

## Transcendental numbers as solutions to arithmetic differential equations

by  
ALEXANDRU BUIUM

*Dedicated to Vasile Brînzănescu in honour of his 70th birthday*

### Abstract

Arithmetic differential equations are analogues of algebraic differential equations in which derivative operators acting on functions are replaced by Fermat quotient operators acting on numbers. Now, various remarkable transcendental functions are solutions to algebraic differential equations; in this note we show that, in a similar way, some remarkable  $p$ -adic transcendental numbers (including certain “ $p$ -adic periods”) are solutions to arithmetic differential equations. Inspired by a recent paper of Manin, we then speculate on the possibility of understanding the algebraic relations among periods via Galois groups of arithmetic differential equations.

**Key Words:** Transcendental numbers.

**2010 Mathematics Subject Classification:** Primary 11E57, Secondary 12H05.

### 1 Arithmetic differential equations [5, 8]

In the classical theory of differential equations (in the complex  $z$ -plane  $\mathbb{C}$ ) one starts with a ring  $\mathcal{R}$  of holomorphic functions in  $z$  that is stable under the derivation operator  $\delta_z = \frac{d}{dz}$ . Then, for  $N \geq 1$ , one defines a *differential polynomial function* (or simply a  $\delta$ -function) of order  $r$  (in  $N$  variables) as a set theoretic map  $f : \mathcal{R}^N \rightarrow \mathcal{R}$  with the property that there exists a polynomial in  $(r+1)N$  variables such that for all  $u \in \mathcal{R}^N$  we have  $f(u) = F(u, \delta_z u, \dots, \delta_z^r u)$ . More generally, if  $X \subset \mathbb{A}^N$  is a smooth closed subscheme of the affine space, a function  $f : X(\mathcal{R}) \rightarrow \mathcal{R}$  on the set of  $\mathcal{R}$ -points of  $X$  can be called a  $\delta$ -function of order  $r$  if it is the restriction of a  $\delta$ -function of order  $r$  on  $\mathcal{R}^N = \mathbb{A}^N(\mathcal{R})$ . One can globalize this notion to the case when  $X$  is not necessarily affine. An *algebraic differential equation* is then an equation of the form  $f(P) = 0$  with  $f$  as above and solutions  $P \in X(\mathcal{R})$ . When investigating transcendence properties one also fixes a subring  $\mathcal{O} \subset \mathcal{R}$  that is stable under the operator  $\delta_z$  and one asks that the  $\delta$ -functions under consideration be defined over  $\mathcal{O}$ , i.e. the polynomials  $F$  have coefficients in  $\mathcal{O}$ ; a typical example of choice for  $\mathcal{O}$  is, of course,  $\mathcal{O} = \mathbb{C}[z]$ , the ring of polynomials. Then one can investigate the algebraic dependence relations over  $\mathcal{O}$  among solutions of various algebraic differential equations. In case the equations are linear, or more generally attached to algebraic groups, this problem is directly related to the differential Galois theory of these equations [16].

Let us now recall from [5, 8] the basics of a theory that replaces functions by numbers and derivations  $\delta_z$  by Fermat quotient operators  $\delta_p$ . The analogue of the ring  $\mathcal{R}$  will be the ring  $R$  described as follows. We start with the ring of integers  $\mathbb{Z}$ , we let  $\mathbb{Z}_p$  be the  $p$ -adic completion of  $\mathbb{Z}$ , we let  $\mathbb{Z}_p^{ur}$  be the maximal unramified extension of  $\mathbb{Z}_p$  (obtained by adjoining to  $\mathbb{Z}_p$  all the roots of unity of order prime to  $p$ ), and we let  $R$  be the  $p$ -adic completion of  $\mathbb{Z}_p^{ur}$ . The ring  $R$  plays a central role in number theory and turns out to have other descriptions (e.g. it is the  $p$ -typical Witt ring  $W(k)$  on the algebraic closure  $k = \overline{\mathbb{F}_p}$  of the field  $\mathbb{F}_p$  with  $p$  elements; it is also the unique complete discrete valuation ring with maximal ideal generated by  $p$  and residue field  $k$ ). It is well known that any element of  $R$  can be written uniquely as a series  $\sum c_i p^i$  where  $c_i$  are either zero or in the group  $\mu(R)$  of roots of unity in  $R^\times$ . Also there is a unique ring automorphism  $\phi_p : R \rightarrow R$  whose reduction mod  $p$  is the Frobenius automorphism of  $k$ ;  $\phi_p$  is given by  $\phi_p(\sum c_i p^i) = \sum c_i^p p^i$ ,  $c_i \in \mu(R) \cup \{0\}$ . We then define the *Fermat quotient operator*  $\delta = \delta_p : R \rightarrow R$  by the formula  $\delta_p u = \frac{\phi_p(u) - u^p}{p}$  and we view this operator as an analogue of a derivation. (Note however that  $\delta$  is *not* additive!) Next recall that by a restricted power series with coefficients in  $R$  one understands a power series whose coefficients tend to 0  $p$ -adically. Here is one of our main definitions in [5]: a set theoretic function  $f : R^N \rightarrow R$  is called a  $\delta$ -function of order  $r$  if there exists a restricted power series  $F$  with coefficients in  $R$ , in  $(r+1)N$  variables, such that for all  $u \in R^N$ , we have  $f(u) = F(u, \delta_p u, \dots, \delta_p^r u)$ . More generally if  $X \subset \mathbb{A}^N$  is a smooth closed subscheme of the affine space then a function  $f : X(R) \rightarrow R$  on the set of  $R$ -points of  $X$  is called a  $\delta$ -function of order  $r$  if it is the restriction of a  $\delta$ -function of order  $r$  on  $R^N = \mathbb{A}^N(R)$ . If  $X$  is an arbitrary (not necessarily affine) smooth scheme over  $R$  a function  $f : X(R) \rightarrow R$  is called a  $\delta$ -function of order  $r$  if its restriction to any affine open set of  $X$  has this property. Finally an *arithmetic differential equation* on an  $X$  as above is, by definition, an equation of the form  $f(P) = 0$  where the solutions  $P$  are in  $X(R)$ . Again, if one wants to investigate transcendence properties of solutions, one fixes a subring  $\mathcal{O} \subset R$  stable under  $\delta_p$  and one assumes that the  $\delta$ -functions under consideration are “defined” over  $\mathcal{O}$ . The latter may mean a number of things. One can ask, for instance, that the coefficients of the series  $F$  defining  $f$  belong to  $\mathcal{O}$ ; this is a natural condition only if  $\mathcal{O}$  is  $p$ -adically complete and the natural choice, in this case, is  $\mathcal{O} = \mathbb{Z}_p$ . Other meanings of “defined over  $\mathcal{O}$ ” may make sense in special situations, however; for instance one can consider the case (which effectively occurs in interesting examples) when the series  $F$  are algebraic over a polynomial ring with coefficients in  $\mathcal{O}$ ; in this case it is natural to take  $\mathcal{O}$  not necessarily  $p$ -adically complete.

