Model theory and diophantine geometry Lectures 3, 4 & 5: A Drinfeld module version of the Mordell-Lang conjecture

Thomas Scanlon

(scanlon@math.berkeley.edu)

Twisted polynomials

Definition 0.1 *Let R be a ring and $\sigma : R \to R$ an endomorphism of R. The ring of twisted polynomials in σ over R is the ring $R\{\sigma\}$ generated by R and the (non-commuting) indeterminate σ subject to the commutation rule $\sigma a = \sigma(a)\sigma$ for $a \in R$.*

There is a natural homomorphism $R\{\sigma\} \to \mathrm{End}(R, +)$ given by sending $a \in R$ to scalar multiplication by a and σ to σ.

Every nonzero element f of $R\{\sigma\}$ may be written uniquely as $\sum_{i=0}^{d} a_i \sigma^i$ for some $d \in \mathbb{N}$, $a_i \in R$ (for $i \leq d$), and $a_d \neq 0$. We define the *degree* of f to be $\deg(f) := d$.

Additive polynomials

Let R be a commutative ring of characteristic $p > 0$. We write the p-power Frobenius morphism $x \mapsto x^p$ as $\tau : R \to R$.

There is a function $\rho : R\{\tau\} \to R[X]$ defined by

$$\sum_{i=0}^{d} a_i \tau^i \to \sum_{i=0}^{d} a_i X^{p^i}$$

Giving the image of ρ a ring structure with addition of polynomials for $+$ and composition of polynomials for $\times$, ρ becomes an isomorphism between $R\{\tau\}$ and its image.

Scheme-theoretically, this ring of additive polynomials over R may be identified with the endomorphism ring of the additive group scheme over R, $\mathrm{End}(\mathbb{G}_{a/R})$.

Drinfeld modules

By way of notation, we write $\mathbf{A} := \mathbb{F}_p[t]$ for the ring of polynomials in one variable over the field of p elements. We write $\mathbf{K} := \mathbb{F}_p(t)$ for the field of fractions of $\mathbf{A}$.

Definition 0.2 *Let K be a field of characteristic $p > 0$. A* Drinfeld module *over K is a homomorphism $\varphi : \mathbf{A} \to K\{\tau\}$ for which* $\deg(\varphi(t)) > 0$*.*

For $a \in \mathbf{A}$ we write φ_a for $\varphi(a)$ thought of as an element of $\mathrm{End}(\mathbb{G}_{a/K})$*.*

$\mathbf{A}$-modules from Drinfeld modules

If $\varphi : \mathbf{A} \to K\{\tau\}$ is a Drinfeld module and L is a K algebra, then φ gives L an $\mathbf{A}$-module structure via $a * x = \varphi_a(x)$ for $a \in \mathbf{A}$ and $x \in L$.

Via the identification of $K\{\tau\}$, φ expresses $\mathbf{A}$ as a subring of $\mathrm{End}(\mathbb{G}_{a/K})$. Via the diagonal action, $\mathbf{A}$ acts on each Cartesian power ${\mathbb{G}_a}^g$ as well.

Definition 0.3 *An algebraic subgroup $G \leq {\mathbb{G}_a}^g$ is an* algebraic $\mathbf{A}$-module *if for every $a \in \mathbf{A}$ we have $\varphi_a G \leq G$.*

Torsion of a Drinfeld module

Definition 0.4 *Let $\varphi : \mathbf{A} \to K\{\tau\}$ be a Drinfeld module and $a \in \mathbf{A}$ an element of $\mathbf{A}$. The a-torsion group is the group scheme $\varphi[a] := \ker \varphi_a$.*

The torsion module is the ind-group scheme $\varphi_{\mathrm{tor}} := \varinjlim_{a \in \mathbf{A}} \varphi[a]$.

As the degree of $\rho(\varphi_a)$ is $p^{\deg \varphi_a}$, the group scheme $\varphi[a]$ is finite of size $p^{\deg \varphi_a}$. If φ_a is separable, then the group $\varphi[a](K^{\mathrm{sep}})$ is a vector space of dimension $\deg \varphi_a$ over $\mathbb{F}_p$.

Characteristic of a Drinfeld module

For any commutative ring R of characteristic p, reduction modulo the two-sided ideal generated by τ gives a natural map $\pi : R\{\tau\} \to R$.

