Manin kernels, algebraic independence and diophantine equations over function fields.

D. Bertrand (IMJ)

Thue 150

Bordeaux, Sept. 30 - Oct. 4, 2013

I . Manin's theorem of the kernel

II . Relative Manin-Mumford for families of semi-abelian surfaces.

$\rightsquigarrow$ boils down (cf. D. Masser's talk) to algebraic independence of functional logarithms.

III. Polynomial Pell equations with non-square free discriminants

$\rightsquigarrow$ replace jacobians by generalized jacobians.

References

[A] Y. André : *Mumford-Tate groups of mixed Hodge structures and the theorem of the fixed part*; Compo. Math., 82 (1992), 1-24.

[C] C-L. Chai : *A note on Manin's theorem of the kernel*; Amer. J. Maths 113, 1991, 387-389.

[B] D. B. : *Galois descent in Galois theories*; Sém. & Congrès, 23, 2011, 1-24.

[MZ] D. Masser, U. Zannier : *Torsion points ...* series : CRAS, 346, 2008, 491-494; Amer. J. Math, 132, 2010, 1677-169; Math. Ann., 2012, 352, 453-484; *.... and Pell's equation over polynomial rings*, preprint, Nov. 2012.

[B-M-P-Z] D. B., D. Masser, A. Pillay, U. Zannier : *Relative Manin-Mumford for semi-abelian schemes*; ArXiv 1307.1008v1

[B-E] D. B, B. Edixhoven : *Pink's conjecture, Poincaré biextensions, and generalized jacobians*, in preparation.

I. Manin's theorem

1. A multiplicative analogue and its use.

$S/\mathbb{C}$ affine curve, $K = \mathbb{C}(S)$ (or its alg. closure), $\partial \in Der(K/\mathbb{C})$.
$T = \mathbb{G}_m^n$, commutative alg. group defined over $\mathbb{C} = K^\partial$.
$LT = Lie(T)$, with connection $\nabla_{LT}(x_1, ..., x_n) = (\partial x_1, ..., \partial x_n)$.
$p = (y_1, ..., y_n) \in T(K) = K^{*n} \to x" = "\ell n(p) \in LT$, analytic on some disk in $S(\mathbb{C})$.
$F_p := K(x) = K(\ell n(p))$ depends only on p.

Theorem (Ax) : *$tr.deg.(F_p/K) < n \Rightarrow \exists$ alg. subgroup $H \subsetneq T$ such that $p \in H(K) + T(\mathbb{C})$.*

Proof in 2 steps, based on the logarithmic derivative

$$\partial \ell n(p) := \nabla_{LT}(\ell n(p)) = (\partial y_1/y_1, ... \partial y_n/y_n) \in LT(K).$$

View x as *any* solution of the inhomogeneous equation

$$\nabla_{LT}(x) = \partial \ell n(p) \ , \ \text{with } Ker(\nabla_{LT}) := (LT)^\nabla \simeq \mathbb{C}^n.$$

Clearly, $F_p = K(x) = K(\ell n(p))$ depends only on the class of $\partial \ell n(p)$ in $LT(K)/\nabla_{LT}(LT(K)) \rightsquigarrow$ a "Manin map" :

$$M_K : T(K) \to LT(K)/\nabla_{LT}(LT(K)) = Coker(\nabla_{LT}; K).$$

• **1st step** (Ostrowski) : take any $a = (a_1, ..., a_n) \in LT(K)$ and consider $\nabla_{LT}(x) = a$. Assume that $deg.tr.K(x)/K) < n$. Then, $a_1, ..., a_n$ are lin. dep. over $\mathbb{C}$ modulo $\partial(K)$.

Proof : *$Gal_\partial(K(x)/K) = N^\nabla \subset (LT)^\nabla$, where N is the smallest ∇_{LT}-submodule N/K of LT such that $a \in N(K) + \nabla_{LT}(T(K))$.*

So, $deg.tr.(F_p/K) < n \Rightarrow \exists c_1, ..., c_n \in \mathbb{C}$, not all zero, and $\xi \in K$ such that $c_1 \frac{\partial y_1}{y_1} + ... + c_n \frac{\partial y_n}{y_n} = \partial \xi$.

