MORDELL-LANG CONJECTURE

C. Berthet, C. Milliet

Abstract : These are notes of a series of talks by Rahim Moosa given in Berlin, September 2007, during a MODNET training workshop on the Model Theory of Fields.

1 The Mordell-Lang Conjecture

One is interested in finding the rational solutions to the equation $P(x, y) = 0$ where $P \in \mathbf{Q}[X, Y]$. For example, starting with the polynomial $xy - y^3 + x^2 + 2 = 0$, we pass to the homogeneous variables $\underline{x}, \underline{y}, \underline{z}$, and consider the projective curve $C \subset \mathbf{P}^2$ over $\mathbf{Q}$ given by $\underline{x}\underline{y}\underline{z} - \underline{y}^3 + \underline{x}^2\underline{z} + 2\underline{z}^3 = 0$.

What does the set of rational points $C(\mathbf{Q})$ look like? The principle is there should be only finitely many such rational points on C unless there is a good reason.

Examples of good reasons.

. *if* $C = \mathbf{P}^1$ *(the genus of* C *is* 0*), then* $C(\mathbf{Q})$ *is infinite.*

. *there may be a concrete way to produce new rational points from a given one. For example if there is a group law* $+ : C \times C \longrightarrow C$ *given by a rational morphism over* $\mathbf{Q}$*. (elliptic curves of genus* 1*)*

In fact, Mordell's Conjecture says that these are the only possible good reasons :

Mordell's Conjecture (*MC***).** *If* C *is a projective curve over* $\mathbf{Q}$ *with Genus*$(C) \geq 1$*, then* $C(\mathbf{Q})$ *is finite.*

It was proved by Faltings in 1983, not just for $\mathbf{Q}$ but for any finite extension K over $\mathbf{Q}$. Let us work towards a reformulation of this theorem in such a way as to allow generalization in higher dimensions.

Fact. *Every projective curve* C *of genus strictly greater than* 0 *embedds in an abelian variety* $J(C)$ *called the Jacobian of* C*.*

Definition. *An abelian variety is a connected algebraic group (i.e. a projective variety* V *together with a group operation* $+ : V \times V \longrightarrow V$ *given by polynomials) whose underlying variety is projective.*

Note.

. *these groups are abelian (fact)*

. *the dimension of the Jacobian is the genus of the curve (an elliptic curve is a one dimensional abelian variety)*

. *if* C *is over* K*, then* $Jac(C)$ *is over* K*.*

We can always view our curves as embedded in their Jacobians (by curve, we mean a smooth projective curve). So if C is a curve over a number field K, then

$$C(K) = C(\mathbf{Q}) \cap Jac(C)(K)$$

$$(geometric\ object \cap arithmetic\ object)$$

Mordell's Conjecture says that if $Genus(C) \geq 2$, then this intersection is finite.

Reformulated Mordell's Conjecture (*RMC***).** *Suppose A is an abelian variety over a number field K and $C \subset A$ is a curve over K. Then $C(\mathbf{Q}) \cap A(K)$ is a finite union of translates of subgroups of $A(K)$.*

This is equivalent to the Mordell Conjecture, but let us just see why

***Proposition* 1.** *RMC implies MC.*

Proof. Assume that C is irreducible, and suppose that $C(K)$ is infinite. Then it is a Zariski dense set, and $\overline{C(K)} = C$. RMC says $C(K)$ is a finite union $\bigcup a_i + G_i$ with $G_i \leq A(K)$. Then $C = \overline{C(K)} = a_i + \overline{G_i}$ for some i.

Fact. *The Zariski closure in A of a subgroup is an algebraic subgroup.*

So C has an algebraic group structure, and $Genus(C) = 1$. □

Natural generalizations.

