

On the Ax-Schanuel property in arbitrary characteristic

Piotr Kowalski

Instytut Matematyczny Uniwersytetu Wrocławskiego
Institut Camille Jordan, Université Lyon 1

La Roche Modnet Workshop, 20-25 April 2008

Set-up

In this characteristic 0 section we have:

- (K, ∂) a differential field of characteristic 0.
- $C := \partial^{-1}(0)$ the field of constants.
- A, B commutative algebraic groups defined over C .
- $G := A \times B$.
- $\dim(A) = \dim(B) := n$.
- LA is the tangent space of A at 0. L is a functor – for any algebraic homomorphism $f : A \rightarrow B$, we have $Lf : LA \rightarrow LB$.
- $l\partial_A : A(K) \rightarrow LA(K)$ the logarithmic derivative map.
- $\ker(l\partial_A) = A(C)$.

The differential equation of an algebraic map

Assume $f : A \rightarrow B$ is an algebraic homomorphism defined over C .

The following diagram is commutative (naturality of $l\partial$):

$$\begin{array}{ccc} LA(K) & \xrightarrow{Lf} & LB(K) \\ l\partial_A \uparrow & & \uparrow l\partial_B \\ A(K) & \xrightarrow{f} & B(K) \end{array}$$

The differential equation of f

- The **differential equation of f** is $Lf(l\partial_A(x)) = l\partial_B(y)$.
- Its solution set Γ_f is a (K, ∂) -definable subgroup of $G(K)$.
- By the diagram above and $\ker(l\partial_G) = G(C)$, we have $\Gamma_f = \text{graph}(f) + G(C)$: the graph of f blurred by constants.

Local analytic maps

Assume $\mathbb{C} \subseteq C$ and A, B are defined over \mathbb{C} .

Complex Lie groups

- $A(\mathbb{C}), B(\mathbb{C})$ are complex manifolds with group operations given by holomorphic maps, so they are **complex Lie groups**.
- Let $f : A(\mathbb{C}) \rightarrow B(\mathbb{C})$ be a (local) analytic homomorphism. Then we still have a \mathbb{C} -linear map $Lf = f'_0 : LA(\mathbb{C}) \rightarrow LB(\mathbb{C})$.
- By tensoring, we get a K -linear map $Lf : LA(K) \rightarrow LB(K)$.

Example

$\exp : \mathbb{G}_a(\mathbb{C}) \rightarrow \mathbb{G}_m(\mathbb{C})$ is an analytic homomorphism. Since $\mathbb{G}_a(\mathbb{C}), \mathbb{G}_m(\mathbb{C})$ are open in \mathbb{C} , we identify $L\mathbb{G}_a(\mathbb{C}) = \mathbb{C} = L\mathbb{G}_m(\mathbb{C})$. Since $\exp'(0) = \exp(0) = 1$, we have $L\exp = \text{id}$.

The differential equation of an analytic map

Remark

There is no map $f : A(K) \dashrightarrow B(K)$, since there is no convergence notion in K ! Therefore, we only have the following diagram:

$$\begin{array}{ccc} LA(K) & \xrightarrow{Lf} & LB(K) \\ \uparrow l\partial_A & & \uparrow l\partial_B \\ A(K) & & B(K) \end{array}$$

The differential equation of f

- The **differential equation of f** is $Lf(l\partial_A(x)) = l\partial_B(y)$.
- Its solution set Γ_f is a (K, ∂) -definable subgroup of $G(K)$.
- Γ_f may be thought of as the graph of the non-existing $f : A(K) \dashrightarrow B(K)$ blurred by constants.

Some analytic maps and their differential equations

Example (Analytic maps)

- ① Any algebraic map $f : A(\mathbb{C}) \rightarrow B(\mathbb{C})$.
- ② There exists an analytic epimorphism $\exp_B : LB(\mathbb{C}) \rightarrow B(\mathbb{C})$.
Topologically, \exp_B is the universal covering map.
- ③ For $\gamma \in \mathbb{C}$, the local map $\mathbb{G}_m(\mathbb{C}) \ni x \mapsto x^\gamma \in \mathbb{G}_m(\mathbb{C})$.
- ④ For E an elliptic curve, $\exp_E : LE(\mathbb{C}) \rightarrow E(\mathbb{C})$ factors through $\mathbb{G}_m(\mathbb{C})$ to give an analytic epimorphism $r : \mathbb{G}_m(\mathbb{C}) \rightarrow E(\mathbb{C})$.