## 2 Transcendental functions/numbers appearing as solutions

### 2.1 Exponential function

The simplest example we would like consider is that of the algebraic differential equation

$$\frac{\delta_z u}{u} = \beta \tag{2.1}$$

where  $\beta \in \mathcal{R}$  is a fixed function and the solutions are  $u \in \mathcal{R}^\times$ . We may interpret this as an algebraic differential equation on the hyperbola  $H \subset \mathbb{A}^2$  defined by  $xy - 1 = 0$ , by viewing  $P := (u, \frac{1}{u}) \in H(\mathcal{R})$  as a point of this hyperbola. Of course this hyperbola identifies, via the

first projection with the multiplicative group scheme  $\mathbb{G}_m$ . The solutions to this equation are of the form

$$u = c \cdot \exp \left( \int \beta dz \right), \tag{2.2}$$

where  $c \in \mathbb{C}$ . By the way, the problem of understanding the algebraic relations among these solutions is closely related to the *Ax-Lindemann-Weierstrass* theorem [2] stating that if  $\alpha_1, \dots, \alpha_n$  are holomorphic functions that are algebraic over  $\mathbb{C}(z)$  and are  $\mathbb{Q}$ -linearly independent modulo  $\mathbb{C}$  then  $\exp(\alpha_1), \dots, \exp(\alpha_n)$  are algebraically independent over  $\mathbb{C}(z)$ . We recall that the latter is the functional analogue of the *Lindemann-Weierstrass* theorem asserting that if  $\alpha_1, \dots, \alpha_n \in \mathbb{C}$  are algebraic over  $\mathbb{Q}$  and are linearly independent over  $\mathbb{Q}$  then  $\exp(\alpha_1), \dots, \exp(\alpha_n)$  are algebraically independent over  $\mathbb{Q}$ .

Here is an arithmetic analogue [5, 10] of the above situation. Consider the hyperbola  $H = \mathbb{G}_m$  over  $R$  and the group homomorphism  $\psi : H(R) = R^\times \rightarrow R$  defined by

$$u \mapsto \psi(u) = \frac{1}{p} \log_p \left( \frac{\phi_p(u)}{u^p} \right) = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{p^{n-1}}{n} \left( \frac{\delta u}{u^p} \right)^n \tag{2.3}$$

where  $\log_p$  is the  $p$ -adic logarithm. Then, for any fixed  $\beta \in R$ , one can consider the arithmetic differential equation

$$\psi(u) = \beta. \tag{2.4}$$

Note that the “defining” restricted power series of  $\psi$  is *not* algebraic over the ring of polynomials with coefficients in  $R$ . Since  $\psi$  in 2.3 is a homomorphism it can be viewed as an analogue of the logarithmic derivative map  $u \mapsto \frac{\delta_x u}{u}$ ; hence 2.4 can be viewed as an analogue of 2.1. By the way note that 2.4 is equivalent to each of the following equations

$$\phi_p(u) = \epsilon \cdot u^p \quad \text{or} \quad \delta_p u = \alpha \cdot u^p \tag{2.5}$$

where  $\epsilon = \exp_p(p\beta) = 1 + p\alpha$ ,  $\exp_p$  the  $p$ -adic exponential; in equation 2.5 the “defining” restricted power series is actually a polynomial. In any case the set of solutions to 2.5 (and hence to 2.5 or 2.4) consists of all  $u \in R^\times$  of the form

$$u = \zeta \cdot \exp_p \left( \sum_{n=1}^{\infty} p^n \phi_p^{-n}(\beta) \right) \tag{2.6}$$

where  $\zeta \in R^\times$ ,  $\delta_p \zeta = 0$ . So 2.6 can be viewed as an analogue of 2.2. It is worth mentioning that equation 2.5 is *not* an instance of what is usually called a *difference equation*; indeed difference equations for an automorphism  $\phi_p$  (cf. [26]) take the form

$$\phi_p(u) = \epsilon \cdot u \tag{2.7}$$

rather than 2.5. Nevertheless difference equations 2.7 are also examples of arithmetic differential equations and their Galois theory as arithmetic differential equations [8] is quite different from their Galois theory as difference equations [26]. In terms of transcendence properties one can easily check the following: there exists a subset  $\Omega$  of the first category in the metric space