- *Replace C with any subvariety of A. (generalize the geometric object)*
- *Generalize the arithmetic object (Mordell-Weil : $A(K)$ is a finitely generated group) Can we replace $A(K)$ with any finitely generated subgroup of $A(\mathbf{C})$? Or even finite rank subgroup of $A(\mathbf{C})$? Given $\Lambda \leq A(\mathbf{C})$, set $div(\Lambda) = \{g \in A(\mathbf{C}) : ng \in \Lambda \text{ for some } n > 0\}$. Λ has finite rank if $\Lambda \leq div(\Lambda')$ for some finitely generated Λ'. Example : $Tor(A) = \{g \in A(\mathbf{C}) : ng = 0 \text{ for some } n\} = div(0)$ is of finite rank but is not finitely generated.*
- *We can also generalize the ambiant algebraic group. Chevalley's theorem : Let S be a connected algebraic subgroup over $\mathbf{C}$. Then there is a unique maximal normal linear algebraic subgroup $L \leq S$ such that S/L is an abelian variety.*

  Definition. *An algebraic group S admitting an exact sequence $0 \to L \to S \to A \to 0$ where A is an abelian variety and $L = (G_m^{\times})^l$ (a power of the multiplicative group) is called a semiabelian variety.*

  Fact. *Semiabelian varieties are commutative.*

  Replace A by a semiabelian variety.

Absolute Mordell-Lang Conjecture in characteristic zero. *Let S be a semiabelian variety over $\mathbf{C}$, $X \subset S$ a subvariety, and $\Gamma \leq S(\mathbf{C})$ some finite rank subgroup. Then $X(\mathbf{C}) \cap \Gamma$ is a finite union of translates of subgroups of Γ.*

Interpretation. *The trace of the ambient geometry on* Γ *is not very rich.*

***Proposition* 2.** *This is false in characteristic* $p > 0$*.*

Proof. Let F be an algebraically closed field of characteristic $p > 0$ with $F \neq \mathbf{F}_p^{alg}$, and C any curve over $\mathbf{F}_p$ of genus $g > 1$. Take $t \in C(F) \setminus C(\mathbf{F}_p^{alg})$, and set $K = \mathbf{F}_p(t)$, $A = Jac(C)$. It has been shown by Lang-Néron that $A(K)$ is a finitely generated group. Mordell would say that $C(K) = C(F) \cap A(K)$ is finite. But $t \in C(K)$, and, for all $n \geq 0$, $Fr^n(t) \in C(K)$, where $Fr : F \longrightarrow F$, $x \mapsto x^p$ (Since A and C are over $\mathbf{F}_p$, Fr acts on A and C). Since $t \notin C(\mathbf{F}_p^{alg})$, these points are all distinct. So $C(K)$ is infinite. □

The point is that in characteristic $p > 0$, there is another good reason for having infinitely many points.

Let S be a semiabelian variety over an algebraically closed field F (in any characteristic). Let $k \subset F$ be an algebraically closed subfield, $X \subset S$ a subvariety over F. X is $k-$special if $X = c + h^{-1}(X_0)$ where $h : S' \to S_0$ is a surjective rational homomorphism between an albegraic subgroup $S' \leq S$ and a semiabelian variety S_0 over k, $X_0 \subset S_0$ is a subvariety over k, $c \in S(F)$.

Example. *Any translate of an algebraic subgroup of S over F.*

Relative Mordell Lang Conjecture (*RML***).** *Let S be a semiabelian variety over an algebraically closed field F,* $X \subset S$ *a subvariety over F,* $\Gamma' \leq S(F)$ *a finitely generated group,* $\Gamma \leq div_p(\Gamma)$*, where* $div_0(\Gamma) = div(\Gamma)$ *and* $div_p(\Gamma) = \{g \in S(F) : ng \in \Gamma$ *with* $n \nmid p\}$ *if* $p > 0$*. Then* $X(F) \cap \Gamma = \bigcup_{i=1}^{l} X_i(F) \cap \Gamma$*, where* $X_i \subset X$ *are* $\mathbf{F}^{alg}-$*special, and* $\mathbf{F}$ *is the prime field of F.*

Remarks.

