Introduction to abelian varieties and Mordell-Lang conjecture

Marc Hindry

20 february 1997

Our aim in this brief survey is to try and give an intuition about abelian varieties to model theorists, working mainly over the complex field. We then try to motivate the Lang Conjecture, showing especially how it generalises Mordell's conjecture.
Finally we present an analogue over function fields, ending with the statement of the result proved by E.Hrushovski [13], which is proved at the end of this volume in [4].
For basic definitions of varieties, algebraic groups, completeness, morphisms see for example [32] or, for a model theoretic presentation [26] in this volume.

1 Abelian varieties

Definition 1.1 *An* abelian variety *is a complete algebraic group.*

Remark: by convention, we include connectedness in the definition of an abelian variety, similarly, when we talk of a variety, we mean an irreducible variety. An abelian subvariety of A is a closed connected subgroup of A.

Over the complex numbers, one can give an apparently totally different definition. Recall that a *lattice* in $\mathbf{C}^g$ is a discrete subgroup of maximal rank, hence isomorphic to $\mathbf{Z}^{2g}$.

Definition 1.2 *A* complex torus *is a quotient* $\mathbf{C}^g/L$*, where* L *is a lattice in* $\mathbf{C}^g$*.*

A complex abelian variety *is a complex torus* $\mathbf{C}^g/L$*, equipped with a non degenerate* Riemann form*, that is a hermitian positive definite form* $H : \mathbf{C}^g \times \mathbf{C}^g \to \mathbf{C}$ *such that* $ImH : L \times L \to \mathbf{Z}$*.*

It is of course quite a deep theorem that the two definitions agree (when the ground field is $\mathbf{C}$).

Example ($dimA = 1$)
Consider a smooth cubic projective curve given by the equation $ZY^2 = X^3 + aXZ^2 + bZ^3$ where $4A^3 + 27B^2 \neq 0$. We take as origin the point "at infinity" $[0, 1, 0]$ and define the group law by the tangent and chord process described in the figure below. Of course the drawing represents the curve in affine coordinates $x = X/Z$, $y = Y/Z$.

This is an abelian variety of dimension 1, an elliptic curve. We will see more examples shortly.

Lemma 1.3 *A complex abelian variety is commutative.*

Proof : In this proof, and only in this proof, we write multiplicatively the group law on A, an abelian variety. Consider the map from A to A defined by $\phi_a(x) = axa^{-1}$; let $d\phi_a$ be the differential at the origin, hence $d\phi_a$ is a linear endomorphism of the tangent space V of A at the origin. We get thus a holomorphic map from A to $End(V) \cong \mathbf{C}^{g^2}$ which maps a to $d\phi_a$. By the maximum principle or Liouville's theorem, the map is constant and its value is Id_V. It follows that $\phi_a = Id_A$ and hence A is commutative. $\bullet$

For an algebraic proof, one replaces compactness by completeness.

Lemma 1.4 *A complex abelian variety is a torus*

Proof : One actually shows that a compact complex Lie group is a complex torus. We saw in the previous lemma that it is commutative, hence the exponential $exp_A : V \to A$ is a surjective homomorphism. Its kernel L is then a discrete subgroup and, since A is compact, L has to be of rank $2g$. •

It can also be shown that all abelian varieties are projective varieties, that is admit an embedding $A \to \mathbf{P}^n$ as a closed subvariety.

Let us now review some classical properties of abelian varieties. We give the easy proofs over $\mathbf{C}$ and just state the results over an arbitrary algebraically closed field k. The extension of the results over an algebraically closed field of characteristic zero is usually straightforward. The extension of the results over an algebraically closed field of characteristic p usually requires entirely different techniques stemming from algebraic geometry.

Let K be an arbitrary algebraically closed field and A an abelian variety over K.

1. A is a divisible group: let $[n]$ denote multiplication by n, then the map $[n] : A \to A$ is surjective.

   Indeed we have a commutative diagram

$$\begin{array}{ccc} \mathbf{C}^g & \stackrel{n}{\to} & \mathbf{C}^g \\ \downarrow & & \downarrow \\ \mathbf{C}^g/L & \stackrel{n}{\to} & \mathbf{C}^g/L \end{array}$$

   This remains true over any algebraically closed field K. The proof is essentially the "same" if $char(K)$ does not divide n and present extra difficulties if $char(K)$ divides n (see [25])

2. Torsion points are dense and are algebraic over the field of definition of A.
   Over $\mathbf{C}$ one gets

$$A_{\text{torsion}} = \mathbf{Q}L/L \cong (\mathbf{Q}/\mathbf{Z})^{2g} \subset (\mathbf{R}/\mathbf{Z})^{2g} \cong A(\mathbf{C})$$

   in fact more precisely $Ker[n] = \frac{1}{n}L/L \cong (\mathbf{Z}/n\mathbf{Z})^{2g}$.

