REVIEW OF KIRAN KEDLAYA’S “p-ADIC DIFFERENTIAL EQUATIONS”

LAURENT BERGER

1. p-ADIC DIFFERENTIAL EQUATIONS

If \( p \) is a prime number, then we have the \( p \)-adic norm \( |·|_p \) on the field \( \mathbb{Q} \) of rational numbers. The completion of \( \mathbb{Q} \) for the metric arising from this norm is the field of \( p \)-adic numbers \( \mathbb{Q}_p \). This construction is analogous to the construction of the real numbers \( \mathbb{R} \), as the completion of \( \mathbb{Q} \) for the usual norm. Hence, one can do analysis in \( \mathbb{Q}_p \) as one can in \( \mathbb{R} \). In particular, one can talk about derivatives and convergent power series. For example, the fact that the \( p \)-adic valuation of \( n! \) is asymptotically equal to \( n/(p - 1) \) implies that the power series \( \exp(t) = \sum_{n\geq 0} t^n/n! \) has a finite \( p \)-adic radius of convergence, equal to \( p^{-1/(p-1)} \). Just as power series in the usual case work better if one sees them as functions of a complex variable, it is convenient to view \( p \)-adic power series as functions on \( \mathbb{C}_p \), the \( p \)-adic completion of the algebraic closure of \( \mathbb{Q}_p \). The field \( \mathbb{C}_p \) is the \( p \)-adic analogue of the complex numbers. In the sequel, a \( p \)-adic field is any \( p \)-adically complete subfield of \( \mathbb{C}_p \).

A \( p \)-adic differential equation is a differential equation, in which the functions involved are \( p \)-adic valued functions of a \( p \)-adic variable. For example, the equation \( y'(t) = y(t) \) admits as a solution \( y(t) = y(0) \cdot \exp(t) \). The power series defining \( \exp(t) \) only converges on the disk \( \{ z \in \mathbb{C}_p, |z|_p < p^{-1/(p-1)} \} \), a fact not apparent on the simple equation \( y' = y \). Hence one of the first concerns of the theory of \( p \)-adic differential equations is the determination of the radii of convergence of various power series.

One of the earliest mentions of \( p \)-adic differential equations in the literature is Elisabeth Lutz’ theorem of 1937 (théorème IV of [Lut37]) to the effect that if one considers a system of equations

\[
y'_i(t) = F_i(t, y_1, \ldots, y_n),
\]

where \( i = 1, \ldots, n \) and the \( F_i \)'s are power series with coefficients in a \( p \)-adic field, and nonzero radii of convergence, then this system admits a system of solutions \( \{ y_i(t) \}_{i=1,\ldots,n} \) where the \( y_i(t) \) are power series, themselves having nonzero radii of convergence. She
then applies her result to the equation
\[ z'(t) = \sqrt{1 - az^4 - bz^6} = 1 - \frac{a}{2}z^4 - \frac{b}{2}z^6 \pm \cdots, \]
where \( y^2 = x^3 - ax - b \) is the equation of an elliptic curve, in order to define \( p \)-adic elliptic functions.

Because \( \mathbb{C}_p \) is a totally disconnected topological space, one cannot use “continuation” in order to study differential equations; for example, any locally constant function on \( \mathbb{C}_p \) is \( C^\infty \) and is a solution of the equation \( y' = 0 \). Because of this, one usually considers solutions which are power series, converging on certain prescribed domains. In addition, one only studies linear differential equations, unlike those in Lutz’ theorem. A rather general setting is then that \( A \) is some ring of power series with coefficients in a \( p \)-adic field (for instance, one could take \( A \) to be the set of power series \( f(X) \in Q_p[[X]] \) which converge on the disk \( \{ z \in \mathbb{C}_p, |z|_p < 1 \} \), or also the field \( Q_p((X)) = Q_p[[X]][1/X] \); in the latter case, there is no convergence condition) and one considers the equation
\[ y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_1y' + a_0y = 0. \]

The goal is to find solutions of the equation, that is functions \( y \) satisfying the equation and belonging to \( A \), or to some extension of \( A \). For example, the equation \( y' = y \) admits \( C \cdot \exp(X) \) as a solution, as we have seen. The equation \( y' = y/2X \) admits \( y = \sqrt{X} \) as a solution, so one needs to pass to an algebraic extension of \( Q_p((X)) \) in order to solve it. More generally, the equation \( y' = s/X \cdot y \) admits \( y = X^s \) as a solution, and if \( s \notin Q \), then it is not obvious how to give a precise meaning to \( X^s \). The number \( s \) which appears here is a special case of what are called the exponents of a differential equation.

2. The \( p \)-adic Monodromy Theorem

Rather than working with differential equations, it is more convenient to work with differential modules, that is free \( A \)-modules \( M \) of finite rank which are endowed with an operator \( D : M \to M \) satisfying the Leibnitz rule \( D(am) = a'm + aD(m) \). The passage from a differential equation
\[ y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_1y' + a_0y = 0 \]

to a differential module is straightforward, by setting \( M = Ae_0 \oplus Ae_1 \oplus \cdots \oplus Ae_{n-1} \) with \( De_0 = a_0e_{n-1}, De_1 = -e_0 + a_1e_{n-1}, \ldots, De_{n-1} = -e_{n-2} + a_{n-1}e_{n-1} \). The operator \( D \) on \( M \) is determined by this and by the Leibnitz rule. The solutions of the differential equation then correspond naturally to elements \( m \in M \) such that \( Dm = 0 \), the so-called horizontal sections of \( M \).
Consider first the case when the ring $A$ of power series involves no convergence condition, so that we are in the so-called formal setting: take $K$ to be a field of characteristic 0 (not necessarily $p$-adic) and let $A$ be the field $K((X)) = K[X][1/X]$.