. *Conclusion is weaker than conclusion of the absolute Mordell Lang Conjecture in characteristic zero. If the* X_i*'s are translates of an algebraic subgroup, then* $X_i(F) \cap \Gamma$ *will be a finite union of translates of subgroups of* Γ*.*

. *Consider the special case where S has* $\mathbf{F}^{alg}-$*trace* 0 *: no algebraic subgroups have infinite homomorphic image defined over* $\mathbf{F}^{alg}$*. Then* $\mathbf{F}^{alg}-$*special means translate of an algebraic subgroup of S. So in this case, RML is exactly the same statement as AML but in all characteristic.*

. *Consider the opposite special case, where S is over* $\mathbf{F}^{alg}$*. Then* $\mathbf{F}^{alg}-$*special means translate of a subvariety over* $\mathbf{F}^{alg}$*. In this case the theorem doesn't tell much except that we may assume X is over* $\mathbf{F}^{alg}$ *as well.*

2 The Dichotomy in Hasse closed fields

We write HCF for the model completion of Hasse fields, HCF_0 if the characteristic is 0 (it is a complete theory) and HCF_p if the characteristic is $p > 0$ (complete theory ; note that if $L \models HCF_p$, then L is separably closed, and we write $C_\infty = \bigcap_n L^{p^n} = L^{p^\infty}$ the set af absolute constants). We will work in a sufficiently saturated model of HCF. Note that in characteristic 0, HCF_0 is just DCF_0, and $C_\infty = \{x \in L : \partial x = 0\}$.

Definition. *A type-definable set X is a subset of $L^{\times n}$, for some $n \geq 0$ defined by a partial type over strictly less than card(L) parameters.*

Definition. *A definable set of a type definable set X is a set of the form $X \cap D$ where $D \subset L^{\times n}$ is definable (with parameters).*

Definition. *A minimal set is a type-definable set all of whose definable subsets are finite or co-finite.*

Equivalently, X is minimal over A if for any $B \supset A$, X has a unique non-algebraic type over B, the generic extension. If X is minimal, for all $A \subset B \subset C$ and $a \in X$, we have $a \not\perp_B C \iff a \in acl(C) \setminus acl(B)$.

Constants

Set $k = C_\infty$ the set of absolute constants. (in characteristic 0, $k = \{x \in L : \partial x = 0\}$, in characteristic $p > 0$, $k = \bigcap_n L^{p^n} = L^{p^\infty}$).

Fact. . *k is a type-definable set.*

. *k is an algebraically closed field.*

. *k is a stably embedded pure algebraicaly closed field, ie every definable subset of $k^{\times n}$ for all $n \geq 0$ is definable in $(k, \times, +, 0, 1)$.*

. *In particular, it is a minimal set.*

Definition. *Let X be a type-definable set over parameters $A \subset L$. X is one-based if for all $a \in dcl(C \cup A)$ and any set $B \supset A$ with $acl(B) = B$, $Cb(a/B) \subset acl(aA)$.*

Example. *k is not one-based. For minimal sets, one has one-based $\iff$ locally modular $\iff$ linear.*

Definition. *Given type-definable sets X, Y, we say that X is fully orthogonal to Y if for any $a \in X$, $b \in Y$ and parameters A over which X and Y are defined, $a \perp_A b$. This is denoted $X \perp Y$.*

Exercises.

. *$X \perp Y \iff$ for any set $A = acl(A)$ over which X, Y are defined, and any $a \in X$, $b \in Y$, $tp(a/A) \cup tp(b/A) \vdash tp(ab/A)$.*

. *if $X \perp Y$, then $X \perp Y^{\times n}$ for all $n > 0$.*

Dichotomy theorem (for HCF). *Every minimal set is either one-based or not fully orthogonal to k.*

AMC in char. 0 is true ; there is no model theoretical proof.
RMC in char. 0 is true (weaker than AMC_0). There is a model th. proof.
AMC in char. $p > 0$ is false.
RMC in char. $p > 0$ is true. There is only a model theoretical proof.

3 The case where X is not fully orthogonal to k

Let X be a minimal set. Recall that X not fully orthogonal to k means there is some B over which X is defined, $a \in X$, $c \in k$ such that $a \not\perp_B c$. As X is minimal, this implies $a \in acl(Bc) \setminus acl(B)$.

