Séminaires & Congrès

COLLECTION SMF

GALOIS GROUPS ARISING FROM ARITHMETIC DIFFERENTIAL EQUATIONS

Alexandru Buium

THÉORIES DE GALOIS GÉOMÉTRIQUE ET DIFFÉRENTIELLE

Numéro 27

D. Bertrand, P. Boalch, J.-M. Couveignes, P. Dèbes, éds.

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

Séminaires & Congrès
27, 2012, p. 13–24

GALOIS GROUPS ARISING FROM ARITHMETIC DIFFERENTIAL EQUATIONS

by

Alexandru Buium

Abstract. — In this note we show (by interpreting results both old and new) that various Galois theoretic statements about algebraic equations in characteristic p, that are "non-liftable" to statements about algebraic equations in characteristic zero, can nevertheless be lifted to statements about "arithmetic differential equations" in characteristic zero.

***Résumé* (Groupes de Galois issus d'équations différentielles arithmétiques).** — Dans cette note, on démontre, en réinterprétant des résultats tant anciens que nouveaux, que divers énoncés de nature galoisienne sur les équations algébriques en caractéristique finie, qui ne peuvent être relevés en des énoncés sur des équations algébriques en caractéristique nulle, peuvent néanmoins l'être en des énoncés portant sur des "équations différentielles algébriques" en caractéristique nulle.

1. Introduction

In the Introduction to this note we discuss our background and motivation. However, from a logical viewpoint, no part of this Introduction is necessary for understanding the rest of the note. So the reader interested in the purely mathematical content of this note can skip directly to section 2.

Our background consists of a series of papers starting with [2] in which the author developed an arithmetic analogue of the theory of ordinary differential equations. Cf. [6] for an account of the state of the theory as of 2005. In this arithmetic theory the variable x is replaced by a prime number p, functions of x are replaced by numbers, the derivative operator $\frac{d}{dx}$ acting on functions of x is replaced by a *Fermat quotient operator* $\delta = \text{“}\frac{d}{dp}\text{”}$ acting on numbers, and differential equations satisfied by functions are correspondingly replaced by *arithmetic differential equations* satisfied by numbers. In this discussion *numbers* are understood to be rational integers or, more generally, integers in number fields or local fields. For an integer $n \in \mathbb{Z}$ we have $\delta n = \frac{n - n^p}{p}$.

2010 Mathematics Subject Classification. — 11 F 32, 11 S 20.

As explained in [6] one can then generalize usual algebraic geometry by replacing algebraic equations with arithmetic differential equations. What one obtains is a geometry referred to as *δ-geometry*; the latter should be viewed as an arithmetic analogue of the Ritt-Kolchin differential algebraic geometry [18, 17]. By analogy with the Ritt-Kolchin theory the prefix δ could be read as "arithmetic-differential".

There are two types of applications of δ-geometry. The first consists of results about "old" (classical) objects; these results can be formulated without reference to the "new" theory but need the "new" theory for their proofs. Applications of the second type are formulated in terms of the "new" theory and are meant to shed some new light on "old" (classical) objects.

Among the first type of applications one has, for instance: 1) an effective uniform bound for the number of torsion points on curves over number fields [3], 2) finiteness results (with uniform bounds) for "Heegner-like" points of elliptic curves, lying in finite rank subgroups [8, 9], and 3) results on congruences of classical modular forms [5, 1, 11].

Among the second type of applications is the construction of new quotient spaces that "do not exist" in algebraic geometry. Cf. [6] and also [7] for a quick exposition of results. Indeed (categorical) quotients of algebraic curves by correspondences that possess infinite orbits reduce to a point in algebraic geometry so they cannot be treated meaningfully within algebraic geometry. One way to address this basic pathology is to enlarge algebraic geometry in a "non-commutative direction" as in the work of A. Connes [12]. An entirely different way to address this pathology is to replace algebraic geometry by δ-geometry. It then turns out that certain quotients that reduce to a point in algebraic geometry become interesting objects in $\delta-$geometry; this is because there are more invariant arithmetic differential equations than invariant algebraic equations.

In both types of applications discussed above an important role is played by certain Galois groups arising from arithmetic differential equations. These Galois groups are typically profinite and arise as covering groups of objects in δ-geometry.

The aim of the present note is to provide a quick introduction to the algebra behind the theory of arithmetic differential equations [2, 6] and to show how Galois groups arise in this context [6, 11]. The main idea put forward here is that various results (especially Galois theoretic results) about algebraic equations in characteristic p, which are non-liftable to results about algebraic equations in characteristic zero, can nevertheless be lifted to results about arithmetic differential equations in characteristic zero.

Our paper is entirely self contained and will proceed by giving all the necessary definitions and statements of Galois theoretic results without any reference to the δ-geometric theory alluded above and without further explaining how these results relate to our original motivation.

Acknowledgment. This material is based upon work partially supported by the NSF under Grant No. 0852591 and by the IHES, Bures sur Yvette, France. Any

opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the NSF or the IHES.

