p-adic structure of integral points

Oberseminar Bielefeld–Hannover–Paderborn

Summer 2011

Introduction

Over the course of the last decade or so, Minhyong Kim has developed a new approach to proving Diophantine finiteness theorems. Kim's theory, while still perhaps at an early stage of development, provides new insight into the structure of integral points. Following Kim, we consider a number field F, a finite set S of primes, and a hyperbolic curve X over the ring R of S-integers of F. We will pay particular attention on the case $X = \mathbb{P}^1_{\mathbb{Z}[S^{-1}]} \setminus \{0, 1, \infty\}$. Let $\mathfrak{p}$ be a prime of F not in S, let $F_\mathfrak{p}$ denote the local field at $\mathfrak{p}$ and let $Y(F_\mathfrak{p})$ denote the set of $F_\mathfrak{p}$-points of X whose reduction modulo $\mathfrak{p}$ lies in $X_\mathfrak{p}$. R-points of X specialize to points of $Y(F_\mathfrak{p})$, so there is a map

$$X(R) \to Y(F_\mathfrak{p})\,.$$

Kim shows that under certain conditions on X (but conjecturally under no conditions on X), the equations (and inequations) defining $X(R)$ imply certain transcendental analytic equations on $Y(F_\mathfrak{p})$.

Central to Kim's theory is the unipotent fundamental group introduced by Deligne in its various guises. Fix an integral point $x \in X(R)$ (whose existence we now assume). Consideration of the category of unipotent vector bundles with integrable connection on $X_{F_\mathfrak{p}}$ gives rise to a unipotent $F_\mathfrak{p}$-group U^{dR}, *the de Rham fundamental group at x*, and to a map $Y(F_\mathfrak{p}) \to D^{\mathrm{dR}}(F_\mathfrak{p})$, *the unipotent Albanese map*, to a space which classifies U^{dR} torsors equipped with certain extra structures. This map is highly transcendental, and has dense image. On the other hand, consideration of the category of unipotent lisse $\mathbb{Q}_p$ sheaves on $X_{\bar{F}}$ gives rise to a unipotent $\mathbb{Q}_p$-group $U^{\text{ét}}$, *the unipotent étale fundamental group at x*, equipped with certain extra structures. Points give rise to torsors equipped with corresponding extra structures, and which are, in an appropriate sense, *crystalline*. Kim constructs a variety, *the Selmer variety*, which we will denote for the moment by $D^{\text{ét}}_{\mathrm{f}}$, which classifies such torsors, as well as a map $X(R) \to D^{\text{ét}}_{\mathrm{f}}(\mathbb{Q}_p)$, *the unipotent étale Kummer map*. Nonabelian p-adic Hodge theory then provides a commuting square

$$\begin{tikzcd} X(R) \arrow[r] \arrow[d] & Y(F_\mathfrak{p}) \arrow[d] \\ D^{\text{ét}}_{\mathrm{f}}(\mathbb{Q}_p) \arrow[r, "c"'] & D^{\mathrm{dR}}(F_\mathfrak{p}) \end{tikzcd}$$

Now the conjecture, and the theorem in certain special cases, is that the image of c is contained inside a closed subscheme.

The algebraic functions which cut out this subscheme pull back to transcendental analytic functions on $Y(F_\mathfrak{p})$. In the case $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$, these functions are generated by p-adic analogs of the classical polylogarithms.

Program

1.Introduction: Chabauty's method

The classical Chabauty method. Introduction to main ideas of Kim's nonabelian generalization. [5], [12]

2. The étale fundamental group

Galois categories and fiber functors. Profinite étale fundamental group. Riemann existence theorem and comparison with Betti fundamental group. [15], [14], [17]

3. The unipotent étale fundamental group

Brief review of Tannaka duality [4]. Unipotent groups: exponential map, equivalence between extensions of additive groups and unipotence of representations, Zariski-triviality of fpqc torsors [8], [7]. Structure of unipotent étale fundamental group and its torsors; cohomological classification [12].

4. Review of isocrystals

Tubes and strict neighborhoods [2], convergence and overconvergence [2, 2.2.5, 2.2.13], pullback by Frobenius [2, 2.2.17].

5. Unipotent overconvergent isocrystals and the de Rham fundamental group

This talk is based on [6]. Let X be the complement of a normal crossings divisor D in a smooth scheme $\bar{X}$ over a mixed characteristic dvr A with fraction field K and residue field k. Then a unipotent overconvergent isocrystal on the special fiber X_k extends uniquely to a unipotent vector bundle with an integrable connection on the generic fiber $\bar{X}_K$ with log poles along D_K; this is in fact an equivalence of categories [6, Proposition 2.4.1]. The main goal of this talk is to sketch the proof of this theorem. As an example, the talk might include a description of the De Rham fundamental group of $\mathbb{G}_m$ following [7, §14].