***Lemma* 3.** *Let X be a minimal set. If X is not fully orthogonal to k, there exists B over which X is defined and a $B-$definable function with finite fibres $f : X \setminus acl(B) \longrightarrow k^{\times n}$.*

Proof. Let be B over which X is defined, $a \in X$, $c \in k$, $a \in acl(Bc) \setminus acl(B)$, and $p(x) = tp(a/B)$. Let $\theta(x, y)$ be such that θ is over B, $\models \theta(a, c)$, and $| \theta(x, c) | \leq l \in \mathbb{N}$. $(y \in k) \cap \theta(a, y)$ defines a type definable subset $C_a \subset k$ over Ba. So C_a is definable in $(k, +, \times, 0, 1)$, and by elimination of imaginaries in $(k, +, \times, 0, 1)$, there is a code $\bar{c} \in k^{\times n}$ such that $\alpha(\bar{c}) = \bar{c} \iff \alpha(C_a) = C_a$ for any automorphism α, so $\bar{c} \in dcl(Ba)$.

Claim. *$a \in acl(B\bar{c})$.*

proof of Claim. assume $a_0, ..., a_l \models tp(a/B\bar{c})$. So we have automorphisms $\alpha_i(a) = a_i$ fixing $B\bar{c}$. So $C_{a_i} = C_{\alpha_i(a)} = \alpha(C_a) = C_a$. But $c \in C_a$, so $c \in C_{a_i}$, $\models \theta(a_i, c)$ for all i and $a_i = a_j$ for some $i \neq j$. □

So there is a definable function with finite fibres f over B such that $f(a) = \bar{c}$. □

***Lemma* 4.** *Let H be a minimal type-definable group. If H is not fully orthogonal to k, then there exists a group G definable in $(k, +, \times, 0, 1)$ and a definable surjective homomorphism $h : H \longrightarrow G$ with finite kernel.*

Proof. Let B such that H is over B, $f : H \setminus acl(B) \to k^{\times n}$ $B-$definable with finite fibres.

step1: f extends to all of H. $D := dom(f) \cap H = H \subset H$. $f : D \to L^{\times n}$ with $f(D \setminus acl(B)) \subset k^{\times n}$. $D \subset H$ is cofinite so we can extend $f : H \longrightarrow L^{\times n}$ such that f is $B-$definable with finite fibres and $f(H \setminus acl(B)) \subset k^{\times n}$.

step2: get image of f a group. Set

$$N = \{h \in H : \text{for some (eq. for all) } a \in H \setminus acl(Bh),\ f(a + h) = f(a)\}$$

Claim. *N is a finite subgroup of H.*

proof of Claim. $h, h' \in N$. Choose $a \in H \setminus acl(Bhh')$ then $a + h' \notin acl(Bh)$. $f(a + h' + h) = f(a + h') = f(a)$; also $a \notin acl(B \cup \{h + h'\})$, so $h + h' \in N$. N is finite since if $h_1, ..., h_l \in N$, choose $a \in H \setminus acl(Bh_1...h_l)$. We have $f(a+h_1) = f(a+h_2) = ... = f(a)$, so the $a + h_i$'s are in the same fibre of f, which is finite. □

Fix a_0, a_1, a_2 independant generic elements of H. Set $\bar{f} : H \to (L^{\times n})^{\times 3}, h \mapsto (f(h + a_0), f(h + a_1), f(h + a_2))$.

Claim. *$h, h' \in H$. If $\bar{f}(h) = \bar{f}(h')$, then $h - h' \in N$.*

proof of Claim. choose some $a_i \notin acl(Bhh')$. So $a_i + h \notin acl(B \cup \{h' - h\})$, and $f((a_i + h) + (h' - h)) = f(a_i + h')$. So $f(a_i + h) = f(a_i + h')$, and $h' - h \in N$. □

Define g on H by $g(h) = Cb(\{\bar{f}(h+d) : d \in N\})$. $g : H \to L^{\times n}$ is definable over Ba_0, a_1a_2.

Claim. *$g(h) = g(h') \iff h - h' \in N$*

g induces a definable bijection between $g(H) = G_1$ and H/N ($g(h) \mapsto h \bmod N$). $g : H \to G_1$ is a surjective $Ba_0a_1a_2$−definable homomorphism.