Example (Differential equations)

- ① $\Gamma_f = \text{graph}(f) + G(C)$.
- ② $\Gamma_{\exp_B} = \Gamma_B$ (Γ_B as in Jonathan's talk).
- ③ $\Gamma_{x \mapsto x^\gamma} : \frac{\partial x}{x} = \gamma \frac{\partial y}{y}$.
- ④ $\Gamma_r : \frac{\partial x}{x} = \frac{\partial y}{z}$, where $(y, z) \in E(K)$.

The differential equation of the exponential map

Example (An analytic solution)

Let $\mathcal{A}(\mathbb{C})$ be the ring of holomorphic functions on \mathbb{C} with a natural derivation ∂_z and $\mathcal{M}(\mathbb{C})$ its field of fractions (meromorphic functions). Then $\exp \in \mathcal{M}(\mathbb{C})$ and $\partial_z(\exp) = \exp$, so the pair $(\text{id}_{\mathbb{C}}, \exp)$ satisfies the differential equation of the exponential map.

Example (A formal solution)

We consider $C[[X]]$, $\exp(X) := \sum \frac{X^i}{i!}$ and a natural derivation

$$\partial\left(\sum_{i=0}^{\infty} a_i X^i\right) = \sum_{i=0}^{\infty} a_{i+1}(i+1)X^i.$$

$(X, \exp(X))$ satisfies the differential equation of the exponential map.

Definition of the Ax-Schanuel property

Let $f : A(\mathbb{C}) \rightarrow B(\mathbb{C})$ be a local analytic homomorphism.

Definition

We say that Γ_f has **the Ax-Schanuel property** if

- $(a, b) \in \Gamma_f$ and $\text{trdeg}_C(a, b) \leq n$

implies

- there are proper algebraic subgroups $A_0 < A, B_0 < B$ over C such that $a \in A_0(K) + A(C)$ and $b \in B_0(K) + B(C)$.

Remark

- If $A = \mathbb{G}_a^n$ and there is $B_0 \not\cong B$ such that $b \in B_0(K) + B(C)$, then there is $A_0 \not\cong A$ such that $a \in A_0(K) + A(C)$. Hence having B_0 alone is enough to get the Ax-Schanuel property.
- If $f = \exp_B$, then we can take $A_0 = LB_0$ as in Jonathan's talk.

Formal maps and the Ax-Schanuel property

- $\exp_{\mathbb{G}_m^n}$ has the Ax-Schanuel property (Ax's theorem).
- \exp_A has the Ax-Schanuel property for A semi-abelian (Jonathan's talk) and even for A with no vectorial quotients.
- Any analytic epimorphism from an algebraic torus to an abelian variety has the Ax-Schanuel property.
- Raising to power γ on \mathbb{G}_m^n has the Ax-Schanuel property, if $[\mathbb{Q}(\gamma) : \mathbb{Q}] > n$.
- Raising to power $\sqrt{2}$ on \mathbb{G}_m^2 DOES NOT have the Ax-Schanuel property.
- Algebraic maps $f : A \rightarrow B$ DO NOT have the Ax-Schanuel property. Take $a \in A(K)$ which is NOT in a constant coset of a proper subgroup. Still $(a, f(a)) \in \Gamma_f$, $\text{trdeg}_C(a, f(a)) \leq n$.

About proofs of the Ax-Schanuel property

The proofs (except the raising to power case) do not differ much from the one given in Jonathan's talk.

- One gets a C -algebraic subgroup $H < A \times B$ such that WLOG $(a, b) \in H(K)$, $H_A := H \cap A \neq A$, $H_B := H \cap B \neq B$.
- In many cases H has to be of the form $H_A \times H_B$, done.
- Let us deal with the case \exp_B , B has no vectorial quotients.
- Let H^B be the image of H by projection to B (similarly H^A). It is enough to show $H^B \neq B$. Assume $H^B = B$.
- Then H induces an algebraic epimorphism $H^A \twoheadrightarrow B/H_B$.
- But $H^A \leq A = LB \cong \mathbb{G}_a^n$, so H^A is a vector group.
- Hence B/H_B is a vector group, being an image of H^A and nontrivial, so B has a vectorial quotient, a contradiction.