2. Fermat quotients

A *p-derivation* $\delta : A \to A$ on a ring A is a map such that

$$\begin{aligned} \delta(x+y) &= \delta x + \delta y + C_p(x,y), \\ \delta(xy) &= x^p \delta y + y^p \delta x + p \delta x \delta y. \end{aligned}$$

Here

$$C_p(X,Y) := \frac{X^p + Y^p - (X+Y)^p}{p} \in \mathbb{Z}[X,Y].$$

The above concept was introduced independently by Joyal and the author [15, 2]. The idea in what follows is to view p-derivations δ as an analogue of a derivation "$\frac{d}{dp}$" with respect to p. Note that if δ is a p-derivation on A then the map $\phi(x) = x^p + p\delta x$ is a ring endomorphism of A. Actually if A is p-torsion free then a map $\delta : A \to A$ is a p-derivation if and only if the map $\phi : A \to A$ above is a ring endomorphism. We sometimes write x^ϕ instead of $\phi(x)$.

If A is any ring we denote by $\widehat{A}$ the p-adic completion of A. Any p-derivation of A induces a p-derivation on $\widehat{A}$.

The ring of integers $\mathbb{Z}$ has a unique p-derivation given by the classical *Fermat quotient operator*

$$\delta n = \frac{n - n^p}{p}.$$

More generally if $R = \widehat{\mathbb{Z}_p^{ur}}$ is the completion of the maximum unramified extension $\mathbb{Z}_p^{ur}$ of the ring $\mathbb{Z}_p$ of p-adic integers then R has a unique p-derivation. It is given by

$$\delta x = \frac{\phi(x) - x^p}{p}$$

where ϕ is the unique ring automorphism of R that lifts the p-power Frobenius automorphism of $\overline{R} := R/pR$. (Recall that $\overline{R}$ is an algebraic closure of the prime field $\mathbb{F}_p$.)

Next let $x, x', x'', ...$ be indeterminates and consider the ring of *δ-polynomials*

$$R\{x\} := R[x, x', x'', ...].$$

This ring possess a unique p-derivation δ such that $\delta x = x', \delta x' = x'', ...$ etc. The same is true if $x, x', x'', ...$ are n-tuple of variables.

Taking one step further we may consider the ring of *δ-rational functions* $\widehat{R\{x\}_{(p)}}$ obtained by p-adically completing the localization of $R\{x\}$ at the prime ideal (p). Again the ring $\widehat{R\{x\}_{(p)}}$ has a unique p-derivation δ such that $\delta x = x', \delta x' = x'', ...$ etc. (Note that the existence of δ fails to hold if we do not take p-adic completion.)

3. Galois groups

Let $\overline{A} \subset \overline{B}$ a ring extension, and Γ a profinite group acting on $\overline{B}$ by $\overline{A}$-automorphisms. We say that $\overline{B}$ is a Γ-*extension* of $\overline{A}$ if one can write $\overline{A}$ and $\overline{B}$ as filtered unions of subrings, $\overline{A} = \bigcup \overline{A}_i$, $\overline{B} = \bigcup \overline{B}_i$, indexed by some partially ordered set, with $\overline{A}_i \subset \overline{B}_i$, and one can write Γ as an inverse limit of finite groups, $\Gamma = \varprojlim \Gamma_i$, such that the Γ-action on $\overline{B}$ is induced by a system of compatible Γ_i-actions on $\overline{B}_i$ and

$$\overline{B}_i^{\Gamma_i} = \overline{A}_i$$

for all i. Then, of course, we also have

$$\overline{B}^{\Gamma} = \overline{A}.$$

In what follows we would like to introduce a δ-analogue of the above definition. By a *δ-ring* we will understand a ring together with a p-derivation. Start with a *δ-ring extension* $A \subset B$ i.e. a ring extension of δ-rings such that the p-derivation on B restricted to A is the p-derivation on A. We shall assume that A and B are p-adically complete, $pB \cap A = pA$, and p is a non-zero divisor in A and B. If these conditions are satisfied we will say our δ-ring extension is *good*. For a good δ-ring extension we may consider the ring extension $\overline{A} \subset \overline{B}$ where $\overline{A} := A/pA$, $\overline{B} := B/pB$. Let $Aut_\delta(B/A)$ be the group of all automorphisms in $Aut(B/A)$ that commute with δ. Then we have an induced group homomorphism

$$\rho : Aut_\delta(B/A) \to Aut(\overline{B}/\overline{A})$$

which is easily seen to be injective.

Now let Γ be a profinite group. A good δ-ring extension B/A will be called a *Γ-δ-extension* if

1) $\Gamma \simeq Aut_\delta(B/A)$;
2) ρ is an isomorphism;
3) $\overline{B}/\overline{A}$ is a Γ-extension.

Note that if B/A is a Γ-δ-extension then we also have

$$B^{\Gamma} = A.$$

Our aim in this paper will be to show that certain remarkable δ-ring extensions (that play a key role in the theory of [6, 5]) are Γ-δ-extensions for some specific groups Γ.

Remark 3.1. — In the context described above Galois groups arising from arithmetic differential equations are profinite and this context may be referred to as *vertical*. There is, however, a different context in which Galois groups can arise from arithmetic differential equations; this different context (that could be referred to as *horizontal*) involves groups Γ which are *inductive* (rather than projective) limits of finite groups. Prototypical examples of such Γ's would be torsion groups of a linear tori or of abelian varieties. Both the horizontal and the vertical cases appear in the theory [6] and actually combinations of the two (extensions of horizontal by vertical) appear as well. The kernels of the δ-characters of abelian varieties ("arithmetic Manin maps") in [2]