Claim. *If $a \in G_1 \setminus acl(Ba_0, a_1, a_2)$, then $a \in k^{\times n}$*

Set $B' = Ba_0a_1a_2$.

Claim. *$G = (G_1 \setminus acl(B')) \times (G_1 \setminus acl(B'))/R$ where $(x, y)R(x', y') \iff x + y = x' + y'$. Then G is definable in $(k, +, \times, 0, 1)$, and there is a bijection $G_1 \to G$.*

□

4 Non full orthogonality to k in semiabelian varieties

Let S be a semiabelian variety over L. Let $H \leq S(L)$ a minimal, type-definable subgroup. One has $H \leq S(L) \leq S(L^{alg})$. Let $\overline{H}$ be the Zariski closure of H in $S(L^{alg})$: $\overline{H}$ is an algebraic subgroup of S over L.

Proposition 5. *If $H \not\perp k$, then there exists a semiabelian variety S_0 over k and a bijective rational homomorphism $g : \overline{H} \to S_0$ over L, such that $g|_H : H \to S_0(k)$ is a bijection.*

Proof. From lemma 4, let $h : H \twoheadrightarrow G$ be a surjective group homomorphism, where G is a group definable in $(k, +, \times, 0, 1)$; h is definable and has finite kernel. Set $f : G \to H$, as follows. Given $x \in G$, choose $y \in H$, s.t. $h(y) = x$, and put $f(x) = ny$, where $n = \sharp Ker(h)$. h is well defined : if also $h(y') = x$, then $h(y') = h(y)$, so $y' - y \in Ker(h)$ and $ny = ny'$.

Fact. *For all m, there is only finitely many m-torsion points in any semiabelian variety.*

So $f : G \to H$ has finite kernel. f is surjective, as $n : H \to H$ is surjective since it has a finite kernel by the fact and H is minimal ($f : G \twoheadrightarrow H$) : this induces a definable bijection $f_1 : G/Ker(f) \to H$, where $G_1 := G/Ker(f)$ is a group definable in $(k, +, \times, 0, 1)$. So up to definable isomorphism, $G_1 = T(k)$, where T is an algebraic group over k. The map $f_1 : T(k) \to H$ is a bijective p-rational homomorphism. It extends to

$$\begin{array}{ccc} T(L^{alg}) & \xrightarrow{f_2} & \overline{H} \\ \uparrow \leq & & \uparrow \leq \\ T(k) & \xrightarrow{f_1} & H \end{array}$$

(one can extend f_1 to the Zariski closure of $T(k)$, which is $T(L^{alg})$ because T is definable over k). f_2 is p-rational, surjective; f_2 is a homomorphism (exercise) since it is so on a Zariski dense set. Note that $Ker(f_2)(k) = Ker(f_1)(k)$.

Claim. *$Ker(f_2)$ is defined over k.*

proof of Claim. We use the following fact.

Fact. *Every commutative algebraic group over k has a smallest algebraic subgroup such that the quotient is a semiabelian variety. This algebraic subgroup is definable over k.*

Take $M \leq T$ be such for T. $\overline{H}$ is a semiabelian variety so $M \leq Ker(f_2)$, hence $M(k) \leq Ker(f_2)(k) = 0$, from where we get $M = 0$ (as M is over k and so its k-points are dense). This shows that T is a semiabelian variety.

Fact. *Every algebraic subgroup of a semiabelian variety over k is itself over k.*

From this fact we get that $Ker(f_2)$ is over k. □

Since $Ker(f_2)(k) = 0$, $Ker(f_2) = 0$ and $f_2 : T \to \overline{H}$ is a bijective p-rational homomorphism, so we have

$$\begin{array}{ccc} \overline{H} & \xrightarrow{f_2^{-1}} & T \\ & {\scriptstyle g}\searrow & \uparrow {\scriptstyle Fr^{-n}} \\ & & T^{(p^n)} \end{array} \qquad\qquad \begin{array}{ccc} \overline{H} & \xrightarrow{f_2^{-1}} & T \\ & {\scriptstyle g}\searrow & \downarrow {\scriptstyle Fr^{n}} \\ & & T^{(p^n)} \end{array}$$

as g is a bijective rational homomorphism over L, and $T^{(p^n)}$ is still in k. Let $S_0 = T^{(p^n)}$: one has $g(H) = Fr^n f_2^{-1}(H) = Fr^n(f_1^{-1}(H)) = Fr^n(T(k)) = T^{(p^n)} = S_0(k)$. □