The situation over an algebraically closed field K is as follows:

$$Ker[\ell^n] \cong \begin{cases} (\mathbf{Z}/\ell^n\mathbf{Z})^{2g}, & \text{if } char(K) \neq \ell \\ (\mathbf{Z}/\ell^n\mathbf{Z})^{r}, & \text{if } char(K) = \ell \qquad \text{(with } 0 \leq r \leq g) \end{cases}$$

If A is defined over k, then so is the morphism $[n]$ and its kernel, hence the points of $Ker[n]$ are defined over the algebraic closure of K. If n is prime to $p = char(K)$, then the points of $Ker[n]$ are defined over the separable closure of K.

Corollary: (strong rigidity) If A is defined over a field K, then all closed subgroups of A are defined over the separable closure of K.

Indeed if $G \subset A$ is such a closed subgroup, then $G \cap A_{\text{torsion}}$ is dense in G and composed of points defined over the algebraic closure of K; if $char(K) = p$ we take only the torsion of order prime to p to stay in the separable closure.

3. (Poincaré's reducibility theorem) If B is an abelian subvariety of an abelian variety A, there exists another abelian subvariety C such that $A = B + C$ and $B \cap C$ is finite (in other words the map from $B \times C$ to A defined by $(b, c) \mapsto b + c$ is an isogeny).

   Proof : Let $A = V/L$ (with L a lattice in $V \cong \mathbf{C}^g$) be an abelian variety. It possesses a non degenerate Riemann form, say H. Let W be the complex tangent space of B at 0, then $B = W/L \cap W$. Let W' be the orthogonal complement of W with respect to H, then one shows that $C = W'/L \cap W'$ is a complex torus and that H induces a non degenerate Riemann form on it. Since $V = W \oplus W'$, the abelian subvariety C does what is required. •

   Remarks: a) This property is false (in general) for complex tori; on the other hand it remains valid for all abelian varieties defined over a field of any characteristic.

   b) One can deduce from Poincaré's reducibility theorem that quotients of A and abelian subvarieties of A are the same up to isogeny. Indeed, if $f : A \to B$ is onto, then the connected component of the kernel of f has a "complementary" abelian subvariety C such that the induced map $f : C \to B$ is an isogeny. For the converse, if B is an abelian subvariety, C a "complementary" abelian subvariety then A/C is isogenous to B.

4. The endomorphism ring $\mathrm{End}(A)$ is isomorphic to some $\mathbf{Z}^r$ with $r \leq 4g^2$ (as a group).

   Proof : Any endomorphism $\alpha : A = \mathbf{C}^g/L \to A = \mathbf{C}^g/L$ induces a linear map $\tilde{\alpha} : \mathbf{C}^g \to \mathbf{C}^g$ such that $\tilde{\alpha}(L) \subset L$ hence we get an injection $\mathrm{End}(A) \hookrightarrow \mathrm{End}_{\mathbf{Z}}(L) \cong Mat(2g \times 2g, \mathbf{Z})$. •

   This property remains true in any characteristic. From this last property or from the strong rigidity property, one easily deduces:

   Corollary: an abelian variety cannot possess an algebraic family of abelian subvarieties.

   Remark: This is somewhat trivial but quite necessary for the plausibility of Lang's conjecture.

   Example: an abelian variety A is called *simple* if its only abelian subvarieties are $\{0\}$ or itself; in this case $\mathrm{End}(A) \otimes \mathbf{Q}$ is a division ring.

The fundamental example of an abelian variety : the jacobian of a curve.

Historically the theory comes from integral calculus, a typical example being attempts to compute integrals like:

$$\int \frac{dx}{\sqrt{x^3+1}}, \ \int \frac{dx}{\sqrt{x^5+1}}$$

Since all algebraic curves are birationally equivalent to a smooth projective curve, we will restrict to the latter.

Definition of the genus of a curve: the complex points of a smooth projective curve X form a compact Riemann surface $X(\mathbf{C})$, hence one of the following shape

Riemann Sphere   a torus $\mathbf{C}/L$ two handles
g=0 $g = 1$ $g = 2$

The genus can also be defined purely algebraically as the number of linearly independant *regular differential 1-forms.* Selecting a point $P_0 \in X(\mathbf{C})$ and $\omega_1, \ldots, \omega_g$ such differential forms we may define

$$P \mapsto \left(\int_{P_0}^{P} \omega_1, \ldots, \int_{P_0}^{P} \omega_g \right)$$

this is actually ill-defined because the integral will depend on the chosen path

but if we mod out by the periods – integrals of the ω_i's along closed paths – we get a well-defined holomorphic map

$$j : X(\mathbf{C}) \to \mathbf{C}^g/\text{periods} =: \mathrm{J}(\mathbf{C})$$

The torus J is called the *jacobian* of X and denoted $\mathrm{J}(X)$. A beautiful theorem of Riemann – Riemann's periods relations (see [2] or [3]) guarantees that J is an abelian variety, in particular the periods generate a lattice. From our point of view the main results concerning the jacobian are:

