Università degli Studi di Padova

Dipartimento di Matematica "Tullio Levi-Civita"
Corso di Laurea Magistrale in Matematica

ON THE MAZUR-TATE-TEITELBAUM CONJECTURE

Relatore:
Prof. Adrian Ioviță

Laureando:
Nguyen Dang Khai Hoan, 2004308

Anno Accademico 2020/2021
21 luglio 2021

Acknowlegements

I would like to express my sincere gratitude to my supervisor, Prof.Adrian Ioviță, for his patient guidance, constant support, kind demeanor and immense knowledge. His insightful teaching pushed me to sharpen my thinking and provided opportunities for me to grow professionally.

Grateful thanks are extended to ALGANT consortium, whose grant funded my master study in Leiden and Padova. It has provided me the last two years a wonderful experience. I would like to give my special thanks to Prof.Jan-Hendrik Evertse, Prof.Peter Bruin, Prof.Márton Hablicsek in Leiden and Prof.Remke Kloosterman, Prof.Nicola Mazzari in Padova for their valuable advice and helpful assistance through my journey. Many thanks to lecturers and staffs in Leiden and Padova for their continuous support and help that as allowed for the completion of this master program.

Thanks also to the many friends, particularly 28 Oosterkade Family and chi Dân, for their encouragement, kindness and assistance during two years.

Finally, I am indebted to my family for their unconditional love and endless support. My accomplishments and success are because they believed in me. My warm and heartfelt thanks go to my love, Chuchi, for being there for me.

July, 2021
Nguyen Dang Khai Hoan

To My Family...
Be Strong Vietnam...

Preface

This thesis is intended to explain the result proved by Greenberg and Stevens on the Mazur-Tate-Teitelbaum conjecture. Specially, the objective of the thesis is to develop all the necessary theory in order to understand Greenberg and Stevens' paper [GS94] in detail.

Let E be an elliptic curve over $\mathbb{Q}$. One of the most important problems in modern number theory is Birch-Swinnerton-Dyer's conjecture which says that the order of vanishing of L-funtion attached to E at 1 is the rank of $E(\mathbb{Q})$. In 1986, Mazur-Tate-Teitelbaum [MTT] proposed p-adic analogues of this conjecture. On their work, the case of an elliptic curve with split multiplicative reduction at the prime p is of special interest. In the so called "exceptional zero" case, the order of vanishing of the p-adic L-function at the central point seems to be one higher than it is in the classical case. When E has split mutiplicative reduction at p, Tate proved that $E(\mathbb{Q}_p) \cong \mathbb{Q}_p^\times / \left\langle q^{\mathbb{Z}} \right\rangle$ where $q \in \mathbb{Q}_p^\times$ is the Tate p-adic period attached to E. Mazur, Tate and Teitelbaum define the $\mathcal{L}$-invariant $\mathcal{L}_p(E)$ by

$$\mathcal{L}_p(E) = \frac{\log_p(q)}{\mathrm{ord}_p(q)}$$

Here $\log_p : \mathbb{Q}_p^\times \to \mathbb{Z}_p$ is the p-adic logarithm on $\mathbb{Z}_p^\times$ extended to $\mathbb{Q}_p^\times$ by the relation $\log_p(p) = 0$ and $\mathrm{ord}_p : \mathbb{Q}_p^\times \to \mathbb{Z}$ is the normalized valuation. They studied numerically the relationship between the special value of the first derivative of the p-adic L-function attached to E and the special value of the classical one. The ratio should conjecturally relate to the $\mathcal{L}$-invariant $\mathcal{L}_p(E)$ of E.

This thesis can be divided in five chapters

Chapter 1: We review the construction of p-adic L-function attached to an elliptic curve in Mazur-Tate-Teitelbaum's paper [MTT] and state the main result.

Chapter 2: We introduce Hida theory which is the crucial technique in the proof of Greenberg and Stevens.

Chapter 3: We reinterpret the $\mathcal{L}$-invariant as the derivative of the p-th coefficient of Hida's cusp form.

Chapter 4: We introduce measure-valued modular symbols and use them to construct two-variable p-adic L-functions.

Chapter 5: We prove the main theorem by combining computations on the previous chapters.

Each chapter contains a little summary and some references at the beginning.

Notation and Terminology

$\mathbb{Q}_p$: the p-adic completion of $\mathbb{Q}$.

$\mathbb{Z}_p$: the p-adic integers in $\mathbb{Q}_p$

GL_2: invertible matrices.

SL_2: matrices with a determinant 1.

$M_k(\Gamma)$ (resp. $S_k(\Gamma)$): modular forms (resp. cusp forms) of weight k on Γ.

T_n: the Hecke operator.

$\mathcal{H}$: the Hecke algebra.

Ta_p: the p-adic Tate module.

m^σ: the action of σ on m.

Contents

CHAPTER 1

Introduction

The classical L-function of a cusp form f is an analytic function which encodes the Fourier coefficients of f. In this chapter, I will mainly follow the paper of Mazur-Tate-Teitelbaum [MTT] to present the modular symbol method which can be used to effectively express the values of the L-function. These symbols are basically line integrals in the upper half plane satisfying certain arithmetic properties. This chapter will also provide the construction of the Mazur-Swinnerton-Dyer p-adic L-function of a cusp form using a p-adic measure. The special values of L-functions twisted by a character can be interpolated p-adically by the p-adic analog L-function. A mystery factor so called p-adic multiplier enters into the formula being the discrepancy between the p-adic and classical special values. Hence, when the p-adic multiplier vanishes, the p-adic L-function is also equal to zero. In which case, Mazur-Tate-Teitelbaum conjecturally suggested the relationship between the special value of the first derivative of the p-adic L-function and the special value of the classical L-function.

1.1 L-functions

In this section, I will outline the construction of L-functions of modular forms and elliptic curves and their relation in the sense of Modularity theorem.

1.1.1 L-functions of Modular Forms

Firstly, we recall the Melin transform in complex analysis.

Proposition 1.1.1. *Let $g : (0, \infty) \to \mathbb{C}$ be a continuous function such that for some real numbers $a < b$ we have*

$$|g(t)| \ll t^{-a} \quad as\, t \to \infty$$

and

$$|g(t)| \ll t^{-b} \quad as\, t \to \infty$$

Then the integral

$$\mathcal{M}g(s) = \int_0^\infty g(t) t^s \frac{dt}{t}$$

converges absolutely and uniformly on compact subsets of the strip $\{s \in \mathbb{C} | a < Re(s) < b\}$

Proposition 1.1.2. *Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, and $f \in S_k(\Gamma)$ a cusp form of weight k with q-expansion at the cusp ∞ given by*

$$f(z) = \sum_{n=0}^{\infty} a_n(f) q^n$$

Then there exists a constant $C \in \mathbb{R}_{>0}$ such that for all $n \in \mathbb{Z}_{>0}$

$$|a_n(f)| \leq C n^{k/2}$$

Suppose that $f \in S_k(\Gamma_0(N))$ has the q-expansion

$$f(z) = \sum_{n \geq 1} a_n q^n, \quad a = e^{2\pi i z}$$

The L-function associated to f is given by

$$L(f, s) := \sum_{n \geq 1} \frac{a_n}{n^s}$$

for $s \in \mathbb{C}$ with $Re(s) > \dfrac{k}{2} + 1$

Theorem 1.1.3. *Let $f \in S_k(\Gamma_0(N))$. The L-function associated to f has the following integral representation*

$$L(f, s) = \sum_{n \geq 1} a_n n^{-s} = \frac{(2\pi)^s}{\Gamma(s)} \int_0^\infty f(it) t^s \frac{dt}{t}$$

which converges uniformly to a holomorphic function on $Re(s) > \frac{k}{2} + 1$. *Moreover, it extends analytically to a holomorphic function on* $\mathbb{C}$, *and the normalised L-function*

$$\Lambda(f, s) = N^{s/2} \frac{\Gamma(s)}{(2\pi)^s} L(f, s)$$

satisfies the functional equation

$$\Lambda(f, s) = \pm \Lambda(f, k - s)$$

For the newforms we also get an Euler product

Theorem 1.1.4. *Let* $f \in S_k^{new}(\Gamma_0(N))$. *The L-function attached to* f *has the Euler product*

$$L(f, s) = \prod_p \frac{1}{1 - a_p p^{-s} + \mathbf{1}_N p^{k-1} p^{-2s}}$$

where $\mathbf{1}_N$ *is the trivial Dirichlet character of conductor* N.

1.1.2 L-function of Elliptic Curves

Let K be a number field and let E be an elliptic curve over K. The points of E over K have an abelian group structure denoted by $E(K)$.

Theorem 1.1.5. *(Mordell-Weil) The group* $E(K)$ *is finitely generated.*

The Mordell-Weil theorem gives us the decomposition

$$E(K) \simeq E(K)_{tors} \oplus \mathbb{Z}^r$$

where the torsion subgroup $E(K)_{tors}$ is finite and the rank r of $E(K)$ is a nonnegative integer.

The L-function of an elliptic curve is a generating function that records information about the reduction of the curve modulo every prime. Consider the Weierstrass equation of an elliptic curve E over $\mathbb{Q}$

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, \quad a_1, .., a_6 \in \mathbb{Q}$$

Two integral Weierstrass equations are equivalent if they are related by a general admissible change of variable over $\mathbb{Q}$:

$$x = u^2x' + r, \quad y = u^3y' + su^2x' + t, \qquad u, r, s, t \in \mathbb{Q},\ u \neq 0$$

After an admissible change of variable of the form $(x, y) = (u^2x', u^3y')$ we can assume that the coefficients a_i's are integers. Moreover, if the field characteristic is neither 2 or 3, then its equation can be written as

$$y^2 = x^3 + AX + B.$$

In which case, the discriminant is given by $\Delta = -16(4A^3 + 27B^2)$. For each prime p, let $v_p(E)$ denote the smallest power of p appearing in the discriminant of any integral Weierstrass equation equivalent to E. That is

$$v_p(E) = \min\{v_p(\Delta(E')) : E' \text{ integral, equivalent to } E\}$$

Define the global mininal discriminant of E to be

$$\Delta_{\min}(E) = \prod_p p^{v_p(E)}$$

This is a finite product since $v_p(E) = 0$ for all $p \nmid \Delta(E)$. One can show that the p-adic valuation of the discriminant can be minimized to $v_p(E)$ simultaneously for all p under an admissible change of variable. That is, E is isomorphic over $\mathbb{Q}$ to an integral model E' with discriminant $\Delta(E') = \Delta_{\min}(E)$. This is the global minimal Weierstrass equation E', the model of E to reduce modulo primes.

One can reduce a global minimal Weierstrass equation E to a Weierstrass equation $\tilde{E}$ over $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ and this defines an elliptic curve over $\mathbb{F}_p$ if and only if $p \nmid \Delta_{\min}(E)$. The reduction is called

1. good, if $\tilde{E}$ is again an elliptic curve
   (a) ordinary, if $\tilde{E}[p] = \mathbb{Z}/p\mathbb{Z}$
   (b) supersingular, if $\tilde{E}[p] = \{0\}$
2. bad if $\tilde{E}$ is not an elliptic curve, in which case it has only one singular point,
   (a) multiplicative, if $\tilde{E}$ has a node
   (b) additive, if $\tilde{E}$ has a cusp

Define the algebraic conductor of E by $N_E = \prod_p p^{f_p}$ where

$$f_p = \begin{cases} 0 & \text{If E has good reduction at p} \\ 1 & \text{If E has multiplicative reduction at p} \\ 2 & \text{If E has additive reduction at p and } p \notin \{2,3\} \\ 2+\delta_p & \text{If E has additive reduction at p and } p \in \{2,3\} \end{cases}$$

here $\delta_2 \leq 6$ and $\delta \leq 3$. There is also a closed-form formula for f_p.

