Transcendence in positive characteristic

Piotr Kowalski

Instytut Matematyczny
Uniwersytetu Wrocławskiego

May 22, 2010

Definable transcendence

Definable conditions

$$\Downarrow$$

Algebraic independence

Ax-Schanuel situation

- K: a field (possibly with extra structure),
- C: a (type-)definable subfield,
- A, B: algebraic groups over C of dimension n (a positive integer n is fixed in this talk),
- $\Gamma < A(K) \times B(K)$: a (type-)definable subgroup,
- $(x, y) \in \Gamma$

Ax-Schanuel type of statement

If x is linearly independent modulo C, then

$$\mathrm{trdeg}_C(x, y) \geqslant n + 1.$$

Ax's theorem

- (K, ∂): a differential field of characteristic 0,
- $C = \partial^{-1}(0)$: the field of constants,
- $A = \mathbb{G}_{\mathrm{a}}^n$, $B = \mathbb{G}_{\mathrm{m}}^n$,
- $\Gamma = \{(x_1, \ldots, x_n, y_1, \ldots, y_n) \mid \partial x_1 = \frac{\partial y_1}{y_1}, \ldots, \partial x_n = \frac{\partial y_n}{y_n}\}$,
- $(x, y) \in \Gamma$

Ax's theorem

If x is linearly independent over $\mathbb{Q}$ modulo C, then

$$\mathrm{trdeg}_C(x, y) \geqslant n + 1.$$

Motivating case

- $K = C((t))$, $\partial = \partial_t$, $\mathrm{char}(C) = 0$,
- $C = \partial^{-1}(0)$,
- $x = (x_1, \ldots, x_n)$, $x_i \in tC[\![t]\!]$,
- $y = (y_1, \ldots, y_n)$, $y_i = \exp(x_i)$,
- $\partial_t(\exp(x_i)) = \partial_t(x_i)\exp(x_i)$, so $(x, y) \in \Gamma$.

Theorem (Power Series Schanuel's Conjecture, Ax)

If $x_1, \ldots, x_n$ are linearly independent over $\mathbb{Q}$, then

$$\mathrm{trdeg}_{C(t)}(x_1, \ldots, x_n, e^{x_1}, \ldots, e^{x_n}) \geqslant n.$$

Logarithmic derivative

- Consider

$$l\partial : \mathbb{G}_{\mathrm{m}}(K) \to \mathbb{G}_{\mathrm{a}}(K), \ \ l\partial(x) = \frac{\partial x}{x}.$$

  This is a definable homomorphism which is called logarithmic derivative.

- Clearly

$$\partial : \mathbb{G}_{\mathrm{a}}(K) \to \mathbb{G}_{\mathrm{a}}(K)$$

  is also a definable homomorphism.

Differential equation of exp

$$\begin{CD} \mathbb{G}_\mathrm{a}(K) @>{\cdot \exp'(0)}>> \mathbb{G}_\mathrm{a}(K) \\ @A{\partial}AA @AA{l\partial}A \\ x \in \mathbb{G}_\mathrm{a}(K) @. y \in \mathbb{G}_\mathrm{m}(K) \end{CD}$$

Since $\exp'(0) = 1$, x and y go to the same thing in the diagram above if and only if $(x, y) \in \Gamma$ ($n = 1$ here).

Ax's theorem in the torus case (char=0)

- (K, ∂): a differential field of characteristic 0,
- $C = \partial^{-1}(0)$: the field of constants,
- $A = \mathbb{G}_{\mathrm{m}}^n$, $B = \mathbb{G}_{\mathrm{m}}^n$,
- $\alpha \in C$ such that $[\mathbb{Q}(\alpha) : \mathbb{Q}] > n$,
- $\Gamma = \{(x_1, \ldots, x_n, y_1, \ldots, y_n) \mid \frac{\partial x_1}{x_1} = \alpha \frac{\partial y_1}{y_1}, \ldots, \frac{\partial x_n}{x_n} = \alpha \frac{\partial y_n}{y_n}\}$,
- $(x, y) \in \Gamma$.