- If $g \geq 1$ then $j : X \hookrightarrow \mathrm{J}$ is an embedding; it is an isomorphism if and only if $g = 1$ (in fact $dim(\mathrm{J}) = g$).
- (Abel-Jacobi) We may extend the map j by linearity to *divisors* (i.e. formal sums of points of X). For a rational (meromorphic) function f on X, define its divisor by $div(f)$ ={Zeroes of f} - { Poles of f} (see [32] for a precise definition of multiplicities). The *degree* of a divisor $D = \sum_i n_i P_i$ is defined as $deg(D) := \sum_i n_i$. The divisors of functions form a subgroup $P(X)$ of the group of divisors of degree zero $Div^0(X)$. The Abel-Jacobi theorem may be summarised by saying that the following canonical sequence is exact:

$$0 \to P(X) \to Div^0(X) \to \mathrm{J} \to 0$$

- One can also construct interesting subvarieties inside jacobians by setting:
$$W_r(X) := \underbrace{j(X) + \ldots + j(X)}_{r \text{ times}} \subset \mathrm{J}$$
It is not hard to show that $dim(W_r) = \min(r, g)$.

All this can be done algebraically by Weil's theory. In fact it is not too hard to see from what we have said that, if the jacobian exists, it is birational to the g-th symmetric product of C. The classical theorem of Riemann-Roch provides a birational group law on this symmetric product. Weil invented the theorem quoted in [26] in order to get a purely algebraic construction of the jacobian. In particular his construction is valid over a field of characteristic p (see [31]).

Remark : this construction may be generalised to an arbitrary smooth projective variety V by selecting $\omega_1, \ldots, \omega_g$ a basis of holomorphic 1-forms and setting:

$$\begin{array}{cccc} j: & V(\mathbf{C}) & \rightarrow & \mathbf{C}^g/\text{periods} =: \mathrm{Alb}(V) \\ & P & \mapsto & \left(\int_{P_0}^P \omega_1, \ldots, \int_{P_0}^P \omega_g\right) \end{array}$$

One still gets an abelian variety called the *Albanese variety* of V. Nevertheless, the construction is not as useful as jacobians because j is almost never an embedding; for example, for a smooth surface V in $\mathbf{P}^3$ we have $\mathrm{Alb}(V) = 0$.

Anticipating, we may note that Lang's conjecture says something only for varieties which admit regular differential 1-forms.

We focus in this paper on abelian varieties but it is interesting to study general (commutative) algebraic groups. We will only mention Chevalley's theorem and the definition of semi-abelian varieties.

Definition 1.5 *An affine algebraic group is an affine variety (i.e. closed in an affine space) with an algebraic group law.*

Examples:

- $GL(n)$ is an affine algebraic group: instead of $\{x \in Mat(n \times n) \mid det(x) \neq 0\}$, think of it as $\{(x,t) \in Mat(n \times n) \times \mathbf{A}^1 \mid tdet(x) - 1 = 0\}$

- Over an algebraically closed field, the only affine algebraic groups of dimension one are: the additive group $\mathbf{G}_a$ with underlying variety the affine line $\mathbf{A}^1$ and group law the addition; the multiplicative group $\mathbf{G}_m$ with underlying variety the affine line minus a point $\mathbf{A}^1 \setminus \{0\}$ and group law the multiplication.

- Any closed subgroup of $GL(n)$ is an affine algebraic group. In fact it can be shown that any affine algebraic group is isomorphic to such a closed subgroup of $GL(n)$.

It is easy to see that the compositum of two affine subgroups of an algebraic group G is again affine, hence there is a *unique maximal connected affine subgroup.*

Theorem 1.6 *(Chevalley) Let G be a connected algebraic group, let L be the maximal connected affine subgroup of G, then G/L is an abelian variety.*

Remark: L is also the smallest closed subgroup of G such that G/L is an abelian variety.

Definition 1.7 *Over an algebraically closed field, a semi-abelian variety is a commutative algebraic group which is an extension of an abelian variety by a multiplicative group $(\mathbf{G}_m)^r$.*

One can formulate (and prove ... see papers by Faltings and Vojta) Lang's conjecture for the wider class of semi-abelian variety. Many properties of abelian varieties are shared by semi-abelian varieties. For example, if G is a semi-abelian variety defined over an algebraically closed field K:

- Torsion point are dense in G

- All closed subgroups are defined over K

- If G is an extension of A with dimension a by $(\mathbf{G}_m)^r$ then $Ker[n]_G \cong (\mathbf{Z}/n\mathbf{Z})^{2a+r}$ as long as $char(K)$ does not divide n.

2 Lang's conjecture

The conjecture of Lang stems from Mordell's conjecture (1922) and a question raised by Manin and Mumford in the seventies. Mordell's conjecture is a problem about diophantine equations. Given a polynomial $P \in \mathbf{Q}[x, y]$, one wants to study the set

$$\{(x, y) \in \mathbf{Q}^2 \mid P(x, y) = 0\}$$

For this we associate the smooth projective curve X birational to the affine curve defined by $P(x, y) = 0$.

- 1st case : The curve X is of genus 0. Then either $X(\mathbf{Q}) = \emptyset$ (e.g. $P(x, y) = x^2+y^2+1$) or all but finitely many solutions are parametrised by rational fractions $x(t), y(t)$ (e.g. all the solutions of $x^2 + y^2 - 1 = 0$ are parametrised by $(x, y) = (\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1})$ except $(0, 1)$).

