Fontaine's rings and p-adic L-functions

by

Shen-Ning Tung

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

in

THE FACULTY OF GRADUATE AND POSTDOCTORIAL STUDIES
(Mathematics)

The University of British Columbia
(Vancouver)

February 2015

Abstract

In the first part, we introduce theory of p-adic analysis for one variable p-adic functions and then use them to construct Kubota-Leopoldt p-adic L-functions.

In the second part, we give a description of the Iwasawa modules attached to p-adic Galois representations of the absolute Galois group of K in terms of the theory of (φ,Γ)-modules of Fontaine. When the representation is de Rham when K be finite extension of $\mathbf{Q}_p$. This gives a natural construction of the exponential map of Perrin-Riou which is used in the construction and the study of p-adic L-functions.

In the third part, we give formulas for Bloch-Kato's exponential map and its dual for an alsolutely crystalline p-adic representation V. As a corollary of these computation, we can give a improved description of Perrin-Riou's exponential map, which interpolates Bloch-Kato's exponentials for the twists of V. Finally we use this map to reconstruct Kubota-Leopoldt p-adic L-functions.

Preface

This thesis is a reorganisation of classical materials on Perrin-Riou's big reciprocity law maps and theory of (φ,Γ) module. The author is benefited from papers of Cherbonnier, Colmez, Berger, Loeffler and Zerbes. The topic of this thesis was suggested by my supervisor, Professor Sujatha Ramdorai.

Table of Contents

Acknowledgments

I would like to thank my supervisors Sujatha Ramdorai for her continuous support and guidance, for suggesting me this topic and giving a seminar on this subject and for the innumerable things that I have learned from them throughout graduate school.

I owe an enormous debt of gratitude to Ming-Lun Hsieh, from whom I have learned so much and helping me finishing this thesis. Ming-Lun has always been unfailingly patient and willing to share his knowledge and expertise. I have benefitted tremendously from his intellectual generosity, attentiveness to detail, and time, and his feedback on multiple drafts of this thesis has led to significant improvements in clarity and exposition. As an undergraduate at National Taiwan University, I was fortunate to have terrific mentors who encouraged me to develop my passions and mathematical foundation.

It is a pleasure and privilege to thank Subhajit Juna and Li Zheng for many helpful discussions and exchanges related to this project. We have shared conversations and experiences that have been an invaluable part of this journey. I also thank Justin Scarfy for pointing out several errors in my previous draft.

Chapter 1

Introduction

1.1 Overview

We fix an algebraic closure $\overline{\mathbf{Q}}_p$ of $\mathbf{Q}_p$. If K is a finite extension of $\mathbf{Q}_p$ and $n \in \mathbf{N}$, we put $K_n = K(\mu_p)$ with μ_p the p-th root of unity and we denote by K_∞ the union of K_n. We denote by G_K the Galois group $\mathrm{Gal}(\overline{\mathbf{Q}}_p/K)$ and H_K the kernel of the restriction of χ on G_K where $\chi : G_{\mathbf{Q}_p} \to \mathbf{Z}_p^*$ is the cyclotomic units. Thus $H_K = Gal(\overline{\mathbf{Q}}_p/K_\infty)$ and we put $\Gamma_K = G_K/H_K = \mathrm{Gal}(K_\infty/K)$.

The theory of (φ,Γ)-modules, introduced by Fontaine, associate a p-adic representation V of H_K to a module $\mathbf{D}(V)$ over a dimension 2 local field (ring of Laurent series in one variable with coefficient in a finite unmarried extension of $\mathbf{Q}_p$ with a Frobenius action φ and a left invere ψ of φ. If V is a representation of G_K, then the module $\mathbf{D}(V)$ is endowed with an residue action Γ_K commuting with φ. The reason this theory is interested is because we can reconstruct V via $\mathbf{D}(V)$, which is a more amenable object. Indeed, since Γ_K is procyclic, the structure of $\mathbf{D}(V)$ is totally decided by the action of two operators (φ and the generator of Γ_K) verifying the commutative relation. Thus, to study the p-adic Galois representations of G_K is equivalent to (φ,Γ)-modules. Two main results we will prove are

1. the construction of the isomorphism $\mathrm{Exp}^*_{V^*(1)}$ from the Iwasawa module $H^1_{K,V} = \mathbf{Q}_p \otimes (\varprojlim H^1(K_n,T))$ to $\mathbf{D}(V)^{\psi=1}$ where T is a Galois fixed lattice in V.

2. an explicit reciprocity law of $\mathrm{Exp}^*_{V^*(1)}$ where V is a de Rham representation in terms of the the Bloch-Kato's exponential maps.

The first one using the result of Herr, which gives a description of $H^1_{Iw}(K,V)$ in terms of $\mathbf{D}(V)$. In the case $V = \mathbf{Q}_p(1)$ and K is unramified extension over $\mathbf{Q}_p$, the map $\mathrm{Exp}^*_{V^*(1)}$ can be described in terms of derivatives of classical Coleman's power series (See [8]). We therefore obtain a generalized Coleman power series without any restriction of K. To prove the explicit reciprocity law, we use the fact that every representation of G_K is overconvergent. This is an ingredient permits us to link $\mathbf{D}(V)$ and the of $\mathbf{D}_{\mathrm{dR}}(V)$.

When K is unramified extension of $\mathbf{Q}_p$ and V is crystalline representation of G_K, Perrin-Riou has constructed in [18] a period map $\Omega_{V,h}$ which interpolates the $\exp_{K,V(k)}$ as k runs over the positive integers. It is a generalization of Coleman's map. Using the inverse of Perrin-Riou's map, one can then associate to an Euler system a p-adic L-function. If one starts with $V = \mathbf{Q}_p(1)$, then Perrin-Riou's map is the inverse of the Coleman isomorphism and one recovers Kubota-Leopoldt's p-adic L-functions.

1.2 Structure of the thesis

In chapter 2-3, following [11] and [12], we introduce the theory of one variable p-adic functions and use it to construct Kubota-Leopoldt p-adic L-functions which interpolate the value of Dirichlet L-functions at negative integers.

In chapter 4-6, we begin with background of (φ,Γ)-modules and its relation with p-adic Galois representations. Following [14], we can use Herr complexes to compute Galois cohomology groups of p-adic Galois representations. Finally, we prove the Fontaine's isomorphism in [6] which relates Iwasawa cohomology groups of p-adic Galois representations with its associated (φ,Γ)-modules.

In chapter 7-8, we introduce Fontaine's period rings and overconvergent representations. Following [5], we can compare $\mathbf{D}_{\mathrm{dR}}$ and $\mathbf{D}^{\dagger}$. We then introduce Bloch-Kato's exponential map and its dual in [4] and use overconvergent representation to deduce Colmez's explicit reciprocity law in [6].

In chapter 9, we recall the definition of Coleman's power series in [8]. Following [6], we study its relation with the (φ,Γ)-modules associated to $\mathbf{Z}_p(1)$. Combining with Colmez's explicit reciprocity laws, we reinterpret classical Coates-Wiles homomorphisms.

In chapter 10-11, we first introduce the Robba ring $\mathbf{B}^{\dagger}_{\mathrm{rig}}$, which can be used to reinterpret Fontaine's isomorphism. By [2], we can get three explicit reciprocity formulas for Bloch-Kato's exponential map and its dual and use these explicit reciprocity formulas to deduce Perrin-Riou's big exponential map in [18].

In chapter 12, we follows the variance in appendix of [17], which allows us to add a finite order character in the inverse of Perrin-Riou's big exponential map constructed in chapter 10. Via this map, we can reconstruct Kubota-Leopoldt p-adic L-functions via cyclotomic units.

Chapter 2

One variable p-adic functions

2.1 Functions on $\mathbf{Z}_p$

Let $\mathscr{C}^0(\mathbf{Z}_p, L)$ be the space of continuous functions from $\mathbf{Z}_p$ to L. Since $\mathbf{Z}_p$ is compact, every continuous function on $\mathbf{Z}_p$ is bounded. This allows us to define a valuation $v_{\mathscr{C}^0}$ on $\mathscr{C}^0(\mathbf{Z}_p, L)$ by $v_{\mathscr{C}^0}(\phi) = \inf_{x \in \mathbf{Z}_p}(\phi(x))$, which makes $\mathscr{C}^0(\mathbf{Z}_p, L)$ an L-Banach space.

If $n \in \mathbf{N}$, let $\binom{x}{n}$ be the polynomial defined by

$$\binom{x}{n} = \begin{cases} 1 & \text{if } n = 0 \\ \frac{x(x-1)\cdots(x-n+1)}{n!} & \text{if } n \geq 1. \end{cases}$$

Theorem 2.1.1. *(Mahler)* $\{\binom{x}{n}, n \in \mathbf{N}\}$ *forms a Banach basis of* $\mathscr{C}^0(\mathbf{Z}_p, L)$.

If $h \in \mathbf{N}$, let $\mathrm{LA}_h(\mathbf{Z}_p, L)$ be the space of functions from $\mathbf{Z}_p$ to L which is analytic on $a + p^h\mathbf{Z}_p$ for all $a \in \mathbf{Z}_p$. i.e. if $\phi \in \mathrm{LA}_h(\mathbf{Z}_p, L)$, $x_0 \in \mathbf{Z}_p$, then ϕ can be written as the form

$$\phi(x) = \sum_{k=0}^{\infty} a_k(\phi, x_0)(x - x_0)^k \ \forall x \in x_0 + p^h\mathbf{Z}_p,$$

where $a_k(x_0, \phi)$ is a sequence in L such that $v_p(a_k(\phi, x_0)) + kh$ tends to $+\infty$ as k tends to $+\infty$. We endow $\mathrm{LA}_h(\mathbf{Z}_p, L)$ a valuation v_{LA_h} defined by

$$v_{\mathrm{LA}_h}(\phi) = \inf_{x_0 \in \mathbf{Z}_p} \inf_{k \in \mathbf{N}} v_p(a_k(\phi, x_0)) + kh,$$

which makes $\mathrm{LA}_h(\mathbf{Z}_p, L)$ an L-Banach space. One can show that $v_{\mathrm{LA}_h}(\phi) = \inf_{a \in S} \inf_{k \in \mathbf{N}} v_p(\phi, a_k(a)) + kh$ where S is a representative of $\mathbf{Z}_p/p^h\mathbf{Z}_p$. (See [12, remark I.4.4.])

We denote $\mathrm{LA}(\mathbf{Z}_p, L)$ the space of locally analytic functions on $\mathbf{Z}_p$. Since $\mathbf{Z}_p$ is compact, it is an inductive limit of $\mathrm{LA}_h(\mathbf{Z}_p, L)$, $h \in \mathbf{N}$, and we endow it with the inductive limit topology.

Theorem 2.1.2. *(Amice)* $\{[\frac{n}{p^h}]!\binom{x}{n}, n \in \mathbf{N}\}$ *forms a Banach basis of* $\mathrm{LA}_h(\mathbf{Z}_p, L)$*, where* $[\ ]$ *is the Gauss symbol and* $!$ *is the factorial.*

Theorem 2.1.3. *The function* $\phi = \sum_{n=0}^{+\infty} a_n(\phi)\binom{x}{n} \in \mathscr{C}^0(\mathbf{Z}_p, L)$ *is in* $\mathrm{LA}(\mathbf{Z}_p, L)$ *if and only if* $\liminf_{n\mapsto\infty} \frac{1}{n} v_p(a_n(\phi)) > 0$.

A function $\phi : \mathbf{Z}_p \to L$ is differentiable at $x_0 \in \mathbf{Z}_p$ if $\lim_{h\to 0} \frac{\phi(x_0+h)-\phi(x_0)}{h}$ exists. The limit is denoted by $\phi'(x_0)$. A function is said to be differentiable of order 1 if it is differentiable at all $x_0 \in \mathbf{Z}_p$. Inductively, we say that a function is differentiable of order k if its differentiation is of order $k-1$.

If $r \geq 0$, we say that $\phi : \mathbf{Z}_p \to L$ is of class $\mathscr{C}^r$ if there exist functions $\phi^{(j)} : \mathbf{Z}_p \to L$ for $0 \leq j \leq [r]$, such that, if we define $\varepsilon_{\phi,r} : \mathbf{Z}_p \times \mathbf{Z}_p \to L$ and $C_{\phi,r} : \mathbf{N} \to \mathbb{R} \cup \{+\infty\}$ by

$$\varepsilon_{\phi,r}(x,y) = \phi(x+y) - \sum_{j=0}^{[r]} \phi^{(j)}(x)\frac{y^j}{j!} \quad \text{and} \quad C_{\phi,r}(h) = \inf_{x\in\mathbf{Z}_p, y\in p^h\mathbf{Z}_p} v_p(\varepsilon_{\phi,r}(x,y)) - rh,$$

then $C_{\phi,r}(h)$ tends to $+\infty$ as h tends to $+\infty$.

We denote $\mathscr{C}^r(\mathbf{Z}_p, L)$ the set of functions $\phi : \mathbf{Z}_p \to L$ of class $\mathscr{C}^r$. We endow $\mathscr{C}^r(\mathbf{Z}_p, L)$ the valuation $v_{\mathscr{C}^r}$ defined by

$$v_{\mathscr{C}^r}(\phi) = \inf\left(\inf_{0\leq j\leq [r], x\in\mathbf{Z}_p} v_p\left(\frac{\phi^{(j)}(x)}{j!}\right), \inf_{x,y\in\mathbf{Z}_p} v_p\big(\varepsilon_{\phi,r}(x,y) - r v_p(y)\big)\right),$$

which makes it an L-Banach space.

Proposition 2.1.4. *If* $h \in \mathbf{N}$*, and if* $r \geq 0$*, then* $\mathrm{LA}_h(\mathbf{Z}_p, L) \subset \mathscr{C}^r(\mathbf{Z}_p, L)$*. Moreover, if* $\phi \in \mathrm{LA}_h(\mathbf{Z}_p, L)$*, then*

$$v_{\mathscr{C}^r}(\phi) \geq v_{\mathrm{LA}_h}(\phi) - rh.$$

Proof. See [12, proposition I.5.7]. □

If $i \in \mathbf{N}$, we denote $l(i)$ the least integer n such that $p^n > i$, then we have

$$l(0) = 0 \quad \text{and} \quad l(i) = [\frac{\log i}{\log p}] + 1, \text{ if } i \geq 1.$$

Theorem 2.1.5. *(Mahler) The function* $\phi = \sum_{n=0}^{+\infty} a_n(\phi)\binom{x}{n} \in \mathscr{C}^0(\mathbf{Z}_p, L)$ *is in* $\mathscr{C}^r(\mathbf{Z}_p, L)$*,* $r \geq 0$ *if and only if* $v_p(a_n(\phi)) - rl(n) \to +\infty$ *as* $n \to +\infty$*. Moreover, the valuation* $v'_{\mathscr{C}^r}$ *defined on* $\mathscr{C}^r(\mathbf{Z}_p, L)$ *by the formula*

$$v'_{\mathscr{C}^r}(\phi) = \inf_{n\in\mathbf{N}}\left(v_p(a_n(\phi)) - rl(n)\right)$$

is equivalent to the valuation $v_{\mathscr{C}^r}$.

Proof. See [12, proposition I.5.18]. □

Corollary 2.1.6. *$p^{[rl(n)]}\binom{x}{n}$, $n \in \mathbf{N}$ forms a Banach basis of $\mathscr{C}^r(\mathbf{Z}_p, L)$.*

2.2 Distributions on $\mathbf{Z}_p$

A continuous distribution on $\mathbf{Z}_p$ is a continuous linear function on $\mathrm{LA}(\mathbf{Z}_p, L)$, that is, a linear function on $\mathrm{LA}(\mathbf{Z}_p, L)$ whose restriction to $\mathrm{LA}_h(\mathbf{Z}_p, L)$ is continuous. We denote $\mathscr{D}(\mathbf{Z}_p, L)$ the set of continuous distributions on $\mathbf{Z}_p$ with values in L and endow $\mathscr{D}(\mathbf{Z}_p, L)$ with the Fréchet topology defined by the family of valuations v_{LA_h}, $h \in \mathbf{N}$.

Given a continuous distribution μ, we associate it with the formal series:

$$\mathscr{A}_\mu(T) = \int_{\mathbf{Z}_p} (1+T)^x \mu = \sum_{n=0}^{+\infty} T^n \int_{\mathbf{Z}_p} \binom{x}{n} \mu,$$

which is called the Amice transform of μ. Hence we define a map $\mu \mapsto \mathscr{A}_\mu$ from continuous distributions to formal power series.

Lemma 2.2.1. *If $\mu \in \mathscr{D}(\mathbf{Z}_p, L)$ and if $v_p(x) > 0$, then $\int_{\mathbf{Z}_p} (1+z)^x \mu(x) = \mathscr{A}_\mu(z)$.*

Let $\mathscr{R}^+$ be the ring of power series $f = \sum_{n=0}^{\infty} a_n T^n$ with coefficients in L, which is convergent if $v_p(T) > 0$.

We say that an element $f = \sum_{n=0}^{\infty} a_n T^n \in \mathscr{R}^+$ is of order r if $v_p(a_n) + rl(n)$ is bounded. We denote by $\mathscr{R}_h^+$ the subset of $\mathscr{R}^+$ of elements of order r, and we endow $\mathscr{R}_r^+$ the valuation v_r defined by $v_r(f) = \inf_{n \in \mathbf{N}} v_p(a_n) + rl(n)$, which makes it a L-Banach space. We endow $\mathscr{R}^+$ the Fréchet topology defined by the family of valuations v_r.

Theorem 2.2.2. *The map $\mu \mapsto \mathscr{A}_u$ is an isomorphism of* Fréchet *space from $\mathscr{D}(\mathbf{Z}_p, L)$ to $\mathscr{R}^+$.*

Proof. See [12, Theorem II.2.2]. □

If $r \geq 0$, we say a continuous distribution μ on $\mathbf{Z}_p$ is of order r if it can be extended by continuity to $\mathscr{C}^r$. We denote $\mathscr{D}_r(\mathbf{Z}_p, L)$ the set of distributions of order r, which is equipped with a valuation $v_{\mathscr{D}_r}$ defined by

$$v_{\mathscr{D}_r}(\mu) = \inf_{f \in \mathscr{C}^r(\mathbf{Z}_p, L) - \{0\}} \left(v_p\Big(\int_{\mathbf{Z}_p} f\mu\Big) - v_{\mathscr{C}^r}(f) \right),$$

which gives $\mathscr{D}_r(\mathbf{Z}_p, L)$ the dual topology of $\mathscr{C}^r(\mathbf{Z}_p, L)$.

A distribution is said to be tempered if there exist $r \in \mathbb{R}^+$ such that it is of order r. We denote $\mathscr{D}_{temp}(\mathbf{Z}_p, L)$ the space of tempered distributions.

Proposition 2.2.3. *The map $\mu \mapsto \mathscr{A}_\mu$ induces an isometry from $\mathscr{D}_r(\mathbf{Z}_p, L)$ equipped with valuation $v_{\mathscr{D}_r}$ to $\mathscr{R}_r^+$ equipped with valuation v_r.*

A distribution of order 0 is called measure. By definition, $\mathscr{D}_0(\mathbf{Z}_p,L)$ is the topological dual of the space of continuous functions. By proposition 2.2.3, we have a one-one correspondence from a measure to a power series of bounded coefficients.

To sum up, we have

$$\mathscr{C}^0 \supset \mathscr{C}^r \supset \mathrm{LA} \supset \mathrm{LA}_r$$

$$\mathscr{D}_0 \subset \mathscr{D}_r \subset \mathscr{D} \subset \mathrm{LA}_r^*$$

2.3 Operations on the distributions

1. Haar measure: $\mu(\mathbf{Z}_p) = 1$ and μ is invariant by translation. We must have $\mu(i+p^n\mathbf{Z}_p) = \frac{1}{p^n}$ which is not bounded. Hence there exists no Harr measure on $\mathbf{Z}_p$.

2. Dirac measure: For $a \in \mathbf{Z}_p$, we define δ_a the Dirac measure associated to $f(a)$. The Amice transform of δ_a is $\mathscr{A}_{\delta_a}(T) = (1+T)^a$.

3. Multiplication by a function: If μ is a distribution on $\mathbf{Z}_p$ and f is a locally analytic function on $\mathbf{Z}_p$, we define the distribution $f\mu$ by $\int_{\mathbf{Z}_p}\phi(f\mu) = \int_{\mathbf{Z}_p}(f\phi)\mu$.

   - Multiplication by x: We have $x\cdot\binom{x}{n} = ((x-n)+n)\binom{x}{n} = (n+1)\binom{x}{n+1} + n\binom{x}{n}$, and hence we have

     $$\mathscr{A}_{x\mu}(T) = \partial\mathscr{A}_\mu \quad \text{where}\, \partial = (1+T)\frac{d}{dT}.$$

   - Multiplication by z^x when $v_p(z-1) > 0$: By lemma 2.2.1, if $v_p(y-1) > 0$, and if λ is a continuous distribution on $\mathbf{Z}_p$, then $\int_{\mathbf{Z}_p} y^x\lambda(x) = \mathscr{A}_\lambda(y-1)$. Applying this to $\lambda = z^x\mu$, we obtain $\mathscr{A}_\lambda(y-1) = \mathscr{A}_\mu(yz-1)$. We have the formula

     $$\mathscr{A}_{z^x\mu}(T) = \mathscr{A}_\mu((1+T)z-1).$$

4. Restriciton to compact open subset: If X is a compact open subset of $\mathbf{Z}_p$, then the characteristic function 1_X is continuous on $\mathbf{Z}_p$. If μ is a distribution on $\mathbf{Z}_p$, the measure $1_X\mu$ is the restriction of μ to X and is denoted by $\mathrm{Res}_X(\mu)$. In particular for $n \in \mathbf{N}$ and $a \in \mathbf{Z}_p$, we have $1_{a+p^n\mathbf{Z}_p}(x) = p^{-n}\sum_{z^{p^n}=1} z^{-a}z^x$, hence

   $$\mathscr{A}_{\mathrm{Res}_{a+p^n\mathbf{Z}_p}(\mu)}(T) = p^{-n}\sum_{z^{p^n}=1} z^{-a}\mathscr{A}_\mu((1+T)z-1).$$

5. Derivation of distribution: If $\mu \in \mathscr{D}(\mathbf{Z}_p,L)$, we define $d\mu$ by

   $$\int_{\mathbf{Z}_p}\phi(x)d\mu = \int_{\mathbf{Z}_p}\phi'(x)\mu, \quad \text{and therefore} \quad \mathscr{A}_{d\mu}(T) = \log(1+T)\cdot\mathscr{A}_\mu(T).$$

6. Actions of $\mathbf{Z}_p^*$, φ and ψ:

   - If $a \in \mathbf{Z}_p^*$, and if $\mu \in \mathscr{D}(\mathbf{Z}_p, L)$, we define $\sigma_a(\mu) \in \mathscr{D}(\mathbf{Z}_p, L)$ by

   $$\int_{\mathbf{Z}_p} \phi(x)\sigma_a(\mu) = \int_{\mathbf{Z}_p} \phi(ax)\mu, \text{ and therefore } \mathscr{A}_{\sigma_a(\mu)}(T) = \mathscr{A}_\mu((1+T)^a - 1).$$

   - φ acts on distribution μ by

   $$\int_{\mathbf{Z}_p} \phi(x)\varphi(\mu) = \int_{\mathbf{Z}_p} \phi(px)\mu, \text{ and therefore } \mathscr{A}_{\varphi(\mu)}(T) = \mathscr{A}_\mu((1+T)^p - 1).$$

   - If μ is a distribution on $\mathbf{Z}_p$, we denote $\psi(\mu)$ the distribution on $\mathbf{Z}_p$ defined by

   $$\int_{\mathbf{Z}_p} \phi(x)\psi(\mu) = \int_{p\mathbf{Z}_p} \phi(p^{-1}x)\mu \quad \text{and therefore} \quad \mathscr{A}_{\psi(\mu)} = \psi(\mathscr{A}_\mu),$$

   where $\psi : \mathscr{R}^+ \to \mathscr{R}^+$ is defined by $\psi(F)((1+T)^p - 1) = \frac{1}{p}\sum_{\zeta^p=1} F((1+T)\zeta - 1)$.

   The action of $\mathbf{Z}_p^*$, φ and ψ satisfy the relations:

   (a) $\psi \circ \phi =$id.

   (b) $\psi \circ \sigma_a = \sigma_a \circ \psi$ and $\varphi \circ \sigma_a = \sigma_a \circ \varphi$ if $a \in \mathbf{Z}_p^*$.

   (c) $\psi(\mathscr{A}_\mu) = 0$ if and only if μ has support on $\mathbf{Z}_p^*$, and $\mathscr{A}_{\mathrm{Res}_{\mathbf{Z}_p^*}(\mu)} = (1 - \varphi\psi)\mathscr{A}_\mu$.

7. Convolution of distribution: If λ and μ are two distributions on $\mathbf{Z}_p$, we define the convolution $\lambda * \mu$ by

   $$\int_{\mathbf{Z}_p} \phi \cdot \lambda * \mu = \int_{\mathbf{Z}_p} \big(\int_{\mathbf{Z}_p} \phi(x+y)\mu(x)\big)\lambda(y).$$

   Let $\phi(x)$ be the function $x \mapsto z^x$, where $v_p(z-1) > 0$, then we have $\mathscr{A}_{\lambda*\mu}(z) = \mathscr{A}_\lambda(z)\mathscr{A}_\mu(z)$. Hence we deduce $\mathscr{A}_{\lambda*\mu} = \mathscr{A}_\lambda \cdot \mathscr{A}_\mu$.

Chapter 3

Kubota-Leopoldt p-adic L-functions

3.1 The Riemann zeta function

Let $\zeta(s) = \sum_{n=1}^{+\infty} n^{-s} = \prod_{p:Prime}(1-p^{-s})^{-1}$ be the Riemann zeta function. Let $\Gamma(s) = \int_{t=0}^{+\infty} e^{-t} t^s \frac{dt}{t}$ be the Gamma function, which is holomorphic on $Re(s) > 0$ and satisfies the functional equation $\Gamma(s+1) = s\Gamma(s)$, and thus it can be extended to a meromorphic function on $\mathbb{C}$.

Recall we have:

Lemma 3.1.1. *If $Re(s) > 1$, then*

$$\zeta(s) = \frac{1}{\Gamma(s)} \int_0^{+\infty} \frac{1}{e^t - 1} t^s \frac{t}{dt}.$$

Proposition 3.1.2. *If f is a $\mathscr{C}^\infty$ function on $\mathbb{R}^+$ which decreases rapidly at infinity, then the function*

$$L(f,s) = \frac{1}{\Gamma(s)} \int_0^{+\infty} f(t) t^s \frac{dt}{t}$$

defined on $Re(s) > 0$ admits a holomorphic extension to $\mathbb{C}$ and if $n \in \mathbf{N}$, then $L(f,-n) = (-1)^n f^{(n)}(0)$.

Apply proposition 3.1.2 to $f_0(t) = \frac{t}{e^t - 1}$. Let $\sum_{n=0}^{+\infty} B_n \frac{t^n}{n!}$ be the Taylor expension of f_0 at 0, where B_n is the Bernoulli number. We have, in particular

$$B_0 = 1, \quad B_1 = -\frac{1}{2}, \quad B_2 = \frac{1}{6}, \quad B_4 = \frac{-1}{30} \cdots.$$

Since $f_0(t) - f_0(-t) = -t$, we have $B_{2k+1} = 0$ if $k \geq 1$.

Theorem 3.1.3.

i) The function ζ has a meromorphic continuation to $\mathbb{C}$, which has a simple pole at $s = 1$ with residue 1.

ii) If $n \in \mathbf{N}$, then $\zeta(-n) = (-1)^n \frac{B_{n+1}}{n+1}$, and in particular $\zeta(-n) \in \mathbf{Q}$.

3.2 Kummer congruences

If $a \in \mathbb{R}_+^*$, by applying proposition 3.1.2 to the function $f_a(t) = \frac{1}{e^t - 1} - \frac{a}{e^{at}-1}$, which is $\mathscr{C}^\infty$ (the pole at $t = 0$ canceling out) on $\mathbb{R}^+$ and decreases rapidly at infinity, we have

Corollary 3.2.1. *If $a \in \mathbb{R}_+^*$, the function $(1 - a^{1-s})\zeta(s) = L(f_a, s)$ has an analytic continuation on $\mathbb{C}$, and if $n \in \mathbf{N}$, then $(1 - a^{1+n})\zeta(-n) = (-1)^n f_a^{(n)}(0)$. In particular, if $a \in \mathbf{Q}$, then $(1 - a^{1+n})\zeta(-n) \in \mathbf{Q}$.*

Given a continuous distribution μ, we associate it with the formal series:

$$\mathscr{L}_\mu(t) = \sum_{n=0}^{+\infty} \int_{\mathbf{Z}_p} e^{tx}\mu = \sum_{n=0}^{+\infty} \frac{t^n}{n!} \int_{\mathbf{Z}_p} x^n \mu,$$

which is called the Laplace transform of μ.

We have $\mathscr{L}_\mu(t) = \mathscr{A}_\mu(e^t - 1)$.

Proposition 3.2.2. *If $a \in \mathbf{Z}_p^*$, there exists a measure μ_a whose Laplace transform is $f_a(t)$. Moreover $v_{\mathscr{D}_0}(\mu_a) \geq 0$ and if $n \in \mathbf{N}$, then $\int_{\mathbf{Z}_p} x^n \mu_a = (-1)^n(1 - a^{1+n})\zeta(-n)$.*

Proof. To show the existance of μ_a, it suffices to prove that the coefficients of series obtained by replace e^t by $1 + T$ (Amice transform of μ_a) is bounded by proposition 2.2.3. Since $(1+T)^a - 1$ is of the form $aT(1 + Tg(T))$ where $g(T) = \sum_{n=2}^{+\infty} \frac{1}{a}\binom{a}{n} T^{n-2} \in \mathbf{Z}_p[[T]]$, we have

$$\frac{1}{T} - \frac{a}{(1+T)^a - 1} = \sum_{n=1}^{+\infty} (-T)^{n-1} g^n \in \mathbf{Z}_p[[T]].$$

Since the coefficients are in $\mathbf{Z}_p$, we have $v_{\mathscr{D}_0}(\mu_a) \geq 0$. Moreover, we have $\int_{\mathbf{Z}_p} x^n \mu_a = \mathscr{L}_{\mu_a}^{(n)}(0) = f_a^{(n)}(0)$. □

Corollary 3.2.3. *(Kummer congruences) If $a \in \mathbf{Z}_p^*$ and $k \geq 1$, if n_1 and n_2 are two integers $\geq k$ such that $n_1 \equiv n_2$ mod $(p-1)p^{k-1}$, then*

$$v_p\left((1 - a^{1+n_1})\zeta(-n_1) - (1 - a^{1+n_2})\zeta(-n_2)\right) \geq k.$$

Proof. Since by assumption $n_1 \geq k$ and $n_2 \geq k$, we have $v_p(x^{n_1}) \geq k$ and $v_p(x^{n_2}) \geq k$ if $x \in p\mathbf{Z}_p$. On the other hand, since the order of $(\mathbf{Z}/p^k\mathbf{Z})^*$ is $(p-1)p^{k-1}$, and by assumption $n_1 \equiv n_2$ mod $(p-1)p^{k-1}$, we have $x^{n_1} - x^{n_2} \in p^k\mathbf{Z}_p$ if $x \in \mathbf{Z}_p^*$. To sum up, we have $v_p(x^{n_1} - x^{n_2}) \geq k$ if $x \in \mathbf{Z}_p$ and hence $v_{\mathscr{C}^0}(x^{n_1} - x^{n_2}) \geq k$. Since $v_{\mathscr{D}_0}(\mu_a) \geq 0$, which implies

$$v_p((1 - a^{1+n_1})\zeta(-n_1) - (1 - a^{1+n_2})\zeta(-n_2)) = v_p(\int_{\mathbf{Z}_p} (x^{n_1} - x^{n_2})\mu_a(x)) \geq k.$$

$\square$

Proposition 3.2.4. *If $a \in \mathbf{Z}_p^*$, then*

i) $\psi(\mu_a) = \mu_a$.

ii) $\mathrm{Res}_{\mathbf{Z}_p^*}(\mu_a) = (1-\varphi)\mu_a$

iii) $\int_{\mathbf{Z}_p^*} x^n \mu_a = (1-p^n)\int_{\mathbf{Z}_p} x^n \mu_a$ *for all* $n \in \mathbf{N}$.

Proof. Let $F(T) = \psi(\frac{1}{T})$. By definition, we have

$$\begin{aligned} F((1+T)^p - 1) =& \frac{1}{p}\sum_{\zeta^p=1} \frac{1}{(1+T)\zeta - 1} = \frac{-1}{p}\sum_{\zeta^p=1}\sum_{n=0}^{+\infty}((1+T)\zeta)^n \\ =& -\sum_{n=0}^{+\infty}(1+T)^{pm} = \frac{1}{(1+T)^p - 1}. \end{aligned}$$

Thus, we have $\psi(\frac{1}{T}) = \frac{1}{T}$. On the other hand, since the Amice transform of μ_a is $\frac{1}{T} - \frac{a}{(1+T)^a - 1} = \frac{1}{T} - a\sigma_a(\frac{1}{T})$, the action of ψ commutes with σ_a, and by $\psi(\mathscr{A}_\mu) = \mathscr{A}_{\psi(\mu)}$ if μ is a distribution, we deduce i).

ii) follows from i) since we have $\mathrm{Res}_{\mathbf{Z}_p^*}(\mu) = (1-\varphi\psi)\mu$ if μ is a distribution. iii) follows from ii) and $\int_{\mathbf{Z}_p} x^n \varphi(\mu) = \int_{\mathbf{Z}_p} (px)^n \mu$. $\square$

Corollary 3.2.5. *Let $a \in \mathbf{N} - \{1\}$ be prime to p. Let $k \geq 1$. If n_1 and n_2 are two integers $\geq k$ such that $n_1 \equiv n_2$ mod $(p-1)p^{k-1}$, then*

$$v_p((1-a^{1+n_1})(1-p^{n_1})\zeta(-n_1) - (1-a^{1+n_2})(1-p^{n_2})\zeta(-n_2)) \geq k.$$

By corollary 3.2.5, the function $n \mapsto (1-p^n)\zeta(-n)$ is continuous under the p-adic topology. To have a uniform formula, we put $q = 4$ if $p = 2$ and $q = p$ if $p \neq 2$. We denote by ϕ the Euler $\phi-$ function, and thus $\phi(q) = 2$ if $q = 4$ and $\phi(q) = p-1$ if $p \neq 2$.

Theorem 3.2.6. *If $i \in \mathbf{Z}/\phi(q)\mathbf{Z}$, there exist an unique function $\zeta_{p,i}$ continuous on $\mathbf{Z}_p$ (resp. $\mathbf{Z}_p - \{1\}$) if $i \neq 1$ (resp. $i = 1$) such that the function $(s-1)\zeta_{p,i}$ is analytic on $\mathbf{Z}_p$ (resp. $i + 2\mathbf{Z}_p$ if $p = 2$) and one has $\zeta_{p,i}(-n) = (1-p^n)\zeta(-n)$ if $n \in \mathbf{N}$ satisfying $-n \equiv i$ mod $p-1$.*

Remark 3.2.7. $\zeta_{p,i}$ is called the i-th branch of Kubota-Leopoldt zeta function. If i is even, then $\zeta_{p,i}$ is identically zero since $\zeta(-n) = 0$ if $n \geq 2$ is even.

3.3 p-adic Mellin transform and Leopoldt's Γ-transform

We denote Δ the group of roots of unity of $\mathbf{Q}_p^*$. Therefore Δ is a cyclic group of order $\phi(q)$ and $\mathbf{Z}_p^*$ is disjoint union of $\varepsilon + q\mathbf{Z}_p$ with $\varepsilon \in \Delta$. We denote $\omega : \mathbf{Z}_p \to \Delta \cup \{0\}$ the function defined by $\omega(x) = 0$ if $x \in p\mathbf{Z}_p$, and $x - \omega(x) \in q\mathbf{Z}_p$, if $x \in \mathbf{Z}_p^*$. If $x \in \mathbf{Z}_p^*$, we define $\langle x \rangle \in 1 + q\mathbf{Z}_p$ by $\langle x \rangle = x\omega(x)^{-1}$.

Proposition 3.3.1. *If $i \in \mathbf{Z}/\phi(q)\mathbf{Z}$, the function $x \mapsto \omega(x)^i \langle x \rangle^s$ is a locally analytic function on $\mathbf{Z}_p$. Moreover, we have*

i) $\omega(x)^i \langle x \rangle^n = x^n$ *if $n \equiv i$ mod $\phi(q)$ and if $x \in \mathbf{Z}_p^*$*

ii) $\omega(x)^i \langle x \rangle^s = \lim_{\substack{n \to s \\ n \equiv i \bmod \phi(q)}} x^n$ *for $x \in \mathbf{Z}_p$.*

Proof. Note that we have $\omega(x)^i \langle x \rangle^s = 0$ on $p\mathbf{Z}_p$ and

$$\omega(x)^i \langle x \rangle^s = \varepsilon^i (\frac{x}{\varepsilon})^s = \sum_{n=0}^{+\infty} \binom{s}{n} \varepsilon^{i-n} (x-\varepsilon)^n,$$

if $x \in \varepsilon + q\mathbf{Z}_p$ and $\varepsilon \in \Delta$, thus the function is locally analytic.

Since the order of Δ is $\phi(q)$, we have $\omega(x)^n = \omega(x)^i$ if $n \equiv i$ mod $\phi(q)$, i) and ii) follows. $\square$

If $i \in \mathbf{Z}/\phi(q)\mathbf{Z}$, we defined the i-th branch of the Mellin transform of a continuous distribution μ by the formula

$$\mathrm{Mel}_{i,\mu}(s) = \int_{\mathbf{Z}_p} \omega(x)^i \langle x \rangle^s \mu(x) = \int_{\mathbf{Z}_p^*} \omega(x)^i \langle x \rangle^s \mu(x)$$

the second equality is because $\omega(x) = 0$ if $x \in p\mathbf{Z}_p$. On the other hand, we have $\mathrm{Mel}_{i,\mu}(n) = \int_{\mathbf{Z}_p^*} x^n \mu$ if $n \equiv i$ mod $\psi(q)$.

Let u be a topological generator of multiplicative group of $1 + q\mathbf{Z}_p$, and let $\theta : 1 + q\mathbf{Z}_p \to \mathbf{Z}_p$ the homomorphism which sends x to $\frac{\log x}{\log u}$. This homomorphism is analytic and also its inverse be. If f is a locally analytic function (resp. continuous) function on $1 + q\mathbf{Z}_p$, the function $\theta^* f$ defined by $\theta^* \phi(x) = \phi(\theta(x))$ is locally analytic (resp. continuous) on $\mathbf{Z}_p$.

If μ is a distribution support on $1 + q\mathbf{Z}_p$, we define a distribution $\theta_* \mu$ on $\mathbf{Z}_p$ by the formula

$$\int_{\mathbf{Z}_p} \phi(\theta_* \mu) = \int_{1+q\mathbf{Z}_p} (\theta^* \phi) \mu.$$

In particular, θ_* sends measure to measure.