Theorem (K.)

If x is multiplicatively independent modulo C, then

$$\mathrm{trdeg}_C(x, y) \geqslant n + 1.$$

Independence conditions

The following are equivalent:

1. x is multiplicatively independent modulo C, i.e. for each non-zero tuple $k_1, \ldots, k_n \in \mathbb{Z}$ we have $x_1^{k_1} \ldots x_n^{k_n} \notin C$.
2. For any proper subtorus $T < \mathbb{G}_{\mathrm{m}}^n$ and $c \in \mathbb{G}_{\mathrm{m}}^n(C)$ we have $x \notin cT(K)$.
3. $l\partial(x)$ is linearly independent over $\mathbb{Q}$.

If $\partial(x) = l\partial(y)$ (the Ax's theorem case), then TFAE:

1. y is multiplicatively independent modulo C.
2. $\partial(x)$ is linearly independent over $\mathbb{Q}$.
3. x is linearly independent over $\mathbb{Q}$ modulo C.

The field $\mathbb{Q}$ appears here as fractions of $\mathbb{Z} = \mathrm{End}_{\mathrm{alg}}(\mathbb{G}_{\mathrm{m}})$.

Differential equation of raising to power α

$$
\begin{array}{ccc}
\mathbb{G}_{\mathrm{a}}(K) & \xrightarrow{\cdot (X^{\alpha})'(1)} & \mathbb{G}_{\mathrm{a}}(K) \\
\Big\uparrow {\scriptstyle l\partial} & & \Big\uparrow {\scriptstyle l\partial} \\
x \in \mathbb{G}_{\mathrm{m}}(K) & & y \in \mathbb{G}_{\mathrm{m}}(K)
\end{array}
$$

Since $(X^{\alpha})'(1) = \alpha$, x and y go to the same thing in the diagram above if and only if $(x, y) \in \Gamma$.

Non-algebraicity of α

- Taking e.g. $\alpha = 1$ clearly does not yield any transcendence.
- There is always a counterexample to the "torus-Ax" if $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leqslant n$.
- To see the analogy with the positive characteristic cases (coming soon), notice that if we think of α as $X^\alpha \in \mathrm{End}_{\mathrm{formal}}(\mathbb{G}_{\mathrm{m}})$, then the non-algebraicity of α over $\mathbb{Q}$ corresponds to the non-algebraicity of X^α over $\mathrm{End}_{\mathrm{alg}}(\mathbb{G}_{\mathrm{m}})$.

Additive case

- K: a field of characteristic $p > 0$ (no derivation),
- $C = K^{p^\infty}$: a type definable subfield,
- $A = \mathbb{G}_a^n$, $B = \mathbb{G}_a^n$,
- $\Gamma < A(K) \times B(K)$: a type-definable subgroup,
- linear independence comes from $C[\mathrm{Fr}] = \mathrm{End}_{\mathrm{alg}}(\mathbb{G}_a)$, the ring of additive polynomials (with composition),
- $C[\mathrm{Fr}]$ is isomorphic to the Frobenius skew-polynomial ring, so it is commutative if and only if $C = \mathbb{F}_p$.

What is Γ?

Let

$$F = \sum_{m=0}^{\infty} c_m X^{p^m} \in C[\![\mathrm{Fr}]\!].$$

Take $(x, y) \in A(K) \times B(K)$. Then $(x, y) \in \Gamma$ if and only if:

$$y_i - c_0 x_i \in K^p,$$

$$y_i - c_0 x_i - c_1 x_i^p \in K^{p^2},$$

$$\ldots$$

$$y_i - c_0 x_i - c_1 x_i^p - \ldots - c_m x^{p^m} \in K^{p^{m+1}},$$

$$\ldots$$

Additive Ax's theorem

We assume that:

- F is sufficiently non-algebraic (to be explained later) over $C[\mathrm{Fr}]$ (as α before in the characteristic 0 torus case),
- $(x, y) \in \Gamma$.