Theorem 1.1.6. *Let E be an elliptic curve over $\mathbb{Q}$ with conductor N_E. Assume E is in reduced form. Let p be a prime and let $\tilde{E}$ be the reduction of E modulo p. Then define*

$$a_1(E) = 1$$
$$a_p(E) = p + 1 - \#\tilde{E}(\mathbb{F}_p)$$

Then there is a newform $f \in S_2(\Gamma_0(N_E))$ such that for primes p we have

$$a_p(f) = a_p(E)$$

Moreover, the coefficients $a_{p^e}(E)$ satisfy the same recurrence as the coefficients $a_{p^e}(f)$,i.e.,

$$a_{p^e}(E) = a_p(E)a_{p^{e-1}}(E) - p\mathbf{1}_{N_E}(p)a_{p^{e-2}}(E) \;\; \forall e \geq 2$$

where $\mathbf{1}_{N_E}$ is the trivial character modulo the algebraic conductor N_E of E.

Theorem 1.1.7. *(Hasse's theorem) Let $E/\mathbb{F}_p$ be an elliptic curve defined over a finite field. Then*

$$|a_p| = |\#E(\mathbb{F}_p) - p - 1| \leq 2\sqrt{p}$$

We can reinterpret the Modularity theorem in term of L-functions

Definition 1.1.8. The Hasse-Weil L-function of E is defined by

$$\begin{aligned} L(E,s) &= \sum_{n=1}^{\infty} \frac{a_n(E)}{n^s}, \quad s \in \mathbb{C} \\ &= \prod_p \frac{1}{1 - a_p(E)p^{-s} + \mathbf{1}_{N_E}(p)p^{1-2s}} \end{aligned}$$

where $\mathbf{1}_{N_E}$ is the trivial character modulo the algebraic conductor N_E of E.

This L-function encodes the solution-counts $a_p(E)$.

Theorem 1.1.9. *Let E be an elliptic curve over $\mathbb{Q}$ with conductor N_E. Then there is a newform $f \in S_2^{new}(\Gamma_0(N_E))$ such that for primes p we have*

$$L(f, s) = L(E, s)$$

Define the normalised L-function

$$\Lambda(E, s) = N^{s/2} \frac{\Gamma(s)}{(2\pi)^s} L(E, s)$$

satisfies the functional equation

$$\Lambda(E, s) = \pm\Lambda(f, 2 - s)$$

Using the Hasse bound, one can get the functional half-plane convergence of $L(E, s)$ for $Re(s) > 2$ and the functional equation that determines $L(E, s)$ for $Re(s) < 0$. Theorem 1.1.9 implies that $L(E, s)$ is analytic on all $\mathbb{C}$.

Birch and Swinnerton-Dyer Conjecture: Let E be an elliptic curve defined over $\mathbb{Q}$. Then the order of vanishing of $L(E, s)$ at $s = 1$ is the rank of $E(\mathbb{Q})$. That is, if $E(\mathbb{Q})$ has rank r then

$$L(E, s) = (s - 1)^r g(s), \quad g(1) \neq 0, \infty$$

1.2 Modular Integrals

Recall that $A \in \mathrm{GL}_2(\mathbb{R})$ acts on $\mathbb{C} \cup \infty$ by the formula

$$A(z) = \frac{az + b}{cz + d} \text{ and } A(\infty) = \frac{a}{c}$$

Fix an integer $k \geq 2$. Let $S_k(\Gamma_0(N), \chi)$ denote the space of cusp forms of weight k with Dirichlet character χ on $\Gamma_0(N)$. Let

$$S_k = \sum_{N,\chi} S_k(\Gamma_0(N), \chi)$$

denote the space of all cusp forms of weight k which are on $\Gamma_1(N)$ for some N. Define actions of $\mathrm{GL}_2(\mathbb{Q})^+$ on S_k by the formula

$$\left(f|A\right)(z) := \frac{\det A^{k/2}}{(cz + d)^k} \cdot f\left(A(z)\right)$$

Let $\mathcal{P}_k(R)$ denote the space of polynomials of the degree $\leq k-2$ with coefficient in a commutative ring R. Define actions of $\mathrm{GL}_2(\mathbb{Q})^+$ on $\mathcal{P}_k(\mathbb{C})$ by the formula

$$\big(P|A\big)(z) := \frac{\det A^{1-k/2}}{(cz+d)^{2-k}} \cdot P\left(A(z)\right)$$

Definition 1.2.1. Let $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$. Define a map

$$\Phi : S_k \times \mathcal{P}_k(\mathbb{C}) \times \mathbb{P}^1(\mathbb{Q}) \to \mathbb{C}$$

by the formula

$$\Phi(f,P,r) = 2\pi i \int_\infty^r f(z)\cdot P(z)dz = \begin{cases} 2\pi \displaystyle\int_0^\infty f(r+it)\cdot P(r+it)dt & \text{if } r \in \mathbb{Q} \\ 0 & \text{if } r = \infty \end{cases}$$

Proposition 1.2.2. *The map Φ has the following properties*

1. *For any $r \in \mathbb{P}^1(\mathbb{Q})$, the map $\Phi(f,P,r)$ is $\mathbb{C}$-bilinear in f and P*
2. *For any matrix $A \in GL_2(\mathbb{Q})^+$ we have*

$$\Phi(f|A, P|A, r) = \Phi(f,P,A(r)) - \Phi(f,P,A(\infty))$$

It follows that $\Phi(f,P,\infty) = 0$.

Proof. The first property follows from the linearity of the integral. For the latter one, by definition, note that

$$(f|A)(z)\cdot(P|A)(z)dz = f(A(z))\cdot P(A(z))d(A(z))$$

Hence we obtain

$$\begin{aligned} \phi(f|A,P|A,r) &= 2\pi i \int_{A(\infty)}^{A(r)} f(z)\cdot P(z)dz \\ &= 2\pi i \int_\infty^{A(r)} f(z)\cdot P(z)dz - 2\pi i \int_\infty^{A(\infty)} f(z)P(z)dz \\ &= \phi(f,P,A(r)) - \phi(f,P,A(\infty)) \end{aligned}$$

Applying to $A = \mathit{identity}$ yields $\phi(f,P,\infty) = 0$. □

Definition 1.2.3. For $a, m \in \mathbb{Q}$, $m > 0$, $f \in S_k(\Gamma_1(N))$ and $P \in \mathcal{P}_k(\mathbb{C})$ we define

$$\lambda(f,P,a,m) := \Phi(f, P(mz+a), -\frac{a}{m})$$

Remark 1.2.4. By the definition of the action of $\mathrm{GL}_2(R)$ on $\mathcal{P}_k$, we consider the matrix $A = \begin{pmatrix} m & a \\ 0 & 1 \end{pmatrix}$ and get $P(mz+a) = m^{k/2-1}P\Big|\begin{pmatrix} m & a \\ 0 & 1 \end{pmatrix}$. Note that $A^{-1} = \begin{pmatrix} 1 & -a \\ 0 & m \end{pmatrix}$, using proposition 1.2.2.2 we obtain the following equivalent formula

$$\begin{aligned}\lambda(f,P,a,m) &:= \Phi(f, P(mz+a), -\frac{a}{m}) \\ &= m^{(k/2)-1}\Phi\left(f, P\Big|\begin{pmatrix} m & a \\ 0 & 1 \end{pmatrix}, -\frac{a}{m}\right) \\ &= m^{(k/2)-1}\Phi\left(f\Big|\begin{pmatrix} 1 & -a \\ 0 & m \end{pmatrix}, P, 0\right)\end{aligned}$$

Proposition 1.2.5. *The map $\lambda(f,P,a,m)$ is $\mathbb{C}$-bilinear in (f,P). For fixed f and P, this map depends only upon a modulo m.*

Proof. The $\mathbb{C}$-bilinearity of λ follows from $\mathbb{C}$-bilinearity of Φ. Note that

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_1(N) \text{ and } f|A = f$$

It follows that

$$\begin{aligned}\lambda(f,P,a,m) &= m^{(k/2)-1}\Phi(f\Big|\begin{pmatrix} 1 & -a \\ 0 & m \end{pmatrix}, P, 0) \\ &= m^{(k/2)-1}\Phi(f\Big|\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\cdot\begin{pmatrix} 1 & -a \\ 0 & m \end{pmatrix}, P, 0) \\ &= m^{(k/2)-1}\Phi(f\Big|\begin{pmatrix} 1 & -a+m \\ 0 & m \end{pmatrix}, P, 0) \\ &= \lambda(f,P,a+m,m)\end{aligned}$$

□

We can express the special values of the L-function of f in terms of the modular symbol for f. Recall that

$$L(f,s) = \sum_{n\geq 1} a_n n^{-s} = \frac{(2\pi)^s}{\Gamma(s)}\int_0^\infty f(it)t^s\frac{dt}{t}$$

Proposition 1.2.6. *We have*

$$\lambda(f, z^n, 0, 1) = -2\pi i \int_0^{i\infty} f(z) z^n dz = i^n \frac{n!}{(2\pi)^n} L(f, n+1)$$

for $0 \leq n \leq k-2$.

We can twist a cusp form by a Dirichlet character χ. Assume that $f(z) = \sum_{n\geq 1} a_n q^n$ with $q = e^{2\pi i z}$, then we define the twisting of f by χ by the formula

$$f_\chi(z) := \sum_{n\geq 1} \chi(n) a_n q^n$$

Suppose that χ is a Dirichlet character mod m. The Gauss sums are defined by

$$\tau(n, \chi) := \sum_{a \mod m} \chi(a) \cdot e^{2\pi i n a/m}$$
$$\tau(\chi) := \tau(1, \chi)$$

Proposition 1.2.7. *We have*

$$\tau(n, \chi) = \overline{\chi}(n) \cdot \tau(\chi)$$

for all $n \in \mathbb{Z}$, *if* χ *is primitive mod* m, *and for* $(n, m) = 1$, *if* χ *is any character mod* m.

Conversely, if $\tau(n, \chi) = \overline{\chi}(n) \cdot \tau(\chi)$ *for all* $n \in \mathbb{Z}$ *then* χ *is primitive mod* m, *and in that case*

$$|\tau(\chi)|^2 = \chi(-1)\tau(\chi)\tau(\overline{\chi}) = m$$

We can decompose the twisting of f by χ in terms of f with change of variable by the following lemma.

