Galois descent in Galois theories

Daniel Bertrand
(Inst. Math. Jussieu)

I . The case of Kummer theory
(and applications to Diophantine Geometry)

II . The differential case
(and applications to Schanuel problems)

NDMTF, Durham, July 2009

I . Kummer theory on abelian varieties

• K = number field, $\overline{K}$ = algebraic closure.

• A = an abelian variety over K, $dimA := g$. Set $End(A/K) = End(A/\overline{K}) := \mathcal{O}$.

• $y \in A(K)$. Assume that y *generates* A, i.e. $\mathbb{Z}.y$ is Zariski closed in $A \Leftrightarrow Ann_{\mathcal{O}}(y) = 0$.

Following the elliptic work of Bashmakov and Tate-Coates ($\sim$ 1970), we have :

Theorem K : *there exists $c = c(A, K, y) > 0$ such that for all $n > 0$, $[K(\frac{1}{n}y) : K] \geq cn^{2g}$.*

Refs.: K. Ribet : Duke math. J. 46, 1979, 745-761;
D.B. : Proc. Durham Conference 1986, "New advances in transcendence theory", ed. A. Baker, CUP 1988, 37-55.

- $A_{tor} = \cup_n A[n], \ K_\infty = K(A_{tor})$

- $L_\infty = \cup_n K_\infty(\frac{1}{n}y), \quad L_{(\ell)} = \cup_m K_\infty(\frac{1}{\ell^m}y)$.

- $T_\infty(A) := proj.lim_n \ A[n] = \Pi_{\ell\in\mathcal{P}} T_\ell(A)$

We will actually prove that $Gal(L_\infty/K_\infty)$ *is isomorphic to an open subgroup of* $T_\infty(A)$, or equivalently (Nakayama) :

i) for all primes ℓ, $Gal(L_{(\ell)}/K_\infty)$ is an open subgroup of $T_\ell(A) \simeq \mathbb{Z}_\ell^{2g}$;

ii) for almost all ℓ, $Gal(K_\infty(\frac{1}{\ell}y)/K_\infty) \simeq A[\ell]$.

$$\begin{array}{cccc} \overline{K} & & & \\ | & & & \\ K_\infty(\frac{1}{n}y) & & \xi_y & \\ | & \}N & \hookrightarrow & A[n] \simeq (\mathbb{Z}/n\mathbb{Z})^{2g} \\ K_\infty & & \rho & \\ | & \}J & \hookrightarrow & GL(T_\infty(A)) \\ K & & & \end{array}$$

$$\xi_y(\sigma) = \sigma(\tfrac{1}{n}y) - \tfrac{1}{n}y, \quad \xi_y(\tau\sigma\tau^{-1}) = \tau(\xi_y(\sigma)).$$

Proof (in the mod ℓ case)

1. Galois theoretic step .
(Of necessity, base extension to $K_\infty \rightsquigarrow A$ becomes "K_∞-large" for the morphism $[\ell]_A$.)

$Im(\xi_y) \simeq N$ is a J-submodule of $A[\ell]$. Assume $N \neq A[\ell]$. Then $\exists \alpha \in \mathcal{O}, \alpha \notin \ell\mathcal{O}$ s.t.

$\alpha.y$ is divisible by ℓ in $A(K_\infty)$.

2. Galois descent

There exists $\ell_0(A, K)$ such that $\forall \ell > \ell_0$, if a point $y' \in A(K)$ is divisible by ℓ in $A(K_\infty)$, then, y' is already divisible by ℓ in $A(K)$, i.e.

$$A(K)/\ell.A(K) \hookrightarrow A(K_\infty)/\ell.A(K_\infty)$$

3. (Diophantine) geometric step

There exists $\ell_1(A, K, y)$ such that $\alpha.y \in \ell.A(K)$ with $\ell > \ell_1$ implies $\alpha \in \ell.\mathcal{O}$.

Proof of 1.

- $A[\ell]$ is a semi-simple J-module (Faltings), so there exists $\alpha_\ell \in End_J(A[\ell])$ killing N.
- $End_J(A[\ell]) \simeq End(A) \otimes \mathbf{F}_\ell$ (Faltings), so α_ℓ yields $\alpha \in \mathcal{O}, \alpha \notin \ell\mathcal{O}$ killing N.
- $\xi_{\alpha.y} = \alpha\xi_y$, so, $\frac{1}{\ell}\alpha.y$ is fixed by N.

Proof of 2.

$$\begin{array}{ccccc} ? & \rightarrow & A(K)/\ell.A(K) & \rightarrow & A(K_\infty)/\ell.A(K_\infty) \\ \downarrow & & \downarrow & & \downarrow \\ H^1(J, A[\ell]) & \rightarrow & H^1(\Gamma_K, A[\ell]) & \rightarrow & H^1(\Gamma_{K_\infty}, A[\ell])^J \end{array}$$

Serre's result on homotheties and Sah's lemma imply $H^1(J, A[\ell]) = 0$ for large ℓ.