Hasse-Schmidt derivations needed

Problem

Assume $\text{char}(K) = p > 0$. Then for each $x \in K^p$, $\partial(x) = 0$, so K is algebraic over $C \supseteq K^p$ and the statement of Ax is meaningless, since $\text{trdeg}_C(x)$ is always 0.

Solution

Replace the derivation ∂ with a **Hasse-Schmidt derivation** (**HS-derivation**) $D = (D_n : K \rightarrow K)_{n < \omega}$, i.e.

- 1 D_0 is the identity map,
- 2 each D_n is additive,
- 3 $D_n(xy) = \sum_{i+j=n} D_i(x)D_j(y)$ (Leibniz rule),
- 4 $D_i \circ D_j = \binom{i+j}{i} D_{i+j}$ (iterativity condition).

Let C be the constant field of **all** D_n , i.e. $C := \bigcap_{n > 0} \ker(D_n)$. Then K is usually not algebraic over C .

What has really happened?

Derivations as homomorphisms

A map $\partial : K \rightarrow K$ is a derivation if and only if the map $K \ni a \mapsto a + \partial(a)X \in K[X]/(X^2)$ is a ring homomorphism.

HS-derivations as homomorphisms

A sequence of maps $D = (D_i : K \rightarrow K)_{i < \omega}$ is an HS-derivation if and only if $D_0 = \text{id}_K$, the map $K \ni a \mapsto \sum D_i(a)X^i \in K[[X]]$ is a ring homomorphism and D satisfies the iterativity condition.

Moral

We always have to make the following replacement:

$$K[X]/(X^2) \rightsquigarrow K[[X]].$$

What happens to the tangent space after the replacement?

Let V be a C -variety and R a C -algebra.

A new interpretation of the tangent space

The tangent space TV satisfies the following canonical bijection

$$TV(R) \longleftrightarrow V(R[X]/(X^2)).$$

The space of arcs

- The n^{th} -arc space of V , $\text{Arc}^n(V)$, is a variety satisfying the following canonical bijection

$$\text{Arc}^n(V)(R) \longleftrightarrow V(R[X]/(X^{n+1})).$$

- Since $R[[X]] = \varprojlim R[X]/(X^n)$, the role of the tangent space is played by the **full arc space** $\text{Arc}(V) := \varprojlim \text{Arc}^n(V)$, which is a pro-algebraic variety. Note that $\text{Arc}^1(V) = TV$.

What happens to LG after the replacement?

Let G be a commutative algebraic group over C .

Relation between LG and TG

Recall from Jonathan's talk:

- 1 TG is a commutative algebraic group.
- 2 The projection map $TG \rightarrow G$ is a group homomorphism.
- 3 LG is the fiber over 0 of the projection map.
- 4 TG canonically decomposes as $LG \times G$.

U_G is the HS-replacement of LG

- 1 $\text{Arc}(G)$ is a commutative pro-algebraic group.
- 2 The projection map $\text{Arc}(G) \rightarrow G$ is a group homomorphism.
- 3 Let U_G denote the fiber over 0 of the map $\text{Arc}(G) \rightarrow G$.
- 4 $\text{Arc}(G)$ canonically decomposes as $U_G \times G$.

More on $\text{Arc}(G)$ and U_G

Let G be a commutative algebraic group over C and $m < \omega$.

U_G is pro-unipotent

- Let U_G^m denote the fiber over 0 of the map $\text{Arc}^m(G) \rightarrow G$.
- There is an exact sequence of algebraic groups:

$$0 \rightarrow LG \rightarrow U_G^{m+1} \rightarrow U_G^m \rightarrow 0.$$

- Therefore U_G^m is unipotent, so U_G is pro-unipotent.

Remark

One computes the group law of $\text{Arc}^m(G)$ by formally HS-differentiating the group law of G .