Proposition 1.2.8. *(Birch's lemma) If* χ *is primitive mod* m, *then*

$$f_{\overline{\chi}}(z) = \frac{1}{\tau(\chi)} \sum_{a \mod m} \chi(a) \cdot f\left(z + \frac{a}{m}\right)$$

Proof. Note that $\tau(\chi) \neq 0$ and $\overline{\chi}(n) = \dfrac{\tau(n, \chi)}{\tau(\chi)}$ we get

$$f_{\overline{\chi}} = \sum_{n\geq 1} \overline{\chi(n)} a_n q^n = \sum_{n\geq 1} \frac{\tau(n, \psi)}{\tau(\psi)} a_n q^n$$

$$= \frac{1}{\tau(\chi)} \sum_{n\geq 1} \sum_{a \bmod m} \psi(a) e^{2\pi i n a/m} a_n e^{2\pi i n z}$$
$$= \frac{1}{\tau(\chi)} \sum_{a \bmod m} \psi(a) \sum_{n\geq 1} a_n e^{2\pi i n(z+a/m)}$$
$$= \frac{1}{\tau(\chi)} \sum_{a \bmod m} \chi(a) f\left(z + \frac{a}{m}\right)$$

□

This gives us the twisting rule for modular integral. If χ is primitive mod m we get

$$\Phi(f_{\overline{\chi}}, P, r) = \frac{1}{\tau(\chi)} \sum_{a \bmod m} \chi(a) \cdot \Phi\left(f\Big|\begin{pmatrix} 1 & a/m \\ 1 & 1 \end{pmatrix}, P, r\right)$$
$$= \frac{1}{\tau(\chi)} \sum_{a \bmod m} \chi(a) \cdot \Phi\left(f, P\Big|\begin{pmatrix} 1 & -a/m \\ 1 & 1 \end{pmatrix}, r + \frac{a}{m}\right)$$

Corollary 1.2.9. *Suppose χ is a primitive Dirichlet character mod m. For the modular symbol λ we have*

$$\lambda\left(f_{\overline{\chi}}, P(mz), b, n\right) = \frac{1}{\tau(\chi)} \sum_{a \bmod m} \chi(a) \lambda(f, P, mb - na, mn)$$

In particular, putting $b = 0$, $n = 1$ we obtain, for $0 \leq n \leq k-2$

$$L(f_{\overline{\chi}}, n+1) = \frac{1}{n!} \frac{(-2\pi i)^n}{m^{n+1}} \cdot \tau(\overline{\chi}) \cdot \sum_{a \bmod m} \chi(a) \lambda(f, z^n, a, m)$$

1.3 p-adic Distribution

Definition 1.3.1. Let X be any open compact subset of $\mathbb{Q}_p$, a p-adic distribution μ on X is defined to be an additive map from the collection of open compact subsets in X to $\mathbb{Q}_p$. That is

$$\mu\left(\bigcup_{k=1}^{n} U_k\right) = \sum_{k=1}^{n} \mu(U_k)$$

where $n \geq 1$ and $\{U_1, ..., U_n\}$ is any finite collection of pairwise disjoint compact open subsets of X.

Recall that $\mathbb{Q}_p$ has a topological basis of the form $D(a,n) = a + p^n\mathbb{Z}_p$, where $a \in \mathbb{Q}_p$ and $n \in \mathbb{N}$. It is remarkable since $D(a,n)$ are open compact sets. Any open compact subset U of $\mathbb{Q}_p$ hence can be written as a finite disjoint union of this kind of sets

$$U = \bigcup_{j=1}^{k} \left(a_j + p^N\mathbb{Z}_p\right)$$

for some $N \in \mathbb{N}$ and $a_1, .., a_k \in \mathbb{Q}_p$. In particular, every p-adic ball $a + p^n\mathbb{Z}_p$ can be represented as

$$a + p^n\mathbb{Z}_p = \bigcup_{b=0}^{p-1} \left(a + bp^n + p^{n+1}\mathbb{Z}_p\right)$$

This is a disjoint union since these smaller balls intersect if and only if one is contained in the other.

Now we can interpret the additivity condition into a more precise way called distribution property.

Proposition 1.3.2. *Let X be any open compact subset of $\mathbb{Q}_p$. Every map μ on open compact sets of the form $a + p^n\mathbb{Z}_p$ extends to a p-adic distribution if and only if*

$$\mu(a + p^n\mathbb{Z}_p) = \sum_{b=0}^{p-1} \mu\left(a + bp^n + p^{n+1}\mathbb{Z}_p\right)$$

More generally, we can consider the "twisting" p-adic space associated to a character χ of conductor M. Precisely, let $M > 0$ be a fixed integer and prime to p. Set

$$X = \mathbb{Z}_{p,M} = \varprojlim_v (\mathbb{Z}/p^vM\mathbb{Z}) = \mathbb{Z}_p \times (\mathbb{Z}/M\mathbb{Z})$$

$$X^* = \mathbb{Z}^*_{p,M} = \varprojlim_v (\mathbb{Z}/p^vM\mathbb{Z})^* = \mathbb{Z}^*_p \times (\mathbb{Z}/M\mathbb{Z})^*$$

In the same fashion, let denote

$$D(a,n) := a + p^nM\mathbb{Z}_{p,M}$$

with $(a, pM) = 1$ and $n \in \mathbb{N}$. We can view $\mathbb{Z}^*_{p,M}$ as a p-adic analytic Lie group with a fundamental system of neighborhoods of the form $D(a,n)$. A function μ on open compact sets of the form $a + p^nM\mathbb{Z}_p$ extends to a p-adic distribution if and only if the additivity is verified for the disjoint unions $a + p^nM\mathbb{Z}_p = \cup b + p^{n+1}M\mathbb{Z}_p$ with the union taken over the p values of b, $0 \leq b < p^{N+1}M$, for which $b \equiv a \mod p^nM$.

We are now ready to define a distribution attached to a cusp form. Suppose that $f \in S_k(\Gamma_0(N), \epsilon)$ is an eigenform for T_p with eigenvalue a_p. Suppose that the characteristic polynomial of Frobenius of f

$$X^2 - a_p X + \epsilon(p)p^{k-1}$$

has a non-zero root. Choose such a root $\alpha \neq 0$.

Definition 1.3.3. Let $v(m) = \mathrm{ord}_p(m)$ be the order of m, we define

$$\mu_{f,\alpha}(P, a, m) = \frac{1}{\alpha^{v(m)}}\lambda_{f,P}(a, m) - \frac{\epsilon(p)p^{k-2}}{\alpha^{v(m)+1}}\lambda_{f,P}(a, m/p)$$

for $a, m \in \mathbb{Z}$, $m > 0$.

It is natural to investigate the action of Hecke operators on modular symbols. Recall that

$$f|T_p := p^{k/2-1}\left(\sum_u^{p-1} f\left|\begin{pmatrix}1 & u\\ 0 & p\end{pmatrix} + \epsilon(p)\cdot f\right|\begin{pmatrix}p & 0\\ 0 & 1\end{pmatrix}\right)$$

Proposition 1.3.4. *For $f \in S_k(\Gamma_0(N), \epsilon)$ and for any prime number p we have the formula*

$$\lambda(f|T_p, P, a, m) = \sum_{u=0}^{p-1} \lambda(f, P, a - um, lm) + \chi(p)p^{k-2}\cdot\lambda(f, P, a, m/p)$$

Proof. By definition we have

$$\begin{aligned}
\lambda(f|T_p, P, a, m) &= p^{k/2-1}\left(\sum_u^{p-1}\lambda\left(f\left|\begin{pmatrix}1 & u\\ 0 & p\end{pmatrix}, P, a, m\right.\right) + \epsilon(p)\cdot\lambda\left(f\left|\begin{pmatrix}p & 0\\ 0 & 1\end{pmatrix}, P, a, m\right.\right)\right)\\
&= (pm)^{k/2-1}\sum_{u=0}^{p-1}\Phi\left(f\left|\begin{pmatrix}1 & u\\ 0 & p\end{pmatrix}\begin{pmatrix}1 & -a\\ 0 & m\end{pmatrix}P, 0\right.\right)\\
&+ (pm)^{k/2-1}\epsilon(p)\Phi\left(f\left|\begin{pmatrix}p & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & -a\\ 0 & m\end{pmatrix}, P, 0\right.\right)\\
&= (pm)^{k/2-1}\sum_{u=0}^{p-1}\Phi\left(f\left|\begin{pmatrix}1 & -a+um\\ 0 & mp\end{pmatrix}, P, 0\right.\right)
\end{aligned}$$

$$
\begin{aligned}
&+ (pm)^{k/2-1}\epsilon(p)\Phi\left(f\middle|\begin{pmatrix} p & -ap \\ 0 & m \end{pmatrix}, P, 0\right) \\
&= \sum_{u=0}^{p-1} \Phi\left(f, P, a-um, pm\right) + (pm)^{k/2-1}\epsilon(p)\Phi\left(f\middle|\begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}\begin{pmatrix} 1 & -a \\ 0 & m/p \end{pmatrix}, P, 0\right) \\
&= \sum_{u=0}^{p-1} \Phi\left(f, P, a-um, pm\right) + p^{k/2-1}\epsilon(p)\Phi\left(f\middle|\begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}, P, a, \frac{m}{p}\right) \\
&= \sum_{u=0}^{p-1} \lambda\left(f, P, a-um, lm\right) + \epsilon(p)p^{k-1}\cdot\lambda\left(f, P, a, m/p\right)
\end{aligned}
$$

□

Applying this formula we have the distribution property for $\mu_{f,\alpha}$.

Proposition 1.3.5. *For $a, m \in \mathbb{Z}$, $m > 0$ we have*

$$\sum_{\substack{b \equiv a \mod m \\ b \mod pm}} \mu_{f,\alpha}(P, b, pm) = \mu_{f,\alpha}(P, a, m)$$

Proof. By definition we have

$$
\begin{aligned}
\sum \mu_{f,\alpha}(P, b, pm) &= \sum_{u \mod p} \mu_{f,\alpha}(P, a-um, pm) \\
&= \sum_{u \mod p} \left[\frac{1}{\alpha^{v(pm)}}\lambda_{f,P}(a-um, pm) - \frac{\epsilon(p)p^{k-2}}{\alpha^{v(pm)+1}}\lambda_{f,P}(a-um, m)\right]
\end{aligned}
$$

Since $\lambda_{f,P}(a, m)$ depends only upon $a \mod m$, we have $\lambda_{f,P}(a-um, m) = \lambda_{f,P}(a, m)$. Moreover, by Vieta theorem we get $\alpha\beta = \epsilon(p)p^{k-1}$. Hence

$$\sum_{u \mod p} \frac{\epsilon(p)p^{k-2}}{\alpha^{v(pm)+1}}\lambda_{f,P}(a-um, m) = \frac{\beta}{\alpha^{v(m)+1}}\lambda_{f,P}(a, m)$$

Using the action formula of the Hecke operator we have

$$
\begin{aligned}
\sum_{u \mod p} \lambda_{f,P}(a-um, pm) &= \lambda(f|T_p, P, a, m) - \epsilon(p)p^{k-1}\lambda(f, P, a, m/p) \\
&= a_p\lambda(f, P, a, m) - \epsilon(p)p^{k-2}\lambda(f, P, a, m/p)
\end{aligned}
$$

Not that $a_p - \beta = \alpha$, we obtain

$$\begin{aligned}\sum \mu_{f,\alpha}(P, b, pm) &= \frac{a_p}{\alpha^{v(m)+1}}\lambda_{f,P}(a, m) - \frac{\epsilon(p)p^{k-1}}{\alpha^{v(m)+1}}\lambda_{f,P}(a, m/p) - \frac{\beta}{\alpha^{v(m)+1}}\lambda_{f,P}(a, m) \\ &= \frac{1}{\alpha^{v(m)}}\lambda_{f,P}(a, m) - \frac{\epsilon(p)p^{k-2}}{\alpha^{v(m)+1}}\lambda_{f,P}(a, m/p) \\ &= \mu_{f,\alpha}(P, a, m)\end{aligned}$$

□

For $x \in \mathbb{Z}_{p,M}$, we denote by x_p the projection of x in $\mathbb{Z}_p$.

Definition 1.3.6. Let $U \subset \mathbb{Z}_{p,M}$ be an open subset, a function $F : U \to \mathbb{C}_p$ is called locally analytic if there is a covering of U by disks $D(a, v)$ such that on each $D(a, v)$, F is given by the convergent power series

$$F(x) = \sum_{n\geq 0} c_n(x - a)_p^n$$

Assume that $v(a) < k-1$, Vishik [Vi76] and Amice-Velu [AV75] defined an integration

$$(U, F) \mapsto \int_U F d\mu_{f,\alpha} \in \mathbb{C}_p$$

for a compact open subset U of $\mathbb{Z}_{p,M}^\times$ and a locally analytic function F on U.