Definition 0.5 *If $\varphi : \mathbf{A} \to K\{\tau\}$ is a Drinfeld module, then we set $\iota := \pi \circ \varphi : \mathbf{A} \to K$.*

We say that φ has generic characteristic *if ι is injective. Otherwise, we say that φ has* finite characteristic.

Denis' Conjecture

Conjecture 0.6 (Denis) *Let $\varphi : \mathbf{A} \to K\{\tau\}$ be a Drinfeld module of generic characteristic. Let $\Gamma \leq K^g$ be an $\mathbf{A}$-submodule with $\dim_{\mathbf{K}}(\Gamma \otimes_{\mathbf{A}} \mathbf{K}) < \infty$. If $X \subseteq {\mathbb{G}_a}^g$ is an algebraic subvariety, then $X(K) \cap \Gamma$ is a finite union of translates of $\mathbf{A}$-submodules of Γ.*

The special case of $\Gamma = \varphi_{\text{tor}}(K^{\text{sep}})^g$ is the analogue of the Manin-Mumford conjecture.

Finite characteristic variant

Definition 0.7 *Let* $\varphi : \mathbf{A} \to K\{\tau\}$ *be a Drinfeld module. The* modular transcendence degree of φ *is the minimum* d *such that there is some field* L *of absolute transcendence degree* d *and a nonzero scalar* $\lambda \in (K^{\text{alg}})^\times$ *such that* $\lambda^{-1}\varphi\lambda : \mathbf{A} \to L\{\tau\}$*.*

Theorem 0.8 *Let* K *be a finitely generated field of characteristic* p*. Let* $\varphi : \mathbf{A} \to K\{\tau\}$ *be a Drinfeld module of finite characteristic and postive modular transcendence degree. If* $\Gamma \leq \mathbb{G}_a{}^g(K^{\text{alg}})$ *is a finitely generated* $\mathbf{A}$*-module and* $X \subseteq \mathbb{G}_a{}^g$ *is any subvariety, then* $X(K^{\text{alg}}) \cap \Gamma$ *is a finite union of cosets of subgroups of* Γ*.*

Generalizations?

In Theorem 0.8 we assert only that $X(K) \cap \Gamma$ is a finite union of cosets of subgroups of Γ, but we do not assert that the subgroups in question are $\mathbf{A}$-modules. A complete version of this theorem should include this extra assertion.

Theorem 0.8 is *not* a special case of Denis' conjecture as we require φ to have finite characteristic. However, the following special case of Denis' conjecture should follow.

Conjecture 0.9 (Function-field Denis-Mordell-Lang) *Let* K *be a field of characteristic* $p > 0$ *and* $\varphi : \mathbf{A} \to K\{\tau\}$ *a Drinfeld module of generic characteristic over* K*. Suppose that* φ *has modular transcendence degree of at least two and that* $\Gamma \leq \mathbb{G}_a{}^g(K)$ *is a finitely generated* $\mathbf{A}$*-module. Then for* $X \subseteq \mathbb{G}_a{}^g$ *an algebraic subvariety of* $\mathbb{G}_a{}^g$*, the set* $X(K) \cap \Gamma$ *is a finite union of cosets of subgroups of* Γ*.*

Reduction to the case of $\varphi_t \in K\{\tau\}\tau$

To say that φ has finite characteristic means that there is some nonzero $s \in \mathbf{A}$ with $\varphi_s \in K\{\tau\}\tau$. Let $\mathbf{A}' := \mathbb{F}_p[s] \subseteq \mathbf{A}$ and $\varphi' := \varphi \restriction_{\mathbf{A}'} : \mathbf{A}' \to K\{\tau\}$. Then, every algebraic $\mathbf{A}$-module is naturally an algebraic $\mathbf{A}'$-module and every finitely generated $\mathbf{A}$-module is a finitely generated $\mathbf{A}'$-module.

Thus, replacing t with s and $\mathbf{A}$ with $\mathbf{A}'$ we may assume that $\varphi_t \in K\{\tau\}\tau$ is inseparable.

Modular groups

Definition 0.10 *Let G be a group definable in some structure and $\Psi \leq G$ an abstract subgroup. We say that Ψ is* (quantifier-free) modular *if for any quantifier free definable subset $X \subseteq G^n$ of some Cartesian power of G there is another set Y which is a finite Boolean combination of cosets of definable subgroups of G^n for which $X \cap \Psi^n = Y \cap \Psi^n$.*

We drop the phrase *quantifier-free* throughout the rest of these lectures.