- 2nd case : The genus of X is one. Then either $X(\mathbf{Q}) = \emptyset$ or, taking one of the rational points as origin, X is an elliptic curve (an abelian variety of dimension 1) and hence we have a group law on the set $X(\mathbf{Q})$.

  Theorem 2.1 *(Mordell-Weil) $X(\mathbf{Q})$ is a finitely generated group. Much more generally, if K is a field finitely generated over $\mathbf{Q}$ (for example a number field) and A is an abelian variety defined over K then $A(K)$ is a finitely generated group.*

- 3rd case : The genus of X is ≥ 2. Then Faltings proved the Mordell conjecture : $X(\mathbf{Q})$ is finite.

We can reformulate the Mordell conjecture as follows : embed $X \hookrightarrow A =$ jacobian of X, then $X(\mathbf{Q}) = X \cap A(\mathbf{Q})$, so we are reduced to proving:
Let Γ be a finitely generated subgroup of $A = \mathrm{J}(X)$ then $\Gamma \cap X$ is finite
or slightly more generally:
Let X be a curve in an abelian variety A and Γ be a finitely generated subgroup of A then $\Gamma \cap X$ is finite, except if X is a translate of an elliptic curve.
Granting the Mordell-Weil theorem, this last statement is actually easily seen to be equivalent to Mordell's conjecture.
The *Manin-Mumford question* is the following : consider again $X \hookrightarrow A =$

J(X) then is it true that $X \cap A_{\text{torsion}}$ is finite? Analogously one can slightly generalise this to:
Let X be a curve in an abelian variety A, then $X \cap A_{\text{torsion}}$ is finite, except if X is a translate of an elliptic curve.
Remark. The motivations were apparently quite different. Manin had proven with Drinfeld that cusps generate a torsion subgroup of the jacobian of a modular curve. Mumford was studying moduli spaces of curves.

It is easy to put together the two conjectures by introducing the concept of a group of finite rank.

Definition 2.2 *Γ is a group of finite rank r if $\Gamma \otimes \mathbf{Q} \cong \mathbf{Q}^r$*

Or, if you prefer, there is a finitely generated subgroup Γ_0 of rank r, such that for all $\gamma \in \Gamma$, there is an integer $m \geq 1$ such that $m\gamma \in \Gamma_0$.
Note : When working in characteristic p, one requires a bit more, namely that $\Gamma \otimes \mathbf{Z}_{(p)} \cong \mathbf{Z}^r_{(p)}$ or, if you prefer, there is a finitely generated subgroup Γ_0 of rank r, such that for all $\gamma \in \Gamma$, there is an integer $m \geq 1$, coprime with p, such that $m\gamma \in \Gamma_0$.

Lang's conjecture for curves *Let X be a complex curve in an abelian variety A and Γ be a subgroup of finite rank in A then $\Gamma \cap X$ is finite, except if X is a translate of an elliptic curve.*

It is natural to ask what happens for higher dimensional varieties.

Lang's conjecture ("absolute form", characteristic zero) *Let X be a complex subvariety of a complex abelian variety A and Γ be a subgroup of finite rank in A then there exist $\gamma_1, \ldots, \gamma_m \in \Gamma$ and $B_1, \ldots, B_m$ abelian subvarieties such that $\gamma_i + B_i \subset X$ and such that*

$$\Gamma \cap X(\mathbf{C}) = \cup_{i=1}^m \gamma_i + (B_i(\mathbf{C}) \cap \Gamma)$$

Remarks

- The most immediate analog over $k = \overline{\mathbf{F}}_p$ is false since all points in $A(\overline{\mathbf{F}}_p)$ are torsion points. Nevertheless, there is a relative form of Lang's conjecture, which we will state in the next section.

- This is really a diophantine conjecture. Indeed if $K = \mathbf{Q}(x_1, \ldots, x_n)$ is a field finitely generated over $\mathbf{Q}$ (e.g. a number field), if X is a subvariety of an abelian variety A all defined over K then the Mordell-Weil theorem tells us that $\Gamma = A(K)$ is finitely generated, hence the conjecture describes the K-rational points of X.

- The conjecture is easily equivalent to the following statement: *if the set $X \cap \Gamma$ is Zariski dense in X then X is a translate of an abelian subvariety by a point in Γ* (proof : by induction on the dimension of X).

- One may perform a number of reduction in order to prove the conjecture. For example if we define the *stabilizer* of X as the (not necessarily connected) algebraic subgroup $\mathrm{Stab}_X = \{a \in A \mid a + X \subset X\}$ then we may assume that Stab_X is finite or even $\{0\}$. Notice that under the hypothesis that Stab_X is finite, the conclusion must be that $X \cap \Gamma$ is not dense in X.