Theorem 1.3.7. *Fix an integer h such that $1 \leq h \leq k-1$. Suppose the polynomial $X^2 - a_pX + \epsilon(p)p^{k-1}$ has a root $\alpha \in \mathbb{C}_p$ such that $\operatorname{ord}_p \alpha < h$. Fix such an α. Then there exists a unique $\mathbb{C}_p$-valued integral satisfying these axioms, in which $v \geq 1$, $a \in \mathbb{Z}$ throughout*

1. *It is $\mathbb{C}_p$-linear in F and finitely additive in U.*
2. *For $0 \leq j < h$*

$$\int_{D(a,v)} x_p^j d\mu_{f,\alpha} = \mu_{f,\alpha}(z^j, a, p^v M)$$

3. *For any $n \geq 0$*

$$\int_{D(a,v)} (x - a)_p^n d\mu_{f,\alpha} \in \left(\frac{p^n}{\alpha}\right)^v \alpha^{-1}\Omega_f$$

4. If $F(x) = \sum_{n\geq 0} c_n (x-a)_p^n$ *is convergent on the disk* $D(a,v)$*, then*

$$\int_{D(a,v)} F = \sum_{n\geq 0} c_n \int_{D(a,v)} (x-a)_p^n d\mu_{f,\alpha}$$

Proof. Refer [MTT] □

Definition 1.3.8. If α is a root of $X^2 - a_p X + \epsilon(p)p^{k-1}$ such that $\mathrm{ord}_p\, \alpha < k-1$, we call α an allowable p-root for f.

1.4 One Variable p-adic L-function

Definition 1.4.1. A p-adic character is a continuous homomorphism

$$\chi : \mathbb{Z}_{p,M}^* \to \mathbb{C}_p^*$$

for some p prime and $M \in \mathbb{Z}_{>0}$, $(p, M) = 1$.

If $M_1 | M$, then $\mathbb{Z}_{p,M_1}^\times$ is a quotient of $\mathbb{Z}_{p,M}^\times$, and we can deduce characters of $\mathbb{Z}_{p,M_1}^\times$ with certain characters of $\mathbb{Z}_{p,M}^\times$. We say that a character χ as above is primitive on $\mathbb{Z}_{p,M}^\times$ if it does not factor through $\mathbb{Z}_{p,M_1}^\times$ for any proper divisor M_1 of M.

For each p-adic character χ there is a unique M such that χ is primitive on $\mathbb{Z}_{p,M}^\times$. We call this M the p'-conductor of χ; it is an integer ≥ 1, prime to p.

If $p > 2$, we have $\mathbb{Z}_p^* = \mu_{p-1} \times (1 + p\mathbb{Z}_p)$. Hence, every $x \in \mathbb{Z}_p^*$ we can write, uniquely,

$$x = \omega(x)\, \langle x \rangle$$

with $\omega(x) \in \mu_{p-1}$ and $\langle x \rangle \in 1 + p\mathbb{Z}_p$. We have $x \mapsto \omega(x)$ and $x \mapsto \langle x \rangle$ are p-adic characters of p'-conductor 1.

Definition 1.4.2. Let $f \in S_k(\Gamma_0(N), \epsilon)$ is an eigenform for T_p with eigenvalue a_p. Suppose that the characteristic polynomial of the Frobenius of f

$$X^2 - a_p X + \epsilon(p)p^{k-1}$$

has a non-zero root. Suppose that α is an allowable p-root for f. For each p-adic character χ we define

$$L_p(f, \alpha, \chi) = \int_{\mathbb{Z}_{p,M}^*} \chi d\mu_{f,\alpha}$$

where M is the p-conductor of χ, and where the integral is that defined in the theorem of Vishik.

Definition 1.4.3. For $s \in \mathbb{Z}_p$, define

$$\chi_s(x) := \langle x \rangle^s = \exp(s \log x) = \sum_{r=0}^{\infty} \frac{s^r}{r!} (\log \langle x \rangle)^r$$

The p-adic L-function associated to α given by

$$L_p(f, \alpha, s) = \int_{\mathbb{Z}_p^*} \langle x \rangle^{s-1} \, d\mu_{f,\alpha}$$

The p-adic L-function associated to α twisted by ψ is defined to be

$$L_p(f, \alpha, \psi\chi_{s-1}) = \int_{\mathbb{Z}_{p,M}^\times} \psi(x) \cdot \langle x \rangle^{s-1} \, d\mu_{f,\alpha}$$

Definition 1.4.4. Let ψ be a p-adic character of conductor $m = p^v M$. We define the p-adic multiplier

$$e_p(\alpha, \psi) := \frac{1}{\alpha^v} \left(1 - \frac{\bar{\psi}(p)\epsilon(p)p^{k-2}}{\alpha}\right) \left(1 - \frac{\psi(p)}{\alpha}\right)$$

here $\overline{\psi}$ is the conjugate character to ψ.

Theorem 1.4.5. *Let ψ be a p-adic character of conductor $m = p^v M$, then*

$$L_p(f, \alpha, \psi) = e_p(\alpha, \psi) \cdot \frac{m}{\tau(\bar{\psi})} \cdot L(f_{\bar{\psi}}, 1)$$

where $f_{\overline{\psi}}(z) = \sum_{n \geq 1} \psi(n) a_n e^{2\pi i n z}$ a twisting of f by ψ and $\tau(\psi) = \sum_{a \bmod m} \psi(a) \cdot e^{2\pi i a/m}$ the Gauss sum associated to ψ.

In particular, for the trivial character $\psi = \mathbf{1}$, we obtain

$$L_p(f, \alpha, \mathbf{1}) = \left(1 - \frac{\epsilon(p)p^{k-2}}{\alpha}\right) \left(1 - \frac{1}{\alpha}\right) \cdot L(f, 1)$$

Proof. **Case 1**: $v > 0$

It follows that $p|m$, so $\psi(p) = 0$ and $e_p(\alpha, \psi) = \dfrac{1}{\alpha^v}$. By the property of the integral we have

$$L_p(f, \alpha, \psi) = \int_{\mathbb{Z}_{p,M}^\times} \chi d\mu_{f,\alpha} \overset{def}{=} \int_{\mathbb{Z}_{p,M}} \psi(x) d\mu_{f,\alpha}$$

$$= \sum_{a \mod p^v M} \psi(a) \cdot \mu_{f,\alpha}(1, a, p^v M)$$
$$= \sum_{a \mod p^v M} \psi(a) \left[\frac{1}{\alpha^v} \lambda(f, 1, a, p^v M) - \frac{\epsilon(p) p^{k-2}}{\alpha^{v+1}} \lambda(f, 1, a, p^{v-1}) \right]$$

By the distribution property we have

$$\sum_{a \mod p^v M} \psi(a) \lambda(f, 1, a, p^{v-1}) = \sum_{b \mod p^{v-1} M} \left(\sum_{\substack{a \equiv b \mod p^{v-1} M \\ a \mod p^v M}} \psi(a) \right) \lambda(f, 1, b, p^{v-1} M)$$

We have the following well-known lemma

Lemma 1.4.6. *Let ψ be a character of conductor m. For $n|m$ we have*

$$\sum_{\substack{a \mod m \\ a \equiv b \mod n}} \psi(a) = 0$$

for every b modulo n.

Hence $\sum_{\substack{a \equiv b \mod p^{v-1} M \\ a \mod p^v M}} \psi(a) = 0$ and we get

$$L_p(f, \alpha, \psi) = \frac{1}{\alpha^v} \sum_{a \mod p^v M} \psi(a) \lambda(f, 1, a, p^v M) = \frac{1}{\alpha^v} \frac{m}{\tau(\bar{\psi})} \cdot L(f_{\bar{\psi}}, 1)$$

Case 2: $v = 0$

If $(a, M) = 1$, set $D(a, 0) = \mathbb{Z}_{p,M}^{\times} \cap (a + M\mathbb{Z}_{p,M})$. Then we have

$$D(a, 0) = \bigsqcup_{\substack{b \equiv a \mod M \\ b \neq 0 \mod p \\ b \mod pM}} D(b, 1)$$

Note that if $b \equiv a \mod M$ and $b \equiv 0 \mod p$, then $b \equiv pap' \mod pM$ with $pp' \equiv 1 \mod M$. Hence we get

$$\int_{D(a,0)} \psi d\mu_{f,\alpha} = \psi d\mu_{f,\alpha} = \sum_{\substack{b \equiv a \mod M \\ b \neq 0 \mod p \\ b \mod pM}} \psi(b) \mu_{f,\alpha}(1, b, pM)$$

$$= \left[\sum_{\substack{b \equiv a \mod m \\ b \mod pm}} \psi(b)\mu_{f,\alpha}(1, b, pm) \right] - \psi(pap')\mu_{f,\alpha}(1, pap', pm)$$

Note that $\psi(b) = \psi(a) = \psi(pap')$ and by the distribution property we obtain

$$\begin{aligned}
\int_{D(a,0)} \psi d\mu_{f,\alpha} &= \psi(a)\mu_{f,\alpha}(1, a, m) - \psi(a)\mu_{f,\alpha}(1, pap', pm) \\
&= \psi(a) \left(\lambda_{f,1}(a, M) - \frac{\epsilon(p)p^{k-2}}{\alpha} \lambda_{f,1}(a, M/p) \right. \\
&\qquad \left. -\frac{1}{\alpha}\lambda_{f,1}(pap', pM) + \frac{\epsilon(p)p^{k-2}}{\alpha^2}\lambda_{f,1}(pap', M) \right) \\
&= \psi(a) \left(\lambda_{f,1}(a, M) - \frac{\epsilon(p)p^{k-2}}{\alpha} \lambda_{f,1}(pa, M) \right. \\
&\qquad \left. -\frac{1}{\alpha}\lambda_{f,1}(ap', M) + \frac{\epsilon(p)p^{k-2}}{\alpha^2}\lambda_{f,1}(a, M) \right)
\end{aligned}$$

Summing up a modulo m we get

$$\begin{aligned}
L_p(f, \alpha, \psi) &= \sum_{a \mod m} \int_{D(a,0)} \psi d\mu_{f,\alpha} \\
&= \sum_{a \mod m} \psi(a) \left(\lambda_{f,1}(a, M) - \frac{\epsilon(p)p^{k-2}}{\alpha} \lambda_{f,1}(pa, M) \right. \\
&\qquad \left. -\frac{1}{\alpha}\lambda_{f,1}(ap', M) + \frac{\epsilon(p)p^{k-2}}{\alpha^2}\lambda_{f,1}(a, M) \right) \\
&= \frac{m}{\tau(\chi)} L(f_{\overline{\psi}}, 1) \left(1 - \frac{\overline{\psi}(p)\epsilon(p)p^{k-2}}{\alpha} - \frac{\psi(p)}{\alpha} + \frac{\epsilon(p)p^{k-2}}{\alpha^2} \right) \\
&= \left(1 - \frac{\bar{\psi}(p)\epsilon(p)p^{k-2}}{\alpha} \right) \left(1 - \frac{\psi(p)}{\alpha} \right) \frac{m}{\tau(\chi)} L(f_{\overline{\psi}}, 1)
\end{aligned}$$

□

Theorem 1.4.7. *Let E be an elliptic curve over $\mathbb{Q}$ and let $f \in S_2^{new}(\Gamma_0(N))$ be a newform attached to E. Then the p-adic multiplier $e_p(\alpha, \psi)$ of f vanishes if and only if E has multiplicative reduction at p, and $\psi(p) = a_p$*

Proof. Since $k = 2$, the p-adic multiplier has the form

$$e_p(\alpha, \chi) := \frac{1}{\alpha^v}\left(1 - \frac{\bar{\psi}(p)\epsilon(p)}{\alpha}\right)\left(1 - \frac{\psi(p)}{\alpha}\right)$$

Let α and β be the roots of Frobenius associated to f

$$X^2 - a_p X + \epsilon(p)p$$

Then $\alpha + \beta = a_p$ and $\alpha\beta = \epsilon(p)p$. By the definition of $e_p(\alpha, \psi)$, it is vanishes if and only if $\alpha = \psi(p)$ or $\alpha = \overline{\psi(p)}\epsilon(p)$.In cases, we have

$$a_p = \alpha + \beta = \begin{cases} \psi(p) + \overline{\psi(p)}\epsilon(p)p & \text{if } \alpha = \psi(p) \\ \overline{\psi(p)}\epsilon(p) + \psi(p)p & \text{if } \alpha = \overline{\psi(p)}\epsilon(p) \end{cases}$$

Since $\alpha \neq 0$, we see that $\psi(p) \neq 0$ and $|\psi(p)| = 1$. If $\epsilon(p) \neq 0$, it follows that $|a_p| \geq p - 1$ by triangle inequality. On the other hand, by Hasse's theorem we obtain

$$p - 1 \leq |a_p| \leq 2\sqrt{p}$$

which contradicts the assumption $p \geq 5$. Hence $\epsilon(p) = 0$, so $a_p = \psi(p)$ or $a_p = \psi(p)p$. Again, by Hasse's theorem, we excludes the latter case. Thus $a_p = \psi(p) = \pm 1$, since $\psi(p)$ is a root of unity, and a_p is an integer. It follows from $a_p = \pm 1$ that E has multiplicative reduction modulo p. □

1.5 The Main Theorem

1.5.1 Tate's p-adic Uniformization

Recall that every elliptic curve E over $\mathbb{C}$ has the form

$$E(\mathbb{C}) \simeq \mathbb{C}^\times / q^{\mathbb{Z}}$$

with $|q| < 1$. We also get the analogue result for elliptic curves over p-adic fields due to J.Tate.

