Fontaine's rings and p-adic L-functions

Pierre Colmez
C.N.R.S. Institut de Mathématiques de Jussieu

These are notes from a course given at Tsinghua University during the fall of 2004. The aim of the course was to explain how to construct p-adic L-functions using the theory of (φ, Γ)-modules of Fontaine. This construction is an adaptation of an idea of Perrin-Riou. The content of the course is well reflected in the table of contents which is almost the only thing that I modified from the notes taken and typed by the students Wang Shanwen, Chen Miaofen, Hu Yongquan, Yin Gang, Li Yan and Hu Yong, under the supervision of Ouyang Yi, all of whom I thank heartily. The course runs in parallel to a course given by Fontaine in which the theory of (φ, Γ)-modules was explained as well as some topics from p-adic Hodge theory which are used freely in these notes, which means that they are not entirely self-contained. Also, as time runs short at the end, the last chapter is more a survey than a course. For a bibliography and further reading, the reader is referred to my Bourbaki talk of June 2003 published in Astérisque 294.

Contents

Part I

Classical p-adic L-functions: zeta functions and modular forms

Chapter 1

The p-adic zeta function of Kubota-Leopoldt

1.1 The Riemann zeta function at negative integers

We first recall the definitions of Riemann zeta function and the classical Gamma function:

$$\begin{aligned}\zeta(s) &= \sum_{n=1}^{+\infty} n^{-s} = \prod_p (1-p^{-s})^{-1}, \text{ if } \mathrm{Re}\,(s) > 1.\\ \Gamma(s) &= \int_0^{+\infty} e^{-t} t^s \frac{dt}{t}, \text{ if } \mathrm{Re}\,(s) > 0.\end{aligned}$$

The Γ-function has the following properties:

(i) $\Gamma(s+1) = s\Gamma(s)$, which implies that Γ has a meromorphic continuation to $\mathbb{C}$ with simple poles at negative integers and 0.

(ii) $\Gamma(n) = (n-1)!$ if $n \geq 1$.

(iii) $\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin(\pi s)}$, which implies that $\frac{1}{\Gamma(s)}$ is an entire(or holomorphic) function on $\mathbb{C}$ with simple zeros at $-n$ for $n \in \mathbb{N}$.

(iv) $\Gamma(\frac{1}{2}) = \sqrt{\pi}$.

Then we have the following formulas:

$$\begin{aligned} n^{-s} &= \frac{1}{\Gamma(s)}\int_0^{+\infty} e^{-nt}t^s\frac{dt}{t}, \\ \zeta(s) &= \frac{1}{\Gamma(s)}\int_0^{+\infty}\sum_{n=1}^{+\infty} e^{-nt}t^s\frac{dt}{t} = \frac{1}{\Gamma(s)}\int_0^{+\infty}\frac{1}{e^t-1}t^s\frac{dt}{t}. \end{aligned}$$

Lemma 1.1.1. *If $f:\mathbb{R}_+\to\mathbb{C}$ is a $\mathcal{C}^\infty$-function on $\mathbb{R}_+$, rapidly decreasing* (i.e., $t^n f(t)\to 0$ when $t\to+\infty$ for all $n\in\mathbb{N}$)*, then*

$$L(f,s) = \frac{1}{\Gamma(s)}\int_0^{+\infty} f(t)t^s\frac{dt}{t},\ Re(s)>0$$

has an analytic continuation to $\mathbb{C}$, and

$$L(f,-n) = (-1)^n f^{(n)}(0).$$

Proof. Choose a $\mathcal{C}^\infty$-function ϕ on $\mathbb{R}_+$, such that $\phi(t)=1$ for $t\in[0,1]$ and $\phi(t)=0$ for $t\geq 2$.

Let $f=f_1+f_2$, where $f_1=\phi f$, $f_2=(1-\phi)f$. Then $\int_0^\infty f_2(t)t^s\frac{dt}{t}$ is holomorphic on $\mathbb{C}$, hence $L(f_2,s)$ is also holomorphic and $L(f_2,-n)=0=f_2^{(-n)}(0)$. Since, for $\mathrm{Re}\,(s)>0$,

$$L(f_1,s) = \frac{1}{\Gamma(s)}[f_1(t)\frac{t^s}{s}]|_0^{+\infty} - \frac{1}{s\Gamma(s)}\int_0^{+\infty} f_1'(t)t^{s+1}\frac{dt}{t}$$

$$= -L(f_1'(t),s+1) = (-1)^n L(f_1^{(n)},s+n),$$

we get analytic continuation for f_1 and hence for f, moreover,

$$L(f,-n) = L(f_1,-n) = (-1)^{n+1}L(f_1^{(n+1)},1)$$

$$= (-1)^{n+1}\int_0^{+\infty} f_1^{(n+1)}(t)dt = (-1)^n f_1^{(n)}(0) = (-1)^n f^{(n)}(0).$$

$\square$

We now apply the above lemma to the function $f(t)=\frac{t}{e^t-1}$. Note that

$$f(t) = \sum_0^\infty B_n\frac{t^n}{n!},$$

where $B_n \in \mathbb{Q}$ is the n-th *Bernoulli number* with value:

$$B_0 = 1, B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}, B_3 = 0, B_4 = -\frac{1}{30}, B_5 = 0 \cdots$$

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

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

so we obtain the following result.

Theorem 1.1.2. (i) *ζ has a meromorphic continuation to $\mathbb{C}$. It is holomorphic except for a simple pole at $s = 1$ with residue $L(f, 0) = B_0 = 1$.*

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

$$\begin{aligned} \zeta(-n) &= \frac{-1}{n+1} L(f, -n-1) = \frac{(-1)^n}{n+1} f^{(n+1)}(0) \\ &= (-1)^n \frac{B_{n+1}}{n+1} \ \in \mathbb{Q} \\ \Big(&= -\frac{B_{n+1}}{n+1} \ \textit{if } n \geq 2 \Big). \end{aligned}$$

Theorem 1.1.3 (Kummer). *If p does not divide the numerators of $\zeta(-3)$, $\zeta(-5), \cdots, \zeta(2-p)$, then the class number of $\mathbb{Q}(u_p)$ is prime to p.*

Remark. This theorem and a lot of extra work implies Fermat's Last Theorem for these *regular* primes. We will not prove it in these notes, but we will focus on the following result, also discovered by Kummer, which plays an important role in the proof.

Theorem 1.1.4 (Kummer's congruences). *Let $a \geq 2$ be prime to p. Let $k \geq 1$. If $n_1, n_2 \geq k$ such that $n_1 \equiv n_2$ mod $(p-1)p^{k-1}$, then*

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

1.2 p-adic Banach spaces

Definition 1.2.1. A *p-adic Banach space B* is a $\mathbb{Q}_p$-vector space with a lattice B^0($\mathbb{Z}_p$-module) separated and complete for the p-adic topology, i.e.,

$$B^0 \simeq \varprojlim_{n \in \mathbb{N}} B^0 / p^n B^0.$$

For all $x \in B$, there exists $n \in \mathbb{Z}$, such that $x \in p^n B^0$. Define

$$v_B(x) = \sup_{n \in \mathbb{N} \cup \{+\infty\}} \{n : x \in p^n B^0\}.$$

It satisfies the following properties:

$$v_B(x+y) \geq \min(v_B(x), v_B(y)),$$
$$v_B(\lambda x) = v_p(\lambda) + v_B(x), \text{ if } \lambda \in \mathbb{Q}_p.$$

Then $\| x \|_B = p^{-v_B(x)}$ defines a norm on B, such that B is complete for $\|\|_B$ and B^0 is the unit ball.

Example 1.2.2. (i) $B = \mathbb{C}_p = \widehat{\overline{\mathbb{Q}}_p}$, $B^0 = \mathcal{O}_{\mathbb{C}_p}$, $v_B(x) = [v_p(x)] \in \mathbb{Z}$;

(ii) The space $B = \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$ of continuous functions on $\mathbb{Z}_p$. $B^0 = \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Z}_p)$ is a lattice, and $v_B(f) = \inf_{x \in \mathbb{Z}} v_p(f(x)) \neq -\infty$ because $\mathbb{Z}_p$ is compact.

(iii) Let $B = \mathcal{C}^0(\mathbb{Z}_p, \mathbb{C}_p)$, $B^0 = C^0(\mathbb{Z}_p, \mathcal{O}_{\mathbb{C}_p})$; $v_B(f) = \inf_{x \in \mathbb{Z}} [v_p(f(x))]$.

Definition 1.2.3. A *Banach basis* of a p-adic Banach space B is a family $(e_i)_{i \in I}$ of elements of B, satisfying the following conditions:

(i) For every $x \in B$, $x = \sum_{i \in I} x_i e_i$, $x_i \in \mathbb{Q}_p$ in a unique way with $x_i \to 0$ when $i \to \infty$; equivalently for any C, the set $\{i \,|\, v_p(x_i) \leq C\}$ is a finite set.

(ii) $v_B(x) = \inf_{i \in I} v_p(x_i)$.

Theorem 1.2.4. *A family $(e_i)_{i \in I}$ of elements of B is a Banach basis if and only if*

(i) *$e_i \in B^0$ for all i;*

(ii) *the set $(\bar{e}_i)_{i \in I}$ form a basis of B^0/pB^0 as a $\mathbb{F}_p$-vector space.*

Proof. We leave the proof of the theorem as an exercise. □

Let B and B' be two p-adic Banach spaces with Banach basis $(e_i)_{i \in I}$ and $(f_j)_{j \in J}$ respectively, then $B \widehat{\bigotimes} B'$ is a p-adic Banach space with Banach basis $(e_i \otimes f_j)_{(i,j) \in I \times J}$. Thus for all $x \in B \widehat{\bigotimes} B'$,

$$\begin{aligned} x &= \sum_{i,j} x_{i,j} e_i \otimes f_j \quad (x_{i,j} \in \mathbb{Q}_p, x_{i,j} \to 0 \text{ as } (i,j) \to \infty) \\ &= \sum_j y_j \otimes f_j \quad (y_j \in B, y_j \to 0 \text{ as } j \to \infty) \\ &= \sum_i e_i \otimes z_i \quad (z_i \in B', z_i \to 0 \text{ as } i \to \infty). \end{aligned}$$

Exercise. $\mathcal{C}^0(\mathbb{Z}_p, \mathbb{C}_p) = \mathbb{C}_p \widehat{\bigotimes} \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$.

1.3 Continuous functions on $\mathbb{Z}_p$

1.3.1 Mahler's coefficients

We have the binomial function:

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

Lemma 1.3.1. $v_{\mathcal{C}^0}(\binom{x}{n}) = 0$.

Proof. Since $\binom{n}{n} = 1$, $v_{\mathcal{C}^0}(\binom{x}{n}) \leq 0$.

If $x \in \mathbb{N}$, then $\binom{x}{n} \in \mathbb{N}$ implies $v_p(\binom{x}{n}) \geq 0$. Hence for all $x \in \mathbb{Z}_p$, $v_p(\binom{x}{n}) \geq 0$ because $\mathbb{N}$ is dense in $\mathbb{Z}_p$. □

For all $f \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$, we write

$$f^{[0]} = f, \qquad f^{[k-1]}(x) = f^{[k]}(x+1) - f^{[k]}(x)$$

and write the *Mahler's coefficient*

$$a_n(f) = f^{[n]}(0).$$

Hence:

$$\begin{aligned} f^{[n]}(x) &= \sum_{i=0}^{n} (-1)^i \binom{n}{i} f(x+n-i), \\ a_n(f) &= \sum_{i=0}^{n} (-1)^i \binom{n}{i} f(n-i). \end{aligned}$$

Theorem 1.3.2 (Mahler). *If $f \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$, then*

(i) $\lim\limits_{n\to\infty} v_p(a_n(f)) = +\infty$,

(ii) *For all $x \in \mathbb{Z}_p$, $f(x) = \sum\limits_{n=0}^{\infty} a_n(f) \binom{x}{n}$,*

(iii) $v_{\mathcal{C}^0}(f) = \inf v_p(a_n(f))$.

Proof. Let $\ell_\infty = \{a = (a_n)_{n\in\mathbb{N}} : a_n \in \mathbb{Q}_p \text{ bounded}\}$, $v_{\ell_\infty}(a) = \inf_{n\in\mathbb{N}} v_p(a_n)$. Then

- $f \mapsto a(f) = (a_n(f))_{n\in\mathbb{N}}$ is a continuous map from $\mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$ to ℓ_∞. and $v_{\ell_\infty}(a(f)) \geq v_{\mathcal{C}^0}(f)$.
- The space $\ell_\infty^0 = \{(a_n)_{n\in\mathbb{N}} : a_n \to 0, \text{ as } n \to \infty\}$ is a closed subspace of ℓ_∞ and $B = \{f : a(f) \in \ell_\infty^0\}$ is a close subspace of $\mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$.
- For all $a \in \ell_\infty^0$,
$$f_a = \sum_{n=0}^{+\infty} a_n \binom{x}{n} \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$$
because the series converges uniformly. Moreover, $v_{\mathcal{C}^0}(f_a) \geq v_{\ell_\infty}(a)$ and as $\binom{x+1}{n+1} - \binom{x}{n+1} = \binom{x}{n}$,
$$f_a^{[k]} = \sum_{n=0}^{+\infty} a_{n+k} \binom{x}{n}.$$
Hence we have: $a_k(f) = f^{[k]}(0) = a_k$, which implies $a(f_a) = a$.
- $f \mapsto a(f)$ is injective. Since $a(f) = 0$ implies $f(n) = 0$ for all $n \in \mathbb{N}$. Hence $f = 0$ by the density of $\mathbb{N}$ in $\mathbb{Z}_p$.

Now for $f \in B, a(f) \in \ell_\infty^0$ implies $f - f_{a(f)} = 0$ because $a(f - f_{a(f)}) = a(f) - a(f) = 0$ and a is injective. So $f \in B$ implies that f satisfies (ii). Moreover, since

$$v_{\ell_\infty}(a(f)) \geq v_{\mathcal{C}^0}(f) = v_{\mathcal{C}^0}(f_{a(f)}) \geq v_{\ell_\infty}(a(f)),$$

(iii) is also true. It remains to show that:

Claim: $B = \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$. □

(a) First proof. We have a lemma:

Lemma 1.3.3. *If $f \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$, then there exists $k \in \mathbb{N}$ such that*

$$v_{\mathcal{C}^0}(f^{[p^k]}) \geq v_{\mathcal{C}^0}(f) + 1.$$

Proof. We have

$$f^{[p^k]}(x) = f(x+p^k) - f(x) + \sum_{i=1}^{p^k-1} (-1)^i \binom{p^k}{i} f(x+p^k-i) + (1+(-1)^{p^k})f(x).$$

Now $v_p(\binom{p^k}{i}) \geq 1$, if $1 \leq i \leq p^k - 1$ et $v_p(1+(-1)^{p^k}) \geq 1$. Since $\mathbb{Z}_p$ is compact, f is uniformly continuous. For every c, there exists N, when $v_p(x-y) \geq N$, we have $v_p(f(x) - f(y)) \geq c$. It gives the result for $k = N$. □

First proof of the Claim. Repeat the lemma: for every $c = v_{\mathcal{C}^0}(f) + k$, there exists an N, such that $v_{\mathcal{C}^0}(f^{[N]}) \geq c$. Hence, for all $n \geq N$, $v_p(a_n(f)) \geq c$. □

1.3.2 Locally constant functions.

Choose a $z \in \mathbb{C}_p$, such that $v_p(z-1) > 0$. Then

$$f_z(x) = \sum_{n=0}^{+\infty} \binom{x}{n} (z-1)^n \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{C}_p).$$

Note $k \in \mathbb{N}$, $f_z(k) = z^k$. So we write, $f_z(x) = z^x$ and we have $z^{x+y} = z^x z^y$.

Example 1.3.4. (i) $z^{\frac{1}{2}} = \sum_{n=0}^{+\infty} \binom{\frac{1}{2}}{n} (z-1)^n$. $z = \frac{16}{9}, z - 1 = \frac{7}{9}$, the series converges in $\mathbb{R}$ to $\frac{4}{3}$, and converges in $\mathbb{Q}_7$ to $-\frac{4}{3}$.

(ii) If z is a primitive p^n-th root of 1, then

$$v_p(z-1) = \frac{1}{(p-1)p^{n-1}} > 0.$$

Note that $z^{x+p^n} = z^x$ for all x, then z^x is locally constant(constant mod $p^n\mathbb{Z}_p$). The characteristic function of $i + p^n\mathbb{Z}_p$ is given by

$$1_{i+p^n\mathbb{Z}_p}(x) = \frac{1}{p^n} \sum_{z^{p^n}=1} z^{-i} z^x$$

since

$$\sum_{z^{p^n}=1} z^x = \begin{cases} p^n & \text{if } x \in p^n\mathbb{Z}_p; \\ 0 & \text{if not.} \end{cases}$$

Lemma 1.3.5. *The set of locally constant functions* $LC(\mathbb{Z}_p, \mathbb{Q}_p) \subset B$.

Proof. By compactness of $\mathbb{Z}_p$, a locally constant function is a linear combination of $1_{i+p^n\mathbb{Z}^p} z^x, z \in \boldsymbol{\mu}_{p^\infty}$, thus a linear combination of z^x. But $a_n(z^x) = (z-1)^n$ goes to 0, when n goes to ∞, hence $z^x \in B$. □

Lemma 1.3.6. $LC(\mathbb{Z}_p, \mathbb{Q}_p)$ *is dense in* $\mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$.

Proof. For every $f \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$, let

$$f_k = \sum_{i=0}^{p^k-1} f(i) 1_{i+p^k\mathbb{Z}_p}.$$

Then $f_k \to f$ in $\mathcal{C}^0$ because f is uniformly continuous. □

Second proof of the Claim. By the above two lemmas, $LC(\mathbb{Z}_p, \mathbb{Q}_p) \subset B \subset \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$, B is closed and $LC(\mathbb{Z}_p, \mathbb{Q}_p)$ is dense in $\mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$, hence $B = \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$. □

1.4 Measures on $\mathbb{Z}_p$

1.4.1 The Amice transform

Definition 1.4.1. A *measure* μ on $\mathbb{Z}_p$ with values in a p-adic Banach space B is a continuous linear map $f \mapsto \int_{\mathbb{Z}_p} f(x)\mu = \int_{\mathbb{Z}_p} f(x)\mu(x)$ from $C^0(\mathbb{Z}_p, \mathbb{Q}_p)$ to B.

Remark. (i) If $L \subset \mathbb{C}_p$ is a closed subfield and B is an L-vector space, then μ extends by continuity and L-linearity to $\mathcal{C}^0(\mathbb{Z}_p, L) = L \widehat{\bigotimes} C^0(\mathbb{Z}_p, \mathbb{Q}_p)$.

(ii) We denote $\mathcal{D}_0(\mathbb{Z}_p, B)$ the set of the measure on $\mathbb{Z}_p$ with values in B, then $\mathcal{D}_0(\mathbb{Z}_p, B) = \mathcal{D}_0(\mathbb{Z}_p, \mathbb{Q}_p) \widehat{\bigotimes} B$.

Definition 1.4.2. The *Amice transform* of a measure μ is defined to be the map:

$$\mu \mapsto A_\mu(T) = \int_{\mathbb{Z}_p} (1+T)^x \mu(x) = \sum_{n=0}^{+\infty} T^n \int_{\mathbb{Z}_p} \binom{x}{n} \mu.$$

Lemma 1.4.3. *If* $v_p(z-1) > 0$, $A_\mu(z-1) = \int_{\mathbb{Z}_p} z^x \mu(x)$.

Proof. Since $z^x = \sum_{n=0}^{+\infty}(z-1)^n\binom{x}{n}$ with normal convergence in $\mathcal{C}^0(\mathbb{Z}_p,\mathbb{Q}_p)$, one can exchange $\sum$ and $\int$. $\square$

Definition 1.4.4. The valuation on $\mathcal{D}_0$ is

$$v_{\mathcal{D}_0}(\mu) = \inf_{f\neq 0}(v_p(\int_{\mathbb{Z}_p} f\mu) - v_{\mathcal{C}^0}(f)).$$

Theorem 1.4.5. *The map $\mu \mapsto A_\mu$ is an isometry from $\mathcal{D}_0(\mathbb{Z}_p,\mathbb{Q}_p)$ to the set $\{\sum_{n=0}^{+\infty} b_nT^n, b_n$ bounded, and $b_n \in \mathbb{Q}_p\}$ with the valuation $v(\sum_{n=0}^{+\infty} b_nT^n) = \inf_{n\in\mathbb{N}} v_p(b_n)$.*

Proof. On one hand, for all $\mu \in \mathcal{D}_0(\mathbb{Z}_p,\mathbb{Q}_p)$, write $A_\mu(T) = \sum_{n=0}^{+\infty} b_n(\mu)T^n$, then $b_n(\mu) = \int_{\mathbb{Z}_p}\binom{x}{n}\mu$. Since $v_{\mathcal{C}^0}(\binom{x}{n}) = 0$ by Lemma 1.3.1,

$$v_p(b_n(\mu)) \geq v_{\mathcal{D}_0}(\mu) + v_{\mathcal{C}^0}(\binom{x}{n}) \geq v_{\mathcal{D}_0}(\mu)$$

for all n, hence $v(A_\mu) \geq v_{\mathcal{D}_0}(\mu)$.

On the other hand, if $(b_n)_{n\in\mathbb{N}}$ is bounded, $f \mapsto \sum_{n=0}^{+\infty} b_na_n(f)$(by Mahler's theorem, $a_n(f)\to 0$) gives a measure μ_b whose Amice transform is

$$A_{\mu_b}(T) = \sum_{n=0}^{+\infty} T^n\int_{\mathbb{Z}p}\binom{x}{n}\mu_b = \sum_{n=0}^{+\infty} T^n(\sum_{i=0}^{+\infty} b_ia_i(\binom{x}{n})) = \sum_{n=0}^{+\infty} b_nT^n$$

since

$$a_n(\binom{x}{i}) = \begin{cases} 1 & \text{if } i=n, \\ 0 & \text{otherwise.}\end{cases}$$

Hence

$$\begin{aligned} v_p(\sum_{n=0}^{+\infty} b_na_n(f)) &\geq \min_n(v_p(b_n)+v_p(a_n(f))) \\ &\geq \min_n(v_p(b_n)) + \min_n(a_n(f)) \\ &= v(\sum b_nT^n) + v_{\mathcal{C}^0}(f) \\ &= v(A_\mu) + v_{\mathcal{C}^0}(f). \end{aligned}$$

Thus $v_{\mathcal{D}_0}(\mu_b) \geq v(A_\mu)$. Then we have $v(A_\mu) = v_{\mathcal{D}_0}(\mu)$. $\square$

By Lemma 1.3.6, we know that locally constant functions are dense in $\mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$. Explicitly, for all $f \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$, the locally constant functions $f_n = \sum_{i=0}^{p^n-1} f(i) 1_{i+p^n\mathbb{Z}_p} \to f$ in $\mathcal{C}^0$.

Now if $\mu \in \mathcal{D}_0(\mathbb{Z}_p, \mathbb{Q}_p)$, set $\mu(i + p^n\mathbb{Z}_p) = \int_{\mathbb{Z}_p} 1_{i+p^n\mathbb{Z}_p}\mu$. Then $\int_{\mathbb{Z}_p} f\,\mu$ is given by the following "Riemann sums"

$$\int_{\mathbb{Z}_p} f\mu = \lim_{n\to\infty} \sum_{i=0}^{p^n-1} f(i)\mu(i + p^n\mathbb{Z}_p) \tag{1.1}$$

Note that $v_p(\mu(i + p^n\mathbb{Z}_p)) \geq v_{\mathcal{D}_0}(\mu)$.

Theorem 1.4.6. *If μ is an additive bounded function on compact open subsets of $\mathbb{Z}_p$ (by compactness of $\mathbb{Z}_p$ is a finite disjoint union of $i + p^n\mathbb{Z}_p$ for some n), then μ extends uniquely as a measure on $\mathbb{Z}_p$ via* (1.1).

Proof. Since μ is an additive function on compact open subsets, μ is linear on locally constant functions. And μ is bounded, hence μ is continuous for $v_{\mathcal{C}^0}$. As the locally constant functions are dense in $\mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$, we have μ as a measure on $\mathbb{Z}_p$. $\square$

1.4.2 examples of measures on $\mathbb{Z}_p$ and of operations on measures.

Example 1.4.7. *Haar measure*: $\mu(\mathbb{Z}_p) = 1$ and μ is invariant by translation. We must have $\mu(i + p^n\mathbb{Z}_p) = \frac{1}{p^n}$ which is not bounded. Hence, there exists no Haar measure on $\mathbb{Z}_p$.

Example 1.4.8. *Dirac measure*: For $a \in \mathbb{Z}_p$, we define δ_a by $\int_{\mathbb{Z}_p} f(x)\delta_a = f(a)$. The Amice transform of δ_a is $A_{\delta_a}(T) = (1 + T)^a$.

Example 1.4.9. *Multiplication of a measure by a continuous function.* For $\mu \in \mathcal{D}_0$, $f \in \mathcal{C}^0$, we define the measure $f\mu$ by

$$\int_{\mathbb{Z}_p} g \cdot f\mu = \int_{\mathbb{Z}_p} f(x)g(x)\mu$$

for all $g \in \mathcal{C}^0$.

(i) Let $f(x) = x$, since

$$x\binom{x}{n} = (x-n+n)\binom{x}{n} = (n+1)\binom{x}{n+1} + n\binom{x}{n},$$

the Amice transform is

$$\begin{aligned} A_{x\mu} &= \sum_{n=0}^{+\infty} T^n \int_{\mathbb{Z}_p} \binom{x}{n} x\mu \\ &= \sum_{n=0}^{+\infty} T^n \left[(n+1)\int_{\mathbb{Z}_p} \binom{x}{n+1}\mu + n\int_{\mathbb{Z}_p}\binom{x}{n}\mu\right] \\ &= (1+T)\frac{d}{dT}A_\mu. \end{aligned}$$

(ii) Let $f(x) = z^x$, $v_p(z-1) > 0$. For any y, $v_p(y-1) > 0$, then

$$\int_{\mathbb{Z}_p} y^x(z^x\mu) = \int_{\mathbb{Z}_p} (yz)^x\mu = A_\mu(yz-1)$$

which implies that

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

(iii) The *restriction* to a compact open set X of $\mathbb{Z}_p$: it is nothing but the multiplication by 1_X. If $X = i + p^n\mathbb{Z}_p$, then $1_{i+p^n\mathbb{Z}_p}(x) = p^{-n}\sum_{z^{p^n}=1} z^{-i}z^x$, hence

$$A_{\mathrm{Res}_{i+p^n\mathbb{Z}_p}\mu}(T) = p^{-n}\sum_{z^{p^n}=1} z^{-i}A_\mu((1+T)z-1).$$

Example 1.4.10. *Actions of φ and ψ.* For $\mu \in \mathcal{D}_0$, we define the action of φ on μ by

$$\int_{\mathbb{Z}_p} f(x)\varphi(\mu) = \int_{\mathbb{Z}_p} f(px)\mu.$$

Hence

$$A_{\varphi(\mu)}(T) = \sum_{n=0}^{+\infty} T^n \int_{\mathbb{Z}_p}\binom{px}{n}\mu = A_\mu((1+T)^p - 1) = \varphi(A_\mu(T))$$

where $\varphi : T \mapsto (1+T)^p - 1$ (compare this formula with (φ, Γ)-modules). We define the action of ψ by

$$\int_{\mathbb{Z}_p} f(x)\psi(\mu) = \int_{\mathbb{Z}_p} f(\frac{x}{p})\mu.$$

Then $A_{\psi(\mu)} = \psi(A_\mu)$ where

$$\psi(F)((1+T)^p - 1) = \frac{1}{p}\sum_{z^p=1} F((1+T)z - 1).$$

The actions φ and ψ satisfy the following properties:

(i) $\psi \circ \varphi = \mathrm{Id}$;

(ii) $\psi(\mu) = 0 \Leftrightarrow \mu$ has a support in $\mathbb{Z}_p^*$;

(iii) $\mathrm{Res}_{\mathbb{Z}_p^*}(\mu) = (1 - \varphi\psi)\mu$.

The map ψ is very important in the theory of (φ, Γ)-modules.

Example 1.4.11. *Action of* Γ. Let $\Gamma = \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p)$. Let $\chi : \Gamma \xrightarrow{\sim} \mathbb{Z}_p^*$ be the cyclotomic character. For $\gamma \in \Gamma$ and $\mu \in \mathcal{D}_0$, we let $\gamma\mu$ be given by

$$\int_{\mathbb{Z}_p} f(x)\gamma\mu = \int_{\mathbb{Z}_p} f(\chi(\gamma)x)\mu.$$

One can verify that $A_{\gamma\mu}(T) = A_\mu((1+T)^{\chi(\gamma)} - 1) = \gamma(A_\mu(T))$ for $\gamma(T) = (1+T)^{\chi(\gamma)} - 1$. (Compare this formula with (φ, Γ)-modules.)

For all $\gamma \in \Gamma$, γ commutes with ϕ and ψ.

Example 1.4.12. *Convolution* $\lambda * \mu$. Let λ, μ be two measures, their convolution $\lambda * \mu$ is defined by

$$\int_{\mathbb{Z}_p} f(x)\lambda * \mu = \int_{\mathbb{Z}_p} (\int_{\mathbb{Z}_p} f(x+y)\mu(x))\lambda(y).$$

Here we have to verify $y \mapsto \int_{\mathbb{Z}_p} f(x+y)\mu(x) \in \mathcal{C}^0$, which is a direct consequence of the fact f is uniformly continuous.

Let $f(x) = z^x$, $v_p(z-1) > 0$, then

$$\int_{\mathbb{Z}_p} z^x \lambda * \mu = \int_{\mathbb{Z}_p} z^x \mu(x) \int_{\mathbb{Z}_p} z^y \lambda(y),$$

thus $A_{\lambda * \mu} = A_\lambda A_\mu$.

1.5 The p-adic zeta function

1.5.1 Kummer's congruences.

Lemma 1.5.1. *For $a \in \mathbb{Z}_p^*$, there exists a measure $\lambda_a \in \mathcal{D}_0$ such that*

$$A_{\lambda_a} = \int_{\mathbb{Z}_p} (1+T)^x \lambda_a = \frac{1}{T} - \frac{a}{(1+T)^a - 1}.$$

Proof. This follows from Theorem 1.4.5 and the fact

$$\frac{a}{(1+T)^a - 1} = \frac{a}{\sum_{n=1}^{\infty} \binom{a}{n} T^n} = \frac{1}{T} \cdot \frac{1}{1 + \sum_{n=2}^{\infty} a^{-1} \binom{a}{n} T^{n-1}} \in \frac{1}{T} + \mathbb{Z}_p[[T]]$$

since $a^{-1}\binom{a}{n} \in \mathbb{Z}_p$. Moreover, we have $v_{\mathcal{D}_0}(\lambda_a) = 0$. □

Proposition 1.5.2. *For every $n \in \mathbb{N}$, $\int_{\mathbb{Z}_p} x^n \lambda_a = (-1)^n (1 - a^{1+n}) \zeta(-n)$.*

Proof. For $a \in \mathbb{R}_+^*$, for $T = e^t - 1$, let

$$f_a(t) = A_{\lambda_a}(T) = \frac{1}{e^t - 1} - \frac{a}{e^{at} - 1},$$

then f_a is in $\mathcal{C}^\infty$ on $\mathbb{R}^+$ and rapidly decreasing. Hence

$$L(f_a, s) = \frac{1}{\Gamma(s)} \int_0^{+\infty} f_a(t) t^s \frac{dt}{t} = (1 - a^{1-s}) \zeta(s)$$
$$f_a^n(0) = (-1)^n L(f_a, -n) = (-1)^n (1 - a^{1+n}) \zeta(-n)$$

The identity $f_a^n(0) = (-1)^n (1 - a^{1+n}) \zeta(-n)$ is algebric, so is true for all a, hence even on $\mathbb{Z}_p^*$. Thus

$$\int_{\mathbb{Z}_p} x^n \lambda_a = (\frac{d}{dt})^n (\int_{\mathbb{Z}_p} e^{tx} \lambda_a)|_{t=0} = (\frac{d}{dt})^n A_{\lambda_a}(e^t - 1)|_{t=0} = f_a^{(n)}(0).$$

□

Corollary 1.5.3. *For $a \in \mathbb{Z}_p^*$, $k \geq 1$ ($k \geq 2$ if $p = 2$), $n_1, n_2 \geq k$, $n_1 \equiv n_2 \bmod (p-1)p^{k-1}$, then*

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

Proof. The left hand side $LHS = v_p((1-a^{1+n_1})\zeta(-n_1) - (1-a^{1+n_2})\zeta(-n_2))$ is

$$v_p(\int_{\mathbb{Z}_p}(x^{n_1} - x^{n_2})\lambda_a) \geq v_{\mathcal{D}_0}(\lambda_a) + v_{\mathcal{C}^0}(x^{n_1} - x^{n_2}).$$

From the proof of Lemma 1.5.1, $v_{\mathcal{D}_0}(\lambda_a) = 0$, thus $LHS \geq v_{\mathcal{C}^0}(x^{n_1} - x^{n_2})$. It suffices to show $v_{\mathcal{C}^0}(x^{n_1} - x^{n_2}) \geq k$. There are two cases:

If $x \in p\mathbb{Z}_p$, then $v_p(x^{n_1}) \geq k$ and $v_p(x^{n_2}) \geq k$ since $n_1, n_2 \geq k$.

If $x \in \mathbb{Z}_p^*$, $v_p(x^{n_1} - x^{n_2}) \geq k$ because $(\mathbb{Z}/p^k\mathbb{Z})^*$ has order $(p-1)p^{k-1}$ and $n_1 - n_2$ is divisible by $(p-1)p^{k-1}$. □

Remark. The statement is not clean because of $x \in p\mathbb{Z}_p$.

1.5.2 Restriction to $\mathbb{Z}_p^*$.

Lemma 1.5.4. $\psi(\frac{1}{T}) = \frac{1}{T}$.

Proof. Let $F(T) = \psi(\frac{1}{T})$, then

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

□

Proposition 1.5.5. $\psi(\lambda_a) = \lambda_a$.

Proof. We only need to show the same thing on the Amice transform, but

$$A_{\lambda_a}(T) = \frac{1}{T} - \frac{a}{(1+T)^a - 1} = \frac{1}{T} - a\cdot\gamma_a(\frac{1}{T})$$

where $\gamma_a \in \Gamma$ is the inverse of a by $\chi : \Gamma \to \mathbb{Z}_p^*$, i.e., $\chi(\gamma_a) = a$. Since ψ and γ_a commutes and $\psi(\frac{1}{T}) = \frac{1}{T}$, we have

$$\psi(A_{\lambda_a}) = \frac{1}{T} - a\gamma_a(\frac{1}{T}) = A_{\lambda_a}.$$

□

Corollary 1.5.6. (i) $\mathrm{Res}_{\mathbb{Z}_p^*}(\lambda_a) = (1-\phi\psi)\lambda_a = (1-\phi)\lambda_a$,

(ii) $\int_{\mathbb{Z}_p^*} x^n\lambda_a = \int_{\mathbb{Z}_p} x^n(1-\phi)\lambda_a = (-1)^n(1-a^{n+1})(1-p^n)\zeta(-n)$.

Remark. The factor $(1-p^n)$ is the Euler factor of the zeta function at p.

Theorem 1.5.7. *For $i \in \mathbb{Z}/(p-1)\mathbb{Z}$ (or $i \in \mathbb{Z}/2\mathbb{Z}$ if $p=2$), there exists a unique function $\zeta_{p,i}$, analytic on $\mathbb{Z}_p$ if $i \neq 1$, and $(s-1)\zeta_{p,1}(s)$ is analytic on $\mathbb{Z}_p$, such that $\zeta_{p,i}(-n) = (1-p^n)\zeta(-n)$ if $n \equiv -i \bmod p-1$ and $n \in \mathbb{N}$.*

Remark. (i) If $i \equiv 0 \bmod 2$, then $\zeta_{p,i} = 0$ since $\zeta(-n) = 0$ for n even and ≥ 2;

(ii) To get p-adic continuity, one has to modify ζ by some "Euler factor at p".

(iii) Uniqueness is trivial because $\mathbb{N}$ is infinite and $\mathbb{Z}_p$ is compact.

(iv) The existence is kind of a miracle. Its proof relies on Leopoldt's Γ-transform.

1.5.3 Leopoldt's Γ-transform.

Lemma 1.5.8. (i) *Every $x \in \mathbb{Z}_p^*$ can be written uniquely as $x = \omega(x)\langle x\rangle$, with*

$$\omega(x) \in \boldsymbol{\mu}(\mathbb{Q}_p) = \begin{cases} \{\pm 1\} & \text{if } p=2, \\ \boldsymbol{\mu}_{p-1}, & \text{if } p \neq 2 \end{cases} \quad \text{and} \quad \langle x\rangle \in 1+2p\mathbb{Z}_p.$$

(ii) $\omega(xy) = \omega(x)\omega(y)$, $\langle xy\rangle = \langle x\rangle\langle y\rangle$.

Proof. If $p=2$, it is obvious.

If $p \neq 2$, $\omega(x) = \lim\limits_{n\to\infty} x^{p^n} = [\bar{x}]$. ☐

Remark. (i) ω is the so-called *Teichmüller character*;

(ii) $\langle x\rangle = \exp(\log(x))$;

(iii) $x^n = \omega(x)^n\langle x\rangle^n$, here $\langle x\rangle^n$ is the restriction to $\mathbb{N}$ of $\langle x\rangle^s$ which is continuous in s, $\omega(x)^n$ is periodic of period $p-1$, which is not p-adically continuous.

Proposition 1.5.9. *If λ is a measure on $\mathbb{Z}_p^*$, $u = 1+2p$, then there exists a measure $\Gamma_\lambda^{(i)}$ on $\mathbb{Z}_p$ (Leopoldt's transform) such that*

$$\int_{\mathbb{Z}_p^*} \omega(x)^i\langle x\rangle^s\lambda(x) = \int_{\mathbb{Z}_p} u^{sy}\Gamma_\lambda^{(i)}(y) = A_{\Gamma_\lambda^{(i)}}(u^s-1).$$

Proof. We have

$$\begin{aligned}\int_{\mathbb{Z}_p^*} \omega(x)^i \langle x\rangle^s \lambda(x) &= \sum_{\varepsilon\in\boldsymbol{\mu}(\mathbb{Q}_p)} \omega(\varepsilon)^i \int_{\varepsilon+2p\mathbb{Z}_p} \langle x\rangle^s \lambda(x) \\ &= \sum_{\varepsilon\in\boldsymbol{\mu}(\mathbb{Q}_p)} \omega(\varepsilon)^i \int_{1+2p\mathbb{Z}_p} \langle x\varepsilon\rangle^s \gamma_{\varepsilon^{-1}} \cdot \lambda(x),\end{aligned}$$

where $\gamma_\varepsilon \in \Gamma$ is such that $\chi(\gamma_\varepsilon) = \varepsilon$. We have a isomorphism

$$\begin{aligned}\alpha : 1 + 2p\mathbb{Z}_p &\simeq \mathbb{Z}_p \\ x &\mapsto y = \frac{\log(x)}{\log(u)}.\end{aligned}$$

Then

$$\int_{\mathbb{Z}_p} f(y)\alpha_*(\gamma_{\varepsilon^{-1}}\lambda) = \int_{1+2p\mathbb{Z}_p} f(\alpha(x))\gamma_{\varepsilon^{-1}}\lambda.$$

Now $\langle x\rangle^s = \exp(s\log x) = \exp(s\log uy) = u^{sy}$ and hence

$$\sum_{\varepsilon\in\boldsymbol{\mu}(\mathbb{Q}_p)} \omega(\varepsilon)^i \int_{1+2p\mathbb{Z}_p} \langle x\varepsilon\rangle^s \lambda(x) = \sum_{\varepsilon\in\boldsymbol{\mu}(\mathbb{Q}_p)} \omega(\varepsilon)^i \int_{\mathbb{Z}_p} u^{sy} \alpha_*(\gamma_{\varepsilon^{-1}} \cdot \lambda),$$

we just set $\Gamma_\lambda^{(i)} = \sum_{\varepsilon\in\boldsymbol{\mu}(\mathbb{Q}_p)} \omega(\varepsilon)^i \alpha_*(\gamma_{\varepsilon^{-1}} \cdot \lambda)$. □

Definition 1.5.10.

$$\zeta_{p,i}(s) = \frac{-1}{1-\omega(a)^{1-i}\langle a\rangle^{1-s}} \int_{\mathbb{Z}_p^*} \omega(x)^{-i} \langle x\rangle^{-s} \lambda_a(x).$$

Proof of Theorem 1.5.7. If $n \equiv -i \bmod p-1$, then

$$\begin{aligned}\zeta_{p,i}(-n) &= \frac{1}{1-\omega(a)^{1-i}\langle a\rangle^{1+n}} \int_{\mathbb{Z}_p^*} \omega(x)^{-i}\langle x\rangle^n \lambda_a(x) \\ &= \frac{1}{1-\omega(a)^{1+n}\langle a\rangle^{1+n}} \int_{\mathbb{Z}_p^*} \omega(x)^{n}\langle x\rangle^n \lambda_a(x) \\ &= (1-p^{-n})\zeta(-n).\end{aligned}$$

The function $\zeta_{p,i}$ is analytic if $\omega(a)^{1-i} \neq 1$, which can be achieved if $i \neq 1$. If $i = 1$, there is a pole at $s = 1$. □

Remark. (i) A theorem of Mazur and Wiles (originally the Main conjecture of Iwasawa theory) describes the zeros of $\zeta_{p,i}(s)$ in terms of ideal class groups of $\mathbb{Q}_p(\boldsymbol{\mu}_{p^n}), n \in \mathbb{N}$.

(ii) Main open question: For $i \equiv 1 \bmod 2$, can $\zeta_{p,i}(k) = 0$, if $k > 1$ and $k \in \mathbb{N}$?

The case $k = 1$ is known. In this case, $\zeta_{p,i}(1)$ is a linear combination with coefficients in $\bar{\mathbb{Q}}^\times$ of log of algebraic numbers, hence by transcendental number theory (Baker's theorem), $\zeta_{p,i}(1) \neq 0$.

1.6 $\mathcal{C}^k$ functions

1.6.1 Definition.

Let $f : \mathbb{Z}_p \to \mathbb{Q}_p$ be a given function. We define

$$\begin{aligned} f^{\{0\}}(x) &= f(x) \\ f^{\{i\}}(x, h_1, \cdots, h_i) & \\ &= \frac{1}{h_i}(f^{\{i-1\}}(x+h_i, h_1, \cdots, h_{i-1}) - f^{\{i-1\}}(x, h_1, \cdots, h_{i-1})) \\ &= \frac{1}{h_1 \cdots h_i}(\sum_{I \subset \{1, \cdots, i\}} (-1)^{i-|I|} f(x + \sum_{j \in I} h_j)) \end{aligned}$$

One notes that $f^{\{i\}}$ is the analogue of the usual derivation in $\mathcal{C}(\mathbb{R}, \mathbb{C})$. In fact, if $f : \mathbb{R} \to \mathbb{C}$ is in $\mathcal{C}^k$ and $i \leq k$, define $f^{\{i\}}$ by the above formula, then

$$f^{\{i\}}(x, h_1, \cdots, h_i) = \int_{[0,1]^i} f^{(i)}(x + t_1 h_1 + \cdots + t_i h_i) dt_1 \cdots dt_i,$$

hence $f^{\{i\}}$ is continuous and $f^{\{i\}}(x, 0, \cdots, 0) = f^{(i)}(x)$.

Definition 1.6.1. A function $f : \mathbb{Z}_p \to \mathbb{Q}_p$(or $\mathbb{C}_p$) is in $\mathcal{C}^k$ if $f^{\{i\}}$ can be extended as a continuous function on $\mathbb{Z}_p^{i+1}$ for all $i \leq k$.

Remark. If $f \in \mathcal{C}^0$ and $h_1, \cdots, h_i \neq 0$, then we have:

$$v_p(f^{\{i\}}(x, h_1, \cdots, h_i)) \geq v_{\mathcal{C}^0}(f) - \sum_{j=1}^{i} v_p(h_j).$$

Example 1.6.2. The definition of $\mathcal{C}^k$ here is different than the usual case. Here is an example. For all x in $\mathbb{Z}_p$, $x = \sum_{n=0}^{+\infty} p^n a_n(x)$ with $a_n(x) \in \{0, 1, \cdots, p-1\}$. Let $f(x) = \sum_{n=0}^{+\infty} p^{2n} a_n(x)$, then $v_p(f(x) - f(y)) = 2v_p(x-y)$. Hence $f'(x) = 0$ for all $x \in \mathbb{Z}_p$, thus f is in $\mathcal{C}^\infty$ in the usual sense. But f is not $\mathcal{C}^2$ in our case. In fact, let $(x, h_1, h_2) = (0, p^n, p^n)$ and $((p-1)p^n, p^n, p^n)$, here $p \neq 2$, we have:

$$f^{\{2\}}(0, p^n, p^n) = 0;$$
$$f^{\{2\}}((p-1)p^n, p^n, p^n) = p - p^2.$$

We define a valuation on $\mathcal{C}^k$ functions by:

$$v'_{\mathcal{C}^k}(f) = \min_{0 \leq i \leq k} \inf_{(x, h_1, \cdots, h_i) \in \mathbb{Z}_p^{i+1}} v_p(f^{\{i\}}(x, h_1, \cdots, h_i)).$$

Let $L(n,k) = \max\{\sum_{j=1}^{i} v_p(n_j), i \leq k,\ \sum n_j = n, n_j \geq 1\}$

Theorem 1.6.3 (Barsky). *$p^{L(n,k)}\binom{x}{n}$ is a Banach basis of $\mathcal{C}^k$.*

Exercise. there exists a C_k, such that for all $n \geq 1$,

$$k\frac{\log n}{\log p} - C_k \leq L(n,k) \leq k\frac{\log n}{\log p}.$$

Corollary 1.6.4. *The following three conditions are equivalent:*

(i) $\sum_{n=0}^{+\infty} a_n \binom{x}{n} \in \mathcal{C}^k$,

(ii) $\lim_{n \to +\infty} v_p(a_n) - k\frac{\log n}{\log p} = +\infty$,

(iii) $\lim_{n \to +\infty} n^k |a_n| = 0$.

Definition 1.6.5. If $r \geq 0$, $f : \mathbb{Z}_p \to \mathbb{Q}_p$ is in $\mathcal{C}^r$ if

$$f = \sum_{n=0}^{+\infty} a_n(f)\binom{x}{n}$$

and

$$n^r |a_n(f)| \to 0 \text{ when } n \to +\infty.$$

$\mathcal{C}^r$ becomes a Banach space with the valuation:

$$v_{\mathcal{C}^r}(f) = \inf_{n \in \mathbb{N}}\{v_p(a_n) - r\frac{\log(1+n)}{\log p}\}.$$

1.6.2 Mahler's coefficients of $\mathcal{C}^r$-functions.

We need Mähler's Theorem in several variables to prove Barsky's theorem.