  Proof : Call $H = \mathrm{Stab}_X$ and consider the abelian variety $A' := A/H$ with the canonical projection $\pi : A \to A'$ and image $X' := \pi(X)$. One checks easily that $\mathrm{Stab}_{X'} = \{0\}$. Hence, if X is not a translate of an abelian subvariety, X' is not reduced to a point. If we already know that $X' \cap \pi(\Gamma)$ is not Zariski dense in X', we immediately obtain that $X \cap \Gamma$ is not Zariski dense in X, since $\pi(X \cap \Gamma) \subset X' \cap \pi(\Gamma)$. •

- Though the formulation is given over the field of complex numbers, one may assume that A, X and Γ_0 are defined over a field finitely generated over $\mathbf{Q}$ (here Γ_0 is a finitely generated subgroup such that for each $\gamma \in \Gamma$, there is an $n \geq 1$ such that $n\gamma \in \Gamma_0$). By specialisation arguments, one may reduce the conjecture to the case where everything is defined over $\overline{\mathbf{Q}}$.

To illustrate the richness of the content of Lang's conjecture, let us get back to the case of a curve X defined over (say) a number field K and embedded in its jacobian $A = \mathrm{J}(X)$ and consider the subvarieties $W_r = X + \ldots + X$ introduced earlier. The Lang conjecture asserts that $W_r(K)$ is finite unless W_r contains a translate of a non zero abelian subvariety. On the other hand there is an obvious morphism from the r-th symmetric product of the curve X with itself onto W_r. The Abel-Jacobi theorem tells us that this is an isomorphism except when X admits a morphism of degree $\leq r$ to $\mathbf{P}^1$. Since points defined over K on the symmetric product correspond essentially to algebraic points on X with Galois orbit (over K) of cardinal $\leq r$ we get the following result (see [11], [12] for details):

Proposition 2.3 *Let X be a curve defined over a number field K and let r be an integer. Assume that there is no morphism $\pi : X \to \mathbf{P}^1$ of degree $\leq r$ and also that W_r does not contain a translate of a non zero abelian subvariety. Then the union of the set of rational points $X(L)$ for all number fields L containing K with $[L:K] \leq r$ is finite.*

One may formulate obvious generalisations to finitely generated fields. The condition " no morphism $\pi : X \to \mathbf{P}^1$ of degree $\leq r$" is clearly necessary since otherwise the set $\pi^{-1}(\mathbf{P}^1(K))$ is clearly infinite. One would like a geometric description "in terms of the curve" of the condition "W_r does not contain a translate of a non zero abelian subvariety", but that does not seem to be known in general.

Let us digress a bit to explain how the Lang conjecture (for subvarieties of abelian varieties) fits into some general conjecture about classification of algebraic varieties and diophantine properties.

Let V be a smooth projective variety of dimension n, we have already considered regular differential 1-forms, but we may also introduce r-forms (say for $1 \leq r \leq n$) and also powers of r-forms. We refer for example to Shafarevic's book [32] and mention only the abstract definitions: considering the *sheaf* Ω_r of differential r-forms, a *regular differential r-form of weight m* is a global section of $\Omega_r^{\otimes m} = \Omega_r \otimes \ldots \otimes \Omega_r$. The most interesting case (for our purposes) is the case of n-forms (recall $n = dim(V)$) because in this case the sheaves $\Omega_n^{\otimes m}$ are invertible and give rises to linear systems. The sheaves $\Omega_n^{\otimes m}$ are called the *pluri-canonical sheaves* and the dimension g_m of the space of global sections are called the *pluri-genera* of the variety V. More concretely select a basis $\omega_1, \ldots, \omega_{g_m}$ of global sections of $\Omega_n^{\otimes m}$, then the map

$$\begin{array}{cccc} \Phi_m : & V & \cdots \to & \mathbf{P}^{g_m - 1} \\ & x & \to & (\omega_1(x), \ldots, \omega_{g_m}(x)) \end{array}$$

is a rational map and a morphism outside the set of common zeroes of the ω_i. Observe that the "value" of ω_i at x is meaningless but the quotient ω_i/ω_j is a function on V. So we have a collection of rational maps called quite naturally the *pluri-canonical maps*. This is used to define an invariant which is fundamental in the classification of algebraic varieties:

Definition 2.4 *Let V be a smooth projective variety, the Kodaira dimension of V is $\kappa(V) = -1$ if all $g_m(V) = 0$ and $\kappa(V) = \max\{dim(\Phi_m(V)\}$ otherwise. Clearly $-1 \leq \kappa(V) \leq dimV$.*

Examples: For a curve V it is easy (or at least classical) to see that $\kappa(V) = -1$ if the genus is zero ($V \cong \mathbf{P}^1$), $\kappa(V) = 0$ if the genus is 1 and $\kappa(V) = 1$ if the genus is at least 2. An abelian variety A has $\kappa(A) = 0$. A smooth hypersurface V of degree d in $\mathbf{P}^n$ has $\kappa(V) = -1$ if $d \leq n$ and $\kappa(V) = 0$ if $d = n+1$ and $\kappa(V) = n-1 = dim(V)$ if $d \geq n+2$. For a subvariety V of an abelian variety A, it is known that $\kappa(V) = dim(V) - dim(\text{Stab}_V)$.