Theorem 1.5.1. *(Tate curve) Let K be a p-adic field,i.e., a finite extension $K/\mathbb{Q}_p$ with absolute value $|\cdot|$, let $q \in K^*$ satisfy $|q| < 1$, and let*

$$s_k(q) = \sum_{n \geq 1} \frac{n^k q^n}{1 - q^n}, \quad a_4(q) = -5s_3(q), \quad a_6(q) = -\frac{5s_3(q) + 7s_5(q)}{12}$$

1. *The series $a_4(q)$ and $a_6(q)$ converge in K. Define the Tate curve E_q by the equation*

$$E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q)$$

2. *The Tate curve is an elliptic curve defined over K with discriminant*

$$\Delta = q\prod_{n\geq 1}(1-q^n)^2 4$$

and j-invariant

$$j(E_q) = \frac{1}{q} + 744 + 196884q + \cdots = \frac{1}{q} + \sum_{n\geq 0} c(n)q^n \in \frac{1}{q} + \mathbb{Z}[[q]]$$

where $c(n)$'s are the integers.

3. *The series*

$$X(u,q) = \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} - 2s_1(q),$$
$$Y(u,q) = \sum_{n\in\mathbb{Z}} \frac{(q^n u)^2}{(1-q^n u)^3} + s_1(q)$$

converge for all $u \in \overline{K}$, $u \notin q^{\mathbb{Z}}$. They define a surjective homomorphism

$$\phi : \overline{K}^* \to E_q(\overline{K})$$
$$u \mapsto \begin{cases} (X(u,q), Y(u,q)) & \text{if } u \notin q^{\mathbb{Z}}, \\ O & \text{if } u \in q^{\mathbb{Z}} \end{cases}$$

The kernel of ϕ is $q^{\mathbb{Z}}$.

4. *The map ϕ in (c) is compatible with the action of the Galois group $G_{\overline{K}/K}$ in the sense that*

$$\phi(u^\sigma) = \phi(u)^\sigma \quad \forall u \in \overline{K}^*, \sigma \in G_{\overline{K}/K}$$

In particular, for any algebraic extension L/K, ϕ induces an isomorphism

$$\phi : L^*/q^{\mathbb{Z}} \xrightarrow{\sim} E_q(L)$$

Proof. Refer [Sil94], chapter V, theorem 3.1. □

Before giving the p-adic uniformization theorem, we describe an invariant γ of elliptic curves.

Lemma 1.5.2. *Let E/K be an elliptic curve defined over a field of characteristic not equal to 2 or 3, and choose a Weierstrass equation*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

for E/K. Let c_4 and c_6 be the usual quantities associated to this equation. Assume that $j(E) \neq 0, 1728$, we define

$$\gamma(E/K) = -c_4/c_6 \in K^\times/(K^\times)^2$$

Then $\gamma(E/K)$ is well-defined as an element of $K^\times/(K^\times)^2$, independent of the choice of Weierstrass equation for E/K.

Let E'/K be another elliptic curve with $j(E') = j(E) \neq 0, 1728$. Then E and E' are isomorphic over K if and only if

$$j(E) = j(E') \text{ and } \gamma(E/K) = \gamma(E'/K)$$

Proof. Refer [Sil94], chapter V, lemma 5.2. □

Theorem 1.5.3. *(Tate period) Let K be a p-adic field, let E/K be an elliptic curve with $|j(E)| = \left|\frac{1}{q}\right| > 1$, and let $\gamma(E/K) \in K^*/K^{*^2}$ be the invariant defined by lemma 1.5.2*

a There is a unique $q \in \overline{K}^*$ with $|q| < 1$ such that E is isomorphic over $\overline{K}$ to the Tate curve E. Further, this value of q lies in K.

b Let q be chosen as in (a). Then the following three conditions are equivalent

(a) E is isomorphic to E_q over K.

(b) $\gamma(E/K) = 1$

(c) E has split multiplicative reduction.

Proof. Refer [Sil94], chapter V theorem 5.3. □

Suppose that $E/\mathbb{Q}_p$ has the split reduction at p, then we have the isomorphism

$$E(\overline{\mathbb{Q}_p}) \simeq \overline{\mathbb{Q}_p}^\times/q_E^{\mathbb{Z}}$$

1.5.2 The Mazur-Tate-Teitelbaum Conjecture

Recall the q-expansion of the elliptic modular function j given by

$$j = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots = q^{-1} + \sum_{n=0}^{\infty} A_n q^n.$$

Inverting the formula we obtain

$$q = q(j) = \sum_{n=1}^{\infty} B_n j^{-n}.$$

Let K be a finite extension of $\mathbb{Q}_p$, and let E/K with non-integral j-invariant $j(E)$. Evaluating $q(E) = q(j(E))$, the multiplicative period of E, we obtain

$$v_p(q(E)) = -v_p(j(E)) > 0$$

Definition 1.5.4. Let $\lambda : K^* \to \mathbb{Q}_p$ be a continuous homomorphism. We set

$$\mathcal{L}_\lambda(E) := \frac{\lambda(q(E))}{v_p(q(E))} \in \mathbb{Q}_p$$

Definition 1.5.5. Define the p-adic logarithm by the power series

$$\log_p(1+x) = \sum_{n\geq 1} (-1)^{n+1} \frac{x^n}{n}$$

This series is converges on the set $1 + p\mathbb{Z}_p = \{x \in \mathbb{Q}_p || x-1|_p < 1\}$. Recall that $\mathbb{Z}_p^\times \simeq \mu_{p-1} \times (1 + p\mathbb{Z}_p)$, let $\log_p(\xi) = 0$ for all $\xi \in \mu_{p-1}$.

One can extend its domain to $\mathbb{Q}_p^\times$ by defining $\log_p(p) = 0$. That is, for any $x \in \mathbb{Q}_p^\times$, then x can be uniquely written as the form $x = up^n$ with $u \in \mathbb{Z}_p^\times$, then $\log(x) := \log(u)$

We denote by $N_{K/\mathbb{Q}_p}$ the norm map. If λ is the composition

$$K^\times \overset{N_{K/Q_p}}{\longrightarrow} \mathbb{Q}_p^\times \overset{log_p}{\longrightarrow} \mathbb{Q}_p$$

then we call $\mathcal{L}_\lambda(E)$ the $\mathcal{L}$-invariant of E and denote it by $\mathcal{L}_p(E)$.

The $\mathcal{L}$-invariant $\mathcal{L}_\lambda(E)$ is an isogeny-invariant of E, and is linear in λ. We have the following conjecture.

Conjecture: If $j(E)$ is algebraic, the $\mathcal{L}_p(E)$ does not vanish.

The main result of my thesis is the following due to Greenberg and Stevens (refer [GS94], [GS93]).

Theorem 1.5.6. *Let E be an elliptic curve over $\mathbb{Q}$ with split multiplicative reduction at the prime $p \geq 5$. Let $L_\infty(E, z)$ be the Hasse-Weil L-function of $E/\mathbb{Q}$, and let $L_p(E, s)$ be the associated p-adic L-fucntion. Then*

$$\frac{d}{ds} L_p(E, s)\bigg|_{s=1} = \mathcal{L}_p(E) \cdot \frac{L_\infty(E, 1)}{\Omega_E}$$

Here Ω_E is the Neron period of E.

CHAPTER 2

Hida's Theory

The main technique in the proof of Greenberg and Stevens (refer [GS94], [GS93]) is the theory of Hida which investigates the ordinary part of spaces of modular forms. I will also provide the basics of Λ-adic forms which can be seen as families of p-adic modular forms and their Galois representations.

2.1 Iwasawa's Algebra

This section provides basic background on Iwasawa's algebra which is often used throughout my thesis. The main reference for this topic is the notes of Yi Ouyang [Ou].

Definition 2.1.1. (Completed group ring) Let G be a profinite group. The completed group ring of G over $\mathbb{Z}_p$ is

$$\mathbb{Z}_p[[G]] := \varprojlim_N [G/N]$$

where N runs over all finte-index subgroups of G and $\mathbb{Z}_p[G/N]$ is the usual group ring of G/N over $\mathbb{Z}_p$.

The group ring $\mathbb{Z}_p[[G]]$ is a topological ring and every continuous group homomorphism $G \to \overline{\mathbb{Q}}_p^\times$ extends by linearity to a continuous ring homomorphism $\mathbb{Z}_p[[G]] \to \overline{\mathbb{Q}}_p^\times$.

Definition 2.1.2. The augmentation ideal I_G of $\mathbb{Z}_p[G]$ is

$$\ker\left(\mathbb{Z}_p[[G]] \xrightarrow{\epsilon} \mathbb{Z}_p\right)$$

where ϵ is the inverse limit of the $\mathbb{Z}_p$-linear maps $\mathbb{Z}_p[G/N] \to \mathbb{Z}_p$ that takes every group element to 1.

The map ϵ is surjective, and therefore it induces an isomorphism

$$\mathbb{Z}_p[[G]]/I_G \simeq \mathbb{Z}_p$$

Definition 2.1.3. We define the Iwasawa algebra to be the ring of formal power series $\mathbb{Z}_p[[T]]$ with variable T over $\mathbb{Z}_p$. Let v_p be the usual p-adic valuation on $\mathbb{Z}_p$. For $f(T) = \sum_{n\geq 0} a_n T^n \in \mathbb{Z}_p[[T]]$ define the μ-invariant of f to be the least power of p dividing all the coefficients

$$\mu(f) := \min_n v_p(a_n)$$

And the λ-invariant of f is the first coefficient at which the minimum occurs

$$\lambda(f) := \min\{n : v_p(a_n) = \mu(f)\}$$

Theorem 2.1.4. *(Division algorithm for $\mathbb{Z}_p[[T]]$). Let $f(T) \in \mathbb{Z}_p[[T]]$ be non-zero with $\mu(f) = 0$. Let $g(T) \in \mathbb{Z}_p[[T]]$, then there exists unique $q(T) \in \mathbb{Z}_p[[T]]$ and a polynomial $r(T) \in \mathbb{Z}_p[T]$ of degree $< \lambda(f)$ such that*

$$g = fq + r$$

Definition 2.1.5. A polynomial $P(T) \in \mathbb{Z}_p[T]$ is called a distinguished polynomial if it has the form

$$P(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0$$

with $a_i \in p\mathbb{Z}_p$.