Definition. *A type-definable set Y is semiminimal if there exists some finite set F and some minimal set X such that $Y \subset acl(F \cup X)$. In this case, $RM(Y)$ is finite.*

***Proposition* 6.** *Let S be a semiabelian variety over L, $H \leq S(L)$ a connected semiminimal type-definable subgroup, and $\overline{H}$ the Zariski closure oh H. If $H \not\perp k$, then there exists a semiabelian variety S_0 over k and a bijective rational homomorphism $g : \overline{H} \to S_0$ such that $g(H) = S_0(k)$.*

***Corollary* 7.** *(Mordell-Lang for non one-based semiminimal groups) Let S be a semiabelian variety over L, and $H \leq S(L)$ a connected semiminimal type-definable subgroup. If $H \not\perp k$, then for every subvariety $X \subset S$ over L, $X(L) \cap H = \bigcup_{i=1}^{n} X_i(L) \cap H$, where the X_i are k-special subvarieties of X.*

proof. We make some reductions :

. Replacing X by the Zariski closure of $X(L) \cap H$, we may assume that $X(L) \cap H = X$.

. Replacing X by an irreducible component, we may assume that X is irreducible.

Now we will prove that X itself is k-special. By Proposition 6, we have $g : \overline{H} \to S_0/k$ and $g(H) = S_0(k)$. Let $X_0 := \overline{g(X(L) \cap H)}$. Since $g(X(k) \cap H) \subset S_0(k)$, X_0 is over k. Furthermore, $X(L) \cap H \subset g^{-1}(X_0)$ and then $X = \overline{X(L) \cap H} \subset g^{-1}(X_0)$. As g is bijective, $g(X) \supset X_0$, therefore $g(X) = X_0$ and $g^{-1}(X_0) = X$, so X is k-special. □

5 The Relative Mordell-Lang Conjecture for semipluriminimal subgroups of semiabelian varieties

Definition. *A type-definable set Y is semipluriminimal if there exists a finite set F and minimal sets $X_1, \ldots, X_l$ such that $Y \subset acl(F \cup X_1 \cup \ldots \cup X_l)$. Such a set is of finite Morely rank as a set of solutions.*

Fact. *If H is a connected semipluriminimal type-definable group, then $H = H_1 + H_2 + \ldots + H_l$ where the h_i are connected semiminimal definable subgroups pairwise fully orthogonal : $H_i \perp H_j$, $i \neq j$.*

Fact. *If H is a one-based group, type-definable over $A = acl(A)$ and if $p(x) \in S(B)$ is a complete type in H over $B = acl(B) \supset A$, recall $stab(p) = \{h \in H : h + \mathbf{p} = \mathbf{p}\}$ (where $\mathbf{p}$ is the unique global non forking extension of p to L). Then this $stab(p)$ is itself a type-definable subgroup of H over A, and p is the generic type of a B-definable translate of $stab(p)$.*

Remark. *This is used to prove that in a one-based group, every definable subset of $H^{\times n}$ is a finite boolean combination of translates of definable subgroups; in fact of A-definable subgroups. This characterizes one-based groups.*

Theorem 8. *(Mordell-Lang for semipluriminimal subgroups) Let S be a semiabelian variety over L, $H \leq S(L)$ a connected semipluriminimal type-definable subgroup and $X \subset S$ a subvariety, definable over L. Then $X(L) \cap H = \bigcup_{i=1}^{l} X_i(L) \cap H$, where $X_1, \ldots, X_l$ are k-special.*

proof. As before, we may assume that X is irreducible and $\overline{X(L) \cap H} = X$. We have to show that X is k-special. For the reduction, let $stab(X) = \{a \in S : a + X = X\}$, an algebraic subgroup. Working modulo $stab(X)$), we may assume $stab(X) = 0$ (exercise).
Exercise : there exists a complete type p in $X(L) \cap H$ whose set of solutions is Zariski dense in X (by irreducibility of X and $\overline{X(L) \cap H} = X$). Choose a complete type p over some $A = acl(A)$ over which S, X, H are defined, such that $Y = p^L$ is Zariski dense in X and Y has minimal (RM, dM) with this property. $Y \subset X(L) \cap H$.