Definition 2.5 *A variety is of general type if $\kappa(V) = dim(V)$.*

Thus a subvariety of an abelian variety is of general type if and only if its stabiliser is finite; a smooth hypersurface of degree d in $\mathbf{P}^n$ is of general type if and only if $d \geq n+2$.

Conjecture (Bombieri-Lang) *Let V be a variety of general type defined over a number field K then the set of rational points $V(K)$ is not Zariski dense.*

Remark: 1) Bombieri asked this question for surfaces of general type and Lang (independantly) made the general conjecture in a more precise form: he conjectures that there is a fixed "geometric" closed subset Z such that, if $U = V \setminus Z$ then for all number fields K' containing K, the set $U(K')$ is finite.

2) For V a subvariety of an abelian variety, this broad conjecture is true and equivalent to the conjecture discussed in this paper. It is essentially the only case known. In particular, the conjecture is unknown even in the following "simple" example: let V be the quintic surface defined in $\mathbf{P}^3$ by the equation $X_0^5 + X_1^5 + X_2^5 + X_3^5 = 0$. Rational points are presumably not dense and concentrated on a finite number of curves like the lines $X_i + X_j = X_m + X_\ell = 0$. This is unknown, even in the function field case.

3 Diophantine equations over function fields, “relative” case of Lang’s conjecture

The main purpose of diophantine geometry is to describe sets $X(\mathbf{Q})$ of rational points of a variety. It is natural to look for generalisations, first to number fields then to fields finitely generated over $\mathbf{Q}$. The next step would be fields K finitely generated over $\mathbf{F}_p$. For example, some of the main results for X a curve are still true: if X is an elliptic curve, the group $X(K)$ is still finitely generated and if X has genus $g \geq 2$ then $X(K)$ is still finite.

Another motivation can be explained in a somewhat trivial case: if X is a curve defined over $\mathbf{Q}$ before trying to prove that $X(\mathbf{Q})$ is finite, one should perhaps check that $X(\mathbf{Q}(T)) \setminus X(\mathbf{Q})$ is finite. The deepest motivation however comes from the famous analogy between number fields and function fields studied by many mathematicians (let us quote arbitrarily Kronecker, Artin, Hasse, Weil, Néron, Grothendieck, Parshin, Arakelov,...). Let us give a formal definition:

Definition 3.1 *Let K_0 be an algebraically closed field, a function field K over K_0 (of transcendance degree 1) is the field of rational functions of a variety (of dimension 1) defined over K_0.*

This is actually the same as a finitely generated field over K_0 (of transcendance degree 1).
Now the natural question to ask is not “*is $X(K)$ finite?*” but “*is $X(K) \setminus X(K_0)$ finite?*”. Let us give an example dear to number theorists.

Proposition 3.2 *Let X be the Fermat curve defined in the projective plane by $X^n + Y^n = Z^n$ where $n \geq 3$. Let U be the affine open subset of X defined by $XYZ \neq 0$ then $X(\mathbf{C}(T)) \setminus X(\mathbf{C})$ is empty.*

Proof :(see Mason, diophantine equations over function fields, London Math. Soc. L. N. 96, Cambridge U.P., 1984) One proves actually a more general statement which easily implies Fermat. If A, B, C are non constant coprime polynomials with $A + B = C$ and if r, s, t are the number of distinct roots of A, B, C then

$$\max(deg(A), deg(B), deg(C)) \leq r + s + t - 1$$

Indeed if X, Y, Z are coprime polynomials satisfying $X^n + Y^n = Z^n$, set $A = X^n$, $B = Y^n$ and $C = Z^n$. Applying the previous inequality and the observation that $deg(A) \geq nr$, $deg(B) \geq ns$ and $deg(C) \geq nt$, we obtain $n \max(r, s, t) \leq r + s + t - 1 \leq 3 \max(r, s, t) - 1$, hence $n \leq 2$.

In order to prove the inequality, one introduces the polynomial

$$\Delta := det \begin{pmatrix} A & A' \\ B & B' \end{pmatrix} = det \begin{pmatrix} A & A' \\ C & C' \end{pmatrix} = det \begin{pmatrix} C & C' \\ B & B' \end{pmatrix}.$$

This polynomial is non zero and has degree less than $deg(A) + deg(B) - 1$ (mutatis mutandis). If $A = a_0 \prod_{i=1}^{r}(T - a_i)^{\ell_i}$, $B = b_0 \prod_{i=1}^{s}(T - b_i)^{m_i}$ and $C = c_0 \prod_{i=1}^{t}(T - c_i)^{n_i}$ then $\prod_{i=1}^{r}(T - a_i)^{\ell_i - 1} \prod_{i=1}^{s}(T - b_i)^{m_i - 1} \prod_{i=1}^{t}(T - c_i)^{n_i - 1}$ divides Δ. Computing degrees gives the result. •

Since the proof uses derivations, it cannot be adapted to $\mathbf{Q}$!