Theorem 2.1.6. *(p-adic Weierstrass preparation theorem). Let $f(T) \in \mathbb{Z}_p[[T]]^\times$ be a non-zero power series. Then, there is a unique factorization*

$$f(T) = p^{\mu(f)}P(T)u(T)$$

where $P(T)$ is a distinguished polynomial with the degree $\deg(P) = \lambda(f)$, and $u(T) \in \mathbb{Z}_p[[T]]^\times$.

Let G be a topological group isomorphic to the additive group $\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$. Note that as a profinite group, $\mathbb{Z}_p$ is compact and procyclic, i.e. $\mathbb{Z}_p$ is the closure of the cyclic

subgroup $\langle 1 \rangle$. Let γ be any generator of G, i.e., $G = \overline{\langle \gamma \rangle}$ and $G_n = \overline{\langle \gamma^{p^n} \rangle}$ be the unique closed subgroup of index p^n of G. Then G/G_n is cyclic of order p^n generated by $\gamma + G_n$. One has an isomorphism

$$\mathbb{Z}_p[G/G_n] \xrightarrow{\sim} \mathbb{Z}_p[T]/\Big((1+T)^{p^n} - 1\Big)$$
$$\gamma \mod G_n \mapsto (1+T) \mod (1+T)^{p^n} - 1$$

Moreover, if $m \geq n \geq 0$, the natural map $G/G_m \to G/G_n$ induces a natural map $\phi_{m,n} : \mathbb{Z}_p[G/G_m] \to \mathbb{Z}_p[G/G_n]$, which is compatible with the isomorphism. We hence obtain

$$\mathbb{Z}_p[G] = \varprojlim_n \mathbb{Z}_p[G/G_n] = \varprojlim_n \mathbb{Z}_p[T]/\Big((1+T)^{p^n} - 1\Big)$$

Theorem 2.1.7. *Let G be a topological group isomorphic to the additive group $\mathbb{Z}_p$ and let γ be any its generator. There is an isomorphism of topological rings induce by $\gamma - 1 \mapsto T$*

$$\mathbb{Z}_p[[G]] \simeq \mathbb{Z}_p[[T]]$$

Proof. For $n \geq 1$ let $\omega_n(T) = (1+T)^{p^n} - 1$. Then $\omega_n(T)$ is a distinguished polynomial. Furthermore,

$$\frac{\omega_{n+1}(T)}{\omega_n(T)} = (1+T)^{p^n(p-1)} + \cdots + (1+T)^{p^n} + 1 \in (p, T)$$

so $\omega_n(T) \in (p, T)^{n+1}$ for $n \geq 0$.

Hence, for every $n \geq 1$ we have a projection

$$\mathbb{Z}_p[[T]] \to \mathbb{Z}_p[[T]]/(\omega_n) \xrightarrow{\sim} \mathbb{Z}_p[T]/(\omega_n) \xrightarrow{\sim} \mathbb{Z}_p[\Gamma/\Gamma_n]$$

which is compatible with the transition map. By the universal property of projective limits, we obtain a continuous homomorphism

$$\epsilon : \mathbb{Z}_p[[T]] \to \mathbb{Z}_p[[\Gamma]],\ T \mapsto \gamma - 1$$

On the other hand $\ker \epsilon \subset \cap_n(\omega_n) \subset \cap_n(p, T)^{n+1} = 0$, thus ϵ is injective. Moreover, $\mathbb{Z}_[[T]]$ is compact, hence the image is closed, it is also dense since at every level the map is surjective. It follows that ϵ is surjective. □

It is noticable that this isomorphism depends on the choice of the topological generator γ of G.

Proposition 2.1.8. *(Nakayama's lemma) Let M be a compact Λ-module. Then the following are equivalent*

1. *M is finitely generated over Λ*
2. *M/TM is a finitely generated $\mathbb{Z}_p$-module*
3. *$M/(p,T)M$ is a finitely dimensional $\mathbb{F}_p$-vector space*

Proof. (1) $\Rightarrow$ (2) $\Rightarrow$ (3) are straightforward. Assuming (3), let $x_1, ..., x_n$ generate $M/(p,T)M$ as $\mathbb{F}_p$-vector space. Let $N = \Lambda x_0 + \cdots + \Lambda x_n \subseteq M$, then

$$M/N = \frac{N + (pT)M}{N} = (p,T)M/N$$

Thus $M/N = (p,T)^n M/N$ for all $n > 0$.

Consider a small neighborhood U of 0 in M/N. Since $(p,T)^n \to 0$ in Λ, for any $z \in M/N$, there exists a neighborhood U_z of z and some n_z such that $(p,T)^{n_z} U_z \subseteq U$. But M/N is compact, then $(p,T)^n M/N \subseteq U$ for n large, hence $M/N = \cap (p,T)^n M/N = 0$ and $M = N$ is finitely generated over Λ. □

2.2 Ordinary Subspace

Hida defined an idempotent of the Hecke algebra that projects spaces of modular forms to their ordinary parts [Hi93], which are maximal submodules on which U_p acts invertibly. Recall that

$$U_p^n = \sum_{b=0}^{p^n-1} \begin{pmatrix} 1 & b \\ 0 & p^n \end{pmatrix}$$

Definition 2.2.1. The element e_{ord} attached to U_p is given by

$$e_{ord} = \lim_{n \to \infty} U_p^{n!}$$

is an idempotent of Hecke algebra $\mathcal{H}(\Gamma_0(N), \mathbb{Z}_p)$.

Lemma 2.2.2. *Suppose $a \in \bar{\mathbb{Q}}_p$ is an algebraic integer. In $\mathbb{C}_p$ we have*

$$\lim_{n \to \infty} a^{n!} = \begin{cases} 1 & \text{if } a \in \bar{\mathbb{Q}}_p^\times \\ 0 & \text{otherwise} \end{cases}$$

Proof. If a is not a unit of $\overline{\mathbb{Q}_p}$, then it has positive p-adic valuation; thus the limit of $a^{n!}$ is 0. Suppose a is a unit contained in the ring of integers $\mathcal{O}_K$ of a finite extension K of $\mathbb{Q}_p$. Take a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ above $p\mathbb{Z}_p$. As a is a unit, we have

$$a^{|\mathcal{O}_K/\mathfrak{p}^k|-1} \equiv 1 \mod \mathfrak{p}^k$$

For n large enough, $|\mathcal{O}_K/\mathfrak{p}^k|-1$ divides $n!$, so taking limit $n \to \infty$ we have $\lim_{n\to\infty} a^{n!} = 1$. □

Remark 2.2.3. An eigenform of $\Gamma_0(N)$ is called ordinary at p if its U_p-eigenvalue is a p-adic unit, by the lemma we see that an eigenform f is preserved by e_{ord} if it is precisely ordinary, and otherwise e_{ord} maps f to 0.

Definition 2.2.4. The ordinary submodule of $S_k(\Gamma_0(N))$ is

$$S_k^{ord}(\Gamma_0(N)) := e_{ord} S_k(\Gamma_0(N))$$

Remark 2.2.5. If $p \nmid d$, then the diamond operators $\langle d\rangle$ and U_p commute on $S(\Gamma_0(N))$ for any positive integer N. Hence e_{ord} commutes with $\langle d\rangle$ for $p \nmid d$. Also, $\langle d\rangle U_p$ acts as p^{k-1} on $S(\Gamma_0(N))$.

Theorem 2.2.6. *We have the basis for* $S_k(\Gamma_0(N))$

$$\{f|\langle d\rangle : f \in S_k^{new}(\Gamma_0(N')),\ dN'|N\}$$

The following property gives us the action of e_{ord} on the elements of this basis

Proposition 2.2.7. *Suppose that d and N' are positive integers such that $dN'|N$, and suppose f is a newform of level N'. If $a_p(f)$ is not a p-adic unit, then*

$$e_{ord}(f|\langle d\rangle) = 0$$

If $a_p(f)$ is a p-adic unit, let α, β be the roots of Frobenius of f, that is, the root of the equation

$$x^2 - a_p(f)x + \chi_{N'}(p)p^{k-1} = 0$$

Assume that the roots are ordered so that α is a unit and β is a non-unit. Then

$$e_{ord}(f|\langle d\rangle) = \frac{\alpha}{\alpha-\beta}(f|\langle d\rangle - \beta p^{1-k}\cdot f|\langle pd\rangle)$$

for $(p,d) = 1$, and

$$e_{ord}(f|\langle d\rangle) = \frac{p^{k-1}}{\alpha-\beta}(f|\langle d/p\rangle - \beta p^{1-k}\cdot f|\langle d\rangle)$$

for $p|d$.

Proof. Without loss of generality, we can assume that $d = 1$ or $d = p$. Since f is a newform at level N', we have

$$\begin{aligned} f|\big(U_p + \chi_{N'}(p)\,\langle p\rangle\big) &= a_p f \\ \Leftrightarrow f|U_p &= a_p f - \chi_{N'}(p) f|\langle p\rangle \end{aligned}$$

Note that $\langle d\rangle\, U_p$ acts as p^{k-1}, we obtain

$$\begin{pmatrix} f & f|\langle p\rangle \end{pmatrix}\Big|U_p = \begin{pmatrix} f & f|\langle p\rangle \end{pmatrix}\begin{pmatrix} a_p & p^{k-1} \\ -\chi_{N'}(p) & 0 \end{pmatrix}$$

Let $A = \begin{pmatrix} a_p & p^{k-1} \\ -\chi_{N'}(p) & 0 \end{pmatrix}$.

Case 1: a_p is non-unit. Then all entries of A^2 has positive p-adic valuation. It follows that

$$\begin{pmatrix} f & f|\langle p\rangle \end{pmatrix}\Big|U_p^{n!} = \begin{pmatrix} f & f|\langle p\rangle \end{pmatrix}\Big|A^{n!}$$

Taking limit we have $e_{ord}(\langle d\rangle\, f) = 0$.

Case 2: a_p is a unit. By diagonalizing A, we obtain

$$p^{k-1}(\alpha-\beta)f = \alpha(p^{k-1}f - \beta f|\langle p\rangle) - \beta(p^{k-1}f - \alpha f|\langle p\rangle)$$

Set $f_\alpha := p^{k-1}f - \beta f|\langle p\rangle$ and $f_\beta := p^{k-1}f - \alpha f|\langle p\rangle$. We see that they are eigenvectors of U_p with eigenvalues α and β, respectively. Lemma implies that $e_{ord}(f_\alpha) = f_\alpha$ and $e_{ord}(f_\beta) = 0$. Hence, by applying Hida's projector to equation , we get

$$e_{ord}(f) = \frac{\alpha}{p^{k-1}(\alpha-\beta)}(p^{k-1}f - \beta f|\langle p\rangle) = \frac{\alpha}{\alpha-\beta}(f - \beta p^{1-k} f|\langle p\rangle)$$

Similarly, we have

$$(\alpha-\beta)f|\langle p\rangle = (p^{k-1}f - \beta f|\langle p\rangle) - (p^{k-1}f - \alpha f|\langle p\rangle)$$

Thus

$$e_{ord}(\langle d\rangle\, f) = \frac{p^{k-1}}{\alpha-\beta}(\langle d/p\rangle\, f - \beta p^{1-k}\,\langle d\rangle\, f)$$

□

Definition 2.2.8. Suppose $f \in S_k(\Gamma_0(N))$ is a p-ordinary cusp form which is an eigenform of T_p, and let β denote by its non-unit root of the Frobenius. The p-stabilized cusp form g corresponding to f is given by

$$g := f - \beta p^{1-k} \langle p \rangle f$$

which satisfies

$$g(z) = f(z) - \beta f(pz)$$

Note that $g \in S_k(\Gamma_0(Np))$ and if $p|N$, the $\beta = 0$, so f is already p-stabilized.