Theorem (K.)

If x is linearly independent over $C[\mathrm{Fr}]$ modulo C, then

$$\mathrm{trdeg}_C(x, y) \geqslant n + 1.$$

Non-algebraicity of F

Characteristic 0 torus: the condition for α

We have $\alpha \in C = \mathrm{End}_{\mathrm{formal}}(\mathbb{G}_{\mathrm{m}})$ which should have algebraic degree greater than n over $\mathbb{Z} = \mathrm{End}_{\mathrm{alg}}(\mathbb{G}_{\mathrm{m}})$.

Characteristic p additive group: the condition for F

We have $F \in C[\![\mathrm{Fr}]\!] = \mathrm{End}_{\mathrm{formal}}(\mathbb{G}_{\mathrm{a}})$ which should have "algebraic degree" greater than n over $C[\mathrm{Fr}] = \mathrm{End}_{\mathrm{alg}}(\mathbb{G}_{\mathrm{a}})$.

- It makes proper sense if $C = \mathbb{F}_p$, so $C[\mathrm{Fr}]$ is commutative.
- Complicated for $C \neq \mathbb{F}_p$, something as

$$\alpha_{0,n}^{\pm 1} \circ F \circ \alpha_{1,n}^{\pm 1} \circ F \circ \ldots \circ F \circ \alpha_{n,n}^{\pm 1} + \ldots + \alpha_{0,1}^{\pm 1} \circ F \circ \alpha_{1,1}^{\pm 1} + \alpha_{0,0}^{\pm 1} \neq 0.$$

- Still treatable for C finite.

Additive Schanuel's Conjecture

The main case is:

Theorem

Assume $x_1, \ldots, x_n \in t\mathbb{F}_p[[t]]$ *are linearly independent over* $\mathbb{F}_p[\mathrm{Fr}]$*. Then*

$$\mathrm{trdeg}_{\mathbb{F}_p(t)}(x_1, \ldots, x_n, F(x_1), \ldots, F(x_n)) \geqslant n.$$

Carlitz exponential

Transcendence statements of similar forms were already obtained starting from Carlitz's work (1935).

Example

The Carlitz exponential is

$$\exp_C = X + \sum_{i=1}^{\infty} \frac{X^{p^i}}{(t^{p^i} - t)(t^{p^i} - t^p)\dots(t^{p^i} - t^{p^{i-1}})}$$

- Denis obtained some Schanuel-type results for $\exp_C$.
- Papanikolas proved a Carlitz version of the (still open) conjecture on algebraic independence of logarithms of algebraic numbers.

Our case vs Drinfeld modules

- The series $\exp_C$ is the simplest case of the Drinfeld exponential function (related to a Drinfeld module).
- The power series I consider do not fit in the Drinfeld modules framework, since they have constant coefficients, i.e. there is no transcendental element present.
- The Carlitz exponential $\exp_C$ is "algebraic" in our terminology since it satisfies the following functional equation:

$$\exp_C \circ \theta X = \theta X \circ \exp_C + X^p \circ \exp_C .$$

- The Drinfeld (or even Carlitz) version of Schanuel's conjecture is open.

HS-derivation version

- (K, ∂): a field of characteristic $p > 0$ with a Hasse-Schmidt derivation,
- Assume $K^{p^\infty} = \bigcap_{m>0} \ker(\partial_m)$,
- F induces a pro-algebraic homomorphism $U_F : \mathbb{G}_a^\infty \to \mathbb{G}_a^\infty$ corresponding to $(F', F^{(p)}, F^{(p^2)}, \ldots)(0)$.
- Γ is now also described by the following diagram:

$$\begin{array}{ccc} \mathbb{G}_a^\infty(K) & \xrightarrow{U_F} & \mathbb{G}_a^\infty(K) \\ \partial \uparrow & & \uparrow \partial \\ x \in \mathbb{G}_a(K) & & y \in \mathbb{G}_a(K) \end{array}$$

