Séminaires & Congrès

COLLECTION SMF

# GALOIS DESCENT IN GALOIS THEORIES

Daniel Bertrand

## ARITHMETIC AND GALOIS THEORY OF DIFFERENTIAL EQUATIONS

Numéro 23

Lucia Di Vizio, Tanguy Rivoal, eds.

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

*Séminaires & Congrès*
**23**, 2011, p. 1–24

# GALOIS DESCENT IN GALOIS THEORIES

*by*

Daniel Bertrand

***Abstract.*** — Inspired by Kummer theory on abelian varieties, we give similar looking descriptions of the Galois groups occuring in the differential Galois theories of Picard-Vessiot, Kolchin and Pillay, and mention some arithmetic applications.

***Résumé* (Descente de Galois dans les thÃľories de Galois).** — Guidés par la théorie de Kummer sur les variétés abéliennes et motivés par quelques applications arithmétiques, nous donnons des descriptions d'apparences similaires des groupes de Galois issus des théories de Galois différentielles de Picard-Vessiot, Kolchin et Pillay.

The topic I had been assigned by the organizers of the Luminy September 09 School was "Algebraic $D$-groups and non-linear differential Galois theories". The present account is written in an applied maths spirit : how to compute the Galois groups, and what for ? Thus, we start with a motivating question which, in accordance with the theme of the School, comes from diophantine geometry. We then describe the Galois groups of the various theories under study, in terms that bear a strong similarity. Finally, we apply this description to the study of exponentials and logarithms on abelian schemes.

A general argument of Galois descent occurs along the text, hence the title[(1)] of these notes; its number theoretic prototype, given by Kummer theory, is recalled in an Appendix to the paper.

Although the presentation is sometimes novel, the results described here are not new. For original sources, we refer the reader to [29] for the Picard-Vessiot theory, [27] for Kolchin's and Pillay's theories, and to [1] and [10] for the applications to algebraic independence. Actually, this text may serve as an introduction to the survey

***2000 Mathematics Subject Classification.*** — 12H05, 14K15, 11G10, 12G05.

***Key words and phrases.*** — Linear and non-linear differential Galois theory, Abelian varieties, Galois cohomology, Kummer theory.

(1) also borrowed from a set of talks at the Durham July 09 Conference on model theory. I thank the organizers of both Luminy and Durham meetings for having offered me these opportunities to develop this point of view.

[9], which is itself an introduction to the latter papers (and to the descent argument in the non-linear case).

## 1. Ax-Schanuel

**1.1. The multiplicative case.** — The well-known Schanuel conjecture asserts that if $x = \{x_1, ..., x_n\}$ is a "non-degenerate" $n$-tuple of complex numbers whose image under the standard exponential function $exp$ is denoted by $y = \{y_1 = exp(x_1), ..., y_n = exp(x_n)\}$, then $tr.deg._{\mathbb{Q}}\mathbb{Q}(x, y) \geq n$. The expression *non-degenerate* will occur under several acceptions in these notes. Here, it means that

$$\forall (m_1, .., m_n) \in \mathbb{Z}^n \setminus 0, m_1x_1 + ... + m_nx_n \neq 0,$$

or equivalently, that for any proper algebraic subgroup $H$ of the algebraic torus $G = \mathbb{G}_m^n$, the complex point $x$ of the Lie algebra $LG$ of $G$ does not lie in the Lie algebra $LH$ of $H$.

In 1970, Ax [2] proved a functional version of the conjecture, which, in an analytic setting, may be phrased as follows. Let

$$x = (x_1, ..., x_n) \in (\mathbb{C}\{\{z_1, .., z_t\}\})^n$$

be a $n$-tuple of convergent power series in $t$ variables. For each $i$, $y_i(z) := exp(x_i)$ lies in $\mathbb{C}\{\{z_1, .., z_t\}\}^*$, and we set $y = exp(x) \in (\mathbb{C}\{\{z_1, .., z_t\}\}^*)^n$. Assume that $x$ is *non-degenerate*, in the sense that

$$\forall (m_1, .., m_n) \in \mathbb{Z}^n \setminus 0, m_1x_1 + ... + m_nx_n \notin \mathbb{C},$$

or equivalently, that for any proper algebraic subgroup $H$ of the algebraic torus $G = \mathbb{G}_m^n$ and any constant point $\xi \in LG(\mathbb{C})$,

$$x \notin \xi + LH.$$

Then, $tr.deg.(\mathbb{C}(x, y)/\mathbb{C}) \geq n + \mu$, where $\mu$ denotes the rank of the functional jacobian $\frac{Dx}{Dz} \in Mat_{t,n}(\mathbb{C}\{\{z_1, .., z_t\}\})$ of $x$.