Modular subgroups of algebraic groups

Theorem 0.8 may be interpreted as saying that every finitely generated **A**-submodule of some power of the additive group of K is modular.

Proposition 0.11 *Let K be a field, G an algebraic group over K, and $\Gamma \leq G(K)$ a subgroup of the K-rational points of G. Then Γ is modular if and only if for every $n \in \mathbb{Z}_+$ and every subvariety $X \subseteq G^n$ the set $X(K) \cap \Gamma^n$ is a finite union of cosets of subgroups of Γ^n.*

Proof: ($\Rightarrow$) Take $X \subseteq G^n$ a subvariety of G^n. By hypothesis, there is a set $Y \subseteq G^n(K)$ which is a finite Boolean combination of quantifier-free cosets of definable subgroups of $G^n(K)$ such that

$X(K) \cap \Gamma^n = Y \cap \Gamma^n$. Write

$$Y = \bigcup_{i=1}^{d} (a_i H_i(K) \setminus (\bigcup_{j=1}^{m_i} b_{i,j} L_{i,j}(K)))$$

where $H_i = H_i^0$ is a connected algebraic subgroup of G^n, $L_{i,j} < H_i$ is a proper algebraic subgroup of H_i, $[H_i(K) : L_{i,j}(K)] \geq \aleph_0$, and $b_{i,j} L_{i,j} \subseteq a_i H_i$. Considering each irreducible subvariety of X separately, one sees that we may assume that $d = 1$ and $a_1 = 1$. Find $h \in H(K)$ such that $h b_j L_j(K) \cap b_\ell L_\ell(K) = \varnothing$ for all i, j.

Then

$$\begin{aligned}
(hX) \cup X &= \overline{h(Y(K) \cap \Gamma^n)} \cup \overline{Y(K) \cap \Gamma^n} \\
&= \overline{(h(Y(K) \cap \Gamma^n)) \cup (Y(K) \cap \Gamma^n)} \\
&= \overline{H(K) \cap \Gamma^n} \\
&= H
\end{aligned}$$

As $H = H^0$, we have $X = H$ or $hX = H$ (which implies that $X = H$).

($\Leftarrow$) Almost immediate.

Modularity is Hereditary

Proposition 0.12 *Let G be a definable group and $\Gamma \leq \Xi \leq G$ subgroups of G. If Ξ is modular, then so is Γ.*

Proof: Immediate

Reduction to $\Gamma = \Xi^g$

Let $\pi_i : {\mathbb{G}_a}^g \to \mathbb{G}_a$ be the i^{th} coordinate projection. Let $\Xi := \sum_{i=1}^{g} \pi_i(\Gamma)$. Then $\Xi \leq \mathbb{G}_a(K)$ is a finitely **A**-module and $\Gamma \leq \Xi^g$.

Compactness and modularity

Proposition 0.13 *Let G be a definable group in some $\aleph_1$-saturated structure. Let $\Gamma \leq G$ be a subgroup. Suppose that $\langle H_n \rangle_{n \in \omega}$ is some descending chain of definable subgroups of G for which $\Gamma/(\Gamma \cap H_n)$ is finite for each n and $H^\sharp := \bigcap H_n$ is modular. Then, Γ is modular.*

Proof: Let $\{X_b\}_{b \in B}$ be a quantifier-free definable family of subsets of G^m. We show that there is a natural number n and quantifier-free definable family $\{Y_c\}_{c \in C}$ of finite Boolean combinations of cosets of definable subgroups of G^m such that for each coset $a(H_n)^m$ of $(H_n)^m$ we have for each $b \in B$ some $c \in C$ with $X_b \cap a(H_n)^m = Y_c \cap a(H_n)^m$.

If this were to fail, then by $\aleph_1$-saturation we could find some $b \in B$ and $a \in G$ such that $X_b \cap a(H^\sharp)^m$ cannot be expressed as

$Y \cap a(H^\sharp)^m$ for any set $Y \subseteq G^m$ which is a finite Boolean combination of cosets of definable subgroups of G^m. Translating by a^{-1}, this contradicts modularity of $H^\sharp$.

Covering Γ by finitely many cosets of $(H_n)^m$, we finish the proof.

$\varphi^\sharp$

Let $L \succeq K^{\text{sep}}$ be an $\aleph_1$-saturated elementary extension of K^{sep}. We set $\varphi^\sharp := \varphi^\sharp(L) := \bigcap_{n \geq 0} \varphi_{t^n}(L)$.

