DIFFERENTIAL CALCULUS WITH INTEGERS

ALEXANDRU BUIUM

Abstract. Ordinary differential equations have an arithmetic analogue in which functions are replaced by numbers and the derivation operator is replaced by a Fermat quotient operator. In this survey we explain the main motivations, constructions, results, applications, and open problems of the theory.

The main purpose of these notes is to show how one can develop an arithmetic analogue of differential calculus in which differentiable functions $x(t)$ are replaced by integer numbers n and the derivation operator $x \mapsto \frac{dx}{dt}$ is replaced by the Fermat quotient operator $n \mapsto \frac{n-n^p}{p}$, where p is a prime integer. The Lie-Cartan geometric theory of differential equations (in which solutions are smooth maps) is then replaced by a theory of "arithmetic differential equations" (in which solutions are integral points of algebraic varieties). In particular the differential invariants of groups in the Lie-Cartan theory are replaced by "arithmetic differential invariants" of correspondences between algebraic varieties. A number of applications to diophantine geometry over number fields and to classical modular forms will be explained.

This program was initiated in [11] and pursued, in particular, in [12]-[35]. For an exposition of some of these ideas we refer to the monograph [16]; cf. also the survey paper [58]. We shall restrict ourselves here to the *ordinary differential* case. For the *partial differential* case we refer to [20, 21, 22, 7]. Throughout these notes we assume familiarity with the basic concepts of algebraic geometry and differential geometry; some of the standard material is being reviewed, however, for the sake of introducing notation, and "setting the stage". The notes are organized as follows. The first section presents some classical background, the main concepts of the theory, a discussion of the main motivations, and a comparison with other theories. The second section presents a sample of the main results. The third section presents a list of open problems.

Acknowledgement. The author is indebted to HIM for support during part of the semester on Algebra and Geometry in Spring 2013. These notes are partially based on lectures given at the IHES in Fall 2011 and MPI in Summer 2012 when the author was partially supported by IHES and MPI respectively. Partial support was also received from the NSF through grant DMS 0852591.

1. Main concepts

1.1. **Classical analogies.** The analogies between functions and numbers have played a key role in the development of modern number theory. Here are some

classical analogies. All facts in this subsection are well known and entirely classical; we review them only in order to introduce notation and put things in perspective.

1.1.1. *Polynomial functions.* The ring $\mathbb{C}[t]$ of polynomial functions with complex coefficients is analogous to the ring $\mathbb{Z}$ of integers. The field of rational functions $\mathbb{C}(t)$ is then analogous to the field of rational numbers $\mathbb{Q}$. In $\mathbb{C}[t]$ any non-constant polynomial is a product of linear factors. In $\mathbb{Z}$ any integer different from $0, \pm 1$ is up to a sign a product of prime numbers. To summarize

$$\mathbb{C} \subset \mathbb{C}[t] \subset \mathbb{C}(t)$$

are analogous to

$$\{0, \pm 1\} \subset \mathbb{Z} \subset \mathbb{Q}$$

1.1.2. *Regular functions.* More generally rings $\mathcal{O}(T)$ of regular functions on complex algebraic affine non-singular curves T are analogous to rings of integers $\mathcal{O}_F$ in number fields F. Hence curves T themselves are analogous to schemes $Spec\ \mathcal{O}_F$. Compactifications

$$T \subset \overline{T} = T \cup \{\infty_1, ..., \infty_n\} \simeq (\text{compact Riemann surface of genus } g)$$

are analogous to "compactifications"

$$Spec\ \mathcal{O}_F \subset \overline{Spec\ \mathcal{O}_F} = (Spec\ \mathcal{O}_F) \cup \frac{Hom(F, \mathbb{C})}{\text{conjugation}}$$

1.1.3. *Formal functions.* The inclusions

$$\mathbb{C} \subset \mathbb{C}[[t]] \subset \mathbb{C}((t))$$

(where $\mathbb{C}[[t]]$ is the ring of power series and $\mathbb{C}((t))$ is the ring of Laurent series) are analogous to the inclusion

$$\{0\} \cup \mu_{p-1} = \{c \in \mathbb{Z}_p; c^p = c\} \subset \mathbb{Z}_p \subset \mathbb{Q}_p$$

(where $\mathbb{Z}_p$ is ring of p-adic integers and $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$). Recall that

$$\mathbb{Z}_p = \lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z} = \{\sum_{n=0}^{\infty} c_i p^i; c_i \in \{0\} \cup \mu_{p-1}\}$$

So $\{0\} \cup \mu_{p-1}$ plays the role of "constants" in $\mathbb{Z}_p$. Sometimes we need more "constants" and we are led to consider, instead, the inclusions:

$$\{0\} \cup \bigcup_{\nu} \mu_{p^\nu - 1} \subset \widehat{\mathbb{Z}_p^{ur}} \subset \widehat{\mathbb{Z}_p^{ur}}[1/p]$$

where

$$\widehat{\mathbb{Z}_p^{ur}} = \mathbb{Z}_p[\zeta; \zeta^{p^\nu - 1} = 1, \nu \geq 1]\hat{} = \{\sum_{i=0}^{\infty} c_i p^i; c_i \in \{0\} \cup \bigcup_{\nu} \mu_{p^\nu - 1}\}.$$

Here the upper hat on a ring A means its p-adic completion:

$$\widehat{A} := \lim_{\leftarrow} A/p^n A.$$

So in the latter case the monoid $\{0\} \cup \bigcup_\nu \mu_{p^\nu - 1}$ should be viewed as the set of "constants" of $\widehat{\mathbb{Z}_p^{ur}}$; this is consistent with the "philosophy of the field with one element" to which we are going to allude later. Let us say that a ring is a *local p-ring* if it is a discrete valuation ring with maximal ideal generated by a prime $p \in \mathbb{Z}$. Then $\mathbb{Z}_p$ and $\widehat{\mathbb{Z}_p^{ur}}$ are local p-rings. Also for any local p-ring R we denote by

$k = R/pR$ the residue field and by $K = R[1/p]$ the fraction field of R. Sometimes we will view local p-rings as analogues of rings $\mathbb{C}\{x\}$ of germs of analytic functions on Riemann surfaces and even as analogues of rings of global analytic (respectively C^∞ functions) on a Riemann surface T (respectively on a 1-dimensional real manifold T, i.e. on a circle S^1 or $\mathbb{R}$).

1.1.4. *Topology.* Fundamental groups of complex curves (more precisely Deck transformation groups of normal covers $T' \to T$ of Riemann surfaces) have, as analogues, Galois groups $G(F'/F)$ of normal extensions number fields $F \subset F'$. The genus of a Riemann surface has an analogue for number fields defined in terms of ramification. All of this is very classical. There are other, less classical, topological analogies like the one between primes in $\mathbb{Z}$ and nodes in 3-dimensional real manifolds [61].

1.1.5. *Divisors.* The group of divisors

$$Div(\overline{T}) = \{\sum_{P \in \overline{T}} n_P P; n_P \in \mathbb{Z}\}$$

on a non-singular complex algebraic curve $\overline{T}$ is analogous to the group of divisors

$$Div(\overline{Spec\ \mathcal{O}_F}) = \{\sum \nu_P P; \nu_P \in \mathbb{Z} \text{ if } P \text{ is finite}, \nu_P \in \mathbb{R} \text{ if } P \text{ is infinite}\}$$

One can attach divisors to rational functions f on $\overline{T}$ ($Div(f)$ is the sum of poles minus the sum of zeroes); similarly one can attach divisors to elements $f \in F$. In both cases one is lead to a "control" of the spaces of fs that have a "controlled" divisor (the Riemann-Roch theorem). One also defines in both settings divisor class groups. In the geometric setting the divisor class group of $\overline{T}$ is an extension of $\mathbb{Z}$ by the Jacobian

$$Jac(\overline{T}) = \mathbb{C}^g/(\text{period lattice of } \overline{T})$$

where g is the genus of $\overline{T}$. In the number theoretic setting divisor class groups can be interpreted as "Arakelov class groups"; one recaptures, in particular, the usual class groups $Cl(F)$. Exploring usual class groups "in the limit", when one adjoins roots of unity, leads to Iwasawa theory. We will encounter Jacobians later in relation, for instance, to the Manin-Mumford conjecture. This conjecture (proved by Raynaud) says that if one views $\overline{T}$ as embedded into $Jac(\overline{T})$ (via the "Abel-Jacobi map") the the intersection of $\overline{T}$ with the torsion group of $Jac(\overline{T})$ is a finite set. This particular conjecture does not seem to have an analogue for numbers.

1.1.6. *Families.* Maps

$$M \to T$$

of complex algebraic varieties, complex analytic, or real smooth manifolds, where $\dim T = 1$, are analogous to arithmetic schemes i.e. schemes of finite type

$$X \to Spec\ R$$

where R is either the ring of integers $\mathcal{O}_F$ in a number field F or a complete local p-ring respectively. Note however that in this analogy one "goes arithmetic only half way": indeed for $X \to Spec\ R$ the basis is arithmetic yet the fibers are still geometric. One can attempt to "go arithmetic all the way" and find an analogue of $M \to T$ for which both the base and the fiber are "arithmetic"; in particular one would like to have an analogue of $T \times T$ which is "arithmetic" in two directions. This is one of the main motivations in the search for $\mathbb{F}_1$, the "field with one element".

1.1.7. *Sections.* The set of sections

$$\Gamma(M/T) = \{s : T \to M; \pi \circ \sigma = 1\}$$

of a map $\pi : M \to T$ is analogous to the set

$$X(R) = \{s : Spec\ R \to X; \pi \circ s = 1\}$$

of R-points of X where $\pi : X \to Spec\ R$ is the structure morphism. This analogy suggests that finiteness conjectures for sets of the form $X(R)$, which one makes in Diophantine geometry, should have as analogues finiteness conjectures for sets of sections $\Gamma(M/T)$. A typical example of this phenomenon is the Mordell conjecture (Faltings' theorem) saying that if X is an algebraic curve of "genus" ≥ 2, defined by polynomials with coefficients in a number field F, then the set $X(F)$ is finite. Before the proof of this conjecture Manin [55] proved a parallel finiteness result for $\Gamma(M/T)$ where $M \to T$ is a "non-isotrivial" morphism from an algebraic surface to a curve, whose fibers have genus ≥ 2. Manin's proof involved the consideration of differential equations with respect to vector fields on T. Faltings' proof went along completely different lines. This raised the question whether one can develop a theory of differential equations in which one can differentiate numbers.

All these examples of analogies are classical; cf. work of Dedekind, Hilbert, Hensel, Artin, Weil, Lang, Tate, Iwasawa, Grothendieck, and many others.

1.2. **Analogies proposed in** [11]**-**[35]**.** One thing that seems to be missing from the classical picture is a counterpart, in number theory, of the differential calculus (in particular of differential equations) for functions. Morally the question is whether one can meaningfully consider (and successfully use) "arithmetic differential equations" satisfied by numbers. In our research on the subject [11] - [35] we proposed such a theory based on the following sequence of analogies:

1.2.1. *Derivatives.* The derivative operator $\delta_t = \frac{d}{dt} : \mathbb{C}[t] \to \mathbb{C}[t]$ is analogous to the *Fermat quotient operator* $\delta = \delta_p : \mathbb{Z} \to \mathbb{Z}$, $\delta_p a = \frac{a - a^p}{p}$. More generally the derivative operator $\delta_t = \frac{d}{dt} : C^\infty(\mathbb{R}) \to C^\infty(\mathbb{R})$ (with t the coordinate on $\mathbb{R}$) is analogous to the operator $\delta = \delta_p : R \to R$ on a complete local p-ring R, $\delta_p \alpha = \frac{\phi(\alpha) - \alpha^p}{p}$ (where $\phi : R \to R$ is a fixed homomorphism lifting the p-power Frobenius map on R/pR). The map $\delta = \delta_p$ above is, of course, not a derivation but, rather, it satisfies the following conditions:

$$\begin{array}{lcl} \delta(1) & = & 0 \\ \delta(a+b) & = & \delta(a) + \delta(b) + C_p(a,b) \\ \delta(ab) & = & a^p \delta(b) + b^p \delta(a) + p\delta(a)\delta(b), \end{array}$$

where $C_p(x,y) \in \mathbb{Z}[x,y]$ is the polynomial $C_p(x,y) = p^{-1}(x^p + y^p - (x+y)^p)$. Any set theoretic map $\delta : A \to A$ from a ring A to itself satisfying the above axioms will be referred to a *p-derivation*; such operators were introduced independently in [49, 11] and they implicitly arise in the theory of Witt rings. For any such δ, the map $\phi : A \to A$, $\phi(a) = a^p + p\delta a$ is a ring homomorphism lifting the p-power Frobenius on A/pA; and vice versa, given a p-torsion free ring A and a ring homomorphism $\phi : A \to A$ lifting Frobenius the map $\delta : A \to A$, $\delta a = \frac{\phi(a) - a^p}{p}$ is a p-derivation.

1.2.2. *Differential equations.* Differential equations $F(t, x, \delta_t x, ..., \delta_t^n x) = 0$ (with F smooth) satisfied by smooth functions $x \in C^\infty(\mathbb{R})$ are replaced by *arithmetic differential equations* $F(\alpha, \delta_p \alpha, ..., \delta_p^n \alpha) = 0$ with $F \in R[x_0, x_1, ..., x_n]^\wedge$ satisfied by numbers $\alpha \in R$. As we shall see it is crucial to allow F to be in the p-adic completion of the polynomial ring rather than in the polynomial ring itself; indeed if one restricts to polynomial F's the main interesting examples of the theory are left out.

1.2.3. *Jet spaces.* More generally, the Lie-Cartan geometric theory of differential equations has an arithmetic analogue which we explain now. Let $M \to T$ be a submersion of smooth manifolds with $\dim T = 1$, and let

$$J^n(M/T) = \{J_t^n(s); s \in \Gamma(M/T), t \in T\}$$

be the space of n-jets $J_t^n(s)$ of smooth sections s of $M \to T$ at points $t \in T$. Cf. [1, 48, 63] for references to differential geometry. If $M = \mathbb{R}^d \times \mathbb{R}$, $T = \mathbb{R}$, $M \to T$ is the second projection, and $x = (x_1, ..., x_d)$, t are global coordinates on $\mathbb{R}^d$ and $\mathbb{R}$ respectively then $J^n(M/T) = \mathbb{R}^{(n+1)d} \times \mathbb{R}$ with *jet coordinates* $x, x', ..., x^{(n)}, t$. So for general $M \to T$ the map $J^n(M/T) \to M$ is a fiber bundle with fiber $\mathbb{R}^{nd}$ where $d + 1 = \dim(M)$. One has the total derivative operator

$$\delta_t : C^\infty(J^n(M/T)) \to C^\infty(J^{n+1}(M/T))$$

which in coordinates is given by

$$\delta_t = \frac{\partial}{\partial t} + \sum_{j=0}^{n} \sum_{i=1}^{d} x_i^{(j+1)} \frac{\partial}{\partial x_i^{(j)}}.$$

In the arithmetic theory the analogues of the manifolds $J^n(M/T)$ are certain formal schemes (called *arithmetic jet spaces* or *p-jet spaces*) $J^n(X) = J^n(X/R)$ defined as follows. Assume X is affine, $X = Spec\ \frac{R[x]}{(f)}$ with x, f tuples; the construction that follows is easily globalized to the non-affine case. Let $x', ..., x^{(n)}, ...$ be new tuples of variables, consider the polynomial ring $R\{x\} := R[x, x', x'', ...]$, let $\phi : R\{x\} \to R\{x\}$ be the unique ring homomorphism extending ϕ on R and sending $\phi(x) = x^p + px'$, $\phi(x') = (x')^p + px''$,..., and let

$$\delta = \delta_p : R\{x\} \to R\{x\}$$

be the p-derivation

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

Then one defines

$$J^n(X) = Spf\ \frac{R[x, x', ..., x^{(n)}]^\wedge}{(f, \delta f, ..., \delta^n f)}.$$

1.2.4. *Differential equations on manifolds.* Usual *differential equations* are defined geometrically as elements of the ring $C^\infty(J^n(M/T))$; alternatively such elements are referred to as (time dependent) *Lagrangians* on M. Their analogue in the arithmetic theory, which we call *arithmetic differential equations* [16], are the elements of the ring $\mathcal{O}^n(X) := \mathcal{O}(J^n(X))$. For group schemes the following concept [11] plays an important role: if G is a group scheme of finite type over R then we may consider the R-module $\mathcal{X}^n(G) = Hom_{gr}(J^n(G), \widehat{\mathbb{G}}_a) \subset \mathcal{O}^n(G)$.

Going back to arbitrary schemes of finite type X/R note that $\delta_p : R\{x\} \to R\{x\}$ induces maps $\delta = \delta_p : \mathcal{O}^n(X) \to \mathcal{O}^{n+1}(X)$ which can be viewed as arithmetic

analogues of the total derivative operator $\delta_t : C^\infty(J^n(M/T)) \to C^\infty(J^{n+1}(M/T))$. The latter is a "generator" of the Cartan distribution defined by $dx_i - x_i' dt$, $dx_i' - x_i'' dt$, etc. Note however that the forms in differential geometry defining the Cartan distribution do not have a direct arithmetic analogue; for one thing there is no form "dp" analogous to dt. On the other hand in the arithmetic case we have induced ring homomorphisms $\phi : \mathcal{O}^n(X) \to \mathcal{O}^{n+1}(X)$ which have no analogue in differential geometry.