Let $K \simeq \mathbb{C}(z_1, ..., z_\mu)$ be the field generated by the principal variables. In order to check the above lower bound, it suffices to show that $tr.deg.(K(x, y)/K) \geq n$ (and the two statements are actually equivalent). Furthermore, choosing a sufficiently general line in $\mathbb{C}^\mu$, it suffices to check the latter inequality when $\mu = 1$. Using the differential equation satisfied by $exp$, we can therefore view Ax's theorem as a corollary of the following differential algebraic statement. Let $K = \mathbb{C}(z)^{alg}$ be the algebraic closure of $\mathbb{C}(z)$, endowed with the (unique) extension $\partial$ of the derivation $\frac{d}{dz}$, and let $(\mathcal{K}, \partial)$ be a differential extension of $(K, \partial)$, with same constant field $\mathcal{K}^\partial = \mathbb{C}$. Let further $(x, y) \in (\mathcal{K} \times \mathcal{K}^*)^n$ satisfy : $\partial y/y = \partial x$ (where derivations are taken coordinate-wise). Assume that for any proper algebraic subgroup $H$ of $G = \mathbb{G}_m^n$, $x$ does not lie in $LH + LG(\mathbb{C})$. Then $deg.tr.K(x, y)/K \geq n$.

**1.2. The constant case.** — Two years later, Ax [3] extended his results to more general algebraic groups (see also [18]). For instance, making the same analysis as above, we may rephrase Theorem 3 of his paper (actually written in a formal setting and under a slightly stronger hypothesis on $G$) as follows.

Let $K = \mathbb{C}(z)^{alg}, \partial = \frac{d}{dz}$ and $\mathcal{K}$ be as above, and let $G$ be a commutative algebraic group *defined over* $\mathbb{C}$, with no additive quotient. In other words, $G$ is a semi-abelian variety defined over $\mathbb{C}$, or more generally, a quotient of its universal vectorial extension. The Lie algebra $LG$ of $G$ is a vector space over $\mathbb{C}$, so that there is a unique differential operator $\nabla_{LG}$ on $LG(\mathcal{K})$, whose solution space is $LG(\mathbb{C})$ (to define $\nabla_{LG}(x)$, choose any basis of $LG$ *over* $\mathbb{C}$, and take the $\partial$-derivatives of the coordinates of $x$; the outcome is independent of the chosen basis). The exponential map $exp_G : LG(\mathbb{C}) \to G(\mathbb{C})$ is a morphism of commutative Lie groups, admitting as kernel a discrete subgroup $\Omega_G$ of $LG(\mathbb{C})$, and one can consider its inverse $\ell n_G$ as a multivalued function. For any analytic function $x(z)$ with values in $LG(\mathbb{C})$, $y(z) := exp_G(x(z))$ is a well defined analytic function with values in $G(\mathbb{C})$. For any analytic function $y(z)$ with values in $G(\mathbb{C})$, $\nabla_{LG} \circ \ell n_G(y)$ is also well-defined, since $\Omega_G$ is killed by $\nabla_{LG}$. Its explicit expression enables us to extend $\nabla_{LG} \circ \ell n_G$ to a group homomorphism $\partial \ell n_G : G(\mathcal{K}) \to LG(\mathcal{K})$. This is the *logarithmic derivative* of $G/\mathbb{C}$, which we describe in a more algebraic way in §2, then for non constant groups in §3 - and again in the above style in §4.1. Notice that when $x$ and $y$ have an analytic meaning, the relation $\partial \ell n_G(y) = \nabla_{LG}(x)$ is equivalent to the existence of a point $\xi \in LG(\mathbb{C})$ such that $y = exp_G(x - \xi)$.

Exactly as in §1.1, Ax's theorem then reads as follows : let $(x, y) \in (LG \times G)(\mathcal{K})$ satisfy $\partial \ell n_G(y) = \nabla_{LG}(x)$, and suppose that $x$ is non-degenerate : for any proper algebraic subgroup $H/\mathbb{C}$ of $G$, $x \notin LH + LG(\mathbb{C})$. Then, $tr.deg.(K(x, y)/K) \geq dim G$.

In these notes, we will show that differential Galois theories provide proofs of Ax's theorem under the following *restrictions* :

$(L)$ either $y \in G(K)$ (in which case we can apply the linear Picard-Vessiot theory);

$(E)$ or $x \in LG(K)$ (in which case we can apply the non-linear theory of Kolchin).