• **2nd step** (integral structure) : of course, $\partial \ell n(K^*) \hookrightarrow K/\partial K$, i.e. $Ker(M_K) = T(\mathbb{C})$. But in fact : $\boxed{\partial \ell n(K^*) \otimes \mathbb{C} \hookrightarrow K/\partial K.}$

So, for $a = \partial \ell n(p)$, there is a relation *over* $\mathbb{Z}$, with $\xi \in \mathbb{C}$. So $\exists$ *alg.* subgroup $H \subsetneq T$ such that $p \in H(K) + T(\mathbb{C})$.

Assume that $p \in T(K)$ is *non-degenerate* : for any alg. subgroup $H \subsetneq T$, $p \notin H(K) + T(\mathbb{C})$. Then, for any strict ∇_{LT}-submodule N/K of LT, the "Manin-Chai map"

$$\overline{M}_K : T(K) \to Coker\{\nabla_{LT/N} : (LT/N)(K) \to (LT/N)(K)\}$$

sending p to the class of $\partial\ell n(p)$ modulo $N(K) + \nabla_{LT}(LT(K))$ does not vanish at p.

Conclusion : *for any $p \in T(K)$, the smallest ∇_{LT}-submodule N/K such that $\partial\ell n(p) \in N(K) + LT(\mathbb{C})$ is LH, where H is the smallest alg. subgroup of T such that $p \in H + T(\mathbb{C})$.*

So, with H as above, we derive : $deg.tr(F_p/K) = dim(H)$.

2. Abelian Manin-Chai and its use.

A/S abelian scheme $\rightsquigarrow A/K$, with $K/\mathbb{C}$-trace $A_0/\mathbb{C}$.
$p \in A(S) = A(K) \rightarrow x$ " $=$ " $\ell n_A(p) \in LA$, analytic on some disk.
But if $A \neq A_0$, no connection on $LA = Lie(A)$ killing the periods (i.e. the ambiguity on ℓn_A). So, we must introduce the universal vectorial extension $\tilde{A}$, with its Gauss-Manin connection $\nabla_{L\tilde{A}}$:

$$0 \rightarrow W_A \rightarrow \tilde{A} \rightarrow A \rightarrow 0, \ \nabla_{L\tilde{A}} : L\tilde{A} \rightarrow L\tilde{A}$$

where $W_A = H^1(A, O_A)^*$. The periods of $\tilde{A}$ ($\simeq$ quasiperiods of A) generate $(L\tilde{A})^\nabla$ over $\mathbb{C}$.
Lift p to $\tilde{p} \in \tilde{A}$. Then, $\partial \ell n_{\tilde{A}}(\tilde{p}) := \nabla_{L\tilde{A}}(\ell n_{\tilde{A}}(\tilde{p}))$ is well defined, and its class modulo $\nabla_{L\tilde{A}}(L\tilde{A}(K))$ depends only on $p \rightsquigarrow$ the Manin map

$$M_K : A(K) \rightarrow L\tilde{A}(K)/\nabla_{L\tilde{A}}(L\tilde{A}(K)) = Coker(\nabla_{L\tilde{A}}; K).$$

$K(\ell n_{\tilde{A}}(\tilde{p})) = K(\int_0^p \eta, \eta \in H^1_{dR}(A/K))$ depends on the path, so we must introduce $F_A = K((L\tilde{A})^\nabla)$. And now,

$$F_p := F_A(\ell n_{\tilde{A}}(\tilde{p})) = F_A(\tilde{x}),\ \tilde{x} = \ell n_{\tilde{A}}(\tilde{p})$$

depends only on p. Let $n = dim(A)$, so $dim(\tilde{A}) = 2n$.