1.2.5. *Differential functions.* Any differential equation $F \in C^\infty(J^n(M/T))$ defines a natural *differential function* $F_* : \Gamma(M/T) \to C^\infty(T)$; in coordinates sections $s \in \Gamma(M/T)$ correspond to functions $x = x(t)$ and then F_* sends $x(t)$ into $F_*(x(t)) = F(x(t), \delta_t x(t), ..., \delta_t^n x(t))$. Analogously any arithmetic differential equation $f \in \mathcal{O}(J^n(X))$ defines a map of sets $f_* : X(R) \to R$, referred to as a δ-*function*, which in affine coordinates sends $\alpha \in X(R) \subset R^N$ into $f_*(\alpha) := F(\alpha, \delta_p \alpha, ..., \delta_p^n \alpha) \in R$ if $F \in R[x, x', ..., x^{(n)}]^\wedge$ represents f. If $X = G$ is in addition a group scheme and $\psi \in \mathcal{X}^n(G)$ then $\psi_* : G(R) \to \mathbb{G}_a(R) = R$ is a group homomorphism called a δ-*character* of G. For X/R smooth and R/pR algebraically closed f is uniquely determined by f_* so one can identify f with f_* and ψ with ψ_*.

1.2.6. *Prolongations of vector fields.* For any vertical vector field

$$\xi := \sum_{i=1}^{d} a_i(t, x) \frac{\partial}{\partial x_i}$$

on M/T one can consider the canonical prolongations

$$\xi^{(n)} := \sum_{j=0}^{n} \sum_{i=1}^{d} (\delta_t^j a_i(t, x)) \frac{\partial}{\partial x_i^{(j)}}$$

on $J^n(M/T)$. The map

$$\xi^{(n)} : C^\infty(J^n(M/T)) \to C^\infty(J^n(M/T))$$

is the unique $\mathbb{R}$-derivation whose restriction to $C^\infty(M)$ is ξ and which commutes with the total derivative operator δ_t. The above construction has an arithmetic analogue that plays a key technical role in the development of the theory. Indeed for any affine smooth X/R and any R-derivation $\xi : \mathcal{O}(X) \to \mathcal{O}(X)$ the canonical prolongation

$$\xi^{(n)} : \mathcal{O}^n(X)[1/p] \to \mathcal{O}^n(X)[1/p]$$

is defined as the unique $K = R[1/p]$-derivation whose restriction to $\mathcal{O}(X)$ is ξ and which commutes with ϕ. This construction then obviously globalizes.

1.2.7. *Infinitesimal symmetries of differential equations.* Some Galois theoretic concepts based on prolongations of vector fields have arithmetic analogues. Indeed recall that if $\mathcal{L} \subset C^\infty(J^n(M/T))$ is a linear subspace of differential equations then a vertical vector field ξ on M/T is called an *infinitesimal symmetry* of $\mathcal{L}$ if $\xi^{(n)}\mathcal{L} \subset \mathcal{L}$; it is called a *variational infinitesimal symmetry* if $\xi^{(n)}\mathcal{L} = 0$. Similarly given an R-submodule $\mathcal{L} \subset \mathcal{O}^n(X)$ an *infinitesimal symmetry* of $\mathcal{L}$ is an R-derivation $\xi : \mathcal{O}(X) \to \mathcal{O}(X)$ such that $\xi^{(n)}\mathcal{L} \subset \mathcal{L}[1/p]$. One says ξ is a *variational infinitesimal symmetry* of $\mathcal{L}$ if $\xi^{(n)}\mathcal{L} = 0$.

1.2.8. *Total differential forms on manifolds.* Recall that a *total differential form* ([63], p. 351) on M/T is an expression that in coordinates looks like a sum of expressions

$$F(t, x, x', ..., x^{(n)})dx_{j_1} \wedge ... \wedge dx_{j_i},$$

It is important to introduce an arithmetic analogue of this which we now explain. We consider the case of top forms ($i = d$) which leads to what we will call δ-*line bundles*. Denote by $\mathcal{O}^n$ the sheaf $U \mapsto \mathcal{O}^n(U)$ on X for the Zariski topology. Define a δ-*line bundle* of order n on X to be a locally free $\mathcal{O}^n$-module of rank 1. Integral powers of bundles need to be generalized as follows. Set $W = \mathbb{Z}[\phi]$ (ring of polynomials with $\mathbb{Z}$-coefficients in the symbol ϕ). For $w = \sum a_s \phi^s$ write $deg(w) = \sum a_s$. Also let W_+ be the set of all $w = \sum a_s \phi^s \in W$ with $a_s \geq 0$ for all s. If L is a line bundle on X given by a cocycle (g_{ij}) and $w = \sum_{s=0}^n a_s \phi^s \in W$, $w \neq 0$, $a_n \neq 0$, then define a δ-line bundle L^w of order n by the cocycle (g_{ij}^w), $g_{ij}^w = \prod_s \phi^s(g_{ij})^{a_s}$. With all these definitions in place we may define the following rings which, by the way, are the main objects of the theory:

$$R_\delta(X, L) = \bigoplus_{0 \neq w \in W_+} H^0(X, L^w).$$

Note that the above is a graded ring without unity. The homogeneous elements of $R_\delta(X, L)$ can be viewed as arithmetic analogues of Lagrangian densities and can also be referred to as *arithmetic differential equations* [16].

1.2.9. *Differential forms on jet spaces and calculus of variations.* The spaces

$$\Omega^i_\uparrow(J^n(M/T))$$

of vertical smooth i-forms on $J^n(M/T)$ (generated by i-wedge products of forms $dx, dx', ..., dx^{(n)}$) play an important role in the calculus of variations [63]. These spaces fit into a deRham complex where the differential is the vertical exterior differential

$$d_\uparrow : \Omega^i_\uparrow(J^n(M/T)) \to \Omega^{i+1}_\uparrow(J^n(M/T))$$

with respect to the variables $x, x', ..., x^{(n)}$. On the other hand we have unique operators

$$\delta_t : \Omega^i_\uparrow(J^n(M/T)) \to \Omega^i_\uparrow(J^{n+1}(M/T))$$

that commute with $d_\uparrow$, induce a derivation on the exterior algebra, and for $i = 0$ coincide with the total derivative operators. Then one can define spaces of *functional forms* ([63], p. 357)

$$\Omega^i_*(J^n(M/T)) = \frac{\Omega^i_\uparrow(J^n(M/T))}{Im(\delta_t)}$$

and the (vertical part of the) *variational complex* ([63], p. 361) with differentials

$$d : \Omega^i_*(J^n(M/T)) \to \Omega^{i+1}_*(J^n(M/T)).$$

The class of $\omega \in \Omega^i_\uparrow(J^n(M/T))$ in $\Omega^i_*(J^n(M/T))$ is denoted by $\int \omega dt$. For $i = 0$, $\omega = F$, have the formula $d(\int F dt) = \int EL(F) dt$ in $\Omega^i_*(J^{2n}(M/T))$ where $EL(F) = \sum_{i=1}^d F_i dx_i$ is the *Euler-Lagrange* total differential form,

$$F_i = \sum_{j=0}^n (-1)^j \delta_t^j \left(\frac{\partial F}{\partial x_i^{(j)}} \right).$$

Noether's theorem then says that for any vertical vector field ξ on M/T we have the formula

$$\langle \xi, EL(F)\rangle - \xi^{(n)}(F) = \delta_t G$$

for some $G \in C^\infty(J^{2n-1}(M/T))$; G is unique up to a constant. If ξ is a variational infinitesimal symmetry of F then G is referred to as the *conservation law* attached to this symmetry; in this case if $x(t)$ is a solution of all $F_i = 0$ then G evaluated at $x(t)$ will be a constant.

Analogously, for X/R smooth and affine, one can consider the modules $\Omega^i_{\mathcal{O}^n(X)/R}$ defined as the exterior powers of the inverse limit of the Käher differentials

$$\Omega_{\mathcal{O}^n(X)\otimes(R/p^nR)/(R/p^nR)},$$

and the exterior differential

$$d : \Omega^i_{\mathcal{O}^n(X)/R} \to \Omega^{i+1}_{\mathcal{O}^n(X)/R}.$$

Also one may consider the operators

$$\phi^* : \Omega^i_{\mathcal{O}^n(X)/R} \to \Omega^i_{\mathcal{O}^{n+1}(X)/R};$$

again ϕ^* and d commute. Also note that any element in the image of ϕ^* is uniquely divisible by p^i; for any $\omega \in \Omega^i_{\mathcal{O}^n(X)/R}$ and $r \geq 0$ we then set $\omega_r = p^{-ir}\phi^{*r}\omega$. The operation $p^{-ir}\phi^{*r}$ is a characteristic zero version of the inverse Cartier operator. For any element $\mu \in R$ (which we refer to as *eigenvalue*) one can define groups

$$\Omega^i_*(J^n(X)) = \frac{\Omega^i_{\mathcal{O}^n(X)/R}}{Im(\phi^* - \mu)}$$

that fit into a *variational complex* with differentials

$$d : \Omega^i_*(J^n(X)) \to \Omega^{i+1}_*(J^n(X)).$$

The class of $\omega \in \Omega^i_{\mathcal{O}^n(X)/R}$ in $\Omega^i_*(J^n(X))$ is denoted by $\int \omega dp$. For $i = 0$, $\mu = 1$, $\omega = F \in \mathcal{O}^n(X)$ we have $d(\int F dp) = \int \{\sum_{i=1}^d F_i \omega_n^i\} dp$ in $\Omega^1_*(J^{2n}(X))$ where $F_i \in \mathcal{O}^{2n}(X)$, ω^i is a basis of $\Omega_{\mathcal{O}(X)/R}$, and $\omega_n^i = p^{-n}\phi^{*n}\omega^i$. Also an analogue of the Noether theorem holds in this context with $\epsilon(F) := \sum_{i=1}^d F_i \omega_n^i$ playing the role of the Euler-Lagrange form; indeed for any vector field ξ on X there exists $G \in \mathcal{O}^{2n-1}(X)$ such that

$$\langle \xi^{(n)}, \epsilon(F)\rangle - \xi^{(n)}(F) = G^\phi - G.$$

If ξ is a variational infinitesimal symmetry of F then G can be referred to as a *conservation law*; in this case if $P \in X(R)$ is a point which is a solution to all $F_{i*}(P) = 0$ then $G_*(P)^\phi = G_*(P)$.

1.2.10. *Flows and Hamiltonian formalism* [31]. We place ourselves in either the smooth or the complex analytic setting. Assume one is given a section $\sigma : M \to J^1(M/T)$ of the projection $J^1(M/T) \to M$. To give such a σ is equivalent to giving a vector field δ_M on M lifting δ_t; such a vector field can be referred to as a δ_t-flow on M/T. In coordinates, if σ is defined by $(t, x) \mapsto (t, x, s(t, x))$, then

$$\delta_M = \sum s_i(t, x)\frac{\partial}{\partial x_i}.$$

The composition

$$L_{\delta_M} : \Omega^i_\uparrow(M/T) \xrightarrow{\delta_t} \Omega^i_\uparrow(J^1(M/T)) \xrightarrow{\sigma^*} \Omega^i_\uparrow(M/T)$$

induces a derivation on the exterior algebra of vertical forms on M/T, commutes with exterior vertical differentiation $d_\uparrow$, and coincides with δ_M for $i = 0$; one can refer to L_{δ_M} as the "Lie derivative" attached to the vector field δ_M (it is a relative version of the usual Lie derivative).

We consider now the "time dependent" Hamiltonian formalism. The classical treatment of this formalism (e.g. [56] or [62], p. 491) involves the cotangent bundle T^*N of a space-time manifold N and it explicitly involves the differential of time, dt. Say, for instance, that $N = F \times T$ is 2-dimensional with coordinate x on F and t on T; consider the cotangent space T^*F of F with coordinates (x, z), where z corresponds to the global function defined by dx; consider also the cotangent space T^*T of T (the notation involving two different uses of the letter "T" should not be confusing) with coordinates (t, E), where, again, E corresponds to dt, and, morally, the letter E stands for "energy." So the cotangent space $M^* := T^*N$ of N has coordinates (x, z, t, E). Let $H = H(x, z, t)$ be a "time dependent Hamiltonian" and define the *extended Hamiltonian* $\widehat{H} = H(x, z, t) - E$; it is a function on M^*. Then the time dependent Hamilton equations are

$$\begin{aligned} \dot{x} &= \frac{\partial \widehat{H}}{\partial z} = \frac{\partial H}{\partial z}, \\ \dot{z} &= -\frac{\partial \widehat{H}}{\partial x} = -\frac{\partial H}{\partial x}, \\ \dot{t} &= -\frac{\partial \widehat{H}}{\partial E} = 1, \\ \dot{E} &= \frac{\partial \widehat{H}}{\partial t}; \end{aligned}$$

they define a flow on M^*. The *symplectic form* on M^* giving rise to this system is

$$\widehat{\Omega} := dz \wedge dx - dE \wedge dt = d(zdx - Edt).$$

Since "dp" does not exist in the arithmetic setting what we will do will be to first find a presentation of the classical time dependent Hamiltonian formalism without reference to dt and then we shall transpose the latter to the arithmetic case. Our modified formalism will involve the first jet space of N over T hence, morally, the tangent, rather than cotangent, bundle of N; the absence of dt in our modified formalism is compensated by the consideration of the total derivative operator which involves $\frac{\partial}{\partial t}$. To explain our modified formalism assume in what follows that M is a manifold of dimension 3 fibered over the one dimensional manifold T so the fibers of $M \to T$ are 2-dimensional. (In applications one usually takes $M = J^1(N/T)$, where $N \to T$, N of dimension 2. So note the discrepancy with the "usual" Hamiltonian formalism in which M^* has dimension 4 rather than 3.) A *vertical symplectic form* on M is a nowhere vanishing vertical 2-form on M. A *vertical contact form* on M is a vertical 1-form ν on M such that $d\nu$ is symplectic. We shall drop the word "vertical" in what follows. Recall that a δ_t-flow on M is a vector field δ_M on M that lifts the vector field δ_t on T; and recall that to give a δ-flow on M is the same as to give a section of the projection $J^1(M/T) \to M$. Given a δ-flow δ_M as above we may consider the relative Lie derivative L_{δ_M} on the vertical forms $\Omega^i(M/T)$. A δ_t-flow δ_M will be called *Hamiltonian* with respect to a symplectic form η on M if $L_{\delta_M}\eta = \mu \cdot \eta$ for some function μ on T. Note that if $\delta_t\gamma = -\mu \cdot \gamma$ for some function γ on T and if $\eta_1 = \gamma\eta$ then $L_{\delta_M}\eta_1 = 0$. If ν is a contact form, $\eta = d_\uparrow\nu$, and δ_M is a δ_t-flow which is Hamiltonian with respect to

η (hence $L_{\delta_M}\eta = \mu\eta$) then $\epsilon := L_{\delta_M}\nu - \mu\nu$ is closed; the latter can be referred to as an Euler-Lagrange form attached to the symplectic form η and the δ_t-flow δ_M. If ϵ happens to be exact, i.e. $L_{\delta_M}\nu - \mu\nu = d\mathcal{L}$ for some function $\mathcal{L}$ on M, then $\mathcal{L}$ can be referred to as a Lagrangian attached to η and δ_M. (This Euler-Lagrange formalism is related to, but does not coincide with, the Euler-Lagrange formalism in 1.2.9.)

In the special case when $M = J^1(N/T)$ a 1-form on M is called *canonical* if it is a function on M times the pull-back of a 1-form on N. In this situation one is sometimes interested in δ_t-flows defined by sections of $J^1(M/T) \to M = J^1(N/T)$ that arise from sections of $J^2(N/T) \to J^1(N/T)$ (where $J^2(N/T)$ is naturally embedded into $J^1(M/T)$); such δ_t-flows are referred to as *canonical* and are defined by order 2 differential equations (functions on $J^2(N)$).

A justification for the above terminology comes, for instance, from the following local considerations. We will place ourselves in an algebraic setting in what follows; there is a natural C^∞ counterpart of this discussion, of course. Let F be a field equipped with a derivation $\delta : F \to F$ (e.g. $F = \mathbb{C}((t))$, $\delta = \delta_t$) and let A be a ring isomorphic to a power series ring in 2 variables with coefficients in F. Choose formal coordinates $x, y \in A$ (i.e. $A = F[[x, y]]$), and set $\Omega_A = A \cdot dx + A \cdot dy$, $\Omega_A^2 = A \cdot dx \wedge dy$. A form $\eta = u dx \wedge dy \in \Omega_A^2$ is called invertible if $u(0, 0) \neq 0$. (These definitions are independent of the choice of the formal coordinates x, y.) The following is a translation into the language of differential algebra of the classical Hamiltonian/Lagrangian formalism in 2 analytic coordinates. Assume one is given a derivation $\delta : A \to A$ such that $\delta F \subset F$ and sending the maximal ideal of A into itself. Then the following are easy to check:

1) Assume we are given an invertible $\eta \in \Omega_A^2$. Then there exist formal coordinates $x, y \in A$ such that $\eta = dy \wedge dx$. Furthermore if $\delta\eta = 0$ then and there exists an element $\mathcal{H} \in A$ such that

$$\delta y = -\frac{\partial \mathcal{H}}{\partial x}, \quad \delta x = \frac{\partial \mathcal{H}}{\partial y}.$$

2) Assume there exist formal coordinates $x, y \in A$, and a series $\mathcal{H} \in A$ (interpreted as a "Hamiltonian") such that $\delta y = -\frac{\partial \mathcal{H}}{\partial x}$ and $\delta x = \frac{\partial \mathcal{H}}{\partial y}$. Set $\eta = dy \wedge dx$, $\nu = y dx$, $\epsilon = \delta\nu$, and $\mathcal{L} = y\frac{\partial \mathcal{H}}{\partial y} - \mathcal{H} = y\delta x - \mathcal{H}$. (So $\mathcal{L}$ is interpreted as the "Lagrangian.") Then

$$d\nu = \eta, \quad \delta\eta = 0, \quad d\mathcal{L} = \epsilon.$$

3) Assume the notation in 2) and assume the series $\frac{\partial^2 \mathcal{H}}{\partial y^2}$ is invertible in $F[[x, y]]$. Then there exists a unique F-derivation denoted by $\frac{\partial}{\partial \delta x}$ on $F[[x, y]]$ sending $x \mapsto 0$ and $\delta x \mapsto 1$. Moreover we have

$$\frac{\partial \mathcal{L}}{\partial \delta x} = y, \quad \frac{\partial \mathcal{L}}{\partial x} = -\frac{\partial \mathcal{H}}{\partial x},$$

and hence

$$\delta\left(\frac{\partial \mathcal{L}}{\partial \delta x}\right) = \frac{\partial \mathcal{L}}{\partial x}, \quad \delta x \cdot \frac{\partial \mathcal{L}}{\partial \delta x} - \mathcal{L} = \mathcal{H},$$

which can be interpreted as the "Euler-Lagrange equation" and the identification of the "Hamiltonian" with the "energy" respectively.