Let $g(x_0, x_1, \cdots, x_i)$ be a function defined on $\mathbb{Z}_p^{i+1}$. We define the action $\alpha_j^{[k]}$ on g by the following formula:

$$\alpha_j^{[1]} g(x_0, \cdots, x_i) = g(x_0, \cdots, x_j + 1, \cdots, x_i) - g(x_0, \cdots, x_i),$$
$$\alpha_j^{[k]} = \alpha_j^{[1]} \circ \alpha_j^{[1]} \circ \cdots \circ \alpha_j^{[1]},\ k \text{ times }.$$

We set

$$a_{k_0, \cdots, k_i}(g) = \alpha_0^{[k_0]} \cdots \alpha_i^{[k_i]} g(0, \cdots, 0).$$

Recall that

$$\mathcal{C}^0(\mathbb{Z}_p^{i+1}, \mathbb{Q}_p) = \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p) \widehat{\bigotimes} \cdots \widehat{\bigotimes} \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p).$$

Theorem 1.6.6 (Mähler). *If g is continuous on $\mathbb{Z}_p^{i+1}$, then $a_{k_0, \cdots, k_i}(g) \to 0$ when $(k_0, \cdots, k_i) \to \infty$ and we have the following identity:*

$$g(x_0, \cdots, x_i) = \sum_{k_0, \cdots, k_i \in \mathbb{N}} a_{k_0, \cdots, k_i}(g) \binom{x_0}{k_0} \cdots \binom{x_i}{k_i} \tag{1.2}$$

Conversely, if $a_{k_0, \cdots, k_i} \to 0$, then the function g via equation (1.2) is continuous on $\mathbb{Z}_p^{i+1}$, $a_{k_0, \cdots, k_i}(g) = a_{k_0, \cdots, k_i}$, and

$$v_{\mathcal{C}^0}(g) = \inf v_p(a_{k_0, \cdots, k_i}).$$

Proof of Theorem 1.6.3. Let $g_T(x) = (1+T)^x$, then we have:

$$\begin{aligned} g_T^{\{i\}}(x, h_1, \cdots, h_i) &= \frac{1}{h_1 \cdots h_i} \Big(\sum_{I \subset \{1, \cdots, i\}} (-1)^{i-|I|} g_T(x + \sum_{j \in I} h_j) \Big) \\ &= (1+T)^x \prod_{j=1}^{i} \frac{(1+T)^{h_j} - 1}{h_j} \end{aligned}$$

Let $P_n = \binom{x}{n}$. Since $\frac{1}{x}\binom{x}{n} = \frac{1}{n}\binom{x-1}{n-1}$ and $g_T^{\{i\}}(x, h_1, \cdots, h_i) = \sum_{n=0}^{\infty} P_n^{\{i\}}(x, h_1, \cdots, h_i) T^n$, we have the following formulas:

$$P_n^{\{i\}}(x_0, h_1, \cdots, h_i) = \sum_{\substack{n_0 + n_1 + \cdots + n_i = n, \\ n_1, \cdots, n_i \geq 1}} \frac{1}{n_1 \cdots n_i} \binom{x_0}{n_0} \binom{h_1 - 1}{n_1 - 1} \cdots \binom{h_i - 1}{n_i - 1}.$$

Let

$$\begin{aligned} Q_{n,i}(x_0,\cdots,x_i) &= P_n^{\{i\}}(x_0,x_1+1,\cdots,x_i+1) \\ &= \sum_{\substack{n_0+n_1+\cdots+n_i=n,\\ n_1,\cdots,n_i\geq 1}} \frac{1}{n_1\cdots n_i}\binom{x_0}{n_0}\binom{x_1}{n_1-1}\cdots\binom{x_i}{n_i-1}. \end{aligned}$$

For all $f\in\mathcal{C}^0(\mathbb{Z}_p,\mathbb{Q}_p)$, we have $f(x)=\sum_{n=0}^{+\infty}a_n(f)\binom{x}{n}$. We denote

$$g_i(x_0,\cdots,x_i)=\sum_{n=0}^{+\infty}a_n(f)Q_{n,i}(x_0,\cdots,x_i)$$

if $x_j+1\neq 0, j\geq 1$. We have:

$$a_{n_0,n_1-1,\cdots,n_i-1}(g_i)=\sum_{n=0}^{+\infty}a_n(f)a_{n_0,n_1-1,\cdots,n_i-1}(Q_{n,i})$$

where

$$a_{n_0,n_1-1,\cdots,n_i-1}(Q_{n,i})=\begin{cases} 0 & \text{if } n\neq\sum_{j=0}^{i}n_j, \\ \frac{1}{n_1\cdots n_i} & \text{if } n=\sum_{j=0}^{i}n_j. \end{cases}$$

If f is in $\mathcal{C}^k$, $i\leq k$, then g_i is continuous on $\mathbb{Z}_p^{i+1}$, thus

$$\frac{a_{n_0+n_1+\cdots+n_i}(f)}{n_1\cdots n_i}\to 0.$$

Conversely, if $\dfrac{a_{n_0+n_1+\cdots+n_i}(f)}{n_1\cdots n_i}\to 0$, then

$$\sum_{n=0}^{+\infty}\sum_{n_0+n_1+\cdots+n_i=n}^{+\infty}\frac{a_{n_0,n_1,\cdots,n_i}(f)}{n_1\cdots n_i}\binom{x_0}{n_0}\binom{x_1}{n_1-1}\cdots\binom{x_i}{n_i-1}$$

defines a continuous functions G_i on $\mathbb{Z}_p^{i+1}$. But $G_i=g_i$ on $\mathbb{N}^{i+1}$, hence $G_i=g_i$, $x_j+1\neq 0$, for all $j\geq 1$,hence f is in $\mathcal{C}^k$. $\square$

1.7 locally analytic functions

1.7.1 Analytic functions on a closed disk.

Lemma 1.7.1. *Let $(a_n)_{n\in\mathbb{N}}$ with a_n in $\mathbb{C}_p$ be a sequence such that $v_p(a_n) \to \infty$ when $n \to \infty$, let $f = \sum_{n=0}^{+\infty} a_n T^n$. Then:*

(i) *If $x_0 \in \mathcal{O}_{\mathbb{C}_p}$, then $f^{(k)}(x_0)$ converges for all k and*

$$\lim_{n\to\infty} v_p(\frac{f^{(k)}}{k!}(x_0)) = \infty.$$

(ii) *If x_0, x_1 are in $\mathcal{O}_{\mathbb{C}_p}$, then*

$$f(x_1) = \sum_{n=0}^{+\infty} \frac{f^{(n)}(x_0)}{n!}(x_1 - x_0)^n$$

and

$$\inf_{n\in\mathbb{N}} v_p(\frac{f^{(n)}(x_0)}{n!}) = \inf_{n\in\mathbb{N}} v_p(a_n);$$

(iii) $\inf_{n\in\mathbb{N}} v_p(a_n) = \inf_{x\in\mathcal{O}_{\mathbb{C}_p}} v_p(f(x))$ *and* $v_p(f(x)) = \inf_n v_p(a_n)$ *almost everywhere (i.e.,outside a finite number of $x_i + \mathfrak{m}_{\mathbb{C}_p}$).*

Proof. (i) $\frac{f^{(k)}}{k!} = \sum_{n=0}^{+\infty} a_{n+k}\binom{n+k}{k}T^n$. Let $T = x_0$; since $v_p(\binom{n+k}{k}) \geq 0$, $v_p(x_0^n) \geq 0$, we get (1) and also

$$v_p(\frac{f^{(k)}(x_0)}{k!}) \geq \inf_{n\in\mathbb{N}} v_p(a_n) = \inf_{n\in\mathbb{N}} v_p(\frac{f^{(n)}(0)}{n!}).$$

(ii)

$$\begin{aligned} f(x_1) &= \sum_{n=0}^{+\infty} a_n x_1^n = \sum_{n=0}^{+\infty} a_n (\sum_{k=0}^{+\infty} \binom{n}{k} (x_1 - x_0)^k x_0^{n-k}) \\ &= \sum_{k=0}^{+\infty} (\sum_{n=0}^{+\infty} a_n \binom{n}{k} x_0^{n-k})(x_1 - x_0)^k = \sum_{n=0}^{+\infty} \frac{f^{(n)}(x_0)}{n!}(x_1 - x_0)^n. \end{aligned}$$

So we can exchange the the roles of 0 and x_0 to get

$$\inf_{n\in\mathbb{N}} v_p(\frac{f^{(n)}(x_0)}{n!}) = \inf_{n\in\mathbb{N}} v_p(a_n).$$

(iii) That $\inf_{n\in\mathbb{N}} v_p(a_n) \leq \inf_{x\in\mathcal{O}_{\mathbb{C}_p}} v_p(f(x))$ is clear. As $v_p(a_n)$ goes to $+\infty$, $v_p(a_n)$ reaches its infimum at some $n_0 \in \mathbb{N}$. So we can divide everything by a_{n_0} and we may assume that $\inf_{n\in\mathbb{N}} v_p(a_n) = 0$. Let $\overline{f}(T) = f(T) \bmod \mathfrak{m}_{\mathbb{C}_p} \in \mathbb{F}_p[T]$. If $x \in \mathcal{O}_{\mathbb{C}_p}$ doesn't reduce $\bmod\, \mathfrak{m}_{\mathbb{C}_p}$ to a root of $\overline{f}$, then $\overline{f}(x) \neq 0$, equivalently, $v_p(f(x)) = 0$. □

Corollary 1.7.2. *Let* $f = \sum_{n=0}^{+\infty} a_n T^n$, $g = \sum_{n=0}^{+\infty} b_n T^n$, *then* $fg = \sum_{n=0}^{+\infty} c_n T^n$, *where* $c_n = \sum_{i=0}^{n} a_i b_{n-i}$. *Suppose that* $v_p(a_n)$ *and* $v_p(b_n)$ *go to infinity when* n *goes to infinity, then* $v_p(c_n)$ *goes to infinity and* $\inf_n v_p(c_n) = \inf_n(a_n) + \inf_n(b_n)$.

Definition 1.7.3. For $x_0 \in \mathbb{C}_p$, $r \in \mathbb{R}$, we define

$$D(x_0, r) = \{x \in \mathbb{C}_p, v_p(x - x_0) \geq r\}.$$

Definition 1.7.4. A function $f : D(x_0, r) \to \mathbb{C}_p$ is analytic if it is sum of its Taylor expansion at x_0 or equivalently, if

$$\lim_{n\to+\infty} (v_p(\frac{f^{(n)}(x_0)}{n!}) + nr) = +\infty.$$

We define $v_{x_0}^{\{r\}}(f) = \inf_n (v_p(\frac{f^{(n)}(x_0)}{n!}) + nr)$.

Proposition 1.7.5. *If the function* $f : D(x_0, r) \to \mathbb{C}_p$ *is analytic, then*

(i) *For all* $k \in \mathbb{N}$, $f^{(k)}$ *is analytic on* $D(x_0, r)$,

$$v_{x_0}^{\{r\}}(\frac{f^{(k)}(x_0)}{k!}) + kr \geq v_{x_0}^{\{r\}}(f)$$

and goes to $+\infty$ *if* k *goes to* $+\infty$.

(ii) f *is the sum of its Taylor expansion at any* $x \in D(x_0, r)$.

(iii) $v_{x_0}^{\{r\}}(f) = \inf_{x\in D(x_0,r)} v_p(f(x))$.

(iv) $v_{x_0}^{\{r\}}(fg) = v_{x_0}^{\{r\}}(f) + v_{x_0}^{\{r\}}(g)$.

Proof. If $r \in \mathbb{Q}$, one can choose $\alpha \in \mathbb{C}_p$, such that $v_p(\alpha) = r$. Let $F(x) = f(x_0 + \alpha x), x \in \mathcal{O}_{\mathbb{C}_p}$. Apply the previous lemma, we can get the result.

If $r \notin \mathbb{Q}$, choose r_n decreasing with the limit r, $r_n \in \mathbb{Q}$. Use $D(x_0, r) = \cup_n D(x_0, r_n)$ and the case $r \in \mathbb{Q}$, we get the result. □

1.7.2 Locally analytic functions on $\mathbb{Z}_p$.

Definition 1.7.6. Let $h \in \mathbb{N}$ be given. The space $LA_h(\mathbb{Z}_p, \mathbb{Q}_p)$ is the space of f whose restriction to $x_0+p^h\mathbb{Z}_p$ is the restriction of an analytic function f_{x_0} on $D(x_0, h)$, for all $x_0 \in \mathbb{Z}_p$. The valuation of the space is $v_{LA_h} = \inf_{x_0 \in S} v_{x_0}^{\{h\}}(f_{x_0})$, S be any set of representations of $\mathbb{Z}_p/p^h\mathbb{Z}_p$. (Use above proposition to prove that this does not depend on S.)

Lemma 1.7.7. *LA_h is a Banach space. Moreover, let*

$$e_n = 1_{i+p^h\mathbb{Z}_p}(\frac{x+i}{p^h})^{m-1}, n = mp^h - i, m \geq 1, 1 \leq i \leq p^h,$$

then e_n's are a Banach basis of LA_h.

Theorem 1.7.8 (Amice). *The functions $[\frac{n}{p^h}]!\binom{x}{n}, n \in \mathbb{N}$ are a Banach basis of LA_h.*

Proof. The idea is to try to relate the $g_n = [\frac{n}{p^h}]!\binom{x}{n}$ to the e_n.

(i) First step: For $1 \leq j \leq p^h$, we denote

$$g_{n,j}(x) = g_n(-j + p^h x) = [\frac{n}{p^h}]!\frac{1}{n!}\prod_{k=0}^{n-1}(-j - k + p^h x).$$

If $v_p(j + k) < h$, then $v_p(-j - k + p^h x) = v_p(j + k)$, for all x in $\mathcal{O}_{\mathbb{C}_p}$. If $v_p(j + k) \geq h$, then $v_p(-j - k + p^h x) \geq h$ with equality if $\overline{x} \notin \mathbb{F}_p \subset \overline{\mathbb{F}_p}$. So, we get

$$v_0^{\{0\}}(g_{n,j}) = v_p([\frac{n}{p^h}]!) - v_p(n!) + \sum_{k=0}^{n-1}\inf(v_p(j+k), h) = \sum_{i=1}^{\infty}\#\{k : v_p(k) \geq i, 1 \leq k \leq n\}.$$

Since $v_p(n!) = \sum_{k=1}^{n} v_p(k) = \sum_{i=1}^{+\infty}[\frac{n}{p^i}]$, we have

$$v_p(n!) - v_p([\frac{n}{p^h}]!) = \sum_{i=1}^{h}\#\{k : v_p(k) \geq i, 1 \leq k \leq n\} = \sum_{k=1}^{n}\inf(v_p(k), h).$$

Thus,

$$\begin{aligned} v_0^{\{0\}}(g_{n,j}) &= \sum_{k=1}^{n}[\inf(v_p(j + k - 1), h) - \inf(v_p(k), h)] \\ &= \sum_{l=1}^{h}([\frac{n + j - 1}{p^l}] - [\frac{j - 1}{p^l}] - [\frac{n}{p^l}]). \end{aligned}$$

As $[x+y] \geq [x]+[y]$, we have $v_0^{\{0\}}(g_{n,j}) \geq 0$, for all $1 \leq j \leq p^h$. So, we have $v_{LA_h}(g_n) \geq 0$.

(ii) Second step: we need a lemma

Lemma 1.7.9. *Let* $n = mp^h - i$, $\overline{g_{n,j}} \in \mathbb{F}_p[x]$, *then:*

(i) $\overline{g_{n,j}} = 0$, *if* $j > i$,

(ii) $\deg \overline{g_{n,j}} = m-1$, *if* $j = i$,

(iii) $\deg \overline{g_{n,j}} \leq m-1$ *if* $j < i$.

The lemma implies the theorem: $\overline{g_n}$ can be written in terms of the $\overline{e_n}$, multiplying by an invertible upper triangular matrix. Now use the fact that x_n is a Banach basis if and only if $\overline{x_n}$ is a basis of LA_h^0/pLA_h^0 over $\mathbb{F}_p$. $\square$

Proof of Lemma 1.7.9. (i) If $j > i$, then $j-1 \geq i$. Since

$$[\frac{n+j-1}{p^h}] - [\frac{j-1}{p^h}] - [\frac{n}{p^h}] = m - (m-1) = 1,$$

we have $v_0^{\{0\}}(g_{n,j}) \geq 1$, then $\overline{g_{n,j}} = 0$.

(ii) and (iii):If $j \leq i$, write

$$g_{n,j}(x) = \sum_{k=0}^{n} a_k x^k, a_k \in \mathbb{Z}_p.$$

The zeros of $g_{n,j}$ are the $\frac{j+k}{p^h}, 0 \leq k \leq n-1$ and

$$\#\{\text{zeros in } \mathbb{Z}_p\} = \#\{k : v_p(j+k) \geq h\} = [\frac{n+j-1}{p^h}] - [\frac{j-1}{p^h}] = m-1.$$

Let $\{\alpha_i : 1 \leq i \leq m-1\}$ be the set of the roots with $\alpha_1, \cdots, \alpha_{m-1}$ in $\mathbb{Z}_p$ and $\alpha_m, \cdots, \alpha_n$ not in $\mathbb{Z}_p$. Then

$$g_{n,j} = c \prod_{l=1}^{m-1} (x - \alpha_l) \prod_{l=m}^{n} (1 - \alpha_l^{-1} x), (c \text{ is a constant }).$$

Since $v_p(\alpha_l^{-1}) > 0$ when $l \geq m$, then $v_p(a_{m-1}) = v_p(c) = v_0^{\{0\}}(g_{n,j})$. It implies $c \in \mathbb{Z}_p$. Hence

$$\overline{g_{n,j}} = \overline{c} \prod_{l=1}^{m-1} (x - \overline{\alpha}_l).$$

It remains to prove $v_0^{\{0\}}(g_{n,i}) = 0$. Since

$$v_0^{\{0\}}(g_{n,i}) = \sum_{l=1}^{h}([\frac{mp^h-1}{p^l}] - [\frac{i-1}{p^l}] + [\frac{mp^h-i}{p^l}])$$

and $-[\frac{-i}{a}] = [\frac{i-1}{a}] + 1$, we get the result. □

Let $LA = \{$locally analytic functions on $\mathbb{Z}_p\}$. Because $\mathbb{Z}_p$ is compact, $LA = \cup LA_h$ and is an inductive limit of Banach spaces. So

(i) A function $\varphi : LA \to B$ is continuous if and only if $\varphi|_{LA_h} : LA_h \to B$ is continuous for all h.

(ii) A sequence $f_n \to f$ converges in LA if and only if there exists h, such that for all n, $f_n \in LA_h$ and $f_n \to f$ in LA_h.

Since $\frac{1}{n}v_p([\frac{n}{p^h}]!) \sim \frac{1}{(p-1)p^h}$, we have the following theorem:

Theorem 1.7.10. *The function* $f = \sum_{n=0}^{+\infty} a_n \binom{x}{n}$ *is in* LA *if and only if there exists* $r > 0$*, such that* $v_p(a_n) - rn \to +\infty$ *when* $n \to +\infty$*.*

1.8 Distributions on $\mathbb{Z}_p$

1.8.1 The Amice transform of a distribution.

Definition 1.8.1. A distribution μ on $\mathbb{Z}_p$ with values in B is a continuous linear map $f \mapsto \int_{\mathbb{Z}_p} f\mu$ from LA to B. We denote the set of distributions from LA to B by $\mathcal{D}(\mathbb{Z}_p, B)$.

Remark. (i) $\mu|_{LA_h}$ is continuous for all $h \in \mathbb{N}$. Set

$$v_{LA_h}(\mu) = \inf_{f \in LA_h}(v_B(\int_{\mathbb{Z}_p} f\mu) - v_{LA_h}(f)).$$

Then v_{LA_h} is a valuation on $\mathcal{D}(\mathbb{Z}_p, B)$ for all h, and $\mathcal{D}(\mathbb{Z}_p, B)$ is complete for the Fréchet topology defined by $v_{LA_h}, h \in \mathbb{N}$ which means that μ_n goes to μ if and only if $v_{LA_h}(\mu_n - \mu) \to +\infty$ for all h.

(ii) $\mathcal{D}(\mathbb{Z}_p, B) = \mathcal{D}(\mathbb{Z}_p, \mathbb{Q}_p)\widehat{\bigotimes}B$. From now on, we will denote $\mathcal{D}(\mathbb{Z}_p, \mathbb{Q}_p)$ by $\mathcal{D}$.

Let $\mathcal{R}^+$ be the ring of analytic functions defined on $D(0,0^+) = \{x \in \mathbb{C}_p, v_p(x) > 0\}$. A function $f \in \mathcal{R}^+$ can be written as $f = \sum_{n=0}^{+\infty} a_n T^n$, $a_n \in \mathbb{Q}_p$ for all $n \in \mathbb{N}$.

Let $v_h = \frac{1}{(p-1)p^h} = v_p(\varepsilon - 1)$, where ε is a primitive p^{h+1} root of 1.

If $F(T) = \sum_{n=0}^{+\infty} b_n T^n \in \mathcal{R}^+$, we define $v^{(h)}(F)$ to be

$$v^{(h)}(F) = v_0^{\{v_h\}}(F) = \inf_{n\in\mathbb{N}} v_p(b_n) + nv_h.$$

Then, for $F, G \in \mathcal{R}^+$,

$$v^{(h)}(FG) = v^{(h)}(F) + v^{(h)}(G).$$

We put on $\mathcal{R}^+$ the Fréchet topology defined by the $v^{(h)}$, $h \in \mathbb{N}$.

Definition 1.8.2. The Amice transform of a distribution μ is the function:

$$A_\mu(T) = \sum_{n=0}^{+\infty} T^n \int_{\mathbb{Z}_p} \binom{x}{n} \mu = \int_{\mathbb{Z}_p} (1+T)^x \mu.$$

Note that the last identity in the above definition is only a formal identity here. However, we have

Lemma 1.8.3. *If $v_p(z) > 0$, then* $\int_{\mathbb{Z}_p} (1+z)^x \mu = A_\mu(z)$

Proof. Choose h such that $v_h < v_p(z)$. Then

$$v_p\left(\frac{z^n}{[\frac{n}{p^h}]!}\right) \to +\infty,$$

therefore $\sum_{n=0}^{+\infty} z^n \binom{x}{n}$ converges to $(1+z)^x$ in LA_h. $\square$

Theorem 1.8.4. *The map $\mu \mapsto A_\mu$ is an isomorphism of Fréchet spaces from $\mathcal{D}$ to $\mathcal{R}^+$. moreover,*

$$v^{(h)}(A_\mu) \geq v_{LA_h}(\mu) \geq v^{(h+1)}(A_\mu) - 1.$$

Proof. Let $A_\mu(T) = \sum_{n=0}^{+\infty} b_n T^n$. Since $b_n = \int_{\mathbb{Z}_p} \binom{x}{n}\mu$ and $v_p(n!) \le \frac{n}{p-1}$, then we have:

$$\begin{aligned} v_p(b_n) &= v_p(b_n) - v_{LA_h}(\binom{x}{n}) + v_{LA_h}(\binom{x}{n}) \\ &\ge v_{LA_h}(\mu) + v_{LA_h}(\binom{x}{n}) = v_{LA_h}(\mu) - v_p([\frac{n}{p^h}]!) \\ &\ge v_{LA_h}(\mu) - \frac{n}{(p-1)p^h} = v_{LA_h}(\mu) - nv_h. \end{aligned}$$

Hence $A_\mu \in \mathcal{R}^+$ and $v^{(h)}(A_\mu) \ge v_{LA_h}(\mu)$.

Conversely, for $F \in \mathcal{R}^+$, $F = \sum_{n=0}^{+\infty} b_n T^n$, then for all h,

$$v_p([\frac{n}{p^h}]!b_n) = v_p(b_n) + \frac{n}{(p-1)p^h} \to \infty.$$

So $f \mapsto \sum_{n=0}^{+\infty} b_n a_n(f)$ is a continuous map on LA_h. Denote the left hand side by $\int_{\mathbb{Z}_p} f\mu$, this defines a distribution $\mu \in \mathcal{D}$. Moreover,

$$\begin{aligned} v_{LA_h}(\mu) &= \inf_{n\in\mathbb{N}} v_p([\frac{n}{p^h}]!b_n) \ge \inf_{n\in\mathbb{N}} v_p([\frac{n}{p^{h+1}}]!b_n) \\ &\ge \inf_{n\in\mathbb{N}} (v_p(b_n) + \frac{n}{(p-1)p^{h+1}}) - 1 = v_{LA_h}^{(h+1)}(A_\mu) - 1. \end{aligned}$$

□

1.8.2 Examples of distributions.

(i) Measures are distributions and $\mathcal{D}_0 \subset \mathcal{D}$.

(ii) One can multiply a distribution $\mu \in \mathcal{D}$ by $g \in LA$, and one gets

- $A_{x\mu} = \partial A_\mu$, $\partial = (1+T)\frac{d}{dT}$;
- $A_{z^x\mu}(T) = A_\mu((1+T)z - 1)$;
- $A_{Res_{a+p^n\mathbb{Z}_p}\mu}(T) = p^{-n} \sum_{z^{p^n}=1} z^{-a} A_\mu((1+T)z-1)$

(iii) one gets actions φ, ψ, Γ with the same formulas than on measures.

(iv) Convolution of distributions: If $f \in LA_h$ and for all $y \in y_0 + p^h\mathbb{Z}_p$,

$$f(x+y) = \sum_{n=0}^{+\infty} \frac{p^{nh} f^{(n)}(x+y_0)}{n!} (\frac{y-y_0}{p^h})^n \in LA_h(x) \widehat{\bigotimes} LA_h(y),$$

and $v_{LA_h}(\frac{p^{nh} f^{(n)}(x+y_0)}{n!})$ goes to $+\infty$, when $n \to +\infty$. Hence

$$\int_{\mathbb{Z}_p} (\int_{\mathbb{Z}_p} f(x+y)\mu(x))\lambda(y) = \int_{\mathbb{Z}_p} f\, \lambda * \mu$$

is well defined, $A_{\lambda*\mu} = A_\lambda A_\mu$.

(v) The derived distribution: $\mu \mapsto d\mu$ given by $\int_{\mathbb{Z}_p} f d\mu = \int_{\mathbb{Z}_p} f'\mu$. Easy to check $A_{d\mu}(T) = \log(1+T)A_\mu(T)$. μ can't be integrated because $\log(1+T) = 0$ if $T = \varepsilon - 1, \varepsilon \in \boldsymbol{\mu}_{p^\infty}$.

(vi) Division by x, the Amice transform $A_{x^{-1}\mu}$ of $x^{-1}\mu$ is a primitive(or called antiderivative) of $(1+T)^{-1}A_\mu$, so $A_{x^{-1}\mu}$ is defined up to $\alpha\delta_0, \alpha \in \mathbb{Q}_p$ (we have $x\delta_0 = 0$).

1.8.3 Residue at $s = 1$ of the p-adic zeta function.

The Kubota-Leopoldt distribution μ_{KL} given by $A_{\mu_{KL}}(T) = \frac{\log(1+T)}{T}$. Then

$$\begin{aligned}\int_{\mathbb{Z}_p} x^n \mu_{KL} &= \left(\frac{d}{dt}\right)^n_{t=0} (\int_{\mathbb{Z}_p} e^{tx}\mu_{KL}) = \left(\frac{d}{dt}\right)^n_{t=0} A_{\mu_{KL}}(e^t - 1) \\ &= \left(\frac{d}{dt}\right)^n_{t=0} (\frac{t}{e^t-1}) = (-1)^n n\zeta(1-n), \text{ for all } n \in \mathbb{N}.\end{aligned}$$

Since

$$\psi(\frac{1}{T}) = \frac{1}{T} \text{ and } \varphi(\log(1+T)) = p\log(1+T),$$

we get $\psi(\mu_{KL}) = \frac{1}{p}\mu_{KL}$ and

$$\int_{\mathbb{Z}_p^*} x^n \mu_{KL} = (1-p^{n-1}) \int_{\mathbb{Z}_p} x^n \mu_{KL} = (-1)^n n(1-p^{n-1})\zeta(1-n);$$

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

The integral is analytic in s by the same argument as for measures.

Proposition 1.8.5. $\lim_{s\to 1}(s-1)\zeta_{p,1}(s) = \int_{\mathbb{Z}_p^*}\mu_{KL} = 1-\frac{1}{p}$, *(compare with* $\lim_{s\to 1}(s-1)\zeta(s) = 1$*).*

Proof. It follows from the following lemma. □

Lemma 1.8.6. $\int_{a+p^n\mathbb{Z}_p}\mu_{KL} = p^{-n}$, *for all* n, *for all* $a \in \mathbb{Z}_p$ *(almost a Haar measure but* $\mu * \delta_a \neq \mu$*).*

Proof.

$$\int_{a+p^n\mathbb{Z}_p}\mu_{KL} = p^{-n}\sum_{z^{p^n}=1} z^{-a}A_{\mu_{KL}}(z-1) = p^{-n}(1+\sum_{z^{p^n}=1, z\neq 1}\frac{\log z}{z-1}),$$

and $\frac{\log z}{z-1} = 0$, if $z^{p^n}=1, z\neq 1$. □

1.9 Tempered distributions

1.9.1 Analytic functions inside $\mathcal{C}^r$ functions

Theorem 1.9.1. *For all* $r \geq 0$, $LA \subset \mathcal{C}^r$. *Moreover there exists a constant* $C(r)$ *depending on* r, *such that for all* $h \in \mathbb{N}$ *and for all* f *in* LA_h,

$$v_{\mathcal{C}^r}(f) \geq v_{LA_h}(f) - rh - C(r).$$

Proof. Since $v_{LA_h}(f) = \inf_n(v_p(a_n(f)) - v_p([\frac{n}{p^h}]!))$, we have

$$v_{\mathcal{C}^r}(f) = \inf_n(v_p(a_n(f)) - r\frac{\log(1+n)}{\log p}) \geq v_{LA_h}(f) + \inf_n(v_p([\frac{n}{p^h}]!) - r\frac{\log(1+n)}{\log p}).$$

We have a formula for every a:

$$v_p(a!) = [\frac{a}{p}] + \cdots + [\frac{a}{p^h}] + \cdots \geq \frac{a}{p-1} - \frac{\log(1+a)}{\log p}.$$

Write $n = p^h a + b$, $0 \leq b \leq p^h - 1$, then we have

$$\begin{aligned} v_{\mathcal{C}^r}(f) - v_{LA_h}(f) &\geq \inf_n(v_p([\frac{n}{p^h}]!) - r\frac{\log(1+n)}{\log p}) \\ &= \inf_{\substack{a\in\mathbb{N} \\ 0\leq b\leq p^h-1}}(v_p(a!) - r\frac{\log(ap^h+b+1)}{\log p}) \\ &\geq \frac{a}{p-1} - (r+1)\frac{\log(a+1)}{\log p} - rh. \end{aligned}$$

The function $-\frac{a}{p-1}+(r+1)\frac{\log(a+1)}{\log p}$ of a is bounded above, we just let $C(r)$ be its maximum. $\square$

Observe that the function log is well defined on $\mathbb{Z}_p^*$. First if $v_p(x-1)>0$, let

$$\log x=\sum_{n=1}^{+\infty}\frac{(-1)^{n+1}}{n}(x-1)^n;$$

in general, if $x=\omega(x)\langle x\rangle$, let $\log x=\log\langle x\rangle$. If $x=p$, let $\log p=0$. By the formula $\log xy=\log x+\log y$, log is well defined in $\mathbb{Q}_p-\{0\}$. This *log* is the so-called Iwasawa's log, or $\log_0$.

However, we can define the value at p arbitrarily. For $\mathcal{L}\in\mathbb{Q}_p$, define $\log_{\mathcal{L}} p=\mathcal{L}$, then $\log_{\mathcal{L}} x=\log_0 x+\mathcal{L}v_p(x)$.

Theorem 1.9.2. *Choose a $\mathcal{L}$ in $\mathbb{C}_p$. Then there exists a unique $\log_{\mathcal{L}}:\mathbb{C}_p^*\mapsto\mathbb{C}_p$ satisfying:*

(i) $\log_{\mathcal{L}} x=\sum_{n=1}^{+\infty}\frac{(-1)^{n-1}}{n}(x-1)^n$, *here $v_p(x-1)>0$,*
(ii) $\log_{\mathcal{L}} xy=\log_{\mathcal{L}} x+\log_{\mathcal{L}} y$,
(iii) $\log_{\mathcal{L}}=\mathcal{L}$.

Proposition 1.9.3. *If $r\geq 0$, $j>r$, then $x^j\log_{\mathcal{L}} x\in\mathcal{C}^r$.*

Proof. We have

$$x^j\log_{\mathcal{L}} x=\sum_{n=0}^{+\infty}\sum_{a=1}^{p-1}1_{p^na+p^{n+1}\mathbb{Z}_p}x^j\log_{\mathcal{L}} x.$$

Let $f_{n,a}=1_{p^na+p^{n+1}\mathbb{Z}_p}x^j\log_{\mathcal{L}} x$. We have to prove the sum converges in $\mathcal{C}^r$. On $p^na+p^{n+1}\mathbb{Z}_p$, we have

$$\begin{aligned}x^j\log_{\mathcal{L}} x &= (x-p^na+p^na)^j\log_{\mathcal{L}}(p^na+(x-p^na))\\ &= p^{nj}(a+p\frac{x-p^na}{p^{n+1}})^j(\log_{\mathcal{L}} p^na+\log_0(1+p\frac{x-p^na}{p^{n+1}a})).\end{aligned}$$

So $f_{n,a}\in LA_{n+1}$, $v_{LA_{n+1}}(f_{n,a})\geq nj$. Use the previous theorem, we get $v_{\mathcal{C}^r}(f_{n,a})\geq nj-r(n+1)-C(r)$ and it goes to $+\infty$. $\square$

1.9.2 Distributions of order r

Definition 1.9.4. Let $r \geq 0$ and B be a Banach space. A distribution $\mu \in \mathcal{D}(\mathbb{Z}_p, B)$ is a distribution of order r if $f \mapsto \int_{\mathbb{Z}_p} f\mu$ is a continuous map from $\mathcal{C}^r(\mathbb{Z}_p, \mathbb{Q}_p)$ to B. We denote the set of distributions of order r by $\mathcal{D}_r(\mathbb{Z}_p, B)$. We define a valuation on $\mathcal{D}_r(\mathbb{Z}_p, B)$ by

$$v'_{\mathcal{D}_r}(\mu) = \inf_{f \in \mathcal{C}^r}(v_p(\int_{\mathbb{Z}_p} f\mu) - v_{\mathcal{C}^r}(f)).$$

Remark. (i) Under the above valuation, $\mathcal{D}_r(\mathbb{Z}_p, B)$ is a p-adic Banach space and $\mathcal{D}_r(\mathbb{Z}_p, B) = \mathcal{D}_r(\mathbb{Z}_p, \mathbb{Q}_p)\widehat{\bigotimes} B$. We denote $\mathcal{D}_r(\mathbb{Z}_p, \mathbb{Q}_p)$ by $\mathcal{D}_r$.

(ii) $\mathcal{D}_{temp} = \cup \mathcal{D}_r$=set of tempered distributions.

(iii) Since $LA_h \subset \mathcal{C}^r$, and for $f \in LA_h$, $v_{\mathcal{C}^r}(f) \geq v_{LA_h}(f) - rh - C(r)$, we get, for $\mu \in \mathcal{D}_r \subset LA_h^*$,

$$v_{LA_h^*}(\mu) = \inf_{f \in LA_h}(v_p(\int_{\mathbb{Z}_p} f\mu) - v_{LA_h}(f)) \geq v'_{\mathcal{D}_r}(\mu) - rh - C(r).$$

Theorem 1.9.5. *$\mu \in \mathcal{D}$, the following are equivalent:* (i) *$\mu \in \mathcal{D}_r$ i.e. μ can be extended by continuity to $\mathcal{C}^r$.*

(ii) *There exists a constant C, such that $v_p(\int_{\mathbb{Z}_p} \binom{x}{n}\mu) \geq C - r\frac{\log(1+n)}{\log p}$, for all n.*

(iii) *There exists a constant C, such that $v_p(\int_{a+p^h\mathbb{Z}_p}(x-a)^j\mu) \geq C + h(j - r)$, for all $a \in \mathbb{Z}_p, j \in \mathbb{N}, h \in \mathbb{N}$.*

(iv) *There exists a constant C, such that $v_{LA_h}(\mu) \geq C - rh$, for all $h \in \mathbb{N}$.*

Remark. It follows that

$$v_{\mathcal{D}_r}(\mu) = \inf_{\substack{a \in \mathbb{Z}_p \\ j \in \mathbb{N}, n \in \mathbb{N}}}(v_p(\int_{a+p^h\mathbb{Z}_p}(x-a)^j\mu) - h(j-r))$$

is equivalent to $v'_{\mathcal{D}_r}$.

Proof. $(i) \Leftrightarrow (ii)$ is just the definition of $v'_{\mathcal{D}_r}$. $(iii) \Leftrightarrow (iv)$ is true by the definition of LA_h (with some C). Remains to prove $(ii) \Leftrightarrow (iv)$. We have $v^{(h)}(A_\mu) \geq v_{LA_h}(\mu) \geq v^{(h+1)}(A_\mu) - 1$, hence the proof is reduce to the following lemma with $F = A_\mu$. $\square$

Lemma 1.9.6. *Suppose $F \in \mathcal{R}^+$, $F = \sum_{n=0}^{+\infty} b_n T^n$, the following are equivalent:*
(i) *there exists C, such that $v^{(h)}(F) \geq C - rh$, for all $h \in \mathbb{N}$,*
(ii) *there exists C', such that $v_p(b_n) \geq C' - r\frac{\log(1+n)}{\log p}$ for all n.*

Proof. Let

$$C_0 = \inf_{h\in\mathbb{N}}(v^{(h)}(F) + rh) = \inf_{h\in\mathbb{N}}(\inf_{n\in\mathbb{N}}(v_p(b_n) + \frac{n}{(p-1)p^h}) + rh),$$

$$C_1 = \inf_{n\in\mathbb{N}}(v_p(b_n) + r\frac{\log(1+n)}{\log p}).$$

Let $h = [\frac{\log(1+n)}{\log p}]$, then

$$v_p(b_n) \geq C_0 - rh - \frac{n}{(p-1)p^h} \geq C_0 - r\frac{\log(1+n)}{\log p} - 2,$$

which implies $C_1 \geq C_0 - 2$.

Now, if h is fixed, then $C_1 - r\frac{\log(1+n)}{\log p} + \frac{n}{(p-1)p^h}$ is minimal for $(1+n) = (p-1)p^h r$. Hence,

$$C_1 - r\frac{\log(1+n)}{\log p} + \frac{n}{(p-1)p^h} \geq C_1 - rh - \frac{\log(p-1)r}{\log p}.$$

Thus, $C_0 \geq C_1 - r\frac{\log(p-1)r}{\log p}$. ☐

For $N \geq 0$, let $LP^{[0,N]}$ be the set of the locally polynomial functions of degree no more than N on $\mathbb{Z}_p$.

Theorem 1.9.7. *Suppose $r \geq 0$, $N > r-1$. If $f \mapsto \int_{\mathbb{Z}_p} f\mu$ is linear function from $LP^{[0,N]}$ to a Banach space B , such that there exists C,*

$$v_p(\int_{a+p^n\mathbb{Z}_p}(x-a)^j\mu) \geq C + (j-r)n$$

for all $a \in \mathbb{Z}_p$ and $n, j \in \mathbb{N}$, then μ extends uniquely to an element of $\mathcal{D}_r$.

Remark. (i) Let $r = 0, N = 0$, we recover the construction of measures as bounded additive functions on open compact sets.

(ii) We define a new valuation on $\mathcal{D}_r$

$$v_{\mathcal{D}_{r,N}}(\mu) = \inf_{a\in\mathbb{Z}_p n\in\mathbb{N}, j\in\mathbb{N}} v_p(\int_{a+p^n\mathbb{Z}_p}(x-a)^j\mu) - n(j-r),$$

then $v_p(\int_{\mathbb{Z}_p} f\mu) \geq v_{LA_h}(f) + v_{\mathcal{D}_{r,N}}(\mu) - rn$ for all $f \in LP^{[0,N]} \cap LA_h$;

(iii) The open mapping theorem in Banach spaces implies that $v_{\mathcal{D}_{r,N}}$ is equivalent to $v_{\mathcal{D}_r}$.

Proposition 1.9.8. *If $f \in LA$, $r \geq 0$, $N > r-1$, put*

$$f_n = \sum_{i=0}^{p^n-1} 1_{i+p^n\mathbb{Z}_p}(\sum_{k=0}^{N} \frac{f^{(k)}(i)}{k!}(x-i)^k) \in LP^{[0,N]},$$

then $f_n \to f$ in $\mathcal{C}^r$. Hence $LP^{[0,N]}$ is dense in $\mathcal{C}^r$.

Proof. There exists h, such that $f \in LA_h$. We assume $n \geq h$, then

$$v_{LA_h}(f - f_n) = \inf_{0\leq i\leq p^n-1} \inf_{k\geq N+1} v_p(p^{nk}\frac{f^{(k)}(i)}{k!}).$$

$f \in LA_h$ implies $v_p(\frac{p^{hk}f^{(h)}(i)}{h!}) \geq v_{LA_h}(f)$. Hence

$$v_{LA_h}(f - f_n) \geq v_{LA_h}(f) + (N+1)(n-h).$$

Then

$$\begin{aligned} v_{\mathcal{C}^r}(f - f_n) &\geq v_{LA_h}(f - f_n) - rn - C(r) \\ &\geq v_{LA_h}(f) - C(r) - (N+1)h + (N+1-r)n \to +\infty, \end{aligned}$$

because $N + 1 - r > 0$. $\square$

Proof of Theorem 1.9.7. The proposition implies the uniqueness in the theorem. We only need to prove the existence.

We show that if $f \in LA_h$, then $\lim_{n\to\infty} \int_{\mathbb{Z}_p} f_n\mu$ exists:

$$\begin{aligned} v_p(\int_{\mathbb{Z}_p}(f_{n+1} - f_n)\mu) &\geq v_{LA_{n+1}}(f_n - f_{n+1}) + v_{\mathcal{D}_{r,N}}(\mu) - r(n+1) \\ &\geq \inf(v_{LA_{n+1}}(f - f_n), v_{LA_{n+1}}(f - f_{n+1})) + v_{\mathcal{D}_{r,N}}(\mu) - r(n+1) \\ &\geq v_{\mathcal{D}_{r,N}}(\mu) + v_{LA_h}(f) - r(h-1) + (n-h)(N+1-r) \to +\infty. \end{aligned}$$

Set $\int_{\mathbb{Z}_p} f\mu = \lim_{n\to+\infty} \int_{\mathbb{Z}_p} f_n\mu$, then

$$\begin{aligned} v_p(\int_{\mathbb{Z}_p} f\mu) &\geq \inf(v_p(\int_{\mathbb{Z}_p} f_n\mu), v_p(\inf_{n\geq h} \int_{\mathbb{Z}_p} (f_{n-1} - f_n)\mu)) \\ &\geq v_{LA_h}(f) - rh + (v_{\mathcal{D}_{r,N}}(\mu) - r). \end{aligned}$$

This implies that $\mu \in \mathcal{D}_r$.

1.10 Summary

To summarize what we established:

(i) We have the inclusions:

$$\mathcal{C}^0 \supset \mathcal{C}^r \supset LA \supset LA_h$$

$$\mathcal{D}_0 \subset \mathcal{D}_r \subset \mathcal{D} \subset LA_h^*.$$

Now, if f is a function on $\mathbb{Z}_p$ and μ is a linear form on polynomials, then we have:

$$f \mapsto a_n(f) = \sum_{i=0}^{n} (-1)^i \binom{n}{i} f(n-i)$$

$$\mu \mapsto b_n(\mu) = \int_{\mathbb{Z}_p} \binom{x}{n} \mu$$

(ii) For f a function,

- $f \in \mathcal{C}^0$ if only if $v_p(a_n(f)) \to +\infty$ and

$$v_{\mathcal{C}^0}(f) = \inf_{x\in\mathbb{Z}_p} v_p(f(x)) = \inf_n v_p(a_n(f)).$$

- $f \in \mathcal{C}^r$ if only if $v_p(a_n(f)) - r\frac{\log(1+n)}{\log p} \to +\infty$ and

$$v_{\mathcal{C}^r}(f) = \inf_n v_p(a_n(f) - r\frac{\log(1+n)}{\log p}).$$

- $f \in LA$ if only if there exists $r > 0$ such that $v_p(a_n(f)) - rn \to +\infty$. LA is not a Banach space; it is a compact inductive limit of Banach spaces.

- $f \in LA_h$ if and only if $v_p(a_n(f)) - v_p([\frac{n}{p^h}]!) \to +\infty$ and

$$v_{LA_h}(f) = \inf_{x\in\mathbb{Z}_p} \inf_{k\in\mathbb{N}} v_p(\frac{p^{kh} f^{(k)}(x)}{h!}) = \inf_n (v_p(a_n(f)) - v_p([\frac{n}{p^h}]!)).$$

(iii) For μ a distribution,

- $\mu \in \mathcal{D}_0$ if and only if $v_{\mathcal{D}_0}(\mu) = \inf_n v_p(b_n(\mu)) > -\infty$.
- $\mu \in \mathcal{D}_r$ if and only if $v'_{\mathcal{D}_r}(\mu) = \inf_n v_p(b_n(\mu)) + r\frac{\log(1+n)}{\log p} > -\infty$.
- $\mu \in \mathcal{D}$ if and only if for all $r > 0$, $\inf_n v_p(b_n(\mu)) + rn > -\infty$.

(iv) $f = \sum_{n=0}^{+\infty} a_n(f)\binom{x}{n}$ and $\int_{\mathbb{Z}_p} f\mu = \sum_{n=0}^{+\infty} a_n(f)b_n(\mu)$.

Chapter 2

Modular forms

2.1 Generalities

2.1.1 The upper half-plane

By SL_2 we mean the group of 2×2 matrices with determinant 1. We write $SL_2(A)$ for those elements of SL_2 with entries in a ring A. In practice, the ring A will be $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$.
Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $SL_2(\mathbb{R})$, z in $\mathbb{C} - \{-\frac{d}{c}\}$, let $\gamma z = \frac{az+b}{cz+d}$, then

$$\mathrm{Im}(\gamma z) = \frac{(ad-bc)}{|cz+d|^2}\mathrm{Im}(z) = \frac{\mathrm{Im} z}{|cz+d|^2}.$$

We denote $\mathcal{H} = \{z, \mathrm{Im} z > 0\}$ the upper half plane. It is stable under $z \mapsto \gamma z$ and one can verify $(\gamma_1\gamma_2)z = \gamma_1(\gamma_2 z)$.

Proposition 2.1.1. *The transform action $z \mapsto \gamma z$ defines a group action of $SL_2(\mathbb{R})$ on $\mathcal{H}$.*

Proposition 2.1.2. *$\frac{dx \wedge dy}{y^2}$ is invariant under $SL_2(\mathbb{R})$.*

(hint : $dx \wedge dy = \frac{i}{2} dz \wedge d\bar{z}$ and $z \mapsto \gamma z$ is holomorphic.)

Definition 2.1.3. Let $f : \mathcal{H} \mapsto \mathbb{C}$ be a meromorphic function and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ be in $SL_2(\mathbb{R})$. If k in $\mathbb{Z}$, we define the weight k action of $SL_2(\mathbb{R})$ by $(f|_k\gamma)(z) = (cz+d)^{-k} f(\gamma z)$.

Exercise. $(f|_k\gamma_1)|_k\gamma_2 = f|_k\gamma_1\gamma_2$.

2.1.2 Definition of modular forms

Definition 2.1.4. Let Γ be a subgroup of $SL_2(\mathbb{Z})$ of finite index, χ is a finite order character of Γ (i.e. $\chi(\Gamma) \subset \mu_N$). $f : \mathcal{H} \mapsto \mathbb{C}$ is a modular form of weight k, character χ for Γ, if:

(i) f is holomorphic on $\mathcal{H}$;

(ii) $f|_k\gamma = \chi(\gamma)f$, if $\gamma \in \Gamma$;

(iii) f is slowly increasing at infinity, i.e. for all $\gamma \in \Gamma\backslash SL_2(\mathbb{Z})$, there exists $C(\gamma)$ and $r(\gamma)$ such that $\mid f|_k\gamma(z) \mid \leq y^{r(\gamma)}$, if $y \geq C(\gamma)$.

Definition 2.1.5. Γ is a congruence subgroup if $\Gamma \supset \Gamma(N) = \mathrm{Ker}\,(SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z}))$ for some N in $\mathbb{N}$.

Example 2.1.6.

$$\Gamma_0(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \bmod N\} \supset \Gamma(N).$$

Any character $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ extends to a congruence character

$$\chi : \Gamma_0(N) \to \mathbb{C}^* \quad \chi(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) \to \chi(d).$$

Let $M_k(\Gamma, \chi)$ be the set of modular forms of weight k, character χ for Γ. Then $M_k(\Gamma, \chi)$ is a $\mathbb{C}$-vector space.

Remark. (i) If $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) = -I \in \Gamma$ and $\chi(-I) \neq (-1)^k$, then $M_k(\Gamma, \chi) = 0$;

(ii) $f \in M_k(\Gamma, \chi)$, $g \in SL_2(\mathbb{Z})$, $f|_k g \in M_k(g^{-1}\Gamma g, \chi_g)$ where $\chi_g(\gamma) = \chi(g\gamma g^{-1})$.

2.1.3 q-expansion of modular forms.

Lemma 2.1.7. *If Γ is a subgroup of finite index of $SL_2(\mathbb{Z})$ and $\chi : \Gamma \mapsto \mathbb{C}^*$ is of finite order, then there exists M in $\mathbb{N} - \{0\}$, such that $\left(\begin{smallmatrix} 1 & M \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$ and $\chi(\left(\begin{smallmatrix} 1 & M \\ 0 & 1 \end{smallmatrix}\right)) = 1$.*

Proof. We can replace Γ by $\mathrm{Ker}\,\chi$ and assume $\chi = 1$. There exists $n_1 \neq n_2$, such that $\left(\begin{smallmatrix} 1 & n_1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & n_2 \\ 0 & 1 \end{smallmatrix}\right)$ have the same image in $\Gamma\backslash SL_2(\mathbb{Z})$, then $M = \mid n_1 - n_2 \mid$ satisfy the condition. □

For $M \in \mathbb{N} - \{0\}$, let $q_M(z) = e^{\frac{2\pi i z}{M}}$. Then $z \mapsto q_M(z)$ gives a holomorphic bijection $M\mathbb{Z}\backslash\mathcal{H} \simeq \mathcal{D}^* = \{0 <\mid q_M \mid < 1\}$.

Corollary 2.1.8. *If $f \in M_k(\Gamma, \chi)$, then there exists $M \neq 0$, $M \in \mathbb{N}$, such that $f(z+M) = f(z)$. Thus there exists $\tilde{f}$ holomorphic on $\mathcal{D}^*$, such that $f(z) = \tilde{f}(q_M)$.*

Now $\tilde{f}$ has a Laurent expansion $\tilde{f}(q_M) = \sum_{n\in\mathbb{Z}} a_n q_M^n$ with

$$a_n = e^{\frac{2\pi n y}{M}} \cdot \frac{1}{M} \int_{-\frac{M}{2}}^{\frac{M}{2}} f(x+iy) e^{\frac{-2\pi i n x}{M}} dx$$

for all y. If $n < 0$, when $y \to \infty$, the right hand side goes to 0, so $a_n = 0$. Hence we get the following result.

Proposition 2.1.9. *If f is in $M_k(\Gamma, \chi)$, there exists $M \in \mathbb{N} - \{0\}$, and elements $a_n(f)$ for each $n \in \frac{1}{M}\mathbb{N}$, such that*

$$f = \sum_{n \in \frac{1}{M}\mathbb{N}} a_n(f) q^n, \text{ where } q(z) = e^{2\pi i z},$$

which is called the q expansion of modular forms.

2.1.4 Cusp forms.

Definition 2.1.10. (i) $v_\infty(f) = \inf\{n \in \mathbb{Q}, a_n(f) \neq 0\} \geq 0$ and we say that f has a zero of order $v_\infty(f)$ at ∞. We say that f has a zero at ∞ if $v_\infty(f) > 0$.

(ii) A modular form f is a cusp form if $f|_k\gamma$ has a zero at ∞ for all γ in $\Gamma\backslash SL_2(\mathbb{Z})$. We denote S_k the set of cusp form of weight k. $S_k(\Gamma, \chi) \subset M_k(\Gamma, \chi)$.

Remark. If f is a cusp form, then f is rapidly decreasing at ∞ since

$$\mid (f|_k\gamma)(z) \mid = O\left(e^{-v_\infty(f|_k\gamma)2\pi y}\right).$$

Theorem 2.1.11. *$S_k(\Gamma, \chi)$ and $M_k(\Gamma, \chi)$ are finite dimensional $\mathbb{C}$-vector spaces with explicit formulas for the dimensions(if $k \geq 2$).*

Remark. $\oplus_{k,\chi} M_k(\Gamma, \chi) = M(\Gamma)$ is an algebra.

The study of $M_k(\Gamma, \chi)$ for congruence subgroup and congruence characters (Ker χ congruence subgroup) can be reduced to the study of $M_k(\Gamma_0(N), \chi)$ for a simple group theoretic reason. From now on, we write

$$M_k(N, \chi) = M_k(\Gamma_0(N), \chi), \quad S_k(N, \chi) = S_k(\Gamma_0(N), \chi).$$

2.2 The case $\Gamma = \mathrm{SL}_2(\mathbb{Z})$

2.2.1 The generators S and T of $\mathrm{SL}_2(\mathbb{Z})$.

Let $\mathrm{M}_k(1) = \mathrm{M}_k(\mathrm{SL}_2(\mathbb{Z}), 1)$, $\mathrm{S}_k(1) = \mathrm{S}_k(\mathrm{SL}_2(\mathbb{Z}), 1)$. Let

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

It is easy to verify

$$T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \text{ for any } n \in \mathbb{Z}.$$

So $Sz = -\frac{1}{z}$, $T^n z = z + n$.

Proposition 2.2.1. (i) *If $(a, b) = 1$, then there exists $n = n(a, b)$, $(a_0, b_0) = (1, 0)$, $(a_1, b_1) = (0, 1), \cdots (a_n, b_n) = (a, b)$, such that*

$$\begin{pmatrix} a_l & a_{l+1} \\ b_l & b_{l+1} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \quad \textit{for any } l.$$

(ii) $\mathrm{SL}_2(\mathbb{Z}) = \langle S, T \rangle$.

Proof. (i) We prove it by induction on $|a| + |b|$.

If $|a| + |b| = 1$, one can do it by hand:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad S^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad S^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

If $|a| + |b| \geq 2$, there exists $\mu, \nu \in \mathbb{Z}$, such that $b\mu - a\nu = 1$, and $|\nu| < |b|$, which implies $|\mu| \leq |a|$. Then we have $\left(\begin{smallmatrix} \mu & a \\ \nu & b \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $|\mu| + |\nu| < |a| + |b|$. Therefore the conclusion is obtained by the inductive assumption.

(ii) Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, there exists $n = n(a, b)$, $(a_0, b_0) = (1, 0)$, $(a_1, b_1) = (0, 1), \cdots (a_n, b_n) = (a, b)$, such that

$$\gamma_l = \begin{pmatrix} a_l & a_{l+1} \\ b_l & b_{l+1} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \text{ for any } l.$$

As $\gamma_1 = \mathrm{I}$ and

$$\gamma_{l+1}^{-1} \gamma_l = \begin{pmatrix} n_l & 1 \\ -1 & 0 \end{pmatrix} = T^{-n_l} S^3,$$

then $\gamma = \prod (\gamma_{l+1}^{-1} \gamma_l)^{-1} \in \langle T, S \rangle$. $\square$

Corollary 2.2.2. *Let* $f = \sum_{n=0}^{+\infty} a_n q^n$*, where* $q = e^{2\pi i z}$*, then* $f \in \mathrm{M}_k(1)$ *if and only if the following two conditions hold:*

(i) $\sum_{n=0}^{+\infty} a_n q^n$ *converges if* $|q| < 1$.