$X := 1 + pR$  such that for any  $u \in X \setminus \Omega$  there exists a subring  $\mathcal{O}$  of  $R$ , stable under  $\delta_p$  and containing  $\alpha := \frac{\delta_p u}{u^p}$ , with the property that  $u$  is transcendental over  $\mathcal{O}$ ; cf. [10]. On the other hand if  $u$  satisfies 2.5 and lies in  $\mathbb{Z}_p^{ur}$  then it is an easy exercise to see that  $u$  is algebraic over any subring  $\mathcal{O} \subset R$  that is stable under  $\delta_p$  and contains  $\alpha$ ; cf. [10]. On a related note, one has, of course, the profound results due to Mahler, Gelfond, Nesterenko, Philippon, and many others on transcendence (over  $\mathbb{Q}$ !) of exponentials in the  $p$ -adic setting; one prototype of these is Mahler’s theorem stating that if  $a \in \mathbb{C}_p$  is algebraic over  $\mathbb{Q}$  and  $0 < |\alpha|_p < p^{-1/(p-1)}$  then  $\exp_p(\alpha)$  is transcendental over  $\mathbb{Q}$ .

The above example has a matrix analogue [10] which we briefly mention here. In the classical theory of differential equations the matrix analogue of 2.1 is a linear differential equation

$$\delta_z u = \beta \cdot u, \tag{2.8}$$

where  $\beta \in \mathfrak{gl}_n(\mathcal{R})$  is fixed and the solutions are  $u \in GL_n(\mathcal{R})$ ; here  $\mathfrak{gl}_n$  means  $n \times n$  matrices and  $GL_n$  means invertible matrices. The simplest arithmetic analogue of 2.8 considered in [10] is

$$\delta_p u = \beta \cdot u^{(p)}, \tag{2.9}$$

where  $\beta \in \mathfrak{gl}_n(R)$  is fixed and the solutions are  $u \in GL_n(R)$ ; here for  $u = (u_{ij})$  we wrote  $u^{(p)} := (u_{ij}^p)$ . Since the  $\delta$ -functions appearing in 2.9 are actually polynomials it is natural to consider algebraic relations among the entries of solutions to 2.9 over non-complete rings  $\mathcal{O} \subset R$  such that  $\beta \in \mathfrak{gl}_n(\mathcal{O})$ ; this was explored in [10]. The equation 2.8 corresponds to the trivial “arithmetic connection” on  $GL_n$ ; more generally one can consider “arithmetic connections” attached to symmetric/antisymmetric matrices  $q \in GL_n(R)$ ; they lead to equations [9, 10] of the form

$$\delta_p u = \beta \cdot \Phi_p(u), \tag{2.10}$$

where  $\Phi_p$  are appropriate matrices of restricted power series depending on  $q$  and compatible with  $q$  in a way that is reminiscent of the way Chern connections in complex geometry are compatible with hermitian metrics; we refer to [9, 10] for details. Although  $\Phi_p$  are power series (rather than polynomials, as in 2.9) they are “algebraic” and hence it is still natural to consider algebraic relations among the entries of solutions to 2.10 over non-complete rings  $\mathcal{O} \subset R$ ; this is not covered by [10] and deserves being investigated.

### 2.2 Elliptic functions

The next example is taken from [21, 5, 11]. A remarkable class of differential equations in the complex plane is that of Painlevé equations, in particular of the Painlevé VI family which we now describe following the classical work of Fuchs and the modern interpretation of Manin [21]. Let  $E$  be the (smooth projective) elliptic curve over  $\mathbb{Q}(z)$  defined by the equation  $y^2 = x(x-1)(x-z)$ . Then by Fuchs and Manin [20], there is a (unique up to a multiplicative constant) compatible system of  $\delta$ -functions of order 2,  $\psi : E(\mathcal{R}) \rightarrow \mathcal{R}$ , that are group homomorphisms, where  $\mathbb{C}(z) \subset \mathcal{R}$ . If  $P = (X, Y) \in E(\mathcal{R})$  is a point of  $E$  with  $X, Y \in \mathcal{R}$  (so  $x(P) = X$ ,  $y(P) = Y$ ) then

$$\psi(P) = z(1-z) \left( z(1-z)\delta_z^2 + (1-2z)\delta_z - \frac{1}{4} \right) \int_{\infty}^{(X,Y)} \frac{dx}{y} = F(X, Y, \delta_z X, \delta_z^2 X),$$

where  $F$  is a rational function with coefficients in  $\mathbb{Q}(z)$  in 4 variables. (Manin’s original notation for  $\psi$  above is  $\mu$ ; cf. [20].) The expression involving the integral is well defined because the linear differential operator in front of the integral annihilates any function of  $z$  of the form  $\int_{\gamma} \frac{dx}{y}$  where  $\gamma$  is an integral 1-cycle. Functions of the form  $\int_{\gamma} \frac{dx}{y}$  are called in [22] *periods-functions*; the various values of periods-functions at special  $z$ s are then referred to as *numerical periods*, or simply *periods*. According to [21] the Painlevé VI equation(s) are then of the form

