Séminaires & Congrès
13, 2006, p. 79–89

CORRESPONDENCES, FERMAT QUOTIENTS, AND UNIFORMIZATION

by

Alexandru Buium

Abstract. — Ordinary differential equations have an arithmetic analogue in which functions are replaced by integer numbers and the derivative operator is replaced by a Fermat quotient operator. This paper reviews the basics of this theory and explains some of the applications to the invariant theory of correspondences.

***Résumé* (Correspondances, quotients de Fermat et uniformisation).** — Les équations différentielles ordinaires possèdent un analogue arithmétique où les fonctions et leurs dérivées sont remplacées par des nombres entiers et leurs quotients de Fermat. Cet article présente les principes de cette théorie et quelques applications à la théorie des invariants pour les correspondances.

This paper represents a brief overview of some of the author's work on *arithmetic differential algebra* and its applications to the invariant theory of correspondences. Arithmetic differential algebra is an arithmetic analogue of the Ritt-Kolchin differential algebra [**Rit50**], [**Kol73**] in which derivations are replaced by *Fermat quotient operators*. The main foundational results and first applications of arithmetic differential algebra are contained in [**Bui95**], [**Bui96**], [**Bui00**]. A further study of these matters is contained in [**Bar03**], [**Bui03**], [**Bui04**], [**Bui02**]. A program outlining applications to the invariant theory of correspondences was sketched in the last 2 pages of [**Bui02**]. The present paper reports on recent progress along this program. For a detailed exposition of the results announced here we refer to the research monograph [**Bui05**].

The paper closely follows the talk presented at the Luminy conference. The author would like to thank the organizers of the conference for their support and encouragement. This research was supported in part by NSF Grant 0096946.

2000 *Mathematics Subject Classification.* — 11F32, 14G35, 12H05.
Key words and phrases. — Correspondences, $p-$adic numbers, uniformization.

1. Motivation

Let X and $\tilde{X}$ be two complex algebraic curves and $\sigma = (\sigma_1, \sigma_2)$ a pair of dominant maps:

$$X \xleftarrow{\sigma_1} \tilde{X} \xrightarrow{\sigma_2} X. \tag{1}$$

Assume X is irreducible. Denote by $\mathbf{C}(X)$ the field of rational functions on X and by

$$\mathbf{C}(X)^{\sigma} := \{f \in \mathbf{C}(X) \mid f \circ \sigma_1 = f \circ \sigma_2\} \tag{2}$$

the field of *invariants* of the *correspondence* σ. It is a fact that, "most of the times", there are "no non-constant invariants":

$$\mathbf{C}(X)^{\sigma} = \mathbf{C}. \tag{3}$$

There are, of course, exceptions to this: the whole of the classical Galois theory of curves is an exception. Here, when we say *Galois theory*, we mean the case when $\sigma_2 : \tilde{X} := X \times G \to X$ is a finite group action and σ_1 is the first projection; in this case, of course, we have

$$\mathbf{C}(X)^{\sigma} = \mathbf{C}(X)^{G} \neq \mathbf{C}.$$

In this paper we would like to view Galois theory as an exceptional (and "well understood") situation. On the contrary, the fact that the equality (3) holds "most of the times" will be viewed as a basic pathology in algebraic geometry that we would like to address. Indeed equality (3) says in particular that the "categorical quotient" X/σ in the category of algebraic varieties reduces to a point and, hence, the quotient map $X \to X/\sigma$ cannot be viewed, in any reasonable sense, as a Galois cover. Our aim in this paper is to show how one can construct a "larger geometry" (referred to as δ*−geometry*) in which X/σ ceases, in many interesting situations, to reduce to a point; in this new geometry the quotient map $X \to X/\sigma$ will sometimes "looks like" a Galois cover.

Our theory will be p−adic (rather than over the complex numbers $\mathbf{C}$). The basic ring of our theory will be $R = \hat{\mathbf{Z}}_p^{ur}$, the completion of the maximum unramified extension of the p−adic integers; recall that this is the unique complete discrete valuation ring with maximal ideal generated by p and residue field equal to the algebraic closure $\mathbf{F}_p^a$ of the prime field $\mathbf{F}_p$. The ring R has a unique automorphism ϕ lifting the Frobenius on R/pR. We can therefore consider the *Fermat quotient operator* $\delta : R \to R$,

$$\delta x = \frac{\phi(x) - x^p}{p}. \tag{4}$$

We will view δ as an arithmetic analogue of a derivation; our δ−geometry will then be an arithmetic analogue of the Ritt-Kolchin differential algebraic geometry [**Rit50**], [**Kol73**], [**Bui94**].