Theorem 0.8 then follows from the assertions

- $\Gamma/(\Gamma \cap \varphi_{t^n}(L))$ is finite for each $n \in \mathbb{Z}_+$
- $\varphi^\sharp$ is modular

Γ lies in finitely many cosets of $\varphi_{t^n}(L)$

Proof: As $L \geq K^{\text{sep}} \geq K \geq \Gamma$, we have $\varphi_{t^n}(L) \geq \varphi_{t^n}(\Gamma)$. Thus, $|\Gamma/(\Gamma \cap \varphi_{t^n}(L))| \leq |\Gamma/\varphi_{t^n}(\Gamma)|$. As Γ is a finitely generate $\mathbf{A}$-module, the module $\Gamma/\varphi_{t^n}(\Gamma)$ is a finitely generated $\mathbf{A}/t^n\mathbf{A}$-module and therefore a finite set.

Zilber dichotomy for separably closed fields

Definition 0.14 *An ∞-definable group G in some sufficiently saturated structure is* c-minimal *if whenever $H < G$ is a definable subgroup of infinite index, then H is finite.*

Theorem 0.15 (Bouscaren-Delon) *Let G be a c-minimal ∞-definable group in an $\aleph_1$-saturated separably closed field L of finite imperfection degree ($[L : L^p] < \aleph_0$). Let $k := \bigcap_{n \geq 0} L^{p^n}$. If G is not modular, then there is an algebraic group H over k and a surjective definable homomorphism $\psi : G \to H(k)$.*

Definable sets in separably closed fields

Let $L = L^{\text{sep}}$ be a separably closed field of characteristic p with $[L : L^p] = p^e$ finite. Fix a basis $B \subseteq L$ of L over L^p. Then with these with this basis named, we have definable functions $\lambda_b : L \to L$ defined by the equation

$$x = \sum_{b \in B} \lambda_b(x)^p b$$

Theorem 0.16 *The theory of L eliminates quantifiers in the language $\mathcal{L}(+, \times, 0, 1, \{b : b \in B\}, \{\lambda_b : b \in B\})$.*

For any finite sequence $\vec{b} = \langle b_1, \ldots, b_n \rangle \in {}^{<\omega}B$ we write $\lambda_{\vec{b}} := \lambda_{b_n} \circ \cdots \circ \lambda_{b_1}$ and $\vec{b}^* := \prod_{i=1}^n b_i^{p^{i-1}}$.

$\varphi^\sharp$ is c-minimal

An analogous calculation occurs in Hrushovski's proof of the function field Mordell-Lang conjecture.

Using the quantifier elimination theorem, it suffices to show that for any $x \in \varphi^\sharp(L)$ (as L ranges over elementary extensions of K^{sep}) the field $K(\{\lambda_{\vec{b}}(x)\}_{\vec{b} \in {}^{<\omega}B})$ has transcendence degree at most one over K. For this it suffices to consider $\vec{b}$ of length N (for each $N \in \omega$).

Write $x = \varphi_{t^N}(y)$. As φ_t is inseparable, we may write $\varphi_{t^N} = \psi \tau^N$ for some $\psi \in K\{\tau\}$. Write $\psi = \sum_{\vec{b} \in B^N} \vec{b}^* \psi_{\vec{b}}$ for some $\psi_{\vec{b}} \in K^{p^N}\{\tau\}$.

Note that $\psi_{\vec{b}} \tau^N(y) \in L^{p^N}$.

Thus, $\lambda_{\vec{b}}(x) = y \sqrt[p^N]{\psi_{\vec{b}}(y)} \in K(y)$.

$\varphi^\sharp$ non-modular $\Rightarrow \lambda^{-1}\varphi_t\lambda \in L^p\{\tau\}$ for some $\lambda \in L^\times$

This is Lemme 3.4.28 of Thomas Blossier's thesis and is proved via a calculation involving λ-functions.

$\varphi^\sharp$ is modular

Proof: Iterating Blossier's Lemma and using the saturation of L, we find $\lambda \in L^\times$ such that $\lambda^{-1}\varphi_t\lambda \in L^{p^\infty}\{\tau\}$.