$$\psi(P) = \sum_{i=0}^3 \lambda_i \cdot y(P + P_i) \tag{2.11}$$

where  $P \in E(\mathcal{R})$ ,  $\lambda_i \in \mathbb{C}$ ,  $P_0 = 0$ ,  $\{P_1, P_2, P_3\}$  are the points of  $E(\mathcal{R})$  of order 2, and  $P + P_i$  is the sum in the group law of the elliptic curve. The solutions to 2.11, when transcendental, are the famous *Painlevé (VI) transcendents* and their consideration was motivated, in the work of Painlevé, by his search of “new” transcendental functions, solving differential equations, and having “no movable singularity” (by which it is roughly meant that the non-algebraic singularities of the solutions do not depend on the integration constants). There is a vast literature on Painlevé equations which seem to pop up in a number of basic, but apparently unrelated, mathematical (and physical) contexts; in particular these equations have a remarkable “Hamiltonian structure”. Now, an arithmetic analogue of Manin’s  $\psi$  was introduced in [5] where it was proved that, for any elliptic curve  $E$  over  $R$ , there exists a non-zero  $\delta$ -function  $\psi_p : E(R) \rightarrow R$  of order 2 which is a group homomorphism; this  $\psi_p$  is actually unique up to a multiplicative constant, provided  $E$  is not a *canonical lift* (in particular if  $E$  is without complex multiplication). Then the equation 2.11 makes sense in the arithmetic case by replacing  $\psi$  with  $\psi_p$ , taking  $P \in E(R)$ , and  $\lambda_i \in R$ ; more generally one can consider, as analogue of 2.11, the equation

$$\psi_p(P) = \sum_{i=0}^3 \lambda_i \cdot y(P + P_i)^{\phi_p^\nu} \tag{2.12}$$

where  $\nu \in \mathbb{Z}_{\geq 0}$ . For  $\nu = 1$  the equation 2.12 was shown in [11] to possess a structure reminiscent of Hamiltonian structure; on the other hand the solutions of 2.12 can be viewed as arithmetic analogues of the Painlevé transcendents, and could be referred to as *Painlevé numbers*. A question immediately invites itself, although, as stated, it is definitely too vague: do Painlevé numbers have a property that can be viewed as an arithmetic analogue of “no movable singularity”? Another question can be asked, however, that is quite precise: what are the algebraic relations among solutions of 2.11 in the arithmetic case? (In the classical case of differential equations there is ample work on the corresponding question, both classical and modern, cf. [23] and the bibliography therein.) The degenerate case  $\lambda_0 = \dots = \lambda_3 = 0$  is worth examining separately. In this case it is known (a special case of Manin’s theorem of the kernel [20]) that if  $\mathcal{R}$  is a field algebraic over  $\mathbb{C}(t)$  then any solution  $P$  to 2.11 (i.e. any  $P \in E(\mathcal{R})$  with  $\psi(P) = 0$ ) is a torsion point of  $E(\mathcal{R})$ . This, of course, fails if  $\mathcal{R}$  is not assumed algebraic over  $\mathbb{C}(t)$ . By the way, in this general case, for  $P = (X, Y)$  with  $\psi(P) = 0$ , the (multivalued) integral  $\int_{\infty}^P \frac{dx}{y}$ , as a function of  $z$ , is (for each of its branches) a  $\mathbb{C}$ -linear combination of periods-functions, so

$$P = \pi \left( a_1 \cdot \int_{\gamma_1} \frac{dx}{y} + a_2 \cdot \int_{\gamma_2} \frac{dx}{y} \right), \tag{2.13}$$

where  $\pi$  is the uniformization map for our family of elliptic curves (the inverse of the multivalued Abel-Jacobi map  $Q \mapsto \int_{\infty}^Q \frac{dx}{y}$ ),  $a_1, a_2 \in \mathbb{C}$  and  $\gamma_1, \gamma_2$  a basis for the integral homology. Of course  $\pi$  is defined by elliptic functions. Non-torsion  $P$ s as above always exist and are transcendental over  $\mathbb{C}(z)$  so one can refer to such a  $P$  as a (degenerate) Painlevé transcendent. One can also call such a  $P$  a *period-point* of our elliptic curve (family) since it is the composition of the uniformization map with a complex combination of periods.

There are similar results for 2.12 as follows. First it was proved in [5] that, in case  $E$  has ordinary reduction mod  $p$ , the set of solutions to  $\psi_p(P) = 0$  (which is, of course, a subgroup of  $E(R)$ ) contains the group

$$\bigcap_{n=1}^{\infty} p^n E(R) \tag{2.14}$$

as a subgroup of finite index (whose index can be computed explicitly, cf. loc. cit.) On the other hand upon choosing a basis  $(\bar{P}_n)$  of the (physical) Tate module of  $E(k)$  (where  $P_n \in E(R)$ , the image  $\bar{P}_n \in E(k)$  of  $P_n$  generates  $E(k)[p^n]$ , and  $p\bar{P}_n = \bar{P}_{n-1}$ ) the group 2.14 contains the element

$$q(E) = \lim p^n P_n \tag{2.15}$$

which can be canonically identified (via the identification of the formal group of  $E$  with the formal group of  $\mathbb{G}_m$ ) with the Serre-Tate parameter of  $E$ . Finally it is easy to check [6] that, if  $E$  is defined over  $\mathbb{Z}_p$ , then  $q(E)$  is transcendental over  $\mathbb{Z}_p$  and the only solutions to  $\psi_p(P) = 0$  with  $P \in E(\mathbb{Z}_p^{ur})$  are torsion points. One of the morals to the story is that the Serre-Tate parameter  $q(E)$  can be viewed, in some sense, as a *period-point* and plays the role of a (degenerate) Painlevé number; here by *degenerate* we mean “corresponding to the degenerate case” when the  $\lambda$ s are 0. For the “non-degenerate case” the Painlevé numbers should then be viewed as deformations of the Serre-Tate parameter, and hence of the “period-point” of  $E$ .