(ii) $f(-\frac{1}{z}) = z^k f(z)$.

2.2.2 Eisenstein series

Proposition 2.2.3. *If* $k \geq 3$*, then* $G_k \in M_k(1)$*, where*

$$G_k(z) = \frac{1}{2}\frac{\Gamma(k)}{(-2\pi i)^k}\sum_{m,n}{}' \frac{1}{(mz+n)^k} \in \mathrm{M}_k(1),$$

and $\sum'$ *means the summation runs over all pairs of integers* (m,n) *distinct from* $(0,0)$.

Proof. As $|mz+n| \geq \min(y, y/|z|)\sup(|m|,|n|)$, the series converges uniformly on compact subsets of $\mathcal{H}$ and is bounded at ∞.

Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, since

$$(cz+d)^{-k}\sum_{m,n}{}' \frac{1}{(m\frac{az+b}{cz+d}+n)^k} = \sum_{m,n}{}' \frac{1}{((am+cn)z+(bm+dn))^k},$$

and

$$(m,n) \mapsto (am+cn, bm+dn)$$

is a bijection of $\mathbb{Z}^2 - \{(0,0)\}$, it follows that $G_k|_k\gamma = G_k$. □

Proposition 2.2.4.

$$G_k(z) = \frac{\Gamma(k)}{(-2\pi i)^k}\zeta(k) + \sum_{n=1}^{+\infty}\sigma_{k-1}(n)q^n,$$

where $\sigma_s(n) = \sum_{d|n,\ d\geq 1} d^s$*, and* k *is even (if* k *is odd,* $\mathrm{M}_k(1) = 0$*, since* $-\mathrm{I} \in \mathrm{SL}_2(\mathbb{Z})$*).*

Proof.

$$G_k(z) = \frac{\Gamma(k)}{(-2\pi i)^k}\zeta(k) + \frac{\Gamma(k)}{(-2\pi i)^k}\sum_{m=1}^{+\infty} A_k(mz),$$

where

$$A_k(z) = \sum_{n\in\mathbb{Z}} \frac{1}{(z+n)^k} = \sum_{l\in\mathbb{Z}} \hat{\phi}(l) q^l$$

for the last identity given by the Poisson summation formula of Fourier transforms, and (by residue computation)

$$\hat{\phi}(l) = \int_{-\infty}^{+\infty} \frac{e^{-2\pi i l x}}{(x+iy)^k} \mathrm{d}x = \begin{cases} 0, & \text{if } l \le 0, \\ \frac{(-2\pi i)^k}{(k-1)!} l^{k-1}, & \text{if } l \ge 0. \end{cases}$$

It follows that

$$G_k(z) = \frac{\Gamma(k)}{(-2\pi i)^k}\zeta(k) + \sum_{m=1}^{+\infty}\sum_{l=1}^{+\infty} l^{k-1} q^{lm} = \frac{\Gamma(k)}{(-2\pi i)^k}\zeta(k) + \sum_{n=1}^{+\infty} \sigma_{k-1}(n) q^n.$$

$\square$

Remark. (i) $G_2(z) = \frac{\Gamma(2)}{(-2\pi i)^2}\zeta(2) + \sum_{n=1}^{+\infty} \sigma_1(n) q^n$ is not a modular form, but it is almost one. Let

$$G_2^*(z) = G_2(z) + \frac{1}{8\pi y} = \frac{1}{2}\frac{\Gamma(2)}{(-2\pi i)^2} \lim_{s\to 0} \sum_{m,n}{}' \frac{1}{(mz+n)^2} \frac{y^s}{|mz+n|^{2s}},$$

G_2^* is not holomorphic, but $G_2^*|_2\gamma = G_2^*$, for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

(ii) Let $E_k = \frac{G_k}{a_0(G_k)}$, so that $a_0(E_k) = 1$.

2.2.3 The fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$

Theorem 2.2.5. *Let D denotes the shadows in Figure 1.1. Then it is a fundamental domain for $\mathrm{PSL}_2(\mathbb{Z})$. Moreover, the stabilizer of $z \in D$ is*

- $\{\mathrm{I}\}$ *if $z \ne i, \rho$;*
- $\{\mathrm{I}, S\}$ *if $z = i$;*
- $\{\mathrm{I}, TS,\ (TS)^2\}$ *if $z = \rho$.*

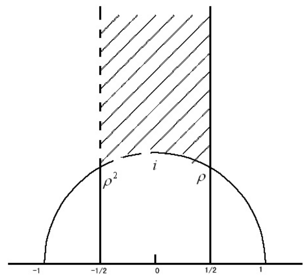


Figure 2.1: The Fundamental Domain.

Proof. Let $z_0 \in \mathcal{H}$,

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

Since $\mathrm{Im}\,(\gamma z_0) = \frac{z_0}{|cz_0+d|^2}$ tends to zero, as (c, d) tends to infinity, there exists γ_0 such that $\mathrm{Im}\,(\gamma_0 z_0)$ is maximal. There exists a unique n such that:

$$-\frac{1}{2} < \mathrm{Re}\,(\gamma_0 z_0) + n \leq \frac{1}{2}.$$

Let $\gamma_1 = T^n \gamma_0$, then

$$\mathrm{Im}\,(\gamma_1 z_0) = \mathrm{Im}\,(\gamma_0 z_0) \geq \mathrm{Im}\,(S\gamma_1 z_0) = \frac{\mathrm{Im}\,(\gamma_1 z_0)}{|\gamma_1 z_0|^2}$$

which implies $|\gamma_1 z_0| \geq 1$. Therefore D contains a fundamental domain.

If $z_1, z_2 \in D$, and there exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, such that $z_1 = \gamma z_2$, we want to show $z_1 = z_2$. By symmetry, we may assume $\mathrm{Im}\,(z_2) \geq \mathrm{Im}\,(z_1)$. If $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, $\mathrm{Im}\,(z_2) \geq \frac{\mathrm{Im}\,(z_2)}{|cz_2+d|^2}$ implies $|cz_2 + d|^2 \leq 1$. As $\mathrm{Im}\,(z_2) \geq \frac{\sqrt{3}}{2}$, we have $c \leq 1, d \leq 1$. It remains only finite number of cases to check.

If $c = 0$, then $d = \pm 1$, and γ is the translation by $\pm b$. Since

$$-\frac{1}{2} < \mathrm{Re}\,(z_1),\ \mathrm{Re}\,(z_2) \leq \frac{1}{2},$$

this implies $b = 0$, and $\gamma = \pm\,\mathrm{I}$.

If $c = 1$, the fact $|z_2 + d| \leq 1$ implies $d = 0$ except if $z_2 = \rho$, in which case we can have $d = 0, -1$. The case $d = 0$ gives $|z_2| \leq 1$, hence $|z_2| = 1$; on the other hand, $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ implies $b = -1$, hence $z_1 = \gamma z_2 = a - 1/z_2 \in D$,

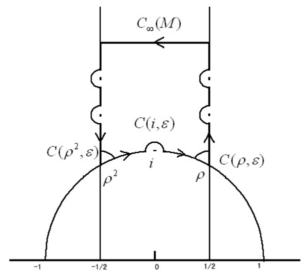


Figure 2.2: The Route $C(M,\varepsilon)$ of Integration.

which implies $a = 0$, and $z_1 = z_2 = i$. The case $z_2 = \rho$, and $d = -1$ gives $a + b + 1 = 0$ and $z_1 = \gamma z_2 = a - \frac{1}{\rho - 1} = a + \rho \in D$, which implies $a = 0$ and $z_1 = z_2 = \rho$.

If $c = -1$, we have similar argument as $c = 1$.

This completes the proof of the Theorem. □

2.2.4 The $\frac{k}{12}$ formula.

The following proposition is usually called "the $\frac{k}{12}$ formula".

Proposition 2.2.6. *Let $f \in \mathrm{M}_k - \{0\}$, then*

$$v_\infty(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_\rho(f) + \sum_{z \in D - \{i,\rho\}} v_z(f) = \frac{k}{12}.$$

Proof. Apply Cauchy residue formula to $d\log f$ over the path showed in Figure 1.2. As $M \to +\infty$, and $\varepsilon \to 0$, we have:

$$\frac{1}{2\pi i}\int_{C(M,\varepsilon)} \mathrm{d}\log f = \sum_{z \in D - \{i,\rho\}} v_z(f),$$

$$\lim_{M \to +\infty} \frac{1}{2\pi i}\int_{C_\infty(M)} \mathrm{d}\log f = \lim_{M \to +\infty} -\frac{1}{2\pi i}\int_{|z| = e^{-2\pi M}} \mathrm{d}\log \sum a_n(f) z^n = -v_\infty(f),$$

$$\lim_{\varepsilon \to 0} \frac{1}{2\pi i}\int_{C(i,\varepsilon)} \mathrm{d}\log f = -\frac{1}{2}v_i(f),$$

$$\lim_{\varepsilon\to 0}\frac{1}{2\pi i}\int_{C(\rho,\varepsilon)}\mathrm{d}\log f = -\frac{1}{6}v_\rho(f) = -\frac{1}{6}v_{\rho^2}(f) = \lim_{\varepsilon\to 0}\frac{1}{2\pi i}\int_{C(\rho^2,\varepsilon)}\mathrm{d}\log f$$

$$\begin{aligned}\frac{1}{2\pi i}(\int_{\rho^2}^{i}\mathrm{d}\log f + \int_i^\rho \mathrm{d}\log f) &= \frac{1}{2\pi i}\int_{\rho^2}^{i}(\mathrm{d}\log f - \mathrm{d}\log f(-\frac{1}{z}))\\ &= -\frac{1}{2\pi i}\int_{\rho^2}^{i}(\mathrm{d}\log f - \mathrm{d}\log z^k f(z))\\ &= -\frac{k}{2\pi i}\int_{\rho^2}^{i}\frac{\mathrm{d}\,z}{z} = -\frac{k}{2\pi i}(\log i - \log\rho^2) = \frac{k}{12}.\end{aligned}$$

Putting all these equations together, we get the required formula. □

Corollary 2.2.7. *G_4 has its only zero on D at $z = \rho$, G_6 has its only zero on D at $z = i$.*

$$\Delta = ((\frac{G_4}{a_0(G_4)})^3 - (\frac{G_6}{a_0(G_6)})^2)\frac{1}{3a_0^{-1}(G_4) - 2a_0^{-1}(G_6)} = q + \cdots \in \mathrm{M}_{12}(1)$$

does not vanish on D ($v_\infty(\Delta) = 1$).

Remark. One can prove $\Delta = q\prod_{n=1}^{+\infty}(1-q^n)^{24}$.

2.2.5 Dimension of spaces of modular forms.

Theorem 2.2.8. (i) $\mathrm{M}_k(1) = 0$*, if k is odd or $k = 2$.*

(ii) $\dim \mathrm{M}_k(1) = 1$*, if $k = 0$ or k is even and $2 < k \leq 10$. In this case* $\mathrm{M}_k(1) = \mathbb{C}\cdot G_k$ *(We have $G_0 = 1$).*

(iii) $M_{k+12}(1) = \mathbb{C}\cdot G_{k+12} \oplus \Delta\cdot\mathrm{M}_k(1)$.

Proof. If $f \in \mathrm{M}_{k+12}$, then

$$f = \frac{a_0(f)}{a_0(G_{k+12})}G_{k+12} + \Delta\, g,$$

where $g \in \mathrm{M}_k(1)$, because Δ does not vanish on $\mathcal{H}$, $v_\infty(\Delta) = 1$ and $v_\infty(f - \frac{a_0(f)}{a_0(G_{k+12})}G_{k+12}) \geq 1$. □

Corollary 2.2.9. *If k is even,* $\dim_{\mathbb{C}} \mathrm{M}_k(1) = \begin{cases} [\frac{k}{12}], & k \equiv 2 \bmod 12, \\ [\frac{k}{12}] + 1, & \textit{if not.} \end{cases}$

Remark. Finite dimensionality of spaces of modular forms has many combinatorical applications. For example, let

$$\theta(z) = \sum_{n\in\mathbb{Z}} q^{\frac{n^2}{2}} = \sum_{n\in\mathbb{Z}} e^{\pi i n^2 z},$$

$$\Gamma_\theta = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}), \gamma \equiv I \text{ or } \gamma \equiv S \mod 2\},$$

$$\chi_\theta : \Gamma_\theta \to \{\pm 1\}. \quad \chi_\theta(\gamma) = \begin{cases} 1 & \text{if } \gamma \equiv I \\ -1 & \text{if } \gamma \equiv S \end{cases}$$

One can check that $\dim \mathrm{M}_2(\Gamma_\theta, \chi_\theta) \leq 1$, $\theta^4 \in \mathrm{M}_2(\Gamma_\theta, \chi_\theta)$, and $4G_2^*(2z) - G_2^*(\frac{z}{2}) \in \mathrm{M}_2(\Gamma_\theta, \chi_\theta)$, so we have

$$4G_2^*(2z) - G_2^*(\frac{z}{2}) = \frac{3\zeta(2)\Gamma(2)}{(-2\pi i)^2}\theta^4,$$

hence

$$|\{(a,b,c,d) \in \mathbb{Z}^4 : a^2 + b^2 + c^2 + d^2 = n\}| = 8 \sum_{d|n, 4\nmid d} d,$$

from which we can deduce that any positive integer can be written as a sum of 4 squares.

2.2.6 Rationality results.

As $\mathrm{M}_8(1)$ and $\mathrm{M}_{10}(1)$ are of dimension 1, we have

$$a_0(G_8)G_4^2 = a_0(G_4)^2 G_8, \quad a_0(G_{10})G_4G_6 = a_0(G_4)a_0(G_6)G_{10}. \qquad (*)$$

Let

$$\alpha = \frac{\Gamma(4)}{(-2\pi i)^4}\zeta(4), \quad \beta = \frac{\Gamma(8)}{(-2\pi i)^8}\zeta(8).$$

Substituting

$$G_4 = \alpha + q + 9q^2 + \cdots, \quad G_8 = \beta + q + 129q^2 + \cdots$$

in $(*)$, compare the coefficients of q and q^2, we have the following equations:

$$\begin{cases} 2\alpha\beta = \alpha^2 \\ \beta(1+18\alpha) = 129\alpha^2 \end{cases}$$

The solution is: $\alpha = \frac{1}{240}$, $\beta = \frac{1}{480}$. In particular, $\alpha, \beta \in \mathbb{Q}$, which implies G_4 and G_8 have rational q-expansions, and $\frac{\zeta(4)}{\pi^4} \in \mathbb{Q}$, $\frac{\zeta(8)}{\pi^8} \in \mathbb{Q}$.

Exercise. $a_0(G_6) = -\frac{1}{504}$, which implies $\frac{\zeta(6)}{\pi^6} \in \mathbb{Q}$.

Let A be a subring of $\mathbb{C}$, let

$$\mathrm{M}_k(\Gamma, A) = \{f \in \mathrm{M}_k(\Gamma), a_n(f) \in A, \text{for all } n\},$$

then $\mathrm{M}(\Gamma, A) = \sum_k \mathrm{M}_k(\Gamma, A)$ is an A-algebra.

Theorem 2.2.10. (i) $\mathrm{M}(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Q}) \xrightarrow{\sim} \mathbb{Q}[X, Y]$, *where* $X = G_4$, $Y = G_6$.
(ii) $\mathrm{M}(\mathrm{SL}_2(\mathbb{Z}), \mathbb{C}) = \mathbb{C} \otimes \mathrm{M}(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Q})$.

Proof. If $\sum_k f_k = 0$, where $f_k \in \mathrm{M}_k(\mathrm{SL}_2(\mathbb{Z}), \mathbb{C})$, then for any z, for any $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, we have $\sum\limits_k (cz+d)^k f_k(z) = 0$. Therefore $\sum\limits_k (Xz+Y)^k f_k(z)$ is identically zero because it (as a polynomial in X and Y) has too many zeros. Hence $f_k(z) = 0$, which implies that

$$\mathrm{M}(\mathrm{SL}_2(\mathbb{Z}), \mathbb{C}) = \bigoplus_k \mathrm{M}_k(\mathrm{SL}_2(\mathbb{Z}), \mathbb{C}).$$

Now if $k = 12n$, $G_4^{3n}, G_4^{3(n-1)}\,\Delta, \cdots, \Delta^n$ is a basis of $\mathrm{M}_k(1)$; if $k = 12n+2$, $G_4^{3(n-1)+2} G_6, G_4^{3(n-2)+2} G_6\,\Delta, \cdots, G_4^2 G_6\,\Delta^{n-1}$ is a basis of $\mathrm{M}_k(1)$, and so on, $\Delta = aG_4^3 + bG_6^2$, $a, b \in \mathbb{Q}$. As $G_4, G_6 \in \mathrm{M}(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Q})$, this proves both results. □

Corollary 2.2.11. *Let* $f \in \mathrm{M}_k(1)$, $\sigma \in \mathrm{Aut}(\mathbb{C})$, *then* $f^\sigma = \sum a_n(f)^\sigma q^n \in \mathrm{M}_k(1)$. *Moreover,* $\frac{\zeta(k)}{(-2\pi i)^k} \in \mathbb{Q}$ *if* k *is even and* $k \geq 4$.

Proof. The first assertion is a direct consequence of Theorem 2.2.10 (ii). For any $\sigma \in \mathrm{Aut}(\mathbb{C})$, we have

$$G_k^\sigma - G_k = a_0(G_k)^\sigma - a_0(G_k) \in \mathrm{M}_k(1).$$

This implies $a_0(G_k)^\sigma = a_0(G_k)$ for any $\sigma \in \mathrm{Aut}(\mathbb{C})$, therefore $a_0(G_k) \in \mathbb{Q}$. □

Remark. When $k = 2$, we can use

$$4G_2^*(2z) - G_2^*(\frac{z}{2}) \in \mathrm{M}_2(\Gamma_\theta, \mathbb{Q})$$

to deduce $\frac{\zeta(2)}{\pi^2} \in \mathbb{Q}$.

Remark. (i) The zeta function ζ is a special case of L-functions, and $\zeta(k)$ are $s$pecial values of L-functions (i.e. values of L-functions at integers).

Siegel used the above method to prove rationality of special values of L-functions for totally real fields.

(ii) With a lot of extra work, we can prove integrality results. As

$$G_k(z) = \frac{\Gamma(k)}{(-2\pi i)^k}\zeta(k) + \sum_{n=1}^{+\infty} \sigma_{k-1}(n) q^n,$$

and $\sigma_{k-1}(n) = \int_{\mathbb{Z}_p} x^{k-1}(\sum\limits_{d|n} \delta_d)$, we have all $a_n(G_k)$ are given by measures on $\mathbb{Z}_p$, therefore $a_0(G_k)$ is also given by measures. From which we can deduce other constructions of Kubota-Leopoldt zeta functions (the work of Serre, Deligne, Ribet).

2.3 The algebra of all modular forms.

Let A be a subring of $\mathbb{C}$, let

$$\mathcal{M}_k(A) = \bigcup_{[\mathrm{SL}_2(\mathbb{Z}):\Gamma]<+\infty} \mathrm{M}_k(\Gamma, A) = \left\{\sum a_n q^n \in \mathrm{M}_k(\Gamma, \mathbb{C}), a_n \in A,\ n \in \mathbb{N}\right\}.$$

Let $\mathcal{M}(A) = \oplus \mathcal{M}_k(A)$, then it is an A-algebra. Let

$$\mathcal{M}^{\mathrm{cong}}(A) = \bigcup_{\Gamma \text{ congruence subgroup}} \mathrm{M}(\Gamma, A).$$

Theorem 2.3.1. (i) *If $f \in \mathcal{M}(\mathbb{C})$, and $\sigma \in \mathrm{Aut}(\mathbb{C})$, then $f^\sigma \in \mathcal{M}(\mathbb{C})$.*

(ii) $\mathcal{M}(\mathbb{C}) = \mathbb{C} \otimes_{\overline{\mathbb{Q}}} \mathcal{M}(\overline{\mathbb{Q}}) = \mathbb{C} \otimes_{\mathbb{Q}} \mathcal{M}(\mathbb{Q})$.

(iii) *Let $\Pi_\mathbb{Q} = \mathrm{Aut}(\mathcal{M}(\overline{\mathbb{Q}})/\,\mathrm{M}(SL_2(\mathbb{Z}), \mathbb{Q}))$, $G_\mathbb{Q} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, then we have an exact sequence:*

$$\begin{tikzcd} 1 \arrow[r] & \mathrm{SL}_2(\mathbb{Z})^\wedge \arrow[r] & \Pi_\mathbb{Q} \arrow[r] & G_\mathbb{Q} \arrow[r] \arrow[l, bend right] & 1 \end{tikzcd}$$

where $G^\wedge \triangleq \varprojlim_{\substack{[G:\Gamma]<\infty \\ \Gamma \ normal}} (G/\Gamma)$, *and* $G_\mathbb{Q} \to \Pi_\mathbb{Q}$ *is induced by the action on Fourier coefficients.*

(iv) $\mathcal{M}^{cong}(\mathbb{Q}^{ab})$ *is stable by* $\Pi_\mathbb{Q}$, *and*

$$\mathrm{Aut}(\mathcal{M}^{cong}(\mathbb{Q}^{ab})/\,\mathrm{M}(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Q})) \xrightarrow{\sim} \mathrm{GL}_2(\hat{\mathbb{Z}}).$$

Moreover, we have the following commutative diagram:

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{SL}_2(\mathbb{Z})^\wedge \arrow[r] \arrow[d] & \Pi_\mathbb{Q} \arrow[r] \arrow[d] & G_\mathbb{Q} \arrow[r] \arrow[d] \arrow[l, bend right] & 1 \\
1 \arrow[r] & \mathrm{SL}_2(\hat{\mathbb{Z}}) \arrow[r] & \mathrm{GL}_2(\hat{\mathbb{Z}}) \arrow[r] & \hat{\mathbb{Z}}^* \arrow[r] \arrow[l, bend right] & 1
\end{tikzcd}$$

where $G_\mathbb{Q} \to \hat{\mathbb{Z}}^*$ *is the cyclotomic character,* $\mathrm{GL}_2(\hat{\mathbb{Z}}) \to \hat{\mathbb{Z}}^*$ *is the determinant map, and* $\hat{\mathbb{Z}}^* \to \mathrm{GL}_2(\hat{\mathbb{Z}})$ *maps* u *to* $\left(\begin{smallmatrix} 1 & 0 \\ 0 & u \end{smallmatrix}\right)$.

Remark. (i) $\mathrm{SL}_2(\mathbb{Z})^\wedge$ is much bigger than $\mathrm{SL}_2(\hat{\mathbb{Z}})$.

(ii) We can get an action of $G_\mathbb{Q}$ on $\mathrm{SL}_2(\mathbb{Z})^\wedge$ by inner conjugation in $\Pi_\mathbb{Q}$. This is a powerful way to study $G_\mathbb{Q}$ (Grothendieck, "esquisse d'un programme").

(iii) There are p-adic representations of $G_\mathbb{Q}$ attached to modular forms (by Deligne) for congruence subgroups. They come from the actions of $G_\mathbb{Q}$ on $\mathrm{H}^1(\mathrm{SL}_2(\mathbb{Z})^\wedge, W)$, where $W = \mathrm{Sym}^{k-2} V_p \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\mathrm{SL}_2(\mathbb{Z})/\Gamma]$, V_p is $\mathbb{Q}_p^2$ with actions of $\Pi_\mathbb{Q}$ through $\mathrm{GL}_2(\mathbb{Z}_p)$ and are cut out using Hecke operators on these spaces.

Proof of Theorem 2.3.1 (i). Let $\mathrm{N}(\Gamma, A)$ denote the set of holomorphic functions $f : \mathcal{H} \to \mathbb{C}$ satisfying the following conditions:

(a) for any $\gamma \in \Gamma$, $f(\gamma z) = f(z)$,

(b) for any $\gamma \in \Gamma\backslash \mathrm{SL}_2(\mathbb{Z})$, $f \circ \gamma = \sum_{\substack{n \geq n_0(\gamma, f) \\ n \in \frac{1}{M}\mathbb{Z}}} a_n q^n$, and $a_n \in A$ for any n.

As $\Delta \in \mathrm{S}_{12}(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Q})$ does not vanish on $\mathcal{H}$, $\Delta^{\frac{1}{12}} \in \mathrm{S}_1(\mathrm{SL}_2(\mathbb{Z}), \chi, \mathbb{Q})$, where $\chi : \mathrm{SL}_2(\mathbb{Z}) \to \mu_{12}$. Let $\Gamma_0 = \mathrm{Ker}\,\chi$. If $f \in \mathrm{M}_k(\Gamma, A)$, $\Delta^{-\frac{k}{12}} f \in \mathrm{N}(\Gamma \cap \Gamma_0, A)$. If $f \in \mathrm{N}(\Gamma, A)$, $\Delta^k f \in \mathrm{M}_{12k}(\Gamma, A)$, where $k + n_0(\gamma, f) \geq 0$ for any $\gamma \in$

$\Gamma\backslash \mathrm{SL}_2(\mathbb{Z})$. Therefore knowing $\mathrm{N}(\Gamma, A)$ is equivalent to knowing $\mathrm{M}(\Gamma, A)$. So it suffices to prove if

$$f = \sum_{n \geq n_0} a_n q^n \in \mathcal{N}(\mathbb{C}) = \bigcup_{\Gamma} \mathrm{N}(\Gamma, \mathbb{C})$$

and $\sigma \in \operatorname{Aut} \mathbb{C}$, then $f^\sigma \in \mathcal{N}(\mathbb{C})$.

Let $j = \frac{G_4^3}{a_0(G_4^3)\,\Delta} = q^{-1} + \cdots \in \mathrm{N}(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Q})$.

Proposition 2.3.2. (i) $\mathrm{N}(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Q}) = \mathbb{Q}[j]$, $N(\mathrm{SL}_2(\mathbb{Z}), \mathbb{C}) = \mathbb{C}[j]$.

(ii) $j : \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H} \to \mathbb{C}$ *is bijective.*

(iii) $j(z) - j(\alpha)$ *has a zero at* $z = \alpha$ *of order* $e(\alpha) = \begin{cases} 3 & \text{if } \alpha \in \mathrm{SL}_2(\mathbb{Z})\rho \\ 2 & \text{if } \alpha \in \mathrm{SL}_2(\mathbb{Z})i, \\ 1 & \text{otherwise.} \end{cases}$

(iv) $j(i), j(\rho) \in \mathbb{Q}$.

Proof. (i) Note that $G_4^{3a}, G_4^{3(a-1)}\Delta, \cdots, \Delta^a$ is a basis of $\mathrm{M}_{12a}(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Q})$.

(ii) and (iii): For any $\beta \in \mathbb{C}$, $f = (j - \beta) \cdot \Delta \in \mathrm{M}_{12}(\mathrm{SL}_2(\mathbb{Z}), \mathbb{C})$, with $v_\infty(f) = 0$. As $D = \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$, and

$$\sum_{z \in D - \{\rho, i\}} \gamma_z(f) + \frac{1}{2}\gamma_i(f) + \frac{1}{3}(f) = 1,$$

we can deduce the required results.

(iv) $G_4(\rho) = 0$, $G_6(i) = 0$. $\square$

Let $f \in \mathrm{N}(\Gamma, \mathbb{C})$,

$$P_f(X) = \prod_{\delta \in \Gamma\backslash \mathrm{SL}_2(\mathbb{Z})} (X - f \circ \delta) \in \mathrm{N}(\mathrm{SL}_2(\mathbb{Z}), \mathbb{C})[X] \subset \mathbb{C}((q))[X]$$

$$P_{f^\sigma}(X) = \prod_{\delta \in \Gamma\backslash \mathrm{SL}_2(\mathbb{Z})} (X - (f \circ \delta)^\sigma) \in \mathrm{N}(\mathrm{SL}_2(\mathbb{Z}), \mathbb{C})[X] \subset \mathbb{C}((q))[X]$$

Denote $P_f(X) = \sum_{l=0}^{n} g_l X^l$, $P_{f^\sigma}(X) = \sum_{l=0}^{n} g_l^\sigma X^l$, where $g_l \in \mathrm{N}(\mathrm{SL}_2(\mathbb{Z}), \mathbb{C})$, and $g_l^\sigma \in \mathrm{N}(\mathrm{SL}_2(\mathbb{Z}), \mathbb{C})$ thanks to the Corollary 2.2.11. We give the proof in two steps.

Step 1: Prove that f^σ is holomorphic on $\mathcal{H}$, by the Proposition 2.3.2. We have

$$P_f(X) = \sum_{l=0}^{n} P_l(j)X^l, \qquad P_{f^\sigma}(X) = \sum_{l=0}^{n} P_l^\sigma(j)X^l.$$

The roots of P_f are the $f \circ \delta$'s, where $\delta \in \Gamma\backslash \mathrm{SL}_2(\mathbb{Z})$. They are holomorphic on $\mathcal{H}$. The roots of P_{f^σ} are multivalued holomorphic functions on $\mathcal{H}$. In order to prove that are single valued, it suffices to show there is no ramification. Let α be an arbitrary element in $\mathcal{H}$. we have, around α, n distinct formal solutions

$$\sum_{k=0}^{+\infty} a_{l,k}(\alpha)(j - j(\alpha))^{\frac{k}{e(\alpha)}} \quad (1 \leq l \leq n)$$

of $P_f(X) = 0$ as $(j - j(\alpha))^{\frac{1}{e(\alpha)}}$ is a local parameter around α by Proposition 2.3.2. Let $\beta_\sigma \in \mathcal{H}$ satisfies $j(\beta_\sigma) = j(\alpha)^\sigma$, then we have $e(\beta_\sigma) = e(\alpha)$. Therefore

$$\sum_{k=0}^{+\infty} a_{l,k}(\alpha)^\sigma(j - j(\beta_\sigma))^{\frac{k}{e(\beta_\sigma)}}, \quad (1 \leq l \leq n)$$

are n distinct formal solutions around β_σ. It follows that there is no ramification around β_σ, for any β_σ. Hence the roots of P_{f^σ} are holomorphic on $\mathcal{H}$. In particular, f^σ is holomorphic on $\mathcal{H}$.

Step 2: Prove that there exists $\Gamma' \subset \mathrm{SL}_2(\mathbb{Z})$ of finite index, such that $f^\sigma \circ \gamma = f^\sigma$ for any $\gamma \in \Gamma$. For any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$,

$$P_{f^\sigma}(f^\sigma \circ \gamma) = \sum_{l=0}^{n} g_l^\sigma (f^\sigma \circ \gamma)^l = \sum_{l=0}^{n} g_l^\sigma \circ \gamma (f^\sigma \circ \gamma)^l = P_{f^\sigma}(f^\sigma) \circ \gamma = 0$$

So $f^\sigma \circ \gamma$ belongs to the finite set of roots of P_{f^σ}, which leads to the required conclusion. $\square$

2.4 Hecke operators

2.4.1 Preliminary.

Let $\Gamma \subset G$ be groups (for example, $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, $G = \mathrm{GL}_2(\mathbb{Q})^+$), let $x \in G$,

$$x\Gamma = \{x\gamma : \gamma \in \Gamma\}, \quad \Gamma x = \{\gamma x : \gamma \in \Gamma\}.$$

Let A be a ring, define $A[\Gamma\backslash G/\Gamma]$ to be the set of $\phi : G \to A$ satisfying the following two conditions:

(i) $\phi(\gamma x) = \phi(x\gamma) = \phi(x)$, for all $x \in G, \gamma \in \Gamma$.

(ii) There exists a finite set I such that $\phi = \sum_{i\in I} \lambda_i 1_{\Gamma x_i}$.

Remark. (i) We impose x_i to be distinct in $\Gamma\backslash G$, in this situation, the decomposition is unique, λ_i's are unique.

(ii) For any $\gamma \in \Gamma$, $1_{\Gamma x_i \gamma}(x) = 1_{\Gamma x_i}(x\gamma^{-1})$. So $\phi = \sum_{i\in I} \lambda_i 1_{\Gamma x_i} \in A[\Gamma\backslash G/\Gamma]$ implies

$$\sum_{i\in I} \lambda_i 1_{\Gamma x_i \gamma}(x) = \sum_{i\in I} \lambda_i 1_{\Gamma x_i}(x\gamma^{-1}) = \phi(x\gamma^{-1}) = \phi(x) = \sum_{i\in I} \lambda_i 1_{\Gamma x_i}(x)$$

Therefore there exists a permutation: $\sigma : I \to I$, and for any $i \in I$, there exists $\gamma_i \in \Gamma$, such that $\lambda_{\sigma(i)} = \lambda_i$, $x_i\gamma = \gamma_i x_{\sigma(i)}$.

Proposition 2.4.1. (i) *If* $\phi = \sum_{i\in I} \lambda_i 1_{\Gamma x_i}$, $\phi' = \sum_{j\in J} \mu_j 1_{\Gamma y_j} \in A[\Gamma\backslash G/\Gamma]$, *then*

$$\phi * \phi' = \sum_{(i,j)\in I\times J} \lambda_i \mu_j 1_{\Gamma x_i y_j} \in A[\Gamma\backslash G/\Gamma],$$

and it does not depend on the choices.

(ii) $(A[\Gamma\backslash G/\Gamma], +, *)$ *is an associative A-algebra with 1_Γ as a unit.*

(iii) *If M is a right G-module with G action $m \mapsto m * g$, and* $\phi = \sum \lambda_i 1_{\Gamma x_i} \in A[\Gamma\backslash G/\Gamma]$, *then for any* $m \in M^\Gamma$, $m * \phi = \sum_{i\in I} \lambda_i m * x_i$ *does not depend on the choices of x_i. Moreover,* $m*\phi \in M^\Gamma$, $m*(\phi_1*\phi_2) = (m*\phi_1)*\phi_2$, $m * (\phi_1 + \phi_2) = (m * \phi_1) + (m * \phi_2)$.

Proof. Exercise, using the previous remark. □

Remark. If $\Gamma = 1$, then $A[\Gamma\backslash G/\Gamma] = A[G]$ is commutative if and only if G is commutative.

2.4.2 Definition of Hecke operators: R_n, T_n, $n \geq 1$.

Let $G = \mathrm{GL}_2(\mathbb{Q})^+$, $\Gamma = \mathrm{SL}_2(\mathbb{Z})$.

Lemma 2.4.2. *Let* $g \in G \cap M_2(\mathbb{Z})$, *then there exists a unique pair* $(a, d) \in \mathbb{N} - \{0\}$, *and* $b \in \mathbb{Z}$ *unique* $\bmod d\mathbb{Z}$, *such that* $\Gamma g = \Gamma\left(\begin{smallmatrix} a & b \\ 0 & d\end{smallmatrix}\right)$

Proof. Let $g = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$, there exists $\mu, \nu \in \mathbb{Z}$, such that $(\mu, \nu) = 1$, and $\mu\alpha + \nu\gamma = 0$. And there exists $x, y \in \mathbb{Z}$, such that $x\nu - \mu y = 1$, Let $\gamma_0 = \left(\begin{smallmatrix} x & y \\ \mu & \nu \end{smallmatrix}\right)$ if $x\alpha + y\gamma \geq 0$; $\gamma_0 = -\left(\begin{smallmatrix} x & y \\ \mu & \nu \end{smallmatrix}\right)$ if $x\alpha + y\gamma < 0$. Then $\gamma_0 g = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$, where $a > 0$. Thus completes the proof of existence.

If $\gamma_1, \gamma_2 \in \Gamma$ satisfies

$$\gamma_1 g = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \qquad \gamma_2 g = \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}$$

then

$$(\gamma_1 g)(\gamma_2 g)^{-1} = \begin{pmatrix} \frac{a_1}{a_2} & \frac{a_2 b_1 - a_1 b_2}{a_2 d_2} \\ 0 & \frac{d_1}{d_2} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

This implies $a_1 = a_2$, $d_1 = d_2$, $b_1 - b_2$ divisible by d_1. $\square$

Lemma-definition 2.4.3. For any $n \geq 1$,

$$R_n = 1_{\Gamma\left(\begin{smallmatrix} n & 0 \\ 0 & n \end{smallmatrix}\right)} \in \mathbb{Z}[\Gamma \backslash G / \Gamma],$$

$$T_n = 1_{\{g \in \mathrm{M}_2(\mathbb{Z}), \det g = n\}} \in \mathbb{Z}[\Gamma \backslash G / \Gamma].$$

Proof. Left and right invariance come from $\det gg' = \det g \det g'$. And Lemma 2.4.2 implies $T_n = \sum_{\substack{ad = n, a \geq 1 \\ b \bmod d}} 1_{\Gamma\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)}$, so get the finiteness needed. $\square$

Remark. If p is prime, Then $T_p = 1_{\Gamma\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)\Gamma}$ by elementary divisors for principle ideal domains.

Theorem 2.4.4. (i) *For any $n \geq 1$ and $l \geq 1$, $R_n R_l = R_{nl} = R_l R_n$, $R_n T_l = T_l R_n$.*

(ii) *If $(l, n) = 1$, $T_l T_n = T_{ln} = T_n T_l$.*

(iii) *If p is prime and $r \geq 1$, $T_{p^r} T_p = T_{p^{r+1}} + p R_p T_{p^{r-1}}$.*

(iv) *Let $\mathbb{T}_{\mathbb{Z}}$ be the subalgebra of $\mathbb{Z}[\Gamma \backslash G / \Gamma]$ generated by R_n and T_n ($n \geq 1$). It is a commutative algebra.*

Proof. (i) It is trivial.

(ii) We have

$$T_n T_l = \sum_{\substack{ad = n, a \geq 1 \\ b \bmod d}} \sum_{\substack{a'd' = n, a' \geq 1 \\ b' \bmod d'}} 1_{\Gamma\left(\begin{smallmatrix} aa' & ab' + bd' \\ 0 & dd' \end{smallmatrix}\right)}.$$

As $(n,l)=1$, $(a,a')=1$, $(a,d')=1$. This implies $\{aa' : a|n, a'|l\} = \{a'' : a''|nl\}$. Therefore in order to show $T_nT_l = T_{nl}$, it suffices to verify that $\{ab'+bd'\}$ is a set of representatives of $\mathbb{Z}/(dd')\mathbb{Z}$, where b is a set of representatives of $\mathbb{Z}/d\mathbb{Z}$, b' is a set of representatives of $\mathbb{Z}/d'\mathbb{Z}$. It suffices to show the injectivity under the $\bmod dd'\mathbb{Z}$ map. If

$$ab'_1 + b_1 d' \equiv ab'_2 + b_2 d',$$

then $b'_1 \equiv b'_2 \bmod d'$, so $b'_1 = b'_2$, which leads to the required conclusion.

(iii) We have

$$T_{p^r} = \sum_{i=0}^{r} \sum_{b \bmod p^i} 1_{\Gamma\left(\begin{smallmatrix} p^{r-i} & b \\ 0 & p^i \end{smallmatrix}\right)}, \quad T_p = 1_{\Gamma\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)} + \sum_{c \bmod p} 1_{\Gamma\left(\begin{smallmatrix} 1 & c \\ 0 & p \end{smallmatrix}\right)}$$

Then

$$\begin{aligned} T_{p^r}T_p =& \sum_{i=0}^{r} \sum_{b \bmod p^i} 1_{\Gamma\left(\begin{smallmatrix} p^{r+1-i} & b \\ 0 & p^i \end{smallmatrix}\right)} + \sum_{i=0}^{r} \sum_{b \bmod p^i} \sum_{c \bmod p} 1_{\Gamma\left(\begin{smallmatrix} p^{r-i} & pb+p^{r-i}c \\ 0 & p^{i+1} \end{smallmatrix}\right)} \\ =& T_{p^{r+1}} + R_p\Big(\sum_{i=0}^{r-1} \sum_{b \bmod p^i} \sum_{c \bmod p} 1_{\Gamma\left(\begin{smallmatrix} p^{r-1-i} & b+p^{r-1-i} \\ 0 & p^i \end{smallmatrix}\right)}\Big) = T_{p^{r+1}} + pR_pT_{p^{r-1}}. \end{aligned}$$

(iv) It follows from (i),(ii),(iii). □

2.4.3 Action of Hecke operators on modular forms.

The following two propositions are exercises in group theory.

Proposition 2.4.5. *Assume $G \supset \Gamma$ are groups. Then*

(i) *If $[\Gamma : \Gamma'] < +\infty$, then Γ' contains some Γ'' which is normal in Γ, and $[\Gamma : \Gamma''] < +\infty$.*

(ii) *If $[\Gamma : \Gamma_1] < +\infty$, $[\Gamma : \Gamma_2] < +\infty$, then $[\Gamma : \Gamma_1 \cap \Gamma_2] < +\infty$.*

(iii) *If $H' \subset H \subset G$, $[H : H'] < +\infty$, then $[H \cap \Gamma : H' \cap \Gamma] < +\infty$.*

Proposition 2.4.6. (i) *Suppose $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$, and $N \in \mathbb{N}$ such that $N\alpha$, $N\alpha^{-1} \in \mathrm{M}_2(\mathbb{Z})$, then*

$$\alpha^{-1}\,\mathrm{SL}_2(\mathbb{Z})\alpha \cap \mathrm{SL}_2(\mathbb{Z}) \supset \Gamma(N^2) := \mathrm{SL}_2(\mathbb{Z}) \cap (1 + N^2\,\mathrm{M}_2(\mathbb{Z})).$$

(ii) *If $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma] < +\infty$, $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$, then*

$$[\mathrm{SL}_2(\mathbb{Z}) : SL_2(\mathbb{Z}) \cap \alpha^{-1}\Gamma\alpha] < +\infty.$$

Proposition 2.4.7.

$$\mathcal{M}_k(\mathbb{C}) = \bigcup_{[\mathrm{SL}_2(\mathbb{Z}):\Gamma]<+\infty} \mathrm{M}_k(\Gamma, \mathbb{C}), \quad \mathcal{S}_k(\mathbb{C}) = \bigcup_{[\mathrm{SL}_2(\mathbb{Z}):\Gamma]<+\infty} \mathrm{S}_k(\Gamma, \mathbb{C})$$

are stable under $\mathrm{GL}_2(\mathbb{Q})^+$.

Proof. For any $\gamma \in \Gamma$, $f_{|k}\gamma = f$. For $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$, we have

$$(f_{|k}\alpha)_{|k}(\alpha^{-1}\gamma\alpha) = f_{|k}\alpha,$$

so $f_{|k}\alpha$ is invariant for the group $\alpha^{-1}\Gamma\alpha \cap \mathrm{SL}_2(\mathbb{Z})$.

To verify that $f_{|k}\alpha$ is slowly increasing at ∞, write $\alpha = \gamma\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, then

$$(f_{|k}\alpha)(z) = (ad)^{k-1}d^{-k}(f_{|k}\gamma)\left(\frac{az+b}{d}\right),$$

then we get the result. □

Let $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, $G = \mathrm{GL}_2(\mathbb{Q})^+$, $\varphi = \sum_{i\in I} \lambda_i 1_{\Gamma\gamma_i} \in \mathbb{Z}[\Gamma\backslash G/\Gamma]$, we define

$$f_{|k}\varphi = \sum_{i\in I} \lambda_i f_{|k}\gamma_i, \quad \text{for } f \in \mathrm{M}_k(1) = \mathcal{M}_k(\mathbb{C})^{\Gamma}.$$

The definition is independent of the choice of γ_i. From the general theory, we have

$$(f_{|k}\varphi)_{|k}\varphi'(z) = f_{|k}(\varphi * \varphi')(z).$$

If $f \in \mathrm{M}_k(1)$ (resp. $\mathrm{S}_k(1)$), then $f_{|k}\varphi \in \mathrm{M}_k(1)$ (resp. $\mathrm{S}_k(1)$).
Facts: $f_{|k}R_n = n^{k-2}f$, and $f_{|k}T_n = n^{k-1} \sum\limits_{\substack{ad=n, a\geq 1 \\ b \bmod d}} d^{-k} f(\frac{az+b}{d})$.

Proposition 2.4.8. *If* $f = \sum\limits_{m=0}^{\infty} a_m(f)q^m$, *then* $a_m(f_{|k}T_n) = \sum\limits_{\substack{a\geq 1, \\ a|(m,n)}} a^{k-1} a_{\frac{mn}{a^2}}(f)$.

Proof. For fixed $d|n$, $d \geq 1$,

$$\begin{aligned}
\sum_{b \bmod d} d^{-k} f(\tfrac{az+b}{d}) &= d^{-k} \sum_{b \bmod d} \sum_{m=0}^{\infty} a_m(f) e^{2\pi i m \frac{az+b}{d}} \\
&= d^{-k} \sum_{m=0}^{\infty} a_m(f) e^{2\pi i n a z/d} \sum_{b \bmod d} e^{2\pi i m b/d} \\
&= d^{1-k} \sum_{\substack{m=0 \\ d|m}}^{\infty} a_m(f) e^{2\pi i m a z/d} \\
&= d^{1-k} \sum_{l=0}^{\infty} a_{dl}(f) q^{al}.
\end{aligned}$$

So

$$f_{|k}T_n = n^{k-1} \sum_{ad=n, a\geq 1} d^{1-k} \sum_{l=0}^{\infty} a_{dl}(f) q^{al},$$

summing the coefficients of q^m, this gives:

$$\begin{aligned} a_m(f_{|k}T_n) &= n^{k-1} \sum_{\substack{a\geq 1 \\ a|(m,n)}} (n/a)^{1-k} a_{\frac{mn}{a^2}}(f) \\ &= \sum_{\substack{a\geq 1 \\ a|(m,n)}} a^{k-1} a_{\frac{mn}{a^2}}(f). \end{aligned}$$

□

Corollary 2.4.9. (i) $\mathrm{M}_k(\Gamma, \mathbb{Z})$ *and* $\mathrm{M}_k(\Gamma, \mathbb{Q})$ *are stable under* T_n *and* R_n.

(ii) $a_0(f_{|k}T_n) = \sum_{a|n} a^{k-1} a_0(f) = \sigma_{k-1}(n) a_0(f)$.

(iii) $a_1(f_{|k}T_n) = a_n(f)$, *therefore* f *is determined by*

$$T \longmapsto a_1(f_{|k}T).$$

2.5 Petersson scalar product.

Lemma 2.5.1.

$$\int_{\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}} \frac{dxdy}{y^2} = \int_{-\frac{1}{2}}^{\frac{1}{2}} \int_{\sqrt{1-x^2}}^{+\infty} \frac{dxdy}{y^2} = \frac{\pi}{3} < \infty.$$

Corollary 2.5.2. (i) *If* $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma] < +\infty$, *then*

$$\int_{\Gamma\backslash\mathcal{H}} \frac{dxdy}{y^2} = \frac{\pi}{3} C(\Gamma),$$

where $C(\Gamma) = [\mathrm{PSL}_2(\mathbb{Z}) : \bar{\Gamma}]$, $\bar{\Gamma}$ *is the image of* Γ *in* $\mathrm{PSL}_2(\mathbb{Z})$.

(ii) *If* $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$ *such that* $\alpha^{-1}\Gamma\alpha \subset \mathrm{SL}_2(\mathbb{Z})$, *then* $C(\alpha^{-1}\Gamma\alpha) = C(\Gamma)$.

Proof. (i) Since $\frac{dxdy}{y^2}$ is invariant under the action of Γ, the integral is well defined. Put $\{\gamma_i\}$ be a family of representatives of $\Gamma\backslash\mathrm{SL}_2(\mathbb{Z})$, then $\Gamma\backslash\mathcal{H} = \coprod \gamma_i(D)$ up to sets of measure 0 (maybe have overlap in $\mathrm{SL}_2(\mathbb{Z})i \cup \mathrm{SL}_2(\mathbb{Z})\rho$).

(ii) Since $\Gamma\backslash\mathcal{H} = \alpha\big(\alpha^{-1}\Gamma\alpha\backslash\mathcal{H}\big)$, the two integrals are the same by the invariance of $\frac{dxdy}{y^2}$. □

Let $f, g \in \mathrm{S}_k(\mathbb{C})$, choose $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ of finite index such that $f, g \in \mathrm{S}_k(\Gamma, \mathbb{C})$.

Proposition 2.5.3.

$$\langle f, g \rangle := \frac{1}{C(\Gamma)} \int_{\Gamma \backslash \mathcal{H}} \overline{f(z)} g(z) y^k \frac{dxdy}{y^2}$$

converges and is independent of the choice of Γ.

Proof. For $\gamma \in \Gamma$, we have

$$\overline{f(\gamma z)} = \overline{(cz+d)^k f(z)}, \quad g(\gamma z) = (cz+d)^k g(z),$$
$$\mathrm{Im}\,(\gamma z) = \frac{\mathrm{Im}\ z}{|cz+d|^2}.$$

so $\overline{f(z)} g(z) y^k$ is invariant under Γ. Now $\Gamma \backslash \mathcal{H} = \bigcup_{i \in I} \gamma_i D$ with $|I| = C(\Gamma)$. So if Γ' also satisfy that $f, g \in \mathrm{S}_k(\Gamma', \mathbb{C})$, then $f, g \in \mathrm{S}_k(\Gamma \cap \Gamma', \mathbb{C})$, and

$$\begin{aligned} \frac{1}{C(\Gamma)} \int_{\Gamma \backslash \mathcal{H}} \overline{f(z)} g(z) y^k \frac{dxdy}{y^2} &= \frac{1}{C(\Gamma \cap \Gamma')} \int_{(\Gamma \cap \Gamma') \backslash \mathcal{H}} \overline{f(z)} g(z) y^k \frac{dxdy}{y^2} \\ &= \frac{1}{C(\Gamma')} \int_{\Gamma' \backslash \mathcal{H}} \overline{f(z)} g(z) y^k \frac{dxdy}{y^2}. \end{aligned}$$

Because $f_{|k}\gamma_i$ and $g_{|k}\gamma_i$ are exponentially decreasing as $y \to \infty$ on D, $\langle f, g \rangle$ converges. □

Remark. In fact, we can choose one modular form and one cusp form, and the integral will still converge.

Proposition 2.5.4. *For* $f \in \mathrm{S}_k(1)$, *we have* $\langle G_k, f \rangle = 0$.