2. Toy examples

To explain what we have in mind we begin by looking at an easy example. Assume, in what follows, that $X = \tilde{X} = \mathbf{A}^1$ is the affine line over R. We assume $\sigma_1 = id$ and $\sigma_2(x) = x^2$. Define the map $\psi : R \to R$,

$$\psi(x) = \sum_{i=1}^{\infty} (-1)^{i+1} \frac{p^{i-1}}{i} \left(\frac{\delta x}{x^p} \right)^i, \tag{5}$$

and consider the (partially defined) map $f : R \to R$,

$$f(x) = \frac{\phi \circ \psi}{\psi}(x) = \psi^{p-1}(x) + p \frac{\delta \psi}{\psi}(x); \tag{6}$$

note that f is not defined precisely at the roots of 1. It is trivial to check that

$$\psi(x^2) = 2 \cdot \psi(x)$$

and, hence,

$$f(x^2) = f(x),$$

so f is an *invariant* for σ. Note that one can write

$$f(x) = \frac{F(x, \delta x, \delta^2 x, x^{-1})}{G(x, \delta x, x^{-1})}, \tag{7}$$

with F, G restricted power series in 4 respectively 3 variables. This example shows that, although no invariants for σ exist in algebraic geometry, invariants as in Equation 7 (which we shall refer to as *$\delta-$invariants*) may very well exist; this suggests to "adjoin" δ to usual algebraic geometry and this is exactly what we shall soon do.

Before proceeding to the general case, let us explore the above example in further detail. Once we discovered the invariant $\eta_0 := \frac{\phi \circ \psi}{\psi}$ it is easy to come up with more invariants namely $\eta_i := \delta^i \circ \eta_0$. Set $\bar{\eta}_i := \eta_i$ mod p. Moreover set $x' = \delta x$, $x'' = \delta^2 x$, e.t.c. One can prove that the field extension

$$\mathbf{F}_p^a(x, \bar{\eta}_0, \bar{\eta}_1, \bar{\eta}_2, ...) \subset \mathbf{F}_p^a(x, x', x'', x''', ...) \tag{8}$$

is Galois with Galois group $\mathbf{Z}_p^\times$. The left hand side of the above extension (8) can be viewed as the compositum of $\mathbf{F}_p^a(x)$ (the "field of rational functions on $X = \mathbf{A}^1$ mod p in the old algebraic geometry") and the field $\mathbf{F}_p^a(\bar{\eta}_0, \bar{\eta}_1, \bar{\eta}_2, ...)$ (which should be viewed as the "field of rational functions mod p on X/σ in the new geometry). The right hand side of the extension (8) can be viewed as the "field of rational functions mod p on X in the new geometry". As we will see the above picture can be generalized.

Let us further postpone our discussion of the general case by looking at yet another example. Assume in what follows that $X = \tilde{X} = \mathbf{A}^1$ over R and $\sigma_1 = id$, $\sigma_2(x) = x^2 - 2$ (the Chebyshev quadratic polynomial). Again one can show that "$\delta-$invariants" exist, more precisely there exist restricted power series F, G in 4 and 3 variables respectively such that

$$f(x) = \frac{F(x, \delta x, \delta^2 x, (x^2-4)^{-1})}{G(x, \delta x, (x^2-4)^{-1})} \tag{9}$$

satisfies

$$f(x^2 - 2) = f(x).$$

Also there is Galois computation similar to that in the previous example.

A natural question is whether the existence of "$\delta-$invariants" in the above 2 examples generalizes to the situation when $X = \tilde{X} = \mathbf{A}^1$, $\sigma_1 = id$, $\sigma_2(x) = x^2 + c$, $c \in \mathbf{Z}$. The answer to this question is NO! (Cf. [**BZ05**] for a precise statement and for related conjectures.)

The next natural question is: what do $x \mapsto x^2$ and $x \mapsto x^2 - 2$ have in common that does not hold for a general quadratic map $x \mapsto x^2 + c$? One possible answer is that the maps corresponding to $c = 0$ and $c = -2$ possess, over the complex numbers, *analytic uniformizations* in the sense that one has commutative diagrams

$$\begin{array}{ccc} \mathbf{C} & \stackrel{2z}{\to} & \mathbf{C} \\ \pi_1 \downarrow & & \downarrow \pi_1 \\ \mathbf{C}^\times & \stackrel{z^2}{\to} & \mathbf{C}^\times \end{array}, \quad \begin{array}{ccc} \mathbf{C} & \stackrel{2z}{\to} & \mathbf{C} \\ \pi_2 \downarrow & & \downarrow \pi_2 \\ \mathbf{C} & \stackrel{z^2-2}{\to} & \mathbf{C}, \end{array}$$

where $\pi_1(z) = e^{2\pi i z}$ and $\pi_2(z) = e^{2\pi i z} + e^{-2\pi i z}$ respectively.

So the next question one is tempted to ask is: are there other correspondences admitting similar "analytic uniformizations"? The answer to this question is: PLENTY! And they can be all classified.

The final question one would then ask would be: Do "$\delta-$invariants" exist for such "uniformizable" correspondences? Again the answer to the above question tends to be YES and the aim of this paper is to explain the theory that provides this answer.