Claim. *stab(p)=0.*

proof of Claim. Let $h \in stab(p)$: Y and $h+Y$ have a common nonforking extension, so $RM((h + Y) \cap Y) = RM(Y)$, hence $RM((h + X(L) \cap H) \cap Y) = RM(Y)$, therefore $(RM, dM)(Y - (h + X(L) \cap H)) < (RM, dM)(Y)$ and $Y - (h + X(L) \cap H)$ cannot be Zariski dense in X. By minimal choice of Y, $\overline{Y \cap (h + X(L) \cap H)} = X$, $h + X = X$, and $h \in stab(X) = 0$, whereby $stab(p) = 0$. □

Note. *H is not one-based : if it were, then p would be the generic type of a translate of $stab(p)$ (if p was algebraic, then as $\overline{Y} = X$, X would be a point and then X would be k-special, so assuming p is not algebraic implies that H is not one-based).*

By the fact one has $H = H_1 + \ldots + H_l$, where the H_i are minimal and $H_i \perp H_j$ for all $i \neq j$. If H_i and H_j are not one-based, then by the dichotomy they are not fully orthogonal to k, so by lemma 4 each one is definably isomorphic to a group definable in $(k, +, \times, 0, 1)$, hence $H_i \not\perp H_j$, and then $i = j$, so there is at most one H_i that is not one-based (Exercise : the sum of fully orthogonal one-based subgroups is one-based). Thus exactly one of the H_i's is not one-based (since H is not based), say the last one, H_l. Let $B := H_1 + \dots H_{l-1}$. B is one-based, H_l is not. Since $H = B + H_l$ and $B \perp Hl$, $Y = p(x)^L = U + V$ where $U \subset B$, $V \subset H_l$ are solution sets to complete types $q_1 \in B$, $q_2 \in H_l$ (exercise : follows from the definition of $\perp$: if $p(x) = tp(b + h/A)$ then $q_1 = tp(b/A)$, $q_2 = tp(h/A)$). As B is one-based, q_1 is the generic type of a translate of $stab(q_1) \subset stab(p)$ so U is a singleton and then Y is a translate of V. Translating the situation, we may assume $Y = V \subset H_l$ (being k-special is preserved under translation). We have $\overline{Y} = X$ so $\overline{X(L) \cap H_l} = X$, but $H_l \not\perp k$, so by corollary 7, $X(L) \cap H_l = \bigcup_{i=1}^{s} X_i(L) \cap H_l$ where $X_1, \dots, X_s$ are special subvarieties of X. Taking Zariski closures of both sides, one gets $\overline{X} \subset \overline{\bigcup_{i=1}^{s} X_i} \subset X$, hence $X = \bigcup_{i=1}^{s} X_i$, so $X = X_i$ (as X is irreducible), which is k-special. □

Now we replace "semipluriminimality" by "finite Morley-rankedness".

Theorem 9. *(Mordell-Lang for subgroups of finite Morley rank) Let S be a semiabelian variety over L, H a finite Morley rank type-definable subgroup of $S(L)$ and $X \subset S$ a subvariety, definable over L. Then $X(L) \cap H = \bigcup_{i=1}^{l} X_i(L) \cap H$, where $X_1, \dots, X_l$ are k-special.*

proof. This theorem is a big step and the point is that semipluriminimality implies arbitrary finite rankedness. □

Now we turn to the proof of the Relative Mordell-Lang Conjecture in characteristic $p > 0$.