6. Tannakian approach to Coleman integration

Existence of a unique Frobenius-invariant path connecting every two points [3, 3.3]. Besser's definition of Coleman functions [3, §4]. p-adic logarithm [**?**]. Coleman integration [3, Theorem 4.15]. Tangential basepoints in the de Rham setting [7, 15.28–15.36]. Extending Coleman functions across the residue annuli about the punctures [3, proof of Theorem 5.7].

The goal of this talk is to establish the terminology and results summarized in [10, §2.1].

7. p-adic polylogarithms

This first part of this talk is based on [10], and is devoted to explaining how Coleman integration replaces analytic continuation in the definition of p-adic multiple polylogarithms. This should include the following. Definition of multiple polylogarithms in the complex analytic setting as power series and as iterated integrals [10, §1]. Definition of p-adic multiple polylogarithms as iterated Coleman integrals [10, 2.9]. The p-adic KZ equation [10, 3.2], existence of the solution G_0^a with given behavior near the origin [10, 3.3]. A rough outline of the explicit formulas of [10, 3.15] expressing the coefficients of G_0^a in terms of polylogarithms.

The second part of this talk is based on [11]. Let $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$, let $U^{\mathrm{dR}}(X_{\mathbb{Q}_p}, \vec{01})$ denote the unipotent de Rham fundamental group at the tangent vector pointing towards 1 at the origin and let $\mathbb{Q}_p << A, B >>$ denote the noncommutative formal power series ring in the variables A, B. Furusho constructs maps

$$X(\mathbb{Q}_p) \to U^{\mathrm{dR}}(X_{\mathbb{Q}_p}, \vec{01})(\mathbb{Q}_p) \hookrightarrow \mathbb{Q}_p << A, B >> \ .$$

This map sends

$$z \mapsto G_0(A, B)(z)$$

[11, §2.1].

8. The unipotent Albanese map

This talk is based on [13, §1]. This requires the definition of the fundamental torsor P^{dR} [7, §10], and some treatment of the Hodge filtration. The talk should cover the following. U^{dR}/F^0 represents the functor of admissible torsors. Explicit construction of U^{dR} and P^{dR} for X affine. Unipotent Albanese map has dense image [13, Theorem 1].

9. Review of p-adic Hodge theory

Philosophy of rings of periods: comparison between Betti and de Rham cohomology in the complex analytic setting. Overview of construction of $\mathbb{B}_{\mathrm{dR}}$ and $\mathbb{B}_{\mathrm{cris}}$. Definition of de Rham and crystalline representations. Discussion of comparison theorems in the good reduction case. [1]

10. Unipotent p-adic Hodge theory

Let X be a variety over a p-adic field K with good reduction. Let $\mathcal{P}_r^{\mathrm{dR}}$ (resp. $\mathcal{P}_r^{\text{ét}}$) denote the canonical deRham (resp. étale) torsor over $X \times X$ of level of unipotency $\leq r$. In [18] Vologodsky constructs (for $r \leq (p-1)/2$) an equivalence of categories

$$\mathcal{P}_r^{\mathrm{dR}} \otimes_K \mathbb{B}_{\mathrm{dR}} \cong \mathcal{P}_r^{\text{ét}} \otimes_{\mathbb{Q}_p} \mathbb{B}_{\mathrm{dR}}.$$

In [16] Olsson proves a similar result for $\mathbb{B}_{\mathrm{cris}}$. Both results rely on Faltings' theory of *variation of p-adic Hodge structures* [9].

The goal of this talk is to sketch a proof of Vologodsky's theorem ([18], Theorem A). To avoid some technicalities (in particular: log structures) it may be a good idea to restrict to the projective case.

The rough plan should be: the category $\mathcal{MF}(X)$, [9], [18, §8]. The Dieudonne functor D, [9], [18, §9]. The p-adic Hodge structure on $\mathcal{P}_r^{\mathrm{dR}}$ [18, Theorems 37, 38]. Deduce Theorem A.

11. Selmer varieties and unipotent étale Kummer map

Let X be a hyperbolic curve over a number field F, x_0 an F-rational point and S a finite set of places of F outside of which (X, x_0) has good reduction, and p a prime outside of S. Let $U_n^{\text{ét}}$ denote the $\mathbb{Q}_p$-unipotent étale fundamental group of X with base point x_0, truncated at level n. Then the Galois cohomology set $H^1(F, U_n^{\text{ét}})$ classifies $U_n^{\text{ét}}$-torsors over F. Assigning to an F-rational x the class of the path torsor $U_n^{\text{ét}}(x)$, we obtain the *unipotent Kummer map*

$$X(F) \to H^1(F, U_n^{\text{ét}}),$$

see Talk 3. The goal of this talk is to explain several important technical points about $H^1(F, U_n^{\text{ét}})$ and the Kummer map ([12], §1 und §3, [13], §2).