### 2.3 Modular functions

One final example we shall discuss here arises in relation to modular forms. First we recall the classical (differential equation) picture; cf. [19, 4, 15]. We begin by recalling from [4] that there exists a rational function  $\rho$  of one variable with coefficients in  $\mathbb{Q}$  (which is entirely explicit) such that, for any  $\beta \in \mathcal{R} \setminus \mathbb{C}$ , the equation

$$\frac{2(\delta_z u)(\delta_z^3 u) - 3(\delta_z^2 u)^2}{4(\delta_z u)^2} + (\delta_z u)^2 \cdot \rho(u) = \beta \tag{2.16}$$

is “constant on isogeny classes” in the following sense: if  $u \in \mathcal{R} \setminus \mathbb{C}$ , is a solution to 2.16 then any  $u^* \in \mathcal{R} \setminus \mathbb{C}$  in the same isogeny class as  $u$  is also a solution to 2.16. Here two elements  $u_1, u_2 \in \mathcal{R}$  are said to be in the same isogeny class if the two elliptic curves over  $\mathcal{R}$  with  $j$ -invariants  $u_1$  and  $u_2$  respectively are isogenous. (Of course, the first term in 2.16 is the classical Schwarzian.) For work on the algebraic relations among the solutions of 2.16, leading to analogues for the  $j$  function of the Ax-Lindemann-Weierstrass theorem, we refer to [24, 25, 15]; the solutions of 2.16 one looks at are of the form

$$j \left( \frac{a\tau(z) + b}{c\tau(z) + d} \right) \tag{2.17}$$

with  $\tau(z)$  an algebraic function, and  $a, b, c, d \in \mathbb{C}$ ; 2.17 should be viewed as an analogue of 2.1 and 2.13 and hence as a “period-point”, as it is the composition of the uniformization map  $j$  with a complex Möbius transformation applied to a “periods function”  $\tau(z)$  (of some elliptic curve). So the function  $j$  in 2.17 is analogous to the function  $\pi$  in 2.13 and to the function  $\exp$  in 2.1. The constants  $a, b, c, d$  in 2.17 are analogues of the constants  $a_1, a_2$  in 2.13 and are also analogues of the constants appearing as coefficients of  $\beta$  in 2.1, if  $\beta$  in 2.1 is, say, a polynomial in  $z$ . Finally the function  $\tau(z)$  in 2.17 is analogous to the integrals in 2.13 and to the integral in 2.1.

The above story has an arithmetic analogue as follows; cf. [7, 3, 8]. Let  $X_1(N)$  be the complete modular curve over  $R$  of level  $N > 4$  and let  $L_{X_1(N)}$  be the line bundle on  $X_1(N)$  with the property that the sections of its various powers are the classical modular forms on  $\Gamma_1(N)$  of various weights. Let  $Y_1(N)$  be  $X_1(N)$  from which one removes the cusps. Let  $L_{Y_1(N)} \rightarrow Y_1(N)$  be the restriction of the above line bundle and let  $V$  be  $L_{Y_1(N)}$  with the zero section removed. The  $R$ -points of  $V$  correspond then to certain Weierstrass cubics equipped with level structure. Let  $M^r$  be the ring of  $\delta$ -functions of order  $r$  on  $V$ . For  $w \in \mathbb{Z}[\phi_p] \subset \text{End}_{\mathbb{Z}\text{-mod}}(R)$  we denote by  $M^r(w)$  the space of all members of  $M^r$  that have “weight”  $w$  (i.e. on which  $\mathbb{G}_m$  acts via the character  $\lambda \mapsto \lambda^w$ ); the elements of  $M^r(w)$  are called  $\delta$ -modular forms of order  $r$  and weight  $w$ . The theory in [8] provides some remarkable  $\delta$ -modular forms  $f_p^r \in M^r(-1 - \phi^r)$ ,  $r \geq 1$ , which have a property (called *isogeny covariance*) that is stronger than the property of being Hecke eigenforms; cf. [7, 8]. This property has no analogue in the classical theory and we refer to loc.cit. for its definition. Then, for any  $\beta \in R$ , one can consider the arithmetic differential equation of order 3 of the following form