Lemma 3.3.2. *If X is a open compact subset of $\mathbf{Z}_p$, If $\alpha \in \mathbf{Z}_p^*$, and if μ is a continuous distribution on $\mathbf{Z}_p$, then*

$$\mathrm{Res}_X(\sigma_\alpha(\mu)) = \sigma_\alpha(\mathrm{Res}_{\alpha^{-1}X}(\mu))$$

Proof. Since we have $1_X(\alpha x) = 1_{\alpha^{-1}X}(x)$ if $X \subset \mathbf{Z}_p$, we deduce the formula

$$\begin{aligned}\int_{\mathbf{Z}_p} \phi(x)\mathrm{Res}_X(\sigma_\alpha(\mu)) &= \int_{\mathbf{Z}_p} 1_X(x)\phi(x)\sigma_\alpha\mu \\ &= \int_{\mathbf{Z}_p} 1_X(\alpha x)\phi(\alpha x)\mu(x) \\ &= \int_{\mathbf{Z}_p} \phi(\alpha x)(1_{\alpha^{-1}X}(x)\mu(x)) \\ &= \int_{\mathbf{Z}_p} \phi(\alpha x)\mathrm{Res}_{\alpha^{-1}X}(\mu) \\ &= \int_{\mathbf{Z}_p} \phi(x)\sigma_\alpha(\mathrm{Res}_{\alpha^{-1}X}(\mu)),\end{aligned}$$

which proves the lemma. □

Definition 3.3.3. If μ is a distribution on $\mathbf{Z}_p^*$ and if $i \in \mathbf{Z}/\phi(q)\mathbf{Z}$, we define $\Gamma_\mu^{(i)}$ the i-th branch of the Γ-transform of μ by

$$\Gamma_\mu^{(i)} = \theta_*\mathrm{Res}_{1+q\mathbf{Z}_p}(\sum_{\varepsilon\in\Delta} \varepsilon^{-i}\sigma_\varepsilon(\mu)) = \theta_*(\sum_{\varepsilon\in\Delta} \varepsilon^{-i}\sigma_\varepsilon(\mathrm{Res}_{\varepsilon^{-1}+q\mathbf{Z}_p}(\mu))),$$

where the second equality follows from the above lemma. Moreover, it is clear that if μ is a measure on $\mathbf{Z}_p^*$, then $\Gamma_\mu^{(i)}$ is a measure on $\mathbf{Z}_p$, and we have $v_{\mathscr{D}_0}(\Gamma_\mu^{(i)}) \geq v_{\mathscr{D}_0}(\mu)$.

Proposition 3.3.4. *If μ is a continuous distribution on $\mathbf{Z}_p^*$ and $i \in \mathbf{Z}/\phi(q)\mathbf{Z}$, then*

$$\mathrm{Mel}_{i,\mu}(s) = \int_{\mathbf{Z}_p^*} \omega(x)^i\langle x\rangle^s\mu(x) = \int_{\mathbf{Z}_p} u^{sy}\Gamma_\mu^{(i)}(y) = \mathscr{A}_{\Gamma_\mu^{(i)}}(u^s-1)$$

Proof. The first equality is by the definition of Mellin transform and the third equality is by the definition of Amice transform. If $y = \theta(x) = \frac{\log x}{\log u}$, we have $u^{sy} = \exp(s\log x) = \langle x\rangle^s$ and

$$\int_{\mathbf{Z}_p} u^{sy}\Gamma_\mu^{(i)}(y) = \int_{1+q\mathbf{Z}_p} \langle x\rangle^s \sum_{\varepsilon\in\Delta} \varepsilon^{-i}\sigma_\varepsilon(\mathrm{Res}_{\varepsilon^{-1}+q\mathbf{Z}_p}(\mu)).$$

Using the fact that $\omega(x) = \varepsilon^{-1}$ if $x \in \varepsilon^{-1} + q\mathbf{Z}_p$ and $\langle\varepsilon x\rangle = \langle x\rangle$, we obtain

$$\int_{\mathbf{Z}_p} u^{sy}\Gamma_\mu^{(i)}(y) = \sum_{\varepsilon\in\Delta}\int_{\varepsilon^{-1}+q\mathbf{Z}_p} \omega(x)^i\langle x\rangle^s\mu(x),$$

and the proposition follows from that $\mathbf{Z}_p^*$ is the disjoint union of $\varepsilon + q\mathbf{Z}_p$ for $\varepsilon \in \Delta$. □

Corollary 3.3.5.

i) If μ is a continuous distribution and $i \in \mathbf{Z}/\phi(q)\mathbf{Z}$, the function $\mathrm{Mel}_{i,\mu}(s)$ *is an analytic function of s and even $u^s - 1$.*

ii) If μ is a measure verifying $v_{\mathscr{D}_0}(\mu) \geq 0$, and if $i \in \mathbf{Z}/\phi(q)\mathbf{Z}$, then there exists $g_{i,\mu} \in \mathscr{O}_L[[T]]$ such that $\mathrm{Mel}_{i,\mu}(s) = g_{i,\mu}(u^s - 1)$.

3.4 Construction of the Kubota-Leopoldt zeta function

If $i \in \mathbf{Z}/\phi(q)\mathbf{Z}$ and $a \in \mathbf{Z}_p^*$ such that $\langle a \rangle \neq 1$, we define the function $g_{a,i}$ on $\mathbf{Z}_p$ by the formula

$$g_{a,i}(s) = \frac{1}{1-\omega(a)^{1-i}\langle a\rangle^{1-s}} \mathrm{Mel}_{-i,\mu_a}(-s) = \frac{1}{1-\omega(a)^{1-i}\langle a\rangle^{1-s}} \int_{\mathbf{Z}_p^*} \omega(a)^{-i}\langle a\rangle^{-s}\mu_a.$$

By corollary 3.3.5, $\mathrm{Mel}_{-i,\mu_a}(-s)$ is an analytic function of s. On the other hand, if $\omega(a)^{1-i} \neq 1$, the function $s \mapsto 1-\omega(a)^{1-i}\langle a\rangle^{1-s}$ is a nonzero analytic function on $\mathbf{Z}_p$ since $\langle a\rangle^s \in 1+q\mathbf{Z}_p$ and $\omega(a)^{1-i} \in \Delta - \{1\}$, therefore $\omega(a)^{1-i} \notin 1+q\mathbf{Z}_p$ and if $\omega(a)^{1-i} = 1$, the function $1-\langle a\rangle^{1-s}$ vanishes only at $s = 1$. We deduce that $g_{a,i}$ is a function continuous on $\mathbf{Z}_p - \{1\}$ and even continuous on $\mathbf{Z}_p$ if $\omega(a)^{1-i} \neq 1$.

Moreover, if $-n \equiv i \bmod \phi(q)$, we have $\omega(a)^{1-i} = \omega(a)^{1+n}$ and $\omega(x)^{-i} = \omega(x)^n$ if $x \in \mathbf{Z}_p^*$. Therefore

$$g_{a,i}(-n) = \frac{1}{1-\omega(a)^{1+n}\langle a\rangle^{1+n}} \int_{\mathbf{Z}_p^*} \omega(x)^n\langle a\rangle^n\mu_a(x) = \frac{1}{1-a^{1+n}} \int_{\mathbf{Z}_p^*} x^n\mu_a(x) = (-1)^n(1-p^n)\zeta(-n)$$

does not depend on the choice of a. If a and a' two elements of $\mathbf{Z}_p^*$, the function $g_{a,i} - g_{a',i}$ is a quotient of analytic functions on $\mathbf{Z}_p$ vanishing at infinitely many points, which implies it identical zero and the function $g_{a,i}$ is independent of choice of a. Thus we set $\zeta_{p,i} = g_{a,i}$ for any a satisfying $\langle a\rangle \neq 1$ and $\omega(a)^{1-i} \neq 1$ if $i \neq 1$ to construct Kubota-Leopoldt zeta function.

Let $F_n = \mathbf{Q}_p(\varepsilon_{p^n})$ and $F_\infty = \cup F_n$. The norm N_{F_{n+1}/F_n} induces a homomorphism from $\mu_{p^{n+1}}$ to μ_{p^n}, where μ_{p^n} be the set of p^n-th roots of unity in F_n. We denote the projective limit of μ_{p^n} with respect to N_{F_{n+1}/F_n} by μ_{p^∞} (the Tate module), which is a compact $\mathbf{Z}_p$-module.

The following theorem is due to Mazur and Wiles:

Theorem 3.4.1. *If $i \in (\mathbf{Z}/(p-1)\mathbf{Z})^*$ is odd and if $s \in \mathbf{Z}_p$, then the following two conditions are equivalent:*

i) $\zeta_{p,i}(s) = 0$;

ii) There exists an element $u \in \mu_{p^\infty}$ which is not killed by a power of p such that $\sigma \in \mathrm{Gal}(F_\infty/\mathbf{Q}_p)$ acts by the formula

$$\sigma(u) = \omega(\chi_{cycl}(\sigma))^i\langle\chi_{cycl}(\sigma)\rangle^s \cdot u.$$

3.5 The residue at $s = 1$ and the p-adic zeta function

The formal power series $\frac{\log(1+T)}{T}$ converges on open unit disk, thus it is an Amice transform of a unique distribution μ_{KL}. The Laplace transform of μ_{KL} is $\frac{t}{e^t-1} = f_0(t)$ and

$$\int_{\mathbf{Z}_p} x^n \mu_{KL} = (-1)^{n-1} n \zeta(1-n)$$

Lemma 3.5.1. $\int_{a+p^n\mathbf{Z}_p} \mu_{KL} = \frac{1}{p^n}$

Proof. Since $\int_{a+p^n\mathbf{Z}_p} \mu_{KL} = \frac{1}{p^n} \sum_{\varepsilon^{p^n}=1} \varepsilon^{-a} \mathscr{A}_{\mu_{KL}}(\varepsilon - 1)$ and since $\log \varepsilon = 0$ if ε is a root of unity of order a power of p, all terms of the sum are zero except for the term corresponding to $\varepsilon = 1$, we get the result. □

Proposition 3.5.2. *We have*

i) $\psi(\mu_{KL}) = p^{-1}\mu_{KL}$

ii) $\mathrm{Res}_{\mathbf{Z}_p^*}(\mu_{KL}) = (1 - p^{-1}\varphi)\mu_{KL}$

iii) $\int_{\mathbf{Z}_p^*} \mu_{KL} = (-1)^{n-1} n(1 - p^{n-1})\zeta(1-n)$ *if* $n \in \mathbf{N}$.

Proof. i) follows from the formula $\psi(\frac{1}{T}) = \frac{1}{T}$ (c.f. proposition 3.2.4) and $\varphi(\log(1+T)) = p\log(1+T)$ and $\psi(\varphi(a)b) = a\psi(b)$. The rest can be deduced from proposition 3.2.4. □

Theorem 3.5.3. *The p-adic zeta function* $\zeta_{p,1}$ *has a simple pole at* $s = 1$ *with residue* $1 - \frac{1}{p}$.

Proof. According to the above, we can define the function $\zeta_{p,i}$, if $i \in \mathbf{Z}/\phi(q)\mathbf{Z}$ by the formula

$$\zeta_{p,i}(s) = \frac{(-1)^{i-1}}{s-1} \mathrm{Mel}_{1-i,\mu_{KL}}(1-s) = \frac{(-1)^{i-1}}{s-1} \int_{\mathbf{Z}_p^*} \omega^{1-i} \langle x \rangle^{1-s} \mu_{KL}(x).$$

Indeed, the function is analytic on $\mathbf{Z}_p - \{1\}$ by the above formula, and takes the same value $\zeta_{p,i}(-n) = (1-p^n)\zeta(-n)$ if $n \in \mathbf{N}$ satisfies $-n \equiv i \bmod p-1$. Moreover,

$$\begin{aligned}\lim_{s\to 1}(s-1)\zeta_{p,i}(s) &= \int_{\mathbf{Z}_p^*} \omega(x)^{1-i} \mu_{KL}(x) \\ &= \sum_{\alpha \in \Delta} \omega(\alpha)^{1-i} \int_{\alpha + p\mathbf{Z}_p} \mu_{KL}(x) = \begin{cases} 1 - \frac{1}{p} & \text{if } i = 1 \\ 0 & \text{otherwise.} \end{cases}\end{aligned}$$

□

3.6 Dirichlet L-function

For χ a Dirichlet character of conductor $D>1$ and if $n\in\mathbf{Z}$, we define the Gauss sum $G(\chi)$ by

$$G(\chi)=\sum_{a \bmod D}\chi(a)e^{2\pi i\frac{a}{D}}.$$

Let

$$L(\chi,s)=\sum_{n=1}^{+\infty}\frac{\chi(n)}{n^s}=\prod_{p:prime}(1-\chi(p)p^{-s})^{-1},\ \text{for Re(s)}\geq 1,$$

be the Dirichlet L-function attached to χ. By the formula

$$\chi(n)=\frac{1}{G(\chi^{-1})}\sum_{b \bmod D}\chi^{-1}(b)e^{2\pi i\frac{nb}{D}},$$

we obtain

$$L(\chi,s)=\frac{1}{G(\chi^{-1})}\sum_{b \bmod D}\chi^{-1}(b)\frac{e^{2\pi i\frac{nb}{D}}}{n^s}.$$

Using the formula $\int_0^{+\infty}e^{-nt}t^s\frac{dt}{t}=\frac{\Gamma(s)}{n^s}$ with $\varepsilon_D:=e^{\frac{2\pi i}{D}}$, we obtain

$$\begin{aligned}L(\chi,s)=&\frac{1}{G(\chi^{-1})}\frac{1}{\Gamma(s)}\sum_{b \bmod D}\chi^{-1}(b)\int_0^{+\infty}\sum_{n=1}^{+\infty}\varepsilon_D^{nb}e^{-nt}t^s\frac{dt}{t}\\ =&\frac{1}{G(\chi^{-1})}\frac{1}{\Gamma(s)}\int_0^{+\infty}\sum_{b \bmod D}\frac{\chi^{-1}(b)}{\varepsilon_D^{-b}e^t-1}t^s\frac{dt}{t}.\end{aligned}$$

In particular, proposition 3.1.2 implies that $L(\chi,s)$ can be extended to a holomorphic function on $\mathbb{C}$. Moreover, $L(\chi,-n)=(\frac{d}{dt})^n\mathscr{L}_\chi(t)\mid_{t=0}$ where

$$\mathscr{L}_\chi(t)=\frac{-1}{G(\chi^{-1})}\sum_{b \bmod D}\frac{\chi^{-1}(b)}{\varepsilon_D^b e^t-1}.$$

3.7 p-adic L-function attached to Dirichlet character

Let χ be a Dirichlet character of conductor $D>1$ prime to p. If $\chi^{-1}(b)\neq 0$, then ε_D^b is a root of unity of order prime to p and distinct from 1, this implies $v_p(\varepsilon_D^b-1)=0$. We deduce that the power series

$$F_\chi(T)=\frac{-1}{G(\chi^{-1})}\sum_{b \bmod D}\frac{\chi^{-1}(b)}{(1+T)\varepsilon_D^b-1}=\frac{1}{G(\chi)^{-1}}\sum_{b \bmod D}\chi^{-1}(b)\sum_{n=0}^{+\infty}\frac{\varepsilon_D^{nb}}{(\varepsilon_D^b-1)^{n+1}}T^n$$

is of bounded coefficients (since $v_p(G(\chi)G(\chi^{-1}))=v_p(D)=0$) and hence there exists an Amice transform of a measure μ_χ on $\mathbf{Z}_p$ whose Laplace transform $F_\chi(e^t-1)=\mathscr{L}_\chi(t)$. We have $\int_{\mathbf{Z}_p}x^n\mu_\chi=\mathscr{L}_\chi^{(n)}(0)=$

$L(\chi,-n)$ and $v_{\mathscr{D}_0}(\mu_\chi)\geq 0$.

Definition 3.7.1. We define the p-adic L-function associated to χ as the Mellin transform of μ_χ, that is, the function $\beta\mapsto L_p(\chi\otimes\beta)$ defined by

$$L_p(\chi\otimes\beta)=\int_{\mathbf{Z}_p^*}\beta(x)\mu_\chi(x).$$

where β is a locally analytic character on $\mathbf{Z}_p^*$. On the other hand, if $i\in\mathbf{Z}/\phi(q)\mathbf{Z}$, we put

$$L_{p,i}(\chi,s)=L_p(\chi\otimes(\omega^{-i}(x)\langle x\rangle^{-s}))=\int_{\mathbf{Z}_p^*}\omega^{-i}\langle x\rangle^{-s}\mu_\chi(x).$$

Proposition 3.7.2. *If $i\in\mathbf{Z}/\phi(q)\mathbf{Z}$, the function $L_{p,i}(\chi,s)$ is an analytic function on $\mathbf{Z}_p$ and thus $L_{p,i}(\chi,-n)=(1-\chi(p)p^n)L(\chi,-n)$ if $n\in\mathbf{N}$ satisfying $-n\equiv i$ mod $\phi(q)$.*

Proof. The fact that $L_{p,i}(\chi,s)$ is an analytic function on $\mathbf{Z}_p$ follows from corollary 3.3.5. On the other hand, we have

$$\sum_{\eta^p=1}\frac{1}{(1+T)\varepsilon_D\eta-1}=p\frac{1}{(1+T)^p\varepsilon_D^{pb}-1},$$

thus we deduce the Amice transform of μ_χ restriction to $\mathbf{Z}_p^*$ is

$$\frac{-1}{G(\chi)}\sum_{b\,\mathrm{mod}\,D}\frac{\chi^{-1}(b)}{(1+T)\varepsilon_D^b-1}-\frac{\chi^{-1}(b)}{(1+T)^p\varepsilon_D^{pb}-1},$$

which can be written as $\mathscr{A}_{\mu_\chi}(T)-\chi(p)\mathscr{A}_{\mu_\chi}((1+T)^p-1)$. Hence we deduce the formula

$$\mathscr{L}_{\mathrm{Res}_{\mathbf{Z}_p^*}(\mu_\chi)}(t)=\mathscr{L}_{\mu_\chi}(t)-\chi(p)\mathscr{L}_{\mu_\chi}(pt)\quad\text{and}\quad\int_{\mathbf{Z}_p^*}x^n\mu_\chi=(1-\chi(p))L(\chi,-n),$$

and the proposition follows. □

3.8 Behavior at $s=1$ of Dirichlet L-function

By section 3.6, we have

$$\begin{aligned}L(\chi,1)=&\frac{1}{G(\chi^{-1})}\sum_{b\,\mathrm{mod}\,D}\chi^{-1}(b)\sum_{n=0}^{+\infty}\frac{\varepsilon_D^{nb}}{n}\\=&\frac{-1}{G(\chi^{-1})}\sum_{b\,\mathrm{mod}\,D}\chi^{-1}(b)\log(1-\varepsilon_D^b).\end{aligned}$$

We will establish the p-adic analogue of this formula by calculating $\int_{\mathbf{Z}_p^*}x^{-1}\mu_\chi$. To do this, we will calculate the Amice transform of $x^{-1}\mu_\chi$ and then restrict it to $\mathbf{Z}_p^*$.

Proposition 3.8.1. *The Amice transform of $x^{-1}\mu_\chi$ is*

$$\mathscr{A}_{x^{-1}\mu_\chi}(T) = \frac{-1}{G(\chi)^{-1}} \sum_{b \bmod D} \chi^{-1}(b) \log((1+T)\varepsilon_D^b - 1).$$

Proof. If μ is a distribution, the relation of Amice transform of μ and $x^{-1}\mu$ is given by

$$(1+T)\frac{d}{dT}\mathscr{A}_{x^{-1}\mu}(T) = \mathscr{A}_\mu(T).$$

Applying the operator $(1+T)\frac{d}{dT}$ on the right hand side of the equality in the proposition we obtain

$$\frac{-1}{G(\chi^{-1})} \sum_{b \bmod D} \chi^{-1}(b) \frac{(1+T)\varepsilon_D^b}{(1+T)\varepsilon_D^b - 1} = \frac{-1}{G(\chi^{-1})} \sum_{b \bmod D} \chi^{-1}(b) \left(\frac{1}{(1+T)\varepsilon_D^b - 1} + 1 \right)$$

which is equal to $\mathscr{A}_{\mu_\chi}$ since $\sum_{b \bmod D} \chi^{-1}(b) = 0$. We deduce that the two elements have the same image by $(1+T)\frac{d}{dT}$ and therefore differ by a locally constant function. To conclude, we must verify that the right hand side is given by a series which converges on the open unit disk. Since

$$\log((1+T)\varepsilon_D^b - 1) = \log(\varepsilon_D^b - 1) + \log(1 + \frac{\varepsilon_D^b T}{\varepsilon_D^b - 1}) = \log(\varepsilon_D^b - 1) + \sum_{n=1}^{+\infty} \frac{(-1)^{n-1}}{n} (\frac{\varepsilon_D^b T}{\varepsilon_D^b - 1})^n$$

and we suppose $(D,p) = 1$, we have $v_p(\varepsilon_D^b - 1) = 0$, and hence the series converges on open unit disk. $\square$

Lemma 3.8.2. *The Amice transform of the restriction of $x^{-1}\mu_\chi$ to $\mathbf{Z}_p^*$ is defined by*

$$\begin{aligned} \mathscr{A}_{\mathrm{Res}_{\mathbf{Z}_p^*}(x^{-1}\mu_\chi)}(T) =& \frac{-1}{G(\chi^{-1})} \sum_{b \bmod D} \chi^{-1}(b) \left(\log((1+T)\varepsilon_D^b - 1) - \frac{1}{p}\log((1+T)^p \varepsilon_D^{pb} - 1) \right) \\ =& \mathscr{A}_{x^{-1}\mu_\chi}(T) - \frac{\chi(p)}{p} \mathscr{A}_{x^{-1}\mu_\chi}((1+T)^p - 1). \end{aligned}$$

Proof. Use the formula for Amice transform of $\mathrm{Res}_{\mathbf{Z}_p^*}$. $\square$

By taking $T = 0$ in the above formula, we obtain

$$L_{p,1}(\chi, 1) = L_p(\chi \otimes x^{-1}) = \int_{\mathbf{Z}_p^*} x^{-1}\mu_\chi = \frac{-1}{G(\chi^{-1})}(1 - \frac{\chi(p)}{p}) \sum_{b \bmod D} \chi^{-1}(b) \log(\varepsilon_D^b - 1).$$

which differs from the complex L-function case by an Euler factor.

3.9 Twist by a character of conductor power of p

Let χ be a Dirichlet character of conductor D prime to p and β be a Dirichlet character of conductor p^k. We denote $\chi \otimes \beta$ to be the Dirichlet character of conductor Dp^k defined by $(\chi \otimes \beta)(a) = \chi(a)\beta(a)$, where χ and β are viewed as characters mod Dp^k via the projections from $(\mathbf{Z}/Dp^k\mathbf{Z})^*$ to $(\mathbf{Z}/D\mathbf{Z})^*$ and $(\mathbf{Z}/p^k\mathbf{Z})^*$.

Lemma 3.9.1. *Let $k \geq 1$, β a Dirichlet character of conductor p^k and μ a continuous distribution on $\mathbf{Z}_p$, then we have*

$$\int_{\mathbf{Z}_p} \beta(x)(1+T)^x \mu(x) = \frac{1}{G(\beta)^{-1}} \sum_{c \, mod \, p^k} \beta^{-1}(c) \mathscr{A}_\mu((1+T)\varepsilon_{p^k}^c - 1).$$

Proof. We have

$$\begin{aligned}
\int_{\mathbf{Z}_p} \beta(x)(1+T)^x \mu(x) &= \sum_{a \bmod p^k} \beta(a) \int_{a+p^k\mathbf{Z}_p} (1+T)^x \mu \\
&= \sum_{a \bmod p^k} \beta(a) \left(\frac{1}{p^k} \sum_{\eta^{p^k}=1} \eta^{-a} \mathscr{A}_\mu((1+T)\eta - 1) \right) \\
&= \sum_{\eta^{p^k}=1} \mathscr{A}_\mu((1+T)\eta - 1) \left(\frac{1}{p^k} \sum_{a \bmod p^k} \beta(a) \eta^{-a} \right),
\end{aligned}$$

and the lemma follows from the identity

$$\frac{1}{p^k} \beta^{-1}(-c) G(\beta) = \frac{\beta^{-1}(c)}{G(\beta^{-1})}.$$

□

Proposition 3.9.2. *If μ is a measure on $\mathbf{Z}_p$ with Amice transform of the form*

$$\mathscr{A}_\mu(T) = \frac{1}{G(\chi^{-1})} \sum_{b \, mod \, D} \chi^{-1}(b) F((1+T)\varepsilon_D^b - 1)$$

and if β is a Dirichlet character of conductor p^k with $k \geq 1$, then

$$\int_{\mathbf{Z}_p} \beta(x)(1+T)^x \mu(x) = \frac{1}{G((\chi \otimes \beta)^{-1})} \sum_{a \, mod \, Dp^k} (\chi \otimes \beta)^{-1}(a) F((1+T)\varepsilon_D^b \varepsilon_{p^k}^c - 1).$$

Proof. By the preceding lemma we have

$$\int_{\mathbf{Z}_p} \beta(x)(1+T)^x \mu(x) = \frac{-1}{G(\chi^{-1})G(\beta^{-1})} \sum_{b \bmod D} \sum_{c \bmod p^k} \chi^{-1}(b) \beta^{-1}(c) F((1+T)\varepsilon_D^b \varepsilon_{p^k}^c - 1).$$

Using the fact that every element of $\mathbf{Z}/Dp^n\mathbf{Z}$ can be written uniquely of the form $Dc + p^k b$, where $b \in$

$\mathbf{Z}/D\mathbf{Z}$ and $c \in \mathbf{Z}/p^k\mathbf{Z}$, we have the following formulas

$$\begin{aligned}
\varepsilon_{Dp^n}^a =& \varepsilon_D^b \varepsilon_{p^k}^c \\
(\chi \otimes \beta)^{-1}(a) =& \chi^{-1}(p^k)\beta^{-1}(D)\chi^{-1}(b)\beta^{-1}(c) \\
G((\chi \otimes \beta)^{-1}) =& \sum_{a \bmod Dp^k} (\chi \otimes \beta)^{-1}(a)\varepsilon_{Dp^k}^a \\
=& \chi^{-1}(p^k)\beta^{-1}(D)\left(\sum_{b \bmod D} \chi^{-1}(b)\varepsilon_D^b\right)\left(\sum_{c \bmod p^k} \beta^{-1}(c)\varepsilon_{p^k}^c\right) \\
=& \chi^{-1}(p^k)\beta^{-1}(D)G(\chi^{-1})G(\beta^{-1})
\end{aligned}$$

and the conclusion follows. □

Proposition 3.9.3. *If β is a non-trivial Dirichlet character of conductor a power of p and if $n \in \mathbf{N}$, then $L_p(\chi \otimes (x^n\beta)) = L(\chi \otimes \beta, -n)$*

Proof. By proposition 3.9.2 and the formula for the Amice transform of μ_χ, we have the Amice transform of $\beta\mu_\chi$ is

$$\frac{-1}{G((\chi \otimes \beta)^{-1})} \sum_{x \bmod Dp^n} \frac{(\chi \otimes \beta)^{-1}(x)}{(1+T)\varepsilon_{Dp^n}^x - 1}$$

and thus its Laplace transform is the function $\mathscr{L}_{\chi\otimes\beta}(t)$. □

Chapter 4

(φ,Γ)-modules and p-adic representations

Throughout this article, k will denote a finite field of characteristic $p > 0$, so if $W(k)$ denotes the ring of Witt vectors over k, then $F = W(k)[\frac{1}{p}]$ is a finite unramified extension of $\mathbf{Q}_p$. Let $\overline{\mathbf{Q}}_p$ be the algebraic closure $\mathbf{Q}_p$, let K be a totally ramified extension of F, and let $G_K = Gal(\overline{\mathbf{Q}}_p/K)$ be the absolute Galois group of K. Let μ_{p^n} be the group of p^n-th roots of unity; for every n, we will choose a generator $\varepsilon^{(n)}$ of μ_{p^n} with the additional requirement that $(\varepsilon^{(n)})^p = \varepsilon^{(n-1)}$, This makes $\varprojlim \varepsilon^{(n)}$ into a generator $\varprojlim \mu_{p^n} \simeq \mathbf{Z}_p(1)$. We set $K_n = K(\mu_{p^n})$ and $K_\infty = \bigcup\limits_{n\geq 0} K_n$. Recall that the cyclotomic character $\chi : G_K \to \mathbf{Z}_p^*$ is defined by the relation: $g(\varepsilon^{(n)}) = (\varepsilon^{(n)})^{\chi(g)}$ for all $g \in G_K$. The kernel of the cyclotomic character is $H_K = \mathrm{Gal}(\mathbf{Q}_p/K_\infty)$, and χ therefore identifies $\Gamma_K = G_K/H_K$ with an open subgroup of $\mathbf{Z}_p^*$.

4.1 The field $\widetilde{\mathbf{E}}$ and its subrings.

Let $\mathbf{C}_p$ be the completion of $\overline{\mathbf{Q}}_p$ for the p-adic topology and let

$$\widetilde{\mathbf{E}} = \varprojlim \mathbf{C}_p = \{(x^{(0)}, x^{(1)}, \ldots) \mid (x^{(n+1)})^p = x^{(n)}$$

and let $\widetilde{\mathbf{E}}^+$ be the set of $x \in \widetilde{\mathbf{E}}$ such that $x^{(0)} \in \mathscr{O}_{\mathbf{C}_p}$. If $x = (x^{(i)})$ and $y = (y^{(i)})$ are two elements of $\widetilde{\mathbf{E}}$, we define the sum $x + y$ and their product xy by

$$(x+y)^{(i)} = \lim_{j\to+\infty} (x^{(i+j)} + y^{(i+j)})^{p^j} \quad \mathit{and} \quad (xy)^{(i)} = x^{(i)}y^{(i)},$$

which makes $\widetilde{\mathbf{E}}$ an algebraically closed field of characteristic p. (c.f. [13] proposition 4.8) If $x = (x^{(n)}) \in \widetilde{\mathbf{E}}$, let $v_E(x) = v_p(x^{(0)})$. This is a valuation on $\widetilde{\mathbf{E}}$ and $\widetilde{\mathbf{E}}$ is complete for this valuation; the ring of integers of $\widetilde{\mathbf{E}}$ is $\widetilde{\mathbf{E}}^+$. If $\mathfrak{a}$ is an ideal satisfying $p \in \mathfrak{a} \subset \mathfrak{m}$, where $\mathfrak{m}$ is the maximal ideal of $\mathscr{O}_{\mathbf{C}_p}$, the $\widetilde{\mathbf{E}}^+$ is identified with the projective limit of A_n, where if $n \in N$, we put $A_n = \mathscr{O}_{\mathbf{C}_p}/\mathfrak{a}$ and the transition amp from A_{n+1} to A_n is given by $x \mapsto x^p$.

Let $\varepsilon = (1, \varepsilon^{(1)}, \ldots, \varepsilon^{(n)}, \ldots)$ be an element of $\widetilde{\mathbf{E}}$ such that $\varepsilon^{(1)} \neq 1$, this implies that $\varepsilon^{(n)}$ is a primitive

p^n-th root of unity if $n \geq 1$. Let $\overline{\pi} = \varepsilon - 1$, we have $v_E(\overline{\pi}) = \frac{p}{p-1}$ and let $\mathbf{E}_{\mathbf{Q}_p}$ be the subfield $\mathbf{F}_p((\overline{\pi}))$ of $\widetilde{\mathbf{E}}$. We denote by $\mathbf{E}$ the separable closure of $\mathbf{E}_{\mathbf{Q}_p}$ in $\widetilde{\mathbf{E}}$ and $\mathbf{E}^+$ (resp. $\mathfrak{m}_{\mathbf{E}}$) the ring of integers (resp. the maximal ideal of $\mathbf{E}^+$).

By ramification theory, if K is a finite extension of $\mathbf{Q}_p$, then for all $\eta > 0$, there exists $n_\eta \in N$ such that if $n \geq n_\eta$, and if $\tau \in \Gamma_{K_n}$, then $v_p(\tau(x) - x) \geq \frac{1}{p} - \eta$. In particular if $\mathfrak{a}$ is an ideal of $\mathscr{O}_{\mathbf{C}_p}$ defined by $\mathfrak{a} = \{x \in \mathscr{O}_{\mathbf{C}_p} \mid v_p(x) \geq \frac{1}{p}\}$, then $N_{K_{n+1}/K_n}(x) - x^p \in \mathfrak{a}$ if n is large enough and $x \in \mathscr{O}_{K_{n+1}}$. This allows us to construct a map ι_K from the projective limit $\varprojlim \mathscr{O}_{K_n}$ of $\mathscr{O}_{K_n}$ with respect to norm map to $\widetilde{\mathbf{E}}^+$ (field of norms), such that $u = (u^{(n)})_{n\in\mathbf{N}}$ is associated to $\iota_K(u) = (x^{(n)})_{n\in\mathbf{N}}$, where $x^{(n)}$ is the image of $u^{(n)}$ in $\mathscr{O}_{\mathbf{C}_p}/\mathfrak{a}$ if n large enough. Hence we have the following proposition:

Proposition 4.1.1. *If K is a finite extension of $\mathbf{Q}_p$, then ι_K induces a bijection from $\varprojlim \mathscr{O}_{K_n}$ to the ring of integers $\mathbf{E}_K^+$ of $\mathbf{E}_K = \mathbf{E}^{H_K}$.*

By this proposition, one can show that $\mathbf{E}_K$ is a finite separable extension of $\mathbf{E}_{\mathbf{Q}_p}$ of degree $[H_{\mathbf{Q}_p} : H_K] = [K_\infty : \mathbf{Q}_p(\mu_{p^\infty})]$ and that one can identify $\mathrm{Gal}(\mathbf{E}/\mathbf{E}_K)$ with H_K.

Remark 4.1.2.

i) If F is a finite unramified extension of $\mathbf{Q}_p$ with residue field k_F, the field $\mathbf{E}_F$ is the composition of k_F and $\mathbf{E}_{\mathbf{Q}_p}$, that is, $k_F((\overline{\pi}))$.

ii) If K is a finite extension of $\mathbf{Q}_p$ and $F = K \cap \mathbf{Q}_p^{nr}$ it maximal unramified subfield, then $\mathbf{E}_K$ is an extension of $\mathbf{E}_F$ of degree $[K_\infty : F_\infty]$ which is equal to $[K_n : F_n]$ for n large enough.

4.2 The field $\widetilde{\mathbf{B}}$ and its subrings

Let $\widetilde{\mathbf{A}} = W(\widetilde{\mathbf{E}})$ (resp. $\widetilde{\mathbf{A}}^+ = W(\widetilde{\mathbf{E}}^+)$) the Witt vectors with coefficients in $\widetilde{\mathbf{E}}$ (resp. $\widetilde{\mathbf{E}}^+$). By construction, we have $\widetilde{\mathbf{A}}/p\widetilde{\mathbf{A}} = \widetilde{\mathbf{E}}$ (resp. $\widetilde{\mathbf{A}}^+/p\widetilde{\mathbf{A}}^+ = \widetilde{\mathbf{E}}^+$). Let

$$\widetilde{\mathbf{B}} = \widetilde{\mathbf{A}}[1/p] = \{\sum_{k \gg -\infty} p^k[x_k] \mid x_k \in \widetilde{\mathbf{E}}\} \quad (\text{resp. } \widetilde{\mathbf{B}}^+ = \widetilde{\mathbf{A}}^+[1/p] = \{\sum_{k \gg -\infty} p^k[x_k] \mid x_k \in \widetilde{\mathbf{E}}^+\}),$$

where $[x] \in \widetilde{\mathbf{A}}$ is the Teichmüller lift of $x \in \widetilde{\mathbf{E}}$ (resp. $\widetilde{\mathbf{E}}^+$).

We endow $\widetilde{\mathbf{A}}$ (resp. $\widetilde{\mathbf{A}}^+$) with the topology by taking the collection of open sets $\{[\overline{\pi}]^k\widetilde{\mathbf{A}}^+ + p^n\widetilde{\mathbf{A}}\}_{k,n\geq 0}$ (resp. $\{([\overline{\pi}]^k + p^n)\widetilde{\mathbf{A}}^+\}_{k,n\geq 0}$) as family of neighborhoods of 0 and endow $\widetilde{\mathbf{B}} = \cup_{n\in\mathbf{N}} p^{-n}\widetilde{\mathbf{A}}$ (resp. $\widetilde{\mathbf{B}}^+$) the inductive limit topology. The action of $G_{\mathbf{Q}_p}$ on $\widetilde{\mathbf{E}}$ can be extended by continuity to $\widetilde{\mathbf{A}}$ and $\widetilde{\mathbf{B}}$ which commutes with the Frobenius action φ.

For F a finite unramified extension over $\mathbf{Q}_p$, let $\pi = [\varepsilon] - 1$, we define $\mathbf{A}_F$ the closure of $\mathscr{O}_F[[\pi, \pi^{-1}]]$ in $\widetilde{\mathbf{A}}$ by the above topology, thus

$$\mathbf{A}_F = \{\sum_{k\in\mathbf{Z}} a_k \pi^n \mid a_n \in \mathscr{O}_F, \lim_{k\to-\infty} v_p(a_k) = +\infty\}$$

which is a complete discrete valuation ring with residue field $\mathbf{E}_F$ and the Galois action and Frobenius action is defined by

$$\varphi(\pi) = (1+\pi)^p - 1 \quad \text{and} \quad g(\pi) = (1+\pi)^{\chi(g)} - 1 \quad g \in G_F,$$

and its fraction field $\mathbf{B}_F = \mathbf{A}_F[\frac{1}{p}]$ is stable by actions of φ and G_F.

Let $\mathbf{B}$ be the completion for the p-adic topology of the maximal unramified extension of $\mathbf{B}_F$ in $\widetilde{\mathbf{B}}$ and $\mathbf{A} = \mathbf{B} \cap \widetilde{\mathbf{A}}$. We have $\mathbf{B} = \mathbf{A}[\frac{1}{p}]$ and $\mathbf{A}$ are complete discrete valuation ring with fraction field $\mathbf{B}$ and residual field $\mathbf{E}$. We then define $\mathbf{B}^+ = \mathbf{B} \cap \widetilde{\mathbf{B}}^+$ and $\mathbf{A}^+ = \mathbf{A} \cap \widetilde{\mathbf{A}}^+$. These rings are endowed with an action of Galois and a Frobenius induced from those on $\widetilde{\mathbf{E}}$.

If K is a finite extension of $\mathbf{Q}_p$, we put $\mathbf{A}_K = \mathbf{A}^{H_K}$ and $\mathbf{B}_K = \mathbf{A}_K[1/p]$, this makes $\mathbf{A}_K$ a complete discrete valuation ring with residue field $\mathbf{E}_K$ and fraction field $\mathbf{B}_K = \mathbf{A}_K[1/p]$. On the other hand, when $K = F$, the definitions of $\mathbf{A}_F$ and $\mathbf{B}_F$ coincide with previous definitions. We put $\mathbf{A}_F^+ = (\mathbf{A}^+)^{H_F}$ and $\mathbf{B}_F^+ = (\mathbf{B}^+)^{H_F}$ then by using fields of norm above, we can show that $\mathbf{A}_F^+ = \mathscr{O}_F[[\pi]]$ and $\mathbf{B}_F^+ = F[[\pi]]$.

If L is a finite extension of K, $\mathbf{B}_L$ is an unramified extension of $\mathbf{B}_K$ of degree $[L_\infty : K_\infty]$. If L/K is a Galois extension, then the extension $\widetilde{\mathbf{B}}_L/\widetilde{\mathbf{B}}_K$ (resp. $\mathbf{B}_L/\mathbf{B}_K$) is Galois with Galois group $\mathrm{Gal}(\widetilde{\mathbf{B}}_L/\widetilde{\mathbf{B}}_K) = \mathrm{Gal}(\mathbf{B}_L/\mathbf{B}_K) = \mathrm{Gal}(\mathbf{E}_L/\mathbf{E}_K) = \mathrm{Gal}(L_\infty/K_\infty) = H_K/H_L$.