Proof of 3.

Mordell-Weil (or a trick of Cassels's), both based on heights.

[Similar arguments *in the ℓ-adic case*.]

Some diophantine applications

C. Khare, D. Prasad : Reduction of homomorphisms mod p and algebraicity, JNT 105, 2004, 322-332.
A/K simple, $y, y' \in A(K)$ s.t. for almost all places v, the order of y mod v divides the order of y' mod v. Then, $\exists \alpha \in \mathcal{O}, y' = \alpha.y$. (This sharpens a result of M. Larsen.)

U. Zannier : On the Hilbert Irreducibility Theorem, Pisa preprint, 2008.
Let $\pi : Y \to A$ be a dominant K-morphism of finite degree, with Y irreducible and $A = E^n$. Let $y \in A(K)$ generate A. Suppose that for any isogeny $\phi : A \to A$, the pull-back $\phi^*(Y)$ is irreducible. Then there is an arithmetic progression $\mathcal{V}$ in $\mathbb{Z}$ such that each $\nu \in \mathcal{V}$, the fiber $\pi^{-1}(\nu.y)$ is K-irreducible.

Also, work of M. Gavrilovich (K-Theory, 38, 2008, 135-152) on $Ext(E(\overline{K}), \mathbb{Z}^2)$; of C. Salgado (PhD. Paris 7, 2009) on ranks of elliptic surfaces, ...

II.a . Logarithms on abelian schemes

• $K = \mathbb{C}(S)$ or $\mathbb{C}(S)^{alg}$, $S/\mathbb{C}$ = smooth affine curve, ∂ = a derivation on K with $K^\partial = \mathbb{C}$, $\hat{K}$ = diff. closure, $\mathcal{U}$ = univ. domain.

• A/K, coming from an abelian scheme $\mathcal{A} \to S$. A_0 = its $K/\mathbb{C}$-trace. Its universal extension $\tilde{A}$ has dimension $2g$:

$$0 \to W_A \to \tilde{A} \to^{\pi} A \to 0$$

Exponential sequence :

$$0 \to T_B\tilde{\mathcal{A}} \to L\tilde{\mathcal{A}}^{an} \to^{exp} \tilde{\mathcal{A}}^{an} \to 0$$

• $y \in \tilde{A}(K)$, generating $\tilde{A}$, i.e. : $\forall H \subsetneq \tilde{A}, y \notin H + \tilde{A}_0(\mathbb{C})$. Chose $\ell n(y) \in exp^{-1}(y)$. Then :

Theorem L (André, 1992)

$$tr.dg.(K(\ell n(y))/K) = 2g.$$

$\tilde{A}$ has a structure of algebraic D-group, with

$$\partial\ell n_{\tilde{A}} : \tilde{A} \to L\tilde{A}$$

Gauss-Manin connection :

$$\partial_{L\tilde{A}} = \partial\ell n_{\tilde{A}} \circ exp : L\tilde{A} \to L\tilde{A}$$

So $\ell n(y) \rightsquigarrow x \in L\tilde{A}(\hat{K})$ solution of the inhomogeneous LDE : $\partial_{L\tilde{A}}(x) = \partial\ell n_{\tilde{A}} y$.

- $K_{L\tilde{A}} = K(T_B(\tilde{A}))$ = Picard-Vessiot extension for $\partial_{L\tilde{A}}(-) = 0$, with solution space $(L\tilde{A})^\partial = T_B(\tilde{A}) \otimes \mathbb{C} \simeq \mathbb{C}^{2g}$.

We will actually prove that

$$Gal_\partial(K_{L\tilde{A}}(\ell n(y))/K_{L\tilde{A}}) \simeq (L\tilde{A})^\partial.$$

$$\begin{array}{cccc}
\hat{K} & & & \\
| & & & \\
K_{L\tilde{A}}(\ell n(y)) & & \xi_y & \\
| & \}N & \hookrightarrow & (L\tilde{A})^\partial \\
K_{L\tilde{A}} & & \rho & \\
| & \}J & \hookrightarrow & GL((L\tilde{A})^\partial) \\
K & & &
\end{array}$$

$$\xi_y(\sigma) = \sigma(\ell n(y)) - \ell n(y), \quad \xi_y(\tau\sigma\tau^{-1}) = \tau(\xi_y(\sigma)).$$

Proof (in a "generic" case)

By Deligne, $L\tilde{A}$ is a semi-simple D-module. For simplicity, suppose that it is irreducible.