$$\frac{f_p^2(P)^{1+\phi_p}}{f_p^1(P)^{1+\phi_p^2}} = \beta, \tag{2.18}$$

with solutions  $P \in V(R)$ . These equations are “constant on isogeny classes”: if  $P$  is a solution to 2.18 (with the denominator in 2.18 invertible) then any  $P^* \in V(R)$  in the same isogeny class as  $P$  is also a solution to 2.18; here two points of  $V$  are said to be in the same isogeny class if and only if there is an isogeny between the Weierstrass cubics representing the two points which is compatible with the standard 1-forms on the cubics (but not necessarily with the level structures). Clearly 2.18 can be viewed as an analogue of 2.16. Note that both 2.16 and 2.18 have order 3 which seems to be expected, since the dimension of  $SL_2$  is 3 and  $SL_2$  is the group behind the isogeny equivalence relation. It is therefore all the more surprising to see, as we shall explain in what follows, that there is an order 2 equation that is analogous to 2.16. Indeed, let  $V_{ord}, M_{ord}(w)$  be the spaces obtained by replacing, everywhere in the construction above, the curve  $Y_1(N)$  with its ordinary locus (i.e. the locus where the Eisenstein series  $E_{p-1}$  is invertible). Then an entirely new actor joins the scene: a remarkable isogeny covariant  $\delta$ -modular form of order 1 and weight  $\phi - 1$ , introduced in [3], and denoted by  $f_p^\partial \in M_{ord}^1(\phi - 1)$ . One can then consider, for any  $\beta \in R$ , the arithmetic differential equation of order 2

$$f_p^1(P)^{\phi_p - 1} \cdot f_p^\partial(P)^{\phi_p + 1} = \alpha, \tag{2.19}$$

with solutions  $P \in V_{ord}(R)$ . This equation is, again, “constant on isogeny classes”: if  $P$  is one of its solutions (with  $E_{p-1}(P)$  invertible) then any  $P^* \in V_{ord}(R)$  in the same isogeny class as  $P$

is also one of its solutions. In fact 2.18 is a consequence of 2.19 for  $\beta = \alpha + p(1 + \alpha^{1-\phi}) + p^2\alpha^{-\phi^2}$ . The fact that 2.19 has order 2 rather than 3 may seem somewhat mysterious but here is one way to think about this phenomenon. It is a fact (known to Mahler [19], see also [4], p.37) that there is no order 2 algebraic differential equation that is “constant on isogeny classes”. This is equivalent to the fact that if  $j$  is the classical holomorphic  $j$ -function,  $j = j(z)$ , defined on the upper half plane then  $j, \delta_z j, \delta_z^2 j$  are algebraically independent over  $\mathbb{C}$ . Now these series belong to  $\mathbb{Z}((q)) = \mathbb{Z}[[q]][q^{-1}]$ ,  $q = \exp(2\pi iz)$ . So setting  $\theta = q \frac{d}{dq}$  the series  $j, \theta j, \theta^2 j$  are algebraically independent over  $\mathbb{Q}$  as elements of  $\mathbb{Z}((q))$ . However it turns out that the images of the series  $j, \theta j$  in  $\mathbb{F}_p((q))$  are algebraically dependent over  $\mathbb{F}_p$ ; cf. [18]; so  $j(q) \bmod p$  satisfies an algebraic differential equation of order 1! This “drop in order” from 3 to 1 is a remarkable phenomenon in characteristic  $p$ . On the other hand we have a “drop in order” from 3 to 2 between 2.16 and 2.19 in the framework of  $\delta$ -modular forms and it is possible to prove that, in some precise sense, no “drop in order” from 3 to 1 exists in this framework. So the drop from 3 to 2 can be viewed as a partial lift to characteristic zero, in  $\delta$ -geometry, of the drop from 3 to 1 that exists in characteristic  $p$ . The existence of such a lift is surprising but it is just one instance of a more general phenomenon where characteristic  $p$  algebro-geometric objects that do not lift to characteristic zero in algebraic geometry *do* lift to characteristic zero in  $\delta$ -geometry; cf. [8] for a series of examples of this.

By analogy with Pila’s results [25] it would be interesting to prove that there are no algebraic relations among the solutions of 2.18 (or 2.19) except those given by “isogeny”. The simplest case of this would be the following conjecture (which pertains to 2.19). *Let  $P, P^* \in V_{\text{ord}}(R)$  be two points corresponding to Weierstrass elliptic curves with coefficients in a number field in which  $p$  splits completely. Assume  $f^\partial(P) = f^\partial(P^*)$ . Then the two elliptic curves are isogenous.*

Note that there is a cocompact analogue of both 2.16 and 2.18, 2.19 (cf. [27] and [8] respectively) with transcendence results in the functional case [27].

### 3 Arithmetic differential Galois groups and periods

Galois groups are a measure of the relations among solutions of equations. Galois’ original work is about algebraic equations and algebraic relations among their roots. Picard-Vessiot theory (or more generally Kolchin theory [16]) is about linear differential equations (respectively differential equations arising from Maurer-Cartan connections on algebraic groups) and about algebraic relations among their solutions. More generally [17] considers differential equations with parameters and differential algebraic relations among solutions; cf. also [12] for the case of linear equations. The same idea can be applied, in certain cases, to arithmetic differential equations and the  $\delta$ -algebraic relations among their solutions; this can be done, e.g., for equations of the form 2.9 (cf. [10]), or 2.7 (cf. [8]), or 2.12, at least in the degenerate case when the  $\lambda$ s are 0 (cf. [8]). No general Galois theory of arithmetic differential equations is yet available. However, if such a theory can be developed and, at the same time, various “ $p$ -adic periods” appearing in algebraic geometry can be shown to satisfy “nice” arithmetic differential equations, then it is conceivable that one could systematically understand relations among “ $p$ -adic periods” (and possibly motivic Galois groups [1]) through a Galois theory of arithmetic differential equations. The possibility suggested above is compatible with suggestions made by Manin in [22]. Whether or not the “ $p$ -adic periods” referred to above should be related to the