Theorem ($\sim$ André) : *$tr.deg.(F_p/F_A) < 2n \Rightarrow \ \exists$ alg. subgroup $H \subsetneq A$ such that $p \in H(K) + A_0(\mathbb{C})$.*

Proof in 2 steps, based on the logarithmic derivative

$$\partial\ell n_{\tilde{A}}(\tilde{p})) := \nabla_{L\tilde{A}}(\ell n_{\tilde{A}}(\tilde{p})) \in L\tilde{A}(K).$$

View $\tilde{x} = \ell n_{\tilde{A}}(\tilde{p})$ as *any* solution of the inhomogeneous equation

$$\nabla_{L\tilde{A}}(\tilde{x}) = \partial\ell n_{\tilde{A}}(\tilde{p}).$$

• **1st step** (Picard-Vessiot theory) Take any $a \in L\tilde{A}(K)$ and consider the inhomogeneous equation $\nabla_{L\tilde{A}}(\tilde{x}) = a$. Then, *$Gal_\partial(F(\tilde{x}))/F) = N^\nabla \subset (L\tilde{A})^\nabla$, where N/K is the smallest $\nabla_{L\tilde{A}}$-submodule of $L\tilde{A}$ such that $a \in N(K) + \nabla_{L\tilde{A}}(L\tilde{A}(K))$.*

Proof **and** statement use the *semi-simplicity* of the ∇-module $L\tilde{A}$.

$deg.tr.(F_p/F_A) < 2n \Rightarrow \exists N \subsetneq L\tilde{A}, \partial\ell n_{\tilde{A}}(\tilde{p}) \in N(K) + \nabla_{L\tilde{A}}(L\tilde{A}(K))$.

- **2nd step** (Hodge structure) : analogue of $\partial\ell n(K^*) \hookrightarrow K/\partial K$ is

$$\text{(Manin)} \ : \ Ker(M_K) = A_{tor} + A_0(\mathbb{C}) \ (= \text{ points of height } 0).$$

And in fact ($\sim$ Manin-Chai) : for any strict $\nabla_{L\tilde{A}}$-submodule N/K of $L\tilde{A}$, the "Manin-Chai map"

$$\overline{M}_K : A(K) \to Coker\{\nabla_{L\tilde{A}/N} : (L\tilde{A}/N)(K) \to (L\tilde{A}/N)(K)\}$$

sending p to the class of $\partial\ell n(\tilde{p})$ modulo $N(K) + \nabla_{L\tilde{A}}(L\tilde{A}(K))$ does not vanish on the set of *non-degenerate p's* (same def. as above).

Conclusion : *for any $p \in A(K)$, the smallest $\nabla_{L\tilde{A}}$-submodule N/K such that $\partial\ell n(\tilde{p}) \in N(K) + \nabla_{L\tilde{A}}(L\tilde{A}(K))$ is $L\tilde{H}$, where H is the smallest alg. subgroup of A such that $p \in H + A_0(\mathbb{C})$.*

So, with H as above, we derive $deg.tr(F_p/F_A) = 2dim(H)$.

The proof of Manin-Chai requires André's *normality theorem on VMHS*: the differential Galois group is a normal subgroup of the generic Mumford-Tate group. Therefore, N is stable under MT_A, hence carries a sub-Hodge structure of $L\tilde{A}$, hence is of the form $L\tilde{H}$.

Remark 1 : further work by J. Ayoub : *Une version relative de la conjecture des périodes de Kontsevich-Zagier* (Ann. Math., 2013).

Remark 2 (current work with A. Pillay, answering a question of Hrushovski) : assume that A is simple and traceless.

i) Then, $M_K \otimes 1_{\mathbb{Q}}$ is injective on $A(K) \otimes \mathbb{Q}$, and by Manin-Chai,

$$\boxed{M_K \otimes 1_{\mathbb{C}} : A(K) \otimes \mathbb{C} \hookrightarrow L\tilde{A}(K)/\nabla_{L\tilde{A}}(L\tilde{A}(K))}.$$

ii) Following Buium, model theory uses another Manin map :

$$\mu : A(K) \to L\tilde{A}/\nabla_{L\tilde{A}}(W_A) \simeq_{DAG} \mathbb{G}_a^n.$$

$Ker(\mu) = A_{tor}$, but $\exists A, Ker(\mu \otimes 1_{\mathbb{C}}) \neq 0$.