(1) The image of the set of S-integral points under the Kummer map lies in a subset $H^1_f(F, U_n^{\text{ét}})$ defined by local conditions at p and at all places in S. (The f-condition at all places over p means *deRham* in [12] and *cristalline* in [13]; for the next talk we rather need the cristalline condition.)
(2) The set $H^1_f(F, U_n^{\text{ét}})$ has a natural structure of an affine $\mathbb{Q}_p$-variety.

(3) For every n we have a 'short exact sequence'

$$1 \to H^1_f(F, Z^{\text{ét}}_{n+1}) \to H^1_f(F, U^{\text{ét}}_{n+1}) \to H^1_f(F, U^{\text{ét}}_n)$$

of affine varieties (where the 'kernel' is actually a $\mathbb{Q}_p$-vector space).

(4) For every place v of F outside S (in particular, for places above p) we can replace F by F_v in (1)-(3) above, and the localization map

$$H^1_f(F, U^{\text{ét}}_n) \to H^1_f(F_v, U^{\text{ét}}_n)$$

is algebraic.

12. Finiteness for $\mathbb{P}^1 \setminus \{0, 1, \infty\}$

Notation as in talk (10), with R the ring of S-integers of F, nonabelian p-adic Hodge theory gives rise to a commuting square:

$$\begin{tikzcd} X(R) \arrow[r] \arrow[d] & Y(F_{\mathfrak{p}}) \arrow[d] \\ H^1_f(G_T, U^{\text{ét}}_n)(\mathbb{Q}_p) \arrow[r] & (U^{\text{dR}}_n/F^0)(F_{\mathfrak{p}}) \end{tikzcd}$$

On the other hand, the representability of $H^1_f(G_T, U^{\text{ét}}_n)$ allows us to talk about its *dimension.* This talk should begin with this square, following [13, §2]. Subsequently, the talk might include a discussion of the ensuing finiteness for $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ [12], presumably quoting the result of Soulé without explanation, as well as a discussion of related conjectures, following [13].

References

[1] Berger, L., An introduction to the theory of p-adic representations. *Geometric aspects of Dwork theory.* Vol. I, II, 255–292, Walter de Gruyter GmbH & Co. KG, Berlin, 2004.

[2] Berthelot, P., Cohomologie rigide et cohomologie rigide à supports propre. Première partie. *preprint*, available at `http://perso.univ-rennes1.fr/pierre.berthelot/`

[3] Besser, A., Coleman integration using the Tannakian formalism, *Mathematische Annalen* **322** (2002), 19–48.

[4] Breen, L., Tannakian categories, in: *Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math.*, **55**, Part 1, Amer. Math. Soc., Providence, RI, 1994, 337–376.

[5] Chabauty, C., Sur les points rationnels des courbes algébriques de genre supérieur à lunité, *C. R. Acad. Sci. Paris* **212** (1941), 882885.

[6] Chiarellotto and, B., LeStum, B., F-isocristaux unipotents, *Compositio Math.* **116** (1999), no. 1, 81110.

[7] Deligne, P., Le groupe fondamental de la droite projective moins trois points, in *Galois groups over* $\mathbb{Q}$ *(Berkeley, CA, 1987)*, Math. Sci. Res. Inst. Publ. **16**, Springer, 1989, 79–297.

[8] Demazure, M.; Gabriel, P., *Groupes algbriques. Tome I: Gomtrie algbrique, gnralits, groupes commutatifs.* Masson & Cie, Éditeur, Paris; North-Holland Publishing Co., Amsterdam, 1970. xxvi+700 pp.

[9] Faltings, G., Crystalline cohomology and p-etale cohomology in *Algebraic Analysis, Geometry and Number Theory*, Johns Hopkins Univ. Press., (1989)

[10] Furusho, H., p-adic multiple zeta values. I. p-adic multiple polylogarithms and the p-adic KZ equation. *Invent. Math.* **155** (2004), no. 2, 253–286.

[11] Furusho, H., p-adic multiple zeta values. II. Tannakian interpretations. *Amer. J. Math.* **129** (2007), no. 4, 1105–1144.

[12] Kim, M., The motivic fundamental group of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ and the theorem of Siegel, *Inventiones Math.* **161** (2005), 629–656.

[13] Kim, M., The unipotent Albanese map and Selmer varieties for curves

[14] Grothendieck, A., Raynaud, M., *Revêtments Étale et Groupe Fondamental (SGA 1)*, LNM **224**, Springer, 1971.

[15] Lenstra, H. W., Galois Theory for Schemes. Available at `www.math.leidenuniv.nl/ jbrakenh/topics2/Galoistheoryschemes.pdf`

[16] Olsson, M., Towards non–abelian P–adic Hodge theory in the good reduction case. *Preprint.* Available at `http://math.berkeley.edu/ molsson/`

[17] Szamuely, T., *Galois groups and fundamental groups.* Cambridge Studies in Advanced Mathematics, **117**. Cambridge University Press, Cambridge, 2009. x+270 pp.

[18] Vologodsky, V., Hodge structure on the fundamental group and its application to p-adic integration, *Moscow Math. J.* **3** No. 1 (2003), 205–247.