ones appearing in the standard comparison isomorphisms [1] is not clear at this time. Let us close by making some comments on this issue, partly inspired by comments in [22]. In the functional case 2.2, 2.13, 2.17, the solutions of our differential equations, which we would like to think of as *period points* on various schemes, are compositions of “uniformizing functions”  $\exp, \pi, j$  with complex linear (respectively “Möbius”) combinations of functions that have the flavor of *periods functions*. So the period points are not really periods functions but rather images of such via uniformization maps. Such uniformization maps *do not exist a priori* in the  $p$ -adic situation (e.g. for elliptic curves no uniformization is known for the good reduction case!) Therefore the solutions to 2.4, 2.12, 2.18 should be viewed as analogues of *period points* and only indirectly as analogues of  *$p$ -adic periods* in the motivic setting [1]. As for the “motivic periods” it is worth recalling from [1] the general philosophy as follows. Say that  $X$  is a smooth projective variety over a field  $k$  of characteristic 0. For  $k \subset \mathbb{C}$  one has a deRham versus Betti comparison isomorphism  $H_{dR}(X) \otimes_k \mathbb{C} \simeq H_{Betti}(X) \otimes_{\mathbb{Q}} \mathbb{C}$ , due to Grothendieck, where  $H_{dR}$  is the algebraic deRham cohomology of  $X/k$  and  $H_{Betti}$  is the Betti cohomology with  $\mathbb{Q}$ -coefficients; this isomorphism, expressed in bases of  $H_{dR}(X)$  and  $H_{Betti}(X)$  provides a complex matrix whose entries are called the *complex periods* of  $X$ . By the way one also has in this case the  $p$ -adic étale versus Betti comparison isomorphism  $H_{et}(X) \simeq H_{Betti}(X) \otimes_{\mathbb{Q}} \mathbb{Q}_p$ , due to Grothendieck and Artin. Assume until further notice that  $k$  is a number field. For any  $k$ -subvariety  $Z$  of any power  $X^n$  the comparison isomorphism for  $X^n$  sends the class of  $Z$  into the corresponding class of  $Z$ ; via Künneth, this induces an algebraic relation over  $k$  between the complex periods. Grothendieck’s period conjecture says roughly that *all* the relations among periods “come from”  $Z$ s as above. Also one defines the *motivic Galois group* of  $X$  as, roughly, the algebraic  $\mathbb{Q}$ -subgroup of  $GL(H_{Betti}(X))$  that fixes all the classes of  $Z$ s as above (viewed, via Künneth, as tensors on  $H_{Betti}(X)$ ). In the  $p$ -adic case one has a similar picture. Indeed for  $k$  a finite extension of  $\mathbb{Q}_p$  one has the deRham versus  $p$ -adic étale comparison isomorphism  $H_{dR}(X) \otimes_k B_{dR} \simeq H_{et}(X) \otimes_{\mathbb{Q}_p} B_{dR}$ , due to Faltings, where  $B_{dR}$  is Fontaine’s field of  $p$ -adic periods [14]. The latter yields, again, period matrices with entries in  $B_{dR}$ ; these  *$p$ -adic periods*, lying in  $B_{dR}$ , are a priori rather different from the *period points*, referred to above, which are  $R$ -points (hence with coordinates lying in  $R$ ) of certain  $R$ -schemes (the hyperbola  $H = \mathbb{G}_m$  over  $R$ , elliptic curves  $E$  over  $R$ ,  $\mathbb{G}_m$ -bundles  $V$  over modular curves over  $R$ , etc.) A link between these two types of periods would allow one to consider arithmetic differential equations in the context of periods lying in  $B_{dR}$ . We end by recalling the definition of  $B_{dR}$  [14] and the  $p$ -adic periods in [13]. Assume, for simplicity, that  $k$  is unramified over  $\mathbb{Q}_p$ . One lets  $\mathcal{O}$  be the ring of integers of  $\mathbb{C}_p := \widehat{\mathbb{Q}_p}$ , one lets  $R_{\mathcal{O}}$  be the projective limit of  $\mathcal{O}/p\mathcal{O} \leftarrow \mathcal{O}/p^2\mathcal{O} \leftarrow \dots$  where the arrows are the  $p$ -power Frobenius, one considers the canonical map  $\theta : W(R_{\mathcal{O}}) \rightarrow \mathcal{O}$  (where  $W$  stands for the  $p$ -typical Witt functor), one lets  $A_{inf}$  be the completion of  $W(R_{\mathcal{O}})$  with respect to  $(p, Ker(\theta))$ , one lets  $\theta_k : A_{inf}[1/p] \rightarrow \mathbb{C}_p$  be the induced map, one lets  $B_{dR}^+$  be the completion of  $A_{inf}[1/p]$  with respect to  $Ker(\theta_k)$ , which is a complete discrete valuation ring with residue field  $\mathbb{C}_p$ , and one lets  $B_{dR} = Frac(B_{dR}^+)$ . Uniformizers in  $B_{dR}$  can be constructed from any basis of the Tate module of  $\mathbb{G}_m(\mathbb{C}_p)$  as follows. Let  $\epsilon_n \in \mathbb{C}_p$  be primitive  $p^n$ -roots of 1,  $\epsilon_n^p = \epsilon_{n-1}$ , and let  $\tilde{\epsilon}_n \in A_{inf}$  be lifts of  $\epsilon_n$ ; then  $\tilde{\epsilon} = \lim \tilde{\epsilon}_n^{p^n}$  exists in  $A_{inf}$  and  $\log_p \tilde{\epsilon} \in B_{dR}^+$  is a uniformizer of  $B_{dR}^+$ ; note that the limit  $\tilde{\epsilon}$  is reminiscent of 2.15. Furthermore, for any abelian variety  $A$  over  $k$ , any 1-form  $\omega$  on  $A$  and any element  $\gamma$  in the Tate module of  $A(\mathbb{C}_p)$  there is, by work of Colmez [13], a well defined period  $\int_{\gamma} \omega = \lim p^n I_n \in B_{dR}^+$ , where  $I_n$  is a certain integral