1. Galois theoretic step .
(Of necessity, base extension to $K_{L\tilde{A}} \rightsquigarrow L\tilde{A}$ becomes "$K_{L\tilde{A}}$-large" for the morphism $[exp]_{\tilde{A}}$.)

$Im(\xi_y) \simeq N$ is a J-submodule of $(L\tilde{A})^{\partial}$. Assume $N \neq (L\tilde{A})^{\partial}$. Then $N = 0, x \in L\tilde{A}(K_{L\tilde{A}})$ and

$$\partial\ell n_{\tilde{A}} y = \partial_{L\tilde{A}}(x) \in \partial_{L\tilde{A}}\Big(L\tilde{A}(K_{L\tilde{A}})\Big).$$

2. Galois descent

If a point $z \in L\tilde{A}(K)$ lies in $\partial_{L\tilde{A}}\Big(L\tilde{A}(K_{L\tilde{A}})\Big)$, then, z already lies in $\partial_{L\tilde{A}}(L\tilde{A}(K))$, i.e.

$$Coker(\partial_{L\tilde{A}}, L\tilde{A}(K)) \hookrightarrow Coker(\partial_{L\tilde{A}}, L\tilde{A}(K_{L\tilde{A}}))$$

Indeed, J is reductive, so $H^1(J, (L\tilde{A})^{\partial}) = 0$.

3. Geometric step

Manin's theorem : if $\partial\ell n_{\tilde{A}} y = \partial_{L\tilde{A}}(x)$ for some $x \in L\tilde{A}(K)$, then $y \in W_A + \tilde{A}_0(\mathbb{C}) + \tilde{A}_{tor}$.

A diophantine application

Theorem L plays a (minor, but not empty) role in

D. Masser, U. Zannier : Torsion anomalous points and families of elliptic curves; CRAS Paris 346, 2008, 491-494,

i.e the following special case of the Zilber-Pink conjecture. Consider the sections y, y' with abscissae 2, 3 of the Legendre elliptic scheme $E/S, S = \lambda-$line. There are finitely many λ's such that both $y(\lambda)$ and $y'(\lambda)$ are torsion points on E_λ. In other words, *the curve* $C = (y, y')$ *on the abelian scheme* A/S, $A = E \times E$, *has finite intersection with* $A^{[>1]}$, where $A^{[>1]} =$ the union of all 2-codim'l algebraic subgroups of all the fibers of A/S.

Uses a result of J. Pila (Quart.J.M 55, 2004, 207-223) on the rational points of a subanalytic surface away from the union of its non-punctual semi-algebraic subsets. The algebraic independence of $\ell n(y), \ell n(y')$ over $K_{L\tilde{A}}$ (plus some knowledge of the size of J as well) shows that there is nothing to withdraw.

II b . Exponentials on abelian schemes

As in II.a,

$$K = \mathbb{C}(S),\ \partial,\ A/K,\ A_0/\mathbb{C},\ \tilde{A}.$$
$$0 \to T_B\tilde{\mathcal{A}} \to L\tilde{\mathcal{A}}^{an} \to^{exp} \tilde{\mathcal{A}}^{an} \to 0$$

• $x \in L\tilde{A}(K)$, generating $L\tilde{A}$, i.e. : $\forall H \subsetneq \tilde{A}, x \notin LH + L\tilde{A}_0(\mathbb{C})$. Then :

Theorem E (Be-Pillay, JAMS, 201?)

$$tr.dg.(K(exp(x)/K) = 2g.$$

As in II.a, we have

$$\partial\ell n_{\tilde{A}} : \tilde{A} \to L\tilde{A}$$
$$\partial_{L\tilde{A}} = \partial\ell n_{\tilde{A}} \circ exp : L\tilde{A} \to L\tilde{A}.$$

So $exp(x) \rightsquigarrow y \in \tilde{A}(\hat{K})$ solution of the inhomogeneous NLDE : $\partial\ell n_{\tilde{A}}(y) = \partial_{L\tilde{A}}x$.

Let $K_{\tilde{A}}$ be the differential extension of $\overline{K}$ generated by all points in

$$\tilde{A}^\partial = \{z \in \tilde{A}(\hat{K}), \partial\ell n_{\tilde{A}}(z) = 0.\}$$