We want to introduce an arithmetic analogue of the above formalism; cf. [31]. To simplify our discussion let X be a smooth surface over R (or the p-adic completion

of such a surface). Recall that by an i-form on X we understand a global section of Ω^i_X (projective limit of usual Kähler differentials of X mod p^n). A symplectic form on X is an invertible 2-form on X. A contact form on X is a 1-form on X such that $d\nu$ is symplectic. By a δ-flow on X we will understand a section $X \to J^1(X)$ of the projection $J^1(X) \to X$. Let us further specialize the situation to the case when $X = J^1(Y)$ where Y is a curve (affine, to simplify). A 1-form ν on $X = J^1(Y)$ is called canonical if $\nu = g\beta$ with $g \in \mathcal{O}(X)$ and β a 1-form on Y. If ν is a canonical 1-form on $X = J^1(Y)$ and is closed, i.e. $d\nu = 0$, then ν is (the pull-back of) a 1-form on Y. Note that $J^2(Y)$ naturally embeds into $J^1(J^1(Y))$. A δ-flow on $X = J^1(Y)$ will be called *canonical* if the section $J^1(Y) = X \to J^1(X) = J^1(J^1(Y))$ factors through a section $J^1(Y) \to J^2(Y)$. This concept is, however, too restrictive for applications. We will need to relax the concept of canonical δ-flow as follows. To simplify the discussion we restrict to the case of order 2 differential equations. Let $f \in \mathcal{O}(J^2(Y))$ and let $Z = Z^2(f) \subset J^2(Y)$ be the closed formal subscheme defined by f. For $i \geq 1$ we define

$$\Omega'^i_Z = \frac{\Omega^i_{J^n(Y)}}{\langle f\Omega^i_{J^n(Y)}, df \wedge \Omega^{i-1}_{J^n(Y)} \rangle}.$$

So $\Omega'^1_Z = \Omega'_Z$. Also we have natural wedge products

$$\wedge : \Omega'^i_Z \times \Omega'^j_Z \to \Omega'^{i+j}_Z,$$

and exterior differentiation maps

$$d : \Omega'^i_Z \to \Omega'^{i+1}_Z.$$

We say that f defines a generalized canonical δ-flow on $J^1(Y)$ if the natural map

$$\pi^*\Omega_{J^1(Y)} \to \Omega'_Z$$

is injective and has a cokernel annihilated by a power of p. Note now that the natural maps $\phi^* : \Omega^i_{J^1(Y)} \to \Omega^i_{J^2(Y)}$ induce natural maps denoted by

$$\phi^*_Z : \Omega^i_{J^1(Y)} \to \Omega'^i_Z.$$

We say that the generalized canonical δ-flow is *Hamiltonian* with respect to a sympletic form η on $J^1(Y)$ if $\phi^*_Z\eta = \mu \cdot \eta$ in $\Omega'^2_{Z^2(f)}$ for some $\mu \in pR$. If in addition $\eta = d\nu$ for some canonical 1-form ν on $J^1(Y)$ we call $\epsilon := \frac{1}{p}(\phi^*_Z\nu - \mu\nu) \in \Omega'_{Z^2(f)}$ an Euler-Lagrange form. (This arithmetic Euler-Lagrange formalism is related to, but does not coincide with, the arithmetic Euler-Lagrange formalism in 1.2.9.) In the notation above $p\epsilon$ is closed in the sense that $d(p\epsilon) = 0$ in $\Omega'^2_{Z^2(f)}$. The above is the framework for the main results in [31] about the arithmetic analogue of Painlevé VI.

1.2.11. *"Category of differential equations".* A categorical framework for differential equations on manifolds can be introduced (cf. [1], for instance). In one variant of this the objects are locally isomorphic to projective systems of submanifolds of $J^n(M/T)$ compatible with the total derivative operator and morphisms are smooth maps between these, again compatible with the total derivative operator. This categorical framework has an arithmetic analogue as follows. Note first that ϕ acts naturally on $R_\delta(X, L)$ but δ does not. Nevertheless for any homogeneous $s \in R_\delta(X, L)$ of degree v the ring $R_\delta(X, L)_{\langle s \rangle}$ of all fractions f/s^w with f homogeneous of degree wv has a natural p-derivation δ on it. This inductive system

$X_\delta(L) = (R_\delta(X,L)_{\langle s\rangle}, \delta)_s$ of rings equipped with p-derivations δ is an object of a natural category underlying a geometry more general than algebraic geometry which we refer to as *δ-geometry* [16]. This geometry is an arithmetic analogue of the categorical setting in [1] and also an arithmetic analogue of the Ritt-Kolchin δ-algebraic geometry [52, 9]. If one restricts to étale maps of smooth schemes we have a functor $X \mapsto X_\delta = X_\delta(K^\nu)$ from "algebraic geometry" to our "δ-geometry" by taking $L = K^\nu$ to be a fixed power of the canonical bundle; the natural choice later in the theory turns out to be the anticanonical bundle $L = K^{-1}$. In δ-geometry X_δ should be viewed as an infinite dimensional object.

1.2.12. *Differential invariants.* Recall the concept of *differential invariant* which plays a key role in the "Galois theoretic" work of Lie and Cartan. Assume that a group G acts on M and T such that $M \to T$ is G-equivariant. (In this discussion assume $d := \dim T$ is arbitrary.) Then G acts on $J^n(M/T)$ and the ring $C^\infty(J^n(M/T))^G$ of G-invariant elements in the ring $C^\infty(J^n(M/T))$ is called the ring of *differential invariants*. There are two extreme cases of special interest: the case when G acts trivially on T and the case when G acts transitively on T. A special case of the first extreme case mentioned above is that in which $M = F \times T$, with G a Lie group acting trivially on T and transitively on F; this leads to the context of Cartan's moving frame method and of Cartan connections. For $\dim T = 1$, T is the "time" manifold, F is the "physical space", and sections in $\Gamma(M/T)$ correspond to particle trajectories. A special case of the second extreme case mentioned above is the situation encountered in the study of "geometric structures" and in the formulation of field theories, in which G is the group $\mathrm{Diff}(T)$ of diffeomorphisms of T, T is viewed as the "physical space" or "physical space-time", and M is a *natural bundle* over T, i.e. a quotient $M = \Gamma\backslash \mathrm{Rep}_n(T)$ of the bundle $\mathrm{Rep}_n(T) \to T$ of n-jets of frames $(\mathbb{R}^d, 0) \to T$ by a Lie subgroup Γ of the group $\mathrm{Aut}_n(\mathbb{R}^d, 0)$ of n-jets of diffeomorphisms of $(\mathbb{R}^d, 0)$; cf. [1], pp. 150-153 and 183. (E.g. the Riemannian metrics on T identify with the sections in $\Gamma(M_{1,O(d)}/T)$ where $O(d) < GL(d) = \mathrm{Aut}_1(\mathbb{R}^d, 0)$ is the orthogonal group.) In the case when the action of G on T is trivial the ring of differential invariants above turns out to have an interesting arithmetic analogue, namely the ring of *δ-invariants of a correspondence*; cf. the discussion below. The special case of Cartan connections has also an arithmetic analogue: the *arithmetic logarithmic derivative* attached to a *δ-flow*. The latter has a flavor different from that of δ-invariants of correspondences and will be discussed later. There are also interesting candidates for arithmetic analogues of the situation when $G = \mathrm{Diff}(T)$; cf. our discussion of Lie groupoids below.

We next explain the ring of δ-invariants of a correspondence. Pursuing an analogy with usual geometric invariant theory assume we are given (X, L), a *correspondence* on X (i.e. a morphism $\sigma = (\sigma_1, \sigma_2) : \tilde{X} \to X \times X$), and a *linearization* of L (i.e. an isomorphism $\beta : \sigma_1^* L \simeq \sigma_2^* L$). Then we may define the ring of *δ-invariants of σ* by

$$R_\delta(X,L)^\sigma = \{f \in R_\delta(X,L);\ \beta\sigma_1^* f = \sigma_2^* f\}.$$

(This ring, again, has no unity!) The homogeneous elements s of $R_\delta(X,L)^\sigma$ can be viewed as arithmetic analogues of total differential forms invariant under appropriate symmetries. The inductive system of rings

$$(R_\delta(X,L)^\sigma_{\langle s\rangle}, \delta)$$

equipped with p-derivations δ can be viewed as an incarnation of the quotient space "X_δ/σ_δ" in δ-geometry (and, under quite general hypotheses, is indeed the categorical quotient of X_δ by σ_δ); note that, in most interesting examples (like the ones in Theorem 2.6 below), the quotient X/σ does not exist in usual algebraic geometry (or rather the categorical quotient in algebraic geometry reduces to a point).

It is worth revisiting the sequence of ideas around differential invariants. Classical Galois theory deals with algebraic equations (satisfied by numbers). Lie and Cartan extended Galois' ideas, especially through the concept of differential invariant, to the study of differential equations (satisfied by functions); roughly speaking they replaced numbers by functions. In the theory presented here functions are replaced back by numbers. But we did *not* come back to where things started because we have added new structure, the operator $\delta = \delta_p$. In particular the δ-invariants mentioned above, although arithmetic in nature, and although attached to algebraic equations (defining X, $\tilde{X}$, σ), are nevertheless *not* "Galois theoretic" in any classical sense.

1.2.13. *Lie groupoids.* Let us go back to the (interrelated) problems of finding arithmetic analogues of $T \times T$ and of $\mathrm{Diff}(T)$. The arithmetic analogue of $S := T \times T$ is usually referred to as the hypothetical tensor product "$\mathbb{Z} \otimes_{\mathbb{F}_1} \mathbb{Z}$" over the "field with one element"; cf. [57] for some history of this. The arithmetic analogue of $\mathrm{Diff}(T)$ could be thought of as the Galois group "$\mathrm{Gal}(\mathbb{Q}/\mathbb{F}_1)$". According to a suggestion of Borger [6] one should take "$\mathbb{Z} \otimes_{\mathbb{F}_1} \mathbb{Z}$" to be, by definition, the big Witt ring of $\mathbb{Z}$. Since we are here in a local arithmetic situation it is convenient, for our purposes, to take, as an arithmetic analogue of $S = T \times T$, the schemes $\Sigma_m = Spec\ W_m(R)$, where W_m is the p-typical functor of Witt vectors of length $m+1$ (we use Borger's indexing) and R is a complete local p-ring. On the other hand an infinitesimal analogue of $\mathrm{Diff}(T)$ is the Lie groupoid of T defined as the projective system of groupoids $\mathcal{G}_n(T) := J^n(S/T)^*$ (where the upper $*$ means taking "invertible" elements and $S = T \times T \to T$ is the second projection.) So an arithmetic analogue of the system $J^n(S/T)^*$ (which at the same time would be an infinitesimal analogue of "$\mathrm{Gal}(\mathbb{Q}/\mathbb{F}_1)$") would be the system $J^n(\Sigma_m)$ equipped with the natural maps induced by the comonad map. This system is a rather non-trivial object [29]. It is worth noting that a good arithmetic analogue of $J^n(S/T)^*$ could also be the "usual" jet spaces (in the sense of [8]) of $W_m(R)/R$ (which in this case can be constructed directly from the module of Käher differentials $\Omega_{W_m(R)/R}$). By the way $\Omega_{W_m(R)/R}$ is also the starting point for the construction of the deRham-Wit complex [44]. However Ω involves usual derivations (rather than Fermat quotients) so taking Ω as a path to an arithmetic analogue of $J^n(S/T)^*$ seems, again, like "going arithmetic halfway". On the contrary taking the system $J^n(\Sigma_m)$ as the analogue of $J^n(S/T)^*$ seems to achieve, in some sense, the task of "going arithmetic all the way".

We end by remarking that if we denote π_1 and π_2 the source and target projections from $\mathcal{G}_n(T)$ into T then there are natural "actions" ρ of the groupoids $\mathcal{G}_n(T)$ on all natural bundles $M_{n,\Gamma} := \Gamma\backslash \mathrm{Rep}_n(T) \to T$ fitting into diagrams:

$$\begin{array}{rcl} M_{n,\Gamma} \times_{T,\pi_1} \mathcal{G}_n(T) & \stackrel{\rho}{\longrightarrow} & M_{n,\Gamma} \\ p_2 \downarrow & & \downarrow \\ \mathcal{G}_n(T) & \stackrel{\pi_2}{\longrightarrow} & T \end{array}$$

where p_2 is the second projection. The above induce "actions"

$$\begin{array}{rcl} J^n(M_{n,\Gamma}/T) \times_{T,\pi_1} \mathcal{G}_n(T) & \stackrel{\rho}{\longrightarrow} & J^n(M_{n,\Gamma}/T) \\ p_2 \downarrow & & \downarrow \\ \mathcal{G}_n(T) & \stackrel{\pi_2}{\longrightarrow} & T \end{array}$$

where p_2 is again the second projection. One can consider rings of differential invariants

$$C^\infty(J^n(M_{n,\Gamma}/T))^\rho := \{F \in C^\infty(J^n(M_{n,\Gamma}/T)); F \circ \rho = F \circ p_1\}$$

where $p_1 : J^n(M_{n,\Gamma}/T) \times_{T,\pi_1} \mathcal{G}_n(T) \to J^n(M_{n,\Gamma}/T)$ is the fist projection. There should be arithmetic analogues of the above "actions" and rings of differential invariants. One can argue that the analogue of $\mathrm{Rep}_n(T)$ is, again, the system $J^n(\Sigma_m)$. Then for $\Gamma = 1$ the analogue of $J^n(M_{n,\Gamma}/T)$ might be $J^n(J^n(\Sigma_m))$; the analogue, for $\Gamma = 1$, of the "action" ρ above could then be the map $J^n(J^n(\Sigma_{m',m''})) \to J^n(J^n(\Sigma_{m'+m''}))$ where $\Sigma_{m',m''} = Spec\ W_{m'}(W_{m''}(R))$. A challenge would then be to find arithmetic analogues of non-trivial Γs.

1.2.14. *Differential Galois theory of linear equations.* This subject is best explained in a complex (rather than real) situation. Classically (following Picard-Vessiot and Kolchin [51]) one starts with a differential field $\mathcal{F}$ of meromorphic functions on a domain D in the complex plane $\mathbb{C}$ and one fixes an $n \times n$ matrix $A \in \mathfrak{gl}_n(\mathcal{F})$ in the Lie algebra of the general linear group $GL_n(\mathcal{F})$. The problem then is to develop a "differential Galois theory" for equations of the form

$$\delta_z U = A \cdot U$$

where $U \in GL_n(\mathcal{G})$, $\mathcal{G}$ a field of meromorphic functions on a subdomain of D, and z a coordinate on D. The start of the theory is as follows. One fixes a solution U and introduces the differential Galois group $G_{U/\mathcal{F}}$ of $U/\mathcal{F}$ as the group of all $\mathcal{F}-$automorphisms of the field $\mathcal{F}(U)$ that commute with d/dz. One can ask for an arithmetic analogue of this theory. There is a well developed difference algebra analogue of linear differential equations [66]; but the arithmetic differential theory is still in its infancy [33, 34, 35]. What is being proposed in loc. cit. in the arithmetic theory is to fix a matrix $\alpha \in \mathfrak{gl}_n(R)$ and define δ-linear equations as equations of the form

$$\delta u = \alpha \cdot u^{(p)}$$

where $u = (u_{ij}) \in GL_n(R)$, $\delta u := (\delta u_{ij})$, and $u^{(p)} := (u_{ij}^p)$. Note that the above equation is equivalent to $\phi(u) = \epsilon \cdot u^{(p)}$ where $\epsilon = 1 + p\alpha$ which is *not* a difference equation for ϕ in the sense of [66]; indeed difference equations for ϕ have the form $\phi(u) = \epsilon \cdot u$. To define the δ-Galois group of such an equation start with a δ-subring $\mathcal{O} \subset R$ and let $u \in GL_n(R)$ be a solution of our equation. Let $\mathcal{O}[u] \subset R$ the ring generated by the entries of u; clearly $\mathcal{O}[u]$ is a δ-subring of R. We define the *δ-Galois group* $G_{u/\mathcal{O}}$ of $u/\mathcal{O}$ as the subgroup of all $c \in GL_n(\mathcal{O})$ for which there exists an $\mathcal{O}$-algebra automorphism σ of $\mathcal{O}[u]$ such that $\sigma \circ \delta = \delta \circ \sigma$ on $\mathcal{O}[u]$ and such that $\sigma(u) = uc$. The theory starts from here.

1.2.15. *Maurer-Cartan connections.* The Maurer-Cartan connection attached to a Lie group G is a canonical map $T(G) \to L(G)$ from the tangent bundle $T(G)$ to the Lie algebra $L(G)$; for $G = GL_n$ it is given by the form $dg \cdot g^{-1}$ and its algebraic incarnation is Kolchin's logarithmic derivative map [51] $GL_n(\mathcal{G}) \to \mathfrak{gl}_n(\mathcal{G})$,

$u \mapsto \delta_z u \cdot u^{-1}$. In our discussion of linear equations above the arithmetic analogue of the Kolchin logarithmic derivative map is the map $GL_n(R) \to \mathfrak{gl}_n(R)$,

$$u \mapsto \delta u \cdot (u^{(p)})^{-1}.$$

This map is naturally attached to the lift of Frobenius $\phi_{GL_n,0} : \widehat{GL_n} \to \widehat{GL_n}$ whose effect on the ring $\mathcal{O}(\widehat{GL_n}) = R[x, \det(x)^{-1}]\hat{}$ is $\phi_{GL_n,0}(x) = x^{(p)}$. The latter lift of Frobenius behaves well (in a precise sense to be explained later) with respect to the maximal torus $T \subset GL_n$ of diagonal matrices and with respect to the Weyl group $W \subset GL_n$ of permutation matrices but it behaves "badly" with respect to other subgroups like the classical groups SL_n, SO_n, Sp_n. (This phenomenon does not occur in the geometry of Lie groups where the Maurer-Cartan form behaves well with respect to *any* Lie subgroup of GL_n, in particular with respect to the classical groups.) In order to remedy the situation one is lead to generalize the above constructions by replacing $\phi_{GL_n,0}$ with other lifts of Frobenius $\phi_{GL_n} : \widehat{GL_n} \to \widehat{GL_n}$ that are adapted to each of these classical groups. Here is a description of the resulting framework.