II. RMM for semi-abelian surfaces

S is now an affine curve over $\overline{\mathbb{Q}}$, $K = \overline{\mathbb{Q}}(S)$. If A/S is an abelian scheme, we let A_{tor} be the union of all torsion points on all fibers $A_\lambda, \lambda \in S(\overline{\mathbb{Q}})$.

In David's talk, we learnt :

Theorem (Masser-Zannier) : *let A/S be an abelian surface scheme, and let $s \in A(S)$ be a section of A/S. Assume that the set $\{\lambda \in S(\overline{\mathbb{Q}}), s(\lambda) \in A_{tor}\}$ is infinite. Then, s factors through a strict subgroup scheme of A/S.*

With an eye on "Pell units in non-maximal orders" (cf. Part III), we would like this to hold for generalized jacobians, in particular semi-abelian surface schemes, such as an S-extension

$$1 \to \mathbb{G}_m \to G \to E \to 0$$

of an elliptic scheme E/S by $\mathbb{G}_m$.

However, there are counterexamples to RMM for certain semi-abelian G's, due to the existence of "Ribet sections" when E has complex multiplications. But they are the only obstruction :

Theorem ([B-M-P-Z]) : *let G/S be an extension of E/S by $\mathbb{G}_m$, and let $s \in G(S)$ be a section of G/S. Assume that the set $\{\lambda \in S(\overline{\mathbb{Q}}), s(\lambda) \in G_{tor}\}$ is infinite. Then,*
i) either s is a Ribet section;
ii) or s factors through a strict subgroup scheme H of G/S.

In particular, the standard RMM Conclusion (ii) holds as soon as E/S is not isoconstant.

Proof : exactly the same strategy as Masser-Zannier, reducing to the transcendence degree of $\ell n_G(s)$ over F_G. More precisely :

let $q \in Pic^0_{E/S}(S) \simeq E(S)$ be the section parametrizing $G \in Ext_S(E, \mathbb{G}_m)$, and let $p \in E(S)$ be the projection of s to E, arbitrarily lifted to $\tilde{p}, \tilde{q}$ in $\tilde{E}(S)$. Then,

$$F_p = F_E(\ell n_{\tilde{E}}(\tilde{p})), F_G = F_E(\ell n_{\tilde{E}}(\tilde{q})) = F_q, F_{pq} := F_p.F_q.$$

Set $L_s := F_{pq}(\ell n_G(s))$ $(= F_G(\ell n_{\tilde{G}}(\tilde{s})).)$ Rather than L_s/F_G, it suffices to concentrate on

$$tr.deg(L_s/F_{pq}), \text{ which is } \leq dim(\mathbb{G}_m).$$

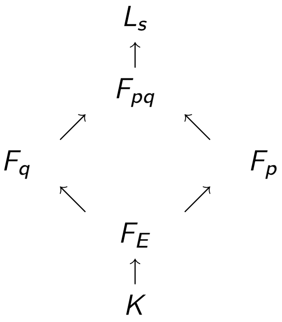
G/K admits a $K/\mathbb{C}$-trace G_0 = "constant part" of G, $\mathbb{G}_m \subset G_0$.

Proposition : *Assume that $tr.deg(L_s/F_{pq}) < 1$. Then, there exists a constant section $s_0 \in G_0(\mathbb{C})$ such that*

i) either $s - s_0$ is a Ribet section;
ii) or $s - s_0$ factors through a strict subgroup scheme of G/S.

Proof : compute commutators in the Galois representation

$$\{\gamma \in Gal_\partial(L_s/K)\} \to \rho_{G,s}(\gamma) = \begin{pmatrix} 1 & {}^t\xi_q(\gamma) & \tau_s(\gamma) \\ 0 & \rho_E(\gamma) & \xi_p(\gamma) \\ 0 & 0 & 1 \end{pmatrix}, \quad \text{where}$$



$$\begin{gathered} \tau_s : Gal_\partial(L_s/F_{pq}) \hookrightarrow (L\mathbb{G}_m)^\nabla \simeq \mathbb{C} \\ {}^t\xi_q : Gal_\partial(F_q/F_E) \hookrightarrow (L\tilde{E})^\nabla \simeq \mathbb{C}^2 \\ \xi_p : Gal_\partial(F_p/F_E) \hookrightarrow (L\tilde{E})^\nabla \simeq \mathbb{C}^2 \\ \rho_E : Gal_\partial(F_E/K) \hookrightarrow SL_2(\mathbb{C}) \end{gathered}$$

$\tau_s = 0$ forces a CM relation between p and q (unless they are torsion or constant sections of E/S) $\rightsquigarrow$ a Ribet section of G/S.