Remark 4.2.1.

i) If $\overline{\pi}_K$ is a uniformizer of $\mathbf{E}_K$, let π_K be any lifting of $\overline{\pi}_K$ in $\mathbf{A}_K$ and F' is the maximal unramified extension of F contained in K_∞. Then,

$$\mathbf{A}_K = \{\sum_{k\in\mathbf{Z}} a_k \pi_K^k \mid a_k \in \mathscr{O}_{F'}, \lim_{k\to-\infty} v_p(a_k) = +\infty\}.$$

ii) In the above construction, the correspondence $R \longrightarrow \widetilde{R}$ is obtained by making φ bijective and then do the completion with respect to the given topology on R, where $R = \{\mathbf{E}_K, \mathbf{E}, \mathbf{A}_K, \mathbf{A}, \mathbf{B}_K, \mathbf{B}\}$.

4.3 (φ, Γ)-module and Galois representations

A p-adic representation V is a finite dimensional $\mathbf{Q}_p$-vector space with a continuous linear action of G_K. It is easy to see that there is always a $\mathbf{Z}_p$-lattice of V which is stable by the action of G_K, and such lattices will be denoted by T (called a $\mathbf{Z}_p$-representation). The main strategy due to Fontaine for studying p-adic representations of a Galois group G is to construct topological $\mathbf{Q}_p$-algebras B (period rings), endowed with an action of G and some additional structures so that if V is a p-adic representation, then

$$D_B(V) := (B \otimes_{\mathbf{Q}_p} V)^G$$

is a B^G-module which inherits these structures, and so that the functor $V \mapsto D_B(V)$ gives interesting invariants of V. We say that a p-adic representation V of G is B-admissible if we have $B \otimes_{\mathbf{Q}_p} V \simeq B^d$ as $B[G]$-modules, where $d = dimV$.

Definition 4.3.1. If K is a finite extension of $\mathbf{Q}_p$, we say

i) A (φ,Γ)-module over $\mathbf{A}_K$ (resp. $\mathbf{B}_K$) is an $\mathbf{A}_K$-module of finite type (resp. a finite dimensional $\mathbf{B}_K$-vector space) equipped with a Γ_K-action and a Frobenius action φ which commutes with Γ_K.

ii) A (φ,Γ)-module D over $\mathbf{A}_K$ is *étale* if $\varphi(D)$ generates D as an $\mathbf{A}_K$-module. A (φ,Γ)-module D over $\mathbf{B}_K$ is *étale* if it has an $\mathbf{A}_K$-lattice which is *étale*, equivalently, there exists a basis $\{e_1,...,e_d\}$ over $\mathbf{B}_K$, such that the matrix of φ in terms of the basis is in $GL_d(\mathbf{A}_K)$.

If K is a finite extension of $\mathbf{Q}_p$ and V is a $\mathbf{Z}_p$-representation (resp. p-adic representation) of G_K, we put

$$D(V) = (\mathbf{A} \otimes_{\mathbf{Z}_p} V)^{H_K} \quad (\text{resp.} \quad D(V) = (\mathbf{B} \otimes_{\mathbf{Q}_p} V)^{H_K})$$

Since the action of φ commutes with G_K, $D(V)$ is a equipped with a Frobenius action φ which commutes with the residual action $G_K/H_K = \Gamma_K$. This make $D(V)$ a (φ,Γ)-module over $\mathbf{A}_K$ (resp. $\mathbf{B}_K$).

On the other hand, if V is a $\mathbf{Z}_p$-representation (resp. a p-adic representation) of G_K, then $(\mathbf{A} \otimes_{\mathbf{A}_K} D(V))^{\varphi=1}$ (resp. $(\mathbf{B} \otimes_{\mathbf{A}_K} D(V))^{\varphi=1}$) is canonically isomorphic to V as a representation of G_K. In other words, V is determined by the (φ,Γ)-module $D(V)$.

Theorem 4.3.2. *(Fontaine) The correspondence*

$$V \longmapsto D(V) = (\mathbf{A} \otimes_{\mathbf{Z}_p} V)^{H_K}$$

is an equivalence of $\otimes$ categories from the category of $\mathbf{Z}_p$-representations (resp. p-adic representation) of G_K to the category of étale (φ,Γ)-module over $\mathbf{A}_K$ (resp. $\mathbf{B}_K$), and its inverse functor is

$$D \longmapsto V(D) = (\mathbf{A} \otimes_{\mathbf{A}_K} D)^{\varphi=1}.$$

Chapter 5

(φ,Γ)-modules and Galois cohomology

5.1 The complex $C_{\varphi,\gamma}(K,V)$

Let K be an finite extension of $\mathbf{Q}_p$ such that Γ_K is isomorphic to $\mathbf{Z}_p$ (i.e. contains $\mathbf{Q}_p(\mu_p)$ if $p \geq 3$ or three quadratic ramified extensions of $\mathbb{Q}_2$ if $p=2$). Let γ be a generator of Γ_K. If V is a $\mathbf{Z}_p$-representation or p-adic representation of G_K and $f : D(V) \to D(V)$ is a $\mathbf{Z}_p$-linear map which commutes with action of Γ, we denote by $C_{f,\gamma}(K,V)$ the complex

$$0 \longrightarrow D(V) \longrightarrow D(V) \oplus D(V) \longrightarrow D(V) \longrightarrow 0$$

where the maps $D(V)$ to $D(V) \oplus D(V)$ and $D(V) \oplus D(V)$ to $D(V)$ are respectively given by

$$x \mapsto ((f-1)x, (\gamma-1)x) \quad and \quad (a,b) \mapsto (\gamma-1)a - (f-1)b$$

we denote $Z^i(C_{f,\gamma}(K,V))$ (resp. $B^i(C_{f,\gamma}(K,V))$, resp. $H^i(C_{f,\gamma}(K,V)) = \frac{Z^i(C_{f,\gamma}(K,V))}{B^i(C_{f,\gamma}(K,V))}$) the i-th cocycles (resp. coboundaries, resp. cohomology) of the complex $C_{f,\gamma}(K,V)$.

The cohomology groups of the complex $C_{f,\gamma}(K,V)$ can be canonically and functorially identified with the Galois cohomology group $H^i(K,V)$ (c.f. [14]). The following proposition gives the case of H^1.

Let $\Lambda_K = \mathbf{Z}_p[[\Gamma_K]]$ the complete group algebra of Γ_K. Since Γ_K acts continuously on $D(V)$, we can view $D(V)$ as a Λ_K-module. On the other hand, Γ_K is pro-cyclic, if γ is a generator of Γ_K and γ' is any element of Γ_K, then the element $\frac{\gamma'-1}{\gamma-1}$ of $\mathrm{Frac}(\Lambda_K)$ is indeed in Λ_K. Moreover, the G_K action factors through Γ_K on $D(V)$, so the expression $\frac{\sigma-1}{\gamma-1}y$ makes sense if $y \in D(V)$, $\sigma \in G_K$ and γ is a generator of Γ_K.

Proposition 5.1.1.

i) If $(x,y) \in Z^1(C_{\varphi,\gamma}(K,V))$ and $b \in \mathbf{A} \otimes_{\mathbf{Z}_p} V$ is a solution of $(\varphi-1)b = x$, then $\sigma \mapsto c_{x,y}(\sigma) = \frac{\sigma-1}{\gamma-1}y - (\sigma-1)b$ is a cocycle of G_K with values in V.

ii) The map which sends $(x,y) \in Z^1(C_{\varphi,\gamma}(K,V))$ to the class of $c_{x,y}$ in $H^1(K,V)$ induces an isomorphism $\iota_{\varphi,\gamma}$ of $H^1(C_{\varphi,\gamma}(K,V))$ to $H^1(K,V)$.

Proof. It clear that $\sigma \mapsto c_{x,y}(\sigma)$ is a cocycle by definition. On the other hand, we have

$$(\varphi-1)(c_{x,y}(\sigma)) = \frac{\sigma-1}{\gamma-1}((\varphi-1)y) - (\sigma-1)x = 0$$

since $(\gamma-1)x = (\varphi-1)y$. Hence $c_{x,y}(\sigma) \in (\mathbf{A} \otimes_{\mathbf{Z}_p} V)^{\varphi=1} = V$. This proves (i).

To prove (ii), suppose the image of $c_{x,y}$ in $H^1(K,V)$ is zero, there exist $z \in V$ such that

$$\frac{\sigma-1}{\gamma-1}y - (\sigma-1)(b+z) = 0 \quad \forall \sigma \in G_K.$$

We deduce that $b+z$ is stable by H_K and therefore belongs to $D(V)$. Take $\sigma = \gamma$, we have $y = (\gamma-1)(b+z)$ and hence $x = (\varphi-1)(b+z)$, which implies $(x,y) \in B^1(C_{\varphi,\gamma}(K,V))$ and the injectivity of $\iota_{\varphi,\gamma}$ follows.

To prove the surjectivity, let $c \in H^1(K,V)$ and V' an extension of $\mathbf{Z}_p$ by V corresponding to c. That is, an exact sequence

$$0 \longrightarrow V \longrightarrow V' \longrightarrow \mathbf{Z}_p \longrightarrow 0$$

such that $e \in V'$ sends to $1 \in \mathbf{Z}_p$ and $\sigma(e) = e + c_\sigma$, where $\sigma \mapsto c_\sigma$ is the cocycle of G_K represents c. Applying functor D, we get

$$0 \longrightarrow D(V) \longrightarrow D(V') \longrightarrow D(\mathbf{Z}_p) \longrightarrow 0,$$

let $\widetilde{e} \in D(V')$ be an element maps to $1 \in \mathbf{Z}_p = D(\mathbf{Z}_p)$ and let x,y be elements of $D(V)$ defined by $x = (\varphi-1)\widetilde{e}$ and $y = (\gamma-1)\widetilde{e}$. Since γ and φ commute, (x,y) is belongs to $Z^1(C_{\varphi,\gamma}(K,V))$. On the other hand, $b = \widetilde{e} - e \in \mathbf{A} \otimes_{\mathbf{Z}_p} V$ satisfies $(\varphi-1)b = x$, so we have

$$c_{x,y}(\sigma) = \frac{\sigma-1}{\gamma-1}y - (\sigma-1)b = (\sigma-1)(\widetilde{e}-b) = (\sigma-1)e = c_\sigma.$$

From this, we deduce the surjectivity of $\iota_{\varphi,\gamma}$. □

If γ' is another generator of Γ_K, then $\frac{\gamma-1}{\gamma'-1} \in \mathrm{Frac}(\Gamma_K)$ is indeed a unit in Γ_K and the diagram

$$\begin{array}{ccccccccc}
C_{\varphi,\gamma}(K,V): 0 & \longrightarrow & D(V) & \longrightarrow & D(V) \oplus D(V) & \longrightarrow & D(V) & \longrightarrow & 0 \\
& & \downarrow{\scriptstyle \frac{\gamma-1}{\gamma'-1}} & & \downarrow{\scriptstyle \frac{\gamma-1}{\gamma'-1} \oplus id} & & \downarrow{\scriptstyle id} & & \\
C_{\varphi,\gamma'}(K,V): 0 & \longrightarrow & D(V) & \longrightarrow & D(V) \oplus D(V) & \longrightarrow & D(V) & \longrightarrow & 0
\end{array}$$

is commutative. It hence induces via cohomology an isomorphism $\iota_{\gamma,\gamma'}$ from $H^1(C_{\varphi,\gamma}(K,V))$ to $H^1(C_{\varphi,\gamma'}(K,V))$.

Since we assume Γ_K is torsion free, we have $\chi(\gamma) \in 1 + p\mathbf{Z}_p$ for $\gamma \in \Gamma_K$, then there exists $k \geq 1$

such that $\log_p(\chi(\Gamma)) \in p^k\mathbf{Z}_p^*$ and we'll write $\log_p^0(\gamma) = \log_p(\chi(\gamma))/p^k$. The following lemma shows that $\log_p^0(\gamma)\iota_{\varphi,\gamma}$ does not depend on the choice of generator γ of Γ_K.

Lemma 5.1.2. *If γ and γ' are two generators of Γ_K, then the isomorphisms $\log_p^0(\gamma)\iota_{\varphi,\gamma}$ and $\log_p^0(\gamma')\iota_{\varphi,\gamma'} \circ \iota_{\gamma,\gamma'}$ from $H^1(C_{\varphi,\gamma}(K,V))$ to $H^1(K,V)$ are equal.*

Proof. If $(x,y) \in Z^1(C_{\varphi,\gamma}(K,V))$. Let b (resp. b') be element of $\mathbf{A} \otimes_{\mathbf{Z}_p} V$ verifies $(\varphi - 1)b = x$ (resp. $(\varphi - 1)b' = \frac{\gamma-1}{\gamma'-1}x$). Since $\frac{\log_p^0(\gamma)}{\gamma-1} - \frac{\log_p^0(\gamma')}{\gamma'-1} \in \mathbf{Z}_p[[\Gamma_K]]$, we can write the cocycle associates to $\log_p^0(\gamma')\iota_{\varphi,\gamma} \circ \iota_{\gamma,\gamma'}(x,y) - \log_p^0(\gamma)\iota_{\varphi,\gamma}(x,y)$ as $\sigma \mapsto (\sigma - 1)c$, where

$$c = (\frac{\log_p^0(\gamma')}{\gamma' - 1} - \frac{\log_p^0(\gamma)}{\gamma - 1})y - (\log_p^0(\gamma')b' - \log_p^0(\gamma)b)$$

and the relation $(\varphi - 1)y = (\gamma - 1)x$ implies $(\varphi - 1)c = 0$, hence $c \in V$ and the cocycle is indeed a coboundary, which leads to the conclusion. □

5.2 The operator ψ

To calculate $H^1(C_{\varphi,\gamma}(K,V))$ we have to understand the group $D(V)^{\varphi=1}$ and $\frac{D(V)}{\varphi-1}$. The problem is that the group $\frac{D(V)}{\varphi-1}$ is too complicated to write down. To solve this difficulty, we introduce the left inverse of φ.

The field $\mathbf{B}$ is an extension of degree p of $\varphi(B)$, which allows up to define the operator $\psi : \mathbf{B} \to \mathbf{B}$ by the formula $\psi(x) = \frac{1}{p}\varphi^{-1}(\mathrm{Tr}_{\mathbf{B}/\varphi(\mathbf{B})}(x))$. More explicitly, one can verify that $\{1, [\varepsilon], ..., [\varepsilon]^{p-1}\}$ is a basis of $\mathbf{A}$ over $\varphi(\mathbf{A})$ (hence $\mathbf{B}$ over $\varphi(\mathbf{B})$) so we have

$$\psi(\sum_{i=0}^{p-1}[\varepsilon]^i\varphi(x_i)) = x_0 \quad x_i \in \mathbf{B} \quad \text{and} \quad \psi(\varphi(x)) = x \quad x \in \mathbf{B}.$$

The operator ψ commute with the action of G_K and $\psi(\mathbf{A}) \subset \mathbf{A}$.

Since ψ commutes with the action of G_K, if V is a $\mathbf{Z}_p$-representation or a p-adic representation of G_K, the module $D(V)$ inherit the action of ψ and commute with Γ_K. That is, the unique map $\psi : D(V) \to D(V)$ with

$$\psi(\varphi(a)x) = a\psi(x), \quad \psi(a\varphi(a)) = \psi(a)x$$

if $a \in \mathbf{A}_K$, $x \in D(V)$.

Proposition 5.2.1. *If V is a $\mathbf{Z}_p$-representation or a p-adic representation of G_K, then $\gamma - 1$ is invertible on $D(V)^{\psi=0}$.*

Proof. See [14]. □

Lemma 5.2.2. *We have a commutative diagram of complexes*

$$\begin{tikzcd}
C_{\varphi,\gamma}(K,V): 0 \arrow[r] & D(V) \arrow[r] \arrow[d, "id"] & D(V)\oplus D(V) \arrow[r] \arrow[d, "(-\psi,id)"] & D(V) \arrow[r] \arrow[d, "-\psi"] & 0 \\
C_{\psi,\gamma}(K,V): 0 \arrow[r] & D(V) \arrow[r] & D(V)\oplus D(V) \arrow[r] & D(V) \arrow[r] & 0
\end{tikzcd}$$

which induces an isomorphism ι from $H^1(C_{\varphi,\gamma}(K,V))$ to $H^1(C_{\psi,\gamma}(K,V))$.

Proof. The commutativity of the diagram follows from definition. Since ψ is surjective, the cokernel complex is 0. The kernel complex is

$$0 \longrightarrow 0 \longrightarrow D(V)^{\psi=0} \xrightarrow{\gamma-1} D(V)^{\psi=0} \longrightarrow 0,$$

which has no cohomology by proposition 5.2.1. □

Notation 5.2.3. We denote $\iota_{\psi,\gamma}$ the isomorphism from $H^1(C_{\psi,\gamma}(K,V))$ to $H^1(K,V)$ obtained by composite $\iota_{\varphi,\gamma}$ (see proposition 5.1.1) and ι^{-1} (see lemma 5.2.2).

Remark 5.2.4. The same proof as lemma 5.1.2 shows that $\log_p^0(\gamma)\iota_{\psi,\gamma}$ does not depend on the generator γ of Γ_K.

Lemma 5.2.5. *The map which sends $(x,y)\in Z^1(C_{\varphi,\gamma}(K,V))$ to the image of x in $\frac{D(V)}{\psi-1}$ induces an exact sequence*

$$0 \longrightarrow D(V)^{\psi=1}_{\Gamma_K} \longrightarrow H^1(C_{\psi,\gamma}(K,V)) \longrightarrow \left(\tfrac{D(V)}{\psi-1}\right)^{\Gamma_K} \longrightarrow 0$$

Proof. $\bar{x}\in\frac{D(V)}{\psi-1}$ is fixed by Γ_K if and only if there exists $(x,y)\in Z^1(C_{\varphi,\gamma}(K,V))$ whose image in $\frac{D(V)}{\psi-1}$ is equal to $\bar{x}$. The kernel of the map is the sum of $B^1(C_{\psi,\gamma}(K,V))$ and the set X of elements of the form $(0,y)$ where $y\in D(V)^{\psi=1}$. One observes that $X\cap B^1(C_{\varphi,\gamma}(K,V))$ is constituted by couples of the form $(0,y)$ where $y\in(\gamma-1)D(V)^{\psi=1}$. □

Remark 5.2.6. By [14], one can show that the Herr complex $C_{\psi,\gamma}(K,V)$ indeed computes the Galois cohomology groups $H^i(K,V)$, hence we have

- $H^0(K,V)\simeq D(V)^{\psi=1,\gamma=1}\simeq D(V)^{\varphi=1,\gamma=1}$.
- $H^2(K,V)\simeq \frac{D(V)}{(\psi-1,\gamma-1)}$.
- $H^i(K,V)=0$ if $i\geq 2$.

Similar to the case of φ, the modules $D(V)^{\psi=1}$ and $\frac{D(V)}{\psi-1}$ can be interpreted naturally as Iwasawa algebra. Moreover, the module $\frac{D(V)}{\psi-1}$ is "small" compared to $\frac{D(V)}{\varphi-1}$, thus we can write $H^1(K,V)$ mainly as the submodule $D(V)^{\psi=1}$. More precisely, we have the following proposition which is proved in the subsequent two subsections.

Proposition 5.2.7. *If V is a $\mathbf{Z}_p$-representation (resp. a p-adic representation) of G_K, then*

i) $D(V)^{\psi=1}$ is compact (resp. locally compact) and generates the $\mathbf{A}_K$-module ($\mathbf{B}_K$-vector space) $D(V)$.

ii) $\frac{D(V)}{\psi-1}$ is a free $\mathbf{Z}_p$-module of finite rank (resp. a finite dimensional $\mathbf{Q}_p$-vector space).

Remark 5.2.8. Since the p-adic representation case can be deduced from the $\mathbf{Z}_p$-representation case by tensoring with $\mathbf{Q}_p$, we only need to treat the $\mathbf{Z}_p$-representation case.

5.3 The compactness of $D(V)^{\psi=1}$

The goal of this paragraph is to prove the following lemma. In particular, when $n=0$ and $N=+\infty$ is equivalent to the compactness of $D(V)^{\psi=1}$.

Lemma 5.3.1. *If V is a $\mathbf{Z}_p$-representation of G_K, $x \in D(V)$ and $N \in \mathbf{N} \cup \{+\infty\}$, the set of solutions $y \in D(V)/p^{N+1}D(V)$ of the equation $(\psi-1)y = x$ is compact.*

Let $\mathbf{A}_{Q_p}^+$ be the subring $\mathbf{Z}_p[[\pi]]$ of $\mathbf{A}_{Q_p}$, and let $A = \mathbf{A}_{Q_p}^+[[\frac{p}{\pi^{p-1}}]]$, then A is a compact subring of $\mathbf{A}_{Q_p}$ such that elements of A can be written as $x = \sum_{n\in\mathbf{Z}} x_n \pi^n$ where $(x_n)_{n\in\mathbf{Z}}$ is a sequence in $\mathbf{Z}_p$ such that we have $v_p(x_n) \geq -\frac{n}{p-1}$ if $n \leq 0$.

If $x \in \mathbf{A}_{Q_p}$, let $w_n(x) \in \mathbf{N}$ be the smallest integer k such that x belongs to $\pi^{-k}A + p^{n+1}\mathbf{A}_{Q_p}$. If x is fixed, the sequence $\{w_n(x)\}_{n\in\mathbf{N}}$ is increasing and we have

$$w_n(x+y) \leq \sup(w_n(x), w_n(y))$$

$$w_n(xy) \leq \sup_{i+j=n}(w_i(x)+w_j(y)) \leq w_n(x)+w_n(y)$$

$$w_n(\varphi(x)) \leq p w_n(x)$$

the first two inequalities follow from the fact that A is a ring and the third one holds because $\frac{\varphi(\pi)}{\pi^p}$ is an unit in A (This is the reason for working with A instead of $\mathbf{A}_{Q_p}^+$ by defining the map w_n) and such that $x \in \pi^{-k}A + p^{n+1}\mathbf{A}_{Q_p}$ implies $\varphi(x) \in \varphi(\pi)^{-k}A + p^{n+1}\mathbf{A}_{Q_p} = \pi^{-pk}A + p^{n+1}\mathbf{A}_{Q_p}$.

Lemma 5.3.2.

i) If $k \in \mathbf{N}$, then $\psi(\pi^k) \in \mathbf{A}_{Q_p}^+$ and $\psi(\pi^{-k}) \in \pi^{-k}\mathbf{A}_{Q_p}^+$

ii) $\psi(A) \subset A$.

Proof. ii) follows from i) and the definition of A. Since $\varphi(\pi) = (1+\pi)^p - 1$ is a monic polynomial of degree p in π and $[\varepsilon]^i = (1+\pi)^i$ is a monic polynomial of degree i in π, hence $\{[\varepsilon]^i\varphi(\pi)^j\}_{0\leq i\leq p-1, j\in\mathbf{N}}$

forms a basis of polynomials in π. Moreover, $\psi([\varepsilon]^i\varphi(\pi)^j)=\begin{cases}0 & i\neq 0\\ \pi^j & i=0\end{cases}$, we thus deduce that $\psi(\pi^k)\in \mathbf{A}_{Q_p}^+$ if $k\geq 0$. If $k\geq 1$, then

$$\mathrm{Tr}_{\mathbf{A}_{Q_p}/\varphi(\mathbf{A}_{Q_p})}(\pi^{-k})=\sum_{\zeta^p=1}((1+\pi)\zeta-1)^{-k},$$

which can be written in the form $\frac{P(\varphi(\pi))}{\varphi(\pi)^k}$, where P is a polynomial with coefficient in $\mathbf{Z}_p$. Thus the conclusion follows. □

Corollary 5.3.3. *If $x\in \mathbf{A}_{Q_p}$ and $n\in \mathbf{N}$, then $w_n(\psi(x))\leq 1+[\frac{w_n(x)}{p}]\leq 1+\frac{w_n(x)}{p}$.*

Proof. Since $\frac{\varphi(\pi)}{\pi^p}$ is an unit in A and $\psi(\frac{x}{\varphi(\pi)^k})=\frac{\psi(x)}{\pi^k}$, we have

$$\psi(\pi^{-kp}A+p^{n+1}\mathbf{A}_{Q_p})=\psi(\varphi(\pi)^{-k}A+p^{n+1}\mathbf{A}_{Q_p})\subset \pi^{-k}A+p^{n+1}\mathbf{A}_{Q_p},$$

the conclusion follows. □

If $U=(a_{i,j})_{1\leq i,j\leq d}\in M_d(\mathbf{A}_{Q_p})$ and $n\in\mathbf{N}$, we define $w_n(U)$ by $w_n(U)=\sup_{i,j}w_n(a_{i,j})$. Similarly if V is a $\mathbf{Z}_p$-representation of G_K and if $e_1,\dots,e_d$ is a basis of $D(V)$ over $\mathbf{A}_{Q_p}$, we put $w_n(a)=\sup_i w_n(a_i)$ if $a=\sum_{i=1}^d a_ie_i\in D(V)$. Note that w_n depends on the choice of basis $e_1,\dots,e_d$.

Lemma 5.3.4. *Let V be a $\mathbf{Z}_p$-representation of G_K, and let $e_1,\dots,e_d$ be a basis of $D(V)$ over $\mathbf{A}_{Q_p}$ and $\Phi=(a_{i,j})$ be the matrix defined by $e_j=\sum_{i=1}^d a_{i,j}\varphi(e_i)$. If $x,y\in\mathbf{A}_{Q_p}$ satisfy the equation $(\psi-1)y=x$, then $w_n(y)\leq sup\left(w_n(x),\frac{p}{p-1}(w_n(\Phi)+1)\right)$ for all $n\in\mathbf{N}$.*

Proof. Since $\varphi(e_1),\dots,\varphi(e_d)$ is a basis of $D(V)$ over $\phi(D(V))$, we can write $x=\sum_{i=1}^d x_i\varphi(e_i)$ and $y=\sum_{i=1}^d y_i\varphi(e_i)$. We have $\psi(y)=\sum_{i=1}^d\psi(y_i)e_i$ and the equation $\psi(y)-y=x$ translates to a system of equations

$$y_i=-x_i+\sum_{j=1}^d a_{i,j}\psi(y_j)\quad 1\leq j\leq d.$$

One gets the inequalities

$$w_n(y_i)\leq \sup\left(w_n(x_i),\sup_{1\leq j\leq d}(w_n(a_{i,j})+w_n(\psi(y_j)))\right)\leq \sup\left(w_n(x),w_n(\Phi)+\frac{w_n(y)}{p}+1\right)$$

for $1\leq i\leq d$, which gives us the inequality

$$w_n(y)\leq \sup\left(w_n(x),w_n(\Phi)+\frac{w_n(y)}{p}+1\right)$$

and the conclusion follows. □

We now deduce lemma 5.3.1. If $n \in \mathbf{N} \cup \{+\infty\}$, let X_n be the set of solutions of the equation $(\psi - 1)y = x$ in $D(V)/p^{n+1}D(V)$. We want to show that X_n is compact. If $n \in N$, let $r_n = \sup(w_n(x), \frac{p}{p-1}(w_n(\Phi)+1))$. The set X_n is closed (since $\psi - 1$ is continuous). By the previous lemma, the image of $(\pi^{-r_n}A)^d$ is compact since A is. If N is finite, it suffices to take $n = N$ to conclude. If $N = +\infty$, the map from $x \in X_{+\infty}$ to the sequence of its images modulo p^{n+1} allows us to identify $X_{+\infty}$ with the closed subset of compact set $\prod_{n \in \mathbf{N}} X_n$, and the conclusion follows.

5.4 The module $\frac{D(V)}{\psi-1}$

Lemma 5.4.1. *Let V be a $\mathbf{Z}_p$-representation of G_K. Then the module $\frac{D(V)}{\psi-1}$ has no nonzero p-divisible element.*

Proof. Let x be a p-divisible element of $\frac{D(V)}{\psi-1}$. For each $n \in \mathbf{N}$, there exist elements y_n, z_n of $D(V)$ such that $x = p^n y_n + (\psi - 1)z_n$. If we fix $m \in \mathbf{N}$ and if $n \geq m+1$, then z_n is a solution of the equation $\psi(z) - z = x$ mod p^{m+1}. Since the set of solutions is compact due to lemma 5.3.1, there exists a subsequence of $\{z_n\}_{n \in \mathbf{N}}$ which converges modulo p^m for all m and we have a limit Z in $D(V)$. By passing to the limit, we obtain $x = (\psi - 1)z$ and hence $x = 0$ in $\frac{D(V)}{\psi-1}$. □

Lemma 5.4.2. *If V is a $\mathbf{F}_p$-representation of G_K and $x \in \mathfrak{m}_{\mathbf{E}} \otimes V$, where $\mathfrak{m}_{\mathbf{E}}$ is the maximal ideal of $\mathbf{E}$, then the series $\sum_{n=0}^{+\infty} \varphi^n(x)$ and $\sum_{n=1}^{+\infty} \varphi^n(x)$ converges in $\mathfrak{m}_{\mathbf{E}} \otimes V$ and we have*

$$(\psi - 1)\left(\sum_{n=0}^{+\infty} \varphi^n(x)\right) = \psi(x) \quad \textit{and} \quad (\psi - 1)\left(\sum_{n=1}^{+\infty} \varphi^n(x)\right) = x.$$

Proof. If $e_1, ..., e_d$ is a basis of V over F_p and $x = x_1e_1 + ... + x_ne_d \in \mathfrak{m}_{\mathbf{E}} \otimes V$, there exists $r \geq 0$ such that if $v_E(x_i) \geq r$ for $1 \leq i \leq d$ implies that $v_E(\varphi^n(x_i)) \geq p^n r$ tends to $+\infty$ and hence we have $\varphi^n(x)$ tends to 0 as n tends to $+\infty$. We thus deduce the convergence of the series. These formulas are the consequences of the fact that ψ is a left inverse of φ. □

Lemma 5.4.3.

i) Let V be a $\mathbf{F}_p$-representation of G_K, then $\frac{D(V)}{\psi-1}$ is a finite dimensional $\mathbf{F}_p$-vector space.

ii) There exists a open subgroup of Γ_K which acts trivially on $\frac{D(V)}{\psi-1}$.

Proof. Let $M = (\mathfrak{m}_{\mathbf{E}} \otimes V)^{H_K}$, which is a lattice of $D(V)$ fixed by φ. If $x \in M$, the sereis $\sum_{n=1}^{+\infty} \varphi^n(x)$ converges in M, and by the previous lemma, we have $x = (\psi - 1)(\sum_{n=1}^{+\infty} \varphi^n(x))$, which proves that $(\psi - 1)D(V)$ contains M.

Since ψ is continuous, there exists $c \in \mathbf{N}$ such that $\psi(M) \subset \pi^{-c}M$ and since $\psi(\pi^{-pk}x) = \pi^{-k}x$, we have $\psi(\pi^{-pk}M) \subset \pi^{-k-c}M$. We deduce that if $n \geq b = [\frac{pc}{p-1}] + 1$, then $\psi = 0$ in $\frac{\pi^{-n+1}M}{\pi^{-n}M}$ and $\psi - 1$ is bijective on $\frac{\pi^{-n+1}M}{\pi^{-n}M}$. Since $D(V) = \bigcup_{n\in\mathbf{N}} \pi^{-n}M$, which implies the natural map from $\frac{\pi^{-b}M}{\psi-1}$ to $\frac{D(V)}{\psi-1}$ is an isomorphism.

To prove i), it suffices to note that $(\psi-1)M$ contained in M, which implies that $\frac{D(V)}{\psi-1}$ is a quotient of $\frac{\pi^{-b}M}{\psi-1}$. To prove ii), we note that Γ_K fixes M and hence $\pi^k M$ for all $k\in\mathbf{Z}$ and the action of Γ_K is continuous on $D(V)$ and M is closed in $D(V)$, there exists an open subgroup of Γ_K acts trivially on $\frac{\pi^{-b}M}{\psi-1}$ since the module is endowed with discrete topology. $\square$

Corollary 5.4.4. *If V is a $\mathbf{Z}_p$-representation of G_K, then $\frac{D(V)}{\psi-1}$ is a $\mathbf{Z}_p$-module of finite type.*

Proof. $\frac{D(V)}{\psi-1}/p\frac{D(V)}{\psi-1} = \frac{D(V)}{(p,\psi-1)} = \frac{D(V/p)}{\psi-1}$ is a $\mathbf{F}_p$-vector space of finite type by the preceding lemma, together with lemma 5.4.1, we get the conclusion. $\square$

Hence we deduce ii) of proposition 5.2.7 and it remains to prove that $D(V)^{\psi=1}$ generate $D(V)$. We will need the following lemma.

Lemma 5.4.5. *Let V be a $\mathbf{F}_p$-representation of G_K and X be a sub-$\mathbf{F}_p$-vector space of $D(V)^{\psi=1}$ of finite codimension. Then X contains a basis of $D(V)$ over $\mathbf{E}_K$.*

Proof. Let $M = (\mathfrak{m}_{\mathbf{E}}\otimes V)^{H_K}$ as above. Note that by lemma 5.4.2, if $x\in M^{\psi=0}$, then the series $\sum_{n=0}^{+\infty}\varphi^n(x)$ converges in $D(V)$ to an element of $D(V)^{\psi=1}$. We denote it by $eul(x)$. Let $e_1,\dots,e_d$ be a basis of M over $\mathbf{E}_K^+$. Let r the codimension of X in $D(V)^{\psi=1}$. If $1\le i\le d$ and $j\ge 1$, let $z_{i,j} = eul(\varepsilon\varphi(\pi^j e_i))$. If i and $n\ge 1$ are fixed, the $\{z_{i,j}\}_{n\le j\le n+r}$ form a set of $r+1$ elements in $D(V)^{\psi=1}$ and since X is of codimension r in $D(V)^{\psi=1}$, we can find elements $\{a_{i,j}^{(n)}\}_{0\le j\le r}$ of $\mathbf{F}_p$ such that $f_{i,n} = \sum_{j=0}^r a_{i,j}^{(n)} z_{i,j+n}$ belongs to X. Let $\beta_{i,n} = \pi^n\sum_{j=0}^r a_{i,j}^{(n)}\pi^j$. We have $\lim_{n\to+\infty}(\varepsilon\varphi(\beta_{i,n}))^{-1}f_{i,n} = \varphi(e_i)$, which implies that the determinant of $f_{1,n},\dots,f_{d,n}$ in the basis $\varphi(e_1),\dots,\varphi(e_d)$ is nonzero if $n\gg 0$ and we have $f_{1,n},\dots,f_{d,n}$ form a basis of $D(V)$ over $\mathbf{E}_K$ if n is large enough. The lemma follows. $\square$

Corollary 5.4.6. *If V is a $\mathbf{Z}_p$-representation of G_K, then $D(V)^{\psi=1}$ generates the $\mathbf{A}_K$-module $D(V)$.*

Proof. The snake lemma shows that the cokernel of the injective map $D(V)^{\psi=1}/pD(V)^{\psi=1}$ to $D(V/p)^{\psi=1}$ is identified with the p-torsion part of $D(V)/(\psi-1)$. In particular, it is of finite dimension over $\mathbf{F}_p$. By the preceeding lemma, we have $D(V)^{\psi=1}/pD(V)^{\psi=1}$ contains a basis of $D(V/p)$ over $\mathbf{E}_K$, which lifts to a basis in $D(V)^{\psi=1}$ that generates $D(V)$ over $\mathbf{A}_K$. $\square$

Chapter 6

Iwasawa theory and p-adic representations

6.1 Iwasawa cohomology

Recall that if $n \in \mathbf{N}$, we denote by K_n the field $K(\varepsilon^{(n)}) = K(\mu_{p^n})$. On the other hand, if $n \geq 1$ (resp. $n \geq 2$ if $p = 2$), the group Γ_{K_n} is isomorphic to Z_p. We choose a generator γ_1 of Γ_{K_1} and put $\gamma_n = \gamma_1^{[K_N:K_1]}$ if $n \geq 1$ (if $p = 2$, we can start from $n = 2$), this makes γ_n a generator of Γ_{K_n}.

Let V be a p-adic representation of G_K. The Iwasawa cohomology groups $H^i_{\mathrm{Iw}}(K,V)$ are defined by $H^i_{\mathrm{Iw}}(K,V) = \mathbf{Q}_p \otimes_{\mathbf{Z}_p} H^i_{\mathrm{Iw}}(K,T)$ where T is any G_K-stable lattice of V and where

$$H^i_{\mathrm{Iw}}(K,T) = \varprojlim_{\mathrm{cor}_{K_{n+1}/K_n}} H^i(K_n,T)$$

Each of the cohomology group $H^i(K,T)$ is a $\mathbf{Z}_p[\Gamma_K/\Gamma_{K_n}]$-module, and $H^i_{\mathrm{Iw}}(K,T)$ is then endowed with the structure of a Λ_K-module. Roughly speaking, theses cohomology groups are where Euler systems live (at least locally).

If V is a Z_p-representation or a p-adic representation of G_K, we endow $\Lambda_K \otimes_{\mathbf{Z}_p} V$ with the natural diagonal action of G_K. If we consider $\Lambda_K \otimes_{\mathbf{Z}_p} V$ as the space of measures of Γ_K with values in V (see section **??**), the measure $\sigma(\mu)$ is the map sends a continuous map $f : \Gamma_K \mapsto V$ to the element

$$\int_{\Gamma_K} f(x)\sigma(\mu) = \sigma(\int_{\Gamma_K} f(\sigma x)\mu) \in V$$

If V is a $\mathbf{Z}_p$-representation or a p-adic representation of G_K and $k \in \mathbf{Z}$, we denote by $V(k)$ the twist of V by the k-th power of the cyclotomic character and if $x \in V$, we denote $x(k)$ its image in $V(k)$.

If $\mu \in H^m(K, \Lambda_K \otimes_{\mathbf{Z}_p} V)$ and if $\tau \mapsto \mu_{\tau_1,\ldots,\tau_m}$ is a continuous m-cocycle represents μ, then $\tau \mapsto (\int_{\Gamma_{K_n}} \chi(x)^k \mu_{\tau_1,\ldots,\tau_m})(k)$ is a m-cocycle of G_K with values in $V(k)$ whose class $(\int_{\Gamma_{K_n}} \chi(x)^k \mu)(k)$ in $H^m(K_n, V(k))$ does not depend on the choice of cocycle representing μ.

Shapiro's lemma allows us to replace the projective limit in the definition of $H^m_{\mathrm{Iw}}(K,V)$ by a group cohomology.

