is finite,
following an approach of Pillay.

- We may assume that $V \cap A[\infty]$ is dense in V,
hence V is over a number field K.
- Now $A[\infty] = A[p]' + A[p^\infty]$.
- Let $D := \bigcup\{(V - t) \cap A[p]' : t \in A[p^\infty]\}$.
- Then D is finite:
By compactness we obtain a uniform in x bound on $|(V - x) \cap B|$,
hence on $|(V - t) \cap A[p]'|$,
hence on the degree over $K(A[p^\infty])$ of elements of D,
hence (Fact) on the order of elements of D,
hence on $|D|$.
- By considering another prime $p' \neq p$ of good reduction,
$(V - x) \cap A[p^\infty] \subseteq (V - x) \cap A[p']'$ is finite for any $x \in A$.
- If $t + t' \in V \cap A[\infty]$ where $t \in A[p^\infty]$ and $t' \in A[p]'$,
then $t' \in D$,
and so $t \in E := \bigcup_{s\in D}(V - s) \cap A[p^\infty]$,
which is finite.
- So $V \cap A[\infty] \subseteq D + E$ is finite.

References

[Cha00] Zoe Chatzidakis. A survey on the model theory of difference fields. *MSRI Publications*, 2000.