First we define an arithmetic analogue of the Lie algebra $\mathfrak{gl}_n$ of GL_n as the set $\mathfrak{gl}_n$ of $n \times n$ matrices over R equipped with the non-commutative group law $+_\delta : \mathfrak{gl}_n \times \mathfrak{gl}_n \to \mathfrak{gl}_n$ given by

$$a +_\delta b := a + b + pab,$$

where the addition and multiplication in the right hand side are those of $\mathfrak{gl}_n$, viewed as an associative algebra. There is a natural "δ-adjoint" action $\star_\delta$ of GL_n on $\mathfrak{gl}_n$ given by

$$a \star_\delta b := \phi(a) \cdot b \cdot \phi(a)^{-1}.$$

Assume now one is given a ring endomorphism ϕ_{GL_n} of $\mathcal{O}(\widehat{GL_n})$ lifting Frobenius, i.e. a ring endomorphism whose reduction mod p is the p-power Frobenius on $\mathcal{O}(GL_n)\hat{}/(p) = k[x, \det(x)^{-1}]$; we still denote by $\phi_{GL_n} : \widehat{GL_n} \to \widehat{GL_n}$ the induced morphism of p-formal schemes and we refer to it as a lift of Frobenius on $\widehat{GL_n}$ or simply as a δ-*flow* on $\widehat{GL_n}$. Consider the matrices $\Phi(x) = (\phi_{GL_n}(x_{ij}))$ and $x^{(p)} = (x_{ij}^p)$ with entries in $\mathcal{O}(GL_n)\hat{}$; then $\Phi(x) = x^{(p)} + p\Delta(x)$ where $\Delta(x)$ is some matrix with entries in $\mathcal{O}(GL_n)\hat{}$. Furthermore given a lift of Frobenius ϕ_{GL_n} as above one defines, as usual, a p-derivation δ_{GL_n} on $\mathcal{O}(GL_n)\hat{}$ by setting $\delta_{GL_n}(f) = \frac{\phi_{GL_n}(f) - f^p}{p}$.

Assume furthermore that we are given a smooth closed subgroup scheme $G \subset GL_n$. We say that G is ϕ_{GL_n}-horizontal if ϕ_{GL_n} sends the ideal of G into itself; in this case we have a lift of Frobenius endomorphism ϕ_G on $\widehat{G}$, equivalently on $\mathcal{O}(G)\hat{}$.

Assume the ideal of G in $\mathcal{O}(GL_n)$ is generated by polynomials $f_i(x)$. Then recall that the Lie algebra $L(G)$ of G identifies, as an additive group, to the subgroup of the usual additive group $(\mathfrak{gl}_n, +)$ consisting of all matrices a satisfying

$$\text{“}\epsilon^{-1}\text{”} f_i(1 + \epsilon a) = 0,$$

where $\epsilon^2 = 0$. Let $f_i^{(\phi)}$ be the polynomials obtained from f_i by applying ϕ to the coefficients. Then we define the δ-Lie algebra $L_\delta(G)$ as the subgroup of $(\mathfrak{gl}_n, +_\delta)$ consisting of all the matrices $a \in \mathfrak{gl}_n$ satisfying

$$p^{-1} f_i^{(\phi)}(1 + pa) = 0.$$

The analogue of Kolchin's logarithmic derivative (or of the Maurer-Cartan connection) will then be the map, referred to as the *arithmetic logarithmic derivative*, $l\delta : GL_n \to \mathfrak{gl}_n$, defined by

$$l\delta a := \frac{1}{p}\left(\phi(a)\Phi(a)^{-1} - 1\right) = (\delta a - \Delta(a))(a^{(p)} + p\Delta(a))^{-1}.$$

For G a ϕ_{GL_n}-horizontal subgroup $l\delta$ above induces a map $l\delta : G \to L_\delta(G)$. Now any $\alpha \in L_\delta(G)$ defines an equation of the form $l\delta u = \alpha$, with unknown $u \in G$; such an equation will be referred to as a δ-linear equation (with respect to our δ-flow). Later in the paper we will explain our results about existence of δ-flows on GL_n compatible with the classical groups. These δ-flows will produce, as explained above, corresponding δ-linear equations.

1.2.16. *Symmetric spaces.* In the classical Cartan theory of symmetric spaces one starts with a (real) Lie group G equipped with a Lie group automorphism $x \mapsto x^\tau$ of order 1 or 2 (which we refer to as an involution). One defines the fixed group of the involution

$$G^+ := \{a \in G; a^\tau = a\} \tag{1.1}$$

and homogeneous spaces G/S where $(G^+)^\circ \subset S \subset G^+$ are Lie groups intermediate between the identity component $(G^+)^\circ$ and G^+. Then τ acts on the Lie algebra $L(G)$ and one denotes by $L(G)^+$ and $L(G)^-$ the $+$ and $-$ eigenspaces of this action. We have a decomposition $L(G) = L(G)^+ \oplus L(G)^-$ which can be referred to as a Cartan decomposition corresponding to τ. One can also consider the closed subset of G defined by

$$G^- := \{a \in G; a^\tau = a^{-1}\}. \tag{1.2}$$

This is not a subgroup of G. Set $a^{-\tau} = (a^\tau)^{-1}$. The map $\mathcal{H} : G \to G^-$, $\mathcal{H}(a) := a^{-\tau}a$ identifies G/G^+ with a subset of G^- and there is an obvious compatibility between the tangent map to $\mathcal{H}$ and the Cartan decomposition.

All of the above has an arithmetic analogue as follows. We start with a linear smooth group scheme G over R and an involution τ on G. We define G^+ and G^- as in 1.1 and 1.2 respectively. One also has an action of τ on the δ-Lie algebra $L_\delta(G)$. One considers the subgroup $L_\delta(G)^+ \subset L_\delta(G)$ of all $b \in L_\delta(G)$ such that $b^\tau = b$. One also considers the closed subscheme $L_\delta(G)^- \subset L_\delta(G)$ whose points b satisfy $b^\tau +_\delta b = 0$; $L_\delta(G)^-$ is not a subgroup. For $G = GL_n$ one easily proves that the map $+_\delta : L_\delta(G)^+ \times L_\delta(G)^- \to L_\delta(G)$ is a bijection on points; this can be viewed as an analogue of the Cartan decomposition. Later we will state results having the above as background.

The classical theory of symmetric spaces also considers bilinear (positive definite) forms B on $L(G)$ such that G^+ acts on $L(G)$ via the adjoint action by orthogonal transformations with respect to B; it would be interesting to find an arithmetic analogue of this condition.

1.3. **Main task of the theory.** At this point we may formulate the main technical tasks of the theory. Let, from now on, $R = \widehat{\mathbb{Z}_p^{ur}}$. First given a specific scheme X (or group scheme G) the task is to compute the rings $\mathcal{O}^n(X)$ (respectively the modules $\mathcal{X}^n(G)$). More generally given a specific pair (X, L) we want to compute the ring $R_\delta(X, L)$. Finally given (X, L), a correspondence σ on X, and a linearization of L, we want to compute the ring $R_\delta(X, L)^\sigma$. *The main applications of the theory (cf.*

the subsection below on motivations) arise as a result of the presence of interesting/unexpected elements and relations in the rings $\mathcal{O}^n(X)$, $R_\delta(X,L)$, $R_\delta(X,L)^\sigma$.

1.4. **Motivations of the theory.** There are a number of motivations for developing such a theory.

1.4.1. *Diophantine geometry.* Usual differential equations satisfied by functions can be used to prove diophantine results over function fields (e.g. the function field analogues of the Mordell conjecture [55] and of the Lang conjecture [8]). In the same vein one can hope to use "arithmetic differential equations" satisfied by numbers to prove diophantine results over number fields. This idea actually works in certain situations, as we will explain below. Cf. [12, 19]. The general strategy is as follows. Assume one wants to prove that a set S of points on an algebraic variety is finite. What one tries to do is find a system of arithmetic differential equations $F_i(\alpha, \delta_p\alpha, ..., \delta_p^n\alpha) = 0$ satisfied by all $\alpha \in S$; then one tries, using algebraic operations and the "differentiation" δ_p, to eliminate $\delta_p\alpha, ..., \delta_p^n\alpha$ from this system to obtain another system $G_j(\alpha) = 0$ satisfied by all $\alpha \in S$, where G_j do not involve the "derivatives" anymore. Finally one proves, using usual algebraic geometry that the latter system has only finitely many solutions.

1.4.2. *"Impossible" quotient spaces.* If X is an algebraic variety and $\sigma : \tilde{X} \to X \times X$ is a correspondence on X then the categorical quotient X/σ usually reduces to a point in the category of algebraic varieties. In some sense this is an illustration of the limitations of classical algebraic geometry and suggests the challenge of creating more general geometries in which X/σ becomes interesting. (The non-commutative geometry of A. Connes [38] serves in particular this purpose.) As explained above we proposed, in our work, to replace the algebraic equations of usual algebraic geometry by "arithmetic differential equations"; the resulting new geometry is called δ_p-geometry (or simply δ-geometry). Then it turns out that important class of quotients X/σ that reduce to a point in usual algebraic geometry become interesting in δ-geometry (due to the existence of interesting δ-invariants). A general principle seems to emerge according to which this class coincides with the class of "analytically uniformizable" correspondences. Cf. [16].

1.4.3. *"Impossible" liftings to characteristic zero.* A series of phenomena belonging to algebraic geometry in characteristic p, which do not lift to characteristic 0 in algebraic geometry, can be lifted nevertheless to characteristic 0 in δ-geometry. This seems to be a quite general principle with various incarnations throughout the theory (cf. [15, 16, 25]) and illustrates, again, how a limitation of classical algebraic geometry can be overcome by passing to δ-geometry.

1.5. **Comparison with other theories.** It is worth noting that the paradigm of our work is quite different from the following other paradigms:

1) Dwork's theory of p-adic differential equations [41] (which is a theory about δ_t acting on functions in $\mathbb{Q}_p[[t]]$ and not about δ_p acting on numbers; also Dwork's theory is a theory of linear differential equations whereas the theory here is about analogues of non-linear differential equations),

2) Vojta's jet spaces [67] (which, again, although designed for arithmetic purposes, are nevertheless constructed from Hasse-Schmidt derivations "$\frac{1}{n!}\delta_t^n$" acting on functions and not from operators acting on numbers),

3) Ihara's differentiation of integers [47] (which, although based on Fermat quotients, goes from characteristic zero to characteristic p and hence, unlike our δ_p, cannot be iterated),

4) the point of view of Kurokawa et. al. [53] (which uses an operator on numbers very different from δ_p namely $\frac{\partial \alpha}{\partial p} := np^{n-1}\beta$ for $\alpha = p^n\beta \in \mathbb{Z}$, $p \not| \beta$),

5) the theory of Drinfeld modules [39](which is entirely in characteristic p),

6) the difference geometry in the work of Cohn, Hrushovski-Chatzidakis [37], and others (in which the jet spaces are n-fold products of the original varieties as opposed to the jet spaces in our work which are, as we shall see, bundles over the original varieties with fibers affine spaces),

7) Raynaud's deformation to Witt vectors $W_2(k)$ over a field k of characteristic p [65] (which again leads to operators from characteristic zero to characteristic p which cannot be iterated; loosely speaking $W_2(k)$ in Raynaud's approach is replaced in our theory by $W_2(W(k))$).

8) the work of Soulé, Deitmar, Connes, Berkovich, and many others on the "geometry over the field $\mathbb{F}_1$ with one element". In their work passing from the geometry over $\mathbb{Z}$ to the geometry over $\mathbb{F}_1$ amounts to *removing* part of the structure defining commutative rings, e.g. removing addition and hence considering multiplicative monoids instead of rings. On the contrary our theory can be seen as a tentative approach to $\mathbb{F}_1$ (cf. the Introduction to [16]) that passes from $\mathbb{Z}$ to $\mathbb{F}_1$ by *adding* structure to the commutative rings, specifically adding the operator(s) δ_p. This point of view was independently proposed (in a much more systematic form) by Borger [6]. Borger's philosophy is global in the sense that it involves all the primes (instead of just one prime as in our work) and it also proposes to see "positivity" as the corresponding story at the "infinite" prime; making our theory fit into Borger's larger picture is an intriguing challenge.

9) the work of Joyal [49] and Borger [4, 5] on the Witt functor; the Witt functor is a right adjoint to the forgetful functor from "δ-rings" to rings as opposed to the arithmetic jet functor which is a left adjoint to the same forgetful functor. As it is usually the case the left and right stories turn out to be rather different.

10) the theory of the Greenberg transform, cf. Lang's thesis and [42] (which attaches to a scheme X/R varieties $G^n(X)$ over k; one can show [12] that $G^n(X) \simeq J^n(X) \otimes_R k$ so the arithmetic jet spaces are certain remarkable liftings to characteristic zero of the Greenberg transforms. The operators δ on $\mathcal{O}^n(X)$ do not survive after reduction mod p as operators on the Greenberg transforms.)

11) the work on the deRham-Witt complex, cf., e.g. [44] (which has as its starting point the study of Kähler differential of Witt vectors; on the contrary, what our research suggests, cf. [29], is to push arithmetization one step further by analyzing instead the *arithmetic* jet spaces of Witt vectors.)

12) the theory ϕ-modules (which is a theory about linear equations as opposed to the theory here which is non-linear).

2. Main results

We present in what follows a sample of our results. We always set $\overline{A} = A \otimes_{\mathbb{Z}} \mathbb{F}_p = A/pA$, $\overline{X} = X \otimes_{\mathbb{Z}} \mathbb{F}_p$ for any ring A and any scheme X respectively. Recall that we denote by $\widehat{A}$ the p-adic completion of A; for X Noetherian we denote by $\widehat{X}$ the p-adic completion of X. Also, in what follows, $R := \widehat{\mathbb{Z}_p^{ur}}$, $k := R/pR$. We begin with completely general facts:

2.1. **Affine fibration structure of p-jet spaces.**

Theorem 2.1. [11]

1) If X/R is a smooth scheme of relative dimension d then X has an affine covering X_i such that $J^n(X_i) \simeq \widehat{X_i} \times \widehat{\mathbb{A}^{nd}}$ in the category of p-adic formal schemes.

2) If G/R is a smooth group scheme of relative dimension d, with formal group law $\mathcal{F} \in R[[T_1, T_2]]^d$ (T_1, T_2 d-tuples), then the kernel of $J^n(G) \to \widehat{G}$ is isomorphic to $\widehat{\mathbb{A}^{nd}}$ with composition law obtained from the formal series

$$\delta\mathcal{F}, ..., \delta^n\mathcal{F} \in R[[T_1, T_2, ..., T_1^{(n)}, T_2^{(n)}]]^d$$

by setting $T_1 = T_2 = 0$.

Note that after setting $T_1 = T_2 = 0$ the series $\delta^n\mathcal{F}$ become restricted i.e. elements of $(R[T_1', T_2', ..., T_1^{(n)}, T_2^{(n)}]\hat{})^d$ so they define morphisms in the category of p-adic formal schemes. Assertion 1) in the theorem makes p-jet spaces resemble the usual jet spaces of the Lie-Cartan theory. Note however that, even if G is commutative, the kernel of $J^n(G) \to \widehat{G}$ is not, in general the additive group raised to some power. Here is the idea of the proof of 1) for $n = 1$. We may assume $X = Spec\ A$, $A = R[x]/(f)$, and there is an étale map $R[T] \subset A$ with T a d-tuple of indeterminates. Consider the unique ring homomorphism $R[T] \to W_1(A[T'])$ sending $T \mapsto (T, T')$ where W_1 is the functor of Witt vectors of length 2 and T' is a d-tuple of indeterminates. Using the fact that $R[T] \subset A$ is formally étale and the fact that the first projection $W_1(A[T']/(p^n)) \to A[T']/(p^n)$ has a nilpotent kernel, one constructs a compatible sequence of homomorphisms $A \to W_1(A[T']/(p^n))$, $T \mapsto (T, T')$. Hence one gets a homomorphism $A \to W_1(A[T']\hat{})$, $a \mapsto (a, \delta a)$. Then one defines a homomorphism $R[x, x']\hat{}/(f, \delta f) \to A[T']\hat{}$ by sending $x \mapsto a := \text{class}(x) \in A$, $x' \mapsto \delta a$. Conversely one defines a homomorphism $A[T']\hat{} \to R[x, x']\hat{}/(f, \delta f)$ by sending $T' \mapsto \delta T$. The two homomorphisms are inverse to each other which ends the proof of 1) for $n = 1$.

2.2. **δ-functions and δ-characters on curves.** The behavior of the rings $\mathcal{O}^n(X)$ for smooth projective curves X depends on the genus of X as follows:

Theorem 2.2. [11, 12, 32] *Let X be a smooth projective curve over R of genus g.*

1) If $g = 0$ then $\mathcal{O}^n(X) = R$ for all $n \geq 0$.

2) Let $g = 1$. If X is not a canonical lift then $\mathcal{O}^1(X) = R$ (hence $\mathcal{X}^1(X) = 0$) and $\mathcal{X}^2(X)$ is a free module of rank 1; in particular $\mathcal{O}^2(X) \neq R$. If, on the other hand, X is a canonical lift then $\mathcal{O}^1(X) = \mathcal{O}(\widehat{\mathbb{A}^1})$ and $\mathcal{X}^1(X)$ is free of rank one.