Proposition 6.1.1. *Let V be a $\mathbf{Z}_p$-representation or a p-adic representation of G_K.If $m \in \mathbf{N}$ and $k \in \mathbf{Z}$, the map which sends μ to $(\ldots, \int_{K_n} \chi(x)^k \mu(k), \ldots)$ is an isomorphism from $H^i(K, \Gamma_K \otimes_{\mathbf{Z}_p} V)$ to $H^i_{\mathrm{Iw}}(K, V(k))$. In particular, if $k \in \mathbf{Z}$, the cohomology groups $H^m_{\mathrm{Iw}}(K,V)$ and $H^m_{\mathrm{Iw}}(K,V(k))$ are isomorphic.*

Proof. The case of $\mathbf{Q}_p$ follows from the case of $\mathbf{Z}_p$ by tensoring $with\mathbf{Q}_p$. If M is a G_{K_n}-module, we denote $\mathrm{Ind}_{K_n}^K M$ the set of continuous maps from G_K to M satisfying $a(hx) = ha(x)$ if $h \in G_{K_n}$. The module $\mathrm{Ind}_{K_n}^K M$ is provided with a continuous action of G_K, the image ga of a by $g \in G_K$, is given by the formula $(ga)(x) = a(xg)$. If M is a G_K module, and $a \in \mathrm{Ind}_{K_n}^K M$, the map sends $x \in G_K$ to $x^{-1}(a(x))$ is constant modulo G_{K_n}, and the map $\mathrm{Ind}_{K_n}^K M \to \mathbf{Z}_p[\mathrm{Gal}(K_n/K)] \otimes M$ $a \mapsto \sum_{x \in \mathrm{Gal}(K_n/K)} x^{-1}(ax)\delta_{x^{-1}}$ is an isomorphism of G_K-modules. By Shapiro's lemma, we have a canonical isomorphism from $H^i(K, \mathbf{Z}_p[\mathrm{Gal}(K_n/K)] \otimes M)$ to $H^i(K_n, M)$. On the other hand, the corestriction map from $H^i(K_{n+1}, M)$ to $H^i(K_n, M)$ is derived from the previous isomorphosm and the natural map from $\mathbf{Z}_p[\mathrm{Gal}(K_{n+1}/K)]$ to $\mathbf{Z}_p[\mathrm{Gal}(K_n/K)]$. we thus obtain a natural map

$$H^i(K, \Lambda_K \otimes M) \to \varprojlim H^i(K, (\Lambda/\omega_n) \otimes M) \simeq \varprojlim H^i(K_n, M).$$

It remains to show that this map is an isomorphism.

Surjectivity is a obvious. To prove injectivity, it suffices to verify that the map from $H^i(K, \Lambda_K \otimes M)$ to $H^i(K, \Lambda/(\omega_n, p^n) \otimes M)$ is injective. Since $\Lambda_K = \varprojlim \Lambda_K/(\omega_n, p^n)$, it suffices to show that $H^i(K, (\Lambda/\omega_n, p^n) \otimes M)$ satifies the Mittag-Leffler condition (c.f. [15]), which is obvious since the group is finite. $\square$

By lemma 5.2.5, the map ι_{ψ,γ_n} identifies $\frac{D(V)^{\psi=1}}{\gamma_n - 1}$ with a subgroup of $H^1(K_n, V)$ if Γ_{K_n} is torsion free, we thus obtain a map $h^1_{K_n,V} : D(V)^{\psi=1} \to H^1(K_n, V)$. Explicitly, if $y \in D(V)^{\psi=1}$, then $(\varphi - 1)y \in D(V)^{\psi=0}$ and since $\gamma_n - 1$ is invertible on $D(V)^{\psi=0}$, there exists $x_n \in D(V)^{\psi=0}$ satisfying $(\gamma_n - 1)x_n = (\varphi - 1)y$ (i.e. $(x_n, y) \in Z^1_{\varphi,\gamma_n}(K_n, V)$). On the other hand, lemma 5.1.2 implies that the image $\iota_{\psi,n}(y)$ and $\log^0_p(\gamma_n)\iota_{\varphi,\gamma_n}(x_n, y)$ in $H^1(K_n, V)$ does not depend on the choice of γ.

By lemma 6.2.1 below, we have $\mathrm{cor}_{K_{n+1}/K_n} \circ h^1_{K_{n+1},V} = h^1_{K_n,V}$. On the other hand, if Γ_{K_n} is no longer torsion free, we define $h^1_{K_n,V}$ by the relation $\mathrm{cor}_{K_{n+1}/K_n} \circ h^1_{K_{n+1},V} = h^1_{K_n,V}$. Thus we associate every element in $D(V)^{\psi=1}$ to a collection of Galois cohomology classes $h^1_{K_n,V}(y) \in H^1(K_n, V)$ for $n \geq 1$. The main result of this section is:

Theorem 6.1.2. *(Fontaine) Let V be a $\mathbf{Z}_p$-representation or a p-adic representation of G_K.*

i) If $y \in D(V)^{\psi=1}$, then $(\ldots, h^1_{K_n,V}(y), \ldots) \in H^1_{\mathrm{Iw}}(K, V)$.

ii) The map $\mathrm{Log}^*_{V^*(1)} : D(V)^{\psi=1} \to H^1_{\mathrm{Iw}}(K, V)$ defined by previous paragraph is an isomorphism.

6.2 Corestriction and (φ, Γ)-modules

i) of theorem 6.1.2 is a consequence of the following lemma.

Lemma 6.2.1. *If $n \geq 1$, let*

$$T_{\gamma,n} : H^1(C_{\varphi,\gamma_n}(K_n,V)) \to H^1(C_{\varphi,\gamma_{n-1}}(K_{n-1},V))$$

be the map induced by $(x,y) \in Z^1(C_{\varphi,\gamma_n}(K_n,V))$ to $(\frac{\gamma_n-1}{\gamma_{n-1}-1}x, y) \in Z^1(C_{\varphi,\gamma_{n-1}}(K_{n-1},V))$. Then the diagram

$$\begin{array}{ccc} H^1(C_{\varphi,\gamma_n}(K_n,V)) & \xrightarrow{T_{\gamma,n}} & H^1(C_{\varphi,\gamma_{n-1}}(K_{n-1},V)) \\ \downarrow{\scriptstyle \iota_{\varphi,\gamma_n}} & & \downarrow{\scriptstyle \iota_{\varphi,\gamma_{n-1}}} \\ H^1(K_n,V) & \xrightarrow{cor_{K_n/K_{n-1}}} & H^1(K_{n-1},V) \end{array}$$

is commutative.

Proof. Recall that if G is a group, M is a G-module and H a subgroup of finite index of G, the corestriction map $\mathrm{cor} : H^1(H,N) \to H^1(G,M)$ can be written in the following way: let $X \subset G$ is a system of representatives of G/H and, if $g \in G$, let τ_g is the permutation of X defined by $\tau_g(x)H = gxH$ if $x \in X$. If $c \in H^1(H,M)$ and $h \mapsto c_h$ is a cocycle which represents c, then

$$g \to \sum_{x \in X} \tau_g(x)(c_{\tau_g(x)^{-1}gx})$$

is a cocycle of G with values in M whose class in $H^1(G,M)$ does not depend on the choice of X and is equal to $\mathrm{cor}(c)$.

If N is a G-submodule of M such that the image of c in $H^1(H,N)$ is trivial (i.e. there exists $b \in N$ such that we have $c_h = (h-1)b$ for all $h \in H$), then $\mathrm{cor}(c)$ is the class of the cocycle $g \mapsto (g-1)(\sum_{x\in X} xb)$.

In particular, we put $G = G_{K_{n-1}}$, $H = G_{K_n}$ and, if $\widetilde{\gamma}_{n-1}$ is a lift of γ_{n-1} in $G_{K_{n-1}}$, we take $X = \{1, \widetilde{\gamma}_{n-1}, ..., \widetilde{\gamma}_{n-1}^{p-1}\}$. Take $N = \mathrm{Frac}(\mathbf{Z}_p[[G_{K_{n-1}}]]) \otimes_{\mathbf{Z}_p[[G_{K_{n-1}}]]} (A \otimes_{\mathbf{Z}_p} V)$. If $(x,y) \in Z^1(C_{\varphi,\gamma}(K_n,V))$ and if $b \in \mathbf{A} \otimes T$, the cocycle $c_{x,y}$ is given by the formula $c_{x,y}(\tau) = (\tau-1)c$, where $c = \frac{y}{\widetilde{\gamma}_n-1} - b \in N$. It follows that $\mathrm{cor}_{K_n/K_{n-1}}(\iota_{\varphi,\gamma_n}(x,y))$ is represented by the cocycle

$$\tau \to (\sigma-1)(\sum_{i=0}^{p-1} \widetilde{\gamma}_{n-1}^i c) = (\sigma-1)(\frac{y}{\widetilde{\gamma}_{n-1}-1} - \sum_{i=0}^{p-1} \widetilde{\gamma}_{n-1}^i b)$$

and since

$$(\varphi-1)(\sum_{i=0}^{p-1} \widetilde{\gamma}_{n-1}^i b) = \sum_{i=0}^{p-1} \widetilde{\gamma}_{n-1}^i((\varphi-1)b) = \frac{\widetilde{\gamma}_{n-1}^p - 1}{\widetilde{\gamma}_{n-1}-1}x = \frac{\gamma_n - 1}{\gamma_{n-1}-1}x,$$

we see that this cocycle is just $\iota_{\varphi,\gamma_{n-1}}(T_{\gamma,n}(x,y))$, and the conclusion follows. $\square$

Remark 6.2.2. One can also hide the explicit calculation by noting that, if $n \geq 1$, the diagram

$$\begin{tikzcd}
C_{\varphi,\gamma_n}(K_n,V): 0 \arrow[r] & D(V) \arrow[r] \arrow[d, "\frac{\gamma_n-1}{\gamma_{n-1}-1}"] & D(V)\oplus D(V) \arrow[r] \arrow[d, "(\frac{\gamma_n-1}{\gamma_{n-1}-1}, id)"] & D(V) \arrow[r] \arrow[d, "id"] & 0 \\
C_{\varphi,\gamma_{n-1}}(K_n,V): 0 \arrow[r] & D(V) \arrow[r] & D(V)\oplus D(V) \arrow[r] & D(V) \arrow[r] & 0
\end{tikzcd}$$

is commutative and functorial on V and induces a homomorphism of cohomology group from $H^*(K_n,\cdot)$ to $H^*(K_{n-1},\cdot)$ which coincides with with the corestriction map at $* = 0$ and hence is corestriction map.

6.3 Interpretation of $D(V)^{\psi=1}$ and $\frac{D(V)}{\psi-1}$ in Iwasawa theory

We now turn to the proof of ii) of theorem 6.1.2. Lemma 6.2.1 implies that the map $(\iota_{\psi,\gamma_n})_{n\in\mathbf{N}}$ induces an isomorphism from the projective limit of $H^1(C_{\psi,\gamma_n}(K_n,V))$ with respect to the map $T_{\gamma,n}$ to $H^1_{\mathrm{Iw}}(K,V)$. On the other hand, lemma 5.2.5, implies by passing to the projective limit, that we have an exact sequence:

$$0 \longrightarrow \varprojlim \frac{D(V)^{\psi=1}}{\gamma_n-1} \longrightarrow \varprojlim H^1(C_{\psi,\gamma_n}(K_n,V)) \longrightarrow \varprojlim (\frac{D(V)}{\psi-1})^{\Gamma_{K_n}}$$

The projective limit of $\frac{D(V)^{\psi=1}}{\gamma_n-1}$ is take with respect to the natural maps induced by the identity on $D(V)^{\psi-1}$ and that of $(\frac{D(V)}{\psi-1})^{\gamma_n=1}$ with respect to the map

$$\frac{\gamma_{n+1}-1}{\gamma_n-1}: (\frac{D(V)}{\psi-1})^{\gamma_n=1} \to (\frac{D(V)}{\psi-1})^{\gamma_{n-1}=1}.$$

Hence ii) of theorem 6.1.2 holds by the following proposition:

Proposition 6.3.1. *If V is a $\mathbf{Z}_p$-representation of G_K, then*

i) The natural map from $D(V)^{\psi=1}$ to $\varprojlim \frac{D(V)^{\psi=1}}{\gamma_n-1}$ is an isomorphism.

ii) $\varprojlim (\frac{D(V)}{\psi-1})^{\gamma_n=1} = 0$

Proof. i) Let $(x_n)_{n\in\mathbf{N}} \in \varprojlim \frac{D(V)^{\psi=1}}{\gamma_n-1}$. The compactness of $D(V)^{\psi=1}$ [c.f. proposition 5.2.7 i)] implies that the sequence x_n admits an accumulation point $x \in D(V)^{\psi=1}$ and the image of x in $\varprojlim \frac{D(V)^{\psi=1}}{\gamma_n-1}$ is by construction $(x_n)_{n\in\mathbf{N}}$. The natural map from $D(V)^{\psi=1}$ to $\varprojlim \frac{D(V)^{\psi=1}}{\gamma_n-1}$ is hence surjective.

By the compactness of $D(V)^{\psi=1}$ and the fact that if $x \in D(V)$, then $(\gamma_n-1)x$ tends to 0 when n tends to $+\infty$ implies that if U is open in $D(V)$ fixed by Γ, then there exist $n_U \in \mathbf{N}$ such that $(\gamma_n-1)D(V)^{\psi=1} \subset U$ if $n \geq n_V$. This implies that $\bigcap_{n\in\mathbf{N}}(\gamma_n-1)(D(V)^{\psi=1}) = \{0\}$ and we prove the injectivity.

ii) $\frac{D(V)}{\psi-1}$ is a free $\mathbf{Z}_p$-module of finite rank [c.f. proposition 5.2.7 ii)], the sequence $(\frac{D(V)}{\psi-1})^{\gamma_n=1}$ is stationary since it is increasing. One can deduce the fact that there exists $n_0 \in \mathbf{N}$ such that $\frac{\gamma_n-1}{\gamma_{n-1}-1}$ is multiplication by p on $(\frac{D(V)}{\psi-1})^{\gamma_n=1}$ if $n \geq n_0$, which proves the statement since $\frac{D(V)}{\psi-1}$ has no p-divisible element [c.f. lemma 5.4.1]. $\square$

Remark 6.3.2. We have $H^2(K_n, V) \cong H^2(C_{\psi,\gamma_n}(K_n, V)) = \frac{D(V)}{(\psi-1,\gamma_n-1)}$. We deduce that if V is a $\mathbf{Z}_p$-representation, then $H^2_{\mathrm{Iw}}(K, V)$ is the projective limit of $\frac{D(V)}{(\psi-1,\gamma_n-1)}$ since $\frac{D(V)}{\psi-1}$ is a $\mathbf{Z}_p$-module of finite type on which Γ_K acts continuously by ii) of lemma 5.4.3, the natural map from $\frac{D(V)}{\psi-1}$ to the projective limit of $\frac{D(V)}{(\psi-1,\gamma_n-1)}$ is an isomorphism, this proves that $\frac{D(V)}{\psi-1}$ is identified with $H^2_{\mathrm{Iw}}(K, V)$.

By the above proposition, one can summarize the above results as follows:

Corollary 6.3.3. *The complex of $\mathbf{Q}_p \otimes_{\mathbf{Z}_p} \Lambda_K$-modules*

$$0 \longrightarrow D(V) \xrightarrow{1-\psi} D(V) \longrightarrow 0$$

computes the Iwasawa cohomology of V. i.e. $H^1_{\mathrm{Iw}}(K, V) = D(V)^{1-\psi}$ and $H^2_{\mathrm{Iw}}(K, V) = \frac{D(V)}{\psi-1}$

There is a natural projection map $\mathrm{pr}_{K_n,V} : H^i_{\mathrm{Iw}}(K, V) \to H^i(K_n, V)$ and when $i = 1$ it is of course equal to the composition of:

$$H^1_{\mathrm{Iw}}(K, V) \longrightarrow D(V)^{\psi=1} \xrightarrow{h^1_{K_n,V}} H^1(K_n, V).$$

The $H^i_{\mathrm{Iw}}(K, V)$ have been studied in detail by Perrin-Riou, who proved the following

Proposition 6.3.4. *If V is a p-adic representation of G_K, then*

- *i) The torsion submodule of $H^1_{\mathrm{Iw}}(K, V)$ is a $\mathbf{Q}_p \otimes_{\mathbf{Z}_p} \Lambda_K$-module isomorphic to V^{H_K} and $H^1_{\mathrm{Iw}}(K, V)/V^{H_K}$ is a free $\mathbf{Q}_p \otimes_{\mathbf{Z}_p} \Lambda_K$-module whose rank is $[K : \mathbf{Q}_p] dim_{\mathbf{Q}_p} V$.*
- *ii) $H^2_{\mathrm{Iw}}(K, V)$ is isomorphic to $V(-1)^{H_K}$ as $\mathbf{Q}_p \otimes_{\mathbf{Z}_p} \Lambda_K$-module. In particular, it is torsion.*
- *iii) $H^i_{\mathrm{Iw}}(K, V) = 0$ when $i \neq 1, 2$.*

Proof. See [18, 3.2.1]. $\square$

Chapter 7

De Rham representations and overconvergent representations

7.1 De Rham representations and crystalline representations

Recall $\widetilde{\mathbf{A}}^+ = W(\widetilde{\mathbf{E}}^+)$, the ring of Witt vectors with coefficients in $\widetilde{\mathbf{E}}^+$. We define the homomorphism $\theta : \widetilde{\mathbf{A}}^+ \to \mathscr{O}_{\mathbf{C}_p}$ by

$$\theta(\sum_{k\geq 0} p^k[x_k]) = \sum_{k\geq 0} p^k x_k^{(0)}$$

One can show that this is a surjective map and $\ker(\theta : \widetilde{\mathbf{A}}^+ \to \mathscr{O}_{\mathbf{C}_p})$ is generated by $\omega = \pi/\varphi^{-1}(\pi)$.

We can extend θ to a homomorphism from $\widetilde{\mathbf{B}}^+ = \widetilde{\mathbf{A}}^+[\frac{1}{p}]$ to $\mathbf{C}_p$, and we denote by $\mathbf{B}_{\mathrm{dR}}^+$ the ring $\varprojlim \widetilde{\mathbf{B}}^+/(\ker\theta)^n$, thus θ can be extended by continuity to a homomorphism from $\mathbf{B}_{\mathrm{dR}}^+$ to $\mathbf{C}_p$. This makes $\mathbf{B}_{\mathrm{dR}}^+$ a discrete valuation ring with maximal ideal $\ker\theta$ and residue field $\mathbf{C}_p$. The action of $G_{\mathbf{Q}_p}$ on $\widetilde{\mathbf{A}}^+$ extends by continuity to an action of $G_{\mathbf{Q}_p}$ on $\mathbf{B}_{\mathrm{dR}}^+$. The series $\log[\varepsilon] = \sum_{n=1}^{+\infty} \frac{(-1)^{n-1}}{n}\pi^n$ converges in $\mathbf{B}_{\mathrm{dR}}^+$ to an element which we denote by t, which is a generator of $\ker\theta$ with a $G_{\mathbf{Q}_p}$ action defined by $\sigma(t) = \chi(\sigma)t$ where $\sigma \in G_{\mathbf{Q}_p}$. This element can be viewed as a p-adic analogue of $2\pi i$.

We put $\mathbf{B}_{\mathrm{dR}} = \mathbf{B}_{\mathrm{dR}}^+[t^{-1}]$, this makes $\mathbf{B}_{\mathrm{dR}}$ a field with filtration defined by $\mathrm{Fil}^i\mathbf{B}_{\mathrm{dR}} = t^i\mathbf{B}_{\mathrm{dR}}^+$. This filtration is stable by the action of G_K.

Let K be a finite extension of $\mathbf{Q}_p$ and V be a p-adic representation of G_K. We say that V is de Rham if it is $\mathbf{B}_{\mathrm{dR}}$-admissible, which is equivalent to the assertion that K-vector space $\mathbf{D}_{\mathrm{dR}}(V) = (\mathbf{B}_{\mathrm{dR}} \otimes_{\mathbf{Q}_p} V)^{G_K}$ is of dimension $d = \dim_{\mathbf{Q}_p}(V)$. On the other hand, $\mathbf{D}_{\mathrm{dR}}(V)$ is endowed with a filtration induced by $\mathbf{B}_{\mathrm{dR}}$. We have $\mathrm{Fil}^i\mathbf{D}_{\mathrm{dR}}(V) = \mathbf{D}_{\mathrm{dR}}(V)$ if $i \ll 0$ and $\mathrm{Fil}^i\mathbf{D}_{\mathrm{dR}}(V) = \{0\}$ if $i \gg 0$.

The ring $\mathbf{B}_{\mathrm{cris}}^+$ is defined by

$$\mathbf{B}_{\mathrm{cris}}^+ = \{\sum_{n\geq 0} a_n \frac{\omega^n}{n!} \mid a_n \in \widetilde{\mathbf{B}}^+ \text{ is a sequence converging to } 0\},$$

and $\mathbf{B}_{\text{cris}} = \mathbf{B}^+_{\text{cris}}[\frac{1}{t}]$. The ring $\mathbf{B}_{\text{cris}}$ is a subring of $\mathbf{B}_{\text{dR}}$ stable under $G_{\mathbf{Q}_p}$ containing t and the action of φ on $\widetilde{\mathbf{B}}^+$ is extended by continuity to an action of $\mathbf{B}^+_{\text{cris}}$. In particular, we have $\varphi(t) = pt$.

We say V is crystalline if it is $\mathbf{B}_{\text{cris}}$-admissible, which is equivalent to the assertion that $F = K \cap \mathbf{Q}_p^{ur}$-vector space $\mathbf{D}_{\text{cris}}(V) = (\mathbf{B}_{\text{cris}} \otimes V)^{G_K}$ is of dimension $d = \dim_{\mathbf{Q}_p}(V)$. The action of φ on $\mathbf{B}_{\text{cris}}$ commutes with the action of $G_{\mathbf{Q}_p}$, which endows $\mathbf{D}_{\text{cris}}(V)$ a natural semi-linear action of φ. i.e $\varphi(fd) = \varphi(f)\varphi(d)$ where $f \in F$ and $d \in \mathbf{D}_{\text{cris}}(V)$.

We have $(\mathbf{B}_{\text{dR}} \otimes_{\mathbf{Q}_p} V)^{G_K} = \mathbf{D}_{\text{dR}}(V) = K \otimes_F \mathbf{D}_{\text{cris}}(V)$, thus the crystalline representation is de Rham and $K \otimes_F \mathbf{D}_{\text{cris}}(V)$ is a filtered K-vector space. Hence if V is de Rham (resp. crystalline) and $k \in \mathbf{Z}$, so is $V(k)$, and we have $\mathbf{D}_{\text{dR}}(V(k)) = t^{-k}\mathbf{D}_{\text{dR}}(V)$ (resp. $\mathbf{D}_{\text{cris}}(V(k)) = t^{-k}\mathbf{D}_{\text{cris}}(V)$).

7.2 Overconvergent elements

Every element x of $\widetilde{\mathbf{B}}$ can be written uniquely in the form $\sum_{k \gg -\infty} p^k [x_k]$, where x_k is an element of $\widetilde{\mathbf{E}}$ and the series converges in $\mathbf{B}^+_{\text{dR}}$ if and only if the series $\sum_{k \gg -\infty} p^k x_k^{(0)}$ converges in $\mathbf{C}_p$, which is equivalent to $k + v_E(x_k)$ tends to $+\infty$ as k tends to $+\infty$. More generally, if $n \in \mathbf{N}$, $\varphi^{-n}(x)$ converges if and only if $k + p^{-n} v_E(x_k)$ tends to $+\infty$ as k tends to $+\infty$.

For $r \geq 0$, we set

$$\widetilde{\mathbf{B}}^{\dagger,r} = \{x \in \widetilde{\mathbf{B}} \mid \lim_{k \to +\infty} v_E(x_k) + \frac{pr}{p-1}k = +\infty\}.$$

This makes $\widetilde{\mathbf{B}}^{\dagger,r}$ into an intermediate ring between $\widetilde{\mathbf{B}}^+$ and $\widetilde{\mathbf{B}}$. We denote $\widetilde{\mathbf{B}}^\dagger = \cup_{r \geq 0} \widetilde{\mathbf{B}}^{\dagger,r}$, which is a subfield of $\widetilde{\mathbf{B}}$ with action of G_K and φ. On the other hand, we have a well-defined injective map $\varphi^{-n} : \widetilde{\mathbf{B}}^{\dagger,r_n} \to \mathbf{B}^+_{\text{dR}}$, where $r_n = p^{n-1}(p-1)$.

We denote $\widetilde{\mathbf{A}}^{\dagger,r} = \widetilde{\mathbf{B}}^{\dagger,r} \cap \widetilde{\mathbf{A}}$, that is, the subring of elements $x = \sum_{k=0}^{+\infty} p^k [x_k]$ of $\widetilde{\mathbf{A}}$ such that $v_E(x_k) + \frac{pr}{p-1}k$ tends to $+\infty$ as k tends to $+\infty$. We have $\widetilde{\mathbf{B}}^{\dagger,n} = \widetilde{\mathbf{A}}^{\dagger,n}[\frac{1}{p}]$.

By putting $\mathbf{B}^\dagger = \mathbf{B} \cap \widetilde{\mathbf{B}}^\dagger$, $\mathbf{A}^{\dagger,r} = \mathbf{A} \cap \widetilde{\mathbf{A}}^{\dagger,r}$ and $\mathbf{B}^{\dagger,r} = \mathbf{B} \cap \widetilde{\mathbf{B}}^{\dagger,r}$, we define a subring $\mathbf{B}^\dagger$ of $\mathbf{B}$ fixed by φ and $G_{\mathbf{Q}_p}$, and if $r \in \mathbb{R}$, subrings $\mathbf{A}^{\dagger,r}$ and $\mathbf{B}^{\dagger,r}$ of $\mathbf{B}$ are fixed by $G_{\mathbf{Q}_p}$. By construction, $\varphi^{-n}(\mathbf{B}^{\dagger,r_n})$ is naturally identified with a subring of $\mathbf{B}^+_{\text{dR}}$. Finally, if K is a finite extension of $\mathbf{Q}_p$, we set $\mathbf{B}^\dagger_K = (\mathbf{B}^\dagger)^{H_K}$, $\mathbf{A}^{\dagger,r}_K = (\mathbf{A}^{\dagger,r})^{H_K}$ and $\mathbf{B}^{\dagger,r}_K = (\mathbf{B}^{\dagger,r})^{H_K}$.

Let e_K be the ramification index of K_∞ over F_∞ and $F' \subset K_\infty$ be the maximal unramified extension of $\mathbf{Q}_p$ contained in K_∞. Let $\overline{\pi}_K$ be a uniformizer of $\mathbf{E}_K = k_{F'}((\overline{\pi}_K))$ and $\overline{P}_K \in E_{F'}$ be a minimal polynomial of $\overline{\pi}_K$ and $\delta = v_E(\overline{P}'(\overline{\pi}_K))$. Choose $P_K \in \mathbf{A}_{F'}$ such that its image modulo p is $\overline{P}_K$. By Hensel's lemma, there exists a unique $\pi_K \in \mathbf{A}_K$ such that $P_K(\pi_K) = 0$ and $\pi_K = \overline{\pi}_K$ modulo p. In particular, if $K = F'$, one can take $\pi_K = \pi$.

The terminology "overconvergent" can be explained by the following proposition:

Proposition 7.2.1. *If $r \geq r(K)$, then the map $f \mapsto f(\pi_K)$ from $\mathscr{B}^{e_K r}_{F'}$ to $\mathbf{B}^{\dagger,r}_K$ is an isomorphism, where $\mathscr{B}^\alpha_{F'}$ is the set of power series $f(T) = \sum_{k \in \mathbf{Z}} a_k T^k$ such that a_k is a bounded sequence of elements of F', and such that $f(T)$ is holomorphic on the p-adic annulus $\{p^{-1/\alpha} \leq \|T\| < 1\}$.*

Proof. See lemma II.2.2 [5]. □

Proposition 7.2.2. *If K is a finite extension of $\mathbf{Q}_p$, then $\mathbf{B}_K^\dagger$ is an extension of $\mathbf{B}_{\mathbf{Q}_p}^\dagger$ of degree $[\mathbf{B}_K : \mathbf{B}_{Q_p}] = [K_\infty : \mathbf{Q}_p(\mu_{p^\infty})]$ and there exists $a(K) \in \mathbf{N}$ such that if $n \geq a(K)$, then $\varphi^{-n}(\mathbf{B}_K^{\dagger,r_n}) \subset K_n[[t]]$, where $r_n = p^{n-1}(p-1)$.*

Proof. In the case K is unramified over $\mathbf{Q}_p$, one can follow proposition 7.2.1 i) using the fact that $K_n[[t]]$ is closed in $\mathbf{B}_{\mathrm{dR}}^+$ and the formula

$$\varphi^{-n}(\pi) = \varphi^{-n}([\varepsilon]-1) = [\varepsilon^{p^{-n}}] - 1 = \varepsilon^{(n)}\exp(t/p^n) - 1 \in K_n[[t]].$$

For the general case, by remark 4.1.2, there exists $\omega = (\omega^{(n)})_{n\in\mathbf{N}} \in \varprojlim \mathscr{O}_{K_n}$ such that $\omega^{(n)}$ is a uniformizer of $\mathscr{O}_{K_n}$ if n is large enough and then $\overline{\pi}_K = \iota_K(\omega)$ is a uniformizer of $\mathbf{E}_K$ such that it is totally ramified of degree e_K over $\mathbf{E}_{F'}$. Let $\overline{P}(X) = X^{e_K} + \overline{a}_{e_K-1}X^{e_K-1} + \ldots + \overline{a}_0 \in \mathbf{E}_{F'}[X]$ be the minimal polynimial of $\overline{\pi}_K$ over $\mathbf{E}_{F'}$ and let $\delta = v_E(\overline{P}'(\overline{\pi}_K))$. If $0 \leq i \leq e_K - 1$, let $a_i \in \mathscr{O}_F[[\pi]] \subset \mathbf{A}_F$ whose reduction modulo p is $\overline{a}_i$ and let $P(X) = X^{e_K} + a_{e_K-1}X^{e_K-1} + \ldots + a_0 \in \mathbf{A}_F[X]$. By Hensel's lemma, the equation $P(X) = 0$ has a unique solution π_K in A_K whose reduction modulo p is $\overline{\pi}_K$ and we can write it in the form

$$\pi_K = [\overline{\pi}_K] + \sum_{i=1}^{+\infty} p^i[\alpha_i], \tag{7.1}$$

where α_i are elements of $\widetilde{\mathbf{E}}$ verifying $v_E(\alpha_i) \geq -i\delta$. In particular, $\pi_K \in \mathbf{A}_K^{\dagger,r}$ if $\frac{p}{p-1}r \geq \delta$, hence we have $\mathbf{A}_K^{\dagger,r} = \mathbf{A}_F^{\dagger,r}[\pi_K]$ if $\frac{p}{p-1}r \geq \delta$. Thus it suffices to prove it when n large enough, then $\pi_{K,n} = \varphi^{-n}(\pi_K) \in K_n[[t]]$.

Let P_n (resp. Q_n) be the polynomial obtained by the map $\theta \circ \varphi^{-n}$ (resp. φ^{-n}) applied on the coefficients of P, which is a polynomial with coefficients in $\mathscr{O}_{F_n}$ (resp. $F_n[[t]]$) with $\theta(\pi_{K,n})$ (resp. $\pi_{K,n}$) as a root. On the other hand, by definition of ι_K (c.f. 4.1.2), we have $v_p(\omega^{(n)} - \overline{\pi}_K^{(n)}) \geq \frac{1}{p}$ if n large enough and formula (7.1) shows that $v_p(\theta(\pi_{K,n}) - \overline{\pi}_K^{(n)}) \geq (1 - \frac{\delta}{p^n})$. Then we have $v_p(P_n(\omega^{(n)})) \geq \frac{1}{p}$ if n large enough and

$$v_p(P_n'(\omega^{(n)}) = \frac{1}{p^n}v_E(P'(\overline{\pi}_K)) = \frac{\delta}{p^n} < \frac{1}{2p}$$

if n large enough. By Hensel's lemma, the equation $P_n(X) = 0$ has a unique solution in $\mathbf{C}_p$ close to $\omega^{(n)}$ and hence belongs to $\mathscr{O}_{K_n}$ since $\omega^{(n)}$ and the coefficients of P_n do. We deduce that $\theta(\pi_{K,n})$ belongs to K_n. By using Hensel's lemma again, one can show that Q_n has a unique solution in $\mathbf{B}_{\mathrm{dR}}^+$ whose image by θ is $\theta(\pi_{K,n})$ and thus belongs to $K_n[[t]]$. □

We endow $\mathbf{B}_{Q_p}$ with the differential operator ∂ defined by continuity and the derivation $\partial\pi = 1+\pi$. We therefore have $\partial = [\varepsilon]\frac{d}{d\pi} = \frac{d}{dt}$ (Note that $t \notin \mathbf{B}_{Q_p}$). The derivation can be extended uniquely to a maximal unramified extension of $\mathbf{B}_{Q_p}$ in $\widetilde{\mathbf{B}}$, hence by continuity to a derivation ∂ from $\mathbf{B}$ to $\mathbf{B}$.

Lemma 7.2.3. *If K is a finite extension of $\mathbf{Q}_p$, there exists $m(K) \in \mathbf{Z}$ such that, if $n \geq m(K)$ and x in $\mathbf{B}_K^{\dagger,r_n}$, then*

i) $\partial x \in \mathbf{B}_K^{\dagger,r_n}$.

ii) $\varphi^{-n}(\partial x) = p^n \partial(\varphi^{-n}(x))$.

Proof. If $K = \mathbf{Q}_p$, explicit calculation using proposition 7.2.1 i), shows that we can take $m(K) = 1$. For the general case, let α be a generator of $\mathbf{B}_K^{\dagger}$ over $\mathbf{B}_{\mathbf{Q}_p}^{\dagger}$ and P be its minimal polynomial. The identity,

$$0 = \partial(P(\alpha)) = P'(\alpha)\partial\alpha + \partial P(\alpha),$$

where ∂P is the polynomial obtained by applying ∂ on the coefficients of P, shows that $\partial\alpha = -\frac{\partial P(\alpha)}{P'(\alpha)} \in \mathbf{B}_K^{\dagger}$. It is then possible to take $m(K)$ any integer such that $\mathbf{B}_K^{\dagger,m(K)}$ contains $\partial\alpha$ and α.

For ii), it suffices to note that $\varphi^{-n} \circ \partial$ is $p^n \partial \circ \varphi^{-n}$ are two derivations of $\mathbf{B}_K^{\dagger,r_n}$ coincides on $\mathbf{B}_{\mathbf{Q}_p}^{\dagger,r_n}$ by

$$\varphi^{-n} \circ \partial([\varepsilon]) = \varphi^{-n}([\varepsilon]) = \varepsilon^{(n)} \exp(p^{-n}t)$$

$$p^n \partial \circ \varphi^{-n}([\varepsilon]) = p^n \frac{d}{dt}(\varepsilon^{(n)} \exp(p^{-n}t)) = \varepsilon^{(n)} \exp(p^{-n}t).$$

□

7.3 Overconvergent representations

Definition 7.3.1. If V is a p-adic representation of G_K, we set

$$\mathbf{D}^{\dagger}(V) = (\mathbf{B}^{\dagger} \otimes_{\mathbf{Q}_p} V)^{H_K} \quad \textit{and} \quad \mathbf{D}^{\dagger,r}(V) = (\mathbf{B}^{\dagger,r} \otimes_{\mathbf{Q}_p} V)^{H_K}$$

We have $\dim_{\mathbf{B}_K^{\dagger}} \mathbf{D}^{\dagger}(V) \leq \dim_{\mathbf{Q}_p} V$ and we say that V is overconvergent if equality holds, which is equivalent to the assertion that $D(V)$ has a basis over $\mathbf{B}_K$ made up of elements of $\mathbf{D}^{\dagger}(V)$.

Proposition 7.3.2.

i) Every p-adic representation of G_K is overconvergent.

ii) There exists $r(V)$ such that $D(V)^{\psi=1} \subset \mathbf{D}^{\dagger,r(V)}(V)$.

iii) If V is overconvergent and $n \in \mathbf{N}$, then $\gamma_n - 1$ admits a an continuous inverse on $\mathbf{D}^{\dagger}(V)^{\psi=0}$. Moreover, there exists $n_2(V)$ such that if $n \geq n_2(V)$, then

$$(\gamma_n - 1)^{-1}(\mathbf{D}^{\dagger,r_n}(V)^{\psi=0}) \subset \mathbf{D}^{\dagger,r_{n+1}}(V)^{\psi=0}$$

Proof. i), iii) see [5]. ii) follows from lemma 5.3.4. □

Chapter 8

Explicit reciprocity laws and de Rham Representation

8.1 The Bloch-Kato exponential map and its dual

Let K be a finite extension of $\mathbf{Q}_p$ and V a p-adic representation of G_K. We have the fundamental exact sequence

$$0 \longrightarrow \mathbf{Q}_p \longrightarrow \mathbf{B}_{\mathrm{cris}}^{\varphi=1} \longrightarrow \mathbf{B}_{\mathrm{dR}}/\mathbf{B}_{\mathrm{dR}}^{+} \longrightarrow 0$$

(c.f. [9, proposition III 3.5]). Tensoring this exact sequence with V and taking the invariants under the action of G_K, we obtain:

$$0 \longrightarrow V^{G_K} \longrightarrow \mathbf{D}_{\mathrm{cris}}(V)^{\varphi=1} \longrightarrow ((\mathbf{B}_{\mathrm{dR}}/\mathbf{B}_{\mathrm{dR}}^{+}) \otimes V)^{G_K} \longrightarrow H^1_e(K,V) \longrightarrow 0$$

where we denote $H^1_e(K,V)$ the kernel of the natural map from $H^1(K,V)$ to $H^1(K,\mathbf{B}_{\mathrm{cris}}^{\varphi=1} \otimes V)$. We call the isomorphism induced by the connecting homomorphism

$$\exp_{K,V} : \frac{\mathbf{D}_{\mathrm{dR}}(V)}{\mathrm{Fil}^0\mathbf{D}_{\mathrm{dR}}(V) + \mathbf{D}_{\mathrm{cris}}(V)^{\varphi=1}} \longrightarrow H^1_e(K,V) \subset H^1(K,V)$$

the Bloch-Kato exponential of V over K and we denote its inverse by

$$\log_{K,V} : H^1_e(K,V) \longrightarrow \frac{\mathbf{D}_{\mathrm{dR}}(V)}{\mathrm{Fil}^0\mathbf{D}_{\mathrm{dR}}(V) + \mathbf{D}_{\mathrm{cris}}(V)^{\varphi=1}}$$

the Bloch-Kato logarithm of V over K. Moreover, if V is de Rham and $k \gg 0$, then $\exp_{K,V(k)}$ is an isomorphism from $\mathbf{D}_{\mathrm{dR}}(V(k))$ to $H^1(K,V(k))$.

The choice of t gives an isomorphism from $\mathbf{D}_{\mathrm{dR}}(\mathbf{Q}_p(1)) = t^{-1}K$ to K. If V is a p-representation of

G_K, the couple $[,]_{\mathbf{D}_{\mathrm{dR}}(V)}$ is defined by the composition of maps

$$\mathbf{D}_{\mathrm{dR}}(V)\otimes\mathbf{D}_{\mathrm{dR}}(V^*(1))\cong\mathbf{D}_{\mathrm{dR}}(V\otimes V^*(1))\longrightarrow\mathbf{D}_{\mathrm{dR}}(\mathbf{Q}_p(1))\cong K\xrightarrow{\mathrm{Tr}_{K/Qp}}\mathbf{Q}_p\ .$$

This composition is non-degenerate, hence $\mathbf{D}_{\mathrm{dR}}(V^*(1))$ can be naturally identified with the dual of $\mathbf{D}_{\mathrm{dR}}(V)$. Similarly, via the cup product

$$H^1(K,V)\times H^1(K,V^*(1))\to H^2(K,\mathbf{Q}_p(1))=\mathbf{Q}_p,$$

$H^1(K,V^*(1))$ is naturally identified with the dual of $H^1(K,V)$. This allows us to view the map $\exp^*_{K,V^*(1)}$ as the transpose of the map $\exp_{K,V^*(1)}:\mathbf{D}_{\mathrm{dR}}(V^*(1))\to H^1(K,V^*(1))$ as a map from $H^1(K,V)$ to $\mathbf{D}_{\mathrm{dR}}(V)$, whose image is contained in $\mathrm{Fil}^0(\mathbf{D}_{\mathrm{dR}}(V))$. If V is de Rham and $k\gg 0$, the map $\exp^*_{K,V^*(1+k)}$ is an isomorphism from $H^1(K,V(-k))$ to $\mathbf{D}_{\mathrm{dR}}(V(-k))$.