Proof. By definition,

$$G_k(z) = \frac{1}{2} \frac{\Gamma(k)}{(-2\pi i)^k} \sum_{m,n}{}' \frac{1}{(mz+n)^k} \in \mathrm{M}_k(1),$$

and

$$\begin{aligned} \sum_{m,n}{}' \frac{1}{(mz+n)^k} &= \sum_{a=1}^{\infty} \sum_{(m,n)=1} \frac{1}{(amz+an)^k} \\ &= \frac{\Gamma(k)}{(2\pi i)^k} \zeta(k) \sum_{\gamma \in \Gamma_\infty \backslash \mathrm{SL}_2(\mathbb{Z})} \frac{1}{(cz+d)^k}, \end{aligned}$$

where Γ_∞ denotes the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ consisting of all upper triangular matrices. So we just compute $\langle \sum_{\gamma\in\Gamma_\infty\backslash\mathrm{SL}_2(\mathbb{Z})} \frac{1}{(cz+d)^k}, f\rangle$. We have

$$\begin{aligned}
\langle \sum_{\gamma\in\Gamma_\infty\backslash\mathrm{SL}_2(\mathbb{Z})} \tfrac{1}{(cz+d)^k}, f\rangle &= \int_{\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}} \big(\sum_{\gamma\in\Gamma_\infty\backslash\mathrm{SL}_2(\mathbb{Z})} \tfrac{1}{\overline{(cz+d)}^k}\big) f(z) y^k \tfrac{dxdy}{y^2} \\
&= \int_{\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}} \sum_{\gamma\in\Gamma_\infty\backslash\mathrm{SL}_2(\mathbb{Z})} f(\gamma z)\,\mathrm{Im}\,(\gamma z)^k \tfrac{dxdy}{y^2} \\
&= \int_{\Gamma_\infty\backslash\mathcal{H}} f(z) y^k \tfrac{dxdy}{y^2} \\
&= \int_0^\infty \int_0^1 f(x+iy) y^{k-2} dxdy = 0,
\end{aligned}$$

where the last equality is because $a_0(f) = 0$ and $\int_0^1 e^{2\pi i n x}dx = 0$ for $n \geq 1$. □

Lemma 2.5.5. (i) *For $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$, we have*

$$\langle f_{|k}\alpha, g_{|k}\alpha\rangle = (\det\alpha)^{k-2}\langle f, g\rangle.$$

(ii) *Let $\alpha' = (\det\alpha)\alpha^{-1}$, then $\langle f_{|k}\alpha, g\rangle = \langle f, g_{|k}\alpha'\rangle$.*

Proof. (i) Choose Γ such that $f, g \in S_k(\Gamma)$ and $\alpha^{-1}\Gamma\alpha \subset \mathrm{SL}_2(\mathbb{Z})$, then

$$\begin{aligned}
C(\alpha^{-1}\Gamma\alpha)\langle f_{|k}\alpha, g_{|k}\alpha\rangle &= (\det\alpha)^{2(k-1)} \int_{\alpha^{-1}\Gamma\alpha\backslash\mathcal{H}} \overline{f(\alpha z)} g(\alpha z) \frac{y^k}{|cz+d|^{2k}} \frac{dxdy}{y^2} \\
&= (\det\alpha)^{k-2} \int_{\Gamma\backslash\mathcal{H}} \overline{f(z)} g(z) y^k \frac{dxdy}{y^2} \\
&= (\det\alpha)^{k-2} C(\Gamma)\langle f, g\rangle.
\end{aligned}$$

(ii) Replace g by $g_{|k}\alpha^{-1}$, then we get

$$\begin{aligned}
\langle f_{|k}\alpha, g\rangle &= (\det\alpha)^{k-2}\langle f, g_{|k}\alpha^{-1}\rangle \\
&= (\det\alpha)^{k-2}\langle f, g_{|k}\big(\tfrac{1}{\det\alpha}\alpha'\big)\rangle \\
&= \langle f, g_{|k}\alpha'\rangle.
\end{aligned}$$

□

2.6 Primitive forms

Theorem 2.6.1. (i) *If $n \geq 1$, then R_n and T_n are hermitian.*

(ii) *The eigenvalues of T_n are integers in a totally real field.*

(iii) *$S_k(1)$ has a basis of common eigenvectors for all T_n, $n \geq 1$.*

Proof. (i) It is trivial for R_n. Since $\mathbb{T}_{\mathbb{Z}}$ is generated by R_p and T_p for p prime, it suffices to consider T_p.

Let $\alpha \in \mathrm{M}_2(\mathbb{Z})$, $\det\alpha = p$, then there exist $\gamma_1,\ \gamma_2 \in \mathrm{SL}_2(\mathbb{Z})$ such that $\alpha = \gamma_1\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)\gamma_2$, then

$$\begin{aligned}
\langle f_{|k}\alpha, g\rangle &= \langle f_{|k}(\gamma_1\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)\gamma_2), g\rangle \\
&= \langle f_{|k}\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right), g_{|k}\gamma_2'\rangle \\
&= \langle f_{|k}\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right), g\rangle \\
&= \langle f, g_{|k}\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)\rangle,
\end{aligned}$$

thus $\langle f_{|k}T_p, g\rangle = (p+1)\langle f_{|k}\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right), g\rangle = \langle f, g_{|k}T_p\rangle$.

(ii) $S_k(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Z})$ is a lattice in $\mathrm{S}_k(1)$ stable under T_n, so $\det(XI - T_n) \in \mathbb{Z}[X]$, so the roots are algebraic integers, and real since T_n is hermitian.

(iii) $T_n{}'s$ are hermitian, hence they are semisimple. Since the T_n commute to each other, by linear algebra, there exists a common basis of eigenvectors for all T_n. □

Theorem 2.6.2. *Let* $f = \sum_{n=0}^{+\infty} a_n(f)q^n \in \mathrm{M}_k(1) - \{0\}$. *If for all* n, $f_{|k}T_n = \lambda_n f$, *then*

(i) $a_1(f) \neq 0$*;*

(ii) *if* f *is normalized, i.e.* $a_1(f) = 1$, *then* $a_n(f) = \lambda_n$, *for all* n, *and*

(*a*) $a_{mn}(f) = a_m(f)a_n(f)$ *when* $(m, n) = 1$.

(*b*) $a_p(f)a_{p^r}(f) = a_{p^{r+1}}(f) + p^{k-1}a_{p^{r-1}}(f)$ *for* p *prime and* $r \geq 1$.

Proof. (i) Since $a_n(f) = a_1(f_{|k}T_n) = a_1(\lambda_n f) = \lambda_n a_1(f)$, if $a_1(f) = 0$, then $f = 0$.

(ii) The first assertion is obvious, and the other two follow by the same formulae for the R_p, T_p. □

Definition 2.6.3. $f \in \mathrm{S}_k(1)$ is called *primitive* if $a_1(f) = 1$ and f is an eigenform for all Hecke operators.

Theorem 2.6.4. (i) *If* f, g *are primitive with the same set of eigenvalues, then* $f = g$. (*called "Multiplicity* 1 *theorem"*).

(ii) *The primitive forms are a basis of* $\mathrm{S}_k(1)$.

Proof. (i) Apply (i) of the previous theorem to $f - g$, since $a_1(f - g) = 0$, so $f = g$.

(ii) By (iii) of Theorem 2.6.1, there exists a basis of primitive forms. For any two distinct such forms f and f', then there exist n and $\lambda \neq \lambda'$ such that

$$f_{|k}T_n = \lambda f, \quad f'_{|k}T_n = \lambda' f,$$

then $\lambda\langle f, f'\rangle = \langle f_{|k}T_n, f'\rangle = \langle f, f'_{|k}T_n\rangle = \lambda'\langle f, f'\rangle$, so $\langle f, f'\rangle = 0$. Therefore one has to take all the primitive forms to get a basis of $\mathrm{S}_k(1)$. $\square$

Remark. Since $(G_k)_{|k}T_n = \sigma_{k-1}(n)G_k$, we get a basis of $M_k(1)$ of eigenforms.

Example 2.6.5. Write

$$\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n,$$

where $\tau(n)$ is Ramanujan's τ-function. Then

$$\tau(mn) = \tau(m)\tau(n), \qquad \text{if } (m,n)=1,$$

$$\tau(p)\tau(p^r) = \tau(p^{r+1}) + p^{11}\tau(p^{r-1}), \quad \text{if } p \text{ is a prime, } n \geq 1.$$

Proof. Since $\mathrm{S}_{12}(1) = \mathbb{C}\cdot\Delta$, and is stable by the T_n, Δ is an eigenform of T_n with eigenvalue $\tau(n)$. $\square$

Remark. In 1973, Deligne proved Ramanujan's conjecture that

$$|\tau(p)| \leq 2p^{11/2} (\Longleftrightarrow \mathrm{Re}\,(s) = 11/2, \quad \text{if } 1 - \tau(p)p^{-s} + p^{11-2s} = 0)$$

as a consequence of the proof of Riemann Hypothesis (Weil Conjecture) for zeta functions of varieties over finite fields.

Chapter 3

p-adic L-functions of modular forms

3.1 L-functions of modular forms.

3.1.1 Estimates for the fourier coefficients

Proposition 3.1.1. *Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a subgroup of finite index, let $f = \sum_{n \in \frac{1}{M}\mathbb{N}} a_n(f) q^n \in \mathrm{M}_k(\Gamma, \mathbb{C})$. Then*

(i)

$$a_n(f) = \begin{cases} O(n^{k-1}), & \text{if } k \geq 3; \\ O(n \log n), & \text{if } k = 2; \\ O(\sqrt{n}), & \text{if } k = 1. \end{cases}$$

(ii) $a_n(f) = O(n^{k/2})$, *if* $f \in \mathrm{S}_k(\Gamma)$.

Proof. We have that

$$a_n(f) = e^{2\pi n y} y^{-\frac{k}{2}} \frac{1}{M} \int_0^M y^{\frac{k}{2}} f(x+iy) e^{-2\pi i n x} dx, \quad \forall\ y.$$

Define

$$\varphi(z) = y^{\frac{k}{2}} \sup_{\delta \in \Gamma \backslash \mathrm{SL}_2(\mathbb{Z})} |f_{|k}\delta(z)|.$$

It is finite since $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma] < +\infty$, and $\varphi(\gamma z) = \varphi(z)$ for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

Let D be the fundamental domain of $\mathrm{SL}_2(\mathbb{Z})$. For any $\delta \in \Gamma\backslash\mathrm{SL}_2(\mathbb{Z})$, there exists C_δ such that, for all $z \in D$,

$$|f_{|k}\delta(z) - a_0(f_{|k}\delta)| \leq C_\delta e^{-\frac{2\pi y}{M}}.$$

Let $C = \sup_\delta C_\delta$, $\psi(z) = \sup_{(c,d)\neq(0,0)} \frac{y}{|cz+d|^2}$, then $\varphi(z) \leq C\psi(z)^{k/2} + B$ for some B.

$$\begin{aligned} a_n(f) &\leq e^{2\pi n y} y^{-\frac{k}{2}} \tfrac{1}{M} \int_0^M \varphi(x+iy)dx \\ &\leq e^{2\pi n y} y^{-\frac{k}{2}} \tfrac{1}{M} \int_0^M (C\psi(x+iy)^{k/2} + B)dx. \end{aligned}$$

If $C = 0$, take $y = \frac{1}{Mn}$, then we get (ii).

We now need to evaluate

$$\int_0^M \psi(x+iy)^{\frac{k}{2}}.$$

Let $y \leq 1$ (in application, $y = \frac{1}{Mn}$), then $\psi(x+iy) \leq \frac{1}{y}$. Let $j \in \mathbb{N}$. If $\psi(x+iy) \geq \frac{1}{4^j}y$, there exists (c,d) such that $c^2y^2 + (cx+y)^2 \leq 4^j y^2$, hence there exist c, $d \in \mathbb{Z}$, such that

$$1 \leq |c| \leq 2^j, \quad |cx+d| \leq 2^j y.$$

Now

$$\mathrm{Meas}(\{x \in [0,M] : \exists d, s.t. |cx+d| \leq 2^j y\}) \leq 2^{j+1} yM,$$

so $\mathrm{Meas}(\{x \in [0,M] : \psi(x+iy) \geq \frac{1}{4^j y}\}) \leq 4^j 2yM$, and

$$\begin{aligned} &\int_0^M \psi(x+iy)^{k/2}dx \\ &\quad \leq \sum_{j=1}^{[-\log_4 y]} \mathrm{Meas}(\{x \in [0,M] : \tfrac{1}{4^j y} \leq \psi(x+iy) \leq \tfrac{1}{4^{j-1}y}\})(\tfrac{1}{4^{j-1}y})^{k/2} \\ &\qquad + 4^{k/2}\mathrm{Meas}(\{x \in [0,M] : \psi(x+iy) \leq 4\}) \\ &\quad \leq M4^{k/2} + \sum_{j=1}^{[-\log_4 y]} 4^j 2yM(\tfrac{1}{4^{j-1}y})^{k/2} \\ &\quad = M4^{k/2}\big(1 + 2\sum_{j=1}^{[-\log_4 y]} y^{1-k/2} 4^{j(1-k/2)}\big). \end{aligned}$$

When $k \geq 3$, let $y = 1/Mn$. As $\sum_{j=1}^{[-\log_4 y]} 4^{j(1-k/2)}$ converges, we get $a_n(f) = O(n^{k-1})$. When $k = 2$, it is obvious. For $k = 1$, $\sum_{j=1}^{[-\log_4 y]} y^{1-k/2}4^{j(1-k/2)} < 2 - y^{1/2} < 2$, then we get the result. $\square$

Remark. (i) $L(f,s) = \sum_{n\neq 0} a_n(f)n^{-s}$ converges for $\mathrm{Re}\,(s) \gg 0$.

(ii) If Γ is a congruence subgroup, $f \in \mathrm{S}_k(\Gamma)$, Deligne showed that

$$a_n(f) = O(n^{(k-1)/2+\varepsilon}), \quad \forall\, \varepsilon > 0$$

in the same theorem mentioned above.

Question: What about the noncongruence subgroups?

3.1.2 Dirichlet series and Mellin transform

Definition 3.1.2. Let $\{a_n\}_{n\geq 1}$ be a sequence in $\mathbb{C}$, the *Dirichlet series* of (a_n) is $D(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$.

Lemma 3.1.3. *If $D(s_0)$ converges, then $D(s)$ converges uniformly on compact subsets of $\mathrm{Re}\,(s) > \mathrm{Re}\,(s_0)$.*

Proof. One can assume $s_0 = 0$, then use Abel's summation. $\square$

Corollary 3.1.4. *There exists a maximal half plane of convergence (resp. absolute convergence).*

Remark. (i) if $f(z) = \sum_{n=0}^{\infty} a_n z^n$, then the maximal open disc of convergence of f is the maximal open disc of absolute converge, and also is the maximal open disc of center 0 on which f can be extended analytically.

(ii) Let $a_n = (-1)^{n-1}$, then $D(s) = (1-2^{1-s})\zeta(s)$, which converges for $\mathrm{Re}\,(s) > 0$, absolutely converges $\mathrm{Re}\,(s) > 1$ and can be extended analytically to $\mathbb{C}$.

(iii) In general you can't extend $D(s)$ outside its half plane of absolute convergence, but for $D(s)$ coming from number theory, it seems that you can always extend meromorphically to $\mathbb{C}$ (Langlands program).

We review some basic facts about Mellin transform:

Proposition 3.1.5. (i) *Let $\varphi : \mathbb{R}_+^* \to \mathbb{C}$ be in $\mathcal{C}^r$, and suppose there exist $A > B$ satisfying, for $0 \leq i \leq n$,*

$$\varphi^{(i)}(t) = \begin{cases} O(t^{A-i}) & \textit{near } 0 \\ O(t^{B-i}) & \textit{near } \infty. \end{cases}$$

Let

$$\mathrm{Mel}(\varphi, s) := \int_0^\infty \varphi(t) t^s \frac{dt}{t}.$$

Then it is holomorphic on $-A < \mathrm{Re}\,(s) < -B$, *and* $O(|s|^{-r})$ *on* $-A < a \leq \mathrm{Re}\,(s) \leq b < -B$.

(ii) *If* $r \geq 2$, $\varphi(x) = \frac{1}{2\pi i} \int_{C-i\infty}^{C+i\infty} \mathrm{Mel}(\varphi, s) x^{-s} ds$, *for any* C *with* $-a < C < -B$.

Proof. (i) The first assertion is clear. For the second, use

$$\mathrm{Mel}(\varphi, s) = (-1)^r \frac{1}{s(s+1)\cdots(s+r-1)} \mathrm{Mel}(\varphi^{(r)}, s+r).$$

(ii) $\mathrm{Mel}(\varphi, C+it) = \hat{\psi}_C(t)$, where $\psi_C(x) = \varphi(e^x)e^{Cx}$, and $\hat{\psi}_C$ is the Fourier transform of ψ_C. Then use Fourier inversion formula. □

3.1.3 Modular forms and L-functions

For $f = \sum_{n=0}^{\infty} a_n(f) q^n \in \mathrm{M}_{2k}(1)$, define

$$L(f, s) = \sum_{n=1}^{\infty} \frac{a_n(f)}{n^s}, \quad \Lambda(f, s) = \frac{\Gamma(s)}{(2\pi)^s} L(f, s).$$

Example 3.1.6. Take $f = G_{2k}$, we get

$$\begin{aligned} L(G_{2k}, s) &= \sum_{n=1}^{\infty} \frac{\sigma_{2k-1}(n)}{n^s} = \sum_{n=1}^{\infty} \Big(\sum_{ad=n} d^{2k-1} \Big) (ad)^{-s} \\ &= \Big(\sum_{a=1}^{\infty} a^{-s} \Big) \Big(\sum_{d=1}^{\infty} d^{2k-1-s} \Big) = \zeta(s)\zeta(s-2k+1). \end{aligned}$$

Theorem 3.1.7. (i) $L(f, s)$ *absolutely converges for* $\mathrm{Re}\,(s) > 2k$;

(ii) (*a*) $\Lambda(f, s)$ *has a meromorphic continuation to* $\mathbb{C}$;

(*b*) $\Lambda(f, s)$ *is holomorphic except for simple poles at* $s = 0$ *of residue* $a_0(f)$ *and* $2k$ *of residue* $(-1)^k a_0(f)$;

(*c*) $\Lambda(f, 2k-s) = (-1)^k \Lambda(f, s)$;

(*d*) $\Lambda(f, s)$ *goes to zero at* ∞ *in each vertical strip.*

Proof. (i) The result follows from $a_n(f) = O(n^{2k-1})$.

(ii) Let $\varphi(t) = f(it) - a_0(f)$, then φ is C^∞ on $\mathbb{R}_+^*$, and $\varphi(t) = O(e^{-2\pi t})$ at ∞. $f \in \mathrm{M}_{2k}(1)$ implies

$$\varphi(t^{-1}) = (-1)^k t^{2k}\varphi(t) + (-1)^k a_0(f) t^{2k} - a_0(f).$$

For $\mathrm{Re}\,(s) > 0$, we have $\int_0^{+\infty} e^{-2\pi n t} t^s \frac{dt}{t} = \frac{\Gamma(s)}{(2\pi n)^s}$. Then for $\mathrm{Re}\,(s) > k$,

$$\begin{aligned}
\Lambda(f,s) &= \sum_{n=1}^{\infty} a_n(f) \tfrac{\Gamma(s)}{(2\pi n)^s} \\
&= \int_0^{+\infty} \varphi(t) t^s \tfrac{dt}{t} \\
&= \int_1^{+\infty} \varphi(t) t^s \tfrac{dt}{t} + \int_1^{+\infty} \varphi(t^{-1}) t^{-s} \tfrac{dt}{t} \\
&= \int_1^{+\infty} \varphi(t)(t^s + (-1)^k t^{2k-s}) \tfrac{dt}{t} - a_0(f)\big(\tfrac{(-1)^k}{2k-s} + \tfrac{1}{s}\big), \quad (*)
\end{aligned}$$

since the first term is holomorphic for all $s \in \mathbb{C}$, this gives (a) and (b). Replacing s by $2k - s$ in $(*)$, we get (c). (d) follows from integration by part. $\square$

Theorem 3.1.8 (Hecke's converse theorem). *Let $(c_n)_{n\in\mathbb{N}}$ be a sequence in $\mathbb{C}$ such that $L(s) = \sum_{n=1}^{\infty} \frac{c_n}{n^s}$ converges for $\mathrm{Re}\,(s) > A$, and $\Lambda(s) = \frac{\Gamma(s)}{(2\pi)^s} L(s)$ satisfy (ii)(a) – (d) of previous theorem, then*

$$f(z) := \sum_{n=0}^{\infty} c_n q^n \in \mathrm{M}_{2k}(1).$$

Proof. Since $f(z)$ converges if $|q| < 1$, it is holomorphic on $\mathcal{H}$. Obviously $f(z+1) = f(z)$, we just have to verify

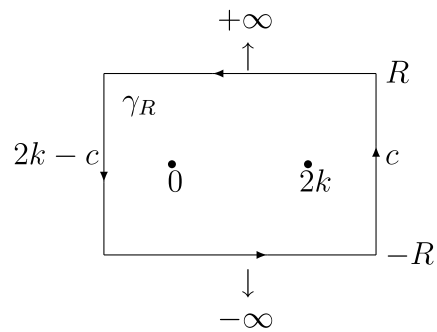
$$g(z) = f(-\frac{1}{z}) - z^{2k} f(z) = 0 \qquad \text{on } \mathcal{H}.$$

It suffices to prove that $g(it) = 0$ for $t > 0$. Let

$$\varphi(t) = f(it) - c_0 = \sum_{n=1}^{\infty} c_n e^{-2\pi n t},$$

one can check that $\Lambda(s) = \mathrm{Mel}(\varphi, s)$. Take $c > A$, then

$$\begin{aligned}
&\varphi(t) - \tfrac{(-1)^k}{t^{2k}} \varphi(t^{-1}) \\
&\quad = \tfrac{1}{2\pi i}\big(\int_{c-i\infty}^{c+i\infty} \Lambda(s) t^{-s} ds - (-1)^k \int_{c-i\infty}^{c+i\infty} \Lambda(s) t^{s-2k} ds \big) \\
&\quad = \tfrac{1}{2\pi i}\big(\int_{c-i\infty}^{c+i\infty} \Lambda(s) t^{-s} ds - \int_{c-i\infty}^{c+i\infty} \Lambda(2k-s) t^{s-2k} ds \big) \\
&\quad = \tfrac{1}{2\pi i}\big(\int_{c-i\infty}^{c+i\infty} \Lambda(s) t^{-s} ds - \int_{2k-c-i\infty}^{2k-c+i\infty} \Lambda(s) t^{-s} ds \big).
\end{aligned}$$



Consider the integral of the function $\Lambda(s)t^{-s}$ around the closed path γ. Since $\Lambda(s) \to 0$ on vertical strips, by Cauchy formula,

$$\begin{aligned}\lim_{R\to+\infty} \int_{\gamma_R} \Lambda(s)t^{-s}ds &= \int_{c-i\infty}^{c+i\infty} \Lambda(s)t^{-s}ds - \int_{2k-c-i\infty}^{2k-c+i\infty} \Lambda(s)t^{-s}ds \\ &= 2\pi i\big(\mathrm{res}_{s=0}(\Lambda(s)t^{-s}) + \mathrm{res}_{s=2k}(\Lambda(s)t^{-s})\big) \\ &= 2\pi i(-c_0 + (-1)^k c_0 t^{-2k}).\end{aligned}$$

So

$$\varphi(t) - \frac{(-1)^k}{t^{2k}}\varphi(t^{-1}) - (-c_0 + (-1)^k c_0 t^{-2k}) = 0,$$

by an easy computation, the left hand is just $\frac{(-1)^k}{t^{2k}}(-g(it))$, then we get $g(it) = 0$, which completes the proof. □

3.1.4 Euler products

Theorem 3.1.9. *If* $f = \sum_{n=0}^{\infty} a_n(f)q^n \in \mathrm{M}_{2k}(1)$ *is primitive, then*

$$L(f,s) = \prod_p \frac{1}{1 - a_p(f)p^{-s} + p^{2k-1-2s}}.$$

Proof. By Theorem 2.6.2, $a_{nm}(f) = a_n(f)a_m(f)$ whenever $(n,m) = 1$, so

$$L(f,s) = \prod_p \big(\sum_{r=0}^{\infty} a_{p^r}(f)p^{-rs}\big).$$

Since,

$$a_{p^{r+1}} - a_p a_{p^r} + p^{2k-1}a_{p^{r-1}} = 0,$$

multiplying by $p^{-(r+1)s}$, and summing over r from 1 to $+\infty$, we get

$$\sum_{r=2}^{\infty} a_{p^r} p^{-rs} - a_p p^{-s} \sum_{r=1}^{\infty} a_{p^r} p^{-rs} + p^{2k-1-2s} \sum_{r=0}^{\infty} a_{p^r} p^{-rs} = 0.$$

Using the fact that $a_1 = 1$, the result follows. $\square$

3.2 Higher level modular forms

3.2.1 Summary of the results

For $N \geq 2$, define

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \ c \equiv 0 \pmod{N} \right\}.$$

and write $\mathrm{S}_k(\Gamma_0(N)) = \mathrm{S}_k(N)$.

Exercise. If $DM|N$, $f \in \mathrm{S}_k(M)$, let $f_D(z) = f(Dz)$, then $f_D \in \mathrm{S}_k(N)$. Such a form is said to be *old* if $M \neq N$.

Definition 3.2.1. $\mathrm{S}_k^{\mathrm{new}}(N) = \{f \in \mathrm{S}_k(N) : \ \langle f, g \rangle = 0, \forall\ g \text{ “old”}\}$.

On $\mathrm{S}_k(N)$, we have the Hecke operators T_n, $(n, N) = 1$,

$$f_{|k} T_n = n^{k-1} \sum_{\substack{ad=n, a>1 \\ b \bmod d}} d^{-k} f\left(\frac{az+b}{d}\right),$$

and for $p \mid n$, the operator

$$f_{|k} U_p = \frac{1}{p} \sum_{i=0}^{p-1} f\left(\frac{z+i}{p}\right).$$

We also have a involution w_N given by

$$f_{|k} w_N = N^{-\frac{k}{2}} z^{-k} f\left(-\frac{1}{Nz}\right).$$

Definition 3.2.2. $f \in \mathrm{S}_k(N)$ is called *primitive* if $f \in \mathrm{S}_k^{\mathrm{new}}(N)$, $a_1(f) = 1$ and $f_{|k} T_n = a_n(f) f$, whenever $(n, N) = 1$.

Theorem 3.2.3. (i) *The primitive forms are a basis of* $\mathrm{S}_k^{\mathrm{new}}(N)$.

(ii) *If f is primitive, then $\mathbb{Q}(\{a_n(f)\}, n \in \mathbb{N})$ is a totally real number field, $a_n(f)$ are integers, and f^σ is primitive for all $\sigma \in \mathrm{Aut}(\mathbb{C})$.*

(iii) *If f is primitive, then*

(a) $a_{nm}(f) = a_n(f)a_m(f)$ *if* $(n,m) = 1$, $(nm, N) = 1$;

(b) *For* $p \nmid N$, $a_{p^{r+1}} - a_p(f)a_{p^r(f)} + p^{k-1}a_{p^{r-1}}(f) = 0$.

(c) $f_{|k}U_p = a_p(f)f$, *and this implies* $a_{p^r}(f) = (a_p(f))^r$ *for* $p|N$;

(d) *There exists* $\varepsilon_f = \pm 1$, *such that* $f_{|k}w_N = \varepsilon_f f$.

Theorem 3.2.4. *Suppose* $f = \sum\limits_{n=1}^{\infty} a_n q^n \in \mathrm{S}_k(N)$ *is primitive. Define*

$$L(f,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \quad \Lambda(f,s) = \Gamma(s)\Big(\frac{\sqrt{N}}{2\pi}\Big)^s L(f,s).$$

Then

(i) $L(f,s) = \prod\limits_{p|N} \frac{1}{1-a_p p^{-s}} \prod\limits_{p\nmid N} \frac{1}{1-a_p p^{-s}+p^{k-1-2s}}$;

(ii) $\Lambda(s)$ *has an analytic continuation to* $\mathbb{C}$. *And*

$$\Lambda(f,s) = i^{-k}\varepsilon_f \Lambda(f, k-s);$$

(iii) *More generally, if* $(D,N) = 1$, $\chi :\ (\mathbb{Z}/D\mathbb{Z})^* \to \mathbb{C}$ *is a character of conductor* D. *Then*

(a) $f \otimes \chi = \sum\limits_{n=1}^{\infty} a_n \chi(n) q^n \in \mathrm{S}_k(ND^2, \chi^2)$;

(b) $L(f\otimes\chi, s) = \prod\limits_{p|N} \frac{1}{1-\chi(p)a_p p^{-s}} \prod\limits_{p\nmid N} \frac{1}{1-\chi(p)a_p p^{-s}+\chi^2(p)p^{k-1-2s}}$;

(c) $\Lambda(f\otimes\chi, s) = \Gamma(s)\big(\frac{D\sqrt{N}}{2\pi}\big)^s L(f\otimes\chi, s)$ *has a analytic continuation to* $\mathbb{C}$ *and*

$$\chi(-N)\frac{\Lambda(f\otimes\chi, s)}{G(x)} = i^{-k}\varepsilon_f \frac{\Lambda(f\otimes\chi^{-1}, s)}{G(\chi^{-1})}$$

where $G(\chi)$ *is the Gauss sum*

$$G(\chi) = \sum_{x\in(\mathbb{Z}/D\mathbb{Z})^*} \chi(x)e^{\frac{2\pi i x}{D}}.$$

Theorem 3.2.5 (Weil's Converse Theorem). *Conversely, if* $(a_m)_{m\geq 1}$ *satisfy (b) and (c) of condition (iii) of the above theorem for all* χ *of conductor* D, $(D,N) = 1$, *then* $\sum\limits_{m=1}^{\infty} a_m q^m \in \mathrm{S}_k(N)$ *and is primitive.*

3.2.2 Taniyama-Weil Conjecture

Let Λ be a finitely generated $\mathbb{Z}$-algebra. Define its Hasse-Weil zeta function $\zeta_\Lambda(s)$ by

$$\zeta_\Lambda(s) = \prod_{\wp \text{ prime in } \Lambda} \frac{1}{(1 - |\Lambda/\wp|^{-s})}.$$

Conjecture 3.2.6 (Hasse-Weil). *ζ_Λ has a meromorphic continuation to $\mathbb{C}$.*

Let $E : y^2 = x^3 + ax^2 + bx + c$, $a, b, c \in \mathbb{Q}$ be an elliptic curve, $\Lambda_E = \mathbb{Z}[x, y]/(y^2 - x^3 - ax^2 - bx - c)$ be its coordinate ring, which is a finitely generated algebra over $\mathbb{Z}$.

Theorem 3.2.7 (Wiles, Breuil-Conrad-Diamond-Taylor). *There exists a unique N_E and $f_E \in \mathrm{S}_2(N_E)$ which is primitive, such that*

$$\zeta_{\Lambda_E} \sim \frac{\zeta(s-1)}{L(f_E, s)}$$

while $\sim$ means up to multiplication by a finite numbers of Euler factors.

Remark. This proves Hasse-Weil conjecture in this case thanks to theorem 3.2.4.

Theorem 3.2.8 (Mordell-Weil). *$E(\mathbb{Q}) \cup \{\infty\} \simeq \mathbb{Z}^{r(E)} \oplus$ finite group.*

Conjecture 3.2.9 (Birch,Swinnerton-Dyer). $\mathrm{ord}_{s=1} L(f_E, s) = r(E)$.

3.3 Algebraicity of special values of L-functions

3.3.1 Modular symbols.

Let $N \geq 1$, $f \in \mathrm{S}_k(N)$, $P \in A[x]^{(k-2)}$ (polynomials of degree $\leq k-2$) with $A \subset \mathbb{C}$ a subring. For $r \in \mathbb{Q}$, the integral $\int_r^{i\infty} f(z)P(z)dz$ converges because f is exponentially small around $i\infty$ and r. These integrals are called modular symbols.

For $0 \leq j \leq k-2$, define

$$r_j(f) = \int_0^{i\infty} f(z) z^j dz = \frac{\Gamma(j+1)}{(-2\pi i)^{j+1}} L(f, j+1).$$

Let L_f be the $\mathbb{Z}$-module generated by $r_j(f_{|k}\delta)$, $1 \leq j \leq k-2$ and $\delta \in \Gamma_0(N)\backslash \mathrm{SL}_2(\mathbb{Z})$. Then L_f is finitely generated.

Theorem 3.3.1. *If $P \in A[x]^{(k-2)}$, $r \in \mathbb{Q}$, then $\int_r^{i\infty} f(z)P(z)dz \in \mathbb{A}\cdot L_f \subset \mathbb{C}$.*

Proof. For $\gamma \in \mathrm{SL}_2(\mathbb{Z})$,

$$\begin{aligned}\int_{\gamma(0)}^{\gamma(i\infty)} f(z)P(z)dz &= \int_0^{i\infty} f(\gamma z)P(\gamma z)d(\gamma z)\\ &= \int_0^{i\infty} f_{|k}\gamma(z)P_{|2-k}\gamma(z)dz,\end{aligned}$$

where $P_{|2-k}\gamma(z) = (cz+d)^{k-2}P(\frac{az+b}{cz+d}) \in A[x]^{(k-2)}$. Take $r = a/b$, $(a,b) = 1$, then there exists $\gamma_l = \begin{pmatrix} a_{l-1} & a_l \\ b_{l-1} & b_l \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ satisfying $(a_0, b_0) = (1, 0)$, $(a_n, b_n) = (a, b)$.

$$\begin{aligned}\int_r^{i\infty} f(z)P(z)dz &= \sum_{l=1}^{n} \int_{\frac{a_l}{b_l}}^{\frac{a_{l-1}}{b_{l-1}}} f(z)P(z)dz\\ &= \sum_{l=1}^{n} \int_{\gamma_l(0)}^{\gamma_l(i\infty)} f(z)P(z)dz\\ &= \sum_{l=1}^{n} \int_0^{i\infty} f_{|k}\gamma_l(z)P_{|2-k}\gamma_l(z)dz \in A\cdot L_f.\end{aligned}$$

□

Exercise. For $N = 1$, let L_f^+ (resp. L_f^-) be the $\mathbb{Z}$-module generated by $r_j(f)$ for all odd (resp. even) j. For $P \in A[X]^{(k-2)}$, $r \in \mathbb{Q}$, $\varepsilon = \pm$, then

$$\int_r^{i\infty} f(z)P(z)dz - \varepsilon\int_{-r}^{i\infty} f(z)P(-z)dz \in A\cdot L_f^{\varepsilon}.$$

Corollary 3.3.2. (i) *Suppose $f \in \sum_{n=1}^{\infty} a_n q^n$, $\phi: \mathbb{Z} \to \bar{\mathbb{Q}}$ is constant* mod *$M\mathbb{Z}$ for some M. Then $L(f,\phi,s) = \sum_{n=1}^{\infty}\phi(n)\frac{a_n}{n^s}$ has an analytic continuation to $\mathbb{C}$ and*

$$\Lambda(f,\phi,j) = \frac{\Gamma(j)}{(-2\pi i)^j}L(f,\phi,j) \in \bar{\mathbb{Q}}\cdot L_f,$$

if $1 \le j \le k-1$.

(ii) *If $N = 1$ and $\phi(-x) = \varepsilon(-1)^j\phi(x)$, then $\Lambda(f,\phi,j) \in \bar{\mathbb{Q}}\cdot L_f^{\varepsilon}$, if $1 \le j \le k-1$.*

Proof. we may assume $\phi(n) = e^{2\pi i \frac{nu}{M}}$ for some $0 \le u \le M-1$ because such functions form a basis, then

$$\begin{aligned}\frac{\Gamma(s)}{(2\pi)^s} L(f,\phi,s) &= \int_0^{+\infty} \sum_{n=1}^{\infty} a_n e^{2\pi i \frac{nu}{M}} e^{-2\pi n y} y^s \frac{dy}{y} \\ &= \int_0^{+\infty} f(\tfrac{u}{M} + iy) y^s \frac{dy}{y},\end{aligned}$$

this proves the first assertion of (i) as f is exponentially small around $i\infty$ and $\frac{u}{M}$.

$$\begin{aligned}\Lambda(f,\phi,j) &= \int_0^{+\infty} f(\tfrac{u}{M} + iy)(iy)^j \frac{d(iy)}{iy} \\ &= \int_{\frac{u}{M}}^{i\infty} f(z)(z - \tfrac{u}{M})^{j-1} dz \\ &\in \mathbb{Q} \cdot L_f.\end{aligned}$$

For (ii), we may assume $\phi(n) = e^{2\pi i \frac{nu}{M}} + \varepsilon(-1)^j e^{-2\pi i \frac{nu}{M}}$, and similarly,

$$\begin{aligned}\Lambda(f,\phi,j) &= \int_{\frac{u}{M}}^{i\infty} f(z)(z - \tfrac{u}{M})^{j-1} dz + \varepsilon(-1)^j \int_{-\frac{u}{M}}^{i\infty} f(z)(z + \tfrac{u}{M})^{j-1} dz \\ &= \int_{\frac{u}{M}}^{i\infty} f(z)(z - \tfrac{u}{M})^{j-1} dz - \varepsilon \int_{-\frac{u}{M}}^{i\infty} f(z)(-z - \tfrac{u}{M})^{j-1} dz,\end{aligned}$$

then one uses the exercise. □

3.3.2 The results

Theorem 3.3.3. *If f is primitive, then there exist Ω_f^+ and $\Omega_f^- \in \mathbb{C}$, if*

$$\phi : \mathbb{Z} \to \bar{\mathbb{Q}} \pmod{M\mathbb{Z}},\ 1 \le j \le k-1,\ \phi(x) = \varepsilon(-1)^j \phi(-x),$$

then $\Lambda(f,\phi,j) \in \bar{\mathbb{Q}} \cdot \Omega_f^\varepsilon$.

Proof. We prove the case $N = 1,\ \varepsilon = 1$.

We shall prove that

$$r_{k-2}(f) r_l(f) \in \bar{\mathbb{Q}}\langle f, f\rangle, \text{ for } l \text{ odd.} \tag{3.1}$$

This implies

$$\Omega_f^+ \sim \frac{\langle f, f\rangle}{r_{k-2}(f)} \sim \frac{\langle f, f\rangle}{L(f, k-1)} \pi^{k-2}$$

where $\sim$ stands for equality up to multiplication by an algebraic number. The method to show (3.1) is the *Rankin's method* in the following section. □

3.3.3 Rankin's method

Assume $k = l + j$ for $k, l, j \in \mathbb{N}$. Suppose $\chi_1, \chi_2 : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ are multiplicative characters. Let

$$f = \sum_{n=1}^{+\infty} a_n q^n \in S_k(N, \chi_1^{-1}), \quad g = \sum_{n=0}^{+\infty} b_n q^n \in M_l(N, \chi_2).$$

So

$$f(\gamma z) = \chi_1^{-1}(d)(cz+d)^k f(z), \quad g(\gamma z) = \chi_2(d)(cz+d)^l g(z).$$

Let

$$\begin{aligned} G_{j,\chi_1\chi_2,s}(z) =& \frac{1}{2} \cdot \frac{\Gamma(j)}{(-2\pi i)^j} \cdot \sum_{\substack{N|m \\ (N,n)=1}}{}' \frac{\chi_1\chi_2(n) y^{s+1-k}}{(mz+n)^j \mid mz+n \mid^{2(s+1-k)}} \\ =& \frac{\Gamma(j)}{(-2\pi i)^j} L(\chi_1\chi_2, j+2(s+1-k)) \cdot \sum_{\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_\infty \backslash \Gamma_0(N)} \frac{\chi_1\chi_2(d)}{(cz+d)^j} \cdot \mathrm{Im}\,(\gamma z)^{s+1-k}. \end{aligned}$$

We have

Proposition 3.3.4.

$$\begin{aligned} D(f,g,s) &= L(\chi_1\chi_2, j+2(s+1-k)) \sum_{n=1}^{+\infty} \frac{\bar{a}_n b_n}{n^s} \\ &= \frac{(4\pi)^s}{\Gamma(s)} \frac{(-2\pi i)^j}{\Gamma(j)} \cdot \langle f, gG_j, \chi_1\chi_2, s \rangle \cdot [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)]. \end{aligned}$$

Proof. Using the Fourier expansion, then

$$\begin{aligned} \sum_{n=1}^{+\infty} \frac{\bar{a}_n b_n}{n^s} &= \frac{\Gamma(s)}{(4\pi)^s} \int_0^{+\infty} \int_0^1 \overline{f(z)} g(z)\ dx \cdot y^s\ \frac{dy}{y} \\ &= \frac{\Gamma(s)}{(4\pi)^s} \int_{\Gamma_\infty \backslash \mathcal{H}} \overline{f(z)} g(z) y^{s+1}\ \frac{dxdy}{y^2} \\ &= \frac{\Gamma(s)}{(4\pi)^s} \int_{\Gamma_0(N) \backslash \mathcal{H}} \sum_{\gamma \in \Gamma_\infty \backslash \Gamma_0(N)} (\overline{f(\gamma z)} g(\gamma z)\, \mathrm{Im}\,(\gamma z)^{s+1})\ \frac{dxdy}{y^2} \\ &= \frac{\Gamma(s)}{(4\pi)^s} \int_{\Gamma_0(N) \backslash \mathcal{H}} \overline{f(z)} \Big(g(z) \sum_{\gamma \in \Gamma_\infty \backslash \Gamma_0(N)} \frac{\chi_1\chi_2(d)}{(cz+d)^j}\, \mathrm{Im}\,(\gamma z)^{s+1-k} \Big) y^k\ \frac{dxdy}{y^2}, \end{aligned}$$

this implies the Proposition. $\square$

Theorem 3.3.5. (i) *$D(f, g, s)$ admits a meromorphic continuation to $\mathbb{C}$, which is holomorphic outside a simple pole at $s = k$ if $l = k$ and $\chi_1\chi_2 = 1$*

(ii) *if f is primitive, $g \in M_l(N, \chi_2, \bar{\mathbb{Q}})$, then*

$$D(f, g, k-1) \in \bar{\mathbb{Q}} \cdot \pi^{j+k-1}\langle f, f\rangle.$$

Proof. As $D(f, g, s) = \langle f, gG_s\rangle$,

(i) we have to prove the same statement for G_s, which can be done by computing its Fourier extension. The pole comes from the constant Fourier coefficients.

(ii) For the case $N = 1$,$\chi_1 = \chi_2 = 1$ and $j \geq 3$, then $G_{j,\chi_1\chi_2,k-1} = G_j$, we are reduced to prove

$$\langle f, gG_j\rangle \in \bar{\mathbb{Q}}\langle f, f\rangle.$$

Let f_i, $i \in I$ be a basis of $S_k(1)$ of primitive forms, with $f_1 = f$. As $gG_j \in M_k(1, \bar{\mathbb{Q}})$, we can write $gG_j = \lambda_0 G_k + \sum_i \lambda_i f_i$, with $\lambda_i \in \bar{\mathbb{Q}}$. Since

$$\langle G_k, f\rangle = 0, \quad \langle f, f_j\rangle = 0, \text{ if } j \neq 1,$$

Then $\langle f, gG_j\rangle = \lambda_1\langle f, f\rangle$.

□

Remark. The general case can be treated in the same way, once we prove that

$$G_{j,\chi_1\chi_2,k-1} \in M_j(N, \chi_1\chi_2, \bar{\mathbb{Q}}) \text{ (if } j \neq 2 \text{ or } \chi_1\chi_2 \neq 1).$$

Proposition 3.3.6. *If*

$$\sum_{n=1}^{+\infty} \frac{\bar{a}_n}{n^s} = \Big(\sum_{n\in\mathbb{Z}[\frac{1}{N}]^\times} \frac{\bar{a}_n}{n^s}\Big)\prod_{p\nmid N}\frac{1}{(1-\alpha_p p^{-s})(1-\beta_p p^{-s})}, \ \alpha_p\beta_p = \chi_1(p)p^{k-1},$$

$$\sum_{n=1}^{+\infty} \frac{b_n}{n^s} = \Big(\sum_{n\in\mathbb{Z}[\frac{1}{N}]^\times} \frac{b_n}{n^s}\Big)\prod_{p\nmid N}\frac{1}{(1-\gamma_p p^{-s})(1-\delta_p p^{-s})}, \ \gamma_p\delta_p = \chi_2(p)p^{l-1},$$

then $D(f, g, s) =$

$$\Big(\sum_{n\in\mathbb{Z}[\frac{1}{N}]^\times} \frac{\bar{a_n}b_n}{n^s}\Big)\prod_{p\nmid N}\frac{1}{(1-\alpha_p\gamma_p p^{-s})(1-\beta_p\gamma_p p^{-s})(1-\alpha_p\delta_p p^{-s})(1-\beta_p\delta_p p^{-s})}.$$

Proof. Exercice, noting that

$$\bar{a}_{p^r} = \frac{\alpha_p^{r+1} - \beta_p^{r+1}}{\alpha_p - \beta_p}, \quad b_{p^r} = \frac{\gamma_p^{r+1} - \delta_p^{r+1}}{\gamma_p - \delta_p}.$$

□

We give one application here:

Corollary 3.3.7. *The claim* (3.1) *holds, i.e.*

$$r_{k-2}(f) r_l(f) \in \bar{\mathbb{Q}}\langle f, f\rangle, \text{ for } l \text{ odd}.$$

Proof. Let $f \in S_k(1)$ be primitive, k given. For l even, let $g = G_l$, then

$$\sum_{n=1}^{+\infty} \frac{b_n}{n^s} = \prod_p \frac{1}{(1-p^{-s})(1-p^{l-s-1})},$$

hence $D(f, G_l, s) = L(f, s)L(f, s-l+1)$. Therefore

$$L(f, k-1)L(f, k-l) \in \bar{\mathbb{Q}} \cdot \pi^{j+k-1}\langle f, f\rangle$$

which implies

$$r_{k-2}(f) r_{k-l-1}(f) \in \bar{\mathbb{Q}}\langle f, f\rangle.$$

□

Remark. In the general case,

$$L(G_j, \chi_1\chi_2, k-1, s) \sim \zeta(s) L(\chi_1\chi_2, s-l+1).$$

If $f_1, f_2, \cdots, f_n$ are primitive forms $\in S_k(N_i)$ for $N_i \mid N$. Write

$$L(f_i, s) = *\prod_{p \nmid N} \frac{1}{(1-\alpha_{p,1}^{(i)} p^{-s})(1-\alpha_{p,2}^{(i)} p^{-s})},$$

then

$$L(f_1 \otimes \cdots \otimes f_n, s) = *\prod_{p \nmid N} \frac{1}{\prod_{j_1, j_2, \cdots, j_n \in \{1,2\}} (1-\alpha_{p,j_1}^{(1)} \cdots \alpha_{p,j_n}^{(n)} p^{-s})}.$$

One has the following conjecture:

Conjecture 3.3.8 (Part of Langlands Program). *$L(f_1 \otimes \cdots \otimes f_n, s)$ has a meromorphic continuation to $\mathbb{C}$, and is holomorphic if $f_i \neq \bar{f}_j$, for all $i \neq j$.*

Remark. Rankin's method implies the above conjecture is OK for $n = 2$. The case for $n = 3$ is due to Paul Garrett. The case for $n \geq 4$ is still open.

3.4 p-adic L-functions of modular forms

In the following, we assume $f \in S_k(N)$ is primitive.

Definition 3.4.1. $\phi^+(x) = \frac{1}{2}(\phi(x) + \phi(-x))$, $\phi^-(x) = \frac{1}{2}(\phi(x) - \phi(-x))$. Then

$$\tilde{\Lambda}(f, \phi, j) = \frac{\Lambda(f, \phi^+, j)}{\Omega_f^{(-1)^j}} + \frac{\Lambda(f, \phi^-, j)}{\Omega_f^{(-1)^{j+1}}} \in \bar{\mathbb{Q}}$$

if $\phi : \mathbb{Z} \to \bar{\mathbb{Q}}$ and $1 \leq j \leq k-1$.

Fix an embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$. The function $L(f, s)$ has an Euler product

$$L(f, s) = \prod_{\ell \text{ prime}} \frac{1}{E_\ell(s)},\ E_\ell(s) \in \bar{\mathbb{Q}}[\ell^{-s}],\ \deg E_\ell(s) \leq 2.$$

Write $E_p(s) = (1 - \alpha p^{-s})(1 - \beta p^{-s})$ and assume $\alpha \neq 0$. Then $\beta = 0$ if and only if $p \mid N$. Set

$$f_\alpha(z) = f(z) - \beta f(pz).$$

Lemma 3.4.2. *$f_\alpha|_k U_p = \alpha f_\alpha$ in all cases.*

Proof. It is clear if $p \mid N$ as in the case $\beta = 0$. If $p \nmid N$, then

$$\alpha + \beta = a_p, \quad \alpha\beta = p^{k-1}.$$

and $f|_k T_p = (\alpha + \beta) f$, thus

$$\begin{aligned} f_\alpha|_k U_p - \alpha f_\alpha =& \frac{1}{p} \sum_{i=0}^{p-1} f\left(\frac{z+i}{p}\right) - \beta f(z+i) - \alpha f(z) + \alpha\beta f(pz) \\ =& -(\alpha+\beta) f(z) + f_k T_p = 0. \end{aligned}$$

□

If we write $f_\alpha = \sum_{n=1}^{+\infty} b_n q^n$, the above lemma implies that $b_{np} = \alpha b_n$ for all n. Define b_n for $n \in \mathbb{Z}\left[\frac{1}{p}\right]$ as

$$b_n = \alpha^{-r} b_{p^r n},\ r \gg 0.$$

Take $\phi \in LC_c(\mathbb{Q}_p, \bar{\mathbb{Q}})$ a locally constant function with compact support and let

$$L(f, \phi, s) = \sum_{n \in \mathbb{Z}\left[\frac{1}{p}\right]} \phi(n) \frac{a_n}{n^s}.$$

If ϕ has support in $p^{-r}\mathbb{Z}_p$, then $\phi(x) = \phi_0(p^r x)$ for $\phi_0 : \mathbb{Z} \to \bar{\mathbb{Q}}$ constant mod $p^m\mathbb{Z}$ for some m.Then

$$L(f, \phi, s) = \alpha^{-r} p^{rs} L(f, \phi_0, s)$$

which implies

$$\tilde{\Lambda}(f, \phi, j) \in \bar{\mathbb{Q}} \subset \bar{\mathbb{Q}_p}, \text{ for all } \phi \in LC_c(\mathbb{Q}_p, \bar{\mathbb{Q}}).$$

Definition 3.4.3. Assume $\phi \in LC_c(\mathbb{Q}_p, \bar{\mathbb{Q}})$ and ϕ is constant modulo $p^n\mathbb{Z}$. The *discrete Fourier transform* of ϕ is

$$\hat{\phi}(x) = p^{-m} \sum_{y \bmod p^m} \phi(y) e^{-2\pi i x y},$$

for $m \geq n - v_p(x)$, where $xy \in \mathbb{Q}_p \to \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow \mathbb{Q}/\mathbb{Z}$. This definition does not depend on the choice of $m \geq n - v_p(x)$.

Exercise. (i) $\hat{\phi}$ is constant mod $p^m\mathbb{Z}_p$ if and only if ϕ has support in $p^{-m}\mathbb{Z}_p$.

(ii) $\hat{\hat{\phi}}(x) = \phi(-x)$.

(iii) For $a \in \mathbb{Q}_p$, let $\phi_a(x) = \phi(ax)$, then $\widehat{\phi_a}(x) = p^{v_p(a)} \hat{\phi}\left(\frac{x}{a}\right)$.