3) If $g \geq 2$ then $J^n(X)$ is affine for $n \geq 1$; in particular $\mathcal{O}^1(X)$ separates the points of $X(R)$.

The proof of 1) is a direct computation. The idea of proof of the statements about $\mathcal{X}^n$ in 2) is as follows. Let $N^n = Ker(J^n(X) \to \widehat{X})$. Then one first proves (using Theorem 2.1) that $Hom(N^n, \widehat{\mathbb{G}}_a)$ has rank at least n over R and one computes the ranks of $\mathcal{X}^n(X)$ by looking at the exact squence

$$Hom(J^2(X), \widehat{\mathbb{G}}_a) \to Hom(N^2, \widehat{\mathbb{G}}_a) \to H^1(X, \mathcal{O}).$$

Here $Hom = Hom_{gr}$. The proof of 3) is based on representing $\overline{J^1(X)}$ as $\mathbb{P}(\mathcal{E})\backslash D$ where $\mathcal{E}$ is a rank 2 vector bundle on $\overline{X}$, and D is an ample divisor.

If $g = 1$ and X is not a canonical lift then a basis ψ for $\mathcal{X}^2(X)$ can be viewed as an analogue of the "Manin map" of an elliptic fibration [55]. Also note that assertion 3) in Theorem 2.2 implies the effective version of the Manin-Mumford conjecture [12]. Indeed Manin and Mumford conjectured that if X is a complex curve of genus ≥ 2 embedded into its Jacobian A then $X \cap A_{tors}$ is a finite set. This was proved by Raynaud [65]. Mazur later asked [59] if $\sharp(X \cap A_{tors}) \leq C(g)$ where $C(g)$ is a constant that depends only on the genus g of X. Using 3) in Theorem 2.2 one can prove:

Theorem 2.3. [12] *For a smooth projective complex curve X in its Jacobian A we have $\sharp(X \cap A_{tors}) \leq C(g, p)$ where $C(g, p)$ is a constant that depends only on the genus g and (in case X is defined over $\overline{\mathbb{Q}}$) on the smallest prime p of good reduction of X.*

Roughly speaking the idea of proof is as follows. First one can replace the complex numbers by R and A_{tors} by its prime to p torsion subgroup $\Gamma < A(R)$. Then one embeds $X(R) \cap \Gamma$ (via the "jet map") into the the set of k-points of $\overline{J^1(X)} \cap p\overline{J^1(A)}$. But the latter is a finite set because $\overline{J^1(X)}$ is affine, $p\overline{J^1(A)}$ is projective, and both are closed in $\overline{J^1(A)}$. Moreover the cardinality of this finite set can be bounded using Bézout's theorem.

One can ask for global vector fields on a smooth projective curve X/R that are infinitesimal symmetries for given δ-functions on X. The only non-trivial care is that of genus 1 (elliptic curves); indeed for genus 0 there are no non-constant δ-functions (cf. Theorem 2.2) while for genus ≥ 2 there are no non-zero vector fields. Here is the result:

Theorem 2.4. [11, 16] *Let X be an elliptic curve over R with ordinary reduction.*

1) If X has Serre-Tate parameter $q(X) \not\equiv 1 \bmod p^2$ then there exists a non-zero global vector field on X which is a variational infinitesimal symmetry for all the modules $\mathcal{X}^n(X)$, $n \geq 1$.

2) If X is a canonical lift (equivalently has Serre-Tate parameter $q(X) = 1$) then there is no non-zero global vector field on X which is a variational infinitesimal symmetry of $\mathcal{X}^1(X)$.

Finally here is a computation of differentials of δ-characters.

Theorem 2.5. [13, 16] *Assume X is an elliptic curve over R which is not a canonical lift and comes from an elliptic curve $X_{\mathbb{Z}_p}$ over $\mathbb{Z}_p$. Let $a_p \in \mathbb{Z}$ be the trace of Frobenius of the reduction mod p of $X_{\mathbb{Z}_p}$ and let ω be a basis for the global 1-forms on $X_{\mathbb{Z}_p}$. Then there exists an R-basis ψ of $\mathcal{X}^2(X)$ such that*

$$p \cdot d\psi = (\phi^{*2} - a_p \phi^* + p)\omega.$$

In particular for the eigenvalue $\mu = 1$ we have

$$p \cdot d\left(\int \psi dp\right) = (1 - a_p + p) \cdot \int \omega dp.$$

A similar result holds in case X is a canonical lift.

2.3. **δ-invariants of correspondences.** Here is now a (rather roughly stated) result about δ-invariants of correspondences on curves; for precise statements we refer to [16].

Theorem 2.6. [16] *The ring $R_\delta(X, K^{-1})^\sigma$ is "δ-birationally equivalent" to the ring $R_\delta(\mathbb{P}^1, \mathcal{O}(1))$ if the correspondence σ on X "comes from" one of the following cases:*

1) (spherical case) The standard action of $SL_2(\mathbb{Z}_p)$ on $\mathbb{P}^1$.

2) (flat case) A dynamical system $\mathbb{P}^1 \to \mathbb{P}^1$ which is post-critically finite with (orbifold) Euler characteristic zero.

3) (hyperbolic case) The action of a Hecke correspondence on a modular (or Shimura) curve.

Here by saying that σ "comes from" a group action on X (respectively from an endomorphism of X) we mean that ("up to some specific finite subschemes" for which we refer to [16]) $\tilde{X}$ is the disjoint union of the graphs of finitely many automorphisms generating the action (respectively $\tilde{X}$ is the graph of the endomorphism). Also δ-birational equivalence means isomorphism (compatible with the actions of δ) between the p-adic completions of the rings of homogeneous fractions of degree zero with denominators not divisible by p. The proofs behind the spherical case involve direct computations. The proofs behind the flat case use the arithmetic Manin map, i.e. the space $\mathcal{X}^2(X)$ in Theorem 2.2, plus an induction in which canonical prolongations of vector fields play a crucial role. The proofs behind the hyperbolic case of Theorem 2.6 are based on a theory of *δ-modular forms* which we quickly survey next.

2.4. **δ-modular forms.** Cf. [15, 2, 16, 26, 17, 25]. Let $X_1(N)$ be the complete modular curve over R of level $N > 4$ and let $L_1(N) \to X_1(N)$ be the line bundle with the property that the sections of its various powers are the classical modular forms on $\Gamma_1(N)$ of various weights. Let X be $X_1(N)$ minus the cusps and the supersingular locus (zero locus of the Eisenstein form E_{p-1} of weight $p-1$). Let $L \to X$ be the restriction of the above line bundle and let V be L with the zero section removed. So $L^2 \simeq K$. The elements of $M^n = \mathcal{O}^n(V)$ are called δ-modular functions. Set $M^\infty = \cup M^n$. The elements of $\mathcal{O}^n(X)$ are called δ-modular forms of weight 0. For $w \in W$, $w \neq 0$, the elements of $H^0(X, L^w) \subset M^\infty$ are called δ-modular forms of weight w. We let $\sigma = (\sigma_1, \sigma_2) : \tilde{X} \to X \times X$ be the union of all the (prime to p) Hecke correspondences. Any δ-modular function $f \in M^n$ has a "δ-Fourier expansion" in $R((q))[q', ..., q^{(n)}]\hat{}$; setting $q' = q'' = ... = 0$ in this δ-Fourier expansion one gets a series in $R((q))\hat{}$ called the Fourier expansion of f. Finally let a_4 and a_6 be variables; then consideration of the elliptic curve $y^2 = x^3 + a_4 x + a_6$ yields an R-algebra map

$$R[a_4, a_6, \Delta^{-1}] \to M^0$$

where $\Delta = \Delta(a_4, a_6)$ is the discriminant polynomial. By universality we have induced homomorphisms

$$R[a_4, a_6, ..., a_4^{(n)}, a_6^{(n)}, \Delta^{-1}]\hat{} \to M^n$$

that are compatible with δ.

Example 2.7. [17, 19] For $f = \sum a_n q^n$ a classical newform over $\mathbb{Z}$ of weight 2, we get a δ-modular form of weight 0 and order 2

$$f^\sharp : J^2(X) \subset J^2(X_1(N)) \overset{J^2(\Phi)}{\to} J^2(E_f) \overset{\psi}{\to} \widehat{\mathbb{G}_a}$$

where $\Phi : X_1(N) \to E_f$ is the Eichler-Shimura map to the corresponding elliptic curve E_f (assumed for simplicity to be non-CM), and ψ the "unique" δ-character

of order 2. Then the δ-Fourier expansion of $f^\sharp$ is congruent mod p to

$$\sum_{(n,p)=1} \frac{a_n}{n} q^n - a_p \left(\sum a_m q^{mp} \right) \frac{q'}{q^p} + \left(\sum a_m q^{mp^2} \right) \left(\frac{q'}{q^p} \right)^p ;$$

hence the Fourier expansion of $f^\sharp$ is congruent mod p to $\sum_{(n,p)=1} \frac{a_n}{n} q^n$.

Example 2.8. [15] There exists a unique δ-modular form $f^1 \in H^0(X, L^{-\phi-1})$ with δ-Fourier expansion

$$\sum_{n \geq 1} (-1)^{n-1} \frac{p^{n-1}}{n} \left(\frac{q'}{q^p} \right)^n = \frac{q'}{q^p} + p\,(...)\,.$$

Hence the Fourier expansion of f^1 is 0. By the way the above δ-Fourier expansion has the same shape as a certain function playing a role in "explicit" local class field theory. Here is the rough idea for the construction of f^1. One considers the universal elliptic curve $E = \bigcup U_i \to Spec\ M^\infty$, one considers sections $s_i : \widehat{U}_i \to J^1(U_i)$ of the projection, one considers the differences

$$s_i - s_j : \widehat{U}_i \cap \widehat{U}_j \to N^1 \simeq \widehat{\mathbb{G}}_a,$$

and one considers the cohomology class $[s_i - s_j] \in H^1(\widehat{E}, \mathcal{O}) = H^1(E, \mathcal{O})$. Then $f^1 \in M^\infty$ is defined as the cup product of this class with the canonical generator of the 1-forms; in fact f^1 is the image of some element

$$f^1(a_4, a_6, a_4', a_6') \in R[a_4, a_6, a_4', a_6', \Delta^{-1}]\hat{}.$$

By the way it is a result of Hurlburt [45] that

$$f^1(a_4, a_6, a_4', a_6') \equiv E_{p-1} \frac{2a_4^p a_6' - 3a_6^p a_4'}{\Delta^p} + f_0(a_4, a_6) \mod p$$

where $f_0 \in R[a_4, a_6, \Delta^{-1}]$ and we recall that E_{p-1} is the Eisenstein form of weight $p-1$. (The polynomial f_0 is related to the Kronecker modular polynomial mod p^2.) This plus the δ-Fourier expansion of f^1 should be viewed as an arithmetic analogue of the fact (due to Ramanujan) that

$$\frac{2a_4 da_6 - 3a_6 da_4}{\Delta} \mapsto \frac{dq}{q}$$

via the map between the Kähler differentials induced by the Fourier expansion map $\mathbb{C}[a_4, a_6, \Delta^{-1}] \to \mathbb{C}((q))$.

Example 2.9. [2] There exists unique δ-modular forms $f^\partial \in H^0(X, L^{\phi-1})$ and $f_\partial \in H^0(X, L^{1-\phi})$ with δ-Fourier expansions 1 (and hence Fourier expansions 1). They satisfy $f^\partial \cdot f_\partial = 1$. The form f^∂ is constructed by applying the "top part" of the canonical prolongation of the "Serre operator" to the form f^1. More precisely f^∂ is a constant times the image of

$$(72\phi(a_6) \frac{\partial}{\partial a_4'} - 16\phi(a_4)^2 \frac{\partial}{\partial a_6'} - p \cdot \phi(P))(f^1(a_4, a_6, a_4', a_6'))$$

where $P \in R[a_4, a_6, \Delta^{-1}, E_{p-1}^{-1}]\hat{}$ is the Ramanujan form.

Theorem 2.10. [2, 15, 16] *The ring $R_\delta(X, K^{-1})^\sigma$ is "δ-generated" by f^1 and f^∂.*

Note that f^1 and f^∂ do not actually belong to $R_\delta(X, K^{-1})$ so the above theorem needs some further explanation which we skip here; essentially, what happens is that f^1 and f^∂ belong to a ring slightly bigger than $R_\delta(X, K^{-1})$ and they "δ-generate" that ring. We also note the following structure theorem for the kernel and image of the δ-Fourier expansion map, in which the forms f^1 and f^∂ play a key role:

Theorem 2.11. [25]

1) The kernel of the Fourier expansion map $M^\infty \to R((q))\hat{}$ is the p-adic closure of the smallest δ-stable ideal containing f^1 and $f^\partial - 1$.

2) The p-adic closure of the image of the Fourier expansion map $M^\infty \to R((q))\hat{}$ equals Katz' ring $\mathbb{W}$ of generalized p-adic modular forms.

The proof of the Theorem above is rather indirect and heavily Galois-theoretic. Statement 2) in Theorem 2.11 says that all Katz' divided congruences between classical modular forms can be obtained by taking combinations of "higher p-derivatives" of classical modular forms. Statement 1) above is a lift to characteristic zero of the Serre and Swinnerton-Dyer theorem about the kernel of the classical Fourier expansion map for classical modular forms mod p. Theorem 2.10 can also be viewed as a lift to characteristic zero of results of Ihara [46] about the Hasse invariant in characteristic p. These mod p results do not lift to characteristic zero in usual algebraic geometry but do lift, as we see, to characteristic zero in δ-geometry.

We mention the following remarkable infinitesimal symmetry property; recall the classical Serre operator $\partial : \mathcal{O}(V) \to \mathcal{O}(V)$. Also consider the Euler derivation operator $\mathcal{D} : \mathcal{O}(V) \to \mathcal{O}(V)$ given by multiplication by the degree on each graded component of $\mathcal{O}(V)$. Finally let P be the Ramanujan form (in the degree 2 component of $\mathcal{O}(V)$) and let $\theta : \mathcal{O}(V) \to \mathcal{O}(V)$ be the derivation $\theta = \partial + P\mathcal{D}$.

Theorem 2.12. [16] *The operator θ is an infinitesimal symmetry of the R-module generated by f^1, f^∂, and f_∂ in $M^1 = \mathcal{O}^1(V)$. Also θ is a variational infinitesimal symmetry of the R-module generated by f^∂ and f_∂ in $M^1 = \mathcal{O}^1(V)$.*

Here is a calculation of differentials of the forms $f^1, f^\partial, f_\partial$.

Theorem 2.13. [16] *Let ω, α be the basis of $\Omega_{\mathcal{O}(V)/R}$ dual to $\theta, \mathcal{D}$. Then*

$$\begin{aligned} d(f^\partial) &= f^\partial \cdot (\phi^*\alpha - \alpha) \\ d(f_\partial) &= -f_\partial \cdot (\phi^*\alpha - \alpha) \\ d(f^1) &= -f^1 \cdot (\phi^*\alpha + \alpha) - f_\partial \cdot \omega + f^\partial \cdot p^{-1}\phi^*\omega. \end{aligned}$$

In particular, for the eigenvalue $\mu = 1$ we have

$$\int \{\frac{d(f^\partial)}{f^\partial}\} dp = \int \{\frac{d(f_\partial)}{f_\partial}\} dp = 0.$$

By the way, the forms $f^\sharp$ and f^1 introduced above can be used to prove some interesting purely diophantine results. For instance we have the following:

Theorem 2.14. [19] *Assume that $\Phi : X = X_1(N) \to A$ is a modular parametrization of an elliptic curve. Let p be a sufficiently large "good" prime and let $Q \in X(R)$ be an ordinary point. Let S be the set of all rational primes that are inert in the*

imaginary quadratic field attached to Q. Let C be the S-isogeny class of Q in $X(R)$ (consisting of points corresponding to isogenies of degrees only divisible by primes in S). Then there exists a constant c such that for any subgroup $\Gamma \leq A(R)$ with $r := rank(\Gamma) < \infty$ the set $\Phi(C) \cap \Gamma$ is finite of cardinality at most cp^r.

Other results of the same type (e.g. involving Heegner points) were proved in [19]. In particular an analogue of the above Theorem is true with C replaced by the locus CL of canonical lifts. To have a rough idea about the arguments involved assume we want to prove that $\Phi(CL) \cap \Gamma$ is finite (and to bound the cardinality of this set) in case Γ is the torsion group of $A(R)$. One considers the order 2 δ-modular form $f^\sharp : X_1(N)(R) \to R$ and one constructs, using f^1, a δ-function of order 1, $f^\flat : X(R) \to R$, on an open set $X \subset X_1(N)$ which vanishes exactly on $CL \cap X(R)$. Then any point P in the intersection $X(R) \cap \Phi(CL) \cap \Gamma$ satisfies the system of "differential equations of order ≤ 2 in 1 unknown"

$$\begin{cases} f^\sharp(P) = 0 \\ f^\flat(P) = 0 \end{cases}$$

One can show that this system is "sufficiently non-degenerate" to allow the elimination of the "derivatives" of the unknown; one is left with a differential equation $f^0(P) = 0$ "of order 0" which has, then, only finitely many solutions (by Krasner's theorem). By that theorem one can also bound the number of solutions.