The group laws of $U_{\mathbb{G}_a}^m$ and $U_{\mathbb{G}_a}$

- Start from $X + Y$, the group law of \mathbb{G}_a .
- Compute formally: $D_i(X + Y) = D_i(X) + D_i(Y)$, $i \leq m$.
- Let us denote the variables related to $\text{Arc}^m(\mathbb{G}_a)$ by:

$$X = D_0(X), X' := D_1(X), \dots, X^{(m)} := D_m(X).$$

- The group law of $\text{Arc}^m(\mathbb{G}_a)$ is given by:

$$(X, \dots, X^{(m)}) + (Y, \dots, Y^{(m)}) = (X + Y, \dots, X^{(m)} + Y^{(m)}),$$

$$\text{so } \text{Arc}^m(\mathbb{G}_a) \cong \mathbb{G}_a^{m+1}.$$

- The group law of $U_{\mathbb{G}_a}^m$ is given by the group law in $\text{Arc}^m(\mathbb{G}_a)$ AFTER plugging $X = Y = 0$ ($U_{\mathbb{G}_a}^m$ is the fiber over 0):

$$(0, X', \dots, X^{(m)}) + (0, Y', \dots, Y^{(m)}) = (0, X' + Y', \dots, X^{(m)} + Y^{(m)}),$$

$$\text{so } U_{\mathbb{G}_a}^m \cong \mathbb{G}_a^m \text{ and } U_{\mathbb{G}_a} \cong \mathbb{G}_a^\infty.$$

The group law of $U_{\mathbb{G}_m}^m$

- Start from XY , the group law of \mathbb{G}_m .
- Compute formally: $D_i(XY) = \sum_{k+l=i} D_k(X)D_l(Y)$, $i \leq m$.
- Let $X, X', \dots, X^{(m)}$ be the $\text{Arc}^m(\mathbb{G}_m)$ -variables as before.
- The group law of $\text{Arc}^m(\mathbb{G}_m)$ is given by:

$$\begin{aligned} & (X, X', \dots, X^{(m)}) + (Y, Y', \dots, Y^{(m)}) = \\ & = (XY, X'Y + Y'X, \dots, \sum_{k+l=m} X^{(k)} Y^{(l)}). \end{aligned}$$

- The group law of $U_{\mathbb{G}_m}^m$ is given by the group law of $\text{Arc}^m(\mathbb{G}_m)$ AFTER plugging $X = Y = 1$ ($U_{\mathbb{G}_m}^m$ is the fiber over 1):

$$\begin{aligned} & (1, X', \dots, X^{(m)}) + (1, Y', \dots, Y^{(m)}) = \\ & = (1, X' + Y', \dots, X^{(m)} + Y^{(m)} + \sum_{i=1}^{m-1} X^{(i)} Y^{(m-i)}). \end{aligned}$$

The group laws of $U_{\mathbb{G}_a}$ and $U_{\mathbb{G}_m}$

Another interpretation of $U_{\mathbb{G}_a}$

- $\text{Arc}(\mathbb{G}_a)(C) = \mathbb{G}_a(C[[X]])$.
- $U_{\mathbb{G}_a}(C) = \ker[\mathbb{G}_a(C[[X]]) \rightarrow \mathbb{G}_a(C)]$.
- $U_{\mathbb{G}_a}(C) = (XC[[X]], +) \cong \mathbb{G}_a^\infty(C)$.

Another interpretation of $U_{\mathbb{G}_m}$

- $U_{\mathbb{G}_m}(C) = \ker[\mathbb{G}_m(C[[X]]) \rightarrow \mathbb{G}_m(C)]$.
- $U_{\mathbb{G}_m}(C) = (1 + XC[[X]], \cdot) \cong \mathbb{G}_a(W(C))$.
- $W(C)$ is the ring of infinite **Witt vectors** over C . For example $W(\mathbb{F}_p) = \mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ – the ring of **p -adic integers**.
- Since $\text{char}(W(C)) = 0$, the group $U_{\mathbb{G}_m}(C) \cong \mathbb{G}_a(W(C))$ is torsion-free, so $U_{\mathbb{G}_a} \not\cong U_{\mathbb{G}_m}$, since $U_{\mathbb{G}_a} \cong \mathbb{G}_a^\infty$ is p -torsion.