on  $A(B_{dR})$ . This construction is, again, reminiscent of 2.15; note however that the image of  $\int_{\gamma} \omega$  in  $\mathbb{C}_p$  turns out to be 0 so (for  $E$  coming from an integral model of  $A/k$ ) this image does not coincide with  $q(E) \in R \subset \mathbb{C}_p$ ; indeed  $q(E) \neq 0$  for  $E$  without complex multiplication.

## References

- [1] Y. ANDRÉ, *Galois theory, motives and transcendental numbers*, arXiv:0805.2569.
- [2] J. AX, *On Schanuel's conjecture*, Annals of Math. 93 (1971), 252-268.
- [3] M. BARCAU, *Isogeny covariant differential modular forms and the space of elliptic curves up to isogeny*, Compositio Math., 137 (2003), 237-273.
- [4] A. BUIUM, *Geometry of differential polynomial functions III: moduli spaces*, Amer J. Math. 117 (1995), 1-73.
- [5] A. BUIUM, *Differential characters of Abelian varieties over  $p$ -adic fields*, Invent. Math., 122 (1995), pp. 309-340.
- [6] A. BUIUM, *Differential characters and characteristic polynomial of Frobenius*, Crelle J. 485 (1997), 209-219.
- [7] A. BUIUM, *Differential modular forms*, J. reine angew. Math., 520, (2000), pp. 95-167.
- [8] A. BUIUM, *Arithmetic Differential Equations*, Math. Surveys and Monographs, 118, American Mathematical Society, Providence, RI, 2005. xxxii+310 pp.
- [9] A. BUIUM, T. DUPUY, *Arithmetic differential equations on  $GL_n$ , II: arithmetic Lie-Cartan theory*, arXiv:1308.0744.
- [10] A. BUIUM, T. DUPUY, *Arithmetic differential equations on  $GL_n$ , III: Galois groups*, arXiv:1308.0747.
- [11] A. BUIUM, YU. I. MANIN, *Arithmetic differential equations of Painlevé VI type*, arXiv:1307.3841
- [12] P. CASSIDY, M. SINGER, *Galois theory of parametrized differential equations and linear differential algebraic group*, IRMA Lectures in Mathematics and Theoretical Physics 9 (2007), 113-157.
- [13] P. COLMEZ, *Intégration sur les variétés  $p$ -adiques*, Astérisque 248, SMF, 1998.
- [14] J-M. FONTAINE, *Le corps des périodes  $p$ -adiques*, Astérisque 223 (1994), 59-111.
- [15] J. FREITAG, T. SCANLON, *Strong minimality of the  $j$ -function*, arXiv:1402.4588.
- [16] E.R. KOLCHIN, *Differential algebra and algebraic groups*. Pure and Applied Mathematics, Vol. 54. Academic Press, New York-London, 1973. xviii+446 pp.
- [17] P. LANDESMAN, *Generalized differential Galois theory*, Transactions of the AMS, 360 (2008), 4441-4495.
- [18] S. LANG, *Introduction to modular forms*, Springer, 1976.
- [19] K. MAHLER, *On algebraic differential equations satisfied by automorphic functions*, J. Austral. Math. Soc. 10 (1969), 445-450.
- [20] YU. I. MANIN, *Rational points on algebraic curves over function fields*, Izv. Acad. Nauk USSR, 27 (1963), 1395-1440.
- [21] YU. I. MANIN, *Sixth Painlevé equation, universal elliptic curve, and mirror of  $\mathbb{P}^2$* . In: geometry of Differential Equations, ed. by A. Khovanskii, A. Varchenko, V. Vassiliev. Amer. Math. Soc. Transl. (2), vol. 186 (1998), 131-151. Preprint alg-geom/9605010.

- [22] YU. I. MANIN, *Numbers as functions*, arXiv:1312.5160.
- [23] J. NAGLOO, A. PILLAY, *On the algebraic independence of generic Painleve transcendents*, arXiv:1209.1562
- [24] J. PILA, *O-minimality and the Andre-Oort conjecture for  $\mathbb{C}^n$* , Annals Math. 173 (2011), 1779-1840.
- [25] J. PILA, *Modular Ax-Lindemann-Weierstrass with derivatives*, Notre Dame J. Formal Logic 54 (2013), 553-565.
- [26] M. SINGER, M. VAN DER PUT, *Galois theory of difference equations*, LNM, Springer 1997.
- [27] E. ULLMO, *The Hyperbolic Ax-Lindemann-Weierstrass conjecture*, arXiv:1307.3965 [math.AG].

Received: 15.08.2014

Accepted: 1.12.2014

University of New Mexico  
Albuquerque, NM 87131  
E-mail: buium@math.unm.edu