Using

. • Pillay's Galois theory

. • + a Galois descent ,

we will actually prove that

$$Gal_\partial(K_{\tilde{A}}(exp(x))/K_{\tilde{A}}) \simeq \tilde{A}^\partial.$$

$$\begin{array}{cccc}
\widehat{K} & & & \\
| & & & \\
K_{\tilde{A}}(exp(x)) & & \xi_x & \\
| & \}N & \hookrightarrow & \tilde{A}^\partial \\
K_{\tilde{A}} & & \rho & \\
| & \}\tilde{J} & \hookrightarrow & Aut(\tilde{A}^\partial) \\
\overline{K} & & &
\end{array}$$

$$\xi_x(\sigma) = \sigma(exp(x)) - exp(x).$$

In generic cases (e.g. when the Kodaira-Spencer rank of A/S is maximal, e.g. when $L\tilde{A}$ is irreducible),

$$K_{\tilde{A}} = \overline{K} :$$

the D-group $\tilde{A}$ is $\overline{K}$-large, and no descent is required ! We then merely need :

1. Galois theoretic step

$Im(\xi_x) \simeq N = H^\partial$ for some algebraic D-subgroup H of $\tilde{A}$. Assume $H \neq \tilde{A}$. Then there is a non trivial D-quotient $\pi : \tilde{A} \to \overline{A}$ sending x to $\overline{x} \in L\overline{A}(K)$, with

$$\partial_{L\overline{A}}(\overline{x}) = \partial\ell n_{\overline{A}}(\overline{y}) \text{ for some } \overline{y} \in \overline{A}(K).$$

3. Geometric step

If $\overline{A} \simeq \tilde{B}$ for some abelian variety quotient B of A, just apply Manin's theorem:
$\overline{x} \in LW_B + L\tilde{B}_0(\mathbb{C})$, so x cannot generate $L\tilde{A}$.

The general case requires Chai's sharpening of Manin's theorem.

That $\overline{A} \simeq \tilde{B}$ happens automatically when W_A contains no non trivial D-subgroup. When $A_0 = 0$, this is equivalent to $\tilde{A}$ being $\overline{K}$-large. In general,

2. Galois descent in Pillay's theory

Write K for $\overline{K}$, and let U be the maximal D-subgroup of $\tilde{A}$ (equivalently D-submodule of $L\tilde{A}$) contained in W_A.

$$0 \to U \to \tilde{A} \to \overline{A} \to 0.$$

• Hrushovski-Sokolovic, Marker-Pillay $\Rightarrow \overline{A}$ is K-large : $\overline{A}^{\partial}(\hat{K}) = \overline{A}^{\partial}(K)$.
• Manin-Chai $\Rightarrow \overline{A}^{\partial}(K) = \overline{A}_{tor} + A_0(\mathbf{C})$.
• $0 \to U^{\partial}(\hat{K}) \to \tilde{A}^{\partial}(\hat{K}) \to \overline{A}^{\partial}(\hat{K}) \to 0$.
Therefore

$K_{\tilde{A}} = K_U$ is a P-V extension of K
and $\tilde{J} = Gal_{\partial}(K_{\tilde{A}}/K) := J_U$ is a
factor of the reductive group $J = Gal_{\partial}(K_{L\tilde{A}}/K)$.
Actually (Deligne), J, hence J_U, is semi-simple.

By Step 1 over $K_{\tilde{A}}$, and rigidity of D-subgroups of $\tilde{A}$, we have :

$\partial_{L\overline{A}}(\overline{x}) = \partial\ell n_{\overline{A}}(\overline{y})$ for some $\overline{y} \in \overline{A}(K_U)$.
and it remains to show that
$L\overline{A}(K)/\partial\ell n_{\overline{A}}(\overline{A}(K)) \hookrightarrow L\overline{A}(K_U)/\partial\ell n_{\overline{A}}(\overline{A}(K_U))$,
i.e. that we may take $\overline{y} \in \overline{A}(K)$.

The cocycle $\hat{\xi}_{\overline{y}} : J_U \to \overline{A}^{\partial} : \sigma \mapsto \sigma\overline{y} - \overline{y}$ is a group homomorphism. Since $J_U = [J_U, J_U]$, while $\overline{A}^{\partial}$ is abelian, $\xi_{\overline{y}}$ vanishes, so that indeed $\overline{y}$ is defined over K.

Conclusion

• No diophantine application (yet) of Theorem E.

• But the method works in other contexts, e.g., considering the differential equation

$$\partial \ell n(y) = \lambda . \partial \ell n(x)$$

on $\mathbb{G}_m$, with $\lambda \in \mathbb{C}, \lambda \notin \mathbb{Q}$:

if $x_1, ..., x_n \in \mathbb{G}_m(K)$ are multiplicatively independent modulo $\mathbb{G}_m(\mathbb{C})$, then, $x_1^{\lambda}, ..., x_n^{\lambda}$ are algebraically independent over $K = \mathbb{C}(z)$.

For more general (Schanuel-type) results on x^{λ}, see:

- M. Bayes, J. Kirby, A. Wilkie, (2008) arXiv: 0810.4457.

- P. Kowalski, Ann. PAL, 156, 2008, 96-109.