Full logarithmic derivative

Derivation case

- 1 $\partial : K \rightarrow K[X]/(X^2)$ gives a (K, ∂) -definable homomorphism

$$\partial_G : G(K) \rightarrow G(K[X]/(X^2)) = TG(K)$$

- 2 After composing with the projection map $TG(K) \rightarrow LG(K)$ we get the logarithmic derivative $l\partial_G : G(K) \rightarrow LG(K)$.

HS-derivation case

- 1 The HS-derivation $D : K \rightarrow K[[X]]$ induces a $*$ -definable in (K, D) homomorphism

$$D_G : G(K) \rightarrow G(K[[X]]) = \text{Arc}(G)(K).$$

- 2 After composing with the projection $\text{Arc}(G)(K) \rightarrow U_G(K)$ we get the **full logarithmic derivative** $ID_G : G(K) \rightarrow U_G(K)$.

Full logarithmic derivatives on \mathbb{G}_a and \mathbb{G}_m

Example (\mathbb{G}_a)

The full logarithmic derivative on \mathbb{G}_a is:

$$\mathbb{G}_a(K) \ni a \mapsto (D_i(a))_{i < \omega} \in U_{\mathbb{G}_a}(K) = \mathbb{G}_a^\infty(K).$$

Example (\mathbb{G}_m)

The full logarithmic derivative on \mathbb{G}_m is:

$$\mathbb{G}_m(K) \ni a \mapsto \left(\frac{D_i(a)}{a} \right)_{i < \omega} \in U_{\mathbb{G}_m}(K) = \mathbb{G}_a(W(K)).$$

Set-up

In the HS-differential case we have:

- (K, D) a field with an HS-derivation.
- $C := \bigcap_{i>0} \ker(D_i)$ the absolute field of constants.
- A, B commutative algebraic groups defined over C .
- $G := A \times B$.
- $\dim(A) = \dim(B) := n$.
- U_A is again a functor – for any algebraic homomorphism $f : A \rightarrow B$, we have a pro-algebraic map $U_f : U_A \rightarrow U_B$.
- $ID_A : A(K) \rightarrow U_A(K)$ the full logarithmic derivative map.
- $\ker(ID_A) = A(C)$.

How to replace a local analytic map (derivation case)?

- The differential equation came from a map $LA(K) \rightarrow LB(K)$ induced by a local analytic map $A(\mathbb{C}) \rightarrow B(\mathbb{C})$.
- Over any field C , we can talk about **formal homomorphisms** between A and B . For example $\exp(X) = \sum \frac{X^i}{i!}$ is a formal homomorphism between \mathbb{G}_a and \mathbb{G}_m , because:

$$\exp(X+Y) = \sum_{i=0}^{\infty} \frac{(X+Y)^i}{i!} = \sum_{i=0}^{\infty} \frac{X^i}{i!} \cdot \sum_{i=0}^{\infty} \frac{Y^i}{i!} = \exp(X) \cdot \exp(Y).$$

- Formal homomorphisms between A and B still induce actual linear maps $LA \rightarrow LB$ (and there is a 1-to-1 correspondence).
- Therefore, we can replace local analytic homomorphisms by formal homomorphisms.

How to replace a local analytic map (HS-derivation case)?

Similarities between characteristic 0 and positive characteristic

Formal homomorphisms between A and B still induce pro-algebraic homomorphisms $U_A \rightarrow U_B$, so we can use them.

Differences between characteristic 0 and positive characteristic

- $U_{\mathbb{G}_a} \not\cong U_{\mathbb{G}_m}$, so in particular there is no formal isomorphism between \mathbb{G}_a and \mathbb{G}_m . This means that the exponential map DOES NOT exist in positive characteristic.
- There may be more maps between U_A and U_B than formal homomorphisms between A and B . E.g. the ring of formal endomorphisms of \mathbb{G}_m is $\mathbb{Z}_p = W(\mathbb{F}_p)$ (Manin) and the ring of pro-algebraic endomorphisms of $U_{\mathbb{G}_m}$ over C is $W(C)$.