Theorem 3.4.4. (i) *There exists a unique $\mu_{f,\alpha} : LP^{[0,k-2]}(\mathbb{Z}_p, \bar{\mathbb{Q}}_p) \to \bar{\mathbb{Q}}_p$, such that for all $\phi \in LC(\mathbb{Z}_p, \bar{\mathbb{Q}})$,*

$$\int_{\mathbb{Z}_p} \phi(x) x^{j-1} \mu_{f,\alpha} = \tilde{\Lambda}(f_\alpha, \hat{\phi}, j), \ 1 \leq j \leq k-1.$$

Moreover, $\psi(\mu_{f,\alpha}) = \frac{1}{\alpha}\mu_{f,\alpha}$, or equivalently

$$\int_{p\mathbb{Z}_p} \phi\left(\frac{x}{p}\right) \mu_{f,\alpha} = \frac{1}{\alpha} \int_{\mathbb{Z}_p} \phi \mu_{f,\alpha}.$$

(ii) *if $v_p(\alpha) < k-1$, then $\mu_{f,\alpha}$ extends uniquely as an element of $\mathcal{D}_{v_p(\alpha)}$.*

Proof. (i) The existence of $\mu_{f,\alpha} : LP^{[0,k-2]}(\mathbb{Z}_p, \bar{\mathbb{Q}}_p) \to \bar{\mathbb{Q}}_p$ is just the linearity of $\phi \to \hat{\phi}$. The uniqueness is trivial. The second claim follows from

$$\begin{aligned}&\int_{p\mathbb{Z}_p} \phi\left(\frac{x}{p}\right)\left(\frac{x}{p}\right)^{j-1}\mu_{f,\alpha} = \frac{1}{p^{j-1}}\tilde{\Lambda}(f_\alpha, p^{-1}\hat{\phi}(px), j)\\ =&\frac{1}{\alpha}\tilde{\Lambda}(f_\alpha, \hat{\phi}, j) = \frac{1}{\alpha}\int_{\mathbb{Z}_p}\phi(x)x^{j-1}\mu_{f,\alpha}.\end{aligned}$$

(ii) One needs to show there exists a constant C, such that

$$v_p(\int_{a+p^n\mathbb{Z}_p}(x-a)^j\mu_{f,\alpha}) \geq C + (j - v_p(\alpha))n,$$

for all $a \in \mathbb{Z}_p,\ n \in \mathbb{N},\ j \leq k-2$. Note that

$$\widehat{1}_{a+p^n\mathbb{Z}_p}(x) = \begin{cases} p^{-n}e^{-2\pi i a x}, & \text{if } x \in p^{-n}\mathbb{Z}_p, \\ 0, & \text{if not.}\end{cases} = p^{-n}\phi_a(p^n x)$$

for

$$\phi_a(x) = \begin{cases} e^{2\pi i \frac{ax}{p^n}} & x \in \mathbb{Z}_p, \\ 0, & \text{otherwise.}\end{cases}$$

Then

$$\begin{aligned}\int_{a+p^n\mathbb{Z}_p}(x-a)^j\mu_{f,\alpha} =& \sum_{l=0}^{j}(-a)^l\binom{j}{l}p^{-n}\tilde{\Lambda}(f_\alpha, \phi_a(p^n x), l+1)\\ =&\alpha^{-n}\sum_{l=0}^{j}(-1)^l\binom{j}{l}p^{nl}\tilde{\Lambda}(f_\alpha, \phi_a, l+1).\end{aligned}$$

Since

$$p^{nl}\tilde{\Lambda}(f_\alpha, \phi_a, l+1) = p^{nl}\int_0^{i\infty} f_\alpha(z - \frac{a}{p^n})z^l\, dz = \int_{-\frac{a}{p^n}}^{i\infty} f_\alpha(z)(p^n z + a)^l\, dz,$$

we get

$$\sum_{l=0}^{j}(-1)^l\binom{j}{l}\int_{a+p^n\mathbb{Z}_p}(x-a)^j\mu_{f,\alpha} = \alpha^{-n}p^{nj}\int_{-\frac{a}{p^n}}^{i\infty} f_\alpha(z)z^j\, dz \in \alpha^{-n}p^{nj}L_{f_\alpha}.$$

We just pick $C = \min(v_p(\tilde{r}_j(f_\alpha|_k\delta)))$. $\square$

Remark. (i) If $p \mid N$, then $\beta = 0$, and $\alpha \neq 0$ implies $v_{p(\alpha)} = \frac{k-2}{2} < k-1$, hence $\mu_{f,\alpha}$ exists by the above Theorem.

(ii) If $p \nmid N$, then $v_p(\alpha)$, $v_p(\beta) \geq 0$. Since $v_p(\alpha) + v_p(\beta) = k-1$, at least one of $\mu_{f,\alpha}$ or $\mu_{f,\beta}$ always exists.

In the case $v_p(\alpha) = k-1$, then $\alpha + \beta = a_p(f)$ is a unit. This case is called the *ordinary case*. The conditions are not strong enough for the uniqueness of $\mu_{f,\alpha}$, as we can add the $(k-1)$-th derivative of any $\lambda \in \mathcal{D}_0$.

(iii) In the case $\alpha = \beta = 0$, we do not understand what happens.

Definition 3.4.5. Let $\chi : \mathbb{Z}_p^* \to \mathbb{C}_p^*$ be a continuous character. Set

$$L_{p,\alpha}(f \otimes \chi, s) = \int_{\mathbb{Z}_p^*} x^{-1}\chi(x)\mu_{f,\alpha}.$$

In particular, take $\chi(x) = x^{\frac{k}{2}}\langle x\rangle^{s-\frac{k}{2}}$ where $\langle x\rangle^t = \exp(t\log x)$. Set

$$L_{p,\alpha}(f, s) = \int_{\mathbb{Z}_p^*} x^{\frac{k}{2}-1}\langle x\rangle^{s-\frac{k}{2}}\mu_{f,\alpha}.$$

Proposition 3.4.6. *For $1 \leq j \leq k-1$,*

$$L_{p,\alpha}(f \otimes \chi^j) = (1 - \frac{p^{j-1}}{\alpha})(1 - \frac{\beta}{p^j})\tilde{\Lambda}(f, j).$$

Proof. Follows from

(i) $\widehat{1_{\mathbb{Z}_p^*}} = 1_{\mathbb{Z}_p} - p^{-1}1_{p^{-1}\mathbb{Z}_p}$,

(ii) $\tilde{\Lambda}(f_\alpha, 1_{\mathbb{Z}_p}, j) = (1 - \frac{\beta}{p^j}\tilde{\Lambda}(f, j))$,

(iii) $\psi(\mu_{f,\alpha}) = \frac{1}{\alpha}\mu_{f,\alpha}$.

$\square$

Remark. (i) As $\Lambda(f, s) = \Lambda(f, k-s)$ and $\alpha\beta = p^{k-1}$ if $p \nmid N$, then

$$(1 - \frac{p^{j-1}}{\alpha}) = 1 - \frac{\beta}{p^{k-j}}.$$

Note $E_p(f, s) = (1 - \alpha p^{-s})(1 - \beta p^{-s})$. Then the Euler factor of the p-adic L-function is actually the product of one part of the Euler factor for $L(f, s)$ and one part of the Euler factor for $L(f, k-s)$. This is a general phenomenon.

(ii) If $p \mid N$, $\alpha \neq 0$, the $v_p(\alpha) = \frac{k-2}{2}$. It can happen that $\alpha = p^{\frac{k-2}{2}}$, which means $L_{p,\alpha}(f, \frac{k}{2}) = 0$. In this case

Conjecture 3.4.7 *(Mazur-Tate-Teitelbaum Conjecture).*

$$L'_{p,\alpha}(f, \frac{k}{2}) = \mathcal{L}_{Font.}(f)\tilde{\Lambda}(f, \frac{k}{2}).$$

Here the p-adic L-function is related to 2*-dimensional* (φ, N)*-filtered modules* D *with* $N \neq 0$ *and* $\mathrm{Fil}^0 D = D$*,* $\mathrm{Fil}^1 D \neq D$*. For the pair* (λ, α) *as in Fontaine's course, where* λ *is the eigenvalue of* φ *and* α *is the parameter associated to the filtration,* λ *is our* α *and* α *is our* $\mathcal{L}_{Font.}$*.*

The conjecture is proved by Kato-Kurihara-Tsuji, Perrin-Riou, and Stevens, Orton, Emerton with other definitions of the $\mathcal{L}$-invariant.

(iii) Mazur, Tate and Teitelbaum have also formulated a p-adic analog of the BSD conjecture. For $E/\mathbb{Q}$ an elliptic curve, by Taniyama-Weil, it is associated to a primitive form $f \in S_2(N)$. Set $L_{p,\alpha}(E, s) = L_{p,\alpha}(f, s)$ if it exists, which is the case if E has either good reduction (hence $p \nmid N$) or multiplicative reduction (hence $p \mid N, p^2 \nmid N$) $\bmod p$.

Conjecture 3.4.8 *(p-adic BSD Conjecture).*

$$\mathrm{ord}_{s=1} L_{p,\alpha}(E, s) = \begin{cases} \mathrm{rank}\, E(\mathbb{Q}), & \textit{if } p \nmid N \textit{ or } \alpha \neq 1; \\ \mathrm{rank}\, E(\mathbb{Q}) + 1, & \textit{if } p \mid N \textit{ and } \alpha = 1. \end{cases}$$

Kato showed that

$$\mathrm{ord}_{s=1} L_{p,\alpha}(E, s) \geq \begin{cases} \mathrm{rank}\, E(\mathbb{Q}), & \text{if } p \nmid N \text{ or } \alpha \neq 1; \\ \mathrm{rank}\, E(\mathbb{Q}) + 1, & \text{if } p \mid N \text{ and } \alpha = 1. \end{cases}$$

(iv) To prove Kato or Kato-Kurihara-Tsuji, we need another construction of p-adic L-functions via Iwasawa theory and (φ, Γ)-modules; this construction is the subject of the next part of the course and is based on ideas of Perrin-Riou.

Part II

Fontaine's rings and Iwasawa theory

Chapter 4

Preliminaries

4.1 Some of Fontaine's rings

This section is a review of notations and results from Fontaine's course. For details, see Fontaine's notes.

4.1.1 Rings of characteristic p

(1) $\mathbb{C}_p$ is the completion of $\overline{\mathbb{Q}_p}$ for the valuation v_p with $v_p(p) = 1$.

$$\mathfrak{a} = \{x \in \mathbb{C}_p, v_p(x) \geqslant \frac{1}{p}\}.$$

(2) $\tilde{E}^+$ is the ring R in Fontaine's course. By definition

$$\tilde{E}^+ := \{x = (x_n)_{n\in\mathbb{N}} \mid x_n \in \mathbb{C}_p/\mathfrak{a}, x_{n+1}^p = x_n, \forall n\}$$

is a ring of characteristic p with an action of $G_{\mathbb{Q}_p}$. For $x = (x_n) \in \tilde{E^+}$, for every x_n, pick a lifting $\hat{x}_n \in \mathcal{O}_{\mathbb{C}_p}$, then

$$\lim_{k\to+\infty} (\hat{x}_{n+k})^{p^k} := x^{(n)} \in \mathcal{O}_{\mathbb{C}_p}$$

is a canonical lifting of x_n such that

$$\tilde{E}^+ = \{x = (x^{(n)})_{n\in\mathbb{N}} \mid x^{(n)} \in \mathcal{O}_{\mathbb{C}_p}, (x^{(n+1)})^p = x^{(n)}, \forall n\}$$

with the addition and multiplication by

$$(x+y)^{(n)} = \lim_{k\to+\infty} (x^{(n+k)} + y^{(n+k)})^{p^k}, \quad (xy)^{(n)} = x^{(n)}y^{(n)}.$$

$\tilde{E}^+$ is a valuation ring with valuation

$$v_E(x) = v_p(x^{(0)})$$

and maximal ideal

$$\mathfrak{m}_{\tilde{E}^+} = \{x \in \tilde{E}^+, v_E(x) > 0\}.$$

(3) Choose once for all

$$\varepsilon = (1, \varepsilon^{(1)}, \cdots) \in \tilde{E}^+, \quad \varepsilon^{(1)} \neq 1.$$

Then $\varepsilon^{(n)}$ is a primitive p^n-th root of 1 for all n. Set

$$\bar{\pi} = \varepsilon - 1 \in \tilde{E}^+.$$

We know that $v_E(\bar{\pi}) = \frac{p}{p-1} > 0$.

From now on, $\chi : G_{\mathbb{Q}_p} \to \mathbb{Z}_p^*$ will be the cyclotomic character. The action of $G_{\mathbb{Q}_p}$ on ε is given by

$$g(\varepsilon) = \varepsilon^{\chi(g)} = \sum_{k=0}^{+\infty} \binom{\chi(g)}{k} \bar{\pi}^k.$$

(4) In the following, without further specification, $K \subseteq \mathbb{Q}_p$ will be a finite extension of $\mathbb{Q}_p$. Denote by $k = k_K$ its residue field. Set

$$K_n = K(\varepsilon^{(n)}), \quad K_\infty = \bigcup_{n \in \mathbb{N}} K_n.$$

Set

$F \subseteq K$= the maximal unramified extension of $\mathbb{Q}_p$ inside K,

$F' \subseteq K_\infty$= the maximal unramified extension of $\mathbb{Q}_p$ inside K_∞.

Set

$$G_K = \mathrm{Gal}(\bar{\mathbb{Q}}_p/K), \quad H_K = \mathrm{Ker}\,\chi = \mathrm{Gal}(\bar{\mathbb{Q}}_p/K_\infty),$$

and

$$\Gamma_K = G_K/H_K = \mathrm{Gal}(K_\infty/K) \xhookrightarrow{\chi} \mathbb{Z}_p^*.$$

(5) For every K, let

$\tilde{E}_K^+ := \{x = (x_n) \in \tilde{E}^+, x_n \in \mathcal{O}_{K_\infty}/\mathfrak{a},\ \forall n\} = (\tilde{E}^+)^{H_K}$ (by Ax-Sen-Tate's Theorem),

$E_K^+ := \{x = (x_n) \in \tilde{E}^+, x_n \in \mathcal{O}_{K_n}/\mathfrak{a},\ \forall n \geq n(K)\}.$

Then

$$\bar{\pi} \in E_K^+ \subseteq \tilde{E}_K^+ \subseteq \tilde{E}^+, \quad \forall K.$$

We set

$$E_K := E_K^+[\bar{\pi}^{-1}] \subseteq \tilde{E}_K := \tilde{E}_K^+[\bar{\pi}^{-1}] \subseteq \tilde{E} = \tilde{E}^+[\bar{\pi}^{-1}] = \operatorname{Fr} R$$

with valuation

$$v_E(\bar{\pi}^{-k}x) = v_E(x) - kv_E(\bar{\pi}).$$

The following Theorem is the topics in the last section of Chapter 2 of Fontaine's Notes.

Theorem 4.1.1. (i) *$\tilde{E}$ is a field complete for v_E with residue field $\bar{\mathbb{F}}_p$, ring of integers $\tilde{E}^+$ and $G_{\mathbb{Q}_p}$ acts continuously with respect to v_E.*

(ii) *$E_F = k_F((\bar{\pi}))$ if $F/\mathbb{Q}_p$ is unramified.*

In general, E_K is a totally ramified extension of $E_{F'}$ of degree $[K_\infty : F'_\infty]$, thus a local field of characteristic p, with ring of integers E_K^+ and residue field $k_{F'}$.

(iii) *$E = \bigcup_{[K:\mathbb{Q}_p]<+\infty} E_K$ is a separable closure of $E_{\mathbb{Q}_p}$, is stable under $G_{\mathbb{Q}_p}$ and $\mathrm{Gal}(E/E_K) = H_K$. So $H_{\mathbb{Q}_p}$ acts continuously on E for the discrete topology.*

(iv) *$\tilde{E}$ (resp. $\tilde{E}_K$) is the completion of the radical closure of E (resp. $\tilde{E}_K$), i.e., $\bigcup_{n\in\mathbb{N}} E^{p-n}$ (resp. $\bigcup_{n\in\mathbb{N}} E_K^{p-n}$). In particular, $\tilde{E}$ is algebraically closed.*

4.1.2 Rings of characteristic 0

(6) Set

$$\tilde{A}^+ := W(\tilde{E}^+) = W(R), \quad \tilde{A} := W(\tilde{E}) = W(\operatorname{Fr} R).$$

Every element $x \in \tilde{A}$ can be written as

$$x = \sum_{k=0}^{+\infty} p^k [x_k]$$

while $x_k \in \tilde{E}$ and $[x_k]$ is its *Teichmüller representative.*

As we know from the construction of Witt rings, there are bijections

$$\tilde{A}^+ \cong (\tilde{E}^+)^{\mathbb{N}}, \quad \tilde{A} \cong (\tilde{E})^{\mathbb{N}}.$$

There are two topologies in $\tilde{A}^+$ and $\tilde{A}$:

(i) *Strong topology or p-adic topology*: topology by using the above bijection and the discrete topology on $\tilde{E}^+$ or $\tilde{E}$. A basis of neighborhoods of 0 are the $p^k\tilde{A}$, $k \in \mathbb{N}$.

(ii) *Weak topology*: topology defined by v_E. A basis of neighborhoods of 0 are the $p^k\tilde{A} + [\bar{\pi}^n]A^+$, $k, n \in \mathbb{N}$.

The commuting actions of $G_{\mathbb{Q}_p}$ and φ on $\tilde{A}$ are given by

$$g(\sum_{k=0}^{+\infty} p^k[x_k]) = \sum_{k=0}^{+\infty} p^k[g(x_k)], \quad \varphi(\sum_{k=0}^{+\infty} p^k[x_k]) = \sum_{k=0}^{+\infty} p^k[x_k^p].$$

(7) $\tilde{B} := \tilde{A}[\frac{1}{p}]$ is the fraction field of $\tilde{A}$. $\tilde{B}$ is complete for the valuation v_p, its ring of integers is $\tilde{A}$ and its residue field is $\tilde{E}$.

For the $G_{\mathbb{Q}_p}$ and φ-actions,

$$\begin{aligned} \tilde{A}^{\varphi=1} &= \mathbb{Z}_p, & \tilde{B}^{\varphi=1} &= \mathbb{Q}_p, \\ \tilde{A}^{H_K} &= W(\tilde{E}_K) := \tilde{A}_K, & \tilde{B}^{H_K} &= \tilde{A}_K[\frac{1}{p}] := \tilde{B}_K. \end{aligned}$$

(8) Set

$$\pi = [\varepsilon] - 1, \quad t = \log[\varepsilon] = \log(1+\pi).$$

The element $[\varepsilon]$ is the p-adic analogue of $e^{2\pi i}$. The $G_{\mathbb{Q}_p}$- and φ- actions are given by

$$\varphi(\pi+1) = (\pi+1)^p, \quad \varphi(\pi+1) = (\pi+1)^{\chi(g)}.$$

(9) Set

$$A^+_{\mathbb{Q}_p} := \mathbb{Z}_p[[\pi]] \hookrightarrow \tilde{A}^+$$

which is stable under φ and $G_{\mathbb{Q}_p}$. Set

$$A_{\mathbb{Q}_p} := \mathbb{Z}_p\widehat{[[\pi]][}\frac{1}{\pi}] \hookrightarrow \tilde{A}$$

while$\widehat{\ }$stands for completion under the strong topology, thus

$$A_{\mathbb{Q}_p} = \{\sum_{k\in\mathbb{Z}} a_k\pi^{-k} \mid a_k \in \mathbb{Z}_p, \lim_{k\to-\infty} v_p(a_k) = +\infty\}.$$

Set $B_{\mathbb{Q}_p} := A_{\mathbb{Q}_p}[\frac{1}{p}]$, then $B_{\mathbb{Q}_p}$ is a field complete for the valuation v_p, with ring of integers $A_{\mathbb{Q}_p}$ and residue field $E_{\mathbb{Q}_p}$.

Moreover, if $[K:\mathbb{Q}_p] < +\infty$, $\tilde{B}$ contains a unique extension B_K of $B_{\mathbb{Q}_p}$ whose residue field is E_K, and $A_K = B_K \cap \tilde{A}$ is the ring of integers. By uniqueness, B_K is stable under φ and G_K acting through Γ_K.

The field

$$\mathcal{E}^{ur} = \bigcup_{[K:\mathbb{Q}_p]<+\infty} B_K$$

is the maximal unramified extension of $B_{\mathbb{Q}_p} = \mathcal{E}$. Set

$$B = \widehat{\mathcal{E}^{ur}}$$

be the closure of $\bigcup_{[K:\mathbb{Q}_p]<+\infty} B_K$ in $\tilde{B}$ for the strong topology. Then $A = B \cap \tilde{A}$ is the ring of integers $\mathcal{O}_{\widehat{\mathcal{E}^{ur}}}$ and the residue field of B is $A/pA = E$. By Ax-Sen-Tate,

$$B^{H_K} = B_K, \quad A^{H_K} = A_K.$$

Remark. If $\bar{\pi}_K$ is a uniformising parameter of E_K, let $\pi_K \in A_K$ be any lifting. Then

$$A_K = \{\sum_{k\in\mathbb{Z}} a_k \pi_K^k | a_k \in \mathcal{O}_{F'}, \lim_{k\to-\infty} v_p(a_k) = +\infty\}.$$

Remark. In the above construction, the correspondence $\Lambda \longrightarrow \tilde{\Lambda}$ is obtained by making φ bijective and then complete, where $\Lambda = (E_K, E, A_K, A, B_K, B)$.

4.2 (φ, Γ)-modules and Galois representations.

Let K be a fixed finite extension over $\mathbb{Q}_p$, let $\Gamma = \Gamma_K$.

Definition 4.2.1. (i) A (φ, Γ)-*module over* A_K is a finitely generated A_K-module with semi-linear continuous (for the weak topology) and commuting actions of φ and Γ.

A (φ, Γ)-*module over* B_K is a finite dimensional B_K-vector space with semi-linear continuous (for the weak topology) and commuting actions of φ and Γ.

(ii) A (φ, Γ)-module D/A_K is *étale* (or *of slope* 0) if $\varphi(D)$ generates D as an A_K-module.

A (φ, Γ)-module D/B_K is *étale* (or *of slope* 0) if it has an A_K-lattice which is étale, equivalently, there exists a basis $\{e_1, \cdots, e_d\}$ over B_K, such that the matrix of $\varphi(e_1), \cdots, \varphi(e_d)$ in $e_1, \cdots, e_d$ is inside $\mathrm{GL}_d(A_K)$.

The following theorem is similar to Theorem 1.5.9 in §1.5.4 of Fontaine's Notes.

Theorem 4.2.2. *The correspondence*

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

is an equivalence of $\otimes$ categories from the category of $\mathbb{Z}_p$-representations (resp. $\mathbb{Q}_p$-resp) of G_K to the category of étale (φ, Γ)-modules over A_K (resp. B_K), and the Inverse functor is

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

Remark. (i) Γ_K is essentially pro-cyclic, so a (φ, Γ)-module is given by two operators and commuting relations between them. For example, if D/A_K is free of rank d, let U be the matrix of γ for $\overline{\langle\gamma\rangle} = \Gamma_K$, let P be the matrix of φ, then

$$U\gamma(P) = P\varphi(U), \ U, \ P \in \mathrm{GL}_d(A_K).$$

(ii) We want to recover from $D(V)$ the known invariants of V:

- $H^i(G_K, V)$; we shall do so in the coming lectures. We will also recover the Iwasawa modules attached to V and thus give another construction of p-adic L-functions.

- $D_{dR}(V)$, $D_{cris}(V)$, $D_{st}(V)$.

Chapter 5

(φ, Γ)-modules and Galois cohomology

5.1 Galois Cohomology

Let M be a topological $\mathbb{Z}_p$-module (e.g. a finite module with discrete topology or a finitely generated $\mathbb{Z}_p$-module with p-adic topology, or a Fontaine's ring $B_{dR}^+ \cdots$), with a continuous action of G_K.

Let $H^i(G_K, M)$ be the i-th cohomology groups of M of continuous cohomology. Then:

$$H^0(G_K, M) = M^{G_K} = \{x \in M : (g-1)x = 0 \ \forall g \in G_K\};$$
$$H^1(G_K, M) = \frac{\{c : G_K \to M \text{ continuous}, \ g_1 c_{g_2} - c_{g_1 g_2} + c_{g_1} = 0, \ \forall g_1, g_2 \in G_K\}}{\{c : g \to (g-1)x, \text{ for some } x \in M\}}$$

To a 1-cocycle c, we associate a G_K module E_c such that

$$0 \to M \to E_c \to N \to 0$$

where $E_c \simeq \mathbb{Z}_p \times M$ as a $\mathbb{Z}_p$-module and G_K acts on E_c by

$$g(a, m) = (a, gm + c_g).$$

One can check easily

$$g_1(g_2(a, m)) = g_1(a, g_2 m + c_{g_2}) = (a, g_1 g_2 m + g_1 c_{g_2} + c_{g_1}) = g_1 g_2(a, m).$$

E_c is trivial if and only if there exists $\hat{1} \in E_c$, such that $g\hat{1} = \hat{1}$ for all g, i.e. $\hat{1} = (1, x), g\hat{1} - \hat{1} = (0, gx - x + c_g) = 0$, that is, $c_g = (1-g)x$ is a coboundary.

Theorem 5.1.1 (Tate's Local Duality Theorem). *Suppose K is a finite extension of $\mathbb{Q}_p$. Let M be a $\mathbb{Z}_p[G_K]$-module of finite length. Then:*

(i) $H^i(G_K, M) = 0$ *for* $i \geq 3$; $H^i(G_K, M)$ *is finite if* $i \leq 2$.

(ii) $\prod_{i=0}^{2} |H^i(G_K, M)|^{(-1)^i} = |M|^{-[K:\mathbb{Q}_p]}$;

(iii) $H^{2-i}(G_K, \mathrm{Hom}(M, \boldsymbol{\mu}_{p^\infty})) \simeq \mathrm{Hom}(H^i(G_K, M), \mathbb{Q}_p/\mathbb{Z}_p)$.

We will give a proof using (φ,Γ)-module (Herr's thesis).

Remark. (i) If M is a finitely generated $\mathbb{Z}_p$-module with p-adic topology, then $M \simeq \varprojlim M/p^nM$, and $H^i(G_K, M) \simeq \varprojlim H^i(G_K, M/p^nM)$.

$\boxed{\text{Z!}}$ Not tautological, the proof uses finiteness of (i) to ensure Mittag-Leffler conditions.

(ii) If V is a $\mathbb{Q}_p$-representation of G_K, let $T \subset V$ be a $\mathbb{Z}_p$-lattice stable by G_K. Then $H^i(G_K, V) \simeq \mathbb{Q}_p \otimes H^i(G_K, T)$.

Corollary 5.1.2. *If V is a $\mathbb{Q}_p$-representation of G_K. Then:*

(i) $\sum_{i=0}^{2}(-1)^i \dim_{\mathbb{Q}_p} H^i(G_K, V) = -[K:\mathbb{Q}_p] \dim_{\mathbb{Q}_p} V$;

(ii) $H^2(G_K, V) = H^0(G_K, V^*(1))^*$.

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

Assume that Γ_K is pro-cyclic ($\Gamma_{\mathbb{Q}_p} \simeq \mathbb{Z}_p^*$), γ is a topological generator of Γ_K. This assumption is automatic if $p \geq 3$, or if $K \supset \mathbb{Q}(\mu_4)$ when $p = 2$. Let V be a $\mathbb{Z}_p$- or $\mathbb{Q}_p$-representation of G_K. Set

$$D(V) = (A \otimes_{\mathbb{Z}_p} V)^{H_K}.$$

Definition 5.2.1. The complex $C^\bullet_{\varphi,\gamma}(K, V) = C_{\varphi,\gamma}(K, V)$ is

$$0 \to D(V) \xrightarrow{(\varphi-1,\ \gamma-1)} D(V) \oplus D(V) \xrightarrow{(\gamma-1)\,\mathrm{pr}_1 - (\varphi-1)\,\mathrm{pr}_2} D(V) \to 0.$$

It is easy to see $C_{\varphi,\gamma}(K, V)$ is really a complex (as φ, γ commute to each other). We shall denote the complex by $C^\bullet(V)$ if no confusion is caused. We have

$$\begin{aligned}
H^0(C^\bullet(V)) &= \{x \in D(V), \gamma(x) = x, \varphi(x) = x\},\\
H^1(C^\bullet(V)) &= \frac{\{(x,y) : (\gamma-1)x = (\varphi-1)y\}}{\{((\varphi-1)z, (\gamma-1)z) : z \in D(V)\}},\\
H^2(C^\bullet(V)) &= \frac{D(V)}{(\gamma-1, \varphi-1)},\\
H^i(C^\bullet(V)) &= 0, \text{for } i \geq 3.
\end{aligned}$$

Theorem 5.2.2. *$H^i(C_{\varphi,\gamma}(K,V)) \simeq H^i(G_K,V)$ for all i in $\mathbb{N}$.*

Proof. We have the following exact sequence (which can be proved by reducing $\bmod p$):

$$0 \to \mathbb{Z}_p \to A \xrightarrow{\varphi-1} A \to 0,$$

here $A = \mathcal{O}_{\widehat{\mathcal{E}^{ur}}}$ in Fontaine's course.

(1) $i = 0$: For $x \in D(V)^{\varphi=1}$, since $D(V) = (A \otimes_{\mathbb{Z}_p} V)^{H_K}$, we have $D(V)^{\varphi=1} = (A^{\varphi=1} \otimes_{\mathbb{Z}_p} V)^{H_K} = V^{H_K}$, and $(V^{H_K})^{\gamma=1} = V^{G_K}$.

(2) $i = 1$: Let (x,y) satisfy the condition $(\gamma-1)x = (\varphi-1)y$. Choose $b \in (A \otimes_{\mathbb{Z}_p} V)^{H_K}$, $(\varphi-1)b = x$. We define the map:

$$g \in G_K \to c_{x,y}(g) = \frac{g-1}{\gamma-1}y - (g-1)b.$$

while the meaning of $\frac{g-1}{\gamma-1}y$ is: as $\chi(g) = \lim_{i\to+\infty} \chi(\gamma)^{n_i}$, y is fixed by H_K, we let

$$\frac{g-1}{\gamma-1}y = \lim_{i\to+\infty}(1+\gamma+\cdots+\gamma^{n_i-1})y.$$

This is a cocycle with values in V, because $g \mapsto (g-1)(\frac{y}{\gamma-1} - b)$ is a cocycle, and $(\varphi-1)c_{xy}(g) = (g-1)x - (\varphi-1)(g-1)b = 0$, which implies that $c_{xy}(g) \in D(V)^{\varphi=1} = V$.

Injectivity: If $c_{xy} = 0$ in $H^1(G_K,V)$, then there exists $z \in V$, $c_{xy}(g) = (g-1)z$ for all $g \in G_K$, that is, $\frac{g-1}{\gamma-1}y = (g-1)(b-z)$ for all g. Now $b-z \in D(V)$, because it is fixed by $g \in H_K$. Then we have: $y = (\gamma-1)(b-z)$ and $x = (\varphi-1)(b-z)$, hence (x,y) equal to 0 in $H^1(C^\bullet(V))$.

Surjectivity: If $c \in H^1(G_K,V)$, we have:

$$0 \to V \longrightarrow E_c \longrightarrow \mathbb{Z}_p \to 0,$$

here $E_c = \mathbb{Z}_p \times V$, $e \in E_c \mapsto 1 \in \mathbb{Z}_p$ and $ge = e + c_g$ for $g \mapsto c_g$ representing c. We have:

$$0 \to D(V) \longrightarrow D(E_c) \longrightarrow A_K \to 0,$$

here $D(E_c) \subset A \otimes E_c$ and $\tilde{e} \in D(E_c) \mapsto 1 \in A_K$. Let

$$x = (\varphi - 1)\tilde{e}, \quad y = (\gamma - 1)\tilde{e},$$

they are both in $D(V)$ and satisfy $(\gamma - 1)x = (\varphi - 1)y$. Let $b = \tilde{e} - e \in A \otimes_{\mathbb{Z}_p} E_c$. Then $c_{x,y}(g) = \frac{g-1}{\gamma-1}y - (g-1)b = c_g$ and $(\varphi - 1)(b) = x$.

(3) i general: from the exact sequence:

$$0 \to \mathbb{Z}_p \to A \xrightarrow{\varphi-1} A \to 0,$$

tensoring with V and taking the cohomology $H^i(H_K, -)$, we get

$$0 \to V^{H_K} \to D(V) \xrightarrow{\varphi-1} D(V) \to H^1(H_K, V) \to 0,$$

because $A \otimes V \simeq \oplus(A/p^i)$ as H_K-modules and $H^i(H_K, E) = 0$, if $i \geq 1$, so $H^i(H_K, A \otimes V) = 0$ for all $i \geq 1$. Hence $H^i(H_K, V) = 0$ for all $i \geq 1$.

By the *Hochschild-Serre Spectral Sequence* for

$$1 \to H_K \to G_K \to \Gamma_K \to 1,$$

we have $H^i(\Gamma_K, H^j(H_K, V)) \Rightarrow H^{i+j}(G_K, V)$. When j or $i \geq 2$, the cohomology vanishes. So we have:

$$\begin{aligned} &H^q(G_K, V) = 0, \text{ if } q \geq 3 \\ &H^2(G_K, V) \simeq H^1(\Gamma_K, H^1(H_K, V)). \end{aligned}$$

Since $H^1(H_K, V) = \frac{D(V)}{\varphi-1}$, we get

$$H^2(G_K, V) \simeq \frac{D(V)}{\varphi - 1}\Big/(\gamma - 1)\frac{D(V)}{\varphi - 1} = \frac{D(V)}{(\varphi - 1, \gamma - 1)}.$$

□

Remark. (1) The inflation-restriction exact sequence becomes the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & H^1(\Gamma_K, V^{H_K}) \arrow[r] \arrow[d, equal] & H^1(G_K, V) \arrow[r] \arrow[d, "\iota_{\varphi,\gamma}"] & H^1(H_K, V^{\Gamma_K}) \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \frac{D(V)^{\varphi=1}}{\gamma-1} \arrow[r] & H^1(C_{\varphi,\gamma}(K, V)) \arrow[r] & (\frac{D(V)}{\varphi-1})^{\Gamma_K} \arrow[r] & 0
\end{tikzcd}$$

where the map $H^1(C_{\varphi,\gamma}(K,V)) \to (\frac{D(V)}{\varphi-1})^{\Gamma_K}$ is given by sending (x,y) to the image of x.

(2) Let γ' be another generator of Γ_K, we have $\frac{\gamma-1}{\gamma'-1} \in (\mathbb{Z}_p[[\Gamma_K]])^*$ and a commutative diagram:

$$\begin{tikzcd}
C_{\varphi,\gamma}: 0 \arrow[r] & D(V) \arrow[r] \arrow[d, "\frac{\gamma-1}{\gamma'-1}"'] & D(V) \arrow[d, "\frac{\gamma-1}{\gamma'-1}"'] & \oplus & D(V) \arrow[r] \arrow[d, "\mathrm{Id}"] & D(V) \arrow[r] \arrow[d, "\mathrm{Id}"] & 0 \\
C_{\varphi,\gamma'}: 0 \arrow[r] & D(V) \arrow[r] & D(V) & \oplus & D(V) \arrow[r] & D(V) \arrow[r] & 0
\end{tikzcd}$$

It induces a commutative diagram

$$\begin{tikzcd}
H^1(C^\bullet_{\varphi,\gamma}) \arrow[rr, "\iota_{\gamma,\gamma'}"] \arrow[dr, "l_K(\gamma)\iota_{\varphi,\gamma}"'] & & H^1(C^\bullet_{\varphi,\gamma'}) \arrow[dl, "l_K(\gamma')\iota_{\varphi,\gamma'}"] \\
& H^1(G_K,V) &
\end{tikzcd}$$

where $l_K(\gamma) = \frac{\log\chi(\gamma)}{p^{r(K)}}$ for $\log\chi(\Gamma_K) \simeq p^{r(K)}\mathbb{Z}_p$. So $l_K(\gamma)c_{,\varphi\gamma}$ "does not depend on the choice of γ".

5.3 Tate's Euler-Poincaré formula.

5.3.1 The operator ψ.

Lemma 5.3.1. (i) $\{1,\varepsilon,\cdots,\varepsilon^{p-1}\}$ *is a basis of* $E_{\mathbb{Q}_p}$ *over* $\varphi(E_{\mathbb{Q}_p})$*;*

(ii) $\{1,\varepsilon,\cdots,\varepsilon^{p-1}\}$ *is a basis of* E_K *over* $\varphi(E_K)$*, for all* $[K:\mathbb{Q}_p] < +\infty$*;*

(iii) $\{1,\varepsilon,\cdots,\varepsilon^{p-1}\}$ *is a basis of* E *over* $\varphi(E)$*;*

(iv) $\{1,[\varepsilon],\cdots,[\varepsilon]^{p-1}\}$ *is a basis of* A *over* $\varphi(A)$*.*

Proof. (i) Since $E_{\mathbb{Q}_p} = \mathbb{F}_p((\bar\pi))$ with $\bar\pi = \varepsilon - 1$, we have $\varphi(E_{\mathbb{Q}_p}) = \mathbb{F}_p((\bar\pi^p))$;

(ii) Use the following diagram of fields, note that $E_{\mathbb{Q}_p}/\varphi(E_{\mathbb{Q}_p})$ is purely inseparable and $\varphi(E_K)/\varphi(E_{\mathbb{Q}_p})$ is separable:

$$\begin{tikzcd}
E_K \arrow[r, dash] \arrow[d, dash] & \varphi(E_K) \arrow[d, dash] \\
E_{\mathbb{Q}_p} \arrow[r, dash] & \varphi(E_{\mathbb{Q}_p})
\end{tikzcd}$$

(iii) Because $E = \cup E_K$.

(iv) To show that

$$(x_0, x_1, \cdots, x_{p-1}) \in A^p \overset{\sim}{\longmapsto} \sum_{i=0}^{p-1} [\varepsilon]^i \varphi(x_i) \in A$$

is a bijection, it suffices to check it $\bmod p$ and use (iii). □

Definition 5.3.2. The operator $\psi : A \to A$ is defined by

$$\psi(\sum_{i=0}^{p-1} [\varepsilon]^i \varphi(x_i)) = x_0.$$

Proposition 5.3.3. (i) $\psi\varphi = \mathrm{Id}$*;*
(ii) ψ *commutes with* $G_{\mathbb{Q}_p}$*.*

Proof. (i) The first statement is obvious.
(ii) Note that

$$g(\sum_{i=0}^{p-1} [\varepsilon]^i \varphi(x_i)) = \sum_{i=0}^{p-1} [\varepsilon]^{i\chi(g)} \varphi(g(x_i)).$$

If for $1 \leq i \leq p-1$, write $i\chi(g) = i_g + pj_g$ with $1 \leq i_g \leq p-1$, then

$$\psi(\sum_{i=0}^{p-1} [\varepsilon]^{i\chi(g)} \varphi(g(x_i))) = \psi(\varphi(g(x_0)) + \sum_{i=1}^{p-1} [\varepsilon]^{i_g} \varphi([\varepsilon]^{j_g} g(x_i))) = g(x_0).$$

□

Corollary 5.3.4. (i) *If* V *is a* $\mathbb{Z}_p$*-representation of* G_K*, there exists a unique operator* $\psi : D(V) \to D(V)$ *with*

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

if $a \in A_K, x \in D(V)$ *and moreover* ψ *commute with* Γ_K*.*
(ii) *If* D *is an étale* (φ,Γ)*-module over* A_K *or* B_K*, there exists a unique operator* $\psi : D \to D$ *with as in* (i)*. Moreover, for any* $x \in D$*,*

$$x = \sum_{i=0}^{p^n-1} [\varepsilon]^i \varphi^n(x_i)$$

where $x_i = \psi^n([\varepsilon]^{-i}x)$*.*

Proof. (i) The uniqueness follows from $A_K \otimes_{\varphi(A_K)} \varphi(D) = D$. For the existence, use ψ on $A \otimes V \supset D(V)$. $D(V)$ is stable under ψ because ψ commutes with H_K, ψ commutes with Γ_K since ψ commutes with G_K.

(ii) $D = D(V(D))$, thus we have existence and uniqueness of ψ. The rest is by induction on n. □

Example 5.3.5. Let $D = A_{\mathbb{Q}_p} \supset A^+_{\mathbb{Q}_p} = \mathbb{Z}_p[[\pi]]$ be the trivial (φ, Γ)-module, here $[\varepsilon] = (1+\pi)$. Then for $x = F(\pi) \in A^+_{\mathbb{Q}_p}$, $\varphi(x) = F((1+\pi)^p - 1)$. Write

$$F(\pi) = \sum_{i=0}^{p-1} (1+\pi)^i F_i((1+\pi)^p - 1),$$

then $\psi(F(\pi)) = F_0(\pi)$. It is easy to see if $F(\pi)$ belongs to $\mathbb{Z}_p[[\pi]]$, $F_i(\pi)$ belongs to $\mathbb{Z}_p[[\pi]]$ for all i. Then $\psi(E^+_{\mathbb{Q}_p}) \subset E^+_{\mathbb{Q}_p} = F_p[[\pi]]$. Hence $\psi(A^+_{\mathbb{Q}_p}) \subset A^+_{\mathbb{Q}_p}$. Consequently, ψ is continuous for the weak topology.

Moreover, we have:

$$\begin{aligned}\varphi(\psi(F)) &= F_0((1+\pi)^p - 1) = \frac{1}{p} \sum_{z^p=1} \sum_{i=0}^{p-1} (z(1+\pi))^i F_i((z(1+\pi))^p - 1) \\ &= \frac{1}{p} \sum_{z^p=1} F(z(1+\pi) - 1).\end{aligned}$$

Recall $\mathcal{D}_0(\mathbb{Z}_p, \mathbb{Q}_p) \simeq B^+_{\mathbb{Q}_p} = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} A^+_{\mathbb{Q}_p}$ by $\mu \mapsto A_\mu(\pi) = \int_{\mathbb{Z}_p} [\varepsilon]^x \mu$. Recall that $\psi(\mu)$ is defined by

$$\int_{\mathbb{Z}_p} \phi(x) \psi(\mu) = \int_{p\mathbb{Z}_p} \phi(\frac{x}{p}) \mu.$$

From the above formula, we get, using formulas for Amice transforms,

$$A_{\psi(\mu)}(\pi) = \psi(A_\mu)(\pi).$$

Proposition 5.3.6. *If D is an étale φ-module over A_K, then ψ is continuous for the weak topology.*

Proof. As A_K is a free $A_{\mathbb{Q}_p}$-module of rank $[K_\infty : \mathbb{Q}_p(\boldsymbol{\mu}_{p^\infty})]$, we can assume $K = \mathbb{Q}_p$. Choose $e_1, e_2, \cdots, e_d$ in D, such that

$$D = \oplus (A_{\mathbb{Q}_p}/p^{n_i}) e_i, \quad n_i \in \mathbb{N} \cup \{\infty\}.$$

Since D is étale, we have $D = \oplus(A_{\mathbb{Q}_p}/p^{n_i})\varphi(e_i)$. Then we have the following diagram:

$$\begin{tikzcd} D \arrow[r, "\psi"] \arrow[d, "\wr"] & D \arrow[d, "\wr"] \\ \oplus(A_{\mathbb{Q}_p}/p^{n_i})\varphi(e_i) \arrow[r] & \oplus(A_{\mathbb{Q}_p}/p^{n_i})e_i \end{tikzcd}$$

$$\sum x_i\varphi(e_i) \longmapsto \sum \psi(x_i)e_i$$

Now $x \mapsto \psi(x)$ is continuous in $A_{\mathbb{Q}_p}$, hence ψ is continuous in D. $\square$

5.3.2 $D^{\psi=1}$ and $D/(\psi-1)$

Lemma 5.3.7. *If D is an étale φ-module over $E_{\mathbb{Q}_p}$, then:*
(i) *$D^{\psi=1}$ is compact;*
(ii) *$\dim_{\mathbb{F}_p}(D/(\psi-1)) < +\infty$.*

Proof. (i) choose a basis $\{e_1,\cdots,e_d\}$, then $\{\varphi(e_1),\cdots,\varphi(e_d)\}$ is still a basis. Set $v_E(x) = \inf_i v_E(x_i)$ if $x = \sum_i x_i\varphi(e_i), x_i \in E^+_{\mathbb{Q}_p}$. We have

$$\psi(x) = \sum_i \psi(x_i)e_i \text{ and } e_i = \sum_{i=1}^d a_{i,j}\varphi(e_j).$$

Let $c = \inf_{i,j} v_E(a_{i,j})$, then we have

$$v_E(\psi(x)) \geq c + \inf_i v_E(\psi(x_i)). \tag{5.1}$$

From $\psi(E^+_{\mathbb{Q}_p}) \subset E^+_{\mathbb{Q}_p}$ and $\psi(\bar\pi^{p^k}x) = \bar\pi^k\psi(x)$, we get $v_E(\psi(x)) \geq \left[\frac{v_E(x)}{p}\right]$. So

$$v_E(\psi(x)) \geq c + \inf_i[\frac{v_E(x_i)}{p}] \geq c + [\frac{v_E(x)}{p}].$$

If $v_E(x) < \frac{p(c-1)}{p-1}$, then $v_E(\psi(x)) > v_E(x)$. Now $D^{\psi=1}$ is closed since ψ is continuous, and is a subset of the compact set

$$M := \{x : v_E(x) \geq \frac{p(c-1)}{p-1}\} \subseteq \sum_{i=1}^d \bar\pi^k\mathbb{F}_p[[\bar\pi]]\cdot\varphi(e_i).$$

Hence $D^{\psi=1}$ is also compact.

(ii) $\psi-1$ is bijective on D/M from the proof of (i). We only need to prove that $M/((\psi-1)D\cap M)$ is finite, equivalently, that $(\psi-1)D$ contains $\{x : v_E(x)\geq c'\}$ for some c'.

$\varphi(x_i)$ can be written uniquely as $\varphi(x_i)=\sum\limits_{j=1}^{d} b_{i,j}e_j$. Let $c_0=\inf\limits_{i,j} v_E(b_{i,j})$, then

$$x=\sum_{i=1}^{d} x_i\varphi(e_i)=\sum_{i=1}^{d} x_i\sum_{j=1}^{d} b_{i,j}e_j=\sum_{j=1}^{d}(\sum_{i=1}^{d} x_ib_{i,j})e_j.$$

Let $y_j=\sum\limits_{i=1}^{d} x_ib_{i,j}$, then $x=\sum\limits_{j=1}^{d} y_je_j$, and

$$v_E(y_j)\geq c_0+v_E(x).$$

From $\varphi(x)=\sum\limits_{j=1}^{d}\varphi(y_j)\varphi(e_j)$, we get

$$v_E(\varphi(x))=\inf v_E(\varphi(y_j))=p\inf v_E(y_j)\geq pv_E(x)+pc_0.$$

So, if $v_E(x)\geq\frac{-pc_0}{p-1}+1$, then $v_E(\varphi^n(x))\geq p^n$. It implies $y=\sum\limits_{i=1}^{+\infty}\varphi^i(x)$ converges in D. Now

$$(\psi-1)y=\sum_{i=0}^{+\infty}\varphi^i(x)-\sum_{i=1}^{+\infty}\varphi^i(x)=x$$

implies that $(\psi-1)D$ contains $\{x|v_E(x)\geq\frac{-pc_0}{p-1}+1\}$. □

Proposition 5.3.8. *If D is an étale φ-module over A_K(resp. over B_K), then:*

(i) *$D^{\psi=1}$ is compact (resp. locally compact);*

(ii) *$D/(\psi-1)$ is finitely generated over $\mathbb{Z}_p$(resp. over $\mathbb{Q}_p$).*

Proof. We can reduce to $K=\mathbb{Q}_p$. B_K follows from A_K by $\mathbb{Q}_p\otimes_{\mathbb{Z}_p}-$. So we consider D over $A_{\mathbb{Q}_p}$.

(i) Note that $D^{\psi=1}=\varprojlim(D/p^nD)^{\psi=1}$. From the previous lemma we have D/p^nD is compact by easy induction on n. So $D^{\psi=1}$ is compact.

(ii) The quotient $(D/(\psi-1))/p\simeq(D/p)/\psi-1$ is finite dimensional over $\mathbb{F}_p$. We have to check that if $x = (\psi - 1)y_n + p^n\mathbb{Z}_p$ for all n, then $x \in (\psi - 1)D$.

If $m \geq n$, $y_m - y_n \in (D/p^n)^{\psi=1}$, which is compact, we can extract a sequence converging $\bmod p^n$. Thus we can diagonally extract a sequence converging $\bmod p^n$ for all n. Then y_n converges to y in D and $x = (\psi - 1)y$. □

5.3.3 The Γ-module $D^{\psi=0}$.

If $p \neq 2$, we let $\Gamma_0 = \Gamma_{\mathbb{Q}_p} \simeq \mathbb{Z}_p^*$. Let $\Gamma_n \subseteq \Gamma_0$ and $\Gamma_n \simeq 1 + p^n\mathbb{Z}_p$ if $n \geq 1$. Then $\Gamma_0 = \triangle \times \Gamma_1$ where $\triangle = \boldsymbol{\mu}_{p-1}$, and $\Gamma_n = \varprojlim_m \Gamma_n/\Gamma_{n+m}$. We define

$$\mathbb{Z}_p[[\Gamma_n]] = \varprojlim \mathbb{Z}_p[\Gamma_n/\Gamma_{n+m}] = \mathcal{D}(\Gamma_n, \mathbb{Z}_p).$$

If $n \geq 1$, let γ_n be a topological generator of Γ_n. So $\Gamma_n = \gamma_n^{\mathbb{Z}_p}$. The correspondence

$$\begin{array}{ccccc} \mathbb{Z}_p[[\Gamma_n]] & \xleftarrow{\sim} & \mathbb{Z}_p[[T]] & \xrightarrow{\sim} & A_{\mathbb{Q}_p}^+ \\ \\ \gamma_n - 1 & \longleftarrow\!\!\shortmid & T & \longmapsto & \pi \end{array}$$

is just the Amice transform. Then

$$\begin{aligned} &\mathbb{Z}_p[[\Gamma_0]] = \mathbb{Z}_p[\triangle] \otimes \mathbb{Z}_p[[\Gamma_1]], \\ &\mathbb{Z}_p\{\{\Gamma_n\}\} := (\mathbb{Z}_p[[\Gamma_n]][(\gamma_n - 1)^{-1}])^\wedge \simeq A_{\mathbb{Q}_p} \text{ (as a ring)}, \\ &\mathbb{Z}_p\{\{\Gamma_0\}\} = \mathbb{Z}_p[\triangle] \otimes \mathbb{Z}_p\{\{\Gamma_1\}\}. \end{aligned}$$

Modulo p, we get $\mathbb{F}_p\{\{\Gamma_n\}\} \simeq E_{\mathbb{Q}_p}$ as a ring.

Remark. $\mathbb{Z}_p[[\Gamma_0]] \simeq \mathcal{D}_0(\Gamma_0, \mathbb{Z}_p) \simeq \mathcal{D}_0(\mathbb{Z}_p^*, \mathbb{Z}_p) \simeq (A_{\mathbb{Q}_p}^+)^{\psi=0}$. So $(A_{\mathbb{Q}_p}^+)^{\psi=0}$ is a free $\mathbb{Z}_p[[\Gamma_0]]$-module of rank 1. This a special case of a general theorem which will come up later on.

Lemma 5.3.9. (i) *If M is a topological $\mathbb{Z}_p$-module ($M = \varprojlim M/M_i$) with a continuous action of Γ_n (i.e. for all i, there exists k, such that Γ_{n+k} acts trivially on M/M_i), then $\mathbb{Z}_p[[\Gamma_n]]$ acts continuously on M;*

(ii) *If $\gamma_n - 1$ has a continuous inverse, then $\mathbb{Z}_p\{\{\Gamma_n\}\}$ also acts continuously on M.*

Lemma 5.3.10. (i) *If* $n \geq 1$, $v_E(\gamma_n(\bar{\pi}) - \bar{\pi}) = p^n v_E(\bar{\pi})$;

(ii) *For all* x *in* $E_{\mathbb{Q}_p}$, *we have* $v_E(\gamma_n(x) - x) \geq v_E(x) + (p^n - 1)v_E(\bar{\pi})$.

Proof. Since $\chi(\gamma) = 1 + p^n u,\ u \in \mathbb{Z}_p^*$, we have

$$\begin{aligned}\gamma_n(\bar{\pi}) - \bar{\pi} =&\gamma_n(1+\bar{\pi}) - (1+\bar{\pi}) = (1+\bar{\pi})((1+\bar{\pi})^{p^n u} - 1)\\ =&(1+\bar{\pi})((1+\bar{\pi})^u - 1)^{p^n}.\end{aligned}$$

Then we get (i).