If $x\in K_\infty$ and $n\in\mathbf{N}$, then $\frac{1}{p^m}\mathrm{Tr}_{K_m/K_n}(x)$ does not depend on the choice of integer $m\geq n+1$ such that x is belongs to K_m. We denote T_n the above $\mathbf{Q}_p$-linear map from K_∞ to K_n. If $n\geq 1$ and $x\in K_n$, then $\mathrm{T}_n(x)=p^{-n}x$. We have

$$\mathrm{T}_m=\mathrm{Tr}_{K_n/K_m}\circ\mathrm{T}_n\quad\text{if } n\geq m.$$

We also denote by T_n the map from $K_\infty((t))$ to $K_n((t))$ defined by $\mathrm{T}_n(\sum_{k=0}^{+\infty}a_kt^k)=\sum_{k=0}^{+\infty}\mathrm{T}_n(a_k)t^k$.

Proposition 8.1.1.

i) $K_\infty((t))$ *is dense in* $\mathbf{B}_{\mathrm{dR}}^{H_K}$ *and* T_n *can be extended to a* $\mathbf{Q}_p$*-linear map from* $\mathbf{B}_{\mathrm{dR}}^{H_K}$ *to* $K_n((t))$.

ii) If $F\in\mathbf{B}_{\mathrm{dR}}^{H_K}$*, then* $\lim_{n\to+\infty}p^n\mathrm{T}_n(F)=F$.

Proof. See [9], proposition V.4.5. ☐

Let V be a de Rham representation of G_K, we have $\mathbf{B}_{\mathrm{dR}}\otimes_{\mathbf{Q}_p}V\cong\mathbf{B}_{\mathrm{dR}}\otimes_K\mathbf{D}_{\mathrm{dR}}(V)$ and $H^1(K,\mathbf{B}_{\mathrm{dR}}\otimes V)=H^1(K,\mathbf{B}_{\mathrm{dR}}\otimes\mathbf{D}_{\mathrm{dR}}(V))=H^1(K,\mathbf{B}_{\mathrm{dR}})\otimes\mathbf{D}_{\mathrm{dR}}(V)$. Since $K\cong H^1(K,\mathbf{B}_{\mathrm{dR}})$ via $x\mapsto x\cup\log\chi$. We thus get an isomorphism

$$\mathbf{D}_{\mathrm{dR}}(V)\to H^1(K,\mathbf{B}_{\mathrm{dR}}\otimes V);\quad x\mapsto x\cup\log\chi$$

Proposition 8.1.2. *If V is a de Rham representation, the map $x\in\mathbf{D}_{\mathrm{dR}}(V)$ to a cocycle $\tau\mapsto x\log\chi(\tau)\in\mathbf{D}_{\mathrm{dR}}(V)\subset\mathbf{B}_{\mathrm{dR}}\otimes V$ induces an isomorphism from $\mathbf{D}_{\mathrm{dR}}(V)$ to $H^1(K,\mathbf{B}_{\mathrm{dR}}\otimes V)$ and the map $\exp^*_{V^*(1)}$ is the composition of the inverse of the above isomorphism and the natural map from $H^1(K,V)$ to $H^1(K,\mathbf{B}_{\mathrm{dR}}\otimes V)$.*

Proof. See [16] proposition 1.4. of chapter II. ☐

We define the map $\mathrm{pr}_{K_n}:\mathbf{B}_{\mathrm{dR}}^{H_K}\to K_n((t))$ by the formula $\mathrm{pr}_{K_n}(x)=\frac{1}{[K_m:K_n]}\mathrm{Tr}_{K_m/K_n}(x)$ if $x\in K_\infty$ and $m\geq n$ such that $x\in K_m$ and there exists $a'(K)\geq 1$ such that one has $p^n\mathrm{T}_n=\mathrm{pr}_{K_n}$ if $n\geq a'(K)$. From (ii) of proposition 8.1.1, we can show that $\lim_{n\to+\infty}\mathrm{pr}_{K_n}x=x$ if $x\in\mathbf{B}_{\mathrm{dR}}^{H_K}$

If V is a de Rham representation, the natural map from $\mathbf{B}_{\mathrm{dR}}^{H_K} \otimes_K \mathbf{D}_{\mathrm{dR}}(V)$ to $(\mathbf{B}_{\mathrm{dR}} \otimes_{\mathbf{Q}_p} V)^{H_K}$ is an isomorphism and we can extend the map T_n and pr_{K_n} for $n \in \mathbf{N}$ by linearity to $\mathbf{B}_{\mathrm{dR}}^{H_K} \otimes_K \mathbf{D}_{\mathrm{dR}}(V)$. On the other hand, if $F \in K_\infty((t)) \otimes \mathbf{D}_{\mathrm{dR}}(V)$, we can write F uniquely as the form $\sum_{k \gg -\infty} t^k d_k$, where $d_k \in K_\infty \otimes \mathbf{D}_{\mathrm{dR}}(V)$. We denote $\partial_{V(-k)}(F)$ the element $t^k d_k$ of $K_\infty \otimes \mathbf{D}_{\mathrm{dR}}(V(-k))$.

Proposition 8.1.3. *Let V be a p-adic representation of G_K and $n, m \in \mathbf{N}$ be two integers. If $c \in H^1(K_m, V(-k))$, there exists a cocycle $\tau \mapsto c_\tau$ on Γ_{K_m} with values in $(\mathbf{B}_{\mathrm{dR}} \otimes V(-k))^{H_K}$ which has the same image as c in $H^1(K_m, \mathbf{B}_{\mathrm{dR}} \otimes V(-k))$. Moreover, if V is de Rham. then*

$$\exp^*_{V^*(1+k)}(c) = \partial_{V(-k)} \circ \mathrm{pr}_{K_m}\left(\frac{1}{\log_p(\chi(\gamma))} c_\gamma\right)$$

for all $\gamma \in \Gamma_{K_m}$ such that $\log_p(\chi(\gamma)) \neq 0$

Proof. Since $H^1(K_\infty, \mathbf{B}_{\mathrm{dR}} \otimes V)$ is zero (c.f. [9] theorem IV.3.1), the inflation map from $H^1(\Gamma_{K_m}, (\mathbf{B}_{\mathrm{dR}} \otimes V)^{H_K})$ to $H^1(K_m, \mathbf{B}_{\mathrm{dR}} \otimes V)$ is an isomorphism, hence we have the existance of coycle $\tau \mapsto c_\tau$. On the other hand, if V is de Rham, the map $\tau \mapsto \partial_{V(-k)} \circ \mathrm{pr}_{K_m}(c_\tau)$ is a cocycle on Γ_{K_m} with values in $\mathbf{D}_{\mathrm{dR}}(V(-k))$ which Γ_{K_m} acts trivially. It is of the form $\tau \mapsto d \log_p \chi(\tau)$, where $d \in \mathbf{D}_{\mathrm{dR}}(V(-k))$ and if c is zero, which implies $\tau \mapsto c_\tau$ is a coboundary, hence $d = 0$. One cae deduce that $\partial_{V(-k)} \circ \mathrm{pr}_{K_m}(\frac{1}{\log_p \chi(\gamma)} c_\gamma) \in \mathbf{D}_{\mathrm{dR}}(V(-k))$ does not depend on $\gamma \in \Gamma_{K_m}$ such that $\chi(\gamma) \neq 0$ and the choice of cocycle $\tau \mapsto c_\tau$ representing c, which provides us a natural map from $H^1(K, V(-k))$ to $\mathbf{D}_{\mathrm{dR}}(V(-k))$ coincides with $\exp^*_{V^*(1+k)}$ by proposition 8.1.2. □

8.2 Explicit reciprocity law

Let V be a de Rham representation of G_K and let $n(V) \geq n_1(V)$ be the smallest integer satisfies $r_{n(V)} \geq r_V$ (c.f. proposition 7.3.2). If $\mu \in H^1_{\mathrm{Iw}}(K, V)$, then $\mathrm{Exp}^*_{V^*(1)}(\mu) \in D(V)^{\psi=1}$. On the other hand, $D(V)^{\psi=1} \subset \mathbf{D}^{\dagger, r_V}(V)$. If $n \geq n(V)$, we can view $\varphi^{-n}(\mathrm{Exp}^*_{V^*(1)}(\mu))$ as an element in $\mathbf{B}_{\mathrm{dR}} \otimes V$. Since $\varphi^{-n}(\mathrm{Exp}^*_{V^*(1)}(\mu))$ is an element of $\mathbf{B}_{\mathrm{dR}} \otimes V$ fixed by H_K, we can consider its image under T_m.

Theorem 8.2.1. *Let V be a de Rham representation and $m \in \mathbf{N}$.*

i) If $n \geq \sup(m, n(V))$ and $\mu \in H^1_{\mathrm{Iw}}(K, V)$, then $\mathrm{T}_m(\varphi^{-n}(\mathrm{Exp}^*_{V^*(1)}(\mu)))$ is an element in $K_m((t)) \otimes_K \mathbf{D}_{\mathrm{dR}}(V)$ independent of n, we denote it by $\mathrm{Exp}^*_{V^*(1), K_m}(\mu)$.

ii) If $\mu \in H^1_{\mathrm{Iw}}(K, V)$, then

$$\mathrm{Exp}^*_{V^*(1), K_m}(\mu) = \sum_{k \in \mathbf{Z}} \exp^*_{V^*(1+k)}\left(\int_{\Gamma_{K_m}} \chi(x)^{-k} \mu\right).$$

iii) There exists $m(V) \geq n(V)$ such that if $m \geq m(V)$ and $\mu \in H^1_{\mathrm{Iw}}(K, V)$, then

$$\mathrm{Exp}^*_{V^*(1), K_m}(\mu) = p^{-m} \varphi^{-m}(\mathrm{Exp}^*_{V^*(1)}(\mu)).$$

Remark 8.2.2.

i) The image of $H^1(K_m,V(-k))$ by $\exp^*_{V^*(1+k)}$ is contained in $\mathrm{Fil}^0\mathbf{D}_{\mathrm{dR}}(V(-k))=\mathrm{Fil}^0(t^K\mathbf{D}_{\mathrm{dR}}(V))$ which is zero if $k\ll 0$. Hence the series in ii) converges in $\mathbf{B}_{\mathrm{dR}}\otimes\mathbf{D}_{\mathrm{dR}}(V)$.

ii) We have a map $\mu\in H^1_{\mathrm{Iw}}(K,V)\mapsto\int_{\Gamma_{K_n}}\chi^k\mu\in H^1(G_{K_n},V(k))$, thus $\exp^*_{V(1+k)}(\int_{\Gamma_{K_n}}\chi^{-k}\mu)\in t^kK_n\otimes_K\mathbf{D}_{\mathrm{dR}}(V)$.

iii) For $n\geq n(V)$, we have $\varphi^{-n}(\mathbf{D}^{\dagger,r_n}(V))\subset K_n((t))\otimes\mathbf{D}_{\mathrm{dR}}(V)$.

Proof. Given that $\mathrm{T}_r=\mathrm{Tr}_{K_m/K_r}\circ\mathrm{T}_m$ if $r\leq m$ and if $L_1\subset L_2$ are two finite extension of K, then the diagram

$$\begin{array}{ccc} H^1(L_2,V) & \xrightarrow{\exp^*_{V^*(1)}} & L_2\otimes\mathbf{D}_{\mathrm{dR}}(V) \\ \downarrow{\scriptstyle \mathrm{cor}_{L_2/L_1}} & & \downarrow{\scriptstyle \mathrm{Tr}_{L_2/L_1}\otimes id} \\ H^1(L_1,V) & \xrightarrow{\exp^*_{V^*(1)}} & L_1\otimes\mathbf{D}_{\mathrm{dR}}(V) \end{array}$$

is commutative. Thus, to prove i) and ii), it suffices to prove them for m large enough. We can therefore suppose that $m\geq n(V)+1$, $\mathrm{pr}_{K_m}=p^m\mathrm{T}_m$ and $\log_p^0(\gamma_m)=\frac{\log_p(\chi(\gamma_m))}{p^m}$.

Denote y the element $\mathrm{Exp}^*_{V^*(1)}(\mu)$ in $D(V)^{\psi=1}$ and if $i\in\mathbf{Z}$, denote $y(i)$ the image of y in $D(V(i))^{\psi=1}=D(V)^{\psi=1}$ (same as set but differerent as Galois module by twist χ^i). By construction of $\mathrm{Exp}^*_{V^*(1)}$ (indeed its inverse), $\int_{\Gamma_{K_n}}\chi(x)^{-k}\mu$ is represented by the cocycle

$$\sigma\mapsto c'_\sigma=\log_p^0(\gamma_m)\big(\frac{\sigma-1}{\gamma_m-1}y(-k)-(\sigma-1)b\big),$$

where $b\in\mathbf{A}\otimes V$ is a solution of the equation $(\varphi-1)b=(\gamma_m-1)^{-1}((\varphi-1)y)(-k))$.

By definition of $n(V)$, we have $y\in\mathbf{D}^{\dagger,r_{n(V)}}(V)\subset\mathbf{D}^{\dagger,r_{m-1}}(V)$ and $(\varphi-1)y\in\mathbf{D}^{\dagger,r_m}(V)$, which implies that $(\gamma_m-1)^{-1}(\varphi-1)y(-k)\in\mathbf{D}^{\dagger,r_{m+1}}(V)$ by proposition 7.3.2, and the same argument as lemma 5.3.4 implies that $b\in\mathbf{A}^{\dagger,r_m}\otimes V$. Since we suppose that $n\geq\sup(m,n(V))$, we have $\varphi^{-n}(b)$ and $\varphi^{-n}(y)$ are both in $\mathbf{B}^+_{\mathrm{dR}}\otimes V$ and $c'_\sigma=\varphi^{-n}(c'_\sigma)$ is a cocycle with values in $\mathbf{B}_{\mathrm{dR}}\otimes V$ which differs from the coycle

$$\sigma\mapsto c_\sigma=\frac{\log_p\chi(\gamma_m)}{p^m}\frac{\sigma-1}{\gamma_m-1}\varphi^{-n}(y(-k))$$

by a coboundary $\sigma\mapsto\frac{\log_p\chi(\gamma_m)}{p^m}(\sigma-1)\varphi^{-n}(b)$. Since y is fixed by H_K, the cocycle $\sigma\mapsto c_\sigma$ has values in $(\mathbf{B}_{\mathrm{dR}}\otimes V)^{H_K}$ which allows us to use proposition 8.1.3 to calculate it and we obtain

$$\exp^*_{V^*(1+k)}\left(\int_{\Gamma_{K_m}}\chi(x)^{-k}\mu\right)=\frac{1}{\log_p\chi(\gamma_m)}\partial_{V(-k)}(\mathrm{pr}_{K_m}(c_{\gamma_m}))=\frac{1}{p^m}\partial_{V(-k)}(\mathrm{pr}_{K_m}(\varphi^{-n}(y)))$$

and since $\frac{1}{p^m}\mathrm{pr}_{K_m}=\mathrm{T}_m$ and $\mathrm{T}_m(x)=\sum_{k\in\mathbf{Z}}\partial_{V(-k)}(\mathrm{T}_m(x))$ if $x\in(\mathbf{B}_{\mathrm{dR}}\otimes V)^{H_K}$, we deduce i) and ii).

To prove iii), it suffices to show that if m is large enough, then $\varphi^{-m}(\mathrm{Exp}^*_{V^*(1)}(\mu)) \in K_m((t)) \otimes_K \mathbf{D}_{\mathrm{dR}}(V)$. We need the following lemma:

Lemma 8.2.3. *Let d be an integer ≥ 1. If $U \in GL_d(\mathbf{B}_{\mathrm{dR}}^{H_K})$ and there exists $n \in \mathbf{N}$ such that $U^{-1}\gamma(U) \in GL_d(K_n((t)))$, then there exists $m \in \mathbf{N}$ such that $U \in GL_d(K_m((t)))$.*

Proof. Let $A = U^{-1}\gamma(U)$. If $m \geq n$, let $U_m = \mathrm{pr}_{K_m}(U)$. Using the fact that pr_{K_m} is $K_n((t))$-linear if $m \geq n$, we obtain, by applying pr_{K_m} to the identity $UA = \gamma(U)$, the relation $U_m A = \gamma(U_m)$. On the other hand, since $\lim_{m\to+\infty} U_m = U$, there exists $m \geq n$ such that U_m is invertible. Subtract A by the above identity, We have UU_m^{-1} is fixed by γ and therefore belongs to $GL_d(K)$. We hence deduce that U belongs to $GL_d(K_m((t)))$. □

Let $e_1, ..., e_d$ be a basis of $\mathbf{D}^{\dagger, r_{n(V)}}(V)$ over $\mathbf{B}_K^{\dagger, r_{n(V)}}$ which contains $D(V)^{\psi=1}$ and $f_1, ..., f_d$ a basis of $\mathbf{D}_{\mathrm{dR}}(V)$ over K. Let $A = (a_{i,j}) \in GL_d(\mathbf{B}_K^{\dagger})$, $B = (b_{i,j}) \in GL_d(\mathbf{B}_K^{\dagger})$ and if $m \geq n(V)$, $C^{(m)} = (c_{i,j}^{(m)}) \in GL_d(\mathbf{B}_{\mathrm{dR}}^{H_K})$ the matrices defined by

$$\gamma(e_i) = \sum_{j=1}^{d} a_{i,j} e_j, \quad \varphi(e_i) = \sum_{j=1}^{d} b_{i,j} e_j \quad \text{and} \quad \varphi^{-m}(e_i) = \sum_{j=1}^{d} c_{i,j}^{(m)} f_j.$$

The relation $\gamma \circ \varphi^{-m} = \varphi^{-m} \circ \gamma$ and $\varphi^{-m} = \varphi^{-(m+1)} \circ \varphi$ is translated to

$$\gamma(C^{(m)}) = C^{(m)} \varphi^{-m}(A) \quad \textit{and} \quad C^{(m)} = C^{(m+1)} \varphi^{-(m+1)}(C^{-1})$$

since $f_1, ..., f_d$ is fixed by γ. There exists $n_0 \geq n(V)$ such that A and B belongs to $GL_d(\mathbf{B}_K^{\dagger, r_{n_0}})$. Since there exists $m_0 \in \mathbf{N}$ such that $\varphi^{-m}(\mathbf{B}_K^{\dagger, r_m}) \in K_m[[t]]$, if $m \geq m_0$. By above relations and lemma 8.2.3, there exists $m(V) \geq \sup(n_0, m_0) = m_1$ such that $C^{(m_1)} \in GL_d(K_{m(V)}((t)))$, which implies that $C^{(m)} \in GL_d(K_{m(V)}((t)))$ for $m \geq m(V)$ by second relation. Since $x \in D(V)^{\psi=1}$ is of the form $\sum_{i=1}^{d} x_i e_i$ where $x \in \mathbf{B}^{\dagger, r_{n(V)}}$ and $\varphi^{-m}(\mathbf{B}^{\dagger, r_{n(V)}}) \subset K_m[[t]]$ if $m \geq m(V)$ by the choice of $m(V)$, we have the inclusion $\varphi^{-m}(D(V)^{\psi=1}) \subset K_m((t)) \otimes_K \mathbf{D}_{\mathrm{dR}}(V)$ if $m \geq m(V)$. This proves iii). □

8.3 Connection with the Perrin-Riou's logarithm

Our Goal in this paragraph is to compare $\mathrm{Exp}^*_{V^*(1)}$ and Perrin-Riou's logarithm constructed in [9]. Let us recall the construction of logarithm map.

Proposition 8.3.1. *Let V be a de Rham representation. Let W be the finite dimensional $\mathbf{Q}_p$-vector space $\cup_{n\in\mathbf{N}} (\mathbf{B}_{\mathrm{cris}}^{\varphi=1} \otimes V)^{G_{K_n}}$. Let $\mu \in H^1_{\mathrm{Iw}}(K_n, V)$ such that $\int_{\Gamma_{K_n}} \mu \in H^1_e(K, V)$ for all $n \in \mathbf{N}$ and $\tau \to \mu_\tau$ a continuous cocycle representing μ. Finally, if $n \gg 0$, let c_n be the unique element of $(\mathbf{B}_{\mathrm{cris}}^{\varphi=1} \otimes V)/W$ verifying $(1-\tau)c_n = \int_{K_n} \mu_\tau$ for all $\tau \in G_{K_n}$.*

i) *The sequence $p^n c_n$ converges in $(\mathbf{B}_{\mathrm{cris}}^{\varphi=1} \otimes V)/W$ to an element of $(\mathbf{B}_{\mathrm{cris}}^{\varphi=1} \otimes V)^{G_K}/W$ denoted by* $\mathrm{Log}_V(\mu)$.

ii) *If $n \in \mathbf{N}$, then*

$$t\frac{d}{dt}T_n(\mathrm{Log}_V(\mu)) = \sum_{k\in\mathbf{N}} \exp^*_{V^*(1+k)}(\int_{\Gamma_{K_n}} \chi(x)^{-k}\mu).$$

Proof. See [9, Theorem VI.3.1 and Theorem VII.1.1]. □

Remark 8.3.2.

i) There exists $k_0 \in \mathbf{N}$ such that the condition $\int_{\Gamma_{K_n}} \mu \in H^1_e(K,V)$ for all $n \in \mathbf{N}$ holds automatically if we replace V by $V(k)$ for $k \geq k_0$.

ii) The operator $\frac{d}{dt}$ annihilates $K_\infty \otimes \mathbf{D}_{\mathrm{dR}}(V)$ and hence W, which explains why we don't need to pass to quotient W in formula (ii).

The connection between Log_V and $\mathrm{Exp}^*_{V^*(1)}$ in the case V is de Rham is given by:

Theorem 8.3.3. *Let V be a de Rham representation of G_K. There exists $m(V) \geq n(V)$ such that if $m \geq m(V)$ and $\mu \in H^1_{\mathrm{Iw}}(K,V)$ such that $\int_{\Gamma_{K_n}} \mu \in H^1_e(K_n,V)$ for all $n \in \mathbf{N}$, then*

$$p^{-m}\varphi^{-m}(\mathrm{Exp}^*_{V^*(1)}(\mu)) = t\frac{d}{dt}(T_m(\mathrm{Log}_V(\mu)))$$

Proof. Given ii) of proposition 8.3.1, it follows immediately by theorem 8.2.1. □

Remark 8.3.4. It is possible that the theorem is empty, that is there exists no nonzero element in $H^1_{\mathrm{Iw}}(K,V)$ satisfying the assumptions in proposition 8.3.1, but as we noted above, if we replace V by $V(k)$ for $k \gg 0$, then the assumptions of the theorem is verified for all elements of $H^1_{\mathrm{Iw}}(K,V)$.

Chapter 9

The $\mathbf{Q}_p(1)$ representation and Coleman's power series

9.1 The module $D(\mathbf{Z}_p(1))^{\psi=1}$

The module $\mathbf{Z}_p(1)$ is just $\mathbf{Z}_p$ with the action of $G_{\mathbf{Q}_p}$ defined by $g \in G_{\mathbf{Q}_p}$, $x \in \mathbf{Z}_p(1)$, $g(x) = \chi(g)x$. We shall study the exponential map

$$\mathrm{Exp}^*_{\mathbf{Q}_p} : H^1_{\mathrm{Iw}}(\mathbf{Q}_p, \mathbf{Z}_p(1)) \to D(\mathbf{Z}_p(1))^{\psi=1}.$$

Note that $D(\mathbf{Z}_p(1)) = (\mathbf{A} \otimes \mathbf{Z}_p(1))^{H_{\mathbf{Q}_p}} = \mathbf{A}_{Q_p}(1)$, with usual actions of φ and ψ, and for $\gamma \in \Gamma$, $\gamma(f(\pi)) = \chi(\gamma) f((1+\pi)^{\chi(\gamma)} - 1)$, for all $f(\pi) \in \mathbf{A}_{Q_p}(1)$.

Proposition 9.1.1. $(\mathbf{A}_{Q_p})^{\psi=1} = \mathbf{Z}_p \cdot \frac{1}{\pi} \oplus (\mathbf{A}^+_{Q_p})^{\psi=1}$.

Proof. Note that we have $\psi(\mathbf{A}^+_{Q_p}) \subset \mathbf{A}^+_{Q_p}$, $\psi(\frac{1}{\pi}) = \frac{1}{\pi}$ and $v_E(\psi(x) \geq [\frac{v_E(x)}{p}]$ if $x \in \mathbf{E}^+_{\mathbf{Q}_p}$. These facts imply that $\psi - 1$ is bijective on $\mathbf{E}_{\mathbf{Q}_p}/\overline{\pi}^{-1}\mathbf{E}^+_{\mathbf{Q}_p}$ and hence it is also bijective on $\mathbf{A}_{Q_p}/\pi^{-1}\mathbf{A}^+_{Q_p}$. Thus $\psi(x) = x$ implies $x \in \pi^{-1}\mathbf{A}^+_{Q_p}$. □

9.2 Kummer theory

We define the Kummer map $\kappa : K^* \to H^1(K, \mathbf{Q}_p(1))$ as follows: For $a \in K^*$, we choose x any element in $\widetilde{\mathbf{E}}$ satisfying $x^{(0)} = a$, then $\tau \mapsto (1-\tau)(\frac{\log[x]}{t}(1))$ is a 1-cocycle on G_K with values in $\mathbf{Q}_p(1)$ whose image in $H^1(K, \mathbf{Q}_p(1))$ is defined to be $\kappa(a)$.

Recall that $\varepsilon = (1, \varepsilon^{(1)}, \cdots) \in \mathbf{E}^+_{\mathbf{Q}_p}$, $\varepsilon^{(1)} \neq 1$. Let $F_n = \mathbf{Q}_p(\varepsilon^{(n)})$ and $\kappa_n : F_n^* \to H^1(F_n, \mathbf{Q}_p(1))$ be the Kummer maps defined above. Since $\mathrm{cor}_{F_{n+1}/F_n} \circ \kappa_{n+1} = \kappa_n \circ \mathrm{N}_{F_{n+1}/F_n}$, which induces a map

$$\kappa : \varprojlim F_n^* \to H^1_{\mathrm{Iw}}(\mathbf{Q}_p, \mathbf{Q}_p(1)).$$

We have

$$H^1_{\mathrm{Iw}}(\mathbf{Q}_p,\mathbf{Z}_p(1)) = \mathbf{Z}_p\cdot\kappa(\pi)\oplus\kappa(\varprojlim \mathscr{O}^*_{F_n}).$$

9.3 Multiplicative representatives

Recall that $\mathbf{B}$ is a purely inseparable extension of degree p of $\varphi(\mathbf{B})$ (totally ramified since residual extension is purely inseparable). Define the multiplicative map $\mathrm{N}:\mathbf{B}\to\mathbf{B}$ by the formula $\mathrm{N}(x) = \varphi^{-1}(\mathrm{N}_{\mathbf{B}/\varphi(\mathbf{B})}(x))$. This is an multiplicative analogue of ψ.

Lemma 9.3.1. *If $x\in\mathbf{E}^*$ and U_x denote the set $y\in\mathbf{A}$ whose reduction modulo p is x, then N is a contractible map of U_x for the p-adic topology.*

Proof. Note that N induces the identity on $\mathbf{E}$ and thus fixes U_x. On the other hand, if $y\equiv 1 \mod p^k$, we have

$$\mathrm{N}(y)\equiv 1+\varphi^{-1}\mathrm{Tr}_{\mathbf{B}/\varphi(\mathbf{B})}(y-1) = 1+p\psi(y-1) \mod p^{2k},$$

which implies in particular that $\mathrm{N}(y)-1\in p^{k+1}\mathbf{A}$. We deduce that if y_1,y_2 two elements of U_x verifying $y_1-y_2\in p^k\mathbf{A}$, then $\mathrm{N}(y_1)-\mathrm{N}(y_2) = \mathrm{N}(y_2)(\mathrm{N}(y_2^{-1}y_1)-1)\in p^{k+1}\mathbf{A}$, which proves the lemma. □

Corollary 9.3.2.

i) If $x\in\mathbf{E}$, there exists an unique element $\hat{x}\in\mathbf{A}$ whose image modulo p is x and $\mathrm{N}(\hat{x})=\hat{x}$.

ii) If x and y are two elements in $\mathbf{E}$, the $\widehat{xy}=\hat{x}\hat{y}$.

Proof. i) follows from the above lemma if $x\neq 0$ and completeness of U_x for the p-adic topology. On the other hand, $\mathrm{N}(p^k\mathbf{A})\subset p^{pk}\mathbf{A}$, this proves that 0 is the only element of y in $p\mathbf{A}$ satisfying $\mathrm{N}(y)=y$. Thus we prove the uniqueness. ii) follows from the uniqueness in i). □

Remark 9.3.3. There are two multiplicative maps from $\mathbf{E}$ to $\widetilde{\mathbf{A}}$, namely the map $x\to\hat{x}$ and the Techmuller map $[x]$. We have $\hat{x}\neq[x]$ unless $x\in\overline{\mathbf{F}}_p$.

Lemma 9.3.4. *Let K be a finite extension of $\mathbf{Q}_p$ and $d=[\mathbf{B}_K:\mathbf{B}_{Q_p}] = [K_\infty:\mathbf{Q}_p(\mu_{p^\infty})]$. If $n(K)$ is the smallest integer $n\geq 2$ such that there exist $e_1,\dots,e_d\in\widetilde{\mathbf{A}}_K^{\dagger,r_n}$ such that $\varphi(e_1),\dots,\varphi(e_d)$ form a basis of $\widetilde{\mathbf{A}}_K^{\dagger,r_{n+1}}$ over $\widetilde{\mathbf{A}}_{\mathbf{Q}_p}^{\dagger,r_{n+1}}$ and if $n\geq n(K)$, then $\mathrm{N}(\widetilde{\mathbf{A}}_K^{\dagger,r_{n+1}})\subset\widetilde{\mathbf{A}}_K^{\dagger,r_n}$.*

Proof. By definition of $n(K)$, if $n\geq n(K)$ and $x\in\mathbf{A}_K^{\dagger,r_{n+1}}$, we can write x in the form $x=\sum_{i=1}^d x_i\varphi(e_i)$ where $x_i\in\mathbf{A}_{\mathbf{Q}_p}^{\dagger,r_{n+1}}$. On the other hand, we can write x_i in the form $x_i=\sum_{j=0}^{p-1}x_{i,j}[\varepsilon]^j$ where $x_{i,j} = \varphi(\psi([\varepsilon]^{-j}x_i))$ and corollary 5.3.3 and proposition 7.2.1 show that we have $x_{i,j}\in\varphi(\mathbf{A}_{\mathbf{Q}_p}^{\dagger,r_n})$. We hence deduce that the coordinate $y_j=\sum_{i=1}^d x_{i,j}\varphi(e_i)$ of x in basis $1,[\varepsilon],\dots,[\varepsilon]^{p-1}$ of $\mathbf{B}$ over $\varphi(\mathbf{B})$ belongs to to

$\mathbf{A}_K^{\dagger,r_{n+1}} \cap \varphi(\mathbf{B}) = \varphi(\mathbf{A}_K^{\dagger,r_n})$. On the other hand, $\mathrm{N}_{\mathbf{B}/\varphi(\mathbf{B})}$ is the determinant of the multiplication by x in $\mathbf{B}$ considered as a vector space of dimension p over $\varphi(\mathbf{B})$, therefore the determinant of the matrix

$$\begin{pmatrix} y_0 & [\varepsilon]^p y_{p-1} & \cdots & [\varepsilon]^p y_1 \\ y_1 & y_0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & [\varepsilon]^p y_{p-1} \\ y_{p-1} & y_{p-2} & \cdots & y_0 \end{pmatrix}.$$

We deduce that $\mathrm{N}_{\mathbf{B}/\varphi(\mathbf{B})}$ belongs to $\varphi(\mathbf{A}_K^{\dagger,r_n})$ Together with the relation $\mathrm{N} = \varphi^{-1} \circ \mathrm{N}_{\mathbf{B}/\varphi(\mathbf{B})}$, we complete the proof. □

Corollary 9.3.5. *If $x \in \mathbf{E}_K^+$, then $\hat{x} \in \mathbf{A}_K^{\dagger,r_{n(K)}}$. Moreover, if K is a unramified extension over $\mathbf{Q}_p$ and $x \in \mathbf{E}_K^+$, then $\hat{x} \in \mathbf{A}_K^+ = \mathbf{A}_K \cap \mathbf{A}_{Q_p}^+ = \mathscr{O}_K[[\pi]]$.*

Proof. Let $v \in \mathbf{A}_K^{\dagger}$ whose image in $\mathbf{E}_K$ is x and let $n \geq n(K)$ such that $v \in \mathbf{A}_K^{\dagger,r_n}$. Let $(v_k)_{k\in\mathbf{N}}$ the sequence of elements in $\mathbf{A}_K$ defined by $v_0 = v$ and $v_k = \mathrm{N}(v_{k-1})$ if $k \geq 1$. By lemma 9.3.1, the sequence tends to $\hat{x}$ in $\mathbf{A}_K$ as k tends to $+\infty$. On the other hand, lemma 9.3.4, implies that $v_k \in \mathbf{A}_K^{\dagger,r_n}$ for $k \in \mathbf{N}$ and since $\mathbf{A}_K^{\dagger,r_n}$ is relatively compact in $\mathbf{A}_K^{\dagger,r_{n+1}}$, which implies that $\hat{x} \in \mathbf{A}^{\dagger,r_{k+1}}$ and the result follows by using lemma 9.3.4 by descending $\mathbf{A}_K^{\dagger,r_{n+1}}$ to $\mathbf{A}_K^{\dagger,r_{n(K)}}$.

In the case where K is unramified over $\mathbf{Q}_p$, the reduction modulo p induces a surjection from $\mathbf{A}_K^+$ to $\mathbf{E}_K^+$ and since $\mathbf{A}_K^+$ is a closed subring of $\mathbf{A}_K$ fixed by N, a similar argument shows that $v \in \mathbf{A}_K^+$ implies that $\hat{x} \in \mathbf{A}_K^+$. □

9.4 Generalized Coleman's power series

Let us recall the construction of the classical Coleman's power series.

Proposition 9.4.1. *Let F be a finite unramified extension of $\mathbf{Q}_p$. If $u = (u^{(n)})_{n\in\mathbf{N}}$ is an element of the projective limit $\varprojlim \mathscr{O}_{F_n}^*$ of $\mathscr{O}_{F_n}^*$ with respect to the norm map, there exists a unique power series $\mathrm{Col}_u(T)$ in $\mathscr{O}_F[[T]]^*$ such that we have $\mathrm{Col}_u^{\varphi^{-n}}(\varepsilon^{(n)} - 1) = u^{(n)}$ for all $n \in \mathbf{N}$.*

Proof. See [8]. □

Lemma 9.4.2. *If K is a finite extension of $\mathbf{Q}_p$ and $n \geq n(K)$, then the diagram*

$$\begin{array}{ccc} \mathbf{A}_K^{\dagger,r_{n+1}} & \xrightarrow{\mathrm{N}} & \mathbf{A}_K^{\dagger,r_n} \\ {\scriptstyle \varphi^{-(n+1)}}\downarrow & & \downarrow{\scriptstyle \varphi^{-n}} \\ K_{n+1}[[t]] & \xrightarrow{\mathrm{N}_{K_{n+1}/K_n}} & K_n[[t]] \end{array}$$

is commutative.

Proof. By definition, $\mathrm{N}_{\mathbf{B}/\varphi(\mathbf{B})}$ (resp. $\mathrm{N}_{K_{n+1}/K_n}(\varphi^{-(n+1)}(x))$) is the determinant of the multiplication by x (resp. $\varphi^{-(n+1)}(x)$) over $\mathbf{B}$ (resp. $K_{n+1}[[t]]$) considered as a $\varphi(\mathbf{B})$-vector space (resp. $K_n[[t]]$-module) and the commutativity of the diagram follows from the fact $\varphi^{(n+1)}$ is a ring homomorphism and $\varphi^{-n}\circ \mathrm{N} = \varphi^{-(n+1)}\circ \mathrm{N}_{\mathbf{B}/\varphi(\mathbf{B})}$. □

Denote the map θ_n the homorphism $\theta\circ\varphi^{-n}$ where $\theta : \mathbf{B}_{\mathrm{dR}} \to \mathbf{C}_p$ and $\varphi^{-n} : \mathbf{B}^{\dagger,r_n} \to \mathbf{B}_{\mathrm{dR}}$.

Lemma 9.4.3. *If $u = (u^{(n)}) \in \varprojlim \mathscr{O}_{K_n}$ and $n \geq n(K)$, then $\theta_n(\widehat{\iota_K(u)}) = u^{(n)}$.*

Proof. By the preceeding lemma, $(\theta_n(\widehat{\iota_K(u)}))_{n\geq n(K)}$ belongs to $\varprojlim \mathscr{O}_{K_n}$. On the other hand, since $[\iota_K(u)] - \widehat{\iota_K(u)} \in \widetilde{\mathbf{A}}_K^{\dagger,r_{n(K)}} \cap p\widetilde{\mathbf{A}}$, which implies that if $n \geq n(K)$, then $v_p(\theta_n([\iota_K(u)] - \theta_n(\widehat{\iota_K(u)})) \geq 1 - \frac{1}{p^{n-n(K)}}$ and since $v_p(\theta_n([\iota_K(u)] - u^{(n)}) \geq \frac{1}{p}$ if n large enough, we show that $(\theta_n(\widehat{\iota_K(u)})_{n\geq n(K)}$ has same image as u in $\mathbf{E}_K^+$ (c.f. proposition 4.1.1), so it is equal. □

Proposition 9.4.4. *Let K be a finite extension of $\mathbf{Q}_p$, $F = K_\infty \cap \mathbf{Q}_p^{ur}$ and $e_K = [K_\infty : F_\infty]$.*

i) If $e_K = 1$ and $u \in \varprojlim \mathscr{O}_{K_n}$, then $\widehat{\iota_K(u)} = \mathrm{Col}_u(\pi)$.

ii) When $e_K \geq 2$, there exist Laurent series $f_0, \cdots, f_{e_K-1} \in \mathscr{O}_F((T))$ converges in the annulus $0 < v_p(x) < \frac{1}{(p-1)p^{n(K)-1}}$ such that, if $n \geq n(K)$, then $(u^n)^{e_K} + f_{e_K-1}^{\varphi^{-n}}(\varepsilon^{(n)}-1)(u^{(n)})^{e_K-1} + \cdots + f_0^{\varphi^{-n}}(\varepsilon^{(n)}-1) = 0$.