Formal maps

Example

- Any sequence $(c_i \in \mathbb{C})_{i < \omega}$ gives a formal endomorphism of \mathbb{G}_a

$$\sum_{i=0}^{\infty} c_i X^{p^i}.$$

- For any p -adic number $\sum_{i=0}^{\infty} a_i p^i$ the sequence

$$((X + 1)^{\sum_{i=0}^n a_i p^i} - 1)_{n < \omega}$$

converges to a non-algebraic formal endomorphism of \mathbb{G}_m .

- There is a formal isomorphism between \mathbb{G}_m and an ordinary elliptic curve E . The analytic epimorphism $r : \mathbb{G}_m(\mathbb{C}) \rightarrow E(\mathbb{C})$ „survives“ to positive characteristic (unlike \exp).

The HS-differential equation of a formal map

Assume f is a formal map between A and B and let $U_f : U_A \rightarrow U_B$ be the induced pro-algebraic homomorphism. Again, there is no map $f : A(K) \dashrightarrow B(K)$, so we only have the following diagram:

$$\begin{array}{ccc} U_A(K) & \xrightarrow{U_f} & U_B(K) \\ \uparrow ID_A & & \uparrow ID_B \\ A(K) & & B(K) \end{array}$$

The HS-differential equation of f

- The **HS-differential equation of f** is $U_f(ID_A(x)) = ID_B(y)$.
- Its solution set $\Gamma_f \leq G(K)$ is type-definable in (K, D) .
- Again, Γ_f may be thought of as the graph of the non-existing $f : A(K) \dashrightarrow B(K)$ blurred by constants.

Some HS-differential equations

Example

We will hopefully compute on the board Γ_f for:

- $f = \sum_{i=0}^{\infty} c_i X^{p^i}$ on \mathbb{G}_a .
- $f = \lim_n (X + 1)^{\sum_{i=0}^n a_i p^i} - 1$ on \mathbb{G}_m .

The HS-differential Ax-Schanuel property

Let f be a formal homomorphism between A and B .

Definition

We say that Γ_f has **the Ax-Schanuel property** if

- $(a, b) \in \Gamma_f$ and $\text{trdeg}_C(a, b) \leq n$

implies

- there are proper algebraic subgroups $A_0 < A, B_0 < B$ over C such that $a \in A_0(K) + A(C)$ and $b \in B_0(K) + B(C)$.

Not much is known

Proving the HS-differential Ax-Schanuel property for certain formal homomorphisms is work in progress. The candidates are:

- $f = \sum_{i=0}^{\infty} c_i X^{p^i}$ on \mathbb{G}_a .
- $f = \lim_n (X + 1)^{\sum_{i=0}^n a_i p^i} - 1$ on \mathbb{G}_m .
- A formal isomorphism f between \mathbb{G}_m and an ordinary elliptic curve E . This is the best candidate, since it is NOT a limit of algebraic homomorphisms between \mathbb{G}_m and E (each such is 0), so f is „very“ non-algebraic.

Vojta's HS-differential forms

In the proof from Jonathan's talk the **module** of differential forms Ω was crucial. Here, the role of Ω is played by the **graded ring** of HS-differential forms introduced by Vojta.

Let $m < \omega$, V be an affine C -variety and R be a C -algebra.

HS-differential forms

- $\text{HS}_{R/C}^m$ is the R -algebra generated by the set of symbols $\{d_i a \mid i \leq m, a \in R\}$ and subject to the relations:
 - 1 $d_i(x + y) = d_i x + d_i y, \quad x, y \in R, \quad i \leq m;$
 - 2 $d_i(c) = 0, \quad c \in C;$
 - 3 $d_i(xy) = \sum_{k+l=i} d_k x \cdot d_l y, \quad x, y \in R, \quad i \leq m.$
- $\text{HS}_{R/C}^1 \cong S(\Omega_{R/C})$ – the symmetric algebra.
- $C[\text{Arc}^m(V)] \cong \text{HS}_{C[V]/C}^m$.
- In particular $C[TV] \cong \text{HS}_{C[V]/C}^1 = S(\Omega_{C[V]/C})$.

HS-forms and the Ax-Schanuel property

Time permitting, I will try to explain the connection between the HS-forms and the Ax-Schanuel property.