In general, for $x = \sum_{k=k_0}^{+\infty} a_k \bar{\pi}^k$, then $v_E(x) = k_0 v_E(\bar{\pi})$. Now

$$\frac{\gamma_n(x) - x}{\gamma_n(\bar{\pi}) - \bar{\pi}} = \sum_{k=k_0}^{+\infty} a_k \frac{\gamma_n(\bar{\pi})^k - \bar{\pi}^k}{\gamma_n(\bar{\pi}) - \bar{\pi}},$$

and

$$v_E(\frac{\gamma_n(\bar{\pi})^k - \bar{\pi}^k}{\gamma_n(\bar{\pi}) - \bar{\pi}}) \geq (k-1)v_E(\bar{\pi}).$$

□

Proposition 5.3.11. *Let* D *be an étale* (φ, Γ)*-module of dimension* d *over* $E_{\mathbb{Q}_p}$. *Assume* $n \geq 1$, $(i,p) = 1$. *Then*

(i) $\gamma \in \Gamma$ *induces* $\varepsilon^i \varphi^n(D) \simeq \varepsilon^{\chi(\gamma)i}\varphi^n(D)$;

(ii) $\gamma_n - 1$ *admits a continuous inverse on* $\varepsilon^i\varphi^n(D)$. *Moreover if* $\{e_1, \cdots, e_d\}$ *is a basis of* D, *then:*

$$\begin{aligned}\mathbb{F}_p\{\{\Gamma_n\}\}^d &\xrightarrow{\sim} \varphi^n(D)\\ (\lambda_1, \cdots, \lambda_d) &\longmapsto \lambda_1 * \varepsilon^i\varphi^n(e_1) + \cdots + \lambda_d * \varepsilon^i\varphi^n(e_d)\end{aligned}$$

is a topological isomorphism.

Proof. (i) is obvious. Now, remark that (ii) is true for $n+1$ implies (ii) is true for n, since

$$\varepsilon^i\varphi^n(D) = \varepsilon^i\varphi^n(\oplus_{j=0}^{p-1}\varepsilon^j\varphi(D)) = \oplus_{j=0}^{p-1}\varepsilon^{i+p^n j}\varphi^{n+1}(D),$$

and for $n > 1$, $\gamma_{n+1} = \gamma_n^p$, so $\frac{1}{\gamma_n - 1} = \frac{1}{\gamma_{n+1}-1}(1 + \gamma_n + \cdots + \gamma_n^{p-1})$, and

$$\mathbb{F}_p\{\{\Gamma_n\}\} = \mathbb{F}_p\{\{\Gamma_{n+1}\}\} + \cdots + \gamma_n^{p-1}\mathbb{F}_p\{\{\Gamma_{n+1}\}\}.$$

So we can assume n big enough.

Recall $v_E(x) = \inf_i v_E(x_i)$ if $x = \sum_i x_i e_i$. We can, in particular, assume $v_E(\gamma_n(e_i) - e_i) \geq 2v_E(\bar{\pi})$, it implies $v_E(\gamma_n(x) - x) \geq v_E(x) + 2v_E(\bar{\pi})$ for all $x \in D$ (as $v_E(\gamma_n(x) - x) \geq v_E(x) + (p^n - 1)v_E(\bar{\pi})$ for all $x \in E_{\mathbb{Q}_p}$). Now

$$\chi(\gamma_n) = 1 + p^n u,\ u \in \mathbb{Z}_p^*,$$

so

$$\gamma_n(\varepsilon^i \varphi^n(x)) - \varepsilon^i \varphi^n(x) = \varepsilon^i(\varepsilon^{ip^n u}\varphi^n(\gamma_n(x)) - \varphi^n(x)) = \varepsilon^i \varphi^n(\varepsilon^{iu}\gamma_n(x) - x).$$

So we have to prove $x \mapsto f(x) = \varepsilon^{iu}\gamma_n(x) - x$ has a continuous inverse on D, and D is a $\mathbb{F}_p\{\{f\}\}$-module with basis $\{e_1, \cdots, e_d\}$. Let $\alpha = \varepsilon^{iu} - 1$; $iu \in \mathbb{Z}_p^*$, so $v_E(\alpha) = v_E(\bar{\pi})$. Then $v_E(\frac{f}{\alpha}(x) - x) \geq v_E(x) + v_E(\bar{\pi})$. It implies $\frac{f}{\alpha}$ has an inverse

$$g = \sum_{n=0}^{+\infty}(1 - \frac{f}{\alpha})^n \text{ and } v_E(g(x) - x) \geq v_E(x) + v_E(\bar{\pi}).$$

So f has an inverse $f^{-1}(x) = g(\frac{x}{\alpha})$ and $v_E(f^{-1}(x) - \frac{x}{\alpha}) \geq v_E(x)$.

By induction, for all k in $\mathbb{Z}$, we have

$$v_E(f^k(x) - \alpha^k x) \geq v_E(x) + (k+1)v_E(\bar{\pi}).$$

Let $M = E_{\mathbb{Q}_p}^+ e_1 \oplus \cdots \oplus E_{\mathbb{Q}_p}^+ e_d$, then f^k induces

$$M/\bar{\pi}M \simeq \alpha^k M/\alpha^{k+1}M \simeq \bar{\pi}^k M/\bar{\pi}^{k+1}M.$$

So $f^k\mathbb{F}_p[[f]]e_1 \oplus \cdots \oplus f^k\mathbb{F}_p[[f]]e_d$ is dense in $\bar{\pi}^k M$ and is equal by compactness. □

Corollary 5.3.12. *$\gamma - 1$ has a continuous inverse on $D^{\psi=0}$, and $D^{\psi=0}$ is a free $\mathbb{F}_p\{\{\Gamma_0\}\}$-module with basis $\{\varepsilon\varphi(e_1), \cdots, \varepsilon\varphi(e_d)\}$.*

Proof. Copy the proof that (ii) for $n+1$ implies (ii) for n in the previous proposition, using $\gamma_1 = \gamma_0^{p-1}$. □

Proposition 5.3.13. *If D is an étale (φ,Γ)-module over A_K or B_K, then $\gamma - 1$ has a continuous inverse on $D^{\psi=0}$.*

Proof. B_K follows from A_K by $\mathbb{Q}_p \otimes_{\mathbb{Z}_p}$; and we can reduce A_K to $A_{\mathbb{Q}_p}$.

Since $D^{\psi=0} \to (D/p)^{\psi=0}$ is surjective, $(\sum\limits_{i=1}^{p-1} \varepsilon^i \varphi(x_i)$ can be lifted to $\sum\limits_{i=1}^{p-1} [\varepsilon]^i \varphi(\hat{x}_i))$, so we have the following exact sequence:

$$0 \longrightarrow (pD)^{\psi=0} \longrightarrow D^{\psi=0} \longrightarrow (D/p)^{\psi=0} \longrightarrow 0.$$

Everything is complete for the p-adic topology, so we just have to verify the result $\bmod p$, which is in corollary 5.3.12. □

5.3.4 Computation of Galois chomology groups

Proposition 5.3.14. *Let $C_{\psi,\gamma}$ be the complex*

$$0 \to D(V) \xrightarrow{(\psi-1,\ \gamma-1)} D(V) \oplus D(V) \xrightarrow{(\gamma-1)\,\mathrm{pr}_1 - (\psi-1)\,\mathrm{pr}_2} D(V) \to 0.$$

Then we have a commutative diagram of complexes

$$\begin{array}{ccccccccc}
C_{\varphi,\gamma} : 0 & \longrightarrow & D(V) & \longrightarrow & D(V) \ \oplus \ D(V) & \longrightarrow & D(V) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathrm{Id}} & & \downarrow{\scriptstyle -\psi} \quad \downarrow{\scriptstyle \mathrm{Id}} & & \downarrow{\scriptstyle -\psi} & & \\
C_{\psi,\gamma} : 0 & \longrightarrow & D(V) & \longrightarrow & D(V) \ \oplus \ D(V) & \longrightarrow & D(V) & \longrightarrow & 0
\end{array}$$

which induces an isomorphism on cohomology.

Proof. Since $(-\psi)(\varphi - 1) = \psi - 1$ and ψ commutes with γ (i.e. $\psi\gamma = \gamma\psi$), the diagram commutes. ψ is surjective, hence the cokernel complex is 0. The kernel is nothing but

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

it has no cohomology by Proposition 5.3.13. □

Theorem 5.3.15. *If V is a $\mathbb{Z}_p$ or a $\mathbb{Q}_p$-representation of G_K, then $C_{\psi,\gamma}(K, V)$ computes the Galois cohomology of V:*

(i) $H^0(G_K, V) = D(V)^{\psi=1,\gamma=1} = D(V)^{\varphi=1,\gamma=1}$.

(ii)$H^2(G_K, V) \simeq \frac{D(V)}{(\psi-1,\gamma-1)}$.

(iii) *One has an exact sequence*

$$\begin{array}{ccccccccc}
0 \longrightarrow & \dfrac{D(V)^{\psi=1}}{\gamma-1} & \longrightarrow & H^1(G_K, V) & \longrightarrow & \left(\dfrac{D(V)}{\psi - 1}\right)^{\gamma=1} & \longrightarrow 0 \\
 & & & (x, y) & \longmapsto & x &
\end{array}$$

Let $\mathcal{C}(V)=(\varphi-1)D^{\psi-1}\subset D^{\psi=0}$, the exact sequence

$$0\longrightarrow D(V)^{\varphi=1}\longrightarrow D(V)^{\psi=1}\longrightarrow \mathcal{C}(V)\longrightarrow 0$$

induces an exact sequence

$$0\longrightarrow \frac{D(V)^{\varphi=1}}{\gamma-1}\longrightarrow \frac{D(V)^{\psi=1}}{\gamma-1}\longrightarrow \frac{\mathcal{C}(V)}{\gamma-1}\longrightarrow 0$$

since $\mathcal{C}(V)^{\gamma=1}\subset (D^{\psi=0})^{\gamma=1}=0$.

Proposition 5.3.16. *If D is an étale (φ,Γ)-module of dimension d over $E_{\mathbb{Q}_p}$, then $\mathcal{C}=(\varphi-1)D^{\psi=1}$ is a free $\mathbb{F}_p[[\Gamma_0]]$-module of rank d.*

Proof. We know:

- $\mathcal{C}\subset D^{\psi=0}$, it implies $\mathcal{C}$ is a $\mathbb{F}_p[[\Gamma_0]]$-module of rank less than d;
- $\mathcal{C}$ is compact, because $D^{\psi=1}$ is compact;
- So we just have to prove (see proposition 5.3.11 and corollary 5.3.12) that $\mathcal{C}$ contains $\{\varepsilon\varphi(e_1),\cdots,\varepsilon\varphi(e_d)\}$, where $\{e_1,\cdots,e_d\}$ is any basis of D over $E_{\mathbb{Q}_p}$.

Let $\{f_1,\cdots,f_d\}$ be any basis. Then $\varphi^n(\bar{\pi}^k f_i)$ goes to 0 when n goes to $+\infty$ if $k\gg 0$. Let $g_i=\sum\limits_{n=0}^{+\infty}\varphi^n(\varepsilon\varphi(\bar{\pi}^k f_i))$. Then we have:

- $\psi(g_i)=g_i$, because $\psi(\varepsilon\varphi(\bar{\pi}^k f_i))=0$;
- $(\varphi-1)g_i=-\varepsilon\varphi(\bar{\pi}^k f_i)\in\mathcal{C}$.

We can take $e_i=\bar{\pi}^k f_i$. □

5.3.5 The Euler-Poincaré formula.

Theorem 5.3.17. *If V is a finite $\mathbb{Z}_p$-representation of G_K, then*

$$\chi(V)=\prod_{i=0}^{2}|H^i(G_K,V)|^{(-1)^i}=|V|^{-[K:\mathbb{Q}_P]}.$$

Proof. From Shapiro's lemma, we have

$$H^i(G_K, V) \simeq H^i(G_{\mathbb{Q}_p}, \mathrm{Ind}_{G_K}^{G_{\mathbb{Q}_p}} V).$$

Since $|\mathrm{Ind}_{G_K}^{G_{\mathbb{Q}_p}} V| = |V|^{[K:\mathbb{Q}_p]}$, we can assume $K = \mathbb{Q}_p$. Given an exact sequence

$$0 \to V_1 \to V \to V_2 \to 0,$$

then $\chi(V) = \chi(V_1)\chi(V_2)$ and $|V| = |V_1||V_2|$ from the long exact sequence in Galois Cohomology, thus we can reduce to the case that V is a $\mathbb{F}_p$-representation of G_K. Then we have:

$$\begin{aligned} |H^0| &= |D(V)^{\varphi=1,\gamma=1}|; \\ |H^1| &= |\frac{D(V)^{\varphi=1}}{\gamma-1}| \cdot |\frac{\mathcal{C}(V)}{\gamma-1}| \cdot |\left(\frac{D(V)}{\psi-1}\right)^{\gamma=1}|; \\ |H^2| &= |\frac{D(V)}{(\psi-1,\gamma-1)}|. \end{aligned}$$

So $|H^0||H^2||H^1|^{-1} = |\frac{\mathcal{C}(V)}{\gamma-1}|^{-1}$, because $D(V)^{\varphi=1}$ and $\frac{D(V)}{\psi-1}$ are finite groups, and for a finite group M, the exact sequence:

$$0 \longrightarrow M^{\gamma=1} \longrightarrow M \xrightarrow{\gamma-1} M \longrightarrow \frac{M}{\gamma-1} \longrightarrow 0$$

implies that $|M^{\gamma=1}| = |\frac{M}{\gamma-1}|$. Now $\frac{\mathcal{C}(V)}{\gamma-1}$ is a $(\mathbb{F}_p[[\Gamma_0]]/(\gamma-1)) = \mathbb{F}_p$-module of rank $\dim_{E_{\mathbb{Q}_p}} D(V) = \dim_{\mathbb{F}_p} V$. Hence $|\frac{\mathcal{C}(V)}{\gamma-1}| = |V|$. □

5.4 Tate's duality and residues

Let M be a finite $\mathbb{Z}_p$ module. We want to construct a perfect pairing

$$H^i(G_K, M) \times H^{2-i}(G_K, M^\wedge(1)) \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p.$$

By using Shapiro's lemma, we may assume $K = \mathbb{Q}_p$.

Definition 5.4.1. Let $x = \sum_{k\in\mathbb{Z}} a_k\pi^k \in B_{\mathbb{Q}_p}$, define

$$\mathrm{res}(x\mathrm{d}\pi) = a_{-1}.$$

The residue of x, denoted by $\mathrm{Res}(x)$ is defined as

$$\mathrm{Res}(x) = \mathrm{res}(x\frac{\mathrm{d}\pi}{1+\pi}).$$

The map Res : $B_{\mathbb{Q}_p} \to \mathbb{Q}_p$ maps $A_{\mathbb{Q}_p}$ to $\mathbb{Z}_p$, thus it induced a natural map $B_{\mathbb{Q}_p}/A_{\mathbb{Q}_p} \to \mathbb{Q}_p/\mathbb{Z}_p$.

Proposition 5.4.2.

$$\begin{aligned} \operatorname{Res}(\psi(x)) &= \operatorname{Res}(x); \\ \operatorname{Res}(\gamma(x)) &= \chi(\gamma)^{-1}\operatorname{Res}(x) \end{aligned}$$

Proof. Exercise. □

Let D be an étale (φ,Γ)-module over $A_{\mathbb{Q}_p}$, denote $D^\vee = \operatorname{Hom}_{A_{\mathbb{Q}_p}}(D, B_{\mathbb{Q}_p}/A_{\mathbb{Q}_p})$, let $x \in D^\vee,\ y \in D$, denote

$$\langle x, y\rangle = x(y) \in B_{\mathbb{Q}_p}/A_{\mathbb{Q}_p}.$$

Then

$$\begin{aligned} \langle \gamma(x), \gamma(y)\rangle &= \gamma(\langle x, y\rangle), \\ \langle \varphi(x), \varphi(y)\rangle &= \varphi(\langle x, y\rangle) \end{aligned}$$

determines the (φ,Γ)-module structure on $D^\vee$. Set

$$[x, y] := \operatorname{Res}(\langle x, y\rangle) \in \mathbb{Q}_p/\mathbb{Z}_p.$$

The main step is following proposition.

Proposition 5.4.3. (i) *The map $x \mapsto (y \mapsto [x, y])$ gives an isomorphism from $D^\vee$ to $D^\wedge(V) = \operatorname{Hom}_{cont}(D, \mathbb{Q}_p/\mathbb{Z}_p)$.*

(ii) *The following formulas hold:*

$$\begin{aligned} [x, \varphi(y)] &= [\psi(x), y] \\ [\gamma(x), y] &= \chi(\gamma)^{-1}[x, \gamma^{-1}(y)]. \end{aligned}$$

Corollary 5.4.4. *Let $V^\wedge(1) = \operatorname{Hom}_{\mathbb{Z}_p}(V, (\mathbb{Q}_p/\mathbb{Z}_p)(1))$, then $D(V^\wedge(1)) = D^\vee(1)$.*

Now the two complexes

$$C_{\varphi,\gamma}(\mathbb{Q}_p, V): \quad D(V) \xrightarrow{d_1} D(V) \oplus D(V) \xrightarrow{d_2} D(V)$$

$$D^\vee(V) \xleftarrow{d_2{}'} D^\vee(1) \oplus D^\vee(1) \xleftarrow{d'{}_1} D^\vee(1) \ : C_{\psi,\gamma^{-1}}(\mathbb{Q}_p, V^\wedge(1))$$

are in duality, where $d_1 z = ((\varphi - 1)z, (\gamma - 1)z)$, $d_2(x, y) = (\gamma - 1)x - (\varphi - 1)y$, ${d'}_1 z' = ((\psi - 1)z', (\gamma^{-1} - 1)z')$, ${d_2}'(x', y') = (\gamma^{-1} - 1)x' - (\psi - 1)y'$, and the duality map in the middle given by $[(x, y), (x', y')] = [x', x] - [y', y]$.

One can check that the images are closed. Therefore their cohomology are in duality. For details, see Herr's paper in Math Annalen (2001?).

Chapter 6

(φ, Γ)-modules and Iwasawa theory

6.1 Iwasawa modules $H^i_{\mathrm{Iw}}(K, V)$

6.1.1 Projective limits of cohomology groups

In this chapter we assume that K is a finite extension of $\mathbb{Q}_p$ and G_K is the Galois group of $\bar{K}/K$. Then $K_n = K(\boldsymbol{\mu}_{p^n})$ and $\Gamma_n = \mathrm{Gal}(K_\infty/K_n) = \gamma_n^{\mathbb{Z}_p}$ if $n \geq 1$ ($n \geq 2$ if $p = 2$) where γ_n is a topological generator of Γ_n. We choose γ_n such that $\gamma_n = \gamma_1^{p^{n-1}}$. The *Iwasawa algebra* $\mathbb{Z}_p[[\Gamma_K]]$ is isomorphic to $\mathbb{Z}_p[[T]]$ with the (p,T)-adic topology by sending T to $\gamma - 1$. We have

$$\mathbb{Z}_p[[\Gamma_K]]/(\gamma_n - 1) = \mathbb{Z}_p[\mathrm{Gal}(K_n/K)].$$

Furthermore $\mathbb{Z}_p[[\Gamma_K]]$ is a G_K-module: let $g \in G_K$ and $x \in \mathbb{Z}_p[[\Gamma_K]]$, then $gx = \bar{g}x$, where $\bar{g}$ is the image of g in Γ_K. By the same way, G_K acts on $\mathbb{Z}_p[\mathrm{Gal}(K_n/K)]$.

Using Shapiro's Lemma, we get, for M a $\mathbb{Z}_p[G_K]$-module,

$$H^i(G_{K_n}, M) \xrightarrow{\sim} H^i(G_K, \mathbb{Z}_p[\mathrm{Gal}(K_n/K)] \otimes M),$$

with the inverse map given by

$$\big((\sigma_1, ..., \sigma_i) \mapsto \sum_{g \in \mathrm{Gal}(K_n/K)} g \otimes C_g(\sigma_1, ..., \sigma_i)\big) \longmapsto \big((\sigma_1, ..., \sigma_i) \mapsto C_{\mathrm{id}}(\sigma_1, ..., \sigma_i)\big).$$

Thus we have a commutative diagram:

$$\begin{tikzcd} H^i(G_{K_{n+1}}, M) \arrow[r, "\sim"] \arrow[d, "\mathrm{cor}"'] & H^i(G_K, \mathbb{Z}_p[\mathrm{Gal}(K_{n+1}/K)] \otimes M) \arrow[d] \\ H^i(G_{K_n}, M) \arrow[r, "\sim"] & H^i(G_K, \mathbb{Z}_p[\mathrm{Gal}(K_n/K)] \otimes M) \end{tikzcd}$$

One can check that the second vertical arrow is just induced by the natural map $\mathrm{Gal}(K_{n+1}/K) \to \mathrm{Gal}(K_n/K)$.

Definition 6.1.1. (i) If V is a $\mathbb{Z}_p$-representation of G_K, define

$$H^i_{\mathrm{Iw}}(K, V) = \varprojlim_n H^i(G_{K_n}, V)$$

while the transition maps are the corestriction maps.

(ii) If V is a $\mathbb{Q}_p$-representation, choose T a stable $\mathbb{Z}_p$-lattice in V, then define

$$H^i_{\mathrm{Iw}}(K, V) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^i_{\mathrm{Iw}}(K, T).$$

6.1.2 Reinterpretation in terms of measures

Proposition 6.1.2. $H^i(G_K, \mathbb{Z}_p[[\Gamma_K]] \otimes V) \cong H^i_{\mathrm{Iw}}(K, V)$.

Proof. The case of $\mathbb{Q}_p$ follows from the case of $\mathbb{Z}_p$ by using $\mathbb{Q}_p \otimes_{\mathbb{Z}_p}$. Now assume that V is a $\mathbb{Z}_p$-representation of G_K. By definition,

$$\Lambda = \mathbb{Z}_p[[\Gamma_K]] = \varprojlim \mathbb{Z}_p[[\Gamma_K]]/(\gamma_n - 1),$$

it induces the map θ:

$$\begin{tikzcd} H^i(G_K, \Lambda \otimes V) \arrow[r, "\theta"] \arrow[dr, "\alpha"] & \varprojlim H^i(G_K, \Lambda/(\gamma_n - 1) \otimes V) = H^i_{\mathrm{Iw}}(K, V) \arrow[d] \\ & \varprojlim H^i(G_K, \Lambda/(p^n, \gamma_n - 1) \otimes V) \end{tikzcd}$$

The surjectivity is general abstract nonsense.

The injectivity of α implies the injectivity of θ; to prove that of α, it is enough to verify the Mittag-Leffler conditions of H^{i-1}, which are automatic, because of the Finiteness Theorem: $\Lambda/(p^n, \gamma_n - 1) \otimes V$ is a finite module, so $H^{i-1}(G_K, \Lambda/(p^n, \gamma_n - 1) \otimes V)$ is a finite group. $\square$

Remark. (i) Recall that $\mathcal{D}_0(\Gamma_K, V)$ is the set of p-adic measures from Γ_K to V:

$$\mathbb{Z}_p[[\Gamma_K]] \otimes V \cong \mathcal{D}_0(\Gamma_K, V), \quad \gamma \otimes v \mapsto \delta_\gamma \otimes v,$$

where δ_γ is the Dirac measure at γ. Let $g \in G_K$, $\mu \in \mathcal{D}_0(\Gamma_K, V)$; the action of G_K on $\mathcal{D}_0(\Gamma_K, V)$ is as follow:

$$\int_{\Gamma_K} \phi(x)(g\mu) = g(\int_{\Gamma_K} \phi(\bar{g}x)\mu).$$

Hence, for any $n \in \mathbb{N}$, the map $H^i(G_K, \mathbb{Z}_p[[\Gamma_K]] \otimes V) \to H^i(G_{K_n}, V)$ (translation of Shapiro's lemma) can be written in the following concrete way:

$$\big((\sigma_1, ..., \sigma_i) \mapsto \mu(\sigma_1, ..., \sigma_i)\big) \longmapsto \big((\sigma_1, ..., \sigma_i) \mapsto \int_{\Gamma_K} 1_{\Gamma_{K_n}} \cdot \mu(\sigma_1, ..., \sigma_i) \in V\big)_{n\in\mathbb{N}}.$$

(ii) Let $g \in G_K$, $\lambda, \mu \in \mathbb{Z}_p[[\Gamma_K]]$, $x \in V$, then

$$g(\lambda\mu \otimes v) = \bar{g}\lambda\mu \otimes gv = \lambda\bar{g}\mu \otimes gv = \lambda g(\mu \otimes \mu).$$

So λ and g commutes, it implies that $H^i_{\mathrm{Iw}}(K, V)$ are $\mathbb{Z}_p[[\Gamma_K]]$-modules.

6.1.3 Twist by a character (à la Soulé)

Let $\eta : \Gamma_K \to \mathbb{Q}_p^*$ be a continuous character. It induces a transform

$$\mathcal{D}_0(\Gamma_K, V) \to \mathcal{D}_0(\Gamma_K, V), \quad \mu \mapsto \eta \cdot \mu.$$

For $\lambda \in \mathbb{Z}_p[[\Gamma_K]]$, we have

$$\eta \cdot (\lambda\mu) = (\eta \cdot \lambda)(\eta \cdot \mu).$$

Indeed, it is enough to check it on Dirac measures. In this case

$$\eta \cdot (\delta_{\lambda_1}\delta_{\lambda_2} \otimes v) = \eta(\lambda_1\lambda_2)\delta_{\lambda_1}\delta_{\lambda_2} \otimes v = (\eta \cdot \delta_{\lambda_1})(\eta \cdot \delta_{\lambda_2}) \otimes v.$$

Recall that $\mathbb{Z}_p(\eta) = \mathbb{Z}_p \cdot e_\eta$, where, if $g \in G_K$, then $ge_\eta = \eta(\bar{g})e_\eta$. Define $V(\eta) = V \otimes \mathbb{Z}_p(\eta)$.

Exercise. The map $\mu \in \mathcal{D}_0(\Gamma_K, V) \mapsto (\eta \cdot \mu) \otimes e_\eta \in \mathcal{D}_0(\Gamma_K, V)$ is an isomorphism of $\mathbb{Z}_p[G_K]$-modules.

By the above exercise, we have a commutative diagram:

$$\begin{tikzcd} H^i_{\mathrm{Iw}}(K,V) \arrow[r, "i_\eta"] \arrow[d, equal] & H^i_{\mathrm{Iw}}(K,V(\eta)) \arrow[d, equal] \\ H^i(G_K,\mathcal{D}_0(\Gamma_K,V)) \arrow[r, "\sim"] & H^i(G_K,\mathcal{D}_0(\Gamma_K,V(\eta))) \end{tikzcd}$$

So i_η is an isomorphism of cohomology groups. It can be written in a concrete way

$$i_\eta : \ \big((\sigma_1,...,\sigma_i)\mapsto \mu(\sigma_1,...,\sigma_i)\big) \ \longmapsto \ \Big((\sigma_1,...,\sigma_i)\mapsto \int_{\Gamma_K} 1_{\Gamma_{K_n}}\eta\cdot\mu(\sigma_1,...,\sigma_i)\otimes e_\eta\Big)_{n\in\mathbb{N}}.$$

It is an isomorphism of $\mathbb{Z}_p$-modules.
Warning: i_η is not an isomorphism of $\mathbb{Z}_p[[\Gamma_K]]$-modules, because $i_\eta(\lambda x) = (\eta\cdot\lambda)i_\eta(x)$: there is a twist.

6.2 Description of H^i_{Iw} in terms of $D(V)$

Remark. $H^i_{\mathrm{Iw}}(K,V) = \varprojlim_{n\geq n_0} H^i(G_{K_n},V)$, so we can always assume $n \gg 0$.

Lemma 6.2.1. *Let* $\tau_n = \frac{\gamma_n-1}{\gamma_{n-1}-1} = 1+\gamma_{n-1}+,...,+\gamma_{n-1}^{p-1} \in \mathbb{Z}_p[[\Gamma_K]]$, *the diagram*

$$\begin{tikzcd} C_{\psi,\gamma_n}(K_n,V): & 0 \arrow[r] & D(V) \arrow[r] \arrow[d, "\tau_n"'] & D(V)\oplus D(V) \arrow[r] \arrow[d, "\tau_n \oplus \mathrm{Id}"] & D(V) \arrow[r] \arrow[d, "\mathrm{Id}"] & 0 \\ C_{\psi,\gamma_{n-1}}(K_{n-1},V): & 0 \arrow[r] & D(V) \arrow[r] & D(V)\oplus D(V) \arrow[r] & D(V) \arrow[r] & 0 \end{tikzcd}$$

is commutative and induces corestrictions on cohomology via

$$H^i(C_{\psi,\gamma_n}(K_n,V)) \xrightarrow{\sim} H^i(G_{K_n},V).$$

Proof. τ_n is a cohomological functor and induces $\mathrm{Tr}_{K_n/K_{n-1}}$ on H^0, so it induces corestrictions on H^i. $\square$

Theorem 6.2.2. *If V is a $\mathbb{Z}_p$ or $\mathbb{Q}_p$ representation of G_K, then we have:*

(i) $H^i_{\mathrm{Iw}}(K,V)=0$, *if* $i\neq 1,2$.

(ii) $H^1_{\mathrm{Iw}}(K,V)\cong D(V)^{\psi=1}$, $H^2_{\mathrm{Iw}}(K,V)\cong \frac{D(V)}{\psi-1}$, *and the isomorphisms are canonical.*

Remark. (i) The isomorphism

$$\mathrm{Exp}^*:\ H^1_{\mathrm{Iw}}(K,V)\to D(V)^{\psi=1}$$

is the map that will produce p-adic L-functions. Let's describe $(\mathrm{Exp}^*)^{-1}$. Let $y\in D(V)^{\psi-1}$, then $(\varphi-1)y\in D(V)^{\psi=0}$. There exists unique $x_n\in D(V)^{\psi=0}$ satisfying that $(\gamma_n-1)x_n=y_n$, then we can find $b_n\in A\otimes V$ such that $(\varphi-1)b_n=x_n$. Then

$$g\mapsto\frac{\log\chi(\gamma_n)}{p^n}\left(\frac{(g-1)}{(\gamma_n-1)}y-(g-1)b_n\right)$$

gives a cocycle on G_{K_n} with values in V, and $\frac{\log\chi(\gamma_n)}{p^n}$ does not depend on n. Denote by $\iota_{\psi,n}(y)\in H^1(G_{K_n},V)$ the image of this cocycle, then

$$(\mathrm{Exp}^*)^{-1}:\ y\longmapsto(\cdots,\iota_{\psi,n}(y),\cdots)_{n\in\mathbb{N}}\in H^1_{\mathrm{Iw}}(K,V)$$

doesn't depend on the choice of γ_n.

(ii) We see that $\frac{D(V)}{\psi-1}$ is dual to $D(V^\wedge(1))^{\psi=1}=V^\wedge(1)^{H_K}$, so $H^2_{\mathrm{Iw}}(K,V)=\frac{D(V)}{\psi-1}=(V^\wedge(1)^{H_K})^\wedge$.

Before proving the theorem, we introduce a lemma.

Lemma 6.2.3. *If M is compact with continuous action of Γ_K, then*

$$M\simeq\varprojlim_n(M/\gamma_n-1).$$

Proof. We have a natural map from M to $\varprojlim_n(M/\gamma_n-1)$.

Injectivity: let V be an open neighborhood of 0. For all $x\in M$, there exists $n_x\in\mathbb{N}$ and $U_x\ni x$, an open neighborhood of x such that $(\gamma-1)x'\in V$ for $\gamma\in\Gamma_{K_{n_x}}$ and $x'\in U_x$. By compactness, $M=\bigcup_{i\in I}U_{x_i}$, where I is a finite set. Let $n=\max_{i\in I}n_{x_i}$. It implies that $(\gamma-1)M\subset V$, if $\gamma\in\Gamma_n$, then $\bigcap_{n\in\mathbb{N}}(\gamma_n-1)M=0$, this shows the injectivity.

Surjectivity: Let $(x_n)_{n\in\mathbb{N}}\in\varprojlim_n(M/\gamma_n-1)$. From the proof of injectivity, we know that x_n is a Cauchy-sequence. Because M is compact, there exists $x=\lim x_n$. We have $x_{n+k}-x_n=(\gamma_n-1)y_k$ for all $k\geq 0$, as M is compact, there exists a subsequence of y_k converging to y, passing to the limit, we get $x-x_n=(\gamma_n-1)y$. This shows the surjectivity. $\square$

Proof of Theorem 6.2.2. $H^i_{\mathrm{Iw}}(K,V)$ is trivial if $i \geq 3$ and the case of $\mathbb{Q}_p$ follows from $\mathbb{Z}_p$ by $\mathbb{Q}_p \otimes_{\mathbb{Z}_p}$.

For $i=0$,

$$H^0_{\mathrm{Iw}}(K,V) = \varprojlim_{\mathrm{Tr}} V^{G_{K_n}}.$$

$V^{G_{K_n}}$ is increasing and $\subset V$, as V is a finite dimensional $\mathbb{Z}_p$-module, the sequence is stationary for $n \geq n_0$. Then $\mathrm{Tr}_{K_{n+1}/K_n}$ is just multiplication by p for $n \geq n_0$, but V does not contain p-divisible elements. This shows that $\varprojlim_{\mathrm{Tr}} V^{G_{K_n}} = 0$.

For $i=2$: $H^2(G_{K_n},V) = \frac{D(V)}{(\psi-1,\gamma_n-1)}$. The corestriction map is induced by Id on $D(V)$, thus

$$H^2_{\mathrm{Iw}}(K,V) = \varprojlim \frac{D(V)}{\psi-1}\Big/(\gamma_n-1) = \frac{D(V)}{\psi-1}$$

by Lemma 6.2.3, as $\frac{D(V)}{\psi-1}$ is compact (and even finitely generated over $\mathbb{Z}_p$).

For $i=1$: we have commutative diagrams:

$$\begin{tikzcd}
0 \arrow[r] & \frac{D(V)^{\psi=1}}{\gamma_n-1} \arrow[r] \arrow[d, "p_1"] & H^1(G_{K_n},V) \arrow[r, "p_2"] \arrow[d, "\mathrm{cor}"] & (\frac{D(V)}{\psi-1})^{\gamma_n=1} \arrow[r] \arrow[d, "\tau_n"] & 0 \\
0 \arrow[r] & \frac{D(V)^{\psi=1}}{\gamma_{n-1}-1} \arrow[r] & H^1(G_{K_{n-1}},V) \arrow[r] & (\frac{D(V)}{\psi-1})^{\gamma_{n-1}=1} \arrow[r] & 0
\end{tikzcd}$$

where $p_1(\bar{y}) = \bar{y}$, $p_2((\bar{x},\bar{y})) = \bar{x}$, for any $x,y \in D(V)$. Using the functor $\varprojlim$, we get:

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

Because $D(V)^{\psi=1}$ is compact, by Lemma 6.2.3 we have $D(V)^{\psi=1} \simeq \varprojlim \frac{D(V)^{\psi=1}}{\gamma_n-1}$. By definition, $H^1_{\mathrm{Iw}}(K,V) = \varprojlim H^1(G_{K_n},V)$. The same argument for showing $H^0_{\mathrm{Iw}}(K,V)=0$ shows that $\varprojlim (\frac{D(V)}{\psi-1})^{\gamma_n=1} = 0$. So we get

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

□

6.3 Structure of $H^1_{\mathrm{Iw}}(K,V)$

Recall that we proved that if D is an étale (φ,Γ)-module of dim d over $E_{\mathbb{Q}_p}$, then $\mathcal{C}=(\varphi-1)D^{\psi=1}$ is a free $\mathbb{F}_p[[\Gamma_{\mathbb{Q}_p}]]$-module of rank d. The same proof shows that if $n\geq 1$, $i\in\mathbb{Z}_p^*$, $\mathcal{C}\cap\varepsilon\varphi^n(D)$ is free of rank d over $\mathbb{F}_p[[\Gamma_n]]$.

Corollary 6.3.1. *If D is an étale (φ,Γ)-module of dimension d over E_K, then $\mathcal{C}$ is a free $\mathbb{F}_p[[\Gamma_K]]$-module of rank $d\cdot[K:\mathbb{Q}_p]$.*

Proof. Exercise. Hint: D is of dimension $d\cdot[H_{\mathbb{Q}_p}:H_K]$ over $E_{\mathbb{Q}_p}$ and $[K:\mathbb{Q}_p]=[G_{\mathbb{Q}_p}:G_K]=[\Gamma_{\mathbb{Q}_p}:\Gamma_K][H_{\mathbb{Q}_p}:H_K]$. □

Proposition 6.3.2. *If V is a free $\mathbb{Z}_p$ or $\mathbb{Q}_p$ representation of rank d of G_K, then*

(i) *$D(V)^{\varphi=1}$ is the torsion sub-$\mathbb{Z}_p[[\Gamma_K\cap\Gamma_1]]$-module of $D(V)^{\psi=1}$.*

(ii) *We have exact sequences:*

$$0\longrightarrow D(V)^{\varphi=1}\longrightarrow D(V)^{\psi=1}\xrightarrow{\varphi-1}\mathcal{C}(V)\longrightarrow 0.$$

and $\mathcal{C}(V)$ is free of rank $d\cdot[K:\mathbb{Q}_p]$ over $\mathbb{Z}_p[[\Gamma_K]]$ (or over $\mathbb{Q}_p\otimes_{\mathbb{Z}_p}\mathbb{Z}_p[[\Gamma_K]]$).

Corollary 6.3.3. *If V is a free $\mathbb{Z}_p$ representation of rank d of G_K, then the torsion $\mathbb{Z}_p[[\Gamma_K\cap\Gamma_1]]$-module of $H^1_{\mathrm{Iw}}(K,V)$ is $D(V)^{\varphi=1}=V^{H_K}$, and $H^1_{\mathrm{Iw}}(K,V)/V^{H_K}$ is free of rank $d\cdot[K:\mathbb{Q}_p]$ over $\mathbb{Z}_p[[\Gamma_K]]$.*

Proof of Proposition 6.3.2. $D(V)^{\varphi=1}=V^{H_K}$ is torsion because it is finitely generated over $\mathbb{Z}_p$, so (ii) implies (i). To prove (ii), we have to prove $\mathcal{C}(V)/p\mathcal{C}(V)$ is free of rank $d\cdot[K:\mathbb{Q}_p]$ over $\mathbb{F}_p[[\Gamma_K]]$.

Consider the following commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & D(V)^{\varphi=1} \arrow[r] \arrow[d] & D(V)^{\psi=1} \arrow[r, "\varphi-1"] \arrow[d] & \mathcal{C}(V) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & (D(V)/p)^{\varphi=1} \arrow[r] & (D(V)/p)^{\psi=1} \arrow[r, "\varphi-1"] & \mathcal{C}(V/p) \arrow[r] & 0
\end{tikzcd}$$

Using the exact sequence

$$0\to pV\to V\to V/p\to 0$$

and apply the snake lemma to the vertical rows of the diagram above, we have the cokernel complex is

$$p-\text{torsion of } \frac{D(V)}{(\varphi-1)} \to p-\text{torsion of } \frac{D(V)}{(\psi-1)} \to \frac{\mathcal{C}(V/p)}{\mathcal{C}(V)/p\mathcal{C}(V)} \to 0.$$

Note that the p-torsion of $\frac{D(V)}{(\psi-1)}$ is a finite dimensional $\mathbb{F}_p$-vector space, thus $\frac{\mathcal{C}(V/p)}{\mathcal{C}(V)/p\mathcal{C}(V)}$ is also a finite dimensional $\mathbb{F}_p$-vector space, hence $\mathcal{C}(V)/p\mathcal{C}(V)$ is a $\mathbb{F}_p[[\Gamma_K]]$-lattice of $\mathcal{C}(V/p)$, but $\mathcal{C}(V/p)$ is a free $\mathbb{F}_p[[\Gamma_K]]$-module of rank $d\cdot[K:\mathbb{Q}_p]$ by Corollary 6.3.1. □

Remark. (i) The sequence

$$0 \to D(V)^{\varphi=1} \to D(V)^{\psi=1} \to \mathcal{C}(V) \to 0$$

is just the inflation-restriction exact sequence

$$0 \to H^1(\Gamma_K, \Lambda\otimes V^{H_K}) \to H^1(G_K, \Lambda\otimes V) \to H^1(H_K, \Lambda\otimes V)^{\Gamma_K} \to 0.$$

(ii) Let $0 \to V_1 \to V \to V_2 \to 0$ be an exact sequence, then the exact sequence

$$0 \to D(V_1) \to D(V) \to D(V_2) \to 0$$

and the snake lemma induces

$$0 \to D(V_1)^{\psi=1} \to D(V)^{\psi=1} \to D(V_2)^{\psi=1} \to \frac{D(V_1)}{\psi-1} \to \frac{D(V)}{\psi-1} \to \frac{D(V_2)}{\psi-1} \to 0.$$

By Theorem 6.2.2, this is just

$$\begin{aligned}0 \to H^1_{\mathrm{Iw}}(K,V_1) \to& H^1_{\mathrm{Iw}}(K,V) \to H^1_{\mathrm{Iw}}(K,V_2)\\ \to& H^2_{\mathrm{Iw}}(K,V_1) \to H^2_{\mathrm{Iw}}(K,V) \to H^2_{\mathrm{Iw}}(K,V_2) \to 0.\end{aligned}$$

It can also be obtained from the longer exact sequence in continuous cohomology from the exact sequence

$$0 \to \mathbb{Z}_p[[\Gamma_K]]\otimes V_1 \to \mathbb{Z}_p[[\Gamma_K]]\otimes V \to \mathbb{Z}_p[[\Gamma_K]]\otimes V_2 \to 0.$$

Chapter 7

$\mathbb{Z}_p(1)$ and Kubota-Leopoldt zeta function

7.1 The module $D(\mathbb{Z}_p(1))^{\psi=1}$

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

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

Note that $D(\mathbb{Z}_p(1)) = (A \otimes \mathbb{Z}_p(1))^{H_{\mathbb{Q}_p}} = A_{\mathbb{Q}_p}(1)$, 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 $f(\pi) \in A_{\mathbb{Q}_p}(1)$.

Proposition 7.1.1. (i) $A_{\mathbb{Q}_p}^{\psi=1} = \mathbb{Z}_p \cdot \frac{1}{\pi} \oplus (A^+_{\mathbb{Q}_p})^{\psi=1}$.

(ii) *We have an exact sequence:*

$$0 \longrightarrow \mathbb{Z}_p \longrightarrow (A^+_{\mathbb{Q}_p})^{\psi=1} \xrightarrow{\varphi-1} (\pi A^+_{\mathbb{Q}_p})^{\psi=0} \longrightarrow 0.$$

Remark. Under the map $\mu \mapsto \int_{\mathbb{Z}_p} [\varepsilon]^x \mu$, $(\pi A^+_{\mathbb{Q}_p})^{\psi=0}$ is the image of measures with support in $\mathbb{Z}_p^*$ ($\psi = 0$) and $\int_{\mathbb{Z}_p^*} \mu = 0$

$$(\pi A^+_{\mathbb{Q}_p})^{\psi=0} = \mathcal{C}(\mathbb{Z}_p) = (\gamma - 1)\mathbb{Z}_p[[\Gamma_{\mathbb{Q}_p}]].$$

$\mathbb{Z}_p[[\Gamma_{\mathbb{Q}_p}]]$ can be viewed as measures on $\Gamma_{\mathbb{Q}_p} \cong \mathbb{Z}_p^*$, and $\mu \in (\gamma - 1)\mathbb{Z}_p[[\Gamma_{\mathbb{Q}_p}]]$ means $\int_{\mathbb{Z}_p} \mu = 0$. It implies that $\mathcal{C}(\mathbb{Z}_p)$ is free of rank 1 over $\mathbb{Z}_p[[\Gamma_{\mathbb{Q}_p}]]$ which is a special case of what we have proved.

Proof. (i) We have proved

$$\psi(A^+_{\mathbb{Q}_p}) \subset A^+_{\mathbb{Q}_p}, \quad \psi(\frac{1}{\pi}) = \frac{1}{\pi},$$
$$v_E(\psi(x)) \geq [\frac{v_E x}{p}], \quad \text{if } x \in E_{\mathbb{Q}_p}.$$

These facts imply that $\psi - 1$ is bijective on $E_{\mathbb{Q}_p}/\bar{\pi}^{-1}E^+_{\mathbb{Q}_p}$ and hence it is also bijective on $A_{\mathbb{Q}_p}/\pi^{-1}A^+_{\mathbb{Q}_p}$. So

$$\psi(x) = x \Rightarrow\ x \in \pi^{-1}A^+_{\mathbb{Q}_p}.$$

(ii) We know that $(\varphi - 1)A^+_{\mathbb{Q}_p} \subset \pi A^+_{\mathbb{Q}_p}$ For $x \in (\pi A^+_{\mathbb{Q}_p})^{\psi=0}$, then

$$\varphi^n(x) \in \varphi^n(\pi)A^+_{\mathbb{Q}_p} \to 0 \text{ if } n \to \infty.$$

Hence $y = \sum_{n=0}^{+\infty} \varphi^n(x)$ converges, and one check that $\psi(y) = y$, $(\varphi - 1)y = -x$. This implies the surjectivity of $\varphi - 1$. □

7.2 Kummer theory

Recall that

$$\varepsilon = (1, \varepsilon^{(1)}, \varepsilon^{(2)}, ..., \varepsilon^{(n)}, ...) \in E^+_{\mathbb{Q}_p} \subset \tilde{E}^+ = R,\ \varepsilon^{(1)} \neq 1.$$

Let $\pi_n = \varepsilon^{(n)} - 1$, $F_n = \mathbb{Q}_p(\pi_n)$ for $n \geq 1$. Then π_n is a uniforming parameter of F_n, and

$$\mathrm{N}_{F_{n+1}/F_n}(\pi_{n+1}) = \pi_n, \quad \mathcal{O}_{F_{n+1}} = \mathcal{O}_{F_n}[\pi_{n+1}]/((1 + \pi_{n+1})^p = 1 + \pi_n).$$

For an element $a \in F_n^*$, choose $x = (a, x^{(1)}, ...) \in \tilde{E}$. This x is unique up to ε^u with $u \in \mathbb{Z}_p$. So if $g \in G_{F_n}$, then

$$\frac{g(x)}{x} = \varepsilon^{c(g)}, \quad c(g) \in \mathbb{Z}_p$$

gives a 1-cocycle c on G_{F_n} with values in $\mathbb{Z}_p(1)$. This defines the Kummer map:

$$\begin{aligned} \kappa :\ F_n^* &\longrightarrow H^1(G_{F_n}, \mathbb{Z}_p(1)) \\ a &\longmapsto \kappa(a). \end{aligned}$$

By Kummer theory, we have $H^1(G_{F_n}, \mathbb{Z}_p(1)) = \mathbb{Z}_p \cdot \kappa(\pi_n) \oplus \kappa(\mathcal{O}_{F_n}^*)$. The diagram

$$\begin{array}{ccc} F_{n+1}^* & \xrightarrow{\kappa} & H^1(G_{F_{n+1}}, \mathbb{Z}_p(1)) \\ \downarrow{\scriptstyle \mathrm{N}_{F_{n+1}/F_n}} & & \downarrow{\scriptstyle \mathrm{cor}} \\ F_n^* & \xrightarrow{\kappa} & H^1(G_{F_n}, \mathbb{Z}_p(1)) \end{array}$$

is commutative, we have a map:

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

and

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

7.3 Coleman's power series

Theorem 7.3.1 (Coleman's power series). *Let $u = (u_n)_{n \geq 1} \in \varprojlim(\mathcal{O}_{F_n}) - \{0\}$ (pour les applications N_{F_{n+1}/F_n}), then there exists a unique power series $f_u \in \mathbb{Z}_p[[T]]$ such that $f_u(\pi_n) = u_n$ for all $n \geq 1$.*

Lemma 7.3.2. (i) *If $x \in \mathcal{O}_{F_n}$, $\gamma \in \mathrm{Gal}(F_{n+1}/F_n)$, then $\gamma(x) - x \in \pi_1 \mathcal{O}_{F_{n+1}}$.*
(ii) $\mathrm{N}_{F_{n+1}/F_n} x - x^p \in \pi_1 \mathcal{O}_{F_{n+1}}$.

Proof. It is easy to see that (i) implies (ii) since $[F_{n+1} : F_n] = p$. Write $\chi(\gamma) = 1 + p^n u$ for $u \in \mathbb{Z}_p$. Let $x = \sum_{i=0}^{p-1} x_i(1+\pi_{n+1})^i$, where $x_i \in \mathcal{O}_{F_n}$. Then

$$\gamma(x) - x = \sum_{i=0}^{p-1} x_i(1+\pi_{n+1})^i((1+\pi_1)^{iu} - 1) \in \pi_1 \mathcal{O}_{F_{n+1}}.$$

□

Corollary 7.3.3. *$\bar{u} = (\bar{u}_1^p, \bar{u}_1, ..., \bar{u}_n, ...) \in E_{\mathbb{Q}_p}^+$, where $\bar{u}_n$ is the image of $u_n \bmod \pi_1$.*

Definition 7.3.4. Let $\mathrm{N} : \mathcal{O}_{F_1}[[T]] \to \mathcal{O}_{F_1}[[T]]$ such that

$$\mathrm{N}(f)((1+T)^p - 1) = \prod_{z^p=1} f((1+T)z - 1).$$

Lemma 7.3.5. (i) $\mathrm{N}(f)(\pi_n) = \mathrm{N}_{F_{n+1}/F_n}(f(\pi_{n+1}))$,
(ii) $\mathrm{N}(\mathbb{Z}_p[[T]]) \subset \mathbb{Z}_p[[T]]$,
(iii) $\mathrm{N}(f) - f \in \pi_1\mathcal{O}_{F_1}[[T]]$,
(iv) *If* $f \in \mathcal{O}_{F_1}[[T]]^*$, $k \geq 1$, *if* $(f-g) \in \pi_1^k\mathcal{O}_{F_1}[[T]]$, *then*

$$\mathrm{N}(f) - \mathrm{N}(g) \in \pi_1^{k+1}\mathcal{O}_{F_1}[[T]].$$

Proof. (i) The conjugates of π_{n+1} under $\mathrm{Gal}(F_{n+1}/F_n)$ are those $(1+\pi_n)z-1$ for $z^p = 1$, this implies (i).

(ii) Obvious, is just Galois theory.

(iii) Look mod π_1, because $z = 1 \bmod \pi_1$, we have $\mathrm{N}(f)(T^p) = f(T)^p$.

(iv) We have $\mathrm{N}(\frac{f}{g}) = \frac{\mathrm{N}(f)}{\mathrm{N}(g)}$, so we can reduce to $f = 1$ and $g = 1 + \pi_1^k h$. Then

$$\mathrm{N}(g)((1+T)^p - 1) = 1 + \pi_1^k \sum_{z^p=1} h((1+T)z-1) \bmod \pi_1^{k+1},$$

and $\sum_{z^p=1} h((1+T)z-1)$ is divisible by p. □

Corollary 7.3.6. (i) *If* $\bar{u} \in E^+_{\mathbb{Q}_p}$ *and* $v_E(\bar{u}) = 0$, *then there exists a unique* $g_u \in \mathbb{Z}_p[[T]]$ *such that* $\mathrm{N}(g_u) = g_u$ *and* $g_u(\bar{\pi}) = \bar{u}$.
(ii) *If* $x \in 1 + \pi_1^k\mathcal{O}_{F_{n+1}}$, *then* $\mathrm{N}_{F_{n+1}/F_n}(x) \in 1 + \pi_1^{k+1}\mathcal{O}_{F_n}$.