But the interesting point about these Galois approaches is that in fact, they then provide an *extension* of these results to the case of *non-constant* algebraic groups, where $G$ will only be defined over $K$. In the second situation, this is made possible by Pillay's generalization of Kolchin's theory (although the initial proof given in [10] uses a different method). See Theorems 4.1 to 4.4 for the outcome in the case of abelian varieties.

**1.3. Motivations.** — The Manin-Mumford conjecture was proved by Raynaud in 1984, and has known since then a remarkable number of interesting new proofs. Based on work of Bombieri, Pila, Wilkie, and Zannier, Pila recently obtained another one [24], where the strategy of [25] is combined with Ax's theorem[(2)] on abelian varieties over

(2) That Ax's earlier version on tori [2] can play a similar role for the multiplicative analogue of Manin-Mumford, had already been observed in [25], Final Remark 2.

$\mathbb{C}$. By a general argument (see [11], Thm. 1 and proof of Thm. 4; also [25]), the conjecture reduces to :

**Manin-Mumford** (key point): *Let $A/\mathbb{Q}^{alg}$ be an abelian variety. An algebraic subvariety $X/\mathbb{Q}^{alg}$ of $A$ passes through finitely many torsion points of $A$, unless $X$ contains a translate of a non-zero abelian subvariety of $A$.*

We now sketch Pila's approach : first, as in [25], write $A(\mathbb{C}) = LA(\mathbb{C})/\Omega_A \simeq \mathbb{R}^{2g}/\mathbb{Z}^{2g}$, so that the torsion points become the rational points of the box $[0,1[^{2g}$ while $X$ pulls back to a complex analytic subvariety $\mathcal{X}$ of $LA$. By $o$-minimality, $\mathcal{X}$ meets $<< T^{\epsilon}$ rational points of denominator $\leq T$, *outside of the real semi-algebraic subvarieties $\mathcal{W}$ of positive dimension it contains.* But back to $A(\mathbb{Q}^{alg})$, any such torsion point generates many others[(3)] by Galois action, so their orders are bounded.

To conclude, we must control the possible irreducible complex algebraic subvarieties $W$ of positive dimension in $\mathcal{X}$. Assuming that $X$ contains no translate of a non zero abelian subvariety of $A$, we claim that no such $W$ exists. Assuming otherwise, consider the function field $K = \mathbb{C}(W)$, and let $x \in LA(K)$ be a generic point over $\mathbb{C}$ of $W$. Since $exp_A(W) \subset X$, the transcendence degree of $y = exp_A(x)$ over $\mathbb{C}$ is $< dim(A)$. Ax's theorem on the constant abelian variety $G = A$ (in its original formulation, or in the above one, using A. Pillay's remark that it suffices to check the claim when $W$ is a curve) then implies that $x$ lies in $\xi + LA'$, for some abelian subvariety $A'$ of $A$, with $0 \neq A' \subsetneq A$, and some $\xi \in LA(\mathbb{C})$. Set $\eta = exp_A(\xi)$, and notice that $x' = x - \xi \in LA'(K)$ is still a generic point over $\mathbb{C}$ of the irreducible algebraic variety $W' = W - \xi$, which is therefore contained in $LA'$. The image of $W'$ under $exp_{A'}$ is contained in the intersection $X'$ of $X - \eta$ and $A'$, which is a subvariety of $A'$ containing no translate of a non zero abelian subvariety. Since the inverse image $\mathcal{X}' \subset LA'$ of $X'$ under $exp_{A'}$ contains $W'$, the proof can now be concluded by induction on the dimension of $A$. We point out that Ax's theorem was here used only in the $(E)$ setting.

In his unpublished note [28], Pink extended the conjecture to a relative context, including the following case :

**Relative Manin-Mumford** (over curves) : *let $X$ be the image of a non-torsion section of an abelian scheme $\mathcal{A}/S$ of relative dimension $\geq 2$ over a curve $S/\mathbb{C}$. Assume that $X$ is not contained in a translate of an elliptic subscheme of $\mathcal{A}/S$. Then, $X$ should meet finitely many of the torsion points of the various fibers of $\mathcal{A}/S$.*

So, we here have an abelian variety $A$ over $K = \mathbb{C}(S)$. It need not come from $\mathbb{C}$, but one may hope that again, an Ax-type theorem, now over a non-constant algebraic group, will help. And indeed, in their work on the conjecture, Masser and Zannier do appeal to such an algebraic independence statement, though now in the $(L)$ setting : see [22], p. 493, line 14, for the test case of the square of an elliptic scheme.

(3) i.e. more than $T^{\delta}$, where $\delta > \epsilon$. The Kummer theory described in the Appendix would similarly yield large Galois orbits for the division points in the Mordell-Lang conjecture.