III. Non-square free polynomial (Pell-) Fermat equations

SECOND DÉFI AUX MATHÉMATICIENS, FÉVRIER 1657.

Il est à peine quelqu'un qui propose des questions purement arithmétiques, il est à peine quelqu'un qui sache les résoudre. J'attends la solution de ces questions; si elle n'est fournie ni par l'Angleterre, ni par la Gaule Belgique ou Celtique, elle le sera par la Narbonnaise, qui l'offrira à Sir Digby et la lui dédiera en gage d'une amitié naissante.
Pour éclairer leur marche, je leur propose de démontrer comme théorème ou de résoudre comme problème l'énoncé suivant; s'ils y parviennent, ils reconnaîtront au moins que des questions de ce genre ne le cèdent ni pour la subtilité, ni pour la difficulté, ni pour le mode de démonstration, aux plus célèbres de la Géométrie :

Étant donné un nombre non carré quelconque, il y a une infinité de carrés déterminés tels qu'en ajoutant l'unité au produit de l'un d'eux par le nombre donné, on ait un carré.

[Oeuvres de Fermat, Tannery - Henry , p. 312, No 81.]

So, for any $D \in \mathbb{Z}_{>0}$, D not a square,

$$X^2 - DY^2 = 1$$

has at least one (hence infinitely many) solutions $X, 0 \neq Y \in \mathbb{Z}$. Of course, we now see this as a theorem on units of orders in a real quadratic field. Notice that the order needs not be maximal, so the non-square D can have square factors.

Now, replace $\mathbb{Z}$ by $\mathbb{C}[t]$, with a polynomial $D(t)$ of even degree.

Let $D \in \mathbb{C}[t]$ be a polynomial of degree 6 , not a square in $\mathbb{C}[t]$, and let C be the normalization of the curve $w^2 = D(t)$, with two points ∞_+, ∞_- at infinity. We have just seen in David's talk that *if D has no multiple root* (i.e. is square free, i.e. genus$(C) = 2$), then the "polynomial Pell-Fermat equation"

$$X^2 - DY^2 = 1$$

has a solution in polynomials $\{X, 0 \neq Y\} \in \mathbb{C}[t]$ if and only if the divisor $(\infty_+) - (\infty_-)$ is a torsion point on the Jacobian $A = Pic^0_C$ of C, and that RMM for a family of abelian surfaces A_λ implies :

Corollary (Masser-Zannier) : *consider the family of polynomials $D_\lambda(t) = t^6 + t + \lambda$, where λ runs through $\mathbb{C}$. There are only finitely many complex numbers λ such that there exist polynomials $X(t), 0 \neq Y(t) \in \mathbb{C}[t]$ satisfying $X^2(t) - D_\lambda(t)Y^2(t) \equiv 1$.*

Now, what happens if $D_\lambda(t)$ is (generically) not square-free ? For instance, what about the family of polynomials

$$D_\lambda(t) = t^2(t^4 + t + \lambda) \quad ?$$

More generally, let $\rho(\lambda)$ be an algebraic function of λ, defining a Rieman surface S, and consider the family $C/S = \{C_\lambda, \lambda \in S\}$ of singular curves $v^2 = (t - \rho(\lambda))^2(t^4 + t + \lambda)$. The normalisation of C_λ is the (normalisation of the) curve of genus 1 :

$$(E_\lambda) : w^2 = \Delta_\lambda(t), \text{ with } \Delta_\lambda(t) = t^4 + t + \lambda.$$

We recover C_λ by pinching E_λ at its points $\{q_+(\lambda), q_-(\lambda)\}$ with abscissa $t = \rho(\lambda)$.

The generalized jacobian $G^q = G = Pic^0_{C/S}$ identifies with the group of relative divisors of degree 0 on E/S prime to $\{q_+, q_-\}$, modulo the strict equivalence $\approx$, which for $f \in K(E)$, is defined by

$$div(f) \approx 0 \Leftrightarrow f(q_+)/f(q_-) = 1.$$

Identifying the usual jacobian $Pic^0_{E/S}$ (defined via the standard equivalence of divisors $\sim$) with E/S, we have an S-extension

$$1 \to \mathbb{G}_m \to G \to E \to 0,$$

whose class in $\hat{E}(S) \simeq E(S)$ is given by $(q_+) - (q_-)$.

Consider the two points $\infty_+(\lambda), \infty_-(\lambda)$ on E_λ, and let

$s(\lambda) =$ class of $(\infty_+(\lambda)) - (\infty_-(\lambda))$ for $\approx$, i.e. in G_λ,
$p(\lambda) =$ class of $(\infty_+(\lambda)) - (\infty_-(\lambda))$ for $\sim$, i.e. in $\hat{E}_\lambda \simeq E_\lambda$;

So, $p \in E(S)$ is the projection of the section $s \in G(S)$.

As we have just learnt, the family of elliptic curves E/S (marked at ∞_+) is not isoconstant, and p is not a torsion section, so ("likely intersections") : there is an *infinite set* Λ_p of (necessarily algebraic) values of λ for which $p(\lambda) \in E_{tor}$, equivalently

$\lambda \in \Lambda_p \Rightarrow X^2 - \Delta_\lambda \tilde{Y}^2 = 1$ solvable in $X, 0 \neq \tilde{Y} \in \mathbb{C}[t]$

For $\lambda \in \Lambda_p$, denote by $f = f_\lambda = X(t) + w\tilde{Y}(t)$ a rational function on E_λ with $(f) = N.(\infty_+(\lambda)) - N.(\infty_-(\lambda))$, where $\mathrm{ord}(p(\lambda))|N$.

Since $D_\lambda(t) = (t - \rho(\lambda))^2\Delta_\lambda(t)$, D_λ is "Pell solvable" iff Δ_λ has a Pell solution $X, \tilde{Y}$ with $\tilde{Y}(\rho(\lambda)) = 0$, which occurs iff one of these f's satisfies $f(q_+(\lambda)) = f(q_-(\lambda))$, so iff

$$s(\lambda) \in G_{tor},$$

i.e. ("unlikely intersections") iff s lifts the torsion point $p(\lambda)$ to a torsion point on G_λ. By RMM on G/S (and since E has no CM), this may occur only if s factor through a strict subgroup scheme H/S of G/S. Now,

- if $G = G^q$ is not isosplit, H^0 must be $\mathbb{G}_m$, so p must be torsion, which it is not $\Rightarrow$ *D_λ is Pell solvable for only finitely many λ's.*

• if $G^q \sim \mathbb{G}_m \times E$, i.e. $\exists \phi \in K(E)$, with $(\phi) =$ a multiple of $(q_+) - (q_-)$: since p is not torsion, s will then factor iff its "isoprojection" to $\mathbb{G}_m$, which is given by $\phi(\infty_+)/\phi(\infty_-) \in K^*$, is a root of unity.

In our example with $\rho(\lambda) = 0$, the extension G^q is not isosplit. Indeed, $q_\pm(\lambda) = (0, \pm\sqrt{\lambda})$ while by Serre-Tate, torsion sections do not ramify at $\lambda = 0$. We derive :

Corollary ([B-M-P-Z]) : *consider the family of polynomials $D_\lambda(t) = t^2(t^4 + t + \lambda)$, where λ runs through $\mathbb{C}$. There are only finitely many complex numbers λ such that there exist polynomials $X(t), 0 \neq Y(t) \in \mathbb{C}[t]$ satisfying $X^2(t) - D_\lambda(t)Y^2(t) \equiv 1$.*

Or better said : there are infinitely many complex λ's such that $X^2 - (t^4 + t + \lambda)\tilde{Y}^2 = 1$ has a solution $X, 0 \neq \tilde{Y} \in \mathbb{C}[t]$, but only finitely many produce a solution with $\tilde{Y}(0) = 0$.