Γ in the multiplicative case

- Let K be a field of characteristic $p > 0$,
- $A = \mathbb{G}_{\mathrm{m}}^n$, $B = \mathbb{G}_{\mathrm{m}}^n$,
- Let $\gamma = \sum c_i p^i \in \mathbb{Z}_p$,
- $\Gamma < A(K) \times B(K)$ is defined by:

$$yx^{-c_0} \in K^p,$$

$$yx^{-c_0 - c_1 p} \in K^{p^2},$$

$$\ldots$$

$$yx^{-c_0 - c_1 p - \ldots - c_m p^m} \in K^{p^{m+1}},$$

$$\ldots$$

Ax's theorem in the torus case (char=p)

Assume:

- $K^{p^\infty} = \mathbb{F}_p$ (specified constants),
- $[\mathbb{Q}(\gamma) : \mathbb{Q}] > n$ (non-algebraicity condition),
- $(x, y) \in \Gamma$.

Theorem (K.)

If x is multiplicatively independent modulo $\mathbb{F}_p$, then

$$\mathrm{trdeg}_{\mathbb{F}_p}(x, y) \geqslant n + 1.$$

Formal endomorphisms of $\mathbb{G}_{\mathrm{m}}$

- $\mathrm{End}_{\mathrm{alg}}(\mathbb{G}_{\mathrm{m}}) = \mathbb{Z}$ as in the characteristic 0 case.
- But $\mathrm{End}_{\mathrm{formal}}(\mathbb{G}_{\mathrm{m}}) = \mathbb{Z}_p$ (p-adic integers).
- Why? We can go to the limit with powers of Frobenius and $\mathrm{Fr} \in \mathrm{End}_{\mathrm{alg}}(\mathbb{G}_{\mathrm{m}})$ corresponds to $p \in \mathbb{Z}$, so

$$\mathrm{End}_{\mathrm{formal}}(\mathbb{G}_{\mathrm{m}}) = \widehat{(\mathbb{Z}, p)} = \mathbb{Z}_p.$$

- Similarly in the additive case

$$\mathrm{End}_{\mathrm{formal}}(\mathbb{G}_{\mathrm{a}}) = (\widehat{C[\mathrm{Fr}], \mathrm{Fr}}) = C[\![\mathrm{Fr}]\!].$$

- The non-algebraicity condition for $\gamma \in \mathbb{Z}_p$ is exactly the same as before: a formal endomorphism should be non-algebraic enough over the algebraic ones.

HS-derivation version for torus

- (K, ∂): a field of characteristic $p > 0$ with an HS-derivation.
- The logarithmic derivative is now a homomorphism:

$$l\partial(x) = \left(\frac{\partial_1 x}{x}, \frac{\partial_2 x}{x}, \ldots\right)$$

$$l\partial : \mathbb{G}_{\mathrm{m}}(K) \to \mathbb{G}_{\mathrm{a}}(W(K)).$$

- Note that $\mathbb{Z}_p = W(\mathbb{F}_p)$. Γ is given by:

$$\begin{array}{ccc}
\mathbb{G}_{\mathrm{a}}(W(K)) & \xrightarrow{\ \cdot\gamma\ } & \mathbb{G}_{\mathrm{a}}(W(K)) \\
\uparrow{\scriptstyle l\partial} & & \uparrow{\scriptstyle l\partial} \\
x \in \mathbb{G}_{\mathrm{m}}(K) & & y \in \mathbb{G}_{\mathrm{m}}(K)
\end{array}$$

Multiplicative-elliptic case

Originally, I wanted to establish an Ax-Schanuel statement for a formal isomorphism between an ordinary elliptic curve and the multiplicative group. So far, I think, I can only do it when this isomorphism is defined over $\mathbb{F}_p$ which is probably never the case.