We end the discussion here by noting that the main players in the theory above enjoy a certain remarkable property which we call δ-overconvergence. Morally this is a an overconvergence property (in the classical sense of Dwork, Monsky, Washnitzer) "in the direction of the variables $x', x'', ..., x^{(n)}$" (but not necessarily in the direction of x). We prove:

Theorem 2.15. [27] *The δ-functions $f^\sharp, f^1, f^\partial$ are δ-overconvergent.*

2.5. **δ-Hecke operators.** Next we discuss the Hecke action on δ-modular forms. For $(n, p) = 1$ the Hecke operators $T_m(n)$ act naturally on δ-series (i.e. series in $R((q))[q', ..., q^{(r)}]\hat{}$) by the usual formula that inserts roots of unity of order prime to p which are all in R. However no naive definition of $T_m(p)$ seems to work. Instead we consider the situation mod p and make the following definition. Let x be a p-tuple $x_1, ..., x_p$ of indeterminates and let s be the p-tuple $s_1, ..., s_p$ of fundamental symmetric polynomials in x. An element $f \in k[[q]][q', ..., q^{(r)}]$ is called δ-p-symmetric mod p if the sum

$$f(x_1, ..., x_1^{(r)}) + ... + f(x_p, ..., x_p^{(r)}) \in k[[x]][x', ..., x^{(r)}]$$

is the image of an element

$$f_{(p)} = f_{(p)}(s_1, ..., s_p, ..., s_1^{(r)}, ..., s_p^{(r)}) \in k[[s]][s', ..., s^{(r)}].$$

For f that is δ-p-symmetric mod p define

$$\text{"}pT_m(p)\text{"} f = f_{(p)}(0, ..., 0, q, ..., 0, ..., 0, q^{(r)}) + p^m f(q^p, ..., \delta^r(q^p)) \in k[[q]][q', ..., q^{(r)}].$$

Eigenvectors of "$pT_m(p)$" will be automatically understood to be δ-p-symmetric. Also let us say that a series in $k[[q]][q', ..., q^{(r)}]$ is primitive if the series in $k[[q]]$ obtained by setting $q' = ... = q^{(r)} = 0$ is killed by the classical U-operator. Then one can give a complete description (in terms of classical Hecke eigenforms mod p) of δ-"eigenseries" mod p of order 1 which are δ-Fourier expansions of δ-modular forms of arbitrary order and weight:

Theorem 2.16. [26] *There is a* $1-1$ *correspondence between:*

1) Series in $k[[q]]$ *which are eigenvectors of all* $T_{m+2}(n), T_{m+2}(p)$, $(n,p)=1$, *and which are Fourier expansions of classical modular forms over* k *of weight* $\equiv m+2$ *mod* $p-1$.

2) Primitive series in $k[[q]][q']$ *which are eigenvectors of all* $nT_m(n)$, "$pT_m(p)$", $(n,p)=1$, *and which are* δ*-Fourier expansions of* δ*-modular forms of some order* ≥ 0 *with weight* w, $deg(w)=m$.

Note that the δ-Fourier expansion of the form $f^\sharp$ discussed in Example 2.7 is an example of series in 2) of Theorem 2.16. (Note that $f^\sharp$ has order 2 although its δ-Fourier expansion reduced mod p has order 1!) More generally the series in 1) and 2) of Theorem 2.16 are related in an explicit way, similar to the way f and $f^\sharp$ of Example 2.7 are related. The proof of Theorem 2.16 involves a careful study of the action of δ-Hecke operators on δ-series plus the use of the canonical prolongations of the Serre operator acting on δ-modular forms.

2.6. **δ-functions on finite flat schemes.** The p-jet spaces of finite flat schemes over R seem to play a key role in many aspects of the theory. These p-jet spaces are neither finite nor flat in general and overall they seem quite pathological. There are two remarkable classes of examples, however, where some order seems to be restored in the limit; these classes are finite flat p-group schemes that fit into p-divisible groups and finite length p-typical Witt rings. Recall that for any ring A we write $\overline{A}=A/pA$. Then for connected p-divisible groups we have:

Theorem 2.17. [28] *Let* $\mathcal{F}$ *be a formal group law over* R *in one variable* x, *assume* $\mathcal{F}$ *has finite height, and let* $\mathcal{F}[p^\nu]$ *be the kernel of the multiplication by* p^ν *viewed as a finite flat group scheme over* R. *Then*

$$\lim_{\overrightarrow{n}} \overline{\mathcal{O}^n(\mathcal{F}[p^\nu])} \simeq \frac{k[x,x',x'',...]}{(x^{p^\nu},(x')^{p^\nu},(x'')^{p^\nu},...)}$$

sending $x,\delta x,\delta^2 x,...$ *into the classes of* $x,x',x'',....$

A similar result is obtained in [28] for the divisible group $E[p^\nu]$ of an ordinary elliptic curve; some of the components of $J^n(E[p^\nu])$ will be empty and exactly which ones are so is dictated by the valuation of $q-1$ where q is the Serre-Tate parameter. The components that are non-empty (in particular the identity component) behave in the same way as the formal groups examined in Theorem 2.17 above.

In the same spirit one can compute p-jet spaces of Witt rings. Let us consider the ring $W_m(R)$ of p-typical Witt vectors of length $m+1$, $m\geq 1$, and denote by $\Sigma_m = Spec\, W_m(R)$ its spectrum. Set $v_i=(0,...,0,1,0,...,0)\in W_m(R)$, (1 preceded by i zeroes, $i=1,...,m$), set $\pi=1-\delta v_1\in \mathcal{O}^1(\Sigma_m)$, and let $\Omega_m=\{1,...,m\}$. The following is a description of the identity component of the limit of p-jet spaces mod p:

Theorem 2.18. [29] *For* $n\geq 2$ *the image of* π^p *in* $\overline{\mathcal{O}^n(\Sigma_m)}$ *is idempotent and we have an isomorphism*

$$\lim_{\overrightarrow{n}} \overline{\mathcal{O}^n(\Sigma_m)}_\pi \simeq \frac{k[x_i^{(r)}; i\in\Omega_m; r\geq 0]}{(x_ix_j,(x_i^{(r)})^p; i,j\in\Omega_m, r\geq 1)}$$

sending each $\overline{\delta^r v_i}$ *into the class of the variable* $x_i^{(r)}$.

A similar description is obtained in [29] for the p-jet maps induced by the Witt comonad maps. We recall that the data consisting of $\mathcal{O}^n(\Sigma_m)$ and the maps induced by the comonad maps should be viewed as an arithmetic analogue of the Lie groupoid of the line.

2.7. **δ-Galois groups of δ-linear equations.** Recall that for any solution $u \in GL_n(R)$ of a δ-linear equation

$$\delta u = \alpha \cdot u^{(p)}$$

(where $\alpha \in \mathfrak{g}l_n(R)$) and for any δ-subring $\mathcal{O} \subset R$ we defined the δ-Galois group $G_{u/\mathcal{O}} \subset GL_n(\mathcal{O})$. We want to explain a result proved in [34]. Consider the maximal torus $T \subset GL_n(R)$ of diagonal matrices, the Weyl group $W \subset GL_n(R)$ of permutation matrices, the normalizer $N = WT = TW$ of T in $GL_n(R)$, and the subgroup N^δ of N consisting of all elements of N whose entries are in the monoid of constants R^δ. We also use below the notation K^a for the algebraic closure of the fraction field K of R; the Zariski closed sets Z of $GL_n(K^a)$ are then viewed as varieties over K^a. The next result illustrates some "generic" features of our δ-Galois groups; assertion 1) of the next theorem shows that the δ-Galois group is generically "not too large". Assertion 2) show that the δ-Galois group are generically "as large as possible". As we shall see presently, the meaning of the word *generic* is different in each of the 2 situations: in situation 1) *generic* means *outside a Zariski closed set*; in situation 2) *generic* means *outside a set of the first category* (in the sense of Baire category).

Theorem 2.19.

1) There exists a Zariski closed subset $\Omega \subset GL_n(K^a)$ not containing 1 such that for any $u \in GL_n(R)\backslash\Omega$ the following holds. Let $\alpha = \delta u \cdot (u^{(p)})^{-1}$ and let $\mathcal{O}$ be a δ-subring of R containing α. Then $G_{u/\mathcal{O}}$ contains a normal subgroup of finite index which is diagonalizable over K^a.

2) There exists a subset Ω of the first category in the metric space

$$X = \{u \in GL_n(R); u \equiv 1 \mod p\}$$

such that for any $u \in X\backslash\Omega$ the following holds. Let $\alpha = \delta u \cdot (u^{(p)})^{-1}$. Then there exists a δ-subring $\mathcal{O}$ of R containing R^δ such that $\alpha \in \mathfrak{g}l_n(\mathcal{O})$ and such that $G_{u/\mathcal{O}} = N^\delta$.

The groups W and N^δ should be morally viewed as "incarnations" of the groups "$GL_n(\mathbb{F}_1)$" and "$GL_n(\mathbb{F}_1^a)$" where "$\mathbb{F}_1$" and "$\mathbb{F}_1^a$" are the "field with element" and "its algebraic closure" respectively [6]. This suggests that the δ-Galois theory we are proposing here should be viewed as a Galois theory over "$\mathbb{F}_1$".

2.8. **δ-flows attached to outer involutions of GL_n.** The main results in [34] concern the existence of certain δ-flows on $\widehat{GL_n}$ that are attached to the outer involutions defining the (forms of the) classical groups GL_n, SL_n, SO_n, Sp_n. These δ-flows can be viewed as analogues of the Chern connections attached to hermitian vector bundles on complex manifolds.

Let $G = GL_n$ and let H be a smooth closed subgroup scheme of G. We say that a δ-flow ϕ_G is left (respectively right) compatible with H if H is ϕ_G-horizontal and

the left (respectively right) diagram below is commutative:

$$\begin{array}{ccc} \widehat{H}\times\widehat{G} & \to & \widehat{G} \\ {\scriptstyle \phi_H\times\phi_G}\downarrow & & \downarrow{\scriptstyle \phi_G} \\ \widehat{H}\times\widehat{G} & \to & \widehat{G} \end{array} \qquad \begin{array}{ccc} \widehat{G}\times\widehat{H} & \to & \widehat{G} \\ {\scriptstyle \phi_G\times\phi_H}\downarrow & & \downarrow{\scriptstyle \phi_G} \\ \widehat{G}\times\widehat{H} & \to & \widehat{G} \end{array}$$

where $\phi_H : \widehat{H} \to \widehat{H}$ is induced by ϕ_G and the horizontal maps are given by multiplication.

Next recall that by an involution on G we understand an automorphism $\tau : G \to G$ over R, $x \mapsto x^\tau$, of order 1 or 2. For each such τ one may consider the subgroup $G^+ = \{a \in G; a^\tau = a\}$. The identity component $(G^+)^\circ$ is referred to as the subgroup defined by τ. Also set $\mathcal{H} : G \to G$, $\mathcal{H}(x) = x^{-\tau}x$ and $\mathcal{B} : G \times G \to G$, $\mathcal{B}(x, y) = x^{-\tau}y$. More generally, for any $g \in G$, we may consider the maps $\mathcal{H}_g : G \to G$, $\mathcal{H}_g(x) = gx^{-\tau}x$, and $\mathcal{B}_g : G \times G \to G$, $\mathcal{B}_g(x, y) = gx^{-\tau}y$.

Let us fix now a lift of Frobenius $\phi_{G,0}$ on $\widehat{G}$. A lift of Frobenius ϕ_G on $\widehat{G}$ is said to be $\mathcal{H}_g$-horizontal (respectively $\mathcal{B}_g$-symmetric) with respect to $\phi_{G,0}$ if the left (respectively right) diagram below is commutative:

$$\begin{array}{ccc} \widehat{G} & \stackrel{\phi_G}{\longrightarrow} & \widehat{G} \\ {\scriptstyle \mathcal{H}_g}\downarrow & & \downarrow{\scriptstyle \mathcal{H}_g} \\ \widehat{G} & \stackrel{\phi_{G,0}}{\longrightarrow} & \widehat{G} \end{array} \qquad \begin{array}{ccc} \widehat{G} & \stackrel{\phi_{G,0}\times\phi_G}{\longrightarrow} & \widehat{G}\times\widehat{G} \\ {\scriptstyle \phi_G\times\phi_{G,0}}\downarrow & & \downarrow{\scriptstyle \mathcal{B}_g} \\ \widehat{G}\times\widehat{G} & \stackrel{\mathcal{B}_g}{\longrightarrow} & \widehat{G} \end{array} \tag{2.1}$$

If this is the case for $g = 1$ and $\phi_{G,0}(1) = 1$ then the group $S := (G^+)^\circ$ defined by τ is ϕ_G-horizontal; in particular there is an induced lift of Frobenius ϕ_S on $\widehat{S}$. Also note that if we set $\phi_{G,0}(x) = x^{(p)}$, viewing $\mathcal{H}$ as a matrix $\mathcal{H}(x)$ with entries in $R[x, \det(x)^{-1}]\hat{}$, we have that $\delta_G\mathcal{H} = 0$, which can be interpreted as saying that $\mathcal{H}$ is a *prime integral* for our δ-flow ϕ_G.

The basic split classical groups GL_n, SO_n, Sp_n are defined by involutions on $G = GL_n$ as follows. We start with GL_n itself which is defined by $x^\tau = x$. We call τ the canonical involution defining GL_n. We also recall that if $T \subset G$ is the maximal torus of diagonal matrices, N is its normalizer in G, and $W \subset G$ is the group of permutation matrices then $N = TW = WT$ and W is isomorphic to the Weyl group N/T. Throughout our discussion we let $\phi_{G,0}(x)$ be the lift of Frobenius on $\widehat{GL_n}$ defined by $\phi_{G,0}(x) := x^{(p)}$; one can prove that this $\phi_{G,0}(x)$ is the unique lift of Frobenius on $\widehat{G}$ that is left and right compatible with N and extends to a lift of Frobenius on $\widehat{\mathfrak{gl}_n}$ (where we view $\widehat{GL_n}$ as an open set of $\widehat{\mathfrak{gl}_n}$). On the other hand the groups $Sp_{2r}, SO_{2r}, SO_{2r+1}$ are defined by the involutions on $G = GL_n$ given by $x^\tau = q^{-1}(x^t)^{-1}q$ where q is equal to

$$\begin{pmatrix} 0 & 1_r \\ -1_r & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1_r \\ 1_r & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1_r \\ 0 & 1_r & 0 \end{pmatrix},$$

$n = 2r, 2r, 2r+1$ respectively, x^t is the transpose, and 1_r is the $r \times r$ identity matrix. We call this τ the canonical involution defining $Sp_{2r}, SO_{2r}, SO_{2r+1}$ respectively. All these groups are smooth over R. If S is any of these groups and we set $T_S = T \cap S$ and $N_S = N \cap S$ then these groups are smooth, T_S is a maximal torus in S and N_S is the normalizer of T_S in S. Call a root of one of these groups *abnormal* if it is a shortest root of a group SO_n with n odd.

Here is our result for arbitrary outer involutions:

Theorem 2.20. *Let $q \in GL_n$ be any matrix with $q^t = \pm q$ and let τ be the involution on GL_n defined by $x^\tau = q^{-1}(x^t)^{-1}q$. Let $\mathcal{H}_q(x) = qx^{-\tau}x = x^t qx$ and $\mathcal{B}_q(x,y) = qx^{-\tau}y = x^t qy$. Then there is a unique lift of Frobenius ϕ_{GL_n} on $\widehat{GL_n}$ that is $\mathcal{H}_q$-horizontal and $\mathcal{B}_q$-symmetric with respect to $\phi_{GL_n,0}$.*

The above theorem can be viewed as an analogue of results on the existence and uniqueness result for Chern connections on hermitian vector bundles on complex manifolds. In our context vector bundles are replaced by principal bundles. The role of the hermitian metric is played by the matrix q (or, rather, by the involution τ). The condition that the left diagram in 2.1 is commutative is the analogue of the condition that the Chern connection is compatible with the hermitian metric. The condition that the right diagram in 2.1 is commutative is an analogue of the condition that the Chern connection is compatible with the complex structure. These analogies are not direct and not obvious; for a detailed explanation of these analogies see [34]. On the other hand let ϕ_{GL_n} be the lift of Frobenius in Theorem 2.20 and consider the matrix $\phi_{GL_n}(x) = \Phi(x)$ with entries in $R[x\det(x)^{-1}]\hat{}$. Then our proof of Theorem 2.20 provides the following formula for the value of $\Phi(x)$ at the identity matrix 1:

$$\Phi(1) = (1 + p(q^{(p)})^{-1}\delta q))^{-1/2} := 1 + \sum_{i=1}^{\infty} \left(\begin{array}{c} -1/2 \\ i \end{array} \right) p^i ((q^{(p)})^{-1}\delta q)^i, \tag{2.2}$$

where $\left(\begin{array}{c} -1/2 \\ i \end{array} \right)$ are the binomial coefficients. For $n = 1$ and $q \in \mathbb{Z}$ this simplifies to the following formula (cf. [15], Introduction):

$$\Phi(1) = q^{(p-1)/2} \cdot \left(\frac{q}{p} \right), \tag{2.3}$$

where $\left(\frac{q}{p} \right)$ denotes the Legendre symbol. (Indeed $q^{(p-1)/2} \cdot \Phi(1)$ has square 1 and is $\equiv q^{(p-1)/2} \bmod p$.) This makes 2.2, "up to a polynomial function of the entries of in q", a matrix analogue of the Legendre symbol.

For the involutions defining the split classical groups we have the following result:

Theorem 2.21. *Let S be any of the groups GL_n, SO_n, Sp_n and let τ be the canonical involution on $G = GL_n$ defining S. Then the following hold.*

1) (Compatibility with involutions) There exists a unique lift of Frobenius ϕ_G on $\widehat{G}$ that is $\mathcal{H}$-horizontal and $\mathcal{B}$-symmetric with respect to $\phi_{G,0}$. In particular if $l\delta, l\delta_0 : GL_n \to \mathfrak{gl}_n$ are the arithmetic logarithmic derivative associated to $\phi_G, \phi_{G,0}$ then for all $a \in S$ we have that the Cartan decomposition

$$l\delta_0(a) = (l\delta_0(a))^+ +_\delta (l\delta_0(a))^-$$

of $l\delta_0(a)$ satisfies $(l\delta_0(a))^+ = l\delta(a)$.

2) (Compatibility with the normalizer of maximal torus.) ϕ_G is right compatible with N and left and right compatible with N_S. In particular for all $a \in N_S$ and $b \in GL_n$ (alternatively for all $a \in GL_n$ and $b \in N$) we have

$$l\delta(ab) = a \star_\delta l\delta(b) +_\delta l\delta(a).$$

3) (Compatibility with root groups.) If χ is a root of S which is not abnormal then the corresponding root group $U_\chi \simeq \mathbb{G}_a$ is ϕ_{GL_n}-horizontal.