Corollary 2.2.9. *The space $S_k^{ord}(\Gamma_0(N))$ has basis*

$$\{f(dz) - \beta f(pdz) : f \in S_k(\Gamma_0(N'))^{new} p - ordinary, (p, d) = 1, dN'|N\}$$

where β denotes the non-unit root of the Frobenius of f at p.

2.3 Λ-adic families

Thoughout this section, p is a prime number ≥ 5 and $\Lambda := \mathbb{Z}_p[[T]]$ is the Iwasawa's algebra. Given a cusp form f of weight 2, we will construct a family which p-adically "converges" to f. I mainly follow Hida's blue book [Hi93] and the lecture notes [Laf], [BNG].

2.3.1 Λ-adic modular forms

We will explore the modular forms in families. Let p be a prime number $p \geq 5$ and N an integer prime to p. Recall that the group $\mathbb{Z}_p^\times$ of p-adic units is cannonically equal to the product of the group of principal units $1 + p\mathbb{Z}_p$ and the group μ_{p-1} of $(p-1)$th roots of unity

$$\mathbb{Z}_p^\times = \mu_{p-1}^\times \times (1 + p\mathbb{Z}_p)$$
$$x = \omega(x) \cdot \langle a \rangle$$

We denote the projection to principal units by $\langle \cdot \rangle$ and the projection to roots of unity by the Teichmuller character ω.

Let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be an arbitrary Dirichlet character for some positive integer N, and let d_χ denote its conductor. We know that either $(d_\chi, p) = 1$ or $p|d_\chi$, so

$$d_\chi = M \ \ or \ \ d_\chi = Mp^{r+1}$$

for some positive integer M coprime to p and some integer $r \geq 0$. Now we have

$$(\mathbb{Z}/Mp^{r+1}\mathbb{Z})^\times \simeq (\mathbb{Z}/Mp\mathbb{Z})^\times \times (1+p\mathbb{Z})/(1+p^{r+1}\mathbb{Z})$$
$$\alpha \mod Mp^{r+1} \mapsto (\alpha \mod Mp, \alpha \mod (1+p^{r+1}\mathbb{Z})$$

Hence we obtain $\chi = \chi_F\chi_S$, where

$$\chi_F : (\mathbb{Z}/Mp\mathbb{Z})^\times \to \overline{\mathbb{Q}}^\times \ \ and \ \ \chi_S : (1+p\mathbb{Z})/(1+p^{r+1}\mathbb{Z}) \to \overline{\mathbb{Q}}^\times$$

are characters of conductor Mp and p^{r+1} respectively. Note that for any character $\chi : (\mathbb{Z}/p^r\mathbb{Z})^\times \to \mathbb{C}^\times$, the image of χ_F is contained in $\mathbb{Z}_p$, while the image of χ_S has p-power order.

Definition 2.3.1. For any character $\chi : (\mathbb{Z}/Np^r\mathbb{Z})^\times \to \mathbb{C}^\times$ and integer $k > 1$, we have $\chi = \chi_F\chi_S$ given as above. Let $u = 1 + p$, we define the specialization

$$\begin{aligned} \nu_{k,\chi} : \Lambda &\to \overline{\mathbb{Q}}_p \\ T &\mapsto \xi_\chi u^k - 1, \quad \xi_\chi = \chi_S(u) \end{aligned}$$

Since ξ_χ is a p-power root of unity and $u^k = (1+p)^k \equiv 1 \mod p$, we see that $|\xi_\chi u^k - 1|_p < 1$ for all integer $k > 1$. Hence, the evaluation of any element of Λ at $\xi_\chi u^k - 1$ results in a power series converges p-adically.

We denote by $A(\chi, \Lambda)$ the set of all specializations $T \mapsto \xi_\chi u^k - 1$ associated to character $\chi : (\mathbb{Z}/Np^r\mathbb{Z}) \to \mathbb{C}^\times$ running over all $k \in \mathbb{N}$. Since Λ has no zero divisors, the kernel of the specialization map $\nu_{k,\chi}$ is a prime ideal of Λ. Hence, the specialization map $\nu_{k,\chi}$ can be seen as an embedding of $\Lambda/\ker(\nu_{k,\chi})$ into $\overline{\mathbb{Q}}_p$. We can view $A(\chi, \Lambda)$ as the set of $\mathbb{Z}_p$-algebra homomorphisms from Λ to $\overline{\mathbb{Q}}_p$.

Definition 2.3.2. Let N be a positive interger coprime to p. For any character $\chi : (\mathbb{Z}/Np^r\mathbb{Z})^\times \to \overline{\mathbb{Q}}^\times$, where $r \geq 0$, a Λ-adic modular form F of character χ and level Np^r is a formal q-expansion

$$F(T) = \sum_{n \geq 0} a_n(F)(T)q^n \in \Lambda[[q]] = \mathbb{Z}_p[[T, q]]$$

such that for all but finitely many integer $k > 1$ we have

$$\nu_k(F) = \sum_{n\geq 0} \nu_k\left(a_n(F)(T)\right) q^n \in M_k(Np^r, \chi\omega^{-k})$$

for all $\nu_k \in A(\chi, \Lambda)$. Here ω is the Teichmuller character.

Similarly, if $\nu_k(F) \in S_k(Np^r, \chi\omega^{-k})$ (resp. $M_k^{ord}(Np^r, \chi\omega^{-k})$, $S_k^{ord}(Np^r, \chi\omega^{-k})$ for all but finitely many positive integers k, we say F is a Λ-adic cusp form (resp. ordinary Λ-adic form, ordinary Λ-adic cusp form) .

Thus a Λ-adic form is a family of classical forms of varying weights with identical residual q-expansions. The family $\nu_k(F)$ can be view as the evaluation of F at $T = \xi_\chi u^k - 1$ for $k \in \mathbb{N}$.

Let $\mathbf{M}(Np^r, \chi, \Lambda)$ (resp. $\mathbf{S}(Np^r, \chi, \Lambda)$) be the Λ-module of all Λ-adic modular forms (resp. Λ-adic cusp forms) associated to χ.

Let $\mathbf{M}(Np^r, \Lambda) := \bigoplus_\chi \mathbf{M}(Np^r, \chi, \Lambda)$ be the Λ-module of all Λ-adic forms. We also have the corresponding decomposition $\mathbf{S}(Np^r, \Lambda) := \bigoplus_\chi \mathbf{S}(Np^r, \Lambda)$

2.3.2 Hecke Operators on Λ-adic cusp forms

Proposition 2.3.3. *Consider the following character*

$$\begin{aligned} \kappa : 1 + p\mathbb{Z}_p &\to \Lambda^\times \\ u^s &\mapsto \kappa(u^s) : (X \mapsto (1+X)^s) \end{aligned}$$

Then κ is a continuous character with respect to the $\mathfrak{m}$-adic topology on Λ, where $\mathfrak{m}$ is the maximal ideal of Λ.

Proof. For the proof, we need two following lemmas.

Lemma 2.3.4. *If $z \in 1 + p\mathbb{Z}_p$, then $z = u^{s(z)}$ where $s(z) = \dfrac{\log_p(z)}{\log_p(u)} \in \mathbb{Z}_p$*

Proof. Let $\exp_p(z) = \sum_{n\geq 0} \dfrac{z^n}{n!}$ denote the p-adic exponential, which converges on $|z|_p <$

$p^{-1/p-1}$. Then

$$u^{s(z)} = \exp_p(s(z)\log_p(u)) = z$$

□

The following lemma is a consequent of the previous one.

Lemma 2.3.5. *If $s \in \mathbb{Z}_p$, then $\binom{s}{m} \in \mathbb{Z}_p$ for any integer $m \geq 0$.*

Proof. We see that $\binom{s}{m}$ is a polynomial in $\mathbb{Q}_p$ with variable s, so it is a continuous map from $\mathbb{Z}_p$ to $\mathbb{Q}_p$. This map takes $\mathbb{Z}$ to $\mathbb{Z}$, and since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, it induces a continuous map from $\mathbb{Z}_p$ to $\mathbb{Z}_p$. Thus for $s \in \mathbb{Z}_p$, we have $\binom{s}{m} \in \mathbb{Z}_p$. □

It follows that

$$(1+X)^s = \sum_{m=0}^{s} \binom{s}{m} X^m \in \Lambda^\times$$

□

One can view κ as a Galois character via the natural restriction map $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) = 1 + p\mathbb{Z}_p$ where $\mathbb{Q}_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$.

Note that for integers n prime to p

$$\kappa(\langle n\rangle)(u^k - 1) = \kappa(u^{s(n)})(u^k - 1) = u^{ks(n)} = \omega^{-k}(n)n^k$$

where we write $\langle n\rangle = \omega(n)^{-1}n = u^{s(n)}$ with $s(n) = \dfrac{\log(\langle n\rangle)}{\log(u)}$. Consider the group homomorphism

$$\begin{aligned} \varphi : \mathbb{Z}_p &\to 1 + p\mathbb{Z}_p \\ s &\mapsto u^s \qquad u := 1 + p \end{aligned}$$

It is a group isomorphism with the inverse given by

$$s \mapsto \frac{\log_p(s)}{\log_p(u)}$$

here $\log_p$ is the p-adic logarithm. Thus we have $s = u^{\varphi^{-1}(s)}$ for all $s \in 1 + p\mathbb{Z}_p$.

For a given positive integer n and divisor b of n with $b \equiv 1 \mod p$, we have

$$\begin{aligned}\left(1 + (\xi_\chi u^k - 1)\right)^{\varphi^{-1}(d)} &= \left(\xi_\chi u^k\right)^{\varphi^{-1}(d)} = \chi_S(u)^{\varphi^{-1}(d)} \cdot \left(u^{\varphi^{-1}(d)}\right)^k \\ &= \chi_S(d)d^k = \omega(d)^{-k}\chi_S(d)d^k\end{aligned}$$

with the last equality following from the fact that $\omega(d) = 1$.

Definition 2.3.6. Then we define for each Λ-adic form $F \in \mathbf{M}(\chi, \Lambda)$ a formal q-expansion $F|T_n$ by

$$a_m\left(F|T_n\right)(T) = \sum_{\substack{b|(m,n)\\(b,p)=1}} (T+1)^{\varphi^{-1}(\langle d\rangle}(\chi_F(b)b^{-1}a_{mn/b^2}(F)(T)$$

where b runs over all common divisors prime to p of m and n.

We evaluate this formal power series $F|T_n$ at $\xi_\chi u^k - 1$ we see that $F(\xi_\chi u^k - 1, q) = f_k \in M_k(Np^r, \chi\omega^{-k})$. Moreover

$$\begin{aligned}a_m\left(F|T_n\right)(\xi_\chi u^k - 1) &= \sum_{\substack{b|(m,n)\\(b,p)=1}} (\xi_\chi u^k - 1)^{\varphi^{-1}(\langle d\rangle}\chi(b)b^{-1}a_{mn/b^2}(F)(\xi_\chi u^k - 1) \\ &= \sum_{\substack{b|(m,n)\\(b,p)=1}} \chi(b)\omega(b)^{-k}d^{k-1}a_{mn/b^2}(f_k) = a_m(f_kT_n)\end{aligned}$$

This shows that $F|T_n(\xi_\chi u^k - 1) = F(\xi_\chi u^k - 1)|T_n \in M_k(Np^r, \chi\omega^{-k})$. Therefore, F is again a Λ-adic form. Thus the operator T_n is well-defined and commutes with the specialization map $X \mapsto \xi_\chi u^k - 1$. So we have Hecke operators T_n acting on $\mathbf{M}$ and $\mathbf{S}$.