Proof. By corollary 9.3.5, $\widehat{\iota_K(u)} \in \mathbf{A}_F^+$ if $u \in \varprojlim \mathscr{O}_{K_n}$. In particular, there exists $f \in \mathscr{O}_F[[T]]$ such that $\widehat{\iota_K(u)} = f(\pi)$. On the other hand, by applying lemma 9.4.3 to the map θ_n, we obtain $u^{(n)} = f^{\varphi^{-n}}(\varepsilon^{(n)}-1)$, which shows $f = \mathrm{Col}_u$ by the characterization of Col_u.

ii) By corollary 9.3.5, $\widehat{\iota_K(u)} \in \mathbf{A}_K^{\dagger,r_{n(K)}}$. On the other hand, $\mathbf{A}_K^{\dagger,r_{n(K)}}$ is of dimension e_K over $\mathbf{A}_F^{\dagger,r_{n(K)}}$ (by the definition of $n(K)$); so we can find elements $\widetilde{f}_0, \cdots, \widetilde{f}_{e-1} \in \mathbf{A}_F^{\dagger,r_{n(K)}}$ such that we have $\widehat{\iota_K(u)}^{e_K} + \widetilde{f}_{e-1}\widehat{\iota_K(u)}^{e_K-1} + \cdots + \widetilde{f}_0 = 0$, by lemma 9.4.3, we obtain the result. □

9.5 The map $\mathrm{Log}_{\mathbf{Q}_p(1)}$ and $\mathrm{Exp}^*_{\mathbf{Q}_p}$

Lemma 9.5.1. *If $u \in \mathbf{E}_K$, the sequence $(\varphi^{-n}(\widehat{\iota_K(u)}))^{p^n}$ converges to $[\iota_K(u)]$ in $\widetilde{\mathbf{A}}$ and $\mathbf{B}_{\mathrm{dR}}^+$.*

Proof. Since $\widehat{\iota_K(u)} \in \mathbf{A}^{\dagger,r_{n(K)}}$ with image $\iota_K(u)$ in $\mathbf{E}$, it can be written in the form $[\iota_K(u)] + \sum_{k=1}^{+\infty} p^k[x_k]$, where x_k are elements of $\widetilde{\mathbf{E}}$ satisfying $v_E(x_k) \geq -kp^{n(K)}$. We have the formula $v_n = \varphi^{-n}(\widehat{\iota_K(u)}) = [\iota_K(u)^{p^{-n}}] + \sum_{k=1}^{+\infty} p^k[x_k^{p^{-n}}]$ and the congruence $v_n^{p^n} \equiv [\iota_K(u)] \bmod p^{n+1}\widetilde{\mathbf{A}}$, thus it converges in $\widetilde{\mathbf{A}}$.

Let α an element in $\widetilde{\mathbf{E}}^+$ verifying $v_E(\alpha) = \frac{p-1}{p}$, thus $(\frac{p}{[\alpha]})^i$ tends to 0 in $\mathbf{B}_{\mathrm{dR}}^+$ as i tends to $+\infty$. If $n \geq n(K)+1$, the above formula shows that v_n belongs to the subring A (c.f. section 5.4) of $\mathbf{B}_{\mathrm{dR}}^+$ of elements of the form $y = \sum_{i=0}^{+\infty} y_i(\frac{p}{[\alpha]})^i$, where y_i are elements in $\mathbf{A}$ and we have $v_n - [\iota_K(u)^{p^{-n}}] \in \frac{p}{[\alpha]}A$. We deduce that $v_n^{p^n}$ tends to $[\iota_K(u)]$ in A and a fortiori in $\mathbf{B}_{\mathrm{dR}}^+$. □

Proposition 9.5.2. *Let K be a finite extension of $\mathbf{Q}_p$ and $u \in \varprojlim \mathscr{O}^*_{K_n}$.*

i) $\mathrm{Log}_{\mathbf{Q}_p(1)}(\kappa(u)) = t^{-1}\log[\iota_K(u)]$

ii) If $n \geq n(K)$, then $T_n(\mathrm{Log}_{\mathbf{Q}_p(1)}(\kappa(u))) = t^{-1}\log\varphi^{-n}(\widehat{\iota_K(u)})$.

iii) $\mathrm{Exp}^*_{\mathbf{Q}_p}(\kappa(u)) = \widehat{\iota_K(u)}^{-1}\partial\widehat{\iota_K(u)}$*, where ∂ is the derivation $(1+\pi)\frac{d}{d\pi}$ (see 7.2).*

Proof. By construction of the Kummer map, if u_n is any element in $\widetilde{\mathbf{E}}^+$ satisfying $u_n^{(0)} = u^{(n)}$, then $\tau \mapsto (1-\tau)(\frac{\log[u_n]}{t}(1))$ is a 1-cocycle on G_{K_n} with values in $\mathbf{Q}_p(1)$ whose image in $H^1(K_n, \mathbf{Q}_p(1))$ is equal to $\kappa_n(u^{(n)})$. Since we suppose that $u^{(n)} \in \mathscr{O}^*_{K_n}$, we have $\log[u_n] \in \mathbf{B}_{\mathrm{cris}}$ and $\frac{\log[u_n]}{t}(1) \in \mathbf{B}_{\mathrm{cris}}^{\varphi=1} \otimes \mathbf{Q}_p(1)$, proving that $\kappa_n(u^{(n)}) \in H^1_e(K_n, \mathbf{Q}_p(1))$. Hence we deduce the formula

$$\mathrm{Log}_{\mathbf{Q}_p(1)}(\kappa(u)) = \lim_{n\to+\infty} p^n \frac{\log[u_n]}{t}(1) = t^{-1}\lim_{n\to+\infty}\log([u_n]^{p^n}).$$

Finally, we have $v_p(\theta([\iota_K(u)^{p^{-n}}]) - \theta([u_n])) \geq \frac{1}{p}$ if n large enough, therefore $[u_n]^{p^n}$ tends to $[\iota_K(u)]$ as n tends to $+\infty$. We complete i).

By i) and lemma 9.5.1, we have

$$\mathrm{T}_n(\mathrm{Log}_{\mathbf{Q}_p(1)}(\kappa(u))) = t^{-1}\lim_{m\to+\infty}\mathrm{T}_n(p^m\log(\varphi^{-m}(\widehat{\iota_K(u)}))).$$

On the other hand, if $m \geq n$, we have $\mathrm{T}_n = \mathrm{Tr}_{K_m[[t]]/K_n[[t]]} \circ T_m$ and sicne $\varphi^{-m}(\widehat{\iota_K(u)})) \in K_m[[t]]$ and the restriction of T_m on $K_m[[t]]$ is multiplication by p^{-m}, we obtain the formula

$$\begin{aligned}\mathrm{T}_n(\mathrm{Log}_{\mathbf{Q}_p(1)}(\kappa(u))) =& t^{-1}\lim_{m\to+\infty}\mathrm{Tr}_{K_m[[t]]/K_n[[t]]}(\log(\varphi^{-m}(\widehat{\iota_K(u)})))\\ =& t^{-1}\lim_{m\to+\infty}\log(\mathrm{N}_{K_m[[t]]/K_n[[t]]}(\varphi^{-m}(\widehat{\iota_K(u)})))\end{aligned}$$

and this completes ii) by using lemma 9.4.2.

Note that t^{-1} is a generator of $\mathbf{D}_{\mathrm{dR}}(\mathbf{Q}_p(1))$. ii) and theorem 8.3.3 implies that if n is large enough, we have

$$\begin{aligned}\varphi^{-n}(\mathrm{Exp}^*_{\mathbf{Q}_p}(\kappa(u))) =& t^{-1}\left(t\frac{d}{dt}\left(p^n\log\varphi^{-n}((\widehat{\iota_K(u)}))\right)\right)\\ =& p^n\frac{\frac{d}{dt}(\varphi^{-n}(\widehat{\iota_K(u)}))}{\varphi^{-n}(\widehat{\iota_K(u)})}\\ =& \varphi^{-n}\left(\widehat{\iota_K(u)}^{-1}\partial\widehat{\iota_K(u)}\right) \quad \text{by lemma 7.2.3},\end{aligned}$$

which completes iii). ☐

9.6 Cyclotomic units and Coates-Wiles homomorphisms

Example 9.6.1. Let $K=\mathbf{Q}_p$, $V=\mathbf{Q}_p(1)$ and $u=(\frac{\zeta_{p^n}-1}{\zeta_{p^n}})_{n\geq 1}\in\varprojlim \mathscr{O}_{F_n}^*$. Then its Coleman's power series is $\mathrm{Col}_u(T)=\frac{1+T}{T}$. By iii) of proposition 9.5.2, we have $\mathrm{Exp}^*_{\mathbf{Q}_p}(\kappa(u))=(\frac{\partial\mathrm{Col}_u(T)}{\mathrm{Col}_u(T)})(\pi)=\frac{1}{\pi}$. On the other hand, since

$$\varphi^{-1}(\pi)^{-1}=([\varepsilon^{\frac{1}{p}}]-1)^{-1}=\frac{1}{\varepsilon^{(1)}\exp(t/p)-1},$$

by iii) of theorem 8.2.1, we have

$$\begin{aligned}\mathrm{Exp}^*_{\mathbf{Q}_p,F_1}(\kappa(u))=&\frac{1}{p}\mathrm{Tr}_{F_1/\mathbf{Q}_p}\varphi^{-1}(\frac{1}{\pi})\\ =&\frac{1}{p}\sum_{\zeta^p=1,\zeta\neq 1}\frac{1}{\zeta\exp(t/p)}\\ =&\frac{-1}{t}(\frac{t}{1-\exp(t)}-\frac{t/p}{1-\exp(t/p)})\\ =&\sum_{k=1}^{+\infty}(1-p^{-k})\zeta(1-k)\frac{(-t)^{k-1}}{(k-1)!}.\end{aligned}$$

Thus by ii) of theorem 8.2.1,

$$\exp^*_{\mathbf{Q}_p(1+k)^*}(\int_{\Gamma_{F_1}}\chi^{-k}\kappa(\mu))=\begin{cases}0 & \text{if } k\leq 0\\ (1-p^{-k})\zeta(1-k)\frac{(-t)^{k-1}}{(k-1)!} & \text{if } k\geq 1\end{cases}.$$

Example 9.6.2. Let $K=\mathbf{Q}_p$, $V=\mathbf{Q}_p(1)$ and $u=(\frac{\zeta^a_{p^n}-1}{\zeta_{p^n}-1})_{n\geq 1}\in\varprojlim \mathscr{O}_{F_n}^*$, where $a\in\mathbf{Z}$. Then its Coleman's power series is $\mathrm{Col}_u(T)=\frac{(1+T)^a-1}{T}$. By iii) of proposition 9.5.2, we have $\mathrm{Exp}^*_{\mathbf{Q}_p}(\kappa(u))=(\frac{\partial\mathrm{Col}_u(T)}{\mathrm{Col}_u(T)})(\pi)=\frac{a(1+\pi)^a}{(1+T)^a-1}-\frac{1+T}{T}$. On the other hand, since

$$\varphi^{-1}(\pi)^{-1}=([\varepsilon^{\frac{1}{p}}]-1)^{-1}=\frac{1}{\varepsilon^{(1)}\exp(t/p)-1},$$

by iii) of theorem 8.2.1, we have

$$\begin{aligned}\mathrm{Exp}^*_{\mathbf{Q}_p,F_1}(\kappa(u))=&\frac{1}{p}\mathrm{Tr}_{F_1/\mathbf{Q}_p}\varphi^{-1}(\mathrm{Exp}^*_{\mathbf{Q}_p}(\kappa(u)))\\ =&a-1+\frac{1}{p}\sum_{\zeta^p=1,\zeta\neq 1}\frac{a}{\zeta\exp at/p-1}-\frac{1}{\zeta\exp t/p}\\ =&a-1+\frac{-1}{t}(\frac{at}{1-\exp(at)}-\frac{at/p}{1-\exp(at/p)}-\frac{t}{1-\exp(t)}+\frac{t/p}{1-\exp(t/p)})\\ =&\sum_{k=1}^{+\infty}(1-p^{-k})(a^k-1)\zeta(1-k)\frac{(-t)^{k-1}}{(k-1)!}.\end{aligned}$$

Thus by ii) of theorem 8.2.1,

$$\exp^*_{\mathbf{Q}_p(1+k)^*}(\int_{\Gamma_{F_1}} \chi^{-k}\kappa(\mu)) = \begin{cases} 0 & \text{if } k \le 0 \\ (a^k-1)(1-p^{-k})\zeta(1-k)\frac{(-t)^{k-1}}{(k-1)!} & \text{if } k \ge 1 \end{cases}.$$

Example 9.6.3. Let $K = \mathbf{Q}_p(\zeta_d)$, $V = \mathbf{Q}_p(1)$ and ε be a Dirichlet character of conductor $d \ge 1$ prime to p. Set $u = \left(\frac{-1}{G(\varepsilon^{-1})}\sum_{b \bmod d} \frac{\varepsilon^{-1}(b)}{\zeta_d^b \zeta_{p^n}-1}\right)_{n\ge 1} \in \varprojlim \mathscr{O}^*_{K_n}$, then we have

$$\mathrm{Col}_u(T) = \frac{-1}{G(\varepsilon^{-1})}\sum_{b \bmod d} \frac{\varepsilon^{-1}(b)}{\zeta_d^b(1+T)-1}$$

and thus

$$\mathrm{Exp}^*_{\mathbf{Q}_p}(\kappa(u)) = \frac{-1}{G(\varepsilon^{-1})}\sum_{b \bmod d} \frac{\varepsilon^{-1}(b)}{\zeta_d^b(1+\pi)-1}.$$

Hence we have,

$$\begin{aligned}
\mathrm{Exp}^*_{\mathbf{Q}_p,K_1}(\kappa(u)) =& p^{-1}\mathrm{Tr}_{K_1/K}\varphi^{-1}(\mathrm{Exp}^*_{\mathbf{Q}_p}(\kappa(u))) \\
=& p^{-1}\frac{-1}{G(\varepsilon^{-1})}\sum_{z^p=1, z\neq 1}\sum_{b \bmod d}\varepsilon^{-1}(b)\frac{1}{\zeta_d^{b/p} z\exp(t/p)-1} \\
=& \frac{-1}{G(\varepsilon^{-1})}\sum_{b \bmod d}\varepsilon^{-1}(b)\left(\frac{1}{1-\zeta_d^b\exp(t)} - p^{-1}\frac{1}{1-\zeta_d^{b/p}\exp(t/p)}\right) \\
=& \sum_{b \bmod d}\frac{\varepsilon(b)\exp(bt)}{1-\exp(dt)} - p^{-1}\varepsilon(p)\frac{\varepsilon(b)\exp(bt/p)}{1-\exp(dt/p)} \\
=& \sum_{k=1}^{+\infty}(1-\varepsilon(p)p^{-k})\mathrm{L}(1-k,\varepsilon)\frac{t^{k-1}}{(k-1)!}
\end{aligned}$$

and thus

$$\exp^*_{\mathbf{Q}_p^*(1+k)}(\int_{\Gamma_{K_1}} \chi^{-k}\kappa(\mu)) = \begin{cases} 0 & \text{if } k \le 0 \\ (1-\varepsilon(p)p^{-k})\mathrm{L}(1-k,\varepsilon)\frac{t^{k-1}}{(k-1)!} & \text{if } k \ge 1 \end{cases}.$$

This allow us to define a homomorphism $\mathrm{CW}_{k,n}$ from $H^1_{\mathrm{Iw}}(K,V)$ to $K_n \otimes \mathbf{D}_{\mathrm{dR}}(V)$ by putting

$$\mathrm{CW}_{k,n}(\mu) = \partial_k(\mathrm{T}_{K_n}(\mathrm{Log}_V(\mu))).$$

for each $n \in \mathbf{N}$ and $k \in \mathbf{Z}$, the homomorphism is a generalization of Coates-Wiles homomorphism and we have the following theorem by proposition 8.3.1.

Theorem 9.6.4. *If $\mu \in H^1_{\mathrm{Iw}}(K,V)$, if $n \in \mathbf{N}$ and $k \in \mathbf{Z}$, then*

$$\mathrm{CW}_{k,n}(\mu) = -\exp^*(\int_{\Gamma_{K_n}} \chi(x)^{-k}\mu).$$

Remark 9.6.5. The map

$$\varprojlim \mathscr{O}^*_{\mathbf{Q}_p(\mu_{p^n})} \to H^1_{\mathrm{Iw}}(\mathbf{Q}_p, \mathbf{Q}_p(1)) \to \mathbf{Q}_p, \quad u \mapsto \exp^*_{\mathbf{Q}_p^*(1+k)}(\int_{\Gamma_{F_1}} \chi^{-k}\kappa(\mu))$$

is just the classical Coates-Wiles homomorphism ([7] section 2.6).

Chapter 10

(φ,Γ)-modules and differential equations

10.1 The rings $\mathbf{B}_{\max}$ and $\widetilde{\mathbf{B}}^+_{\mathrm{rig}}$

The ring $\mathbf{B}^+_{\max}$ is defined by

$$\mathbf{B}^+_{\max} = \{\sum_{n\geq 0} a_n \frac{\omega^n}{p^n} \mid a_n \in \widetilde{\mathbf{B}}^+ \text{ is a sequence converges to } 0\},$$

and $\mathbf{B}_{\max} = \mathbf{B}^+_{\max}[\frac{1}{t}]$. It is closely related to $\mathbf{B}_{\mathrm{cris}}$ but tends to be more amenable. One could replace ω by any generator of $\ker(\theta)$ in $\widetilde{\mathbf{A}}^+$. The ring $\mathbf{B}_{\max}$ injects canonically into $\mathbf{B}_{\mathrm{dR}}$ and, in particular, it is endowed with the induced Galois action and filtration, as well as with a continuous Frobenius φ, extending the map $\varphi : \widetilde{\mathbf{B}}^+ \to \widetilde{\mathbf{B}}^+$. Note that φ deos not extend continuously to $\mathbf{B}_{\mathrm{dR}}$. We set $\widetilde{\mathbf{B}}^+_{\mathrm{rig}} = \cap_{n=0}^{+\infty} \varphi^n(\mathbf{B}^+_{\max})$.

We call a representation V of G_K is crystalline if it is $\mathbf{B}_{\mathrm{cris}}$-admissible, which is equivalent to $\mathbf{B}_{\max}$-admissible or $\widetilde{\mathbf{B}}^+_{\mathrm{rig}}[\frac{1}{t}]$-admissible (because $\cap_{n=0}^{+\infty}\varphi^n(\mathbf{B}^+_{\max}) = \cap_{n=0}^{+\infty}\varphi^n(\mathbf{B}^+_{\mathrm{cris}})$ and the periods of crystalline representations live in finite dimensional F-vector subspaces of $\mathbf{B}_{\max}$, stable by φ and so in fact in $\cap_{n=0}^{\infty}\varphi^n(\mathbf{B}^+_{\max}[\frac{1}{t}])$; that is, the F-vector space

$$\mathbf{D}_{\mathrm{cris}}(V) = (\mathbf{B}_{\mathrm{cris}} \otimes_{\mathbf{Q}_p} V)^{G_K} = (\mathbf{B}_{\max} \otimes_{\mathbf{Q}_p} V)^{G_K} = (\widetilde{\mathbf{B}}^+_{\mathrm{rig}}[\frac{1}{t}] \otimes_{\mathbf{Q}_p} V)^{G_K}$$

is of dimension $d = \dim_{\mathbf{Q}_p}(V)$. Then $\mathbf{D}_{\mathrm{cris}}(V)$ is endowed with a Frobenius φ induced by that of $\mathbf{B}_{\max}$ and $(\mathbf{B}_{\mathrm{dR}} \otimes_{\mathbf{Q}_p} V)^{G_K} = \mathbf{D}_{\mathrm{dR}}(V) = K \otimes_F \mathbf{D}_{\mathrm{cris}}(V)$ so that a crystalline representation is also de Rham and $K \otimes_F \mathbf{D}_{\mathrm{cris}}(V)$ is a filtered K-vector space.

If V is a p-adic representation, we say V is Hodge-Tate, with Hodge Tate weights $h_1,\dots,h_d$, if we have a decomposition $\mathbf{C}_p \otimes_{\mathbf{Q}_p} V \cong \oplus_{j=1}^d \mathbf{C}_p(h_j)$. We say that V is positive if its Hodge-Tate weights are all negative. By using the map $\theta : \mathbf{B}^+_{\mathrm{dR}} \to \mathbf{C}_p$, it is easy to see that a de Rham representation is Hodge-Tate and that the Hodge-Tate weights of V are those integers h such that $\mathrm{Fil}^{-h}\mathbf{D}_{\mathrm{dR}}(V) \neq \mathrm{Fil}^{-h+1}\mathbf{D}_{\mathrm{dR}}(V)$.

10.2 The structure of $D(T)^{\psi=1}$

Recall in section 4, we introduced (φ,Γ)-modules and their relation with Galois representations. Let us now set $K=F$ (i.e. we are working in an unramified extension of $\mathbf{Q}_p$). We say that a p-adic representation V of G_F is of finite height if $D(V)$ has a basis over $\mathbf{B}_F$ made up of elements of $D^+(V)=(\mathbf{B}^+\otimes_{\mathbf{Q}_p}V)^{H_F}$. A result of [10, proposition III.2] shows that V is of finite height if and only if $D(V)$ has a sub-$\mathbf{B}_F^+$-module which is free of rank d, and stable by φ. Let us recall the main result of [10, theorem 1] regarding crystalline representation of G_F:

Theorem 10.2.1. *If V is a crystalline representation of G_F, then V is of finite height.*

Let V be a crystalline representation of G_F and let T denote a G_F stable lattice of V. The following proposition is proved in [2, proposition II.1.1]

Proposition 10.2.2. *If T is a lattice in a positive crystalline representation V, then there exists a unique sub-$\mathbf{A}_F^+$-module $\mathbf{N}(T)$ of $D^+(T)$, which satisfies the following conditions:*

1. *$\mathbf{N}(T)$ is an free $\mathbf{A}_F^+$-module of rank $d=dim_{\mathbf{Q}_p}V$;*

2. *the action of Γ_F preserves $\mathbf{N}(T)$ and is trivial on $\mathbf{N}(T)/\pi\mathbf{N}(T)$;*

3. *there exists an integer $r\geq 0$ such that $\pi^r D^+(T)\subset\mathbf{N}(T)$.*

Moreover, $\mathbf{N}(T)$ is stable by φ, and the $\mathbf{B}_F^+$-module $\mathbf{N}(V)=\mathbf{B}_F^+\otimes_{\mathbf{A}_F^+}\mathbf{N}(T)$ is the unique sub-$\mathbf{B}_F^+$-module of $D^+(V)$ satisfying the corresponding conditions.

The $\mathbf{A}_F^+$-module $\mathbf{N}(T)$ is called the Wach module associated to T.

Notice that $\mathbf{N}(T(-1))=\pi\mathbf{N}(T)\otimes e_{-1}$. When V is no longer positive, we can therefore define $\mathbf{N}(T)$ as $\pi^{-h}\mathbf{N}(T(-h))\otimes e_h$ for h large enough so that $V(-h)$ is positive. Using the results of [2, III.4], one can show that:

Proposition 10.2.3. *If T is a lattice in a crystalline representation V of G_F, whose Hodge-Tate weights are in $[a;b]$, then $\mathbf{N}(T)$ is the unique sub-$\mathbf{A}_F^+$-module of $D^+(T)[1/\pi]$ which is free of rank d, stable by Γ_F with the action of Γ_F being trivial on $\mathbf{N}(T)/\pi\mathbf{N}(T)$ and such that $\mathbf{N}(T)[1/\pi]=D^+(T)[1/\pi]$.*

Finally, we have $\varphi(\pi^b\mathbf{N}(R))\subset\pi^b\mathbf{N}(T)$ and $\pi^b\mathbf{N}(T)/\varphi^*(\pi^b)$ is killed by q^{b-a}, where $q=\varphi(\omega)$. The construction $T\mapsto\mathbf{N}(T)$ gives a bijection between Wach modules over $\mathbf{A}_F^+$ which are lattices in $\mathbf{N}(V)$ and Galois lattices T in V.

Indeed $D(V)^{\psi=1}$ is not very far from being included in $\mathbf{N}(V)$:

Theorem 10.2.4. *If V is a crystalline representation of G_F, whose Hodge-Tate weights are in $[a;b]$, then $D(V)^{\psi=1}\subset\pi^{a-1}\mathbf{N}(V)$. In addition, if V has no quotient isomorphic to $\mathbf{Q}_p(a)$, then actually $D(V)^{\psi=1}\subset\pi^a\mathbf{N}(V)$.*

Proof. See [1, Theorem A.3]. □

10.3 p-adic representations and differential equations

In this paragraph, we recall some of the results of [3], which allow us to recover $\mathbf{D}_{\mathrm{cris}}(V)$ from the (φ,Γ)-module associated to V. Let $\mathscr{H}_{F'}^{\alpha}$ be the set of power series $f(T)=\sum_{k\in\mathbf{Z}} a_k T^k$ such that a_k is a sequence (not necessarily bounded) of elements of F', and such that $f(T)$ is holomorphic on the p-adic annulus $\{p^{-1/\alpha}\leq |T|<1\}$.

For $r\geq r(K)$ (c.f. proposition 7.2.1), define $\widetilde{\mathbf{B}}_{\mathrm{rig},K}^{\dagger,r}$ as the set of $f(\pi_K)$ where $f(T)\in\mathscr{H}_{F'}^{e_K r}$. Obviously, $\mathbf{B}_K^{\dagger,r}\subset\widetilde{\mathbf{B}}_{\mathrm{rig},K}^{\dagger,r}$ and the second ring is the completion of the first one for the natural Fréchet topology. If V is a p-adic representation, let

$$\mathbf{D}_{\mathrm{rig}}^{\dagger,r}(V)=\widetilde{\mathbf{B}}_{\mathrm{rig},K}^{\dagger,r}\otimes_{\mathbf{B}_K^{\dagger,r}}\mathbf{D}^{\dagger,r}(V)\quad\text{and}\quad\mathbf{D}_{\mathrm{rig}}^{\dagger}(V)=(\widetilde{\mathbf{B}}_{\mathrm{rig}}^{\dagger})^{H_K}\otimes_{\mathbf{B}_K^{\dagger}}\mathbf{D}^{\dagger}(V).$$

One of the main technical tools of [3] is the construction of a large ring $\widetilde{\mathbf{B}}_{\mathrm{rig}}^{\dagger}$, which contains $\widetilde{\mathbf{B}}_{\mathrm{rig}}^{+}$ and $\widetilde{\mathbf{B}}^{\dagger}$. This ring is a bridge between p-adic Hodge theory and the thoery of (φ,Γ)-modules.

As a consequence of the above two inclusions, we have:

$$\mathbf{D}_{\mathrm{cris}}(V)\subset(\widetilde{\mathbf{B}}_{\mathrm{rig}}^{\dagger}[\frac{1}{t}]\otimes_{\mathbf{Q}_p}V)^{G_K}\quad\text{and}\quad\mathbf{D}_{\mathrm{rig}}^{\dagger}(V)[\frac{1}{t}]\subset(\widetilde{\mathbf{B}}_{\mathrm{rig}}^{\dagger}[\frac{1}{t}]\otimes_{\mathbf{Q}_p}V)^{H_K}.$$

One of the main result of [3] is:

Theorem 10.3.1. *If V is a p-adic representation of G_K then $\mathbf{D}_{\mathrm{cris}}(V)=(\mathbf{D}_{\mathrm{rig}}^{\dagger}(V)[\frac{1}{t}])^{\Gamma_K}$. If V is positive, then $\mathbf{D}_{\mathrm{cris}}(V)=\mathbf{D}_{\mathrm{rig}}^{\dagger}(V)^{\Gamma_K}$.*

Proof. See [3, theorem 3.6]. □

Note that $\widetilde{\mathbf{B}}_{\mathrm{rig},K}^{\dagger,r}$ is the completion of $\mathbf{B}_K^{\dagger,r}$ for the ring's natural Fréchet topology and that $\mathbf{B}_{\mathrm{rig},K}^{\dagger}$ is the union of the $\widetilde{\mathbf{B}}_{\mathrm{rig},K}^{\dagger,r}$. Similarly, there is a natural Fréchet topology on $\widetilde{\mathbf{B}}^{\dagger,r}$, $\widetilde{\mathbf{B}}_{\mathrm{rig}}^{\dagger,r}$ is the completion of $\widetilde{\mathbf{B}}^{\dagger,r}$ for that topology and $\widetilde{\mathbf{B}}_{\mathrm{rig}}^{\dagger}=\cup_{r\geq 0}\widetilde{\mathbf{B}}_{\mathrm{rig}}^{\dagger,r}$. Actually, one can show that $\widetilde{\mathbf{B}}_{\mathrm{rig}}^{+}\subset\widetilde{\mathbf{B}}_{\mathrm{rig}}^{\dagger,r}$ for any r and there is an exact sequence

$$0\longrightarrow\widetilde{\mathbf{B}}^{+}\longrightarrow\widetilde{\mathbf{B}}_{\mathrm{rig}}^{+}\oplus\widetilde{\mathbf{B}}^{\dagger,r}\longrightarrow\widetilde{\mathbf{B}}_{\mathrm{rig}}^{\dagger,r}\longrightarrow 0$$

which one can take as providing a definition of $\widetilde{\mathbf{B}}_{\mathrm{rig}}^{\dagger,r}$.

Recall that if $n\geq 0$ and $r_n=p^{n-1}(p-1)$, then there is a well-defined injective map $\varphi^{-n}:\widetilde{\mathbf{B}}^{\dagger,r_n}\to\mathbf{B}_{\mathrm{dR}}^{+}$ (c.f. section 7.2), and the map extends to an injective map $\varphi^{-n}:\widetilde{\mathbf{B}}_{\mathrm{rig}}^{\dagger,r_n}\to\mathbf{B}_{\mathrm{dR}}^{+}$ (see [3, corollary 2.13]).

Let $\mathbf{B}_{\mathrm{rig},F}^{+}$ be the set of $f(\pi)$ where $f(T)=\sum_{k\geq 0}a_kT^k$ with $a_k\in F$, and such that $f(T)$ is holomorphic on the p-adic open unit disk. Set $\mathbf{D}_{\mathrm{rig}}^{+}(V)=\mathbf{B}_{\mathrm{rig},F}^{+}\otimes_{\mathbf{B}_F^{+}}D^{+}(V)$. One can show the following refinement of theorem 10.3.1:

Proposition 10.3.2. *We have $\mathbf{D}_{\mathrm{cris}}(V)=(\mathbf{D}_{\mathrm{rig}}^{+}(V)[1/t])^{\Gamma_F}$ and if V is positive then $\mathbf{D}_{\mathrm{cris}}(V)=\mathbf{D}_{\mathrm{rig}}^{+}(V)^{\Gamma_F}$.*

Indeed if $\mathbf{N}(V)$ is the Wach module associated to V, then $\mathbf{N}(V)\subset D^{+}(V)$ when V is positive and it is shown in [1, II.2] that under that hypothesis, $\mathbf{D}_{\mathrm{cris}}(V)=(\mathbf{B}_{\mathrm{rig},F}^{+}\otimes_{\mathbf{B}_F^{+}}\mathbf{N}(V))^{\Gamma_F}$.

10.4 The Fontaine isomorphism revisited

The purpose of this section is to recall the constructions in section 5.2 and extend them a little bit. Let V be a p-adic representation of G_K. Recall in section 5.2, we constructed a map $h^1_{K,V} : D(V)^{\psi=1} \to H^1(K,V)$ such that when Γ_K is torsion free, it gives rise to an exact sequence:

$$0 \longrightarrow D(V)^{\psi=1}_{\Gamma_K} \xrightarrow{h^1_{K,V}} H^1(K,V) \longrightarrow \left(\frac{D(V)}{\psi-1}\right)^{\Gamma_K} \longrightarrow 0$$

We shall extend $h^1_{K,V}$ to a map $h^1_{K,V} : \mathbf{D}^{\dagger}_{\mathrm{rig}}(V)^{\psi=1} \to H^1(K,V)$.

Lemma 10.4.1. *If r is large enough and $\gamma \in \Gamma_K$ then*

$$1-\gamma : \mathbf{D}^{\dagger,r}_{\mathrm{rig}}(V)^{\psi=0} \to \mathbf{D}^{\dagger,r}_{\mathrm{rig}}(V)^{\psi=0}$$

is an isomorphism

Proof. We first show that $1-\gamma$ is injective. By theorem 10.3.1, an element in the kernel of $1-\gamma$ would be in $\mathbf{D}_{\mathrm{cris}}(V)$ and therefore in $\mathbf{D}_{\mathrm{cris}}(V)^{\psi=0}$, which is obviously 0.

To prove surjectivity. Recall that by iii) of proposition 7.3.2, if r is large enough and $\gamma \in \Gamma_K$ thern $1-\gamma : \mathbf{D}^{\dagger,r}(V)^{\psi=0} \to \mathbf{D}^{\dagger,r}(V)^{\psi=0}$ is an isomorphism whose inverse is uniformly continuous for the Fréchet topology of $\mathbf{D}^{\dagger,r}(V)$.

In order to show the surjectivity of $1-\gamma$ it is therefore enough to show that $\mathbf{D}^{\dagger,r}(V)^{\psi=0}$ is dense in $\mathbf{D}^{\dagger,r}_{\mathrm{rig}}(V)^{\psi=0}$ for the Fréchet topology. For r large enough, $\mathbf{D}^{\dagger,r}(V)$ has a basis in $\varphi(\mathbf{D}^{\dagger,r/p}(V))$ so that

$$\begin{aligned}\mathbf{D}^{\dagger,r}(V)^{\psi=0} &= (\mathbf{B}^{\dagger,r}_K)^{\psi=0} \cdot \varphi(\mathbf{D}^{\dagger,r/p}(V))\\ \mathbf{D}^{\dagger,r}_{\mathrm{rig}}(V)^{\psi=0} &= (\widetilde{\mathbf{B}}^{\dagger,r}_{\mathrm{rig},K})^{\psi=0} \cdot \varphi(\mathbf{D}^{\dagger,r/p}_{\mathrm{rig}}(V)).\end{aligned}$$

The fact that $\mathbf{D}^{\dagger,r}(V)^{\psi=0}$ is dense in $\mathbf{D}^{\dagger,r}_{\mathrm{rig}}(V)^{\psi=0}$ for the Fréchet topology will therefore follow from the density of $(\mathbf{B}^{\dagger,r}_K)^{\psi=0}$ in $(\widetilde{\mathbf{B}}^{\dagger,r}_{\mathrm{rig},K})^{\psi=0}$. The last statement follows from the facts that by definition $\mathbf{B}^{\dagger,r/p}_K$ is dense in $\widetilde{\mathbf{B}}^{\dagger,r/p}_{\mathrm{rig},K}$ and that

$$(\mathbf{B}^{\dagger,r}_K)^{\psi=0} = \oplus_{i=1}^{p-1}[\varepsilon]^i\varphi(\mathbf{B}^{\dagger,r/p}_K) \quad \textit{and} \quad (\widetilde{\mathbf{B}}^{\dagger,r}_{\mathrm{rig},K})^{\psi=0} = \oplus_{i=1}^{p-1}[\varepsilon]^i\varphi(\widetilde{\mathbf{B}}^{\dagger,r/p}_{\mathrm{rig},K}).$$

□

Lemma 10.4.2. *The following maps are all surjective and the kernel is $\mathbf{Q}_p$*

$$1-\varphi : \widetilde{\mathbf{B}}^{\dagger} \to \widetilde{\mathbf{B}}^{\dagger}, \quad 1-\varphi : \widetilde{\mathbf{B}}^{+}_{\mathrm{rig}} \to \widetilde{\mathbf{B}}^{+}_{\mathrm{rig}} \quad \textit{and} \quad 1-\varphi : \widetilde{\mathbf{B}}^{\dagger}_{\mathrm{rig}} \to \widetilde{\mathbf{B}}^{\dagger}_{\mathrm{rig}}$$

Proof. Since $\widetilde{\mathbf{B}}^+_{\mathrm{rig}} \subset \mathbf{B}^\dagger_{\mathrm{rig}}$ and $\widetilde{\mathbf{B}}^\dagger \subset \widetilde{\mathbf{B}}^\dagger_{\mathrm{rig}}$ it is enough to show that $(\widetilde{\mathbf{B}}^\dagger_{\mathrm{rig}})^{\varphi=1} = \mathbf{Q}_p$. If $x \in (\widetilde{\mathbf{B}}^\dagger_{\mathrm{rig}})^{\varphi=1}$, then [3, proposition 3.2] shows that actually $x \in (\widetilde{\mathbf{B}}^+_{\mathrm{rig}})^{\varphi=1}$, and therefore $x \in (\widetilde{\mathbf{B}}^+_{\mathrm{rig}})^{\varphi=1} = (\mathbf{B}^+_{\max})^{\varphi=1} = \mathbf{Q}_p$ by [9, proposition III 3.5].

The surjectivity of $1-\varphi : \widetilde{\mathbf{B}}^+_{\mathrm{rig}} \to \widetilde{\mathbf{B}}^+_{\mathrm{rig}}$ results from the surjectivity of $1-\varphi$ on the first two spaces since by [3, lemma 2.18], one can write $\alpha \in \widetilde{\mathbf{B}}^+_{\mathrm{rig}}$ as $\alpha = \alpha^+ + \alpha^-$ with $\alpha^+ \in \widetilde{\mathbf{B}}^+_{\mathrm{rig}}$ and $\alpha^- \in \widetilde{\mathbf{B}}^\dagger$.

The surjectivity of $1-\varphi : \widetilde{\mathbf{B}}^+_{\mathrm{rig}} \to \widetilde{\mathbf{B}}^+_{\mathrm{rig}}$ follows from the facts that $1-\varphi : \mathbf{B}^+_{\max} \to \mathbf{B}^+_{\max}$ is surjective ([9, proposition III 3.1]) and that $\widetilde{\mathbf{B}}^+_{\mathrm{rig}} = \cap_{n=0}^{\infty} \varphi^n(\mathbf{B}^+_{\max})$.

The surjectivity of $1-\varphi : \widetilde{\mathbf{B}}^\dagger \to \widetilde{\mathbf{B}}^\dagger$ follows from the facts that $1-\varphi : \widetilde{\mathbf{B}} \to \widetilde{\mathbf{B}}$ is surjective (it is surjective on $\widetilde{\mathbf{A}}$ as can be seen by reducing modulo p and using the fact that $\widetilde{\mathbf{E}}$ is algebraically closed) and that if $\beta \in \widetilde{\mathbf{B}}$ is such that $(1-\varphi)\beta \in \widetilde{\mathbf{B}}^\dagger$, then $\beta \in \widetilde{\mathbf{B}}^\dagger$.

If $x = \sum_{i=0}^{+\infty} p^i [x_i] \in \widetilde{\mathbf{A}}$, let us set $w_k(x) = \inf_{i \leq k} v_E(x_i) \in \mathbb{R} \cup \{+\infty\}$. The definition of $\widetilde{\mathbf{B}}^{\dagger,r}$ shows that $x \in \widetilde{\mathbf{B}}^{\dagger,r}$ if and only if $\lim_{k\to+\infty} w_k(x) + \frac{pr}{p-1}k = +\infty$. A short computation shows that $w_k(\varphi(x)) = pw_k(x)$ and that $w_k(x+y) \geq \inf(w_k(x), w_k(y))$ with equality if $w_k(x) \neq w_k(y)$.

It is then clear that

$$\lim_{k\to+\infty} w_k((1-\varphi)x) + \frac{pr}{p-1}k = +\infty \Longrightarrow \lim_{k\to+\infty} w_k(x) + \frac{p(r/p)}{p-1}k = +\infty$$

and so if $x \in \widetilde{\mathbf{A}}$ is such that $(1-\varphi)x \in \widetilde{\mathbf{B}}^{\dagger,r}$ then $x \in \widetilde{\mathbf{B}}^{\dagger,r/p}$ and likewise for $x \in \widetilde{\mathbf{B}}$ by multiplication by a suitable power of p. This shows the second fact. □

Proposition 10.4.3. *If $y \in \mathbf{D}^\dagger_{\mathrm{rig}}(V)^{\psi=1}$ and Γ_K is torsion free, there exists $b \in \widetilde{\mathbf{B}}^\dagger_{\mathrm{rig}} \otimes_{\mathbf{Q}_p} V$ such that $(\gamma-1)(\varphi-1)b = (\varphi-1)y$ and the formula*

$$h^1_{K,V}(y) = \log^0_p(\gamma)[\sigma \mapsto \frac{\sigma-1}{\gamma-1}y - (\sigma-1)b]$$

then defines a map $h^1_{K,V} : \mathbf{D}^\dagger_{\mathrm{rig}}(V)^{\psi=1}_{\Gamma_K} \mapsto H^1(K,V)$ which does not depend either on the choice of generator γ of Γ_K or on the particular solution b, and if $y \in D(V)^{\psi=1} \subset \mathbf{D}^\dagger_{\mathrm{rig}}(V)^{\psi=1}$, then $h^1_{K,V}(y)$ coincides with the cocycle constructed in section 5.2.

Proof. Our construction closely follows section 5.2; to simplify the notations, we may assume that $\log^0_p(\gamma) = 1$. The fact that $h^1_{K,V}$ is independent of the choice of γ is same as lemma 5.1.2.

Let us start by showing the existence of $b \in \widetilde{\mathbf{B}}^\dagger_{\mathrm{rig}} \otimes_{\mathbf{Q}_p} V$. If $y \in \mathbf{D}^\dagger_{\mathrm{rig}}(V)^{\psi=1}$, then $(\varphi-1)y \in \mathbf{D}^\dagger_{\mathrm{rig}}(V)^{\psi=0}$. By lemme 10.4.1, there exists $x \in \mathbf{D}^\dagger_{\mathrm{rig}}(V)^{\psi=0}$ such that $(\gamma-1)x = (\varphi-1)y$. By lemma 10.4.2, there exists $b \in \widetilde{\mathbf{B}}^\dagger_{\mathrm{rig}} \otimes_{\mathbf{Q}_p} V$ such that $(\varphi-1)b = x$.

Recall that we define $h^1_{K,V}(y) \in H^1(K,V)$ by the formula:

$$h^1_{K,V}(y)(\sigma) = \frac{\sigma-1}{\gamma-1}y - (\sigma-1)b.$$

Notice that, a priori, $h^1_{K,V}(y) \in H^1(K, \widetilde{\mathbf{B}}^{\dagger}_{\mathrm{rig}} \otimes_{\mathbf{Q}_p} V)$, but

$$\begin{aligned}(\varphi-1)h^1_{K,V}(y)(\sigma) =& \frac{\sigma-1}{\gamma-1}(\varphi-1)y - (\sigma-1)(\varphi-1)b \\ =& \frac{\sigma-1}{\gamma-1}(\gamma-1)x - (\sigma-1)x \\ =& 0,\end{aligned}$$

so that $h^1_{K,V}(y)(\sigma) \in (\mathbf{B}^{\dagger}_{\mathrm{rig}})^{\varphi=1} \otimes_{\mathbf{Q}_p} V = V$. In addition, two different choices of b differ by an element of $(\widetilde{\mathbf{B}}^{\dagger}_{\mathrm{rig}})^{\varphi=1} \otimes_{\mathbf{Q}_p} V = V$, and therefore give rise to two cohomologous cocycles.

It is clear that if $y \in D(V)^{\psi=1} \subset \mathbf{D}^{\dagger}_{\mathrm{rig}}(V)^{\psi=1}$, then $h^1_{K,V}$ coincide with the cocycle constructed in section 5.2, as can be seen by their identical construction, and it is immediate that if $y \in (\gamma-1)\mathbf{D}^{\dagger}_{\mathrm{rig}}(V)$, then $h^1_{K,V}(y) = 0$. $\square$

Lemma 10.4.4. *We have* $\mathrm{cor}_{K_{n+1}/K_n} \circ h^1_{K_{n+1},V} = h^1_{K_n,V}$.

Proof. Same as lemma 6.2.1. $\square$

10.5 Iwasawa algebra and power series

Given a finite unramified extension F of $\mathbf{Q}_p$, denote by $\Lambda(\Gamma_F)$ (resp. $\Lambda(\Gamma^1_F)$ where $\Gamma^1_F = Gal(F_\infty/F_1)$) the Iwasawa algebra $\mathbf{Z}_p[[\Gamma_F]]$ (resp. $\mathbf{Z}_p[[\Gamma^1_F]]$).

Let

$$\mathscr{H} = \{f \in \mathbf{Q}_p[\Delta][[X]] \mid f \text{ convergs on the open unit disk}\},$$

and define $\mathscr{H}(\Gamma_F)$ to be the set of $f(\gamma-1)$ with $f(X) \in \mathscr{H}$ and γ a topological generator of Γ. We may identify $\Lambda(\Gamma_F) \otimes \mathbf{Q}_p$ with the subring of $\mathscr{H}(\Gamma_F)$ consisting of power series with bounded coefficients. Note that $\mathscr{H}(\Gamma)$ may be identified with the continuous dual of the space of locally analytic functions on Γ_F, with multiplication corresponding to convolution, implying that its definition is independent of the choice of generator γ_F (c.f. section 1.2).

The action of Γ_F on $\mathbf{B}^+_{\mathrm{rig},\mathbf{Q}_p}$ gives an isomorphism of $\mathscr{H}(\Gamma_F)$ with $(\mathbf{B}^+_{\mathrm{rig},\mathbf{Q}_p})^{\psi=0}$ via the Mellin transform [20, corollary B.2.8]

$$\begin{aligned}\mathfrak{M} : \mathscr{H}(\Gamma_F) \to& (\mathbf{B}^+_{\mathrm{rig},\mathbf{Q}_p})^{\psi=0} \\ f(\gamma-1) \mapsto& f(\gamma-1)(\pi+1).\end{aligned}$$

In particular, $\Lambda(\Gamma_F)$ corresponds to $(\mathbf{A}^+_{\mathbf{Q}_p})^{\psi=0}$ under $\mathfrak{M}$. Similarly, we define $\mathscr{H}(\Gamma^1_F)$ as the subring of $\mathscr{H}(\Gamma_F)$ defined by power series over $\mathbf{Q}_p$, rather than $\mathbf{Q}_p[\Delta]$. Then, $\mathscr{H}(\Gamma^1_F)$ (resp. $\Lambda(\Gamma^1_F)$) corresponds to $(1+\pi)\varphi(\mathbf{B}^+_{\mathrm{rig},\mathbf{Q}_p})$ (resp. $(1+\pi)\varphi(\mathbf{A}^+_{\mathbf{Q}_p})$) under $\mathfrak{M}$.

10.6 Iwasawa algebras and differential equations

By [3, proposition 2.24], we have maps $\varphi^{-n}:\widetilde{\mathbf{B}}^{\dagger,r_n}_{\mathrm{rig}}\to\mathbf{B}^{+}_{\mathrm{dR}}$ whose restriction to $\mathbf{B}^{+}_{\mathrm{rig},F}$ satisfies $\varphi^{-n}(\mathbf{B}^{+}_{\mathrm{rig},F})\subset F_n[[t]]$ and which can be characterized by the fact that π maps to $\varepsilon^{(n)}\exp(t/p^n)-1$.

Recall if $z\in F_n((t))\otimes_F\mathbf{D}_{\mathrm{cris}}(V)$, we denote the constant coefficient of z by $\partial_V(z)\in F_n\otimes_F\mathbf{D}_{\mathrm{cris}}(V)$.

Lemma 10.6.1. *If $y\in(\mathbf{B}^{+}_{\mathrm{rig},F}[1/t]\otimes_F\mathbf{D}_{\mathrm{cris}}(V))^{\psi=1}$, then for any $m\geq n\geq 0$, the element*

$$p^{-m}\mathrm{Tr}_{F_m/F_n}\partial_V(\varphi^{-m}(y))\in F_n\otimes\mathbf{D}_{\mathrm{cris}}(V)$$

does not depend on m and we have

$$p^{-m}\mathrm{Tr}_{F_m/F_n}\partial_V(\varphi^{-m}(y))=\begin{cases}p^{-n}\partial_V(\varphi^{-n}(y)) & \text{if } n\geq 1\\ (1-p^{-1}\varphi^{-1})\partial_V(y) & \text{if } n=0\end{cases}$$

Proof. Recall that if $y=t^{-l}\sum_{k=0}^{+\infty}a_k\pi^k\in\mathbf{B}^{+}_{\mathrm{rig},F}[1/t]\otimes_F\mathbf{D}_{\mathrm{cris}}(V)$, then

$$\varphi^{-m}(y)=p^{ml}t^{-l}\sum_{k=0}^{+\infty}\varphi^{-m}(a_k)(\varepsilon^{(m)}\exp(t/p^m)-1)^k,$$

and that by the definition of ψ, $\psi(y)=y$ means that:

$$\varphi(y)=\frac{1}{p}\sum_{\zeta^p=1}y(\zeta(1+T)-1).$$

The lemma then follows from the fact that if $m\geq 2$, then the conjugates of $\varepsilon^{(m)}$ under $\mathrm{Gal}(F_m/F_{m-1})$ are the $\zeta\varepsilon^{(m)}$, where $\zeta^p=1$, while if $m=1$, then the conjugates of $\varepsilon^{(1)}$ under $\mathrm{Gal}(F_1/F)$ are the ζ, where $\zeta^p=1$ but $\zeta\neq 1$. □

Recall that since F is an unramified extension of $\mathbf{Q}_p$, $\Gamma_F\simeq\mathbf{Z}_p^*$ and that $\Gamma_{F_n}=\mathrm{Gal}(F_\infty/F_n)$ is the set of elements $\gamma\in\Gamma_F$ such that $\chi(\gamma)\in 1+p^n\mathbf{Z}_p$.

The Iwasawa algebra of Γ_F is $\Lambda_{\mathscr{O}_F}=\mathbf{Z}_p[[\Gamma_F]]\cong\mathbf{Z}_p[\Delta_F]\otimes_{\mathbf{Z}_p}\mathbf{Z}_p[[\Gamma_{F_1}]]$, and we set $\mathscr{H}(\Gamma_F)=\mathbf{Q}_p[\Delta_F]\otimes_{\mathbf{Q}_p}\mathscr{H}(\Gamma_F^1)$ where $\mathscr{H}(\Gamma_F^1)$ is the set of $f(\gamma-1)$ with $\gamma\in\Gamma_F^1$ and where $f(X)\in\mathbf{Q}_p[[X]]$ is convergent on the p-adic open unit disk. We define $\nabla_i\in\mathscr{H}(\Gamma_F)$ by

$$\nabla_i=\frac{\log(\gamma)}{\log_p(\chi(\gamma))}-i.$$

We will also use the operator $\nabla_0/(\gamma_n-1)$, where γ_n is a topological generator of Γ_F^n. It is defined by the formula

$$\frac{\nabla_0}{\gamma_n-1}=\frac{\log(\gamma_n)}{\log_p(\chi(\gamma_n))(\gamma_n-1)}=\frac{1}{\log_p(\chi(\gamma_n))}\sum_{i\geq 1}\frac{(1-\gamma_n)^{i-1}}{i},$$

or equivalently by

$$\frac{\nabla_0}{\gamma_n - 1} = \lim_{\eta \in \Gamma_F^n, \eta \to 1} \frac{\eta - 1}{\gamma_n - 1} \frac{1}{\log_p(\chi(\eta))}.$$

It is easy to see that $\nabla_0/(\gamma_n - 1)$ acts on F_n by $1/\log_p(\chi(\gamma_n))$.

The algebra $\mathscr{H}(\Gamma_F)$ acts on $\mathbf{B}^+_{\mathrm{rig},F}$ and one can easily check that

$$\nabla_i = t\frac{d}{dt} - i = \log(1+\pi)\partial - i, \quad \text{where} \quad \partial = (1+\pi)\frac{d}{d\pi}.$$

In particular, $\nabla_0 \mathbf{B}^+_{\mathrm{rig},F} \subset t\mathbf{B}^+_{\mathrm{rig},F}$ and if $i \geq 1$, then

$$\nabla_{i-1} \circ \cdots \circ \nabla_0 \subset t^i \mathbf{B}^+_{\mathrm{rig},F}.$$

Lemma 10.6.2. *If $n \geq 1$, then $\nabla_0/(\gamma_n - 1)(\mathbf{B}^+_{\mathrm{rig},F})^{\psi=0} \subset (t/\varphi^n(\pi))(\mathbf{B}^+_{\mathrm{rig},F})^{\psi=0}$ so that if $i \geq 1$, then*

$$\nabla_{i-1} \circ \cdots \circ \nabla_1 \circ \frac{\nabla_0}{\gamma_n - 1}(\mathbf{B}^+_{\mathrm{rig},F})^{\psi=0} \subset (\frac{t}{\varphi^n(\pi)})^i (\mathbf{B}^+_{\mathrm{rig},F})^{\psi=0}.$$

Proof. Since $\nabla_i = t \cdot d/dt - i$, the second claim follows easily from the first one. By the standard properties of p-adic holomorphic functions, what we need to do is to show that if $x \in (\mathbf{B}^+_{\mathrm{rig},F})^{\psi=0}$, then

$$\frac{\nabla_0}{\gamma_n - 1} x(\varepsilon^{(m)} - 1) = 0$$

for all $m \geq n+1$.

On the other hand, up to a scalar factor, one has for $m \geq n+1$:

$$\frac{\nabla_0}{\gamma_n - 1} x(\varepsilon^{(m)} - 1) = \mathrm{Tr}_{F_m/F_n} x(\varepsilon^{(m)} - 1),$$

which can be seen from the fact that

$$\frac{\nabla_0}{\gamma_n - 1} = \lim_{\eta \in \Gamma_F^n, \eta \to 1} \frac{\eta - 1}{\gamma_n - 1} \cdot \frac{1}{\log_p(\chi(\eta))}.$$

On the other hand, the fact $\psi(x) = 0$ implies that for every $m \geq 2$, $\mathrm{Tr}_{F_m/F_{m-1}} x(\varepsilon^{(m)} - 1) = 0$. This completes the proof. □

Finally, let us point out that the actions of any element of $\mathscr{H}(\Gamma_F)$ and φ commute. Since $\varphi(t) = pt$, we also see that $\partial \circ \varphi = p\varphi \circ \partial$.

We will henceforth assume that $\log_p(\chi(\gamma_n)) = p^n$, and in addition $\nabla_0/(\gamma_n - 1)$ acts on F_n by p^{-n}.

10.7 Bloch-Kato's exponential maps: Three explicit reciprocity formulas

In this section, we explain the results of Berger in [1] on explicit reciprocity formulas when V is a crystalline representation of an unramified field.

Recall $H_K = \mathrm{Gal}(\overline{\mathbf{Q}}_p/K_\infty)$, let Δ_K be the torsion subgroup of $\Gamma_K = G_K/H_K = \mathrm{Gal}(K_\infty/K)$ and let $\Gamma_K^1 = \mathrm{Gal}(K_\infty/K(\mu_p))$, so that $\Gamma_K \simeq \Delta_K \times \Gamma_K^1$. Let $\Gamma_K = \mathbf{Z}_p[[\Gamma_K]]$ and $\mathscr{H}(\Gamma_K) = \mathbf{Q}_p[\Delta_K] \otimes_{\mathbf{Q}_p} \mathscr{H}(\Gamma_K^1)$ where $\mathscr{H}(\Gamma_K^1)$ is the set of $f(\gamma_1 - 1)$ with $\gamma_1 \in \Gamma_{K_1}$ and where $f(T) \in \mathbf{Q}_p[[T]]$ is a power series which converges on the p-adic unit disk.

When F is an unramified extension of and V is a crystalline representation of G_F, Perrin-Riou has constructed in [18] a period map $\Omega_{V,h}$ which interpolates the $\exp_{F,V(k)}$ as k runs over the positive integers. It is crucial ingredient in the construction of p-adic L-funtions, and is a vast generalization of Coleman's isomorphism.

The main result of [18] is the construction, for a crystalline representation of V of G_F of a family of maps (parameterized by $h \in \mathbf{Z}$):

$$\Omega_{V,h} : (\mathscr{H}(\Gamma_F) \otimes_{\mathbf{Q}_p} \mathbf{D}_{\mathrm{cris}}(V))^{\Delta=0} \to \mathscr{H}(\Gamma_F) \otimes_{\Lambda_F} H^1_{\mathrm{Iw}}(F,V)/V^{H_F},$$

whose main property is that they interpolate Bloch-Kato's exponential map. More precisely, if $h, j \gg 0$, then the diagram:

$$\begin{tikzcd}
(\mathscr{H}(\Gamma_F) \otimes_{\mathbf{Q}_p} \mathbf{D}_{\mathrm{cris}}(V(j)))^{\Delta=0} \arrow[r, "\Omega_{V(j),h}"] \arrow[d, "\Xi_{n,V(j)}"'] & \mathscr{H}(\Gamma_F) \otimes_{\Gamma_F} H^1_{\mathrm{Iw}}(F,V(j))/V(j)^{H_F} \arrow[d, "\mathrm{pr}_{F_n,V(j)}"] \\
F_n \otimes_F \mathbf{D}_{\mathrm{cris}}(V) \arrow[r, "(h+j-1)!\times\exp^*_{F_n,V(j)}"] & H^1(F_n,V(j)).
\end{tikzcd}$$

is commutative where Δ and Ξ are two maps whose definition is rather technical (see section 10.9 for a precise definition).

Using the inverse of Perrin-Riou's map, one can then associate to an Euler system a p-adic L-function. For example, if one starts with $V = \mathbf{Q}_p(1)$, then Perrin-Riou's map is the inverse of the Coleman isomorphism and one recovers Kubota-Leopoldt p-adic L-functions (See section 11.2).

The goal of this section is to give formulas for $\exp_{K,V}$, $\exp^*_{K,V^*(1)}$ and $\Omega_{V,h}$ in terms of the (φ,Γ)-module associated to V.

10.8 The Bloch-Kato's exponential map and its dual revisited

Recall in section 8.1, we defined the Bloch-Kato's exponential map and its dual. The goal of this paragraph is to compute Bloch-Kato's exponential map and its dual in terms of the (φ,Γ)-module of V. Let $h \geq 1$ be an integer such that $\mathrm{Fil}^{-h}\mathbf{D}_{\mathrm{cris}}(V) = \mathbf{D}_{\mathrm{cris}}(V)$.

Recall that we have seen that $\mathbf{D}_{\mathrm{cris}}(V) = (\mathbf{D}^+_{\mathrm{rig}}[1/t])^{\Gamma_F}$ and by [2, II.3], there is an isomorphism

$$\mathbf{B}^+_{\mathrm{rig},F}[1/t] \otimes_F \mathbf{D}_{\mathrm{cris}}(V) = \mathbf{B}^+_{\mathrm{rig},F}[1/t] \otimes_F \mathbf{D}^+_{\mathrm{rig}}(V).$$

If $y \in \mathbf{B}^+_{\mathrm{rig},F} \otimes_F \mathbf{D}_{\mathrm{cris}}(V)$, then the fact that $\mathrm{Fil}^{-h}\mathbf{D}_{\mathrm{cris}}(V) = \mathbf{D}_{\mathrm{cris}}(V)$ implies by result of [2, II.3] that $t^h y \in \mathbf{D}^+_{\mathrm{rig}}(V)$, so that if

$$y = \sum_{i=0}^{d} y_i \otimes d_i \in (\mathbf{B}^+_{\mathrm{rig},F} \otimes_F \mathbf{D}_{\mathrm{cris}}(V))^{\psi=1},$$

then

$$\nabla_{h-1} \circ \cdots \nabla_0(y) = \sum_{i=0}^{d} t^h \partial^h y_i \otimes d_i \in \mathbf{D}^+_{\mathrm{rig}}(V)^{\psi=1}.$$

One can apply the operator $h^1_{F_n,V}$ to $\nabla_{h-1} \circ \cdots \nabla_0(y)$, then we have:

Theorem 10.8.1. *If $y \in (\mathbf{B}^+_{\mathrm{rig},F} \otimes_F \mathbf{D}_{\mathrm{cris}}(V))^{\psi=1}$, then*

$$h^1_{F_n,V}(\nabla_{h-1} \circ \cdots \nabla_0(y)) = (-1)^{h-1}(h-1)! \begin{cases} \exp_{F_n,V}(p^{-n}\partial_V(\varphi^{-n}(y))) & \text{if } n \geq 1 \\ \exp_{F,V}((1-p^{-1}\varphi^{-1})\partial_V(y)) & \text{if } n = 0 \end{cases}$$

Proof. Because the diagram

$$\begin{array}{ccc} F_{n+1} \otimes_F \mathbf{D}_{\mathrm{cris}}(V) & \xrightarrow{\exp_{F_{n+1},V}} & H^1(F_{n+1},V) \\ \downarrow{\scriptstyle \mathrm{Tr}_{F_{n+1}/F_n} \otimes id} & & \downarrow{\scriptstyle \mathrm{cor}_{F_{n+1}/F_n}} \\ F_n \otimes \mathbf{D}_{\mathrm{cris}}(V) & \xrightarrow{\exp_{F_n,V}} & H^1(F_n,V) \end{array}$$

is commutative, it is enough to prove the theorem under the assumption that Γ^n_F is torsion free. Let us set $y_h = \nabla_{h-1} \circ \cdots \circ \nabla_0(y)$. Since we are assuming for simplicity that $\chi(\gamma_n) = p^n$, the cocycle $h^1_{F_n,V}(y_h)$ is defined by:

$$h^1_{F_n,V}(y_h)(\sigma) = \frac{\sigma - 1}{\gamma_n - 1} y_h - (\sigma - 1) b_{n,h}$$

where $b_{n,h}$ is a solution of the equation $(\gamma_n - 1)(\varphi - 1)b_{n,h} = (\varphi - 1)y_h$. In lemma 10.6.2 above, we prove that

$$\nabla_{i-1} \circ \cdots \circ \nabla_1 \circ \frac{\nabla_0}{\gamma_n - 1} (\mathbf{B}^+_{\mathrm{rig},F})^{\psi=0} \subset (\frac{t}{\varphi^n(\pi)})^i (\mathbf{B}^+_{\mathrm{rig},F})^{\psi=0}.$$

It is then clear that if one sets

$$z_{n,h} = \nabla_{h-1} \circ \cdots \circ \frac{\nabla_0}{\gamma_n - 1} (\varphi - 1) y,$$

then

$$z_{n,h} \in (\frac{t}{\varphi^n(\pi)})^h (\mathbf{B}^+_{\mathrm{rig},F})^{\psi=0} \otimes_F \mathbf{D}_{\mathrm{cris}}(V) \subset \varphi^n(\pi^{-h}) \mathbf{D}^+_{\mathrm{rig}}(V)^{\psi=0} \subset \mathbf{D}^\dagger_{\mathrm{rig}}(V)^{\psi=0}.$$

Let $q = \varphi(\pi)/\pi$. By lemma 10.8.2 below, there exists an element $b_{n,h} \in \varphi^{n-1}(\pi^{-h})\widetilde{\mathbf{B}}^+_{\mathrm{rig}} \otimes_{\mathbf{Q}_p} V$ such that

$$(\varphi - \varphi^{n-1}(q^h))(\varphi^{n-1}(\pi^h)b_{n,h}) = \varphi^n(\pi^h)z_{n,h},$$

so that $(1-\varphi)b_{n,h} = z_{n,h}$ with $b_{n,h} \in \varphi^{n-1}(\pi^{-h})\widetilde{\mathbf{B}}^+_{\mathrm{rig}} \otimes \mathbf{Q}_p$.

If we set $w_{n,h} = \nabla_{h-1} \circ \cdots \circ \frac{\nabla_0}{\gamma_n - 1} y$, then $w_{n,h}$ and $b_{n,h} \in \mathbf{B}_{\max} \otimes_{\mathbf{Q}_p} V$ and the cocycle $h^1_{F_n,V}(y_h)$ is then given by the formula $h^1_{F_n,V}(y_h)(\sigma) = (\sigma - 1)(w_{n,h} - b_{n,h})$. Now $(\varphi-1)b_{n,h} = z_{n,h}$ and $(\varphi - 1)w_{n,h} = z_{n,h}$ as well, so that $w_{n,h} - b_{n,h} \in \mathbf{B}^{\varphi=1}_{\max} \otimes_{\mathbf{Q}_p} V$.

We can also write

$$h^1_{F_n,V}(y_h)(\sigma) = (\sigma-1)(\varphi^{-n}(w_{n,h}) - \varphi^{-n}(b_{n,h})).$$

Since we know that $b_{n,h} \in \varphi^{n-1}(\pi^{-h})\mathbf{B}^+_{\max} \otimes_{\mathbf{Q}_p} V$, we have $\varphi^{-n}(b_{n,h}) \in \mathbf{B}^+_{\mathrm{dR}} \otimes_{\mathbf{Q}_p} V$.

The definition of Bloch-Kato exponential gives rise to the following construction: if $x \in \mathbf{D}_{\mathrm{dR}}(V)$ and $\widetilde{x} \in \mathbf{B}^{\varphi=1}_{\max} \otimes_{\mathbf{Q}_p} V$ is such that $x - \widetilde{x} \in \mathbf{B}^+_{\mathrm{dR}} \otimes_{\mathbf{Q}_p} V$ then $\exp_{K,V}(x)$ is the class of the coclycle $g \mapsto g(\widetilde{x}) - \widetilde{x}$.

The theorem therefore follows from the fact that:

$$\varphi^{-n}(w_{n,h}) - (-1)^{h-1}(h-1)!p^{-n}\partial_V(\varphi^{-n}(y) \in \mathbf{B}^+_{\mathrm{dR}} \otimes_{\mathbf{Q}_p} V,$$

since we already know that $\varphi^{-n}(b_{n,h}) \in \mathbf{B}^+_{\mathrm{dR}} \otimes_{\mathbf{Q}_p} V$.

In order to show this, first notice that

$$\varphi^{-n}(y) - \partial_V(\varphi^{-n}(y)) \in tF_n[[t]] \otimes_F \mathbf{D}_{\mathrm{cris}}(V).$$

We can therefore write

$$\frac{\nabla_0}{\gamma_n - 1}\varphi^{-n}(y) = p^{-n}\partial_V(\varphi^{-n}(y)) + tz_1$$

and a simple recurrence shows that

$$\nabla_{i-1} \circ \cdots \circ \frac{\nabla_0}{1-\gamma_n}\varphi^{-n}(y) = (-1)^{i-1}(i-1)!p^{-n}\partial_V(\varphi^{-n}(y)) + t^i z_i,$$

with $z_i \in F_n[[t]] \otimes_F \mathbf{D}_{\mathrm{cris}}(V)$. By taking $i = h$, we see that

$$\varphi^{-n}(w_{n,h}) - (-1)^{h-1}(h-1)!p^{-n}\partial_V(\varphi^{-n}(y)) \in \mathbf{B}^+_{\mathrm{dR}} \otimes_{\mathbf{Q}_p} V,$$

Since we choose h such that $t^h\mathbf{D}_{\mathrm{cris}}(V) \subset \mathbf{B}^+_{\mathrm{dR}} \otimes_{\mathbf{Q}_p} V$. □

Lemma 10.8.2. *If $\alpha \in \widetilde{\mathbf{B}}^+_{\mathrm{rig}}$, the there exists $\beta \in \widetilde{\mathbf{B}}^+_{\mathrm{rig}}$ such that*

$$(\varphi - \varphi^{n-1}(q^h))\beta = \alpha.$$

Proof. By [3, proposition 2.19], the ring $\widetilde{\mathbf{B}}^+$ is dense in $\widetilde{\mathbf{B}}^+_{\mathrm{rig}}$ for the Fréchet topology. Hence, if $\alpha \in \widetilde{\mathbf{B}}^+_{\mathrm{rig}}$, then there exists $\alpha_0 \in \widetilde{\mathbf{B}}^+$ such that $\alpha - \alpha_0 = \varphi^n(\pi^h)\alpha_1$ with $\alpha_1 \in \widetilde{\mathbf{B}}^+_{\mathrm{rig}}$.

The map $\varphi - \varphi^{n-1}(q^h) : \widetilde{\mathbf{B}}^+ \to \widetilde{\mathbf{B}}^+$ is surjective because $\varphi - \varphi^{n-1}(q^h) : \widetilde{\mathbf{A}}^+ \to \widetilde{\mathbf{A}}^+$ is surjective, as can be seen by reducing modulo p and using the fact that $\widetilde{\mathbf{E}}$ is algebraically closed and that $\widetilde{\mathbf{E}}^+$ is its ring of integers.

One can therefore write $\alpha_0 = (\varphi - \varphi^{n-1}(q^h))\beta_0$. Finally by lemma 10.4.2, there exists $\beta \in \widetilde{\mathbf{B}}^+_{\mathrm{rig}}$ such that $\alpha_1 = (\varphi - 1)\beta_1$, so that $\varphi^n(\pi^h)\alpha_1 = (\varphi - \varphi^{n-1}(q^h))(\varphi^{n-1}(\pi^h)\beta_1)$. □

Theorem 10.8.3. *If $y \in (\mathbf{D}^\dagger_{\mathrm{rig}}(V))^{\psi=1}$ and $y \in \mathbf{D}^+_{\mathrm{rig}}(V)[1/t]$ (so that in particular $y \in (\mathbf{B}^+_{\mathrm{rig},F}[1/t] \otimes_F \mathbf{D}_{\mathrm{cris}}(V))^{\psi=1}$), then*

$$\exp^*_{F_n,V^*(1)}(h^1_{F_n,V}(y)) = \begin{cases} p^{-n}\partial_V(\varphi^{-n}(y)) & \text{if } n \geq 1 \\ (1-p^{-1}\varphi^{-1})\partial_V(y) & \text{if } n = 0 \end{cases}$$

Proof. Since the following diagram

$$\begin{tikzcd} H^1(F_{n+1},V) \arrow[r, "\exp^*_{F_{n+1},V^*(1)}"] \arrow[d, "\mathrm{cor}_{F_{n+1}/F_n}"'] & F_{n+1} \otimes \mathbf{D}_{\mathrm{cris}}(V) \arrow[d, "\mathrm{Tr}_{F_{n+1}/F_n} \otimes id"] \\ H^1(F_n,V) \arrow[r, "\exp^*_{F_n,V^*(1)}"] & F_n \otimes \mathbf{D}_{\mathrm{cris}}(V) \end{tikzcd}$$

is commutative, we only need to prove the theorem when Γ^n_F is torsion free by lemma 10.8.1. We then have (assuming that $\chi(\gamma_n) = p^n$ for simplicity) :

$$h^1_{F_n,V}(y)(\sigma) = \frac{\sigma - 1}{\gamma_n - 1} y - (\sigma - 1)b,$$

where $(\gamma_n - 1)(\varphi - 1)b = (\varphi - 1)y$. Recall that $\widetilde{\mathbf{B}}^\dagger_{\mathrm{rig}} = \cup_{r \geq 0} \widetilde{\mathbf{B}}^{\dagger,r}_{\mathrm{rig}}$. Since $b \in \widetilde{\mathbf{B}}^\dagger_{\mathrm{rig}} \otimes_{\mathbf{Q}_p} V$, there exists $m \gg 0$ such that $b \in \widetilde{\mathbf{B}}^{\dagger,r_m}_{\mathrm{rig}} \otimes_{\mathbf{Q}_p} V$ and that the map φ^{-m} embeds $\widetilde{\mathbf{B}}^{\dagger,r_m}_{\mathrm{rig}}$ into $\mathbf{B}^+_{\mathrm{dR}}$. we can then write

$$h^1(y)(\sigma) = \frac{\sigma - 1}{\gamma_n - 1} \varphi^{-m}(y) - (\sigma - 1)\varphi^{-m}(b),$$

and $\varphi^{-m}(b) \in \mathbf{B}^+_{\mathrm{dR}} \otimes_{\mathbf{Q}_p} V$. In addition, $\varphi^{-m}(y) \in F_m((t)) \otimes_F \mathbf{D}_{\mathrm{cris}}(V)$ and $\gamma_n - 1$ is invertible on $t^k F_m \otimes_F \mathbf{D}_{\mathrm{cris}}(V)$ for every $k \neq 0$ This shows that the cocycle $h^1_{F_n,V}$ is cohomologous in $H^1(F_n, \mathbf{B}_{\mathrm{dR}} \otimes_{\mathbf{Q}_p} V)$ to

$$\sigma \mapsto \frac{\sigma - 1}{\gamma_n - 1}(\partial_V(\varphi^{-m}(y)))$$

which is itself cohomologous (since $\gamma_n - 1$ is invertible on $F_m^{\mathrm{Tr}_{F_m/F_n}=0}$) to

$$\sigma \mapsto \frac{\sigma - 1}{\gamma_n - 1}\left(p^{n-m}\mathrm{Tr}_{F_m/F_n}\partial_V(\varphi^{-m}(y))\right) = \sigma \mapsto p^{-n}\log_p(\chi(\overline{\sigma}))p^{n-m}\mathrm{Tr}_{F_m/F_n}\partial_V(\varphi^{-m}(y)).$$

It follows from this and proposition 8.1.2 and lemma 10.6.1 that

$$\exp^*_{F_n,V^*(1)}(h^1_{F_n,V}(y)) = p^{-m}\mathrm{Tr}_{F_m/F_n}\partial_V(\varphi^{-m}(y)) = \begin{cases} p^{-n}\partial_V(\varphi^{-n}(y)) & \text{if } n \geq 1 \\ (1-p^{-1}\varphi^{-1})\partial_V(y) & \text{if } n = 0. \end{cases}$$

□

10.9 Perrin-Riou's big exponential map

By using the results of the previous paragraphs, we can give a uniform formula for the image of an element $y \in (\mathbf{B}^+_{\mathrm{rig},F} \otimes_F \mathbf{D}_{\mathrm{cris}}(V))^{\psi=1}$ in $H^1(F_n, V(j))$ under the composition of the following maps:

$$\left(\mathbf{B}^+_{\mathrm{rig},F} \otimes_F \mathbf{D}_{\mathrm{cris}}(V)\right)^{\psi=1} \xrightarrow{\nabla_{h-1}\circ\cdots\circ\nabla_0} \mathbf{D}^\dagger_{\mathrm{rig}}(V)^{\psi=1} \xrightarrow{\otimes e_j} \mathbf{D}^\dagger_{\mathrm{rig}}(V(j))^{\psi=1} \xrightarrow{h^1_{F_n,V(j)}} H^1(F_n, V(j))$$

Here e_j is a basis of $\mathbf{Q}_p(j)$ such that $e_{j+k} = e_j \otimes e_k$ so that if V is a p-adic representation, then we have compatible isomorphisms of $\mathbf{Q}_p$-vector spaces $V \to V(j)$ given by $v \mapsto v \otimes e_j$.

Theorem 10.9.1. *If $y \in (\mathbf{B}^+_{\mathrm{rig},F} \otimes_F \mathbf{D}_{\mathrm{cris}}(V))^{\psi=1}$, and $h \geq 1$ is an integer such that $\mathrm{Fil}^{-h}\mathbf{D}_{\mathrm{cris}}(V) = \mathbf{D}_{\mathrm{cris}}(V)$, then for all j with $h+j \geq 1$, we have :*

$$\begin{aligned} h^1_{F_n,V(j)}(\nabla_{h-1}\circ\cdots\nabla_0(y)\otimes e_j) =& (-1)^{h+j-1}(h+j-1)!\times \\ & \begin{cases} \exp_{F_n,V(j)}(p^{-n}\partial_{V(j)}(\varphi^{-n}(\partial^{-j}y\otimes t^{-j}e_j)) & \textit{if } n\geq 1 \\ \exp_{F,V(j)}((1-p^{-1}\varphi^{-1})\partial_{V(j)}(\partial^{-j}y\otimes t^{-j}e_j)) & \textit{if } n=0 \end{cases} \end{aligned}$$

while if $h+j \leq 0$, then we have:

$$\begin{aligned} \exp^*_{F_n,V^*(1-j)}(h^1_{F_n,V}(\nabla_{h-1}\circ\cdots\nabla_0(y)\otimes e_j)) =& \\ & \frac{1}{(-h-j)!}\begin{cases} p^{-n}\partial_{V(j)}(\varphi^{-n}(\partial^j y\otimes t^{-j}e_j)) & \textit{if } n\geq 1 \\ (1-p^{-1}\varphi^{-1})\partial_{V(j)}(\partial^{-j}y\otimes t^{-j}e_j) & \textit{if } n=0 \end{cases} \end{aligned}$$

Proof. If $h+j \geq 1$, then we have the following commutative diagram:

$$\begin{tikzcd} \mathbf{D}^+_{\mathrm{rig}}(V)^{\psi=1} \arrow[r, "\otimes e_j"] & \mathbf{D}^+_{\mathrm{rig}}(V(j))^{\psi=1} \\ \left(\mathbf{B}^+_{\mathrm{rig},F}\otimes_F \mathbf{D}_{\mathrm{cris}}(V)\right)^{\psi=1} \arrow[u, "\nabla_{h-1}\circ\cdots\circ\nabla_0"] \arrow[r, "\partial^{-j}\otimes t^{-j}e_j"] & \left(\mathbf{B}^+_{\mathrm{rig},F}\otimes_F \mathbf{D}_{\mathrm{cris}}(V(j))\right)^{\psi=1}. \arrow[u, "\nabla_{h+j-1}\circ\cdots\circ\nabla_0"'] \end{tikzcd}$$

and the theorem is then a straightforward consequence of theorem 10.8.1 applied to $\partial^{-j}y \otimes t^{-j}e_j$, $h+j$

and $V(j)$.

On the other hand, if $h+j \leq 0$, and Γ_F^n is torsion free, then theorem 10.8.3 shows that

$$\exp^*_{F_n,V*(1-j)}(h^1_{F_n,V(j)}(\nabla_{h-1}\circ\cdots\circ\nabla_0(y)\otimes e_j)) = p^{-n}\partial_{V(j)}(\varphi^{-n}(\nabla_{h-1}\circ\cdots\circ\nabla_0(y)\otimes e_j))$$

in $\mathbf{D}_{\mathrm{cris}}(V(j))$, and a short computation involving Taylor series shows that

$$p^{-n}\partial_{V(j)}(\varphi^{-n}(\nabla_{h-1}\circ\cdots\circ\nabla_0(y)\otimes e_j)) = (-h-j)!^{-1}p^{-n}\partial_{V(j)}(\varphi^{-n}(\partial^{-j}y\otimes t^{-j}e_j)).$$

Finally, to get the case $n=0$, one just needs to use the corresponding statement of theorem 10.8.3 or equivalently corestrict. □

Remark 10.9.2. The notation ∂^{-j} is not injective on $\mathbf{B}^+_{\mathrm{rig},F}$ (it is surjective by integration) but it can be checked that it leads to no ambiguity in the formulas above.