The theorem of Turrittin (see [Tur55]) says that if $M$ is a differential module of dimension $d$ over $K((X))$, then there exists a finite extension $L$ of $K$ such that if one sets $Y = X^{1/d!}$, then $L((Y)) \otimes_{K((X))} M$ contains a chain of submodules

$$0 = M_0 \subset M_1 \subset \cdots \subset M_d = L((Y)) \otimes_{K((X))} M,$$

where each $M_i$ is a differential module over $L((Y))$ and $M_{i+1}/M_i$ is of dimension 1. In other words, a linear differential equation of degree $d$ can be reduced to $d$ inhomogeneous linear differential equations of degree 1, after extending the scalars and performing a change of variable.

The goal of a lot of the work which has gone into the theory of $p$-adic differential equations in the last 50 years or so has been to state and prove an analogue of Turrittin’s theorem when $K$ is a $p$-adic field and $A$ is a ring of power series with coefficients in $K$, satisfying some convergence condition. This $p$-adic analogue of Turrittin’s theorem is known as the $p$-adic monodromy theorem; it can be seen as a $p$-adic analogue of the classical monodromy theorems (see for instance [Meb03]). Let $K$ be a finite extension of $\mathbb{Q}_p$, and let $\mathcal{R}$ be the Robba ring with coefficients in $K$, that is the set of power series $f(X) = \sum_{n=-\infty}^{+\infty} a_n X^n$ where $a_n \in K$ and where $f(X)$ converges on the annulus $r(f) < |X|_p < 1$, for some radius $r(f)$ depending on $f$.

The $p$-adic monodromy theorem states that if $M$ is a differential module over $\mathcal{R}$, which satisfies a technical condition on a certain set of exponents, then there exists a finite extension $\mathcal{R}'$ of $\mathcal{R}$ such that $\mathcal{R}' \otimes_{\mathcal{R}} M$ is an iterated extension of objects of rank 1, as in Turrittin’s theorem. If $M$ arises from a geometrical situation, then there is usually an extra structure on $M$, namely a Frobenius map compatible with the differential operator; the exponents alluded to above are then all rational numbers, and in this case one can find $\mathcal{R}'$ such that $\mathcal{R}' \otimes_{\mathcal{R}} M$ is an iterated extension of objects of rank 1, all of which actually admit a horizontal section. One then says that $M$ is quasi unipotent.

3. Why $p$-adic differential equations?

One may attach to certain algebraic varieties their de Rham cohomology. If these varieties live in a family, then the variation of cohomology in the family gives rise to a differential structure called the Gauss-Manin connection (a generalization of the Picard-Fuchs equations). This construction motivated the study of algebraic linear differential equations. Thanks to some results of John Tate, Bernard Dwork noticed that these differential equations had interesting $p$-adic properties, in connection with the study of
zeta functions of varieties over finite fields and exponential sums, and started the subject of $p$-adic differential equations (see for example [Dwo82]). As the construction of $p$-adic cohomologies progressed, so did the demand for structure results on $p$-adic differential equations. Such results were provided by Bernard Dwork and Philippe Robba, and then by their school, notably Gilles Christol and Zoghman Mebkhout.

The $p$-adic monodromy theorem was conjectured by Richard Crew and shortly thereafter proved independently and simultaneously by Yves André [And02a], Kiran Kedlaya [Ked04] and Zoghman Mebkhout [Meb02], in 2001 (we recommend reading Yves André’s treatment of a special case in [And02b]). Note that, relying on suitable generalizations of the $p$-adic monodromy theorem, Kiran Kedlaya has managed to give a purely $p$-adic proof of the Weil conjectures (see [Ked06]).

4. The book under review

There are currently few books in this area, and the book under review is the first which is meant to be a comprehensive introduction to the subject. Gilles Christol is currently writing another one (“Le théorème de Turrittin $p$-adique”), and several surveys already exist (recent ones include: the course notes [CM02] by Gilles Christol and Zoghman Mebkhout, [Chi11] by Bruno Chiarellotto, [Ked05] by Kiran Kedlaya and [Meb03] by Zoghman Mebkhout).

The book under review grew out of a course given by the author at MIT in 2007. There is an informative introduction, explaining how $p$-adic differential equations arose in geometry, notably thanks to the work of Dwork on zeta functions of varieties over finite fields. Each subsequent chapter contains its own brief introduction, and ends with afternotes and exercises. The book covers all of the required material in order to state and then prove the $p$-adic monodromy theorem. The topics covered include some background material on $p$-adic analysis, Newton polygons and differential algebra. After that, the study of $p$-adic differential equations starts in earnest, in particular the precise study of radii of convergence, the so-called transfer theorems, the use of Frobenius pullbacks and pushforwards, and $p$-adic exponents. Along the way, Frobenius modules over the Robba ring are discussed, a subject largely due to the author himself. A complete proof of the $p$-adic monodromy theorem is then given, following Mebkhout’s approach. The last part of the book contains a discussion of the applications of $p$-adic differential equations in arithmetic geometry: Picard-Fuchs modules, rigid cohomology and $p$-adic Hodge theory.

Written by a leading expert in the subject, this book is both a textbook on a topic of current interest in number theory, and a great overview of the techniques and of the striking applications of the theory of $p$-adic differential equations.
References


UMPA, ENS de Lyon, UMR 5669 du CNRS, Universit´e de Lyon
E-mail address: laurent.berger@ens-lyon.fr