Proposition 2.3.7. *There exists a unique idempotent $e_{ord} : \boldsymbol{M}(\chi, \Lambda) \to \boldsymbol{M}^{ord}(\chi, \Lambda)$ satisfying*

$$(F|e)(\xi_\chi u^k - 1) = F(\xi_\chi u^k - 1)|e$$

for all $F \in \boldsymbol{M}(\chi, \Lambda)$ and all integer $k > 0$ for which $F(\xi_\chi u^k - 1) \in M_k(Np^r, \chi\omega^{-k})$

Theorem 2.3.8. *(A.Wiles). The space of ordinary Λ-adic modular forms (ordinary Λ-adic cusp forms) of character χ is free of finite rank over Λ.*

2.4 Constructing Λ-adic forms

2.4.1 Λ-adic Eisenstein Series

Recall that if k is an even integer greater than or equal to 4, then the Eisenstein series of weight k, level 1 and trivial character has q-expansion given by

$$E_k = \frac{\zeta(1-k)}{2} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

where $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$ is the usual arithmetic function, and $\zeta(s)$ is the Riemann zeta function.

let p be a prime, we consider the p-stabilized form

$$E_k^{(p)} = E_k(z) - p^{k-1} E_k(pz)$$

is a modular form of level p. More generally, for any $k \geq 1$ and character $\chi \mod Np^r$, with χ having the same parity as k, we define the Eisenstein series of weight k, level equal to the conductor of χ, and character χ, given by

$$E_{k,\chi} = \frac{L(1-k,\chi)}{2} + \sum_{n=1}^{\infty} \sigma_{k-1,\chi}(n) q^n$$

where $\sigma_{k-1,\chi}(n) = \sum_{d|n} \chi(d) d^{k-1}$ and $L(s,\chi)$ is the Dirichlet L-series attached to χ. Again, if χ has level N (i.e., it has trivial p-part), then $E_{k,\chi}$ has level N, which is not divisible by Np. We consider its p-stabilization, namely

$$E_{k,\chi}^{(p)} = E_{k,\chi}(z) - \chi(p) p^{k-1} E_{k,\chi}(pz)$$

which has q-expansion

$$E_{k,\chi}^{(p)} = \frac{L^{(p)}(1-k,\chi)}{2} + \sum_{n=1}^{\infty} \sigma_{k-1,\chi}^{(p)}(n) q^n$$

where $\sigma_{k-1,\chi}^{(p)}(n) = \sum_{d|n,(d,p)=1} \chi(d) d^{k-1}$ and $L^{(p)}(s,\chi) = (1-\chi(p)p^{-s}) L(s,\chi)$ the Dirichlet L-series attached to χ derived of the Euler factor at p, has level divisible by Np.

Now we are ready to begin interpolating p-stabilized Eisenstein series.

Proposition 2.4.1. *Let $\chi = \chi_F\chi_S$ be the character of level Np^r. For each $k > 1$ and $\xi \in \mu_{p^{r-1}}$ with $r \geq 1$. Let $\mathbb{Z}_p[\chi_F][[T]]$ for $\chi_F \neq 1$, then there is a Λ-adic form*

$$\mathcal{E}_{\chi_F}(T) = \sum_{n=0}^{\infty} a_{n,\chi_F}(\mathcal{E})(T)q^n \in \mathbb{Z}_p[\chi_F][[T]]$$

which specializes to $E_{k,\psi}$ under the homomorphism of $\mathbb{Z}_p[\chi_F][[T]]$ induced by ν_{k,χ_F}.

Let $f \in S_1(Np, \psi)$ be a fixed cusp form of weight 1. Recall that

$$\mathcal{E}_\chi(\xi u^{k-1} - 1) = E^{(p)}_{k-1,\psi} \in M_{k-1}(Np^r, \psi)$$

where $\psi = \chi\omega^{1-k}$. Hence,

$$f_1 \cdot E^{(p)}_{k-1,\psi} \in S_k(Np^r, \chi'\omega^{-k})$$

with $\chi' := \psi\chi$. We show $f_1 \cdot E^{(p)}_{k-1,\psi}$ are the specializations at $T = \xi u^k - 1$ of a cuspidal Λ-adic form F of level N and character χ' for $k > 1$ and ξ as above.

Assume that the q-expansions of f_1 and ψ are both $\mathbb{Z}_p[\chi_F]$-rational (otherwise extend scalars). Then we may formally multiply the q-expansions in $\mathbb{Z}_p[\chi_F][[T]]$ of f_1 and $\mathcal{E}_\chi$. Say the resulting q-expansion is $f_1 \cdot \mathcal{E}_\chi = \sum_{n=0}^{\infty} a_n(T)q^n$, for some $a_n(T) \in \mathbb{Z}_p[\chi][[T]]$. Now define

$$F := \sum_{n=0}^{\infty} a_n(u^{-1}T + u^{-1} - 1)q^n$$

noting that the substitution made above is an automorphism of $\mathbb{Z}_p[\chi_F][[T]]$. Then on substituting $T = \xi u^k - 1$ we obtain

$$F(\xi u^k - 1) = \sum_{n=0}^{\infty} a_n(\xi u^{k-1} - 1)q^n = f_1 \cdot \mathcal{E}_\chi(\xi u^{k-1} - 1) = f_1 \cdot E^{(p)}_{k-1,\chi\omega^{1-k}}$$

Thus F is the desired cuspidal family.

2.4.2 Hida Families

In this section, I will follow [BD07] parallel with [GS94].

Consider the weight space $W = \mathrm{Hom}(\mathbb{Z}_p^\times, \mathbb{Z}_p^\times)$. Since p is odd, we have the identification

$$W = \mathrm{Hom}(\mathbb{Z}_p^\times, \mathbb{Z}_p^\times) \simeq \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$$

We will define analytic functions on the weight space. If $U \subset W$ is an open subset, let $\mathcal{A}_U$ denote the collection of analytic functions $\alpha : U \to \mathbb{Z}_p$, more precisely, the collection of functions that are power series on each intersection $U \cap (\{a\} \times \mathbb{Z}_p)$. Assume further that U is contained in the residue disk of 2, and then $\mathcal{A}_U$ is simply the ring of power series that converge on an open subset of $\mathbb{Z}_p$. A Hida family is a formal q-expansion

$$F = \sum_{n=1}^{\infty} a_n q^n$$

such that there exists a neighborhood U of 2 in W such that $a_n \in \mathcal{A}_U$ for all n and such that if $k \in U \cap \mathbb{Z}^{\geq 2}$, the weight k specialization

$$f_k := \sum_{n=1}^{\infty} a_n(k) q^n$$

is a normalized ordinary eigenform of weight k on $\Gamma(Np)$. Weights in $\mathbb{Z}^{\geq 2} \subset W$ are called classical.

Let $\tilde{\Lambda} := \mathbb{Z}_p[[\mathbb{Z}_p^\times]]$ and $\tilde{\Lambda}' := \mathbb{Z}_p[[1 + p\mathbb{Z}_p]]$. They are also called Iwasawa's algebras, and $\tilde{\Lambda}' \simeq \Lambda = \mathbb{Z}_p[[T]]$ as we have seen in the section 1. Furthermore, $\tilde{\Lambda}$ can be viewed as functions on the space of continuous $\mathbb{Z}_p$-algebra homomorphism as denoted above by W.

From now, we identify Λ with $\mathbb{Z}_p[[1 + p\mathbb{Z}_p]]$. For each $k \in \mathbb{Z}_p$ the character

$$\begin{aligned} 1 + p\mathbb{Z}_p &\to \mathbb{Z}_p^\times \\ a &\mapsto a^{k-2} \end{aligned}$$

can be extended to a continuous homomorphism $\sigma_{k-2} : \Lambda = \mathbb{Z}_p[[1 + p\mathbb{Z}_p]] \to \mathbb{Z}_p$

For each $\alpha \in \Lambda$ we define the Iwasawa functions on $\mathbb{Z}_p$

$$\alpha(k) := \sigma_{k-2}(\alpha)$$

The map $\alpha \mapsto \alpha(k)$ endows $\mathcal{A}_U$ with a natural structure as Λ-module for every disk U in $\mathbb{Z}_p$.

Definition 2.4.2. We define the abstract Λ-adic Hecke algebra of tame conductor N to be the free polynomial algebra

$$\mathcal{H} = \mathbb{Z}_p[[\mathbb{Z}_p^\times]][T_n (n \in \mathbb{Z}^+)]$$

generated over $\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$ by T_n $(n \in \mathbb{Z}^+)$.

We have the following theorem due to Hida which is crucial in the theory.

Theorem 2.4.3. *There is an integral domain $\mathcal{R}_E$ finite and flat over Λ and a surjective Λ-homomorphism $h_E : \mathcal{H} \to \mathcal{R}_E$ with the following properties.*

1. *$\mathcal{R}_E$ is unramified over the augmentation ideal P_0 in Λ.*
2. *The homomorphism $\lambda_E : \mathcal{H} \to \mathbb{Z}_p$ factors through h_E, i.e., there is a homomorphism $\lambda_E : \mathcal{H} \to \mathbb{Z}_p$ such that*

$$\lambda_E = \pi_E \circ h_E$$

We use this theorem to describe Hida's families as follows. The homomorphism $\lambda_E : \mathcal{H} \to \mathbb{Z}_p$ gives us weight k specialization f_k. For each $n \in \mathbb{N}$, let $\alpha_n := h_E(T_n) \in \mathcal{R}_E$ and define $F := \sum_{n=1}^{\infty} \alpha_n q^n \in \mathcal{R}_E[[q]]$ a Λ-adic form.

Fix a neighborhood of 2 in W on which a_n converge. If $k \in U \cap \mathbb{Z}_{\geq 2}$, the weight k specialization is a normalised eigenform of weight k on $\Gamma_0(Np)$, which is new at the primes dividing N. In particular, if $k \in U \cap \mathbb{Z}_{\geq 2}$, f_k arises from a normalized eigenform on $\Gamma_0(N)$ that we denote by f_k^*. Consider

$$1 - a(f_k^*)p^{-s} + p^{k-1-2s} = (1 - \alpha_p(k)p^{-s})(1 - \beta_p(k)p^{-s})$$

we can order the roots $\alpha_p(k)$ and $\beta_p(k)$ in such a way that $\alpha_p(k) = a_p(f_k)$ and $\beta_p(k) = p^{k-1}a_p(f_k)^{-1}$. Hence we obtain a p-stabilized newform

$$f_k(z) = f_k^*(z) - \beta_p(k) f_k^*(pz)$$

Remark 2.4.4. For the ordinary eigenform f, the Euler factor at p of the L-function of f has a factorization $(1 - \alpha p^{-s})(1 - \beta p^{-s})$ where α is a p-adic unit and β is divisible by p. We call α the unit root of Frobenius and β the non-unit root of Frobenius. Note that if $r > 0$ then $\beta = 0$.

Theorem 2.4.5. *Let E be an elliptic curve curve over $\mathbb{Q}$ of tame conductor N with good ordinary or multiplicative reduction at the prime $p \geq 5$. Then there is an open disk $U \subset \mathbb{Z}_p$ about 2, a formal q-expansion*

$$f = \sum_{n=1}^{\infty} \alpha_n q^n \in \mathcal{A}_U[[q]]$$

such that for each integer $k \geq 2$ in U, the power series

$$f_k := \sum_{n=1}^{\infty} \alpha_n(k) q^n \in \mathbb{Z}_p[[q]]$$

is the q-expansion of a non-zero p-stabilized ordinary newform of tame conductor N, weight k and character ω^{2-k}. Moreover, $f_2 = f_E$.

Proof. Refer [Hi86a] and [Hi86b]. □

For a modular elliptic curve E with good ordinary or multiplicative reduction at p we let f_E be the p-stabilized ordinary newform associated to the newform attached E. Note that for the associated complex L-functions we have the identity

$$(1 - \beta p^{-s}) L(E, s) = L(f_E, s)$$

2.5 Galois Representation Theory

Let K be a field. We denote by $G_K := \mathrm{Gal}(K_S/K)$ the absolute Galois group of K, i.e., the Galois group of a separable closure K_S of K.

Definition 2.5.1. Let k be a topological field. