Introduction to the Ax-Schanuel property

Claudel BERTHET

May 26, 2008

Abstract

Here is an introduction to the talks of Jonathan Kirby and Piotr Kowalski about the Ax-Schanuel property, given in La Roche, April 2008, during the Modnet training workshop. The reader will find here a synthesis of the main part of both talks, the effort being placed on their common features. One should refer to the documents edited by the speakers for technical details and more examples. I want to thank the speakers for their help in answering several questions.

The Lindemann-Weierstrass theorem states that if $x_1, \ldots, x_n$ are algebraic numbers over $\mathbf{Q}$, then the transcendence degree of $e^{x_1}, \ldots, e^{x_n}$ is n, thereby gathering the transcendence of π and e in a single statement. Schanuel's conjecture is a direct attempt to generalize this result : if the x_i's contribute to the trancendance degree, what can we say ?

Conjecture (Schanuel)**.** *Let $x_1, \ldots, x_n \in \mathbf{C}$, such that the x_i's are $\mathbf{Q}$-linearly independent. Then the transcendence degree of $x_1, \ldots, x_n, e^{x_1}, \ldots, e^{x_n}$ over the rationals is at least n.*

Now let $\mathcal{M}(\mathbf{C})$ be the field of meromorphic functions on the complex plane, i.e. the field of fractions of the ring of holomorphic functions on the plane. The field $\mathcal{M}(\mathbf{C})$ can naturally be equiped with the derivation $\partial := \frac{\partial}{\partial_z}$. For every $f \in \mathcal{M}(\mathbf{C})$, the differential equation $\frac{\partial(exp \circ f)}{exp \circ f} = \partial f$ is satisfied in $\mathcal{M}(\mathbf{C})$. Besides, in a characteristic zero filed, $\mathbf{Q}$-linear dependence is equivalent to $\mathbf{Z}$-linear dependence.

The Ax theorem is an analogue of Schanuel's conjecture for differential fields in characteristic zero. It retains from the relation between x and e^x the differential equation $\frac{\partial y}{y} = \partial x$, and for technical reasons the transcendence degree, which is taken on C, the field of constants of the differential field (K, ∂), is increased by 1 in the formulation. Now for $x_i, \ldots, x_n, y_1, \ldots, y_n \in K$ such that for all i $\frac{\partial y_i}{y_i} = \partial x_i$, one has $\partial(\prod_i y_i^{m_i}) = (\prod_i y_i^{m_i}) \sum_i m_i \partial(x_i)$, so one has $\sum_i m_i x_i \in C \Leftrightarrow \partial(\sum_i m_i x_i) = 0 \Leftrightarrow \partial(\prod_i y_i^{m_i}) = 0 \Leftrightarrow \prod_i y_i^{m_i} \in C$. Hence the Ax's theorem is stated as follows.

Theorem (Ax)**.** *Suppose $n \geq 1$, $\partial x_i = \frac{\partial y_i}{y_i}$ for $i = 1, \ldots, n$, and $td(x_1, y_1, \ldots, x_n, y_n/C) < n + 1$. Then there are $m_i \in \mathbf{Z}$, not all zero, such that $\prod_{i=1}^n y_i^{m_i} \in C$.*

The Generalized Schanuel Property in characterictic zero

A geometric version of Ax's theorem

This theorem may be restated in more geometric terms. In order to see it, we introduce the tangent bundle and space of a commutative algebraic group.

Definition (Tangent bundle and space)**.** Let V be a variety over a field F. Another variety TV is a tangent bundle of V, if for any F-algebra R, there is a functorial bijection between $V(R[X]/(X^2))$ and $TV(R)$. Because there is a copy of K in $K[X]/(X^2)$, there is a projection homomorphism $TG \to G$: if P is an R-rational point of V, then the tangent space of the variety $V(R)$ at P is the fiber of the projection $TV \to V$ over P (seen in $V(R[X]/(X^2))$).

Now if G is an algebraic group over a field F, the tangent space at the identity is called the Lie algebra of G.

Proposition. *If G is a commutative algebraic group over a field F, there is an isomorphism between TG and $LG \times G$.*

So from now on, we will identify TG and $LG \times G$. We must notice that if $dim(G) = n$, then $LG \cong \mathbf{G}_a^n$, so we have the canonical identification $\mathbf{G}_a^n \times \mathbf{G}_m^n \cong L\mathbf{G}_m^n \times \mathbf{G}_m^n \cong T\mathbf{G}_m^n$. As before let (K, ∂) be a differential field of characteristic zero, and C its field of constants : the condition $\frac{\partial y}{y} = \partial x$ defines a subgroup Γ of $\mathbf{G}_a \times \mathbf{G}_m$: so the hypothesis on the x_i's and y_i's are replaced by the choice of a tuple in Γ. Next we remark that to the "independence" condition $\prod_{i=1}^n y_i^{m_i} \in C$ corresponds a (commutative) subgroup H of $\mathbf{G}_m^n$, defined by the equation $\prod_{i=1}^n y_i^{m_i} = 1$, so the condition is equivalent to the statement that $\overline{y}$ lies in a C-coset of an algebraic subgroup H of $\mathbf{G}_m^n$. For such an H, the Lie algebra of H is given by the equation $\sum_i m_i x_i = 0$ (remember $(\mathbf{x} = (x_1, \ldots, x_n), \mathbf{y})$ is a tuple in Γ); again the condition $\sum_i m_i x_i$ is equivalent to the statement that $\mathbf{x}$ lies in a C-coset of LH. So the condition on $\mathbf{y}$ is equivalent to a condition on $(\mathbf{x}, \mathbf{y})$, an element of $T\mathbf{G}_m^n$ as we noted before. Finally, the condition on the transcendence degree is replaced by the hypothesis that $(\mathbf{x}, \mathbf{y})$ lies in an algebraic suvariety of $\mathbf{G}_a^n \times \mathbf{G}_m^n$ of dimension $< n + 1$, and we have the

Theorem (Ax's theorem - version 2)**.** *Let V be an algebraic subvariety of $\mathbf{G}_a^n \times \mathbf{G}_m^n$ defined over C, of dimension $dimV < n + 1$ and $(\mathbf{x}, \mathbf{y}) \in \Gamma^n \cap V$. Then $(\mathbf{x}, \mathbf{y}) \in TH(K) + \gamma$, where H is a proper algebraic subgroup of $\mathbf{G}_m^n$ and $\gamma \in T\mathbf{G}_m^n(C)$.*

The exponential differential equation of an algebraic group

Where have we got so far ? We have started from the exponential function, an analytic (épi)morphism from $\mathbf{C}$ onto $\mathbf{C}^*$, two complex Lie groups, the first being the Lie algebra of the second. From this function we got a differential equation $\frac{\partial y}{y} = \partial x$ satisfied by the exponential of every element of the differential field of meromorphic functions. From the solution set of this "exponential" differential equation was then extracted a tuple, upon the transcendence degree (on the constants field) of which is formulated Ax's theorem property. We broaden the setting again. One can check that if K is a field, a map $\partial : K \to K$ is a derivation if and only if the map $K \to K[X]/(X^2)$, $a \mapsto a + \partial(a)X$ is a ring homomorphism. In other words, the structure of a derivation map and a tangent bundle are both "encoded" in the dual numbers construction. In this situation, if C is the field of constants of (K, ∂), and G an algebraic group over C, the map ∂ gives a (K, ∂) definable homomorphism ∂_G from $G(K)$ to $G(K[X]/(X^2)) \cong TG(K)$. In this case we have seen that there is a canonical projection map π from $TG(K) \cong LG(K) \times G(K)$ to $LG(K)$. Composing ∂_G with this projection one gets a map $l\partial_G := \pi \circ \partial_G : G(K) \to LG(K)$, which we call the "logarithmic derivative map", to which is associated the "exponential differential equation of G".

$$l\partial_{LG}(x) = l\partial_G(y).$$

Notice here that $LLG = LG$ so that $l\partial_{LG}$ is from $LG(K)$ to $LG(K)$.

The Generalized Schanuel Property

Once this is said, to each algebraic group we can then associate Γ_G, the solution set in K of its exponential differential equation, thus appealing to another generalization of Ax's result. The decomposition of commutative connected algebraic groups of Chevalley gives in the case of vector groups a counterexample to this generalization, but we have the following, true in particular for semiabelian varieties.

Theorem (Generalized Schanuel Property)**.** *Let G be a nvq-group of dimension n, defined over the field of constants C of a differential field (K, ∂) of characteristic zero, and $\Gamma_G \subseteq TG(K)$ the solution set of the exponential differential equation of G. Let $(x, y) \in \Gamma_G \cap V$, where V is an algebraic subvariety of $TG(K)$ defined over C, and of dimension $dimV < n + 1$. Then there exists a proper algebraic subgroup H of G and an element $\gamma \in TG(C)$ such that $(x, y) \in TH(K) + \gamma$.*

At this point we should explain the "extra 1" which appears in the transcendence degree in Ax's theorem and the generalized Schanuel property. With the above notations, we first define the group rank of x over C ($grk_C(x)$), as the dimension of the largest subgroup H of G such that x lies in a C-coset of LH (In the case where G is a torus, this is just the Q-linear dimension of the Q-vector space $\langle x, C\rangle/C$ (the quotient space)). For a point $(x, y) \in \Gamma_G$, we then define a quantity $\delta_C(x, y) := td_C(x, y) - grk_C(x)$. This δ is a first approximation to the dimension of the pair (x, y) in an appropriate pregeometry. Schanuel's conjecture is that $\delta \geq 0$. It follows from Schanuel's conjecture (and in the case of differential fields is Ax's theorem) that $\delta(x, y) \geq dim(x, y)$ where dim is the dimension in the sense of this pregeometry. In the differential fields case, C is the closure of the empty set. So if $\delta(x, y) = 0$ then in fact (x, y) has dimension 0 over C, so (since C is closed), actually lies in C. Hence if (x, y) does not lie in C, it must be that $dim(x, y) \geq 1$, and here is the extra 1. (In this case, we are assuming that x does not lie in any such coset, which means that $grk_C(x) = n$.)

The Ax-Schanuel Property in characteristic p

The essentials of the characteristic zero case

In this part, (K, ∂) is a differential field of characteristic zero and of field of constants C.

In the first section, we dealt with the exponential differential equation of a commutative algebraic group. This equation was somehow "lifted up" from an analytic morphism, the complex exponential function. This is a particular case of the differential equation associated to an analytic homomorphism. To find a suitable generalization of Schanuel's property in characteristic p, where the exponential function does not exist, one needs to look at the general setting in order to search for suitable analogs.

If A and B are commutative algebraic groups defined over C and $G := A \times B$, we have the logarithmic derivative maps $l\partial_A : A \to LA$ and $l\partial_B : B \to LB$. Now if $f : A \to B$ is an algebraic homomorphism of groups, the functor L (Lie algebra) induces a linear map $Lf : LA \to LB$, and the logarithmic derivative is a natural transformation between the identity functor and the L functor on commutative algebraic groups; in other words, one has $Lf \circ l\partial_A = l\partial_B \circ f$. The differential equation of f is then defined from this natural condition as $Lf(l\partial_A(x)) = l\partial_B(y)$, and its solution set Γ_f is a definable subgroup of $G(K)$.

Of course the exponential function was not an algebraic morphism, but this setting somehow generalizes to analytic morphisms, since the map f does not appear in the definition of its differential equation ! Indeed, if $\mathbf{C} \subseteq C$, and A and B are defined over $\mathbf{C}$, then the analytical structure of $\mathbf{C}$ makes $A(\mathbf{C})$ and $B(\mathbf{C})$ complex Lie groups, and every algebraic morphism between them is analytic. In general, if $f : A(\mathbf{C}) \to B(\mathbf{C})$ is an analytic homomorphism, we can still associate to f a linear map $Lf := f'_0 : LA(\mathbf{C}) \to LB(\mathbf{C})$, where 0 is the identity of $A(\mathbf{C})$. Tensorization lifts up this map to a K-linear map $Lf : LA(K) \to LB(K)$. In this context, even if the morphism f does not lift up to K, because K has no topology in order to speak about analycity, we still can speak about the differential equation of f, given by the information

translated in Lf: $Lf(l\partial_A(x)) = l\partial_B(y)$, and then about the solution set Γ_f, still a definable subgroup of $G(K)$. For example in general there exists an analytic epimorphism $exp_B : LB(\mathbf{C}) \to B(\mathbf{C})$, the universal covering of $B(\mathbf{C})$. In this case, the differential equation associated is the exponential differential equation of the first section.
All this allows to give a still more general version of Schanuel's property, which an analytic morphism would satisfy or not. In the first section case, we considered automatically the exponential case, where A was the Lie algebra of B, so in this version we need to replace the clause of the conclusion concerning $TH(K)$ and γ by a suitable one: the proper algebraic subgroup H of G and its tangent bundle TH are replaced by proper algebraic subgroups $A_0 < A$ and $B_0 < B$ over C, and $TG(C)$ is replaced by $A(C)$ and $B(C)$. This allows the

Definition (Ax-Schanuel Property in characteristic zero)**.** With the same notations, assuming that $\mathbf{C} \subseteq C$ and $f : A(\mathbf{C}) \to B(\mathbf{C})$ is a local analytic homomorphism, we say that Γ_f, the solution set in K of the differential equation of f, has the Ax-Schanuel property, if whenever $(a, b) \in \Gamma_f$ and $td_C(a, b) \leq n$, then there are proper algebraic subgroups $A_0 < A$ and $B_0 < B$ defined over C, such that $a \in A_0(K) + A(C)$ and $b \in B_0(K) + B(C)$.

Ax's theorem says exactly that the exponential function from $\mathbf{G}_a^n$ to $\mathbf{G}_m^n$ has the Ax-Schanuel property, while the Ax-Schanuel property for exp_A for an nvq-group A is the generalized Schanuel property of the first section.

Towards the characteristic p case

Having extracted somewhat the "essence" of the Schanuel property in characteristic zero, one would want to consider this property in characteristic p : more precisely, are there some kind of "analytic" morphisms having the "Ax-Schanuel" property ? Several problems arise in characteristic p; the absence of an analytic structure (what is an analytic morphism ?) and the fact that the statement of Ax is meaningless : if (K, ∂) is a differential field of char p, then for each $x = y^p \in K^p$, the derivation rule implies $\partial(x) = p\partial(y)y^{p-1} = 0$, so $K^p \subseteq C$ and K is algebraic over C ($X^p - x^p$ algebraizes x).
The trick is to get rid of the "problem" by "correcting" the iterations of the derivation by a multiplicative factor. For instance, if ∂ is the derivation on $\mathcal{M}(\mathbf{C})$, let $\partial^{(n)}$ denote the n-th iteration of ∂, and let $D_0 := id$, and $D_n := \frac{1}{n!}\partial^{(n)}$, for $n \geq 1$. In other words, the sequence $(D_n)_{n<\omega}$ "extracts" from a holomorphic function f the sequence $D_n(f)$ of coefficient-functions of the power series expansion of f. The D_i's have the following properties :

. D_0 is the identity map

. Each D_n is additive

. $D_n(xy) = \sum_{i+j=n} D_i(x)D_j(y)$ for all n, x, y (Leibniz rule)

. $D_i \circ D_j = \binom{i+j}{i} D_{i+j}$ for all i, j (iterativity condition)

This turns out to be the suitable generalization of a derivation on a field in characteristic p.

Definitions (Hasse-Schmidt derivation, Hasse field)**.** Let K be a field. A sequence D of maps $D_n : K \to K$, $n < \omega$, satisfying the preceding conditions, is called a Hasse-Schmidt derivation on K. The constant field is the field $C := \bigcap_{n>0} ker(D_n)$. Such a field is called a Hasse field.

In general, the field K is not algebraic over C, and this is the context in which we look for an analog of the Ax-Shanuel property.
We defined in the first section a tangent bundle of a variety through the ring of dual numbers $R[X]/(X^2)$, remarking that this ring was somehow canonically associated to the structure of a derivation on a ring. In similar fashion, a sequence of maps $D := (D_i)_{i<\omega}$ from a field K to itself is a Hasse-Schmidt derivation if and only if the map $K \to K[[X]]$, $a \mapsto \sum_{i<\omega} D_i(a)X^i$ is a ring homomorphism and D satisfies the iterativity condition. Thus in the Hasse fields setting, the role played by $R[X]/(X^2)$ in a differential field for a C-algebra R, will be played by the ring $R[[X]]$ of formal power series. Now we have a canonical isomorphism between $R[[X]]$ and the projective limit of the rings $R[X]/(X^n)$, so we can define an analog of the tangent bundle in the HS setting. From now on let (K, D) be a Hasse field of field of constants C.

Definitions (Arc spaces)**.** Let V be a variety defined over C. The n^{th} arc space of V is a variety $Arc^n(V)$ satisfying a functorial bijection $Arc^n(V)(R) \longleftrightarrow V(R[X]/(X^{n+1}))$, for every C-algebra R. The full arc space of V, $Arc(V)$ is then defined as the projective limit of the $Arc^n(V)$'s. It is a pro-algebraic variety.

Remember that the Lie algebra LG of an algebraic group G was defined as the fiber over the identity of the tangent bundle TG. The equivalent in Hasse fields is defined in the same way, as the fiber U_G over the identity of the projection homomorphism $Arc(G) \to G$, where G is an algebraic group defined over C. If G is commutative, then we still have a canonical isomorphism $Arc(G) \cong U_G \times G$.
Now the logarithmic derivative map on a group $G(K)$ was also introduced in the differential setting through a definable homomorphism from $G(K)$ to $TG(K)$. Similarly in the HS setting, if G is an algebraic group defined over C, the HS derivation D induces a (K, D)-type-definable homomorphism D_G from $G(K)$ to $G(K[[X]]) \cong Arc(G)(K)$. But we have an analog projection π from $Arc(G)(K)$ to $U_G(K)$, so by composing we can define the full logarithmic derivative $lD_G := \pi \circ D_G : G(K) \to U_G(K)$.

The last task is to find an equivalent of an "analytic morphism" between two algebraic groups defined over C, and to the "differential equation" of such a morphism. Concerning the maps, the key notions are those of a formal group law and a formal homomorphism between such group laws. The idea is that the product of a Lie group has a formal power series expansion at the identity, of a certain form, and that in general this kind of formal power series defines a group product.

Definitions (Formal group)**.** A one-dimensional formal group law over a commutative ring R is a power series $F(x, y)$ with coefficients in R, such that

. $F(x, y) = x + y +$ terms of higher degree

. $F(x, F(y, z)) = F(F(x, y), z)$ (associativity)

An n-dimensional formal group law is an n-tuple of power series $F_i(x_1, \ldots, x_n, y_1, \ldots, y_n)$ in $2n$ variables, such that

. $\mathbf{F}(\mathbf{x}, \mathbf{y}) = \mathbf{x} + \mathbf{y} +$ terms of higher degree

. $\mathbf{F}(\mathbf{x}, \mathbf{F}(\mathbf{y}, \mathbf{z})) = \mathbf{F}(\mathbf{F}(\mathbf{x}, \mathbf{y}), \mathbf{z})$

where $\mathbf{F}$ is for $(F_1, ..., F_n)$, $\mathbf{x}$ for $(x_1, ..., x_n)$.