Note that a similar result can be proved for SL_n; the involution τ lives, in this case, on a cover of GL_n rather than on GL_n itself. Note also that the exception in assertion 3 of the Theorem (occurring in case χ is a shortest root of SO_n with n odd) is a curious phenomenon which deserves further understanding.

2.9. **Arithmetic Painlevé VI.** The classical Painlevé VI equation has an elegant geometric description due to Manin [56]. In [31] an arithmetic analogue of this equation has been introduced and studied. We present below the main result in [31]. Recall our framework in 1.2.10 above.

Theorem 2.22. [31] *Let E be an elliptic curve over R which does not have a lift of Frobenius and let $\psi \in \mathcal{O}(J^2(E))$ be δ-character of order 2 attached to an invertible 1-form ω on E. Consider the symplectic form $\eta = \omega \wedge \frac{\phi^*\omega}{p}$ on $J^1(E)$. Let $Y = E\backslash E[2]$ and let $r \in \mathcal{O}(Y)$. Then the following hold:*

1) $f = \psi - \phi(r)$ defines a generalized canonical δ-flow on $J^1(Y)$ which is Hamiltonian with respect to η.

2) There exists a canonical 1-form ν on X such that $d\nu = \eta$; in particular η is exact and if ϵ is the associated Euler-Lagrange form then $p\epsilon$ is closed.

Note that f in the Theorem does not define a δ-flow on $J^1(E)$ (equivalently, $J^1(E)$ has no lift of Frobenius, equivalently the projection $J^1(J^1(E)) \to J^1(E)$ does not have a section):

Theorem 2.23. [32]. *Let E be an elliptic curve over R which does not have a lift of Frobenius. Then $J^1(E)$ does not have a lift of Frobenius.*

3. Problems

Problem 3.1. *Study the arithmetic jet spaces $J^n(X)$ of curves X (and more general varieties) with bad reduction.*

This could be applied, in particular, to tackle Mazur's question [59] about bounding the torsion points on curves unifromly in terms of the genus; in other words replacing $C(g,p)$ by $C(g)$ in Theorem 2.3. Our proof in [12] is based on the study of the arithmetic jet space of $J^1(X)$ at a prime p of good reduction. A study of the arithmetic jet space of curves at primes of bad reduction might lead to dropping the dependence of $C(g,p)$ on p. Evidence that arithmetic jet spaces can be handled in the case of bad reduction comes in particular from the recent paper [27].

Problem 3.2. *Study the δ-modular forms that vanish on arithmetically interesting Zariski dense subsets of Shimura varieties (such as CM loci or individual non-CM isogeny classes). Compute δ-invariants of higher dimensional correspondences.*

This could be applied to extend results in [19], e.g. Theorem 2.14 above. A deeper study of differential modular forms may allow one, for instance, to replace S-isogeny class with the full isogeny class. The arguments might then be extended to higher dimensional contexts and to the global field rather than the local field situation. That such a deeper study is possible is shown by papers like [25], for instance. For the higher dimensional case the theory in [3] might have to be further developed to match the one dimensional theory in [15, 16]. In a related direction one might attempt to use the methods in [19] to tackle Pink's conjectures in [64]. In [19] it was shown that behind finiteness theorems in diophantine geometry one can have reciprocity maps that are somehow inherited from δ-geometry (and that provide

effective bounds); a similar picture might hold for (cases of) Pink's conjecture. The first case to look at for such reciprocity maps would be in the case of the intersection between a multisection X of an abelian (or semiabelian) scheme $G \to S$ over a curve S with the set of torsion points lying in special (CM or otherwise) fibers; more general situations, in which torsion points are replaced by division points of a group generated by finitely many sections, can be considered. Results of André, Ribet, and Bertrand are pertinent to this question.

Problem 3.3. *Compare the δ-geometric approach to quotient spaces with the approach via non-commutative geometry.*

The quotients X/σ for the correspondences appearing in Theorem 2.6 do not exist, of course, in usual algebraic geometry. As Theorem 2.6 shows these quotients exist, however, and are interesting in δ-geometry. Remarkably such quotients also exist and are interesting in non-commutative geometry [60]. More precisely the 3 cases (spherical, flat, hyperbolic) of Theorem 2.6 are closely related to the following 3 classes of examples studied in non-commutative geometry:

1) (spherical) $\frac{\mathbb{P}^1(\mathbb{R})}{SL_2(\mathbb{Z})}$, non-commutative boundary of the classical modular curve;

2) (flat) $\frac{S^1}{\langle e^{2\pi i\tau}\rangle}$ ($\theta \in \mathbb{R}\backslash\mathbb{Q}$): non-commutative elliptic curves;

3) (hyperbolic) Non-commutative space Sh^{nc} containing the classical Shimura variety Sh (2-dimensional analogue of Bost-Connes systems).

It would be interesting to understand why these 3 classes appear in both contexts (δ-geometry and non-commutative geometry); also one would like to see whether there is a connection, in the case of these 3 classes, between the 2 contexts.

Note that non-commutative geometry can also tackle the dynamics of rational functions that are not necessarily post-critically finite of Euler characteristic zero. It is conceivable that some post-critically finite polynomials of non-zero Euler characteristic possess δ-invariants for some particular primes (with respect to the anticanonical bundle or other bundles). A good start would be to investigate the δ-invariants of $\sigma(x) = x^2 - 1$. Another good start would be to investigate δ-invariants of post-critically finite polynomials with Euler characteristic zero that are congruent modulo special primes to post-critically finite polynomials with Euler characteristic zero.

Problem 3.4. *Study the de Rham cohomology of arithmetic jet spaces. Find arithmetic analogues of Kähler differentials Ω and $\mathcal{D}$-modules. Find an object that is to $\mathcal{D}$ what $\mathcal{O}^1$ is to $Sym(\Omega)$.*

The study of de Rham cohomology of arithmetic jet spaces was started in [7] where it is shown that the de Rham cohomology of $J^n(X)$ carries information about the arithmetic of X. The de Rham computations in [7] are probably shadows of more general phenomena which deserve being understood. Also the de Rham setting could be replaced by an overconvergent one; overconvergence is known to give an improved picture of the de Rham story and, on the other hand, as already mentioned, it was proved in [27] that most of the remarkable δ-functions occurring in the theory possess a remarkable overconvergence property in the "δ-variables" called *δ-overconvergence*. Finally one is tempted to try to relate the de Rham cohomology of arithmetic jet spaces $J^n(X)$ to the de Rham-Witt complex of X in characteristic p and in mixed characteristic. Note further that since the arithmetic jet space $J^1(X)$ is an analogue of the (physical) tangent bundle $T(X)$ of X it follows that the sheaf

$\mathcal{O}^1$ is an arithmetic analogue of the sheaf $Sym(\Omega_{X/R})$, symmetric algebra on the Kähler differentials. But there is no obvious arithmetic analogue of the sheaf $\Omega_{X/R}$ itself. Also there is no obvious arithmetic analogue of the sheaf $\mathcal{D}_X$ of differential operators on X and of $\mathcal{D}_X$-modules. The absence of immediate analogues of Ω and $\mathcal{D}$ is of course related to the intrinsic non-linearity of p-derivations. It would be interesting to search for such analogues. It is on the other hand conceivable that there is a sheaf in the arithmetic theory that is to $\mathcal{D}$ what $\mathcal{O}^1$ is to $Sym(\Omega)$. Recall that the associated graded algebra of $\mathcal{D}$ is canonically isomorphic to the algebra of functions on the (physical) cotangent bundle $\mathcal{O}(T^*(X))$ (and not on the tangent bundle); this looks like a discrepancy but actually the arithmetic jet space $J^1(X)$ has a sort of intrinsic self-duality (cf. [16]) that is missing in the classical algebro-geometric case where the tangent bundle $T(X)$ and the cotangent bundle $T^*(X)$ and not naturally dual (unless, say, a symplectic structure is given).

The δ-overconvergence property mentioned in Problem 3.4 may hold the key to:

Problem 3.5. *Define and study the/a maximal space of δ-modular forms on which Atkin's U operator can be defined.*

Indeed the Hecke operators $T(n)$ with $p \not| n$ are defined on δ-modular forms and have a rich theory in this context [15]. In contrast to this $T(p)$ and hence U are still mysterious in the theory of δ-modular forms. An step in understanding U was taken in [26] where the theory mod p for series of order 1 was given a rather definitive treatment. However the theory in characteristic zero seems elusive at this point. There are two paths towards such a theory so far. One path is via *δ-symmetry* [24, 26]; this is a characteristic 0 analogue of the concept of δ-p-symmetry mod p discussed above. Another path is via δ-overconvergence [27]. The two paths seem to lead into different directions and this discrepancy needs to be better understood. Assuming that a good theory of U is achieved, this might lead to a Hida-like theory of families of differential modular forms, including Galois representations attached to such forms. It is conceivable that families in this context are not power series but Witt vectors. Part of the quest for a U theory of δ-modular forms is to seek a δ-analogue of Eisentein series. It is conceivable that the rings $\mathcal{O}^n(X_1(N))$ contain functions that do not vanish at the cusps and are eigenvectors of the Hecke operators; such functions could be viewed as "δ-Eisenstein" forms of weight zero.

Problem 3.6. *Interpret information contained in the arithmetic jet spaces $J^n(X)$ as an arithmetic Kodaira-Spencer "class" of X.*

Indeed some of these arithmetic Kodaira-Spencer classes (e.g in the case of elliptic curves or, more generally, abelian schemes) were studied in [15, 16] and lead to interesting δ-modular forms. For general schemes (e.g for curves of higher genus) these classes were explored in Dupuy's thesis [40]. They are non-abelian cohomology classes with values in the sheaf of automorphisms of p-adic affine spaces $\widehat{\mathbb{A}}^d$ (in the case of curves $d = 1$). These classes arise from comparing the local trivializations of arithmetic jet spaces. In this more general case these classes may hold the key to a "deformation theory over the field with one element". On the other hand Dupuy proved in [40] that if X is a smooth projective curve of genus ≥ 2 over R then $J^1(X)$ is a torsor for some line bundle over X; this is rather surprising in view of the high non-linearity of the theory. One should say that the line bundle in question is still mysterious and deserves further investigation.

Problem 3.7. *Further develop the partial differential theory in* [20, 21, 22].

Indeed in spite of the extensive work done in [20, 21, 22] the arithmetic *partial* differential theory is still in its infancy. The elliptic case of that theory [20] (which, we recall, involves operators δ_{p_1} and δ_{p_2} corresponding to two primes p_1 and p_2) is directly related to the study of the de Rham cohomology of arithmetic jet spaces [7]; indeed one of the main results in [7] shows that the arithmetic Laplacians in [20] are formal primitives (both p_1-adically and p_2-adically) of global 1-forms on the arithmetic jet spaces (these forms being not exact, although formally exact, and hence closed). By the way analogues of these results in [7] probably exist in the case of modular curves; in the one prime case a beginning of such a study was undertaken in [16], where some of the main δ-modular forms of the theory were shown to satisfy some remarkable systems of Pfaff equations. The hyperbolic/parabolic case of the theory [21, 22] (which, we recall, involves a p-derivation δ_p with respect to a prime p and a usual derivation operator δ_q) could be further developed as follows. One could start by "specializing" the variable q in δ_q to elements π in *arbitrarily ramified* extensions of $\mathbb{Z}_p$. This might push the theory in the "arbitrarily ramified direction" which would be extremely desirable for arithmetic-geometric applications. Indeed our ordinary arithmetic differential theory is, at present, a non-ramified (or at most "boundedly ramified") theory. A further idea along these lines would be to use the solutions of the arithmetic partial differential equations in [21, 22] to let points "flow" on varieties defined over number fields. Some of the solutions in [21, 22] have interesting arithmetic features (some look like hybrids between quantum exponentials and Artin-Hasse exponentials, for instance) so the "flows" defined by them might have arithmetic consequences. The challenge is to find (if at all possible) "special values" of these solutions that are algebraic. One should also mention that the arithmetic hyperbolic and parabolic equations in [21, 22] have, in special cases, well defined "indices" that seem to carry arithmetic information; the challenge would be to make the index machinery work in general situations and to study the variation of indices in families.

Problem 3.8. *Find an arithmetic analogue of Sato hyperfunction solutions of both "ordinary" and "partial" arithmetic differential equations.*

Indeed Sato's hyperfunctions, in their simplest incarnation, are pairs $(f(x), g(x))$ of functions on the unit disk (corresponding to the distribution $f(x) - g(x^{-1})$) modulo (c, c), c a constant. The derivative of a pair is then $(\frac{df}{dx}(x), -x^2\frac{dg}{dx}(x))$.) One could then try to consider, in the arithmetic case, pairs (P, Q) of points of algebraic groups with values in δ-rings modulo an appropriate equivalence relation and with an appropriate analogue of differentiation with respect to p; this framework could be the correct one for "non-analytic" solutions of the equations in [20, 21, 22].

Problem 3.9. *Construct p-adic measures from δ-modular forms.*

Indeed one of the main ideas in Katz's approach to p-adic interpolation [50] was to lift some of the remarkable $\mathbb{Z}_p$-valued (p-adic) measures of the theory to $\mathbb{W}$-valued measures where $\mathbb{W}$ is the ring of (generalized) p-adic modular forms. One can hope that some of these $\mathbb{W}$-valued measures of Katz can be further lifted to measures with values in the p-adic completion of the ring of δ-modular functions M^∞. Indeed recall from Theorem 2.11 that there is a canonical homomorphism $M^\infty \to \mathbb{W}$ whose image is p-adically dense, hence the "lifting" problem makes sense. These lifted $\widehat{M^\infty}$-valued measures could then be evaluated at various elliptic

curves defined over δ-rings to obtain new $\mathbb{Z}_p$-valued measures (and hence new p-adic interpolation results) in the same way in which Katz evaluated his measures at special elliptic curves. Another related idea would be to interpret the solutions in $\mathbb{Z}_p[[q]]$ of the arithmetic partial differential equations in Problem 3.7 above as measures (via Iwasawa's representation of measures as power series). There is a discrepancy in this approach in that the derivation of interest in Iwasawa's theory is $(1+q)\frac{d}{dq}$ whereas the derivation of interest in Problem 3.7 is $q\frac{d}{dq}$; nevertheless one should pursue this idea and understand the discrepancy.

Problem 3.10. *Find arithmetic analogues of classical theorems in the theory of differential algebraic groups and further develop the δ-Galois theory in* [35]. *Also further develop the arithmetic analogue of the theory of symmetric spaces in* [34]*, especially on the Riemannian side.*

Indeed the theory of groups defined by (usual) differential equations ("differential algebraic groups") is by now a classical subject: it goes back to Lie and Cartan and underwent a new development, from a rather new angle, through the work of Cassidy and Kolchin [36, 52]. It is tempting to seek an arithmetic analogue of this theory: one would like to understand, for instance, the structure of all subgroups of $GL_n(R)$ that are defined by arithmetic differential equations. The paper [14] proves an arithmetic analogue of Cassidy's theorem about Zariski dense subgroups of simple algebraic groups over differential fields; in [14] the case of Zariski dense mod p groups is considered. But Zariski dense groups such as $GL_n(\mathbb{Z}_p)$ are definitely extremely interesting (and lead to interesting Galois theoretic results such as in [16], Chapter 5). So a generalization of [14] to the case of Zariski dense (rather than Zariski dense mod p) groups, together with a generalization of the Galois theoretic results in [16], would be very desirable. For instance it would be interesting to classify all δ-subgroups of the multiplicative group $\mathbb{G}_m(R) = R^\times$ (or more generally of $GL_2(R)$) and find the invariants of such groups acting on $\widehat{R\{x\}_{(p)}}$ (where $R\{x\} = R[x, x', x'', ...]$). Also remark that, as in the case of usual derivations, there are interesting ("unexpected") homomorphisms in δ-geometry between $GL_1 = \mathbb{G}_m$ and GL_2, for instance

$$\mathbb{G}_m(R) \to GL_2(R), \qquad a \mapsto \begin{pmatrix} a & a\psi_*(a) \\ 0 & a \end{pmatrix}$$

where ψ_* is a δ-character, i.e. $\psi \in \mathcal{X}^n(\mathbb{G}_m)$. Cf. [43] for interesting developments into this subject. The main open problem in the δ-Galois theory of GL_n [35] seems at this point to decide if the δ-Galois groups always contain a subgroup of the diagonal matrices as a subgroup of finite index. Other problems are: to establish a Galois correspondence; to understand the relation (already hinted at in [35]) between δ-Galois groups and Galois problems arising from the dynamics on $\mathbb{P}^n$; to generalize the theory by replacing GL_n with an arbitrary reductive group. With regards to the analogue in [34] of the theory of symmetric spaces the main open problems are to find analogues of the Riemannian metrics and curvature. An analogue of Lie brackets can, by the way, be developed; it would be interesting to use it to develop an "arithmetic Riemannian theory".

Problem 3.11. *Compose some of the basic δ-functions of the theory in* [16] *(e.g. the δ-modular forms on Shimura curves) with p-adic uniformization maps (e.g. with Drinfeld's uniformization map of Shimura curves).*

Indeed this might shed a new light (coming from the analytic world) on δ-geometry. These composed maps would belong to a "δ-rigid geometry" which has yet to be developed in case these maps are interesting enough to require it. By the way it is not at all clear that the functor that attaches to a formal p-adic scheme its arithmetic jet space can be prolonged to a functor in the rigid category. The problem (which seems to boil down to some quite non-trivial combinatorially flavored calculation) is to show that the arithmetic jet space functor sends blow-ups with centers in the closed fiber into (some version of) blow-ups.