Theorem 10. *Let F be an algebraically closed field of characteristic $p > 0$, S a semiabelian variety over F, $\Lambda \leq S(F)$ a finitely generated subgroup, $\Gamma \leq div_p(\Lambda) := \{s \in S(F) : ns \in \Lambda$, for some n prime to $p\}$ and $X \subset S$ a subvariety over F. Then $X(F) \cap \Gamma = \bigcup_{i=1}^{n} X_i(F) \cap \Gamma$ where $X_1, \dots, X_n \subset \Gamma$ are $\mathbf{F_p}$-special.*

proof. We make standard reductions, supposing X is irreducible and $\overline{X(F) \cap \Gamma} = X$, $k := \mathbf{F_p}^{alg}$, K/k is a finitely generated extension over which X, S are defined, and the generators of Λ are in $S(K)$. Let $L \models HCF_p$ be an extension of K such that $L^{p^\infty} = k$. We may assume $F = L^{alg}$, which implies that S, X are over L and $\Lambda \leq S(L)$.

Claim. $\Gamma \leq S(L)$.

proof of Claim. We have indeed $div_p(\Lambda) \leq S(L)$. We use the

Fact. *Let $n : S \to S$ be the multiplication by n, prime to p, $s \in S(L)$ and $t \in S(L^{alg})^{strict}$, such that $nt = s$. Then $t \in S(L^{sep}) = S(L)$.*

□

Thus one has $\overline{X(F) \cap \Gamma} = \overline{X(L) \cap \Gamma} = X$.

Claim. *We may assume that L is saturated.*

proof of Claim. In exercise. Hint :

$$\begin{array}{ccc} L^{alg} = F & & (L^\star)^{alg} \\ \uparrow & & \uparrow \\ L & \leq & L^{star} \text{ sat} \\ \uparrow & & \uparrow \\ F_p^{alg} = K = L^{p^\infty} & & k^\star = (L^{star})^{p^\infty} \end{array}$$

Show that $(k, F) \leq (k^\star, (L^\star)^{alg})$. □

Note. $k \neq \mathbf{F_p}^{alg}$, $k = L^{p^\infty}$.

Theorem 11. *Let L be a saturated model of HCF_0 or HCF_p, $p > 0$. Let k be the constant field, S a semiabelian variety over L, $H \leq S(L)$ a type-definable finite Morely rank subgroup, and $X \subset S$ a subvariety over L. Then $X(L) \cap H = \bigcup_{i=1}^{l} X_i(L) \cap H$, where $X_1, \ldots, X_l \subset X$ are k-special.*

Claim. *$\Gamma/p^n\Gamma$ is finite for any $n \geq 0$.*

proof of Claim. First Λ is a finitely generated $\mathbf{Z}$-module. $\Lambda/p^n\Lambda$ is a finitely generated $\mathbf{Z}/p^n\mathbf{Z}$-module, so is finite. $\Lambda \leq div_p(\Lambda)$ induces a map $\Lambda/p^n\Lambda \to div_p(\Lambda)/p^n div_p(\Lambda)$. Exercise : this is a bijection (use $p \nmid n$). Then $\Gamma/p^n\Gamma$ is finite. □

As $\overline{X(L) \cap \Gamma} = X$ and X is irreducible, X must have a Zariski-dense intersection with some coset of $p^n\Gamma$, for each $n \geq 0$. Let $p^\infty\Gamma := \bigcap_n p^n\Gamma$.
Exercise : X has a Zariski dense intersection with some translate of $p^\infty\Gamma$ (This is essentially due to saturation).
From $\Gamma \leq S(L)$, we get that $p^\infty\Gamma \leq p^\infty S(L)$ (the Manin kernel) is a type definable subgroup of $S(L)$. $p^\infty S(L)$ has finite Morley rank and $\overline{X(L) \cap p^\infty S(L)} = X$, so by theorem 11, $X(L) \cap p^\infty S(L) = \bigcup_{i=1}^{s} X_i(L) \cap p^\infty S(L)$, where $X_1, \ldots, X_l \subset X$ and are k-special. Taking Zariski closures, we have $X \subset \bigcup_{i=1}^{s} X_i \subset X$, so $X = \bigcup_{i=1}^{s} X_i$. As X is irreducible, it means that $X = X_i$ for some i, i.e. that X is k-special. □