There is a notion of homomorphim between such groups.

Definition. Let $\mathbf{F}$ and $\mathbf{G}$ be formal group laws of dimension m and n, respectively. A homomorphism $\mathbf{f}$ from $\mathbf{F}$ to $\mathbf{G}$ is an n-tuple of power series in m variables, such that $\mathbf{G}(\mathbf{f}(\mathbf{x}), \mathbf{f}(\mathbf{y})) = \mathbf{f}(\mathbf{F}(\mathbf{x}, \mathbf{y}))$.

This allows to introduce a formal analog of "analycity" where there is no topology to speak about Lie groups. In characteristic zero, there is an equivalence of categories between finite dimensional Lie algebras and formal group laws. In characteristic p this is not true, and formal group laws are used instead of Lie algebras to avoid loss of information.
Now in generality, to each algebraic group G can be canonically associated a formal group law. The reader interested in formal group laws can find more informations on them in www.wikipedia.org [formal group law]. Analytic maps between Lie groups will then be replaced in the HS setting by formal homomorphisms between algebraic groups, i.e. between their "canonical formal group laws", because in generality a formal homomorphism between algebraic groups still induces a linear map between the Lie algebras of the groups.

The HS-differential Ax-Schanuel property

We are then led to consider the generalized set-up in which we will state the "Generalized Ax-Schanuel Property". (K, D) is still a Hasse field with constants field C; A and B are commutative algebraic groups defined over C, and $G := A \times B$.
A formal homomorphism $f : A \to B$ still induces a pro-algebraic homomorphism U_f from U_A to U_B. Again, although there is no extension of the map f to $A(K)$ and $B(K)$ in general, we still may speak of the HS-differential equation of f, all the ingredients being present : $U_f(lD_A(x) = lD_B(y)$. Its solution set is still named Γ_f, a subgroup of $G(K)$, type-definable in (K, D). This amounts to say that we may state the "HS differential Ax-Schanuel property"; in particular, it will have a proper meaning in characteristic p.

Definition 0.1 (HS-differential Ax-Schanuel Property)**.** With the same notations, assuming that $f : A \to B$ is a formal homomorphism, we say that Γ_f, the solution set in K of the HS-differential equation of f, has the HS-differential Ax-Schanuel property, if whenever $(a, b) \in \Gamma_f$ and $td_C(a, b) \leq n$, then there are proper algebraic subgroups $A_0 < A$ and $B_0 < B$ defined over C, such that $a \in A_0(K) + A(C)$ and $b \in B_0(K) + B(C)$.

Remark that we have not assumed that the characteristic of K is p. The trick already mentionned allows to "transform" any derivation on a field into a "Hasse-Schmidt derivation"; in characteristic zero, the HS-differential Ax-Schanuel property is in this way exactly the classical Ax-Schanuel property, so this is a true generalization.
In characteristic p however, the groups $U_{\mathbf{G}_a}$ and $U_{\mathbf{G}_m}$ are not isomorphic, so there is no nontrivial formal homomorphism between $\mathbf{G}_a$ and $\mathbf{G}_m$, and the exponential map does not exist in this setting. Hence, the exponential differential equation, which was the motivation for Ax's theorem and its successive generalizations, has no equivalent in Hasse fields in characteristic p. So one must ask if certain other formal homomorphisms in characteristic p have the HS-differential Ax-Schanuel property. Some candidates are $f = \sum_{i=0}^{\infty} c_i X^{p^i}$ on $\mathbf{G}_a$ (where the c_i's $\in C$), $f = lim_n (X+1)^{\sum_{i=0}^{n} a_i p^i} - 1$ on $\mathbf{G}_m$ (where $\sum_{i=0}^{\infty} a_i p^i$ is any p-adic number), and a formal isomorphism f between $\mathbf{G}_m$ and an ordinary elliptic curve E.