3. Outline of the theory

To explain our main ideas it is convenient to start with an arbitrary category $\mathcal{C}$; what we have in mind is a category of spaces in some geometry. By a *correspondence* we will understand a pair $\mathbf{X} = (X, \sigma)$ where X is an object in $\mathcal{C}$ and σ is a pair of morphisms in $\mathcal{C}$ as in Equation (1). A *categorical quotient* for $\mathbf{X}$ will mean a pair (Y, π) where $\pi : X \to Y$ is a morphism in $\mathcal{C}$ such that $\pi \circ \sigma_1 = \pi \circ \sigma_2$ and with the property that for any other pair (Y', π') with $\pi' : X \to Y'$, $\pi' \circ \sigma_1 = \pi' \circ \sigma_2$ there exists a unique $\epsilon : Y \to Y'$ such that $\epsilon \circ \pi = \pi'$. We write $Y = X/\sigma$. (Categorical quotients are sometimes called co-equalizers.) We will also give, in each concrete example, a class of objects of $\mathcal{C}$ which we call *trivial*. For instance, if $\mathcal{C}$ is the category of algebraic varieties, the trivial objects will be declared to be the points. If $\mathbf{X}$ is a correspondence between curves, possessing an infinite orbit (i.e., a sequence of distinct points $Q_1, Q_2, ... \in \tilde{X}$ such that $\sigma_2(Q_i) = \sigma_1(Q_{i+1})$ for $i \geq 1$), then clearly X/σ is trivial. To remedy this situation we will proceed as follows.

1) For each p we will "adjoin" the Fermat quotient operator $\delta = \delta_p$ to usual algebraic geometry; this will lead us to consider a category $\mathcal{C}_\delta$ that underlies what we shall refer to as "$\delta-$geometry".

2) For any correspondence $\mathbf{X}_\mathcal{O}$ in the category of smooth curves over the ring of $S-$integers $\mathcal{O}$ of a number field we will consider the correspondences $\mathbf{X}_\wp$ and $\mathbf{X}_\mathbf{C}$ deduced by base change via $\mathcal{O} \subset \hat{\mathcal{O}}_\wp = \hat{\mathbf{Z}}_p^{ur}$ and $\mathcal{O} \subset \mathbf{C}$, where $\wp$ runs through the set of unramified places outside S. To each $\mathbf{X}_\wp = (X_\wp, \sigma_\wp)$ we will associate a correspondence $\mathbf{X}_\delta = (X_\delta, \sigma_\delta)$ in $\mathcal{C}_\delta$, where $\delta = \delta_p$.

3) We will formulate a conjecture (and state results along this conjecture) essentially asserting that if $\mathbf{X}_\mathbf{C}$ has an infinite orbit then X_δ/σ_δ is non-trivial in $\mathcal{C}_\delta$ for almost all places $\wp$ if and only if $\mathbf{X}_\mathbf{C}$ admits an analytic uniformization (in a sense to be explained below).

The rest of the paper is devoted to explaining the above 3 steps.

4. Uniformization

We begin by explaining the concept of analytic uniformization for correspondences on complex algebraic curves. Let $\mathbf{X} = (X, \sigma)$ be a correspondence in the category of complex algebraic curves. We assume $X, \tilde{X}$ are non-singular connected and σ_1 and σ_2 are dominant. We say that $\mathbf{X}$ has an *analytic uniformization* if one can find a diagram of Riemann surfaces

$$\begin{array}{ccccc} \mathbf{S} & \xleftarrow{\tau_1} & \mathbf{S} & \xrightarrow{\tau_2} & \mathbf{S} \\ \pi \downarrow & & \downarrow \tilde{\pi} & & \downarrow \pi \\ X' & \xleftarrow{\sigma_1'} & \tilde{X}' & \xrightarrow{\sigma_2'} & X' \\ u \uparrow & & \uparrow \tilde{u} & & \uparrow u \\ X & \xleftarrow{\sigma_1} & \tilde{X} & \xrightarrow{\sigma_2} & X \end{array}$$

with $\mathbf{S}$ a simply connected Riemann surface, τ_1, τ_2 automorphisms of $\mathbf{S}$, $\pi, \tilde{\pi}$ Galois covers of degree $\leq \infty$, and $u, \tilde{u}$ inclusions with $X' \backslash X$ and $\tilde{X}' \backslash \tilde{X}$ finite sets containing the ramification locus of π and $\tilde{\pi}$ respectively. It is easy to "classify" all correspondences which admit an analytic uniformization and possess an infinite orbit. The details of the classification are tedious and will be skipped here; we content ourselves with a few remarks. There are 3 cases: the spherical, flat and hyperbolic case according as $\mathbf{S}$ is $\mathbf{CP}^1$, $\mathbf{C}$, or $\mathbf{H}$ (the upper half plane) respectively. In the spherical case everything boils down to the (well known) classification of finite groups of automorphisms of $\mathbf{CP}^1$. In the flat case the Galois groups of π and $\tilde{\pi}$ are crystallographic (i.e., contain a normal subgroup of finite index consisting of translations); the resulting list of possible $\mathbf{X}$'s is a variation on "Thurston's list" of postcritically finite non-hyperbolic dynamical systems; cf. [**DH93**]. (The baby examples in the previous section are in