We can look in this context for the analog of Mordell and Lang's conjecture. For example the following was shown in 1963 by Manin ([22]):

Theorem 3.3 *(Mordell's conjecture over function fields) Let X be a curve of genus ≥ 2 defined over K a function field over K_0. Then $X(K)$ is finite unless X is isotrivial (which means that there is a curve X_0 defined over K_0 and isomorphic to X over some finite extension K' of K).*

A simpler but slightly incorrect statement is "$X(K)$ is finite unless X is defined over K_0". Manin proved this for $K_0 = \mathbf{C}$ (and hence for characteristic zero) and the corresponding characteristic p statement was proven later by Samuel.

The theorem proved by Hrushovski (Lang's conjecture for function fields) bears the same relation to the Lang conjecture as this last statement to the classical Mordell conjecture. Before stating it we review the analog of the Mordell-Weil theorem. We will need the notion of K/K_0-trace and K/K_0-image of an abelian variety defined over K (see Lang's book [17] on abelian varieties for details).

Proposition 3.4 *1) Let A be an abelian variety defined over K. There is an abelian variety A_0 defined over K_0 and a homomorphism (with finite kernel) $\tau : A_0 \to A$ such that for all B abelian variety defined over K_0 with a map*

$\tau' : B \to A$ we have a factorisation $\tau' = \tau \circ f$ via a morphism $f : B \to A_0$. Thus A_0 is the "biggest abelian subvariety of A defined over K_0", it is called the K/K_0-trace of A.
2) Let A be an abelian variety defined over K. There is an abelian variety A_1 defined over K_0 and a surjective homomorphism $\pi : A \to A_1$ such that for all B abelian variety defined over K_0 with a map $\pi' : A \to B$ we have a factorisation $\pi' = f \circ \pi$ via a morphism $f : A_1 \to B$. Thus A_1 is the "biggest quotient of A defined over K_0", it is called the K/K_0-image of A.

For our purposes it will clarify things to know that A_0 is zero if and only A_1 is zero (actually much more is true : A_0 and A_1 are "duals" hence have the same dimension). For a proof of the next theorem see [15].

Theorem 3.5 *(Relative Mordell-Weil theorem, Lang-Néron) Let A be an abelian variety defined over K and let $\tau : A_0 \to A$ be its K/K_0-trace, then the group $A(K)/\tau(A_0(K_0))$ is finitely generated.*

Remark: If the K/K_0-trace (or image) is zero then $A(K)$ is finitely generated.
The translation of Lang's conjecture is easier to state when the stabiliser of the subvariety is finite (we saw that this is the crucial case). For a model theoretic translation see [27].

Lang's conjecture over function fields *Let K be a function field over K_0 an algebraically closed field, let X be a subvariety of an abelian variety A both defined over K. Assume that Stab_X is finite. Let Γ be a subgroup of A of finite rank, defined over the algebraic closure of K, then either $X \cap \Gamma$ is not Zariski dense in X or there is a bijective morphism $X \to X_0$ onto a variety X_0 defined over K_0.*

Remark: If the K/K_0-trace of A is zero, then no such X_0 (distinct from a point) can exist because its Albanese variety would produce a non zero K/K_0-image for A. Hence in this case, the usual Lang conjecture is true.

4 Commented bibliography

Abelian and Jacobian varieties are treated in many books. For complex abelian varieties we especially quote as the easiest Swinnerton Dyer's book [33] and Rosen's paper in [7], the book of Lange and Birkenhake [2] being the most complete reference; it also includes Jacobians. The survey of Bost [3] contains also a lot of interesting material. The algebraic theory of abelian varieties is treated in Mumford's book [25] and Milne's first paper in [7]. Milne's second paper in [7] develops the algebraic theory of Jacobians; an exposition quite close to Weil's original treatment can be found in Serre's book [31]. The books of Serge Lang provide also interesting different points of view [15], [16], [17].

One can find a quite thorough discussion of Lang's conjecture by Lang himself in [15], in his survey for the russian encyclopedia [20] as well as in his original papers [18], [19]. The Mordell conjecture was stated in Mordell's paper [24] in 1922 and first proven over function fields by Manin [22] in 1963 and over number fields by Faltings [8] in 1983. The paper of Faltings [9] 1991, contains a proof that $X(k)$ is finite when k is a number field, X is a subvariety of an abelian variety and X does not contain a translate of a (non zero) abelian subvariety; his subsequent paper [10] deals with the case of a subvariety of an abelian variety. The methods rely heavily on ideas introduced by Vojta [34] who gave a completely new proof of Mordell's conjecture over number fields. This implies Lang's conjecture for finitely generated subgroups. The reduction of the general conjecture to this case had already been worked out in Hindry [11]. The Manin-Mumford conjecture was first proven by Raynaud [28], [29], [30] and extended to general commutative algebraic groups by Hindry [11]. Extensions to semi-abelian varieties of Lang's conjecture have been worked out by Vojta [35] for a finitely generated subgroup, and by McQuillan [23] for the reduction from "finite rank" to "finitely generated" group. The case of subvarieties of a multiplicative group $\mathbf{G}_m^r$ was proven before in full generality by Laurent [21].