In the spirit of the last comments on Problem 3.11 one can ask:

Problem 3.12. *Study the morphisms $J^n(X) \to J^n(Y)$ induced by non-étale finite flat covers of smooth schemes $X \to Y$.*

Indeed note that if $X \to Y$ is finite and étale then it is well known that $J^n(X) \to J^n(Y)$ are finite and étale; indeed $J^n(X) \simeq J^n(Y) \times_Y X$. But note that if $X \to Y$ is only finite and flat then $J^n(X) \to J^n(Y)$ is neither finite nor flat in general. One of the simplest examples which need to be investigated (some partial results are available [28], cf. Theorem 2.17) is that of the covers $[p^\nu] : G \to G$ of smooth group schemes (or formal groups) given by multiplication by p^ν. The geometry of the induced endomorphisms of the arithmetic jet spaces is highly complex and mysterious. Understanding it might be, in particular, another path towards introducing/understanding the Atkin operator U on δ-modular forms referred to in Problem 3.5. An obviously closely related problem is to understand the p-jet spaces of p-divisible groups; cf. Theorem 2.17. Yet another example of interest is the study of $J^n(X) \to J^n(X/\Gamma)$ for Γ a finite group acting on a smooth X; even the case $X = Y^n$ with Y a curve and $\Sigma = S_n$ the symmetric group acting naturally is still completely mysterious. This latter case is related to the concept of δ-symmetry mentioned in Problem 3.5 and appeared in an essential manner in the paper [24]: the failure of invariants to commute with formation of jet spaces (in the ramified case) is directly responsible for the existence (and indeed abundance) of δ-functions on smooth projective curves which do not arise from δ-characters of the Jacobian.

Problem 3.13. *Understand which analytic functions $X(\mathbb{Z}_p) \to \mathbb{Z}_p$ for smooth schemes $X/\mathbb{Z}_p$ are induced by δ-functions.*

Indeed it was proved in [23] that a function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is analytic if, and only if, there exists m such that f can be represented as $f(x) = F(x, \delta x, \dots, \delta^m x)$, where $F \in \mathbb{Z}_p[x_0, x_1, ..., x_m]\hat{}$ is a restricted power series with $\mathbb{Z}_p$-coefficients in $m+1$ variables. This can be viewed as a "differential interpolation result": indeed $f(x)$ is given by a finite family of (unrelated) power series $F_i(x)$ convergent on disjoint balls B_i that cover $\mathbb{Z}_p$ and the result says that one can find a single power series $F(x, \delta x, ..., \delta^m x)$ that equals $F_i(x)$ on B_i for each i. One can ask for a generalization of this by asking which analytic functions $f : X(\mathbb{Z}_p) \to \mathbb{Z}_p$ defined on the $\mathbb{Z}_p$-points of a smooth scheme $X/\mathbb{Z}_p$ come from a δ-function $\tilde{f} \in \mathcal{O}^n(X)$ (i.e. $f = \tilde{f}_*$); of course such a $\tilde{f}$ cannot be, in general, unique. If $X = \mathbb{A}^1$ is the affine line then the result in [23] says that any f comes from some $\tilde{f}$. This is probably still the case if X is any affine smooth scheme. On the other hand this fails if $X = \mathbb{P}^1$ is the projective line simply because there are no non-constant δ-functions in $\mathcal{O}^n(\mathbb{P}^1)$ [12] but, of course, there are plenty of non-constant analytic functions $\mathbb{P}^1(\mathbb{Z}_p) \to \mathbb{Z}_p$. There should be a collection of cohomological obstructions to lifting f to some $\tilde{f}$ that should

reflect the global geometry of X. This seems to us a rather fundamental question in understanding the relation between p-adic analytic geometry and δ-geometry.

In the light of Theorem 2.17 one can ask:

Problem 3.14. *Let $\alpha_0, ..., \alpha_\nu$ be elements in the algebraic closure of the fraction field of R which are integral over R. Let $X_i = Spec\ R[\alpha_i]$ be viewed as a closed subscheme of the line $\mathbb{A}^1$ over R. Compute/understand the arithmetic jet spaces $J^n(\cup_{i=0}^{\nu} X_i)$.*

This is a problem "about the interaction" of algebraic numbers. Indeed the case $\nu = 0$ is clear; for instance if $R[\alpha]$ is totally ramified over R (and $\neq R$) then the arithmetic jet spaces are empty: $J^n(Spec\ R[\alpha]) = \emptyset$ for $n \geq 1$. However, for $\nu \geq 1$, an interesting new phenomenon occurs. Indeed if $\alpha_i = \zeta_{p^i}$ (primitive p^i-th root of unity) then although $J^n(Spec\ R[\zeta_{p^i}]) = \emptyset$ for $n \geq 1$ and $i \geq 1$ we have that $J^n(\cup_{i=0}^{\nu} Spec\ R[\zeta_{p^i}]) = J^n(\mu_{p^\nu})$ is non-empty and indeed extremely interesting; cf. Theorem 2.17.

Problem 3.15. *Find arithmetic analogues of Hamiltonian systems and of algebraically completely integrable systems. Find arithmetic analogues of the formal pseudo-differential calculus.*

This problem is motivated by the link (due to Fuchs and Manin [56]) between the Painlevé VI equation (which has a Hamiltonian structure) and the Manin map of an elliptic fibration. Painlevé VI possesses an arithmetic analogue whose study was begun in [31]; this study is in its infancy and deserves further attention. More generally there is an intriguing possibility that other physically relevant differential equations (especially arising in Hamiltonian contexts, especially in the completely integrable situation, both finite and infinite dimensional) have arithmetic analogues carrying arithmetic significance. Finally it is conceivable that a meaningful arithmetic analogue of the formal pseudo-differential calculus in one variable [63]. p. 318 can be developed; in other words one should be able to bring into the picture negative powers of the p-derivation $\delta : \mathcal{O}^n(X) \to \mathcal{O}^{n+1}(X)$ in the same way in which formal pseudo-differential calculus brings into the picture the negative powers of the total derivative operator acting on functions on jet spaces.

Problem 3.16. *Find an arithmetic analogue of the differential groupoids/Lie pseudogroups in the work of Lie, Cartan, Malgrange* [39].

Indeed recall that one can view the p-jet spaces $J^n(\Sigma_m)$ of $\Sigma_m = Spec\ W_m(R)$ and the jet maps induced by the comonad maps as an arithmetic analogue of the Lie groupoid $J^n(\mathbb{R} \times \mathbb{R}/\mathbb{R})^*$ of the line; cf. [29] and Theorem 2.18 above for results on this. It would be interesting to investigate subobjects of the system $J^n(\Sigma_m)$ that play the role of analogues of differential sub-groupoids and to find arithmetic analogues of the differential invariants of diffeomorphism groups acting on natural bundles arising from frame bundles. A theory of $J^n(\Sigma_m)$, suitably extended to other rings and to arithmetic analogues of poly-vector fields, could also be interpreted as an arithmetic analogue of the theory of the deRham-Witt complex [44] because it would replace the usual Kähler differentials Ω by constructions involving the operators δ_p.

Problem 3.17. *Compute $\mathcal{O}^n(\mathbb{T}(N, \kappa))$ where $\mathbb{T}(N, \kappa)$ is the Hecke $\mathbb{Z}$-algebra attached to cusp forms on $\Gamma_1(N)$ of level κ.*

This could lead to a way of associating differential modular forms $f^\sharp$ to classical newforms f of weight $\neq 2$. (Cf. Theorem 2.16.) This might also lead to a link between δ-geometry and Galois representations. The problem may be related to the study of double coset sets of GL_2 (or more generally GL_n) and a link of this to the study in [33, 34, 35] is plausible.

We end by stating two of the most puzzling concrete open problems of the theory.

Problem 3.18. *Compute $\mathcal{O}^n(X)$ for an elliptic curve X.*

Note that $\mathcal{O}^1(X)$ and $\mathcal{X}^n(X)$ have been computed (Theorem 2.2) and one expects $\mathcal{X}^n(X)$ to "generate" $\mathcal{O}^n(X)$. In particular assume X is not a canonical lift and ψ is a basis of $\mathcal{X}^2(X)$; is it true that $\mathcal{O}^n(X) = R[\psi, \delta\psi, ..., \delta^{n-1}\psi]\hat{}$? The analogue of this in differential algebra is true; cf. [9].

Problem 3.19. *Compute $\mathcal{X}^n(G)$ for G an extension of an elliptic curve by $\mathbb{G}_m$.*

One expects that this module depends in an arithmetically interesting way on the class of the extension. The problem is directly related to that of understanding the cohomology of arithmetic jet spaces.

References

[1] D. V. Alexeevski, V. V. Lychagin, A. M. Vinogradov, *Basic ideas and concepts of differential geometry*, in: Geometry I, R. V. Gamkrelidze, Ed., Encyclopedia of Mathematical Sciences, Volume 28, Springer 1991.

[2] M.Barcau, *Isogeny covariant differential modular forms and the space of elliptic curves up to isogeny*, Compositio Math., 137 (2003), 237-273.

[3] M. Barcau, A. Buium, *Siegel differential modular forms*, International Math. Res. Notices, 2002, No. 28, pp.1459-1503.

[4] J. Borger, *The basic geometry of Witt vectors, I*: the affine case, Algebra and Number Theory 5 (2011), no. 2, pp 231-285.

[5] Borger, J., *The basic geometry of Witt vectors, II: Spaces*, Mathematische Annalen 351 (2011), no. 4, pp 877-933.

[6] J. Borger, Λ-*rings and the field with one element*, arXiv:0906.3146v1

[7] J. Borger, A. Buium, *Differential forms on arithmetic jet spaces*, Selecta Math., 17, 2 (2011), pp. 301-335.

[8] A.Buium, *Intersections in jet spaces and a conjecture of S.Lang*, Annals of Math. 136 (1992) 557-567.

[9] A. Buium, *Differential algebra and diophantine geometry*, Hermann, 1994.

[10] A. Buium, *On a question of B.Mazur*, Duke Math. J., 75, 3, (1994), 639-644.

[11] A. Buium, *Differential characters of Abelian varieties over p-adic fields*, Invent. Math., 122 (1995), pp. 309-340.

[12] A. Buium, *Geometry of p-jets*, Duke J. Math. 82, (1996), 2, pp. 349-367.

[13] A. Buium, *Differential characters and characteristic polynomial of Frobenius*, Crelle J. 485 (1997), 209-219.

[14] A. Buium, *Differential subgroups of simple algebraic groups over p-adic fields*, Amer. J. Math. 120 (1998), 1277-1287.

[15] A. Buium, *Differential modular forms*, J. reine angew. Math., 520, (2000), pp. 95-167.

[16] A. Buium, *Arithmetic Differential Equations*, Math. Surveys and Monographs, 118, American Mathematical Society, Providence, RI, 2005. xxxii+310 pp.

[17] A. Buium, Differential eigenforms, J. Number Theory, 128 (2008), 979-1010.

[18] A. Buium, B. Poonen, *Independence of points on elliptic curves arising from special points on modular and Shimura curves, I: global results*, Duke Math. J., 147, 1 (2009), 181-191.

[19] A. Buium, B. Poonen, *Independence of points on elliptic curves arising from special points on modular and Shimura curves, II: local results*, Compositio Math., 145 (2009), 566-602.

[20] A. Buium, S.R. Simanca, *Arithmetic Laplacians*, Adv. Math. 220 (2009), pp. 246-277.

[21] A. Buium, S.R. Simanca, *Arithmetic partial differential equations, I*, Advances in Math. 225 (2010), 689-793.
[22] A. Buium, S.R. Simanca, *Arithmetic partial differential equations II*, Advances in Math., 225 (2010), 1308-1340.
[23] A. Buium, C. Ralph, S.R. Simanca, *Arithmetic differential operators on $\mathbb{Z}_p$*, J. Number Theory 131 (2011), pp. 96-105.
[24] A. Buium, *Differential characters on curves*, in: Number Theory, Analysis and Geometry: In Memory of Serge Lang, D. Goldfeld et al. Editors, Springer, 2011, pp. 111-123.
[25] A. Buium, A. Saha, *The ring of differential Fourier expansions*, J. of Number Theory 132 (2012), 896-937.
[26] A. Buium, A. Saha, *Hecke operators on differential modular forms mod p*, J. Number Theory 132 (2012), 966-997
[27] A. Buium, A. Saha, *Differential overconvergence*, in: Algebraic methods in dynamical systems; volume dedicated to Michael Singer's 60th birthday, Banach Center Publications, Vol 94, 99-129 (2011).
[28] A. Buium, *p-jets of finite algebras, I: p-divisible groups*, Documenta Math., 18 (2013) 943–969.
[29] A. Buium, *p-jets of finite algebras, II: p-typical Witt rings*, Documenta Math., 18 (2013) 971–996.
[30] A. Buium, *Galois groups arising from arithmetic differential equations*, to appear in: Proceedings of a Conference in Luminy, Seminaires et Congrès, Soc. Math. France.
[31] A. Buium, Yu. I. Manin, *Arithmetic differential equations of Painlevé VI type*, arXiv:1307.3841
[32] A. Buium, A. Saha, *The first p-jet space of an elliptic curve: global functions and lifts of Frobenius*, arXiv:1308.0578, to appear in Math. Res. Letters.
[33] A. Buium, T. Dupuy, *Arithmetic differential equations on GL_n, I: differential cocycles*, arXiv:1308.0748v1.
[34] A. Buium, T. Dupuy, *Arithmetic differential equations on GL_n, II: arithmetic Lie theory*, arXiv:1308.0744.
[35] A. Buium, T. Dupuy, *Arithmetic differential equations on GL_n, III: Galois groups*, arXiv:1308.0747
[36] P. Cassidy, *Differential algebraic groups*, Amer. J. Math 94 (1972), 891-954.
[37] Z. Chatzidakis, E. Hrushovski, *Model theory of difference fields*, Trans. AMS, 351 (1999), 2997-3071.
[38] A. Connes, *Non-commutative Geometry*, Academic Press, 1994.
[39] V. G. Drinfeld, *Elliptic modules*, Math. Sbornik 94 (1974), 594-627.
[40] T. Dupuy, Arithmetic deformation theory of algebraic curves, PhD Thesis (UNM).
[41] B. Dwork, G. Gerotto, F. J. Sullivan, *An introduction to G-functions*. Annals of Mathematics Studies, 133. Princeton University Press, Princeton, NJ, 1994. xxii+323 pp.
[42] M.Greenberg, *Schemata over local rings*, Annals of Math. 73 (1961), 624-648.
[43] A. Herras-Llanos, PhD thesis (UNM), in preparation.
[44] L. Hesselholt, The big deRham-Witt complex, preprint, 2011.
[45] C. Hurlburt, *Isogeny covariant differential modular forms modulo p*, Compositio Math. 128, (2001), 1, pp. 17-34.
[46] Y. Ihara, *An invariant multiple differential attached to the field of elliptic modular functions of characteristic p*, Amer. J. Math., XCIII, 1, (1971), 139-147.
[47] Y. Ihara, *On Fermat quotient and differentiation of numbers*, RIMS Kokyuroku 810 (1992), 324-341, (In Japanese). English translation by S. Hahn, Univ. of Georgia preprint.
[48] T. A. Ivey, J. M. Landsberg, *Cartan for beginners: differential geometry via moving frames and exterior differential systems*, GTM 61, AMS 2003.
[49] A. Joyal, *$\delta-$anneaux et vecteurs de Witt*, C.R. Acad. Sci. Canada, Vol. VII, No. 3, (1985), 177-182.
[50] N. Katz, *p-adic interpolation of real Eisenstein series*, Ann. of Math. 104 (1976), 459-571.
[51] E.R. Kolchin, *Differential algebra and algebraic groups*. Pure and Applied Mathematics, Vol. 54. Academic Press, New York-London, 1973. xviii+446 pp.
[52] E.Kolchin, *Differential Algebraic Groups*, Academic Press, 1985.
[53] N. Kurokawa, H. Ochiai, M. Wakayama, *Absolute derivations and zeta functions*, Documenta Math.,Extra Volume Kato (2003), 565-584.

[54] B. Malgrange, Le groupoïde de Galois d'un feuilletage, Monographie 28 Vol 2, L'enseignement Mathématique (2001).
[55] Yu. I. Manin, *Rational points on algebraic curves over function fields*, Izv. Acad. Nauk USSR, 27 (1963), 1395-1440.
[56] Yu. I. Manin, *Sixth Painlevé equation, universal elliptic curve, and mirror of* $\mathbb{P}^2$, arXiv:alg-geom/9605010.
[57] Yu. I. Manin, *Cyclotomy and analytic geometry over* $\mathbb{F}_1$, arXiv:0809.1564.
[58] Yu. I. Manin, *Numbers as functions*, p-Adic Numbers, Ultrametric Analysis, and Applications, Vol. 5, Issue 4 (2013), 313-325.
[59] B.Mazur, *Arithmetic on curves*, Bull. Amer. Math. Soc. 14, 2 (1986), 207-259.
[60] M.Marcolli, *Lectures on Arithmetic Non-commutative Geometry*, Univ. Lecture Series 36, AMS, 2005.
[61] M. Morishita, *Knots and primes*, Springer, 2012.
[62] S. P. Novikov, I. A. Taimanov, *Modern Geometric Structures and Fields*, Graduate Studies in Mathematics, Volume 71, AMS, Providence, 2006.
[63] P. J. Olver, *Appications of Lie Groups to Differential Equations*, GTM 107, Springer, 2000.
[64] R. Pink, *A combination of the conjectures of Mordell-Lang and André-Oort*, in: Progress in Math 235, Birkhauser 2005, pp. 251-282.
[65] M.Raynaud, *Courbes sur une variété abélienne et points de torsion*, Invent. Math. 71 (1983), 207-235.
[66] M. Singer, M. van der Put, *Galois theory of difference equaltions*, LNM, Springer 1997.
[67] P. Vojta, Jets via Hasse-Schmidt derivations, in: Diophantine geometry, pp. 335-361, CRM Series, 4, U. Zannier Ed., Sc. Norm., Pisa, 2007.

Department of Mathematics and Statistics, University of New Mexico, Albuquerque, NM 87131, USA

E-mail address: buium@math.unm.edu