Proof. (i) Take any $g \in \mathbb{Z}_p[[T]]$ such that $g(\bar{\pi}) = \bar{u}$, then $g \in \mathbb{Z}_p[[T]]^*$, by (iv) of Lemma 7.3.5, $\mathrm{N}^k(g)$ converges in $g + \pi_1\mathbb{Z}_p[[T]]$ and g_u is the limit.

(ii) There exists $f \in 1 + \pi_1^k\mathcal{O}_{F_1}[T]$ such that $x = f(\pi_{n+1})$. Then use (i) and (iv) of Lemma 7.3.5. □

Proof of Theorem 7.3.1. The uniqueness follows from the fact that $0 \neq f \in \mathbb{Z}_p[[T]]$ has only many finitely zeros in $\mathfrak{m}_{\mathbb{C}_p}$ (Newton polygons).

Existence: let $u = (u_n)$, write $u_n = \pi_n^k \alpha u_n'$, where $k \in \mathbb{Z}$ and $\alpha \in \mu_{p-1}$ do not depend on n, and $u_n' \in 1 + \mathfrak{m}_{F_n}$. Then $\mathrm{N}_{F_{n+1}/F_n} u_{n+1}' = u_n'$. If for all n, $f_{u'}(\pi_n) = u_n'$, let $f_u = T^k \alpha f_{u'}$, then $f_u(\pi_n) = u_n$. Thus we are reduced to the case that $u_n \in 1 + \mathfrak{m}_{F_n}$ for all n.

By (i) of Corollary 7.3.6, we can find $g_u \in \mathbb{Z}_p[[T]]$ for $\bar{u}$. We have to check that $g_u(\pi_n) = u_n$ for all $n \neq 1$. Write $v_n = g_u(\pi_n)$. Then $\mathrm{N}(g_u) = g_u$, by (i) of Lemma 7.3.5, implies that $\mathrm{N}_{F_{n+1}/F_n}(v_{n+1}) = v_n$; and $g_u(\bar{\pi}) = \bar{u}$ implies that $v_n = u_n \mod \pi_1$ for all n. Let $w_n = \frac{v_n}{u_n}$, then we have

$$\mathrm{N}_{F_{n+1}/F_n}(w_{n+1}) = w_n \ \text{ and } \ w_n \in 1 + \pi_1\mathcal{O}_{F_n}.$$

By (ii) of Corollary 7.3.6, we have

$$w_n = \mathrm{N}_{F_{n+k}/F_n}(w_{n+k}) \in 1 + \pi_1^k \mathcal{O}_{F_n} \quad \text{for all } k,$$

then $w_n = 1$. This completes the proof. $\square$

Corollary 7.3.7.

$$\mathrm{N}(f_u) = f_u, \qquad \psi(\frac{\partial f_u}{f_u}) = \frac{\partial f_u}{f_u}$$

where $\partial = (1+T)\frac{d}{dT}$.

Proof. By (i) of Lemma 7.3.5, we have $\mathrm{N}(f_u)(\pi_n) = \mathrm{N}_{F_{n+1}/F_n}(f_u(\pi_{n+1})) = f_u(\pi_n)$, for all n, thus $N(f_u) = f_u$.

Using the formula $\psi(\partial \log f) = \partial(\log \mathrm{N}(f))$, we immediately get the result for ψ. As for the proof of this last formula, we know that

$$\begin{aligned}
\varphi(\mathrm{N}(f)(T)) &= \mathrm{N}(f)((1+T)^p - 1) = \prod_{z^p=1} f((1+T)z - 1) \\
\psi(f)((1+T)^p - 1) &= \frac{1}{p} \sum_{z^p=1} f((1+T)z - 1)
\end{aligned}$$

Then we have two ways to write $\partial(\log \varphi(\mathrm{N}(f)))$

$$\begin{aligned}
\partial(\log \varphi(\mathrm{N}(f))) &= p\varphi\ (\partial \log \mathrm{N}(f))(\partial \circ \varphi = p\varphi \circ \partial) \\
&= p\varphi(\frac{\partial \mathrm{N}(f)}{\mathrm{N}(f)}) = p(\frac{\partial \mathrm{N}(f)}{\mathrm{N}(f)})((1+T)^p - 1) \\
&= p(\partial \log \mathrm{N}(f))((1+T)^p - 1),
\end{aligned}$$

$$\begin{aligned}
\partial(\log \varphi(\mathrm{N}(f))) &= \partial(\log \prod_{z^p=1} f((1+T)z - 1)) \\
&= \sum_{z^p=1} \frac{(1+T)zf'((1+T)z - 1)}{f((1+T)z - 1)} \\
&= \sum_{z^p=1} \frac{\partial f}{f}((1+T)z - 1) = p\psi(\frac{\partial f}{f})((1+T)^p - 1) \\
&= p(\psi(\partial \log f))((1+T)^p - 1),
\end{aligned}$$

hence the formula. $\square$

7.4 An explicit reciprocity law

Theorem 7.4.1. *The diagram*

$$\begin{tikzcd}
\varprojlim(\mathcal{O}_{F_n} - \{0\}) \arrow[rr, "\kappa"] \arrow[dr, "u \mapsto \frac{\partial f_u}{f_u}(\pi)"'] & & H^1_{\mathrm{Iw}}(\mathbb{Q}_p, \mathbb{Z}_p(1)) \arrow[dl, "\sim", "\mathrm{Exp}^*"'] \\
& D(\mathbb{Z}_p(1))^{\psi=1} &
\end{tikzcd}$$

is commutative.

Remark. (i) The proof is typical of invariants defined via Fontaine's rings: easy to define and hard to compute.

(ii) For another example, let X/K be a smooth and projective variety, then

$$D_{dR}(H^i_{\acute{e}t}(X \times \overline{K}, \mathbb{Q}_p)) = H^i_{dR}(X/K).$$

The proof is very hard and is due to Faltings and Tsuji.

(iii) Let $a \in \mathbb{Z}$ such that $a \neq 1$, $(a,p) = 1$. The element

$$u_n = \frac{e^{-a\frac{2\pi i}{p^n}} - 1}{e^{-\frac{2\pi i}{p^n}} - 1} \in \mathbb{Q}(\mu_{p^n})$$

is a cyclotomic unit in $\mathcal{O}_{\mathbb{Q}(\mu_{p^n})}$ (whose units are called global units). Then

$$u_n \in F_n = \mathbb{Q}_p(\mu_{p^n}), \quad u_n = \frac{\gamma_{-a}(\pi_n)}{\gamma_{-1}(\pi_n)},$$

where $\gamma_b \in \Gamma_{\mathbb{Q}_p}$ such that $\chi(\gamma_b) = b$. From $\mathrm{N}_{F_{n+1}/F_n}(\pi_{n+1}) = \pi_n$, one gets $\mathrm{N}_{F_{n+1}/F_n}(u_{n+1}) = u_n$ (γ commutes with norm), thus

$$u = (u_n) \in \varprojlim \mathcal{O}_{F_n}.$$

Obviously the Coleman power series

$$f_u = \frac{(1+T)^{-a} - 1}{(1+T)^{-1} - 1}, \quad \frac{\partial f_u}{f_u} = \frac{a}{(1+T)^a - 1} - \frac{1}{T}.$$

So $\frac{\partial f_u}{f_u}$ is nothing but the Amice transform of μ_a that was used to construct p-adic zeta function. So Exp^* produces Kubota-Leopoldt zeta function from the system of cyclotomic units.

(iv) The example in (iii) is part of a big conjectural picture. For V a fixed representation of $G_{\mathbb{Q}}$, then conjecturally

$$\begin{aligned}&\{\text{compatible system of global elements of } V\} \longrightarrow H^1_{\mathrm{Iw}}(\mathbb{Q}, V)\\ &\longrightarrow H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V) \xrightarrow{\mathrm{Exp}^*} D(V)^{\psi=1} \xrightarrow[transform]{Amice} p\text{-adic } L\text{-functions.}\end{aligned}$$

At present there are very few examples representation of $G_{\mathbb{Q}}$ for which this picture is known to work. The Amice transform works well for $\mathbb{Z}_p(1)$, because ψ improves denominators in π, and $A_{\mathbb{Q}_p}^{\psi=1} \subset \frac{1}{\pi}A_{\mathbb{Q}_p}^{+}$ can be viewed as measures. In general, to use the properties of ψ, we will have to introduce overconvergent (φ, Γ)-modules.

7.5 Proof of the explicit reciprocity law

7.5.1 Strategy of proof of Theorem 7.4.1

Let $u \in \varprojlim \mathcal{O}_{F_n}$, and $g \mapsto C_n(g)$ be the cocycle on G_{F_n} by Kummer theory, i.e the image of u under the composition of

$$\varprojlim(\mathcal{O}_{F_n} - \{0\}) \xrightarrow{\kappa} H^1_{\mathrm{Iw}}(\mathbb{Q}_p, \mathbb{Z}_p(1)) \longrightarrow H^1(G_{F_n}, \mathbb{Z}_p(1)).$$

Let $y \in D(\mathbb{Z}_p(1))^{\psi=1} = A_{\mathbb{Q}_p}^{\psi=1}(1)$, let $g \mapsto C'_n(g)$ be the image of y under the composition of

$$D(\mathbb{Z}_p(1))^{\psi=1} = A_{\mathbb{Q}_p}^{\psi=1}(1) \xrightarrow{(\mathrm{Exp}^*)^{-1}} H^1_{\mathrm{Iw}}(\mathbb{Q}_p, \mathbb{Z}_p(1)) \longrightarrow H^1(G_{F_n}, \mathbb{Z}_p(1)).$$

We need to prove that $C_n = C'_n$ for all n implies $y = \frac{\partial f_u}{f_u}(\pi)$.

For C'_n, we have

$$C'_n(g) = \frac{\log \chi(\gamma_n)}{p^n}\left(\frac{\chi(g)-1}{\chi(\gamma_n)-1}y - (\chi(g)g-1)b_n\right),$$

where $b_n \in A$ is a solution of $(\varphi-1)b_n = (\chi(\gamma_n)\gamma_n - 1)^{-1}(\varphi-1)y$, we know that $(\varphi-1)y \in A_{\mathbb{Q}_p}^{\psi=0}$. The exact value of b_n is not important.

For C_n, choose $x_n = (x_n^{(0)}, ..., x_n^{(k)}, ...) \in \tilde{E}^+$ such that $x_n^{(0)} = u_n$. Let $\tilde{u}_n = [x_n]$, then

$$\frac{g(\tilde{u}_n)}{\tilde{u}_n} = [\varepsilon]^{C_n(g)}.$$

Proposition 7.5.1. *Assume $n \geq 1$.*

(i) *There exists $k \in \mathbb{Z}$, $b'_n \in \mathcal{O}_{\mathbb{C}_p}/p^n$ such that*

$$p^2 C'_n(g) = p^2 \frac{\log \chi(\gamma_n)}{p^n} \cdot \frac{g-1}{\gamma_n - 1} y(\pi_{n+k}) + (g-1) b'_n$$

in $\mathcal{O}_{\mathbb{C}_p}/p^n$.

(ii) *There exists $k \in \mathbb{Z}$, $b''_n \in \mathcal{O}_{\mathbb{C}_p}/p^n$ such that*

$$p^2 C_n(g) = p^2 \frac{\log \chi(g)}{p^n} \frac{\partial f_u}{f_u} y(\pi_n) + (g-1) b''_n$$

in $\mathcal{O}_{\mathbb{C}_p}/p^n$.

Proposition 7.5.2. *There exists a constant $c \in \mathbb{N}$, such that for all n and for all k, if $x \in \mathcal{O}_{F_{n+k}}$, $b \in \mathcal{O}_{\mathbb{C}_p}$ satisfy*

$$v_p\big(\frac{g-1}{\gamma_n - 1} x + (g-1) b\big) \geq n, \ \forall g \in G_{F_n}$$

then

$$p^{-k} \operatorname{Tr}_{F_{n+k}/F_n} x \in p^{n-c} \mathcal{O}_{F_n}.$$

We shall prove Proposition 7.5.1 in the next n°, and Proposition 7.5.2 in the third n°. We first explain how the above two propositions imply the theorem:

If $h(\pi) = \psi(h(\pi))$, then $h(\pi_n) = p^{-1} \operatorname{Tr}_{F_{n+1}/F_n}(h(\pi_{n+1}))$. By hypothesis, $\psi(y) = y$, we get

$$p^{-k} \operatorname{Tr}_{F_{n+k}/F_n}(y(\pi_{n+k})) = y(\pi_n), \ \forall n, \ \forall k \quad (*).$$

Let

$$x = p^2 \frac{\log \chi(\gamma_n)}{p^n} \big(y(\pi_{n+k}) - \frac{\partial f_u}{f_u}(\pi_n)\big), \quad b = b'_n - b''_n.$$

By Proposition 7.5.1, and the hypothesis $C_n(g) = C'_n(g)$, we get

$$\frac{g-1}{\gamma_n - 1} x + (g-1) b = p^2 (C'_n(g) - C_n(g)) = 0.$$

The first equality is because for every $x \in F_n$, $\frac{g-1}{\gamma_n-1} x = \frac{\log \chi(g)}{\log \chi(\gamma_n)} x$. Using Proposition 7.5.2, we get

$$p^2 \frac{\log(\chi(\gamma_n))}{p^n} \big(y(\pi_n) - \frac{\partial f_u}{f_u}(\pi_n)\big) \in p^{n-c} \mathcal{O}_{F_n},$$

then for every n,

$$y(\pi_n) - \frac{\partial f_u}{f_u}(\pi_n) \in p^{n-c-2}\mathcal{O}_{F_n}.$$

Let $h = y - \frac{\partial f_u}{f_u}$, then $\psi(h) = h$ and $h(\pi_n) \in p^{n-c-2}\mathcal{O}_{F_n}$. Using the fact $p^{-k}\operatorname{Tr}_{F_{n+k}/F_n}\mathcal{O}_{F_{n+k}} \subset \mathcal{O}_{F_n}$ and the formula (*), then for every $i \in \mathbb{N}$, $n \geq i$,

$$h(\pi_i) = p^{-(n-i)}\operatorname{Tr}_{F_n/F_i}(h(\pi_n)) \in p^{n-c-2}\mathcal{O}_{F_i},$$

thus $h(\pi_i) = 0$ for every $i \in \mathbb{N}$, hence $h = 0$.

7.5.2 Explicit formulas for cocyles

This n$^{\text{o}}$ is devoted to the proof of Proposition 7.5.1

(i) Recall that $\pi = [\varepsilon] - 1$, $\theta(\sum p^m[x_m]) = \sum p^m x_m^{(0)}$ and $\theta(\pi) = 1 - 1 = 0$. Let $\tilde{\pi}_n = \varphi^{-n}(\pi) \in \tilde{A}^+$, then $\tilde{\pi}_n = [\varepsilon^{1/p^n}] - 1$, $\theta(\tilde{\pi}_n) = \pi_n$. Write $b_n = \sum\limits_{l=0}^{+\infty} p^l[z_l]$, where $z_l \in \tilde{E}$. As $C'_n(g) \in \mathbb{Z}_p$, we have

$$\varphi^{-(n+k)}C'_n(g) = C'_n(g), \quad \text{for all } n \text{ and } k.$$

As

$$v_E(\varphi^{-k}(z_l)) = \frac{1}{p^k}v_E(z_l),$$

we can find k such that

$$v_E(\varphi^{-(n+k)}(z_l)) \geq -1, \quad \text{for all } l \leqslant n-1.$$

Let $\tilde{p} = (p, ...) \in \tilde{E}^+$, then for every $l \leqslant n-1$, $\tilde{p}\cdot\varphi^{-(n+k)}(z_l) \in \tilde{E}^+$. We have

$$[\tilde{p}]C'_n(g) = \frac{\log\chi(\gamma_n)}{p^n}[\tilde{p}]\cdot\frac{\chi(g)g-1}{\chi(\gamma_n)\gamma_n - 1}y(\tilde{\pi}_{n+k}) + [\tilde{p}](\chi(g)g-1)\varphi^{-(n+k)}(b_n).$$

Both sides live in $\tilde{A}^+ + p^n\tilde{A}$, reduce $\bmod p^n$ and use $\theta: \ \tilde{A}^+/p^n \to \mathcal{O}_{\mathbb{C}_p}/p^n$, then $[\tilde{p}] \mapsto p$ and

$$pC'_n(g) = p\frac{\log\chi(\gamma_n)}{p^n}p\cdot\frac{g-1}{\gamma_n - 1}y(\pi_{n+k}) + (g-1)b'_n$$

where $b'_n = \theta([\tilde{p}]\varphi^{-(n+k)}(b_n))$.

(ii) Write $u = (\pi_n^k)(v_n)$, where v_n are units $\in \mathcal{O}_{F_n}^*$. So we just have to prove the formula for (π_n) and (v_n). Thus we can assume $v_p(u_n) \leqslant 1$.

Let

$$H : 1 + tB_{dR}^+ \to \mathbb{C}_p, \quad x \mapsto \theta(\frac{x-1}{\pi}) = \theta(\frac{x-1}{t}),$$

recall that $t = \log(1+\pi)$. We have

$$H((1+\pi x')(1+\pi y')) = H(1+\pi(x'+y')+\pi^2 x'y') = \theta(x'+y') = H(1+\pi x')+H(1+\pi y'),$$

thus $H(xy) = H(x) + H(y)$.

Write $\tilde{u}_n = [(u_n, u_n^{\frac{1}{p}}, ...)]$, we have $\frac{g(\tilde{u}_n)}{\tilde{u}_n} = [\varepsilon]^{C_n(g)} = 1 + C_n(g)\pi + \cdots$, thus

$$C_n(g) = H(\frac{g(\tilde{u}_n)}{\tilde{u}_n}).$$

We know $u_n = f_u(\pi_n)$ and $\theta(\tilde{u}_n) = u_n$, then

$$\theta(f_u(\tilde{\pi}_n)) = f_u(\theta(\tilde{\pi}_n)) = f_u(\pi_n) = u_n = \theta(\tilde{u}_n).$$

So, if we set $a_n = \frac{f_u(\tilde{\pi}_n)}{\tilde{u}_n}$, then $\theta(a_n) = 1$.

We know that $[\tilde{p}]a_n \in \tilde{A}^+$ since $v_p(u_n) \leq 1$. Then we get $H(a_n) \in \frac{1}{p\pi_1}\mathcal{O}_{\mathbb{C}_p}$ because of the following identity

$$H(a_n) = \theta\Big(\frac{[\tilde{p}]a_n - [\tilde{p}]}{[\tilde{p}]\pi}\Big) = \theta\Big(\frac{[\tilde{p}]a_n - [\tilde{p}]}{\omega}\Big) \cdot \theta\Big(\frac{1}{[\tilde{p}]\tilde{\pi}_1}\Big),$$

and because $\omega = \frac{\pi}{\tilde{\pi}_1}$ is a generator of $\operatorname{Ker}\theta$ in $\tilde{A}^+$ as $\omega \in \operatorname{Ker}\theta$, and

$$\bar{\omega} = \frac{\varepsilon - 1}{\varepsilon^{1/p} - 1}, \text{ so } v_E(\bar{\omega}) = (1 - \frac{1}{p})v_E(\varepsilon - 1) = 1.$$

Then we have

$$\begin{aligned}
\frac{g(f_u(\tilde{\pi}_n))}{f_u(\tilde{\pi}_n)} &= \frac{f_u((1+\tilde{\pi}_n)^{\chi(g)} - 1)}{f_u(\tilde{\pi}_n)} \\
&= \frac{f_u((1+\tilde{\pi}_n)(1+\pi)^{\frac{\chi(g)-1}{p^n}} - 1)}{f_u(\tilde{\pi}_n)} \\
&= 1 + \frac{\partial f_u}{f_u}(\tilde{\pi}_n) \cdot \frac{\chi(g) - 1}{p^n}\pi + \text{terms of higher degree in } \pi,
\end{aligned}$$

hence
$$H\Big(\frac{g(f_u(\tilde{\pi}_n))}{f_u(\tilde{\pi}_n)}\Big) = \frac{\chi(g)-1}{p^n}\cdot\frac{\partial f_u}{f_u}(\pi_n).$$
Using formula $f_u(\tilde{\pi}_n)=\tilde{u}_n a_n$, we get
$$\begin{aligned}C_n(g) = H\big(\frac{g(\tilde{u}_n)}{\tilde{u}_n}\big) &= H\big(\frac{g(f_u(\tilde{\pi}_n))}{f_u(\tilde{\pi}_n)}\big) - H\big(\frac{g(a_n)}{a_n}\big)\\ &= \frac{\chi(g)-1}{p^n}\cdot\frac{\partial f_u}{f_u}(\pi_n) - (\chi(g)g-1)H(a_n).\end{aligned}$$

We conclude the proof by multiplying p^2, noticing that $\chi(g)=1 \mod p^n$, so
$$\frac{\chi(g)-1}{p^n} = \frac{\exp(\log\chi(g))-1}{p^n} = \frac{\log\chi(g)}{p^n} \mod p^n;$$
set $b_n'' = -p^2H(a_n)$, we get the result.

7.5.3 Tate's normalized trace maps

Let $\pi_n = \varepsilon^{(n)}-1$, $F_n = \mathbb{Q}_p(\pi_n)$, $F_\infty = \bigcup\limits_n F_n$.

Lemma 7.5.3. *If $n \geq 1$, $x \in F_\infty$, then $p^{-k}\operatorname{Tr}_{F_{n+k}/F_n} x$ does not depend on k such that $x \in F_{n+k}$.*

Proof. Use the transitive properties of the trace map and the fact $[F_{n+k} : F_n] = p^k$. □

Let $R_n : F_\infty \longrightarrow F_n$ be the above map. Denote
$$Y_i = \{x \in F_i, \operatorname{Tr}_{F_i/F_{i-1}} x = 0\}.$$

Lemma 7.5.4. (i) *R_n commutes with $\Gamma_{\mathbb{Q}_p}$, is F_n linear and $R_n\circ R_{n+k} = R_n$.*

(ii) *Let $x \in F_\infty$, then $x = R_n(x)+\sum\limits_{i=1}^{+\infty} R_{n+i}^*(x)$, where $R_{n+i}^*(x) = R_{n+i}(x)-R_{n+i-1}(x) \in Y_{n+i}$ and is 0 if $i \gg 0$.*

(iii) *Let $k \in \mathbb{Z}$, then $v_p(x) \geqslant kv_p(\pi_n)$ if and only if $v_p(R_n(x)) \geqslant kv_p(\pi_n)$ and $v_p(R_{n+i}^*(x)) \geqslant kv_p(\pi_n)$ for every $i \in \mathbb{N}$.*

Proof. (i) is obvious.

(ii) is also obvious, since $R_{n+i-1}(R^*_{n+i}(x)) = 0 \Rightarrow R^*_{n+i}(x) \in Y_{n+i}$.

(iii) $\Leftarrow$ is obvious. For $\Rightarrow$, let $x \in \mathcal{O}_{F_{n+k}}$, then

$$x = \sum_{j=0}^{p^k-1} a_j(1+\pi_{n+k})^j, \qquad a_j \in \mathcal{O}_{F_n}.$$

Write $j = p^{k-i}j'$ with $(j', p) = 1$, then

$$R_n(x) = a_0, \quad R^*_{n+i}(x) = \sum_{(j',p)=1} a_{p^{n-i}j'}(1+\pi_{n+i})^{j'}$$

since

$$p^{-1}\operatorname{Tr}_{F_{n+i}/F_{n+i-1}}(1+\pi_{n+i})^j = \begin{cases} (1+\pi_{n+i})^j, & \text{if } p \mid j \\ 0, & \text{if } (j,p) = 1. \end{cases}$$

Thus

$$v_p(x) \geqslant 0 \Rightarrow v_p(R_n(x)) \geqslant 0 \text{ and } v_p(R^*_{n+i}(x)) \geqslant 0.$$

By F_n-linearity we get the result. $\square$

Remark. In the whole theory, the following objects play similar roles:

$$\begin{aligned} \psi \quad &\longleftrightarrow p^{-1}\operatorname{Tr}_{F_{n+1}/F_n} \\ \psi = 0 &\longleftrightarrow \quad Y_i. \end{aligned}$$

Lemma 7.5.5. *Assume that $j \leqslant i-1$ and $j \geq 2$. and assume γ_j is a generator of Γ_j. Let $u \in \mathbb{Q}_p^*$. If $v_p(u-1) > v_p(\pi_1)$, then $u\gamma_j - 1$ is invertible on Y_i. Moreover if $x \in Y_i$, $v_p(x) \geqslant kv_p(\pi_n)$, then $v_p((u\gamma_j-1)^{-1}x) \geqslant kv_p(\pi_n) - v_p(\pi_1)$.*

Proof. If $\gamma_{i-1} = \gamma_j^{p^{i-j-1}}$, then

$$(u\gamma_j - 1)^{-1} = (u^{p^{i-j-1}}\gamma_{i-1} - 1)^{-1}(1 + u\gamma_j + \cdots + (u\gamma_j)^{p^{i-j-1}-1}),$$

so it is enough to treat the case $j = i-1$.

Let $x \in \mathcal{O}_{F_i} \cap Y_i$, write

$$x = \sum_{a=1}^{p-1} x_a(1+\pi_i)^a, \quad x_a \in \mathcal{O}_{F_{i-1}},$$

write $\chi(\gamma_{i-1}) = 1 + p^{i-1}v$ with $v \in \mathbb{Z}_p^*$, then

$$(u\gamma_{i-1} - 1)x = \sum_{a=1}^{p-1} x_a(1+\pi_i)^a(u(1+\pi_1)^{av} - 1).$$

We can check directly

$$(u\gamma_{i-1} - 1)^{-1}x = \sum_{a=1}^{p-1} \frac{x_a}{(u(1+\pi_1)^{av} - 1)}(1+\pi_i)^a.$$

Moreover, if $v_p(x) \geq 0$, then $v_p((u\gamma_j - 1)^{-1}x) \geqslant -v_p(\pi_1)$. □

Proposition 7.5.6. *Assume $n \geqslant 1$, $u \in \mathbb{Q}_p^*$ and $v_p(u-1) > v_p(\pi_1)$, then*

(i) *$x \in F_\infty$ can be written uniquely as $x = R_n(x) + (u\gamma_n - 1)y$ with $R_n(y) = 0$, and we have*

$$v_p(R_n(x)) > v_p(x) - v_p(\pi_n), \quad v_p(y) > v_p(x) - v_p(\pi_n) - v_p(\pi_1).$$

(ii) *R_n extends by continuity to $\hat{F}_\infty$, and let $X_n = \{x \in \hat{F}_\infty, R_n(x) = 0\}$. Then every $x \in \hat{F}_\infty$ can be written uniquely as $x = R_n(x) + (u\gamma_n - 1)y$ with $y \in X_n$ and $R_n(x) \in F_n$, and with the same inequalities*

$$v_p(R_n(x)) \geqslant v_p(x) - v_p(\pi_n), \quad v_p(y) \geqslant v_p(x) - v_p(\pi_n) - v_p(\pi_1).$$

Proof. (i) As

$$x = R_n(x) + \sum_{i=1}^{+\infty}(u\gamma_n - 1)((u\gamma_n - 1)^{-1}R_{n+i}^*(x)).$$

we just let $y = \sum_{i=1}^{+\infty}(u\gamma_n - 1)^{-1}R_{n+i}^*(x)$.

(ii) By (i), we have $v_p(R_n(x)) \geqslant v_p(x) - C$, so R_n extends by continuity to $\hat{F}_\infty$; the rest follows by continuity. □

Remark. (i) The maps $R_n : \hat{F}_\infty \longrightarrow F_n$ are *Tate's normalized trace maps.*

(ii) they commutes with $\Gamma_{\mathbb{Q}_p}$ (or $G_{\mathbb{Q}_p}$).

(iii) $R_n(x) = x$ if $x \in F_\infty$ and $n \gg 0$, hence $R_n(x) \to x$ if $x \in \hat{F}_\infty$ and $n \to \infty$.

7.5.4 Applications to Galois cohomology

Proposition 7.5.7. (i) *The map*

$$x \in F_n \longmapsto (\gamma \mapsto x \log \chi(\gamma)) \in H^1(\Gamma_{F_n}, F_n)$$

induces isomorphism

$$F_n \xrightarrow{\sim} H^1(\Gamma_{F_n}, F_n) \xrightarrow{\sim} H^1(\Gamma_{F_n}, \hat{F}_\infty).$$

(ii) *If* $\eta : \Gamma_{F_n} \longrightarrow \mathbb{Q}_p^*$ *is of infinite order, then* $H^1(\Gamma_{F_n}, \hat{F}_\infty(\eta)) = 0$.

Proof. If $n \gg 0$ so that $v_p(\eta(\gamma_n) - 1) > v_p(\pi_1)$. Using the above proposition (let $u = \eta(\gamma_n)$), we get

$$H^1(\Gamma_{F_n}, \hat{F}_\infty(\eta)) = \frac{\hat{F}_\infty}{(u\gamma_n - 1)} = \frac{F_n \bigoplus X_n}{(u\gamma_n - 1)} = \frac{F_n}{u\gamma_n - 1}.$$

If $u = 1$, we get $(\gamma_n - 1)F_n = 0$. If $u \neq 1$, we get $F_n/(u-1)F_n = 0$.

For n small, using inflation and restriction sequence, as $\mathrm{Gal}(F_{n+k}/F_n)$ is finite, and $\hat{F}_\infty(\eta)$ is a $\mathbb{Q}_p$-vector space, we have

$$H^1(\mathrm{Gal}(F_{n+k}/F_n), \hat{F}_\infty(\eta)^{\Gamma_{F_{n+k}}}) = 0, \quad H^2 = 0,$$

then we get an isomorphism

$$H^1(\Gamma_{F_n}, \hat{F}_\infty(\eta)) \xrightarrow{\sim} H^1(\Gamma_{F_{n+k}}, \hat{F}_\infty(\eta))^{\mathrm{Gal}(F_{n+k}/F_n)}.$$

From the case of $n \gg 0$, we immediately get the result. □

Recall that the following result is the main step in Ax's proof of the Ax-Sen-Tate theorem (cf. Fontaine's course).

Proposition 7.5.8. *There exists a constant* $C \in \mathbb{N}$, *such that if* $x \in \mathbb{C}_p$, *if* $H \subset G_{\mathbb{Q}_p}$ *is a closed subgroup, if for all* $g \in H$, $v_p((g-1)x) \geqslant a$ *for some* a, *then there exists* $y \in \mathbb{C}_p^H$ *such that* $v_p(x - y) \geqslant a - C$.

The following corollary is Proposition 7.5.2 in the previous section.

Corollary 7.5.9. *For* $x \in \mathcal{O}_{\hat{F}_\infty}$, *if there exists* $c \in \mathcal{O}_{\mathbb{C}_p}$ *such that*

$$v_p\Big(\frac{g-1}{\gamma_n - 1}x - (g-1)c\Big) \geqslant n, \text{ for all } g \in G_{F_n}.$$

Then we have

$$v_p(R_n(x)) \geqslant n - C - 1(or\ 2).$$

Proof. By assumption, we get

$$v_p((g-1)c) \geqslant n, \ \forall\, g \in H_{\mathbb{Q}_p} = \operatorname{Ker}\chi,$$

then by **Ax**, there exists $c' \in \hat{F}_\infty$ such that

$$v_p(c-c') \geqslant n - C.$$

Take $g = \gamma_n$, then $v_p(x-(\gamma_n-1)c') \geqslant n-C$. As $R_n\gamma_n = \gamma_n R_n = R_n$, we get

$$v_p(R_n(x)) = v_p(R_n(x-(\gamma_n-1)c')) \geqslant n - C - v_p(\pi_1) - v_p(\pi_n),$$

hence the result. □

7.5.5 No $2\pi i$ in $\mathbb{C}_p$!

Theorem 7.5.10. (i) $\mathbb{C}_p$ *does not contain* $\log 2\pi i$*, i.e. there exists no* $x \in \mathbb{C}_p$ *satisfies that* $g(x) = x + \log\chi(g)$ *for all* $g \in G_K$*, where* K *is a finite extension of* $\mathbb{Q}_p$*.*

(ii) $\mathbb{C}_p(k) = 0$*, if* $k \neq 0$*.*

Proof. (i) If $K = \mathbb{Q}_p$, if there exists such an x, by **Ax-Sen-Tate**, we get $x \in \hat{F}_\infty = \mathbb{C}_p^{H_{\mathbb{Q}_p}}$. Then we have:

$$R_n(g(x)) = g(R_n(x)) = R_n(x) + \log\chi(g).$$

Because $R_n(x) \in F_n$, it has only finite number of conjugates but $\log\chi(g)$ has infinitely many values, contradiction!

Now for K general, we can assume $K/\mathbb{Q}_p$ is Galois, let

$$y = \frac{1}{[K:\mathbb{Q}_p]}\sum_{\sigma\in S}\sigma(x)$$

where S are representatives of $G_{\mathbb{Q}_p}/G_K$. For $g \in G_{\mathbb{Q}_p}$, we can write $g\sigma = \sigma'_\sigma h_\sigma$ for $h_\sigma \in G_K$ and $\sigma'_\sigma \in S$. From this we get

$$\sum_{\sigma\in S}\log\chi(h_\sigma) = [K:\mathbb{Q}_p]\log\chi(g).$$

Then we have

$$\begin{aligned} g(y) &= \frac{1}{[K:\mathbb{Q}_p]}\sum_{\sigma\in S} g\sigma(x) = \frac{1}{[K:\mathbb{Q}_p]}\sum_{\sigma\in S} \sigma'_\sigma h_\sigma x \\ &= \frac{1}{[K:\mathbb{Q}_p]}\sum_{\sigma\in S} \sigma'_\sigma(x+\log\chi(h_\sigma)) \\ &= \frac{1}{[K:\mathbb{Q}_p]}\sum_{\sigma\in S} \sigma(x) + \frac{1}{[K:\mathbb{Q}_p]}\sum_{\sigma\in S} \log\chi(h_\sigma) \\ &= y + \log\chi(g). \end{aligned}$$

Then by the case $K = \mathbb{Q}_p$, we get the result.

(ii) If $0 \neq x \in \mathbb{C}_p(k)$, then $g(x) = \chi(g)^{-k}x$. Let $y = \frac{\log x}{-k}$, then we have $g(y) = y + \log\chi(g)$, which is a contradiction by (i). $\square$

Chapter 8

(φ, Γ)-modules and p-adic L-functions

8.1 Tate-Sen's conditions

8.1.1 The conditions (TS1), (TS2) and (TS3)

Let G_0 be a profinite group and $\chi: \ G_0 \to \mathbb{Z}_p^*$ be a continuous group homomorphism with open image. Set $v(g) = v_p(\log \chi(g))$ and $H_0 = \operatorname{Ker} \chi$.

Suppose $\tilde{\Lambda}$ is a $\mathbb{Z}_p$-algebra and

$$v: \ \tilde{\Lambda} \longrightarrow \mathbb{R} \cup \{+\infty\}$$

satisfies the following conditions:

(i) $v(x) = +\infty$ if and only if $x = 0$;

(ii) $v(xy) \geqslant v(x) + v(y)$;

(iii) $v(x+y) \geqslant \inf(v(x), v(y))$;

(iv) $v(p) > 0, \ v(px) = v(p) + v(x)$.

Assume $\tilde{\Lambda}$ is complete for v, and G_0 acts continuously on $\tilde{\Lambda}$ such that $v(g(x)) = v(x)$ for all $g \in G_0$ and $x \in \ \tilde{\Lambda}$.

Definition 8.1.1. The *Tate-Sen's conditions* for the quadruple $(G_0, \chi, \tilde{\Lambda}, v)$ are the following three conditions **TS1–TS3**.

(TS1). For all $C_1 > 0$, for all $H_1 \subset H_2 \subset H_0$ open subgroups, there exists an $\alpha \in \tilde{\Lambda}^{H_1}$ with

$$v(\alpha) > -C_1 \text{ and } \sum_{\tau \in H_2/H_1} \tau(\alpha) = 1.$$

(In Faltings' terminology, $\tilde{\Lambda}/\tilde{\Lambda}^{H_0}$ is called *almost étale*.)

(TS2). *Tate's normalized trace maps*: there exists $C_2 > 0$ such that for all open subgroups $H \subset H_0$, there exist $n(H) \in \mathbb{N}$ and $(\Lambda_{H,n})_{n \geq n(H)}$, an increasing sequence of sub $\mathbb{Z}_p$-algebras of $\tilde{\Lambda}^H$ and maps

$$R_{H,n} : \tilde{\Lambda}^H \longrightarrow \Lambda_{H,n}$$

satisfying the following conditions:

(a) if $H_1 \subset H_2$, then $\Lambda_{H_2,n} = (\Lambda_{H_1,n})^{H_2}$, and $R_{H_1,n} = R_{H_2,n}$ on $\tilde{\Lambda}^{H_2}$;
(b) for all $g \in G_0$,

$$g(\Lambda_{H,n}) = \Lambda_{gHg^{-1},n} \quad g \circ R_{H,n} = R_{gHg^{-1},n} \circ g;$$

(c) $R_{H,n}$ is $\Lambda_{H,n}$-linear and is equal to Id on $\Lambda_{H,n}$;
(d) $v(R_{H,n}(x)) \geqslant v(x) - C_2$ if $n \geqslant n(H)$ and $x \in \tilde{\Lambda}^H$;
(e) $\lim\limits_{n\to+\infty} R_{H,n}(x) = x$.

(TS3). There exists C_3, such that for all open subgroups $G \subset G_0$, $H = G \cap H_0$, there exists $n(G) \geqslant n(H)$ such that if $n \geqslant n(G)$, $\gamma \in G/H$ and $v(\gamma) = v_p(\log \chi(\gamma)) \leqslant n$, then $\gamma - 1$ is invertible on $X_{H,n} = (R_{H,n} - 1)\tilde{\Lambda}$ and

$$v((\gamma-1)^{-1}x) \geqslant v(x) - C_3$$

for $x \in X_{H,n}$.

Remark. $R_{H,n} \circ R_{H,n} = R_{H,n}$, so $\tilde{\Lambda}^H = \Lambda_{H,n} \oplus X_{H,n}$.

8.1.2 Example : the field $\mathbb{C}_p$

Theorem 8.1.2. *The quadruple ($\tilde{\Lambda} = \mathbb{C}_p$, $v = v_p$, $G_0 = G_{\mathbb{Q}_p}$ and χ=the cyclotomic character) satisfies (TS1), (TS2), (TS3).*

Proof. (TS1): In Fontaine's course, we know that for any $\mathbb{Q}_p \subset K \subset L$ such that $[L : \mathbb{Q}_p] < +\infty$, then

$$v_p(\mathfrak{d}_{L_n/K_n}) \to 0 \text{ as } n \to +\infty.$$

The proof showed that $v_p(\gamma(\pi_n) - \pi_n) \to 0$ as $n \to +\infty$, where π_n is a uniformizer of L_n and $\gamma \in \mathrm{Gal}(L_n/K_n) = \mathrm{Gal}(L_\infty/K_\infty)$ when $n \gg 0$. We also have

$$\mathrm{Tr}_{L_\infty/K_\infty} = \mathrm{Tr}_{L_n/K_n}$$

on L_n if $n \gg 0$ and

$$\mathrm{Tr}_{L_n/K_n}(\mathcal{O}_{L_n}) \supset \mathfrak{d}_{L_n/K_n} \bigcap \mathcal{O}_{K_n},$$

thus $\mathrm{Tr}_{L_\infty/K_\infty}(\mathcal{O}_{L_\infty})$ contains elements with v_p as small as we want. Take $x \in \mathcal{O}_{L_\infty}$ and let $\alpha = \frac{x}{\mathrm{Tr}_{L_\infty/K_\infty}(x)}$, then

$$\sum_{\tau \in H_K/H_L} \tau(\alpha) = \mathrm{Tr}_{L_\infty/K_\infty}(\alpha) = 1.$$

Then for all $C_1 > 0$, we can find $x \in \mathcal{O}_{L_\infty}$ such that $v_p(\mathrm{Tr}_{L_\infty/K_\infty}(x))$ is small enough, thus $v_p(\alpha) > -C_1$.

(TS2) and (TS3): By Ax-Sen-Tate, $\mathbb{C}_p^{H_K} = \hat{K}_\infty$, let $\Lambda_{H_K,n} = K_n$, and $R_{H_K,n} = p^{-k}\,\mathrm{Tr}_{K_{n+k}/K_n}$ on K_{n+k}.

If $K = \mathbb{Q}_p$, $R_{H_K,n} = R_n$, that's what we did in last chapter. We are going to use what we know about R_n.

For $G = G_K$, then $H = H_K$, choose m big enough such that for any $n \geqslant m$, $v_p(\mathfrak{d}_{K_n/F_n})$ is small and $[K_\infty : F_\infty] = [K_n : F_n] = d$. Let $\{e_1, ..., e_d\}$ be a basis of $\mathcal{O}_{K_n}$ over $\mathcal{O}_{F_n}$ and $\{e_1^*, ..., e_d^*\}$ be the dual basis of K_n over F_n for the trace map $(x, y) \mapsto \mathrm{Tr}_{K_n/F_n}(xy)$. This implies that $\{e_1^*, ..., e_d^*\}$ is a basis of $\mathfrak{d}^{-1}_{K_n/F_n}$ and $v_p(e_i^*) \geqslant -v_p(\mathfrak{d}_{K_n/F_n})$ are small. Any $x \in K_\infty$ can be written as

$$x = \sum_{i=1}^{d} \mathrm{Tr}_{K_\infty/K}(xe_i)e_i^*,$$

then

$$\inf_i v_p(\mathrm{Tr}_{K_\infty/F_\infty}(xe_i)) \geq v_p(x) \geq \inf_i v_p(\mathrm{Tr}_{K_\infty/F_\infty}(xe_i)) - v_p(\mathfrak{d}_{K_n/F_n}),$$

and

$$R_{H_K,n}(x) = \sum_{i=1}^{d} R_n(\mathrm{Tr}_{K_\infty/F_\infty}(xe_i))e_i^*, \quad n \geqslant m.$$

So use what we know about R_n to conclude. □

Remark. By the same method as Corollary 7.5.7, we get

(i) $H^1(\Gamma, \hat{K}_\infty) \cong K$, where the isomorphism is given by $x \in K \longmapsto (\gamma \mapsto x \log \chi(\gamma))$.

(ii) $H^1(\Gamma, \hat{K}_\infty(\eta)) = 0$ if η is of infinite order.

8.2 Sen's method

Proposition 8.2.1. *Assume $\tilde{\Lambda}$ verifying (TS1), (TS2) and (TS3). Let $\sigma \mapsto U_\sigma$ be a continuous cocycle from G_0 to $\mathrm{GL}_d(\tilde{\Lambda})$. If $G \subset G_0$ is an open normal subgroup of G_0 such that $v(U_\sigma - 1) > 2C_2 + 2C_3$ for any $\sigma \in \ G$. Set $H = G \cap H_0$, then there exists $M \in \mathrm{GL}_d(\tilde{\Lambda})$ with $v(M-1) > C_2 + C_3$ such that*

$$\sigma \longmapsto V_\sigma = M^{-1} U_\sigma \sigma(M)$$

satisfies $V_\sigma \in \mathrm{GL}_d(\Lambda_{H,n(G)})$ and $V_\sigma = 1$ if $\sigma \in H$.

Example 8.2.2. *Example of Sen*: For the case $\tilde{\Lambda} = \mathbb{C}_p$, for U_σ a 1-cocycle on G_K with values in $\mathrm{GL}_d(\mathbb{C}_p)$, there exists $[L:K] < \infty$, such that U_σ is cohomologous to a cocycle that which is trivial on H_L and with values in $\mathrm{GL}_d(L_n)$ for some n.

The proof of Proposition 8.2.1 needs three Lemmas below. It is technical, but the techniques come over again and again.

8.2.1 Almost étale descent

Lemma 8.2.3. *If $\tilde{\Lambda}$ satisfies (TS1), $a > 0$, and $\sigma \mapsto U_\sigma$ is a 1-cocycle on H open in H_0 and*

$$v(U_\sigma - 1) \geqslant a \text{ for any } \sigma \in H,$$

then there exists $M \in \mathrm{GL}_d(\tilde{\Lambda})$ such that

$$v(M-1) \geqslant \frac{a}{2}, \quad v(M^{-1} U_\sigma \sigma(M) - 1) \geqslant a + 1.$$

Proof. The proof is approximating Hilbert's Theorem 90.

Fix $H_1 \subset H$ open and normal such that $v(U_\sigma - 1) \geqslant a + 1 + a/2$ for $\sigma \in H_1$, which is possible by continuity. Because $\tilde{\Lambda}$ satisfies (TS1), we can find $\alpha \in \tilde{\Lambda}^{H_1}$ such that

$$v(\alpha) \geqslant -a/2, \qquad \sum_{\tau \in H/H_1} \tau(\alpha) = 1.$$

Let $S \subset H$ be a set of representatives of H/H_1, denote $M_S = \sum_{\sigma \in S} \sigma(\alpha) U_\sigma$, we have $M_S - 1 = \sum_{\sigma \in S} \sigma(\alpha)(U_\sigma - 1)$, this implies $v(M_S - 1) \geqslant a/2$ and moreover

$$M_S^{-1} = \sum_{n=0}^{+\infty} (1 - M_S)^n,$$

so we have $v(M_S^{-1}) \geqslant 0$ and $M_S \in \mathrm{GL}_d(\tilde{\Lambda})$.

If $\tau \in H_1$, then $U_{\sigma\tau} - U_\sigma = U_\sigma(\sigma(U_\tau) - 1)$. Let $S' \subset H$ be another set of representatives of H/H_1, so for any $\sigma' \in S'$, there exists $\tau \in H_1$ and $\sigma \in S$ such that $\sigma' = \sigma\tau$, so we get

$$M_S - M_{S'} = \sum_{\sigma \in S} \sigma(\alpha)(U_\sigma - U_{\sigma\tau}) = \sum_{\sigma \in S} \sigma(\alpha) U_\sigma (1 - \sigma(U_\tau)),$$

thus

$$v(M_S - M_{S'}) \geqslant a + 1 + a/2 - a/2 = a + 1.$$

For any $\tau \in H$,

$$U_\tau \tau(M_S) = \sum_{\sigma \in S} \tau\sigma(\alpha) U_\tau \tau(U_\sigma) = M_{\tau S}.$$

Then

$$M_S^{-1} U_\tau \tau(M_S) = 1 + M_S^{-1}(M_{\tau S} - M_S),$$

with $v(M_S^{-1}(M_{\tau S} - M_S)) \geq a + 1$. Take $M = M_S$ for any S, we get the result. □

Corollary 8.2.4. *Under the same hypotheses as the above lemma, there exists $M \in \mathrm{GL}_d(\tilde{\Lambda})$ such that*

$$v(M - 1) \geqslant a/2, \ M^{-1} U_\sigma \sigma(M) = 1, \forall\ \sigma \in\ H.$$

Proof. Repeat the lemma ($a \mapsto a+1 \mapsto a+2 \mapsto \cdots$), and take the limits. □

Exercise. Assume $\tilde{\Lambda}$ satisfies (TS1), denote by $\tilde{\Lambda}^+ = \{x \in \tilde{\Lambda} | v(x) \geqslant 0\}$. Let M be a finitely generated $\tilde{\Lambda}^+$-module with semi-linear action of H, an open subgroup of H_0. Then $H^i(H, M)$ is killed by any $x \in \tilde{\Lambda}^H$ with $v(x) > 0$.

Hint: Adapt the proof that if L/K is finite Galois and M is a L-module with semi-linear action of $\mathrm{Gal}(L/K)$, then $H^i(\mathrm{Gal}(L/K), L) = 0$ for all $i \geqslant 1$. Let $\alpha \in L$ such that $\mathrm{Tr}_{L/K}(\alpha) = 1$. For any $c(g_1, \cdots, g_n)$ an n-cocycle, let

$$c'(g_1, \cdots, g_{n-1}) = \sum_{h \in \mathrm{Gal}(L/K)} g_1 \cdots g_{n-1} h(\alpha) c(g_1, \cdots, g_{n-1}, h),$$

then $dc' = c$.

Theorem 8.2.5. (i) *The map* $x \longmapsto (g \mapsto x \log \chi(g))$ *gives an isomorphism* $K \xrightarrow{\sim} H^1(G_K, \mathbb{C}_p)$.

(ii) *If* $\eta : G_K \to \Gamma_K \to \mathbb{Q}_p^*$ *is of infinite order, then* $H^1(G_K, \mathbb{C}_p(\eta)) = 0$.

Proof. Using the inflation and restriction exact sequence

$$0 \longrightarrow H^1(\Gamma_K, \mathbb{C}_p(\eta)^{H_K}) \xrightarrow{\text{inf}} H^1(G_K, \mathbb{C}_p(\eta)) \xrightarrow{\text{res}} H^1(H_K, \mathbb{C}_p(\eta))^{\Gamma_K}.$$

by the above exercise, $H^1(H_K, \mathbb{C}_p(\eta))^{\Gamma_K} = 0$, then the inflation map is actually an isomorphism. We have $\mathbb{C}_p(\eta)^{H_K} = \hat{K}_\infty(\eta)$, and use Corollary 7.5.7. In fact

$$K = H^1(\Gamma_K, \hat{K}_\infty) = H^1(\Gamma_K, K) = \mathrm{Hom}(\Gamma, K) = K \cdot \log \chi,$$

the last equality is because Γ_K is pro-cyclic. $\square$

8.2.2 Decompletion

Now recall that we have the continuous character: $G_0 \xrightarrow{\chi} \mathbb{Z}_p^*$, $H_0 = \mathrm{Ker}\,\chi$. $\widetilde{\Lambda}$ is complete for v, with continuous action of G_0. H is an open subgroup of H_0, and we have the maps:$R_{H,n} : \widetilde{\Lambda}^H \to \Lambda_{H,n}$. By (TS2), $v(R_{H,n}(x)) \geq v(x) - C_2$; and by (TS3), $v((\gamma-1)^{-1}x) \geq v(x) - C_3$, if $R_{H,n}(x) = 0$ and $v_p(\log \chi(\gamma)) \leq n$. We can use these properties to reduce to something reasonable.