All these works deal with characteristic zero. As mentionned before, the statements over number fields implies the general statement in characteristic zero. Nevertheless specific proofs for function fields are of great interest. Buium (see [5], [6]) has given such a proof under the mild assumption that X is smooth. Abramovic and Voloch [1] proved the characteristic p case under extra assumptions. It should therefore be noticed that the proof of the characteristic p case was unknown, in full generality, before Hrushovski[13]! Also note that Hrushovski in fact proves it for semi-abelian varieties. It is also possible to deduce the relative statement in characteristic zero from the corresponding statement in characteristic p (see [14] and the remarks in [20]).

References

[1] D. Abramovic, J. F. Voloch, *Towards a proof of the Mordell-Lang conjecture in characteristic p*, International Math. Research Notices, 2, 1992, 103-115.

[2] C. Birkenhake, H. Lange, *Complex abelian varieties*, Springer Verlag, 1992.

[3] J-B. Bost, *Introduction to compact Riemann surfaces, jacobians and abelian varieties*, in Number Theory and Physics, Springer 1993.

[4] E. Bouscaren, *Hrushovski's proof of the Mordell-Lang conjecture for function fields*, this volume.

[5] A. Buium, *Intersections in jet spaces and a conjecture of Serge Lang*, Annals of Math. 136, 1992, 583-593.

[6] A. Buium, *Effective bounds for geometric Lang conjecture*, Duke J. Math., 71, 1993, 475-499.

[7] G. Cornell, J. Silverman (ed), *Arithmetic geometry*, Springer Verlag, 1986.

[8] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Inv. Math. 73, 1983, 349-366.

[9] G. Faltings, *Diophantine approximation on abelian varieties*, Annals of Math. 133, 1991, 549-576.

[10] G. Faltings, *The general case of Lang's conjecture*, in Barsotti's Symposium in Algebraic geometry, Acad. Press, 1994, 175-182.

[11] M. Hindry, *Autour d'une conjecture de Serge Lang*, Inventiones Math. 94, 1988, 575-603.

[12] M. Hindry, *Sur les conjectures de Mordell et Lang (d'après Vojta, Faltings et Bombieri)*, Astérisque 209, 1992, 39-56.

[13] E. Hrushovski, The Mordell-Lang conjecture for function fields, Journal AMS 9, 1996, 667-690.

[14] E. Hrushovski, *Proof of Manin's theorem by reduction to positive characteristic*, this volume.

[15] S. Lang., *Fundamentals of Diophantine Geometry*, Springer 1983.

[16] S. Lang, *Algebraic functions and abelian functions*, Addison Wesley, 1972.

[17] S. Lang, *Abelian varieties*, Interscience, New York 1959.

[18] S. Lang, *Integral points on curves*, Publ. Math. IHES 6, 1960, 27-43.

[19] S. Lang, *Division points on curves*, Ann. Mat. Pura Appl. LXX, 229-234, 1965.

[20] S. Lang, *Number Theory III*, Encyclopedia of Mathematical Sciences, Springer,1991.

[21] M. Laurent, *Equations diophantiennes exponentielles*, Inventiones Math. 78, 1984, 299-327.

[22] Y. Manin, *Rational points of algebraic curves over function fields*, Izv. Akad. Nauk SSSR 27, 1963, 1395-1440 (in Russian). Transl. II Amer. M.S. 50, 1966, 189-234.

[23] M. McQuillan, *Division points on semi-abelian varieties*, Inventiones Math., 120, 1995, 143-159.

[24] L. Mordell, *On the rational solutions of the indeterminate equation of the 3rd and 4th degree*, Math. Proc. Cambridge Philos. Soc. 21, 1922, 179-192.

[25] D. Mumford, *Abelian varieties*, Oxford University Press, 1974.

[26] A. Pillay, *Model theory of algebraically closed fields*, this volume.

[27] A. Pillay, *The model-theoretic content of Lang's Conjecture*, this volume.

[28] M. Raynaud, *Courbes sur une variété abélienne et points de torsion*, Inventiones Math. 71, 1983, 207-233.

[29] M. Raynaud, *Sous-variétés d'une variété abélienne et points de torsion*, in Arithmetic and Geometry (dedicated to Shafarevic) , Birkhäuser 1983.

[30] M. Raynaud, *Around the Mordell conjecture for function fields and a conjecture of Serge Lang*, in Algebraic Geometry, Springer LN 1016, 1983, 1-19.

[31] J-P. Serre, *Groupes algébriques et corps de classes*, Hermann 1959.

[32] I. Shafarevic, *Basic algebraic geometry*, Spinger 1974.

[33] H. Swinnerton-Dyer, *Introduction to the analytical theory of abelian varieties*, London M.S. LN 14, Cambridge University Press 1974.

[34] P. Vojta, *Siegel's theorem in the compact case*, Annals of Math. 133, 1991, 509-548.

[35] P. Vojta, *Integral points on subvarieties of semi-abelian varieties*, Inventiones Math., 126, 1996, 133-181.