From a theorem of A. Robinson it follows that $(K^{\text{alg}}, \mathbb{F}_p^{\text{alg}}) \preceq (L^{\text{alg}}, L^{p^\infty})$. Thus, there is some $\lambda \in (K^{\text{alg}})^\times$ such that $\lambda^{-1}\varphi_t\lambda \in \mathbb{F}_p^{\text{alg}}\{\tau\}$.

So, $\lambda^{p^d-1}a_d \in (\mathbb{F}_p^{\text{alg}})^\times$ implying that actually $\lambda \in K^{\text{sep}}$ showing that φ has modular transcendence degree zero.

Conclusion for Drinfeld Mordell-Lang

Thus, $\varphi^\sharp$ is modular so that Γ is also modular.

Can we conclude that if $G \leq {\mathbb{G}_a}^g$ is a connected algebraic subgroup of ${\mathbb{G}_a}^g$ for which $G(K) \cap \Gamma$ is Zariski dense, then G is an algebraic $\mathbf{A}$-module? This should be true and it should be related to a recent result of Dragos Ghioca that every point in $\varphi^\sharp(K^{\text{sep}})$ is torsion.

Drinfeld Manin-Mumford

Theorem 0.17 *Let $K = K^{\text{alg}}$ be a field of characteristic $p > 0$ and $\varphi : \mathbf{A} \to K\{\tau\}$ a Drinfeld module of generic characteristic. If $X \subseteq {\mathbb{G}_a}^g$ be a closed subvariety of a power of the additive group. Then $X(K) \cap \varphi_{\text{tor}}(K)^g$ is a finite union of cosets of $\mathbf{A}$-modules.*

Difference equations to capture the torsion

As in the case of abelian varieties over number fields, it is a routine matter to find a polynomial $P(X) \in \mathbf{A}[X]$ and an automorphism σ such that $P(\sigma)$ vanishes on "most" of the torsion (precisely the $\mathfrak{p}$-prime torsion for some prime ideal $\mathfrak{p} \subseteq \mathbf{A}$ where $x \in \varphi(K)_{\mathrm{tor}}$ is $\mathfrak{p}$-prime torsion if $\mathrm{ann}_{\mathbf{A}}(x) + \mathfrak{p} = \mathbf{A}$).

The polynomial P is obtained as the minimal polynomial of a Frobenius on a reduction of φ and σ is a relative Frobenius.

Patching two such equations coming from two different (appropriately chosen primes) we may find a single difference polynomial vanishing on all the torsion.

Zilber dichotomy for ACFA

Theorem 0.18 (Chatzidakis-Hrushovski-Peterzil) *Let* $(K,\sigma) \models \mathrm{ACFA}$ *be an existentially closed difference field of characteristic* p. *Let* G *be a commutative algebraic group over* K *and* $\Gamma \leq G(K)$ *a c-minimal definable subgroup. Then, either* Γ *is modular or there there integers* $n, m \in \mathbb{Z}$ *with either* $m = 0$ *and* $n = 1$ *or* $m \neq 0$ *and* $(n, m) = 1$, *and an algbraic group* H *over* $k := \mathrm{Fix}(\sigma^n \tau^m)$ *and a definable infinite subgroup* $\Upsilon \leq H(k) \times \Gamma$ *for which the projections in each direction have finite kernel and image of finite index.*

Modularity of $\ker P(\sigma)$

After analyzing the splitting of $P(X)$ over $\mathbf{K}^{\text{alg}}$, one shows that if $\ker P(\sigma)$ were not modular, then it must contain a c-minimal non-modular group.

In this case, it would mean that there is a fixed field $k = \text{Fix}(\sigma^n \tau^m)$ and additive maps $\alpha, \beta \in \mathfrak{U}\{\tau\}$ such that $\alpha(\mathbb{G}_a(k)) \cap \beta(\ker P(\sigma))$ is infinite.

From this we find that in the division ring of quotients of $\mathfrak{U}\{\tau\}$ P have specific roots whose sizes contradict the Weil conjectures for Drinfeld modules.

From groups to A-modules

We show that every definable subgroup of $\ker P(\sigma)^n$ is commensurable with an **A**-module.

- Case $n = 1$ follows from Galois theory
- Case $n = 2$ uses nonarchimedian analysis
- Case $n > 2$ is proved by induction using the dimension theory of supersimple theories

Questions

- Can one show that every definable subgroup of some power of $\varphi^\sharp$ is an $\mathbf{A}$-module?
- Are there proofs along the lines of Pillay's proof of Manin-Mumford for these theorems?