We will now use the above result to give a construction of Perrin-Riou's exponential map. If $f \in \mathbf{B}^+_{\mathrm{rig},F}\otimes\mathbf{D}_{\mathrm{cris}}(V)$, we define $\Delta(f)$ to be the image of $\oplus_{k=0}^h \partial^k(f)(0)$ in $\oplus_{k=0}^h(\mathbf{D}_{\mathrm{cris}}(V))/(1-p^k\varphi)(k)$. There is then an exact sequence of $\mathbf{Q}_p\otimes_{\mathbf{Z}_p}\Lambda_F$-modules (cf [18, section 2.2]):

$$0 \longrightarrow \oplus_{k=0}^h t^k\mathbf{D}_{\mathrm{cris}}(V)^{\varphi=p^{-k}} \longrightarrow (\mathbf{B}^+_{\mathrm{rig},F}\otimes\mathbf{D}_{\mathrm{cris}}(V))^{\psi=1} \xrightarrow{1-\varphi}$$
$$(\mathbf{B}^+_{\mathrm{rig},F})^{\psi=0}\otimes_F\mathbf{D}_{\mathrm{cris}}(V) \xrightarrow{\Delta} \oplus_{k=0}^h \frac{\mathbf{D}_{\mathrm{cris}}(V)}{1-p^k\varphi}(k) \longrightarrow 0.$$

If $f\in((\mathbf{B}^+_{\mathrm{rig},F})^{\psi=0}\otimes_F\mathbf{D}_{\mathrm{cris}}(V))^{\Delta=0}$, then by the above exact sequence there exists

$$y\in(\mathbf{B}^+_{\mathrm{rig},F}\otimes\mathbf{D}_{\mathrm{cris}}(V))^{\psi=1}$$

such that $f=(1-\varphi)y$, and since $\nabla_{h-1}\circ\cdots\nabla_0$ kills $\oplus_{k=0}^{h-1}t^k\mathbf{D}_{\mathrm{cris}}(V)^{\varphi=p^{-k}}$ we see that $\nabla_{h-1}\circ\cdots\nabla_0(y)$ does not depend upon the choice of such y unless $\mathbf{D}_{\mathrm{cris}}(V)^{\varphi=p^{-h}}\neq 0$.

Definition 10.9.3. Let $h\geq 1$ be an integer such that $\mathrm{Fil}^{-h}\mathbf{D}_{\mathrm{cris}}(V)=\mathbf{D}_{\mathrm{cris}}(V)$ and such that $\mathbf{D}_{\mathrm{cris}}(V)^{\varphi=p^{-h}}=0$. One deduces from the above construction a well-defined map

$$\Omega_{V,h}:\big((\mathbf{B}^+_{\mathrm{rig},F})^{\psi=0}\otimes_F\mathbf{D}_{\mathrm{cris}}(V)\big)^{\Delta=0}\to\mathbf{D}^+_{\mathrm{rig}}(V)^{\psi=1}$$

given by $\Omega_{V,h}(f)=\nabla_{h-1}\circ\cdots\nabla_0(y)$, where $y\in(\mathbf{B}^+_{\mathrm{rig},F}\otimes\mathbf{D}_{\mathrm{cris}}(V))^{\psi=1}$ is such that $f=(1-\varphi)y$.

If $\mathbf{D}_{\mathrm{cris}}(V)^{\varphi=p^{-h}}\neq 0$ then we get a map

$$\Omega_{V,h}:\big((\mathbf{B}^+_{\mathrm{rig},F})^{\psi=0}\otimes_F\mathbf{D}_{\mathrm{cris}}(V)\big)^{\Delta=0}\to\mathbf{D}^+_{\mathrm{rig}}(V)^{\psi=1}/V^{G_F=\chi^h}.$$

Theorem 10.9.4. *If V is a crystalline representation and $h \geq 1$ is such that we have* $\mathrm{Fil}^{-h}\mathbf{D}_{\mathrm{cris}}(V) = \mathbf{D}_{\mathrm{cris}}(V)$*, then the map*

$$\Omega_{V,h} : \left((\mathbf{B}^{+}_{\mathrm{rig},F})^{\psi=0} \otimes_F \mathbf{D}_{\mathrm{cris}}(V)\right)^{\Delta=0} \to \mathbf{D}^{+}_{\mathrm{rig}}(V)^{\psi=1}/V^{H_F}$$

which takes $f \in ((\mathbf{B}^{+}_{\mathrm{rig},F})^{\psi=0} \otimes_F \mathbf{D}_{\mathrm{cris}}(V))^{\Delta=0}$ to $\nabla_{h-1} \circ \cdots \nabla_0((1-\varphi)^{-1}f)$ is well defined and coincides with Perrin-Riou's exponential map.

Proof. The map $\Omega_{V,h}$ is well defined because as we seen above the kernel of $1-\varphi$ is killed by $\nabla_{h-1} \circ \cdots \circ \nabla_0$, except for $t^h\mathbf{D}_{\mathrm{cris}}(V)^{\varphi=p^{-h}}$, which is mapped to copies of $\mathbf{Q}_p(h) \in V^{H_F}$.

The fact that $\Omega_{V,h}$ coincides with Perrin-Riou's exponential map follows directly from theorem 10.9.1 above applied to those j's for which $h+j \geq 1$, and the fact that by [18, theorem 3.2.3], the $\Omega_{V,h}$ are uniquely determined by the requirement that they satisfy the following diagram for $h, j \gg 0$:

$$\begin{tikzcd}
(\mathscr{H}(\Gamma_F) \otimes_{\mathbf{Q}_p} \mathbf{D}_{\mathrm{cris}}(V(j))^{\Delta=0} \arrow[r, "\Omega_{V(j),h}"] \arrow[d, "\Xi_{n,V(j)}"'] & \mathscr{H}(\Gamma_F) \otimes_{\Gamma_F} (H^1_{\mathrm{Iw}}(F, V(j)/V(j)^{H_F}) \arrow[d, "\mathrm{pr}_{F_n,V(j)}"] \\
F_n \otimes_F \mathbf{D}_{\mathrm{cris}}(V) \arrow[r, "(h+j-1)!\exp_{F_n,V(j)}"] & H^1(F_n, V(j)).
\end{tikzcd}$$

Here $\Xi_{n,V(j)}(g) = p^{-n}(\varphi \otimes \varphi)^{-n}(f)(\varepsilon^{(n)}-1)$ where f is such that

$$(1-\varphi)f = g(\gamma-1)(1+\pi) \in (\mathbf{B}^{+}_{\mathrm{rig},F} \otimes_F \mathbf{D}_{\mathrm{cris}}(V))^{\psi=0}$$

and the φ on the left of $\varphi \otimes \varphi$ is the Frobenius on $\mathbf{B}^{+}_{\mathrm{rig},F}$ while the φ on the right is the Frobenius on $\mathbf{D}_{\mathrm{cris}}(V)$.

Note that by theorem 6.1.2, we have an isomorphism $D(V)^{\psi=1} \simeq H^1_{\mathrm{Iw}}(F,V)$ and therefore we get a map $\mathscr{H}(\Gamma_F) \otimes_{\Lambda_F} H^1_{\mathrm{Iw}}(F,V) \to \mathbf{D}^{\dagger}_{\mathrm{rig}}(V)^{\psi=1}$. On the other hand, there is a map

$$\mathscr{H}(\Gamma_F) \otimes_{\mathbf{Q}_p} \mathbf{D}_{\mathrm{cris}}(V(j)) \to (\mathbf{B}^{+}_{\mathrm{rig},F} \otimes_F \mathbf{D}_{\mathrm{cris}}(V))^{\psi=0}$$

which sends $\sum f_i(\gamma-1) \otimes d_i$ to $\sum f_i(\gamma-1)(1+\pi) \otimes d_i$. These two maps allow us to compare the diagram above with the formulas given by theorem 10.9.1. □

Remark 10.9.5. By the above remarks, if V is a crystalline representation and $h \geq 1$ is such that $\mathrm{Fil}^{-h}\mathbf{D}_{\mathrm{cris}}(V) = \mathbf{D}_{\mathrm{cris}}(V)$ and $\mathbf{Q}_p(h) \not\subset V$, then the map

$$\Omega_{V,h} : \left((\mathbf{B}^{+}_{\mathrm{rig},F})^{\psi=0} \otimes_F \mathbf{D}_{\mathrm{cris}}(V)\right)^{\Delta=0} \to \mathbf{D}^{+}_{\mathrm{rig}}(V)^{\psi=1}$$

which takes $f \in ((\mathbf{B}^{+}_{\mathrm{rig},F})^{\psi=0} \otimes_F \mathbf{D}_{\mathrm{cris}}(V))^{\Delta=0}$ to $\nabla_{h-1} \circ \cdots \nabla_0((1-\varphi)^{-1}f)$ is well defined, without having to kill the Λ_F-torsion of $H^1_{\mathrm{Iw}}(F,V)$.

Remark 10.9.6. It is clear from theorem 10.9.1 that we have:

$$\Omega_{V,h}(x)\otimes e_j = \Omega_{V(j),h+j}(\partial^j x\otimes t^{-j}e_j) \quad \text{and} \quad \nabla_h\circ\Omega_{V,h}(x) = \Omega_{V,h+1}(x)$$

and following Perrin-Riou, one can use these formulas to extend the definition of $\Omega_{V,h}$ to all $h\in\mathbf{Z}$ by tensoring all $\mathscr{H}(\Gamma_F)$-modules with the field of fractions of $\mathscr{H}(\Gamma_F)$

10.10 The explicit reciprocity formula

Recall we have a map $\mathscr{H}(\Gamma_F)\to(\mathbf{B}^+_{\mathrm{rig},\mathbf{Q}_p})^{\psi=0}$ which sends $f(\gamma-1)$ to $f(\gamma-1)(1+\pi)$, and that this map is a bijection and whose inverse is the Mellin transform, and that if $g(\pi)\in(\mathbf{B}^+_{\mathrm{rig},\mathbf{Q}_p})^{\psi=0}$, then $g(\pi)=\mathfrak{M}(g)(1+\pi)$. If $f,g\in(\mathbf{B}^\dagger_{\mathrm{rig},\mathbf{Q}_p})^{\psi=0}$ then we define $f*g$ by the formula $\mathfrak{M}(f*g)=\mathfrak{M}(f)\mathfrak{M}(g)$. Let $[-1]\in\Gamma_F$ be the element such that $\chi([-1])=-1$, and let ι be the involution of Γ_F which sends γ to γ^{-1}. The operator ∂^j on $(\mathbf{B}^+_{\mathrm{rig},\mathbf{Q}_p})^{\psi=0}$ corresponds to Tw_j on Γ_F (Tw_j is defined by $\mathrm{Tw}_j(\gamma)=\chi(\gamma^j)\gamma$). We will make use of the facts that $\iota\circ\partial^j=\partial^{-j}\circ\iota$ and $[-1]\circ\partial^j=(-1)^j\partial^j\circ[-1]$.

If V is a crystalline representation, then the natural maps

$$\mathbf{D}_{\mathrm{cris}}(V)\otimes_F\mathbf{D}_{\mathrm{cris}}(V^*(1))\longrightarrow\mathbf{D}_{\mathrm{cris}}(\mathbf{Q}_p(1))\xrightarrow{\mathrm{Tr}_{F/\mathbf{Q}_p}}\mathbf{Q}_p$$

allow us to define a perfect pairing $[\cdot,\cdot]_V:\mathbf{D}_{\mathrm{cris}}(V)\times\mathbf{D}_{\mathrm{cris}}(V^*(1))$ which we extend by linearity to

$$[\cdot,\cdot]_V:(\mathbf{B}^+_{\mathrm{rig},F}\otimes\mathbf{D}_{\mathrm{cris}}(V))^{\psi=0}\times(\mathbf{B}^+_{\mathrm{rig},F}\otimes\mathbf{D}_{\mathrm{cris}}(V^*(1)))^{\psi=0}\to(\mathbf{B}^+_{\mathrm{rig},\mathbf{Q}_p})^{\psi=0}$$

by the formula $[f(\pi)\otimes d_1,g(\pi)\otimes d_2]_V=(f*g)(\pi)[d_1,d_2]_V$.

We can also define a semi-linear pairing (with respect to ι)

$$\langle\cdot,\cdot\rangle_V:\mathbf{D}^+_{\mathrm{rig}}(V)^{\psi=1}\times\mathbf{D}^+_{\mathrm{rig}}(V)^{\psi=1}\to(\mathbf{B}^+_{\mathrm{rig},\mathbf{Q}_p})^{\psi=0}$$

by the formula

$$\langle\cdot,\cdot\rangle_V=\varprojlim\sum_{\tau\in\Gamma_F/\Gamma_F^n}\left\langle\tau^{-1}(h^1_{F_n,V}(y_1)),h^1_{F_n,V^*(1)}(y_2)\right\rangle_{F_n,V}\cdot\tau(1+\pi)$$

where the pairing $\langle\cdot,\cdot\rangle_{F_n,V}$ is given by the cup product:

$$\langle\cdot,\cdot\rangle_{F_n,V}:H^1(F_n,V)\times H^1(F_n,V^*(1))\to H^2(F_n,\mathbf{Q}_p(1))\cong\mathbf{Q}_p.$$

The pairing $\langle\cdot,\cdot\rangle_V$ satisfies the relation $\langle\gamma_1x_1,\gamma_2x_2\rangle_V=\gamma_1\iota(\gamma_2)\langle x_1,x_2\rangle_V$, where $\gamma_1,\gamma_2\in\Gamma_F$. Perrin-Riou's explicit reciprocity formula is then:

Theorem 10.10.1. *If $x_1\in(\mathbf{B}^+_{\mathrm{rig},F}\otimes_F\mathbf{D}_{\mathrm{cris}}(V))^{\psi=0}$ and $x_2\in(\mathbf{B}^+_{\mathrm{rig},F}\otimes_F\mathbf{D}_{\mathrm{cris}}(V^*(1)))^{\psi=0}$, then for every h,* *we have*

$$(-1)^h\langle \Omega_{V,h}(x_1),[-1]\cdot\Omega_{V^*(1),1-h}(x_2)\rangle_V=-[x_1,\iota(x_2)]_V.$$

Proof. By the theory of p-adic interpolation, it is enough to prove that if $x_i=(1-\varphi)y_i$ with $y_1\in(\mathbf{B}^+_{\mathrm{rig},F}\otimes_F\mathbf{D}_{\mathrm{cris}}(V))^{\psi=1}$ and $y_2\in(\mathbf{B}^+_{\mathrm{rig},F}\otimes_F\mathbf{D}_{\mathrm{cris}}(V^*(1)))^{\psi=1}$, then for all $j\gg 0$;

$$\big(\partial^{-j}(-1)^h\big\langle\Omega_{V,h}(x_1),[-1]\cdot\Omega_{V^*(1),1-h}(x_2)\big\rangle_V\big)(0)=-(\partial^{-j}[x_1,\iota(x_2)]_V)(0).$$

The above formula is equivalent to:

$$\begin{aligned}(1)\qquad (-1)^{h+j}\langle h^1_{F,V(j)}\Omega_{V(j),h+j}(\partial^{-j}x_1\otimes t^{-j}e_{-j}),h^1_{F,V^*(1-j)}\Omega_{V^*(1-j),1-h-j}(\partial^jx_2\otimes t^je_{-j})\rangle_{F,V(j)}\\ =[\partial_{V(j)}(\partial^{-j}x_1\otimes t^{-j}e_j),\partial_{V^*(1-j)}(\partial^jx_2\otimes t^je_{-j}))]_{V(j)}.\end{aligned}$$

By combining theorems 10.9.1 and 10.9.4 with remark 10.9.6, we see that for $j\gg 0$:

$$h^1_{F,V(j)}\Omega_{V(j),h+j}(\partial^{-j}x_1\otimes t^{-j}e_j)=(-1)^{h+j-1}\exp_{F,V(j)}((h+j-1)!(1-p^{-1}\varphi^{-1})\partial_{V(j)}(\partial^{-j}y_1\otimes t^{-j}e_j)),$$

and that

$$\begin{aligned}&h^1_{F,V^*(1-j)}\Omega_{V^*(1-j),1-h-j}(\partial^jx_2\otimes t^je_{-j})\\ &\qquad=(\exp^*_{F,V^*(1-j)})^{-1}(h+j-1)!^{-1}((1-p^{-1}\varphi^{-1})\partial_{V^*(1-j)}(\partial^jy_2\otimes t^je_{-j})).\end{aligned}$$

Using the fact that by definition, if $x\in\mathbf{D}_{\mathrm{cris}}(V(j))$ and $y\in H^1(F,V(j))$ then

$$[x,\exp^*_{F,V^*(1-j)}y]_{V(j)}=\langle\exp_{F,V(j)}x,y\rangle_{F,V(j)},$$

we see that

$$\begin{aligned}&\langle h^1_{F,V(j)}\Omega_{V(j),h+j}(\partial^{-j}x_1\otimes t^{-j}e_j),h^1_{F,V^*(1-j)}\Omega_{V^*(1-j),1-h-j}(\partial^jx_2\otimes t^je_{-j})\rangle_{F,V(j)} \qquad (10.1)\\ &=(-1)^{h+j-1}[(1-p^{-1}\varphi^{-1})\partial_{V(j)}(\varphi^{-j}y_1\otimes t^{-j}e_j),(1-p^{-1}\varphi^{-1})\partial_{V^*(1-j)}(\partial^jy_2\otimes t^je_{-j})]_{V(j)}.\end{aligned}$$

It is easy to see that under $[\quad,\quad]$, the adjoint of $(1-p^{-1}\varphi^{-1})$ is $1-\varphi$ and that if $x_i=(1-\varphi)y_i$, then

$$\begin{aligned}\partial_{V(j)}(\partial^{-j}x_1\otimes t^{-j}e_j)&=(1-\varphi)\partial_{V(j)}(\partial^{-j}y_1\otimes t^{-j}e_j),\\ \partial_{V^*(1-j)}(\partial^jx_2\otimes t^je_{-j})&=(1-\varphi)\partial_{V^*(1-j)}(\partial^jy_2\otimes t^je_{-j}),\end{aligned}$$

So that (10.1) implies (1), and this proves the theorem. □

Chapter 11

Perrin-Riou's big regulator map

Let F be a finite unramified extension over $\mathbf{Q}_p$ and V a continuous p-adic representation of G_F, which is crystalline with Hodge-Tate weights ≥ 0 and with no quotient isomorphic to the trivial representation. In [19], Perrin-Riou construct a big logarithm map

$$\mathscr{L}_{F,V}^{\Gamma_F} : H^1_{\mathrm{Iw}}(F,V) \longrightarrow \mathscr{H}(\Gamma_F) \otimes_{\mathbf{Q}_p} \mathbf{D}_{\mathrm{cris}}(V)$$

which interpolates the values of Bloch-Kato's dual exponential and logarithm maps for $V(j)$, $j \in \mathbf{Z}$, over each F_n.

In this section, we follow [17, Appendix B] to adapt Berger's explicit formulas to construct Perrin-Riou's big logarithm and use it to calculate Kubota-Leopoldt p-adic L-function.

11.1 Perrin-Riou's big logarithm map

Let V be a positive crystalline representation of $\mathrm{Gal}(F_\infty/F)$ and $x \in \mathscr{H}(\Gamma_F) \otimes_{\Lambda_F} H^1_{\mathrm{Iw}}(F,V)$. We write x_j for the image of x in $H^1_{\mathrm{Iw}}(F,V(-j))$, and $x_{j,n}$ for the image of x_j in $H^1(F_n,V(-j))$. If we identify x with its image in $D(V)^{\psi=1}$, then x_j corresponds to the element $x \otimes e_{-j} \in D(V)^{\psi=1} \otimes e_{-j} = D(V(-j))^{\psi=1}$.

Since V is positive, we may interpret x as an element of the module $(\mathbf{B}^+_{\mathrm{rig},F}[1/t] \otimes \mathbf{D}_{\mathrm{cris}}(V))^{\psi=1}$.

We shall assume:

$$x \in (\mathbf{B}^+_{\mathrm{rig},F} \otimes_{\mathbf{B}^+_F} \mathbf{N}(V))^{\psi=1} \subset (\mathbf{B}^+_{\mathrm{rig},F}[1/t] \otimes_F \mathbf{D}_{\mathrm{cris}}(V))^{\psi=1}. \tag{11.1}$$

The condition is satisfied if V has no quotient isomorphoic to $\mathbf{Q}_p$ (c.f. theorem 10.2.4).

Recall in section 7.2, we define ∂ to be the differential operator $(1+\pi)\frac{d}{d\pi}$ (or $\frac{d}{dt}$) on $\mathbf{B}^+_{\mathrm{rig},F}$ and we have a map

$$\partial_V \circ \varphi^{-n} : \mathbf{B}^+_{\mathrm{rig},F}[1/t] \otimes_F \mathbf{D}_{\mathrm{cris}}(V) \to F_n \otimes_F \mathbf{D}_{\mathrm{cris}}(V)$$

which sends $\pi^k \otimes d$ to the constant coefficient of $(\zeta_n \exp(t/p^n) - 1)^k \otimes \varphi^{-n}(d) \in F_n((t)) \otimes_F \mathbf{D}_{\mathrm{cris}}(V)$.

For $m \in \mathbf{Z}$, define $\Gamma^*(m)$ to be the leading term of Taylor series expansion of $\Gamma(x)$ at $x = m$; thus

$$\Gamma^*(m) = \begin{cases} j! & \text{if } n \geq 0 \\ \frac{(-1)^{-j-1}}{(-j-1)!} & \text{if } n \leq -1 \end{cases}$$

Proposition 11.1.1. *Define*

$$R_{j,n}(x) = \frac{1}{j!} \times \begin{cases} p^{-n}\partial_{V(-j)}(\varphi^{-n}(\partial^j x \otimes t^j e_{-j})) & \text{if } n \geq 1 \\ (1 - p^{-1}\varphi^{-1})\partial_{V(-j)}(\partial^j x \otimes t^j e_{-j}) & \text{if } n = 0 \end{cases}$$

Then we have

$$R_{j,n}(x) = \begin{cases} \exp^*_{F_n, V^*(1-j)}(x_{j,n}) & \text{if } j \geq 0 \\ \log_{F_n, V(-j)}(x_{j,n}) & \text{if } j \leq -1 \end{cases}$$

Proof. This result is essentially a minor variation on thoerem 10.9.1. The case $j \geq 0$ is immediate from theorem 10.8.1 applied with V replaced by $V(-j)$ and x by $x \otimes e_{-j}$, using the formula

$$\partial_{V(-j)}(\varphi^{-n}(x \otimes e_{-j})) = \frac{1}{j!}\partial_{V(-j)}(\varphi^{-n}(\partial^j x \otimes t^j e_{-j})).$$

For the formula for $j \leq -1$, we choose h such that $\mathrm{Fil}^{-h}\mathbf{D}_{\mathrm{cris}}(V) = \mathbf{D}_{\mathrm{cris}}(V)$. The element $\partial^j x \otimes t^j e_{-j}$ lies in $(\mathbf{B}^+_{\mathrm{rig},F} \otimes_F \mathbf{D}_{\mathrm{cris}}(V(-j)))^{\psi=1}$. Applying theorem 10.8.1 with V,h and x replaced by $V(-j)$, $h-j$, and $\partial^j x \otimes t^{-j} e_j$, we see that

$$\Gamma^*(j+1)R_{j,n}(x) = \Gamma^*(j-h+1)\log_{F_n,V(-j)}[(\nabla_0 \circ \cdots \circ \nabla_{h-1}x)_{j,n}].$$

For $x \in \mathscr{H}(\Gamma_F) \otimes_{\Lambda_F} H^1_{\mathrm{Iw}}(F, V)$, we have

$$(\nabla_r x)_{j,n} = (j-r)x_{j,n},$$

so se have

$$(\nabla_0 \circ \cdots \circ \nabla_{h-1}x)_{j,n} = (j)(j-1)\cdots(j-h+1)x_{j,n}$$

as require. $\square$

For ω a finite order character on Γ_F of conductor n, we denote

$$G(\omega) = \sum_{\sigma \in \Gamma_F/\Gamma_{F_n}} \omega(\sigma)\zeta^{\sigma}_{p^n}.$$

the Gauss sum of ω.

Proposition 11.1.2. *If x is as above, and $\mathscr{L}_V^{\Gamma_F}(x)$ is the unique element of $\mathscr{H}(\Gamma_F)\otimes_F \mathbf{D}_{\mathrm{cris}}(V)$ such that $\mathscr{L}_V^{\Gamma_F}(x)\cdot(1+\pi) = (1-\varphi)x$, then for any $j \in \mathbf{Z}$ we have*

$$(1-\varphi)\partial_{V(-j)}(\varphi^{-n}(\partial^j x \otimes t^j e_{-j})) = \mathscr{L}_V^{\Gamma_F}(x)(\chi^j)\otimes t^j e_{-j},$$

while for any finite order character ω of Γ_F of conductor $n \geq 1$, we have

$$\left(\sum_{\sigma\in\Gamma_F/\Gamma_F^n} \omega(\sigma)^{-1}\sigma\right)\cdot \partial_{V(-j)}(\varphi^{-n}(\partial^j x\otimes t^j e_{-j}) = G(\omega)\varphi^{-n}(\mathscr{L}_V^{\Gamma_F}(x)(\chi^j\omega)\otimes t^j e_{-j}).$$

Proof. We note that

$$\mathscr{L}_{V(-j)}^{\Gamma_F}(\partial^j x\otimes t^j e_{-j}) = \mathrm{Tw}_j(\mathscr{L}_V^{\Gamma_F}(x))\otimes t^j e_{-j},$$

so it suffices to prove the result for $j=0$. Suppose we have $x = \sum_{k\geq 0} v_k \pi^k$ where $v_k \in \mathbf{D}_{\mathrm{cris}}(V)$. Then

$$\partial_V(\varphi^{-n}(x)) = \sum_{k\geq 0}\varphi^{-n}(v_k)(\zeta_{p^n}-1)^k.$$

On the other hand,

$$\partial_V(\varphi^{-n}((1-\varphi)x)) = \sum_{k\geq 0}\varphi^{-n}(v_k)(\zeta_{p^n}-1)^k - \sum_{k\geq 0}\varphi^{1-n}(v_k)(\zeta_{p^{n-1}}-1)^k.$$

Applying the operator $e_\omega = \sum_{\sigma\in\Gamma_F/\Gamma_F^n}\omega(\sigma)\sigma$, we have for $n \geq 1$

$$e_\omega\cdot\partial_V(\varphi^{-n}(x)) = e_\omega\cdot\partial_V(\varphi^{-n}((1-\varphi)x)),$$

since e_ω is zero on $F_{n-1}((t))$.

However, since the map $\partial_V\circ\varphi^{-n}$ is a homomorphism of Γ_F-modules, we have

$$\begin{aligned} e_\omega\cdot\partial_V(\varphi^{-n}((1-\varphi)x)) =& e_\omega\cdot\partial_V(\varphi^{-n}(\mathscr{L}_V^{\Gamma_F}(x)\cdot(1+\pi))) \\ =&\varphi^{-n}(\mathscr{L}_V^{\Gamma_F}(x))\cdot e_\omega\partial_F(\varphi^{-n}(1+\pi)) \\ =&G(\omega)\varphi^{-n}(\mathscr{L}_V^{\Gamma_F}(x)(\omega)). \end{aligned}$$

This completes the proof of the proposition for $j=0$. □

Definition 11.1.3. Let $x \in H^1_{\mathrm{Iw}}(F,V)$ If η is any continuous character of Γ_F, denote by x_η the image of x in $H^1_{\mathrm{Iw}}(F,V(\eta^{-1}))$. If $n\geq 0$, denote by $x_{\eta,n}$ the image of x_η in $H^1(F_n,V(\eta^{-1}))$.

Thus $x_{\chi^j,n} = x_{j,n}$ in the previous notation. The next lemma is valid for arbitrary de Rham representations of G_F (with no restriction on Hodge-Tate weights):

Lemma 11.1.4. *For any finite-order character ω factoring through Γ_F/Γ_F^n, with values in a finite extension E/F, we have*

$$\sum_{\sigma\in\Gamma_F/\Gamma_F^n}\omega(\sigma)^{-1}\exp^*_{F_n,V^*(1)}(x_{0,n})^{\sigma}=\exp^*_{F_n,V(\omega^{-1})^*(1)}(x_{\omega,0})$$

and

$$\sum_{\sigma\in\Gamma/\Gamma_n}\omega(\sigma)^{-1}\log_{F_n,V}(x_{0,n})^{\sigma}=\log_{F_n,V(\omega^{-1})}(x_{\omega,0})$$

where we identify $\mathbf{D}_{\mathrm{dR}}(V(\omega^{-1}))\cong(E\otimes_F F_n\otimes_F\mathbf{D}_{\mathrm{cris}}(V))^{\Gamma=\omega}$.

Proof. This follows from the compatibility of the maps $\exp^*$ and log with the corestriction maps (c.f. Theorem 10.8.1 and 10.8.3). □

Combining the three results above, we obtain:

Theorem 11.1.5. *Let $j\in\mathbf{Z}$ and let x satisfy (11.1). Let η be a continuous character of Γ_F of the form $\chi^j\omega$, where ω is a finite-order character of conductor n.*

i) If $j\geq 0$, we have

$$\mathscr{L}_V^{\Gamma_F}(x)(\eta)=j!\times\begin{cases}(1-p^j\varphi)(1-p^{-1-j}\varphi^{-1})^{-1}\left(\exp^*_{F,V(\eta^{-1})^*(1)}(x_{\eta,0})\otimes t^{-j}e_j\right) & \text{if } n=0\\ G(\omega)^{-1}p^{n(1+j)}\varphi^n\left(\exp^*_{F,V(\eta^{-1})^*(1)}(x_{\eta,0})\otimes t^{-j}e_j\right) & \text{if } n\geq 1.\end{cases}$$

ii) If $j\leq -1$, we have

$$\mathscr{L}_V^{\Gamma}(x)(\eta)=\frac{(-1)^{-j-1}}{(-j-1)!}\times\begin{cases}(1-p^j\varphi)(1-p^{-1-j}\varphi^{-1})^{-1}\left(\log_{F,V(\eta^{-1})}(x_{\eta,0})\otimes t^{-j}e_j\right) & \text{if } n=0\\ G(\omega)^{-1}p^{n(1+j)}\varphi^n\left(\log_{F,V(\eta^{-1})}(x_{\eta,0})\otimes t^{-j}e_j\right) & \text{if } n\geq 1.\end{cases}$$

In both cases, we assume that $(1-p^{-1-j}\varphi^{-1})$ is invertible on $\mathbf{D}_{\mathrm{cris}}(V)$ when $\eta=\chi^j$.

11.2 Cyclotomic units and Kubota-Leopoldt p-adic L-functions

The relation between Coleman's power series and the Perrin-Riou's big logarithm map is given by the following diagram:

$$\begin{tikzcd}
\varprojlim \mathscr{O}_{F_n}^* \arrow[r, "\kappa"] \arrow[d, "\mathrm{Col}"] & H^1_{\mathrm{Iw}}(F,\mathbf{Z}_p(1)) \arrow[dd, "\mathscr{L}^{\Gamma}_{F,\mathbf{Q}_p(1)}"] \\
\mathscr{O}_F[[\pi]]^* \arrow[d, "(1-\frac{\varphi}{p})\log"] & \\
\mathscr{O}_F[[\pi]]^{\psi=0} \arrow[r] & \mathscr{H}(\Gamma)\otimes_{\mathbf{Q}_p}\mathbf{D}_{\mathrm{cris}}(F,\mathbf{Q}_p(1))
\end{tikzcd}$$

If we identify $\mathbf{D}_{\mathrm{cris}}(F, \mathbf{Q}_p(1))$ with F via the basis vector $t^{-1} \otimes e_1$, then the bottom map sends $f \in \mathscr{O}_F[[\pi]]^{\psi=0}$ to $\nabla_0 \cdot \mathfrak{M}^{-1}(f)$, where $\nabla_0 = \frac{\log \gamma}{\log \chi(\gamma)}$ for any non-identity element $\gamma \in \Gamma_1$ and $\mathfrak{M}$ is the Mellin transform defined in section 10.5. Thus the image of the bottom map is precisely $\nabla_0 \cdot \Lambda_{\mathscr{O}_F}(\Gamma) \subset \mathscr{H}_F(\Gamma)$; and if we define

$$h_F(u) = \nabla_0^{-1} \cdot \mathscr{L}^{\Gamma}_{F, \mathbf{Q}_p(1)}(\kappa(u)) \in \Lambda_{\mathscr{O}_F}(\Gamma),$$

then we have

$$\mathfrak{M}(h_F(u)) = (1 - \frac{\varphi}{p}) \log \mathrm{Col}_u(u).$$

By the calculation in section 9.6, we can use theorem 11.1.5 to calculate the Kubota-Leopoldt p-adic L-functions.

Example 11.2.1. (Kubota-Leopoldt p-adic zeta-function) Let $K = \mathbf{Q}_p$, $V = \mathbf{Q}_p(1)$ and

$$u = (\frac{\zeta_{p^n} - 1}{\zeta_{p^n}})_{n \geq 1} \in \varprojlim \mathscr{O}^*_{\mathbf{Q}_p(\mu_{p^n})}.$$

Then by the calculation in section 9.6, we have

$$\begin{aligned} h_F(u)(\chi^k) =& \chi^k(\nabla_0^{-1}) \cdot k! \cdot \frac{(1 - p^k \varphi)}{(1 - p^{-1-k}\varphi^{-1})}) \left(\exp^*_{\mathbf{Q}_p, V^*(1-j)}(u_{k,0}) \otimes t^{-k} e_k \right) \\ =& \frac{1}{k} k! \cdot \frac{(1 - p^k \varphi)}{(1 - p^{-1-k}\varphi^{-1})} \left((1 - p^{-k}) \zeta(1-k) \frac{t^{k-1}}{(k-1)!} \otimes t^{-k} e_k \right) \\ =& (1 - p^{k-1}) \zeta(1-k) t^{-1} \end{aligned}$$

and for ω a finite order character of Γ of conductor n, we have

$$\begin{aligned} h_F(u)(\chi^k \omega) =& \chi^k(\nabla_0^{-1}) \cdot k! \cdot G(\omega)^{-1} p^{n(1+k)} \varphi^n \left(\exp^*_{\mathbf{Q}_p, V(\eta^{-1})^*(1)}(u_{\eta,0}) \otimes t^{-k} e_k \right) \\ =& \frac{1}{k} k! \cdot G(\omega)^{-1} p^{n(1+k)} \varphi^n \left(p^{-(n+1)k} G(\omega) \mathrm{L}(1-k, \omega) \frac{t^{k-1}}{(k-1)!} \otimes t^{-k} e_k \right) \\ =& \mathrm{L}(1-k, \omega) t^{-1} \end{aligned}$$

Example 11.2.2. (Kubota-Leopoldt p-adic L-function) Let $K = \mathbf{Q}_p(\zeta_d)$, $V = \mathbf{Q}_p(1)$ and ε is a Dirichlet character of conductor $d \geq 1$ prime to p. Set $u = \left(\frac{-1}{G(\varepsilon^{-1})} \sum_{0 \leq a \leq d-1} \varepsilon(a)^{-1} \frac{\zeta_d^a \zeta_{p^n}}{\zeta_d^a \zeta_{p^n} - 1} \right)_{n \geq 1}$. Then by calculation in section 9.6, we have

$$
\begin{aligned}
h_F(u)(\chi^k) =& \chi^k(\nabla_0^{-1}) \cdot k! \cdot \frac{(1-p^k\varphi)}{(1-p^{-1-k}\varphi^{-1})^{-1}} \left(\exp^*_{K,V^*(1-j)}(u_{k,0}) \otimes t^{-k}e_k \right) \\
=& \frac{1}{k} k! \cdot \frac{(1-p^k\varphi)}{(1-p^{-1-k}\varphi^{-1})^{-1}} \left((1-\varepsilon(p)p^{-k}) \mathrm{L}(1-k,\varepsilon) \frac{t^{k-1}}{(k-1)!} \otimes t^{-k}e_k \right) \\
=& (1-\varepsilon(p)p^{k-1}) \mathrm{L}(1-k,\varepsilon) t^{-1}
\end{aligned}
$$

and for ω a finite order character of Γ of conductor n, we have

$$
\begin{aligned}
h_F(u)(\chi^k\omega) =& \chi^k(\nabla_0^{-1}) \cdot k! \cdot G(\omega)^{-1} p^{n(1+k)} \varphi^n \left(\exp^*_{\mathbf{Q}_p,V(\eta^{-1})^*(1)}(u_{\eta,0}) \otimes t^{-k}e_k \right) \\
=& \frac{1}{k} k! \cdot G(\omega)^{-1} p^{n(1+k)} \varphi^n \left(p^{-(n+1)k} G(\omega) \mathrm{L}(1-k,\omega\varepsilon) \frac{t^{k-1}}{(k-1)!} \otimes t^{-k}e_k \right) \\
=& \mathrm{L}(1-k,\omega\varepsilon) t^{-1}
\end{aligned}
$$

Bibliography

[1] L. Berger. Bloch and kato's exponential map: three explicit formulas. *Doc. Math. Extra*, Extra: 99–129, 2003. → pages 56, 57, 63

[2] L. Berger. Limites de représentations cristallines. *Compositio Math.*, 140(6):1473–1498, 2004. → pages 2, 56, 64

[3] L. B. Berger. Représentations p-adiques et équations différentielles. *Invent. Math.*, 148(2):219–284, 2002. → pages 57, 59, 61, 66

[4] S. Bloch and K. Kato. *L-Functions and Tamagawa Numbers of Motives*, pages 333–400. Birkhäuser Boston, 2007. → pages 2

[5] F. Cherbonnier and P. Colmez. Représentations p-adiques surconvergentes. *Invent. Math.*, 133: 581–611, 1998. → pages 2, 39, 40

[6] F. Cherbonnier and P. Colmez. Théorie d'iwasawa des représentations p-adiques d'un corps local. *J. A.M.S*, 12:241–268, 1999. → pages 2

[7] J. Coates and R. Sujatha. *Cyclotomic Fields and Zeta values*. Springer monographs in mathematics. Springer-Verlag, Berlin, 2006. → pages 54

[8] R. Coleman. Division values in local fields. *Invent. Math.*, 53:91–116, 1979. → pages 1, 2, 49

[9] P. Colmez. Théorie d'iwasawa des représentations de de rham d'un corps local. *Annals of Math.*, 148:485–571, 1998. → pages 41, 42, 43, 45, 46, 59

[10] P. Colmez. Représentations cristallines et représentations de hauteur finie. *J. Reine Angew. Math*, 514:119–143, 1999. → pages 56

[11] P. Colmez. Arithmetique de la fonction zeta. *Journees mathematiques*, X-UPS:37–164, 2002. → pages 2

[12] P. Colmez. Fonctions d'une variable p-adique. *Astérisque*, pages 61–153, 2010. → pages 2, 3, 4, 5

[13] J. Fontaine and Y. Ouyang. Theory of p-adic galois represntations. http://math.stanford.edu/ conrad/252Page/handouts/galoisrep.pdf. → pages 20

[14] L. Herr. Sur la cohomologie galoisienne des corps p-adiques. *Bulletin de la Société Mathématique de France*, 126:563–600, 1998. → pages 2, 24, 26, 27

[15] S. J. Neukirch, A and W. K. *Cohomology of number fields*, volume 126 of *Grundleh- ren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, 2000. → pages 33

[16] K. Kato. *Lectures on the approach to Iwasawa theory for Hasse-Weil L-functions via BdR. Part I*, volume 1553, pages 50–163. Springer Berlin Heidelberg, 1993. → pages 42

[17] D. Loeffler and S. L. Zerbes. Iwasawa theory and p-adic l-functions over ${\mathbb z}_{p}^{2}$-extensions. *International Journal of Number Theory*, 10(08):2045–2095, 2015/02/19 2014. → pages 2, 72

[18] B. Perrin-Riou. Théorie d'iwasawa des répresentations p-adiques sur un corps local. *Invent. Math.*, 115:81–149, 1994. → pages 2, 36, 63, 68, 69

[19] B. Perrin-Riou. Fonctions l p-adiques des representations p-adiques. *Astérisque*, pages 81–149, 1995. → pages 72

[20] B. Perrin-Riou. *Théorie d'Iwasawa des représentations p-adiques semi-stables*, volume 84. Mémoires de la SMF, 2001. → pages 60