Lemma 8.2.6. *Assume given* $\delta > 0$, $b \geq 2C_2 + 2C_3 + \delta$, *and* $H \subset H_0$ *is open. Suppose* $n \geq n(H)$, $\gamma \in G/H$ *with* $n(\gamma) \leq n$, $U = 1 + U_1 + U_2$ *with*

$$\begin{aligned} &U_1 \in \mathrm{M}_d(\Lambda_{H,n}), v(U_1) \geq b - C_2 - C_3 \\ &U_2 \in \mathrm{M}_d(\widetilde{\Lambda}^H), v(U_2) \geq b. \end{aligned}$$

Then, there exists $M \in \mathrm{GL}_d(\widetilde{\Lambda}^H), v(M-1) \geq b - C_2 - C_3$ *such that*

$$M^{-1} U \gamma(M) = 1 + V_1 + V_2,$$

with

$$\begin{aligned} &V_1 \in \mathrm{M}_d(\Lambda_{H,n}),\ v(V_1) \geq b - C_2 - C_3), \\ &V_2 \in \mathrm{M}_d(\widetilde{\Lambda}^H),\ v(V_2) \geq b + \delta. \end{aligned}$$

Proof. Using (TS2) and (TS3), one gets $U_2 = R_{H,n}(U_2) + (1-\gamma)V$, with

$$v(R_{H,n}(U_2)) \geq v(U_2) - C_2, \quad v(V) \geq v(U_2) - C_2 - C_3.$$

Thus,

$$\begin{aligned}(1+V)^{-1}U\gamma(1+V) &= (1 - V + V^2 - \cdots)(1 + U_1 + U_2)(1 + \gamma(V)) \\ &= 1 + U_1 + (\gamma - 1)V + U_2 + (\text{terms of degree} \geq 2)\end{aligned}$$

Let $V_1 = U_1 + R_{H,n}(U_2) \in \mathrm{M}_d(\Lambda_{H,n})$ and W be the terms of degree ≥ 2. Thus $v(W) \geq 2(b - C_2 - C_3) \geq b + \delta$. So we can take $M = 1 + V,\ V_2 = W$. □

Corollary 8.2.7. *Keep the same hypotheses as in Lemma 8.2.6. Then there exists $M \in \mathrm{GL}_d(\widetilde{\Lambda}^H), v(M-1) \geq b - C_2 - C_3$ such that $M^{-1}U\gamma(M) \in \mathrm{GL}_d(\Lambda_{H,n})$.*

Proof. Repeat the lemma ($b \mapsto b+\delta \mapsto b+2\delta \mapsto \cdots$), and take the limit. □

Lemma 8.2.8. *Suppose $H \subset H_0$ is an open subgroup, $i \geq n(H)$, $\gamma \in G/H$, $n(\gamma) \geq i$ and $B \in \mathrm{GL}_d(\widetilde{\Lambda}^H)$. If there exist $V_1, V_2 \in \mathrm{GL}_d(\Lambda_{H,i})$ such that*

$$v(V_1 - 1) > C_3, \quad v(V_2 - 1) > C_3, \quad \gamma(B) = V_1 B V_2,$$

then $B \in \mathrm{GL}_d(\Lambda_{H,i})$.

Proof. Take $C = B - R_{H,i}(B)$. We have to prove $C = 0$. Note that C has coefficients in $X_{H,i} = (1 - R_{H,i})\widetilde{\Lambda}^H$, and $R_{H,i}$ is $\Lambda_{H,i}$-linear and commutes with γ. Thus,

$$\gamma(C) - C = V_1 C V_2 - C = (V_1 - 1)CV_2 + V_1 C(V_2 - 1) - (V_1 - 1)C(V_2 - 1)$$

Hence, $v(\gamma(C) - C) > v(C) + C_3$. By (TS3), this implies $v(C) = +\infty$, i.e. $C = 0$. □

Proof of Proposition 8.2.1. Let $\sigma \mapsto U_\sigma$ be a continuous 1-cocycle on G_0 with values in $\mathrm{GL}_d(\widetilde{\Lambda})$. Choose an open normal subgroup G of G_0 such that

$$\inf_{\sigma \in G} v(U_\sigma - 1) > 2(C_2 + C_3).$$

By Lemma 8.2.3, there exists $M_1 \in \mathrm{GL}_d(\widetilde{\Lambda})$, $v(M_1 - 1) > 2(C_2 + C_3)$ such that $\sigma \mapsto U'_\sigma = M_1^{-1}U_\sigma\sigma(M_1)$ is trivial in $H = G \cap H_0$ (In particular, it has values in $\mathrm{GL}_d(\widetilde{\Lambda}^H)$).

Now we pick $\gamma \in G/H$ with $n(\gamma) = n(G)$. In particular, we want $n(G)$ big enough so that γ is in the center of G_0/H. Indeed, the center is open, since in the exact sequence:

$$1 \to H_0/H \to G_0/H \to G/H \to 1,$$

$G/H \simeq \mathbb{Z}_p \times$ (finite), and H_0/H is finite. So we are able to choose such a $n(G)$.

Then we have $v(U'_\gamma) > 2(C_2 + C_3)$, and by Corollary 8.2.7, there exists $M_2 \in \mathrm{GL}_d(\widetilde{\Lambda}^H)$ satisfying

$$v(M_2 - 1) > C_2 + C_3 \text{ and } M_2^{-1} U'_\gamma \gamma(M_2) \in \mathrm{GL}_d(\Lambda_{H,n(G)}).$$

Take $M = M_1 \cdot M_2$, then the cocycle

$$\sigma \mapsto V_\sigma = M^{-1} U_\sigma \sigma(M)$$

a cocycle trivial on H with values in $\mathrm{GL}_d(\widetilde{\Lambda}^H)$, and we have

$$v(V_\gamma - 1) > C_2 + C_3 \text{ and } V_\gamma \in \mathrm{GL}_d(\Lambda_{H,n(G)}).$$

This implies V_σ comes by inflation from a cocycle on G_0/H.

The last thing we want to prove is $V_\tau \in \mathrm{GL}_d(\Lambda_{H,n(G)})$ for any $\tau \in G_0/H$. Note that $\gamma\tau = \tau\gamma$ as γ is in the center, so

$$V_\tau \tau(V_\gamma) = V_{\tau\gamma} = V_{\gamma\tau} = V_\gamma \gamma(V_\tau)$$

which implies $\gamma(V_\tau) = V_\gamma^{-1} V_\tau \tau(V_\gamma)$. Apply Lemma 8.2.8 with $V_1 = V_\gamma^{-1}, V_2 = \tau(V_\gamma)$, then we obtain what we want. □

8.2.3 Applications to p-adic representations

Proposition 8.2.9. *Let T be a free $\mathbb{Z}_p$-representation of G_0, $k \in \mathbb{N}$, $v(p^k) > 2C_2 + 2C_3$, and suppose $G \subset G_0$ is an open normal subgroup acting trivially on T/p^kT, and $H = G \cap H_0$. Let $n \in \mathbb{N}, n \geq n(G)$. Then there exists a unique $D_{H,n}(T) \subset \widetilde{\Lambda} \otimes T$, a free $\Lambda_{H,n}$-module of rank d, such that:*

(i) *$D_{H,n}(T)$ is fixed by H, and stable by G;*

(ii) *$\widetilde{\Lambda} \otimes_{\Lambda_{H,n}} D_{H,n}(T) \xrightarrow{\sim} \widetilde{\Lambda} \otimes T$;*

(iii) *there exists a basis $\{e_1, \ldots, e_d\}$ of $D_{H,n}$ over $\Lambda_{H,n}$ such that if $\gamma \in G/H$, then $v(V_\gamma - 1) > C_3$, V_γ being the matrix of γ.*

Proof. Translation of Proposition 8.2.1, by the correspondence

$$\widetilde{\Lambda}\text{-representations of } G_0 \longleftrightarrow H^1(G_0, \mathrm{GL}_d(\widetilde{\Lambda})).$$

For the uniqueness, one uses Lemma 8.2.8. □

Remark. H_0 acts through H_0/H (which is finite) on $D_{H,n}(T)$. If $\Lambda_{H,n}$ is étale over $\Lambda_{H_0,n}$ (the case in applications), and then $D_{H_0,n}(T) = D_{H,n}(T)^{(H_0/H)}$, is locally free over $\Lambda_{H_0,n}$ (in most cases it is free), and

$$\Lambda_{H,n} \bigotimes_{\Lambda_{H_0,n}} D_{H_0,n}(T) \xrightarrow{\sim} D_{H,n}(T).$$

Example 8.2.10. For $\widetilde{\Lambda} = \mathbb{C}_p$, let V be a $\mathbb{Q}_p$-representation of G_K for $[K:\mathbb{Q}_p] < +\infty$, $T \subset V$ be a stable lattice. Then

$$D_{Sen,n}(V) := D_{H_K,n}(T)$$

is a K_n-vector space of dimension $d = \dim_{\mathbb{Q}_p} V$ with a linear action of Γ_{K_n}. Sen's operator is defined as follows:

$$\Theta_{Sen} = \frac{\log\gamma}{\log\chi(\gamma)}, \text{ where } \gamma \in \Gamma_{K_n}, \log\chi(\gamma) \neq 0.$$

It is easy to see:

Proposition 8.2.11. *V is Hodge-Tate if and only if Θ_{Sen} is semi-simple, and the eigenvalues lie in $\mathbb{Z}$. These eigenvalues are the Hodge-Tate weights of V.*

Remark. For general V, the eigenvalues of Θ_{Sen} are the *generalized Hodge-Tate weights of V.*

8.3 Overconvergent (φ,Γ)-modules

8.3.1 Overconvergent elements

Definition 8.3.1. (i) For $x = \sum_{i=0}^{+\infty} p^i[x_i] \in \widetilde{A}$, $x_i \in \widetilde{E} = \mathrm{Fr}\, R$, $k \in \mathbb{N}$, define $w_k(x) := \inf_{i\le k} v_E(x_i)$ (One checks easily that $w_k(x) \ge v_E(\alpha)$, $\alpha \in \widetilde{E}$, if and only if $[\alpha]x \in \widetilde{A}^+ + p^{k+1}\widetilde{A}$).

(ii) For a real number $r > 0$, define

$$v^{(0,r]}(x) := \inf_{k\in\mathbb{N}} w_k(x) + \frac{k}{r} = \inf_{k\in\mathbb{N}} v_E(x_k) + \frac{k}{r} \in \mathbb{R} \cup \{\pm\infty\}.$$

(iii) $\widetilde{A}^{(0,r]} := \{x \in \widetilde{A} : \lim_{k\to+\infty} \big(v_E(x_k) + \frac{k}{r}\big) = \lim_{k\to+\infty} \big(w_E(x_k) + \frac{k}{r}\big) = +\infty\}.$

Proposition 8.3.2. *$\widetilde{A}^{(0,r]}$ is a ring and $v = v^{(0,r]}$ satisfies the following properties:*

(i) $v(x) = +\infty \Leftrightarrow x = 0$;
(ii) $v(xy) \geq v(x) + v(y)$;
(iii) $v(x + y) \geq \inf(v(x), v(y))$;
(iv) $v(px) = v(x) + \frac{1}{r}$;
(v) $v([\alpha]x) = v_E(\alpha) + v(x)$ *if* $\alpha \in \widetilde{E}$;
(vi) $v(g(x)) = v(x)$ *if* $g \in G_{\mathbb{Q}_p}$;
(vii) $v^{(0,p^{-1}r]}(\varphi(x)) = pv^{(0,r]}(x)$.

Proof. Exercise. □

Lemma 8.3.3. *Given $x \in \sum_{k=0}^{+\infty} p^k[x_k] \in \widetilde{A}$, the following conditions are equivalent:*

(i) $\sum_{k=0}^{+\infty} p^k[x_k]$ *converges in* B_{dR}^+;
(ii) $\sum_{k=0}^{+\infty} p^k x_k^{(0)}$ *converges in* $\mathbb{C}_p$;
(iii) $\lim_{k\to+\infty} (k + v_E(x_k)) = +\infty$;
(iv) $x \in \widetilde{A}^{(0,1]}$.

Proof. (iii) $\Leftrightarrow$ (iv) is by definition of $\widetilde{A}^{(0,r]}$. (ii) $\Leftrightarrow$ (iii) is by definition of v_E. (i) $\Rightarrow$ (ii) is by the continuity of $\theta : B_{dR}^+ \to \mathbb{C}_p$. So it remains to show (ii) $\Rightarrow$ (i).

Write $\widetilde{p} = (p, p^{1/p}, \cdots) \in \widetilde{E}^+$, then $\xi = [\widetilde{p}] - p$ is a generator of $\mathrm{Ker}\,\theta \cap \tilde{A}^+$. We know

$$a_k = k + [v_E(x_k)] \to +\infty \text{ if } k \to +\infty.$$

Write $x_k = \widetilde{p}^{k-a_k} y_k$, then $y_k \in \widetilde{E}^+$. We have

$$p^k[x_k] = \left(\frac{p}{\widetilde{p}}\right)^k [\widetilde{p}]^{a_k}[y_k] = p^{a_k}(1 + \frac{\xi}{p})^{a_k-k}[y_k].$$

Note that $p^k(1+\frac{\xi}{p})^{a_k-k} \in p^{a_k-m}\widetilde{A}^+ + (\operatorname{Ker}\theta)^{m+1}$ for all m. Thus, $a_k \to +\infty$ implies that $p^k[x_k] \to 0 \in B_{dR}^+/(\operatorname{Ker}\theta)^{m+1}$ for every m, and therefore also in B_{dR}^+ by the definition of the topology of B_{dR}^+. □

Remark. We just proved $\widetilde{A}^{(0,1]} := B_{dR}^+ \cap \widetilde{A}$, and we can use

$$\varphi^{-n} : \widetilde{A}^{(0,p^{-n}]} \xrightarrow{\sim} \widetilde{A}^{(0,\,1]}$$

to embed $\widetilde{A}^{(0,r]}$ in B_{dR}^+, for $r \geq p^{-n}$.

Define

$$\widetilde{A}^{\dagger} := \bigcup_{r>0} \widetilde{A}^{(0,\,r]} = \{x \in \widetilde{A} : \varphi^{-n}(x) \text{ converges in } B_{dR}^+ \text{ for } n \gg 0\}.$$

Lemma 8.3.4. *$x \in \sum_{k=0}^{+\infty} p^k[x_k]$ is a unit in $\widetilde{A}^{(0,r]}$ if and only if $x_0 \neq 0$ and $v_E(\frac{x_k}{x_0}) > -\frac{k}{r}$ for all $k \geq 1$.*

Proof. Exercise. Just adapt the proof of *Gauss Lemma*. □

Set

$$\widetilde{B}^{(0,\,r]} = \widetilde{A}^{(0,r]}[\frac{1}{p}] = \bigcup_{n\in\mathbb{N}} p^{-n}\widetilde{A}^{(0,r]},$$

endowed with the topology of inductive limit, and

$$\widetilde{B}^{\dagger} = \bigcup_{r>0} \widetilde{B}^{(0,\,r]},$$

again with the topology of inductive limit.

Theorem 8.3.5. *$\widetilde{B}^{\dagger}$ is a subfield of $\widetilde{B}$, stable by φ and $G_{\mathbb{Q}_p}$, both acting continuously.*

$\widetilde{B}^{\dagger}$ is called the field of *overconvergent elements*. We are going to prove elements of $D(V)^{\psi=1}$ are overconvergent.

Definition 8.3.6. (i) $B^{\dagger} = \widetilde{B}^{\dagger} \cap B$, $A^{\dagger} = \widetilde{A}^{\dagger} \cap B$ (so $B^{\dagger}$ is a subfield of B stable by φ and $G_{\mathbb{Q}_p}$), $A^{(0,\,r]} = \widetilde{A}^{(0,\,r]} \cap B$.

(ii) If $K/\mathbb{Q}_p$ is a finite extension and $\Lambda \in \{\widetilde{A}^{\dagger}, \widetilde{B}^{\dagger}, A^{\dagger}, B^{\dagger}, A^{(0,\,r]}, B^{(0,\,r]}\}$, define $\Lambda_K = \Lambda^{H_K}$. For example $A_K^{(0,\,r]} = \widetilde{A}^{(0,\,r]} \cap A_K$.

(iii) If $\Lambda \in \{A, B, A^{\dagger}, B^{\dagger}, A^{(0,\,r]}, B^{(0,\,r]}\}$, and $n \in \mathbb{N}$, define $\Lambda_{K,n} = \varphi^{-n}(\Lambda_K) \subset \widetilde{B}$.

We now want to make $A_K^{(0,r]}$ more concrete. Let $F' \subset K_\infty$ be the maximal unramified extension of $\mathbb{Q}_p$, $\bar{\pi}_K$ be a uniformizer of $E_K = k_{F'}((\bar{\pi}_K))$, $\bar{P}_K \in E_{F'}[X]$ be a minimal polynomial of $\bar{\pi}_K$. Let $P_K \in A^+_{F'}[X]$ (note that $A^+_{F'} = \mathcal{O}_{F'}[[\pi]]$) be a lifting of $\bar{P}_K$. By Hensel's lemma, there exists a unique $\pi_K \in A_K$ such that $P_K(\pi_K) = 0$ and $\bar{\pi}_K = \pi_K \bmod p$. If $K = F'$, we take $\pi_K = \pi$.

Lemma 8.3.7. *If we define*

$$r_K = \begin{cases} 1, & \text{if } E_K/E_{\mathbb{Q}_p} \text{ is unramified,} \\ (2v_E(\mathfrak{d}_{E_K/E_{\mathbb{Q}_p}}))^{-1}, & \text{otherwise .} \end{cases}$$

then π_K and $P_K'(\pi_K)$ are units in $A_K^{(0,r]}$ for all $0 < r < r_K$.

Proof. The proof is technical but not difficult and is left to the readers. □

Proposition 8.3.8. (i) $A_K = \{\sum_{n\in\mathbb{N}} a_n\pi_K^n : a_n \in \mathcal{O}_{F'}, \lim_{n\to-\infty} v_p(a_n) = +\infty\}$*;*

(ii) $A_K^{(0,r]} = \{\sum_{n\in\mathbb{N}} a_n\pi_K^n : a_n \in \mathcal{O}_{F'}, \lim_{n\to-\infty}(v_p(a_n) + rnv_E(\bar{\pi}_K)) = +\infty\}$.
So $f \mapsto f(\pi_K)$ is an isomorphism from bounded analytic functions on the annulus $0 < v_p(T) \leq rv_E(\bar{\pi}_K)$ to the ring $B_K^{(0,r]}$.

Proof. The technical but not difficult proof is again left as an exercise. See Cherbonnier-Colmez Invent. Math. 1998. □

Corollary 8.3.9. (i) *$A_K^{(0,r]}$ is a principal ideal domain;*

(ii) *If L/K is a finite Galois extension, then $A_L^{(0,r]}$ is an étale extension of $A_K^{(0,r]}$ if $r < r_L$, and the Galois group is nothing but H_K/H_L.*

Define $\widetilde{\pi}_n = \varphi^{-n}(\pi)$, $\widetilde{\pi}_{K,n} = \varphi^{-n}(\pi_{K,n})$.

Proposition 8.3.10. (i) *If $p^n r_K \geq 1$, $\theta(\widetilde{\pi}_{K,n})$ is a uniformizer of K_n;*

(ii) $\widetilde{\pi}_{K,n} \in K_n[[t]] \subset B^+_{dR}$.

Proof. First by definition

$$\widetilde{\pi}_n = [\varepsilon^{1/p^n}] - 1 = \varepsilon^{(n)}e^{t/p} - 1 \in F_n[[t]] \subset B^+_{dR}$$

(for $[\varepsilon^{1/p^n}] = \varepsilon^{(n)}e^{t/p^n}$: the θ value of both sides is $\varepsilon^{(n)}$, and the p^n-th power of both side is $[\varepsilon] = e^t$ (recall $t = \log[\varepsilon]$)). This implies the proposition in the unramified case.

For the ramified case, we proceed as follows.

By the definition of E_K, $\pi_{K,n} = \theta(\widetilde{\pi}_{K,n})$ is a uniformizer of $K_n \bmod \mathfrak{a} = \{x : v_p(x) \geq \frac{1}{p}\}$. Write ω_n be the image of $\pi_{K,n}$ in $K_n \bmod \mathfrak{a}$. So we just have to prove $\pi_{K,n} \in K_n$.

Write

$$P_K(x) = \sum_{i=0}^{d} a_i(\pi)x^i, \ a_i(\pi) \in \mathcal{O}_{F'}[[\pi]].$$

Define

$$P_{K,n}(x) = \sum_{i=0}^{d} a_i^{\varphi^{-n}}(\pi_n)x_i,$$

then $P_{K,n}(\pi_{K,n}) = \theta(\varphi(P_K(\pi_K))) = 0$. Then we have $v_p(P_{K,n}(\omega_n)) \geq \frac{1}{p}$ and

$$v_p(P'_{K,n}(\omega_n)) = \frac{1}{p^n} v_E(P'_K(\bar{\pi}_K)) = \frac{1}{p^n} v_E(\mathfrak{d}_{E_K/E_{\mathbb{Q}_p}}) < \frac{1}{2p} \text{ if } p^n r_K > 1.$$

Then one concludes by Hensel's Lemma that $\pi_{K,n} \in K_n$.

For (ii) , one uses Hensel's Lemma in $K_n[[t]]$ to conclude $\widetilde{\pi}_{K,n} \in K_n[[t]]$. $\square$

Corollary 8.3.11. *If $0 < r < r_K$ and $p^n r \geq 1$, $\varphi^{-n}(A_K^{(0,r]}) \subset K_n[[t]] \subset B_{dR}^+$.*

8.3.2 Overconvergent representations

Suppose V is a free $\mathbb{Z}_p$ representation of rank d of G_K. Let

$$D^{(0,r]} := (A^{(0,r]} \otimes_{\mathbb{Z}_p} V)^{H_K} \subset D(V).$$

This is a $A_K^{(0,r]}$-module stable by Γ_K. As for φ, we have

$$\varphi : D^{(0,r]}(V) \longrightarrow D^{(0,p^{-1}r]}(V).$$

Definition 8.3.12. V is *overconvergent* if there exists an $r_V > 0, r_V \leq r_K$ such that

$$A_K \bigotimes_{A_K^{(0,r_V]}} D^{(0,r_V]}(V) \xrightarrow{\sim} D(V).$$

By definition, it is easy to see for all $0 < r < r_V$,

$$D^{(0,r]}(V) = A_K^{(0,r]} \bigotimes_{A_K^{(0,r_V]}} D^{(0,r_V]}(V).$$

Proposition 8.3.13. *If V is overconvergent, then there exists a C_V such that if $\gamma \in \Gamma_K$, $n(\gamma) = v_p(\log(\chi(\gamma)))$ and $r < \inf\{p^{-1}r_V, p^{-n(\gamma)}\}$, then $\gamma - 1$ is invertible in $D^{(0,r]}(V)^{\psi=0}$ and*

$$v^{(0,r]}((\gamma-1)^{-1}x) \geq v^{(0,r]}(x) - C_V - p^{n(\gamma)}v_E(\bar{\pi}).$$

Proof. Write $x = \sum_{i=1}^{p-1}[\varepsilon]^i\varphi(x_i)$ and adapt the proof of the same statement as in the characteristic p case. One has to use the fact that $[\varepsilon]^{ip^n-1}$ is a unit in $A_K^{(0,r]}$ if $r < p^{-n}$ and $i \in \mathbb{Z}_p^*$. □

Remark. This applies to $(A_K^{(0,r]})^{\psi=0}$.

Theorem 8.3.14 (Main Theorem). (i) *All (free $\mathbb{Z}_p$ or $\mathbb{Q}_p$) representations of G_K are overconvergent.*

(ii) *$D(V)^{\psi=1} \subset D^{(0,r_V]}(V)$.*

Sketch of Proof. (ii) is just because ψ improves convergence.

(i) follows from Sen's method applied to

$$\widetilde{\Lambda} = \widetilde{A}^{(0,1]},\ v = v^{(0,1]},\ G_0 = G_K, \Lambda_{H_{K,n}} = \varphi^{-n}(A_K^{(0,1]}).$$

Now we show how to check the three conditions.

(TS1). Let $L \supset K \supset \mathbb{Q}_p$ be finite extensions, for $\alpha = [\bar{\pi}_L](\sum_{\tau \in H_K/H_L}\tau([\bar{\pi}_L]))^{-1}$, then for all n,

$$\sum_{\tau \in H_K/H_L} \tau(\varphi^{-n}(\alpha)) = 1,$$

and

$$\lim_{n \to +\infty} v^{(0,1]}(\varphi^{-n}(\alpha)) = 0.$$

(TS2). First $\Lambda_{H_{K,n}} = A_{K,n}^{(0,1]}$. Suppose $p^n r_K \geq 1$. We can define $R_{K,n}$ by the following commutative diagram:

$$\begin{tikzcd}
R_{K,n}: & \widetilde{A}_K^{(0,1]} \arrow[r] & A_{K,n}^{(0,1]} \\
& A_{K,n+k}^{(0,1]} \arrow[u, hook] \arrow[ur, "\varphi^n \circ \psi^{n+k} \circ \varphi^{n+k}"'] &
\end{tikzcd}$$

One verifies that $\varphi^{-n}\circ\psi^{n+k}\circ\varphi^{n+k}$ does not depend on the choice of k, using the fact $\psi\varphi=\mathrm{Id}$. Then the proof is entirely parallel to that for $\mathbb{C}_p$ with ψ in the role of $p^{-1}\operatorname{Tr}_{F_{n+1}/F_n}$ and $\widetilde{\pi}_{n+k}$ in the role of π_{n+k}.

(TS3). For an element x such that $R_{K,n}(x)=0$, write

$$x=\sum_{i=0}^{+\infty}R^*_{K,n}(x),\ \text{ where } R^*_{K,n}(x)\in\varphi^{-(n+i+1)}((A_K^{(0,p^{-(n+i+1)}]})^{\psi=0}).$$

Then just apply Proposition 8.3.13 on $(A_K^{(0,p^{-(n+i+1)}]})^{\psi=0}$.

Now Sen's method implies that there exists an n and a $A_{K,n}^{(0,1]}$-module $D_{K,n}^{(0,1]}\subset\widetilde{A}^{(0,1]}\bigotimes V$ such that

$$\widetilde{A}^{(0,1]}\otimes_{A_{K,n}^{(0,1]}}D_{K,n}^{(0,1]}\xrightarrow{\sim}\widetilde{A}^{(0,1]}\otimes V.$$

Play with (TS3) just like Lemma 8.2.8, one concludes that $D_{K,n}^{(0,1]}\subset\varphi^{-n}(D(V))$ and $\varphi^n(D_{K,n}^{(0,1]})\subset D^{(0,p^{-n}]}(V)$. We can just take $r_V=n$. □

8.3.3 p-adic Hodge theory and (φ,Γ)-modules

Suppose we are given a representation V, $0<r<r_V$ and n such that $p^nr>1$. Then we have

$$\varphi^{-n}(D^{(0,r]}(V))\hookrightarrow B_{dR}^+\otimes V\xrightarrow{\theta}\mathbb{C}_p\otimes V$$

and

$$\varphi^{-n}(A_K^{(0,r]})\hookrightarrow K_n[[t]]\xrightarrow{\theta}K_n.$$

So we get the maps

$$\theta\circ\varphi^{-n}:\ K_n\otimes_{A_K^{(0,1]}}D^{(0,r]}(V)\longrightarrow\mathbb{C}_p\otimes V\tag{8.1}$$

and

$$\varphi^{-n}:\ t^iK_n[[t]]\otimes_{A_K^{(0,r]}}D^{(0,r]}(V)\longrightarrow t^iB_{dR}^+\otimes V,\ \forall\ i\in\mathbb{Z}.\tag{8.2}$$

Theorem 8.3.15. *There exists an $n(V)\in\mathbb{N}$ such that if $n\geq n(V)$, then we have*

(i) *the image of $\theta\circ\varphi^{-n}$ in (8.1) is exactly $D_{Sen,n}(V)$;*
(ii) $\mathrm{Fil}^i D_{dR}(V)=(\mathrm{Im}\ \varphi^{-n})^{\Gamma_K}$ *in (8.2) for all i;*
(iii) $D_{dR}(V)=\big(K_n((t))\bigotimes_{A_K^{(0,r]}}D^{(0,r]}(V)\big)^{\Gamma_K}$.

Let $K/\mathbb{Q}_p$ be a finite extension, and define

$$B_K^\dagger = \{F(\pi_K) :\ F \text{ is a bounded analytic function on } 0 < v_p(t) \le r(F),\, r(F) > 0\},$$
$$B_{\mathrm{rig},\,K}^\dagger = \{F(\pi_K) :\ F \text{ is an analytic function on } 0 < v_p(t) \le r(F),\, r(F) > 0\}$$

(this last ring is the Robba ring in the variable π_K), and

$$B_{\log,\,K}^\dagger = B_{\mathrm{rig},\,K}^\dagger[\log \pi_K].$$

Extend φ, Γ_K by continuity on $B_{\mathrm{rig},\,K}^\dagger$, and set

$$\varphi(\log \pi_K) = p \log \pi_K + \log \frac{\varphi(\pi_K)}{\pi_K^p},$$
$$\gamma(\log \pi_K) = \log \pi_K + \log \frac{\gamma(\pi_K)}{\pi_K}$$

where $\log \frac{\varphi(\pi_K)}{\pi_K^p} \in B_K^\dagger$ and $\log \frac{\gamma(\pi_K)}{\pi_K} \in B_{\mathrm{rig},\,K}^\dagger$. Let

$$N = -\frac{1}{v_E(\bar{\pi}_K)} \cdot \frac{d}{d \log \pi_K}.$$

Theorem 8.3.16 (Berger). *For*

$$D^\dagger(V) = (B^\dagger \otimes V)^{H_K} = \bigcup_{r>0} D^{(0,\,r]}(V),$$

if V is semi-stable, then

$$B_{\log,\,K}^\dagger\Big[\frac{1}{t}\Big] \otimes_{K_0} D_{st}(V) = B_{\log,\,K}^\dagger\Big[\frac{1}{t}\Big] \otimes_{B_K^\dagger} D^\dagger(V)$$

is an isomorphism of (φ, N, Γ_K)-modules. This implies that $D_{st}(V)$ is the invariant under Γ_K.

8.3.4 A map of the land of the rings

The following *nice picture* outlines most of the objects that we have discussed till now and that we shall have to discover more about in the future.

$$\begin{tikzcd}
 & \boxed{\begin{array}{c}p\text{-adic}\\ \text{Hodge}\\ \text{Theory}\end{array}} & & B_{dR}^{+} \arrow[ll] \arrow[dddr] & \\
 & & \tilde{B}_{\log}^{\dagger} \arrow[ur, dotted, "\varphi^{-n}"] & \tilde{B}_{\log}^{+} \arrow[l] \arrow[u] \arrow[r] & B_{st}^{+} \\
\boxed{\begin{array}{c}(\varphi,\Gamma)\text{-}\\ \text{modules}\end{array}} & & \tilde{B}_{\mathrm{rig}}^{\dagger} \arrow[u] & \tilde{B}_{\mathrm{rig}}^{+} \arrow[l] \arrow[u] \arrow[r] & B_{cris}^{+} \arrow[u] \\
B \arrow[u] \arrow[r, hook] & \tilde{B} & \tilde{B}^{\dagger} \arrow[l] \arrow[u] & \tilde{B}^{+} \arrow[l] \arrow[u] \arrow[r, "\theta"] & \mathbb{C}_p \\
A \arrow[u, "\frac{1}{p}"] \arrow[d, "\mathrm{mod}\, p"'] \arrow[r, hook] & \tilde{A} \arrow[u] \arrow[d] & \tilde{A}^{\dagger} \arrow[l] \arrow[u] \arrow[d] & \tilde{A}^{+} \arrow[l] \arrow[u] \arrow[d] \arrow[r] & \mathcal{O}_{\mathbb{C}_p} \arrow[u] \arrow[d] \\
E \arrow[r, hook] & \tilde{E} & \tilde{E}^{\dagger} \arrow[l] & \tilde{E}^{+} \arrow[l] \arrow[r] & \mathcal{O}_{C_p}/p
\end{tikzcd}$$

where

$$\tilde{B}_{\mathrm{rig}}^{+} = \bigcap_{n} \varphi^{n}(B_{cris}^{+}), \quad \tilde{B}_{\log}^{+} = \bigcap_{n} \varphi^{n}(B_{st}^{+}).$$

Note that most arrows from (φ, Γ)-modules to p-adic Hodge theory are in the wrong direction, but overconvergence and Berger's theorem allow us to go backwards.

8.4 Explicit reciprocity laws and p-adic L-functions

8.4.1 Galois cohomology of B_{dR}

Suppose K is a finite extension of $\mathbb{Q}_p$. Recall that we have the following:

Proposition 8.4.1. *For $k \in \mathbb{Z}$, then*

(i) *if $k \neq 0$, then $H^i(G_K, \mathbb{C}_p(k)) = 0$ for all i*

(ii) *if $k = 0$, then $H^i(G_K, \mathbb{C}_p) = 0$ for $i \geq 2$, $H^0(G_K, \mathbb{C}_p) = K$, and $H^1(G_K, \mathbb{C}_p)$ is a 1-dimensional K-vector space generated by $\log \chi \in H^1(G_K, \mathbb{Q}_p)$. (i.e, the cup product $x \mapsto x \cup \log \chi$ gives an isomorphism $H^0(G_K, \mathbb{C}_p) \simeq H^1(G_K, \mathbb{C}_p)$).*

Remark. This has been proved for $i \leq 1$. For $i \geq 2$, $H^i(H_K, \mathbb{C}_p(k)) = 0$ by using the same method as for H^1. Then just use the exact sequence

$$1 \longrightarrow H_K \longrightarrow G_K \longrightarrow \Gamma_K \longrightarrow 1$$

and Hochschild-Serre spectral sequence to conclude.

Proposition 8.4.2. *Suppose $i < j \in \mathbb{Z} \cup \{\pm\infty\}$, then if $i \geq 1$ or $j \leq 0$,*

$$H^1(G_K, t^i B_{dR}^+/t^j B_{dR}^+) = 0;$$

if $i \leq 0$ and $j > 0$, then $x \mapsto x \cup \log \chi$ gives an isomorphism

$$H^0(G_K, t^i B_{dR}^+/t^j B_{dR}^+)(\simeq K) \xrightarrow{\sim} H^1(G_K, t^i B_{dR}^+/t^j B_{dR}^+).$$

Proof. Use the long exact sequence in continuous cohomology attached to the exact sequence

$$0 \longrightarrow t^{i+n}\mathbb{C}_p(\simeq \mathbb{C}_p(i+n)) \longrightarrow t^i B_{dR}^+/t^{n+i+1} B_{dR}^+ \longrightarrow t^i B_{dR}^+/t^{i+n} B_{dR}^+ \longrightarrow 0,$$

and use induction on $j-i$ (note that in the base step $j = i+1$, $t^i B_{dR}^+/t^j B_{dR}^+ \cong \mathbb{C}_p(i)$), and Proposition 8.4.1 to do the computation. This concludes for the case where i, j are finite. For the general case, one proves it by taking limits. $\square$

8.4.2 Bloch-Kato's dual exponential maps

Let V be a de Rham representation of G_K, we have

$$B_{dR} \otimes_{\mathbb{Q}_p} V \cong B_{dR} \otimes_K D_{dR}(V) = H^0(G_K,\, B_{dR} \otimes V)$$

and

$$H^1(G_K,\, B_{dR} \otimes V) = H^1(G_K,\, B_{dR} \otimes_K D_{dR}(V)) = H^1(G_K,\, B_{dR}) \otimes_K D_{dR}(V).$$

So we get an isomorphism

$$D_{dR}(V) \xrightarrow{\sim} H^1(G_K,\, B_{dR} \otimes V); \quad x \mapsto x \cup \log \chi.$$

Definition 8.4.3. The exponential map $\exp^*$ is defined through the commutative diagram:

$$\begin{tikzcd}
\exp^* :\ H^1(G_K, V) \arrow[rr] \arrow[dr] & & D_{dR}(V) \arrow[dl, shift right, "\sim"'] \\
& H^1(G_K, B_{dR} \otimes V) \arrow[ur, shift right] &
\end{tikzcd}$$

Proposition 8.4.4. (i) *The image of* $\exp^*$ *lies in* $\operatorname{Fil}^0 D_{dR}(V)$.

(ii) *For* $c \in H^1(G_K, V)$, $\exp^*(c) = 0$ *if and only if the extension* E_c

$$0 \longrightarrow V \longrightarrow E_c \longrightarrow \mathbb{Q}_p \longrightarrow 0,$$

is de Rham as a representation of G_K.

Proof. (ii) is just by the definition of de Rham. For (i), $c \in H^1(G_K, V)$ implies $c = 0 \in H^1(G_K, (B_{dR}/B_{dR}^+) \otimes V)$. But $x \mapsto x \cup \log\chi$ gives an isomorphism

$$D_{dR}(V)/\operatorname{Fil}^0(D_{dR}(V))(= H^0(G_K, (B_{dR}/B_{dR}^+)\otimes V)) \longrightarrow H^1(G_K, (B_{dR}/B_{dR}^+)\otimes V)).$$

So $\exp^*(c) = 0 \pmod{\operatorname{Fil}^0}$ □

Remark. $\exp^*$ is a very useful tool to prove the non-triviality of cohomology classes.

Now suppose $k \in \mathbb{Z}$, L is a finite extension of K. Then $V(k)$ is still de Rham as a representation of G_L. Define

$$D_{dR,L}(V(k)) := H^0(G_L, B_{dR} \otimes V(k)) = t^{-k} L \otimes_K D_{dR}(V)$$

by an easy computation. Thus,

$$\operatorname{Fil}^0(D_{dR,L}(V(k))) = t^{-k} \otimes_K \operatorname{Fil}^k D_{dR}(V)$$

and this is 0 if $k \gg 0$. So for every $k \in \mathbb{Z}$, for L/K finite,

$$\exp^* : H^1(G_L, V(k)) \longrightarrow t^{-k} L \otimes_K D_{dR}(V)$$

is identically 0 for $k \gg 0$.

8.4.3 The explicit reciprocity law

Recall that

$$H^1_{\mathrm{Iw}}(K, V) \xrightarrow{\sim} H^1(G_K, \mathbb{Z}_p[[\Gamma_K]] \otimes V) = H^1(G_K, \mathcal{D}_0(\Gamma_K, V)).$$

If $\eta : \Gamma_K \to \mathbb{Q}_p^*$ is a continuous character, for $n \in \mathbb{N}$,

$$\mu \in H^1(G_K, \mathcal{D}_0(\Gamma_K, V)) \longmapsto \int_{\Gamma_{K_n}} \eta\mu \in H^1(G_{K_n}, V \otimes \eta).$$

where we write $V \otimes \eta$, not as $V(\eta)$ to distinguish from $V(k) = V \otimes \chi^k$. Then

$$\exp^*(\int_{\Gamma_{K_n}} \chi^k \mu) \in t^{-k} K_n \otimes_K D_{dR}(V)$$

and is 0 if $k \gg 0$.

Recall also that we have the isomorphism $\mathrm{Exp}^* : H^1(K, V) \xrightarrow{\sim} D(V)^{\psi=1}$, that $D(V)^{\psi=1} \subset D^{(0, r_V]}(V)$ and that there exists $n(V)$ such that

$$\varphi^{-n}(D^{(0, r_V]}(V)) \subset K_n((t)) \otimes_K D_{dR}(V), \text{ for all } n \geq n(V).$$

Now denote by

$$\mathrm{Tr}_{K_{n+k}/K_n} = \mathrm{Tr}_{K_{n+k}((t))/K_n((t))} \otimes \mathrm{Id} :\ K_{n+k}((t)) \otimes D_{dR}(V) \to K_n((t)) \otimes D_{dR}(V).$$

Theorem 8.4.5 (Explicit Reciprocity Law). *Let V be a de Rham representation of G_K and $\mu \in H^1_{\mathrm{Iw}}(K, V)$.*

(i) *If $n \geq n(V)$, then*

$$p^{-n}\varphi^{-n}(\mathrm{Exp}^*(\mu)) = \sum_{k \in \mathbb{Z}} \exp^*(\int_{\Gamma_{K_n}} \chi^k \mu).$$

(ii) *For $n \in \mathbb{N}, n+i \geq n(V)$, then*

$$\mathrm{Exp^*}_{K_n}(\mu) := \mathrm{Tr}_{K_{n+i}/K_n}\big(p^{-(n+i)}\varphi^{-(n+i)}(\mathrm{Exp}^*(\mu))\big)$$

does not depend on i, and $\mathrm{Exp^*}_{K_n}(\mu) = \sum_{k \in \mathbb{Z}} \exp^*(\int_{\Gamma_{K_n}} \chi^k \mu)$.

Proof. (ii) follows from (i) and from the commutative diagram:

$$\begin{array}{ccc} H^1(G_{L_2,V}) & \xrightarrow{\exp^*} & L_2 \otimes_K D_{dR}(V) \\ {\scriptstyle\mathrm{cor}}\downarrow & & \downarrow{\scriptstyle \mathrm{Tr}_{L_2/L_1} \otimes_K \mathrm{Id}} \\ H^1(G_{L_1,V}) & \xrightarrow{\exp^*} & L_1 \otimes_K D_{dR}(V) \end{array}$$

where $L_1 \subset L_2$ are two finite extensions of K.

For (i), suppose $y = \mathrm{Exp}^*(\mu)$, $x \in D(V)$, and $x(k)$ is the image of x in $D(V(k)) = D(V)(k)$ (Thus, $\varphi(x(k)) = \varphi(x)(k)$ and $\gamma(x(k)) = \chi(\gamma)^k\gamma(x)(k)$).

The integral $\int_{\Gamma_{K_n}} \chi^k\mu$ is represented by the cocycle:

$$g \mapsto c_g = \frac{\log\chi(\gamma_n)}{p^n} \cdot \big(\frac{g-1}{\gamma_n - 1} y(k) - (g-1)b\big)$$

where $b \in A \otimes V$ is the solution of

$$(\varphi - 1)b = (\gamma_n - 1)^{-1}\big((\varphi - 1)(y)(k)\big).$$

From $y \in D^{(0,r_V]}(V)^{\psi=1}$ one gets

$$(\varphi - 1)y \in D^{(0,p^{-1}r_V]}(V)^{\psi=0}$$

and then

$$(\gamma_n - 1)^{-1}(\varphi - 1)y \in D^{(0,p^{-n}]}(V)^{\psi=0}.$$

Thus $b \in A^{(0,p^{1-n}]} \otimes V$. This implies that $\varphi^{-n}(b)$ and $\varphi^{-n}(y)$ both converge in $B^+_{dR} \otimes V$. Then $c_g = \varphi^{-n}(c_g)$ differs from

$$c'_g = \frac{\log\chi(\gamma_n)}{p^n} \cdot \frac{g-1}{\gamma_n - 1} \cdot \varphi^{-n}(y)(k)$$

by the coboundary $(g-1)(\varphi^{-n}(b))$. Therefore, they have the same image in $H^1(G_{K_n} B^+_{dR} \otimes V(k))$. Write

$$p^{-n}\varphi^{-n}(y) = \sum_{i \geq i_0} y_i t^i, \quad y_i \in K_n \otimes_K D_{dR}(V),$$

then

$$\begin{aligned} c'_g &= \log\chi(g) y_{-k} t^{-k} + \sum_{i \neq -k} \frac{\chi(g)^{i+k} - 1}{\chi(\gamma_n)^{i+k} - 1} \cdot y_i t^i \\ &= \log\chi(g) y_{-k} t^{-k} + (g-1) \sum_{i \neq -k} \frac{y_i t^i}{(\chi(\gamma_n)^{i+k} - 1)}. \end{aligned}$$

So we get $\exp^*\big(\int_{\Gamma_{K_n}} \chi^k\mu\big) = y_{-k}t^{-k}$. $\square$

8.4.4 Cyclotomic elements and Coates-Wiles morphisms.

Let $K=\mathbb{Q}_p$, $V=\mathbb{Q}_p(1)$, $u=\left(\frac{\pi_n}{1+\pi_n}\right)_{n\geq 1}\in\varprojlim\mathcal{O}_{F_n}$, $\kappa(u)\in H^1_{\mathrm{Iw}}(\mathbb{Q}_p,\,\mathbb{Q}_p(1))$, the Coleman power series $f_u=\frac{T}{1+T}$. Then we have

$$\mathrm{Exp}^*(\kappa(u))=(1+T)\frac{df_u}{dT}(\pi)=\frac{1}{\pi}.$$

Note that

$$\varphi^{-1}(\pi)^{-1}=([\varepsilon^{1/p}]-1)^{-1}=\frac{1}{(1+\pi_1)e^{t/p}-1},$$

then

$$\begin{aligned}\mathrm{Exp^*}_{\mathbb{Q}_p}(\kappa(u))&=\frac{1}{p}\operatorname{Tr}_{\mathbb{Q}_p(\pi_1)/\mathbb{Q}_p}\varphi^{-1}(\pi)^{-1}=\frac{1}{p}\sum_{z^p=1,\,z\neq 1}\frac{1}{e^{t/p}-1}\\ &=\frac{1}{e^t-1}-\frac{1}{p}\cdot\frac{1}{e^{t/p}-1}=\frac{1}{t}\cdot\Big(\frac{t}{e^t-1}-\frac{t/p}{e^{t/p}-1}\Big)\\ &=\sum_{n=1}^{+\infty}(1-p^{-n})\zeta(1-n)\frac{(-t)^{n-1}}{(n-1)!}.\end{aligned}$$

So

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

Remark. (i) The map

$$\varprojlim\mathcal{O}_{F_n}-\{0\}\longrightarrow H^1_{\mathrm{Iw}}(\mathbb{Q}_p,\,\mathbb{Q}_p(1))\longrightarrow\mathbb{Q}_p,\quad u\mapsto t^{k+1}\exp^*\Big(\int_{\Gamma_{\mathbb{Q}_p}}\chi^k\kappa(u)\Big)$$

is the *Coates-Wiles homomorphism*.

(ii) Since $\zeta(1+k)\neq 0$ if $k\leq -1$ is even, the above formula implies that the extensions of $\mathbb{Q}_p$ by $\mathbb{Q}_p(k+1)$ constructed via cyclotomic elements are non-trivial and are even not de Rham.

(iii) $\dim_{\mathbb{Q}_p}H^1(G_{\mathbb{Q}_p},\,\mathbb{Q}_p(k))=1$ if $k\neq 0,1$.

Corollary 8.4.6. *Non-trivial extensions of $\mathbb{Q}_p$ by $\mathbb{Q}_p(k)$ are not de Rham if $k\leq 0$ is odd.*

Exercise. (i) Prove that this is also true for $k\leq -1$ even by taking a general element of $D(\mathbb{Q}_p(1))^{\psi=1}$.

(ii) For $[K:\mathbb{Q}_p]<\infty$, prove the same statement.

8.4.5 Kato's elements and p-adic L-functions of modular forms.

Now we come to see the relations with modular forms. Suppose

$$f = \sum_{n=1}^{\infty} a_n q^n \in S_k(N),\ k \geq 2$$

is primitive. So $\mathbb{Q}(f) = \mathbb{Q}(a_1, \cdots, a_n, \cdots)$ is a finite extension of $\mathbb{Q}$, and $\mathbb{Q}_p(f) = \mathbb{Q}_p(a_1, \ldots, a_n, \ldots)$ is a finite extension of $\mathbb{Q}_p$.

Theorem 8.4.7 (Deligne). *There exists a representation V_f of $G_{\mathbb{Q}}$ of dimension 2 over $\mathbb{Q}_p(f)$, non-ramified outside Np, such that if $\ell \nmid Np$, for φ_ℓ the arithmetic Frobenius at ℓ ($\varphi_\ell(e^{\frac{2\pi i}{p^n}}) = e^{\frac{2\pi i \ell}{p^n}}$), then*

$$\det(1 - X\varphi_\ell^{-1}) = 1 - a_\ell X + \ell^{k-1} X^2.$$

Remark. A $\mathbb{Q}_p(f)$-representation V of dimension d is equivalent to a $\mathbb{Q}_p$ representation of dimension $d \cdot [\mathbb{Q}_p(f) : \mathbb{Q}_p]$ endowed with a homomorphism $\mathbb{Q}_p(f) \hookrightarrow \mathrm{End}(V)$ commuting with $G_{\mathbb{Q}}$. Therefore, $D_{cris}(V), D_{st}(V), D_{dR}(V)$ are all $\mathbb{Q}_p(f)$-vector spaces.

Theorem 8.4.8 (Faltings-Tsuji-Saito). (i) *V_f is a de Rham representation of $G_{\mathbb{Q}_p}$ with Hodge-Tate weights 0 and $1-k$, the 2-dimensional $\mathbb{Q}_p(f)$-vector space $D_{dR}(V_f)$ contains naturally f, and*

$$D^0_{dR}(V_f) = D_{dR}(V_f),\ D^k_{dR}(V_f) = 0,\ D^i_{dR}(V_f) = \mathbb{Q}_p(f)f \text{ if } 1 \leq i \leq k-1.$$

(ii) *If $p \nmid N$, then V_f is crystalline and*

$$\det(X - \varphi) = X^2 - a_p X + p^{k-1}.$$

If $p | N$ but $a_p \neq 0$, then V_f is semi-stable but not crystalline and a_p is the eigenvalue of φ on $D_{cris}(V)$; if $a_p = 0$, then V_f is potentially crystalline.

Remark. If V is a representation of G_K, $\mu \in H^1_{\mathrm{Iw}}(K, V)$,

$$\int_{\Gamma_{K_n}} \chi^k \mu \in H^1(G_{K_n}, V(k)),$$

then this is also true for $\int_{a\Gamma_{K_n}} \chi^k \mu$ for all $a \in \Gamma_K$ and for $\int_{\Gamma_K} \phi(x) \chi^k \mu$, with $\phi : \Gamma_K \to \mathbb{Z}_p$ being constant modulo Γ_{K_n}.

Theorem 8.4.9 (Kato). *There exists a unique element* $z_{\text{Kato}} \in H^1_{\text{Iw}}(\mathbb{Q}_p, V_f)$ (*obtained by* global methods *using Siegel units on modular curves*), *such that if* $0 \le j \le k-2$, ϕ *is locally constant on* $\mathbb{Z}_p^* \cong \Gamma_{\mathbb{Q}_p}$ *with values in* $\mathbb{Q}(f)$, *then*

$$\exp^*\Big(\int_{\mathbb{Z}*_p} \phi(x)x^{k-1-j}\cdot z_{\text{Kato}}\Big) = \frac{1}{j!}\widetilde{\Lambda}(f,\,\phi, j+1)\cdot \frac{f}{t^{k-1-j}}$$

where

$$\widetilde{\Lambda}(f,\,\phi, j+1) \in \mathbb{Q}(f,\,\mu_{p^n}), \qquad \frac{f}{t^{k-1-j}} \in \mathrm{Fil}^0(D_{dR}\big(V_f(k-1-j)\big)\big).$$

Our goal is to recover $L_{p,\alpha}(f,\,s)$ from z_{Kato} (recall $L_{p,\alpha}$ is obtained from $\mu_{f,\alpha} \in \mathcal{D}_{v_p(\alpha)}(\mathbb{Z}_p)$ before). We have $\mathrm{Exp}^*(z_{\text{Kato}}) \in D(V_f)^{\psi=1}$, but the question is how to relate this to $D_{cris}(V_f), D_{st}(V_f)$.

If $p \mid N$, let α be a root of $X^2 - a_pX + p^{k-1}$ with $v_p(\alpha) < k-1$; if $p \nmid N$, let $\alpha = a_p \neq 0$ (in this case $p\alpha^2 = p^{k-1}$). In both cases, take $\beta = p^{k-1}\alpha^{-1}$. Thus, α, β are eigenvalues of φ on $D_{st}(V_f)$.

Assume $\alpha \neq \beta$ (which should be the case for modular forms by a conjecture). Define $\Pi_\beta = \frac{\varphi-\alpha}{\beta-\alpha}$ to be the projection on the β-eigenspace in $D_{st}(V_f)$ and extend it by $B^\dagger_{\log,K}$-linearity to

$$B^\dagger_{\log,K}\Big[\frac{1}{t}\Big] \otimes_{K_0} D_{st}(V_f) \longrightarrow B^\dagger_{\log,K} \otimes_{B^\dagger_K} D^\dagger(V_f).$$

Theorem 8.4.10. (i) $\Pi_\beta(f) \neq 0$*;*

(ii)

$$\Pi_\beta\big(\mathrm{Exp}^*(z_{\text{Kato}})\big) = \Big(\int_{\mathbb{Z}_p} [\varepsilon]^x \mu_{f,\alpha}\Big)\frac{\Pi_\beta(f)}{t^{k-1}}.$$

Remark. $\mu_{f,\alpha}$ exists up to now only in the semi-stable case, but z_{Kato} exists all the time. So a big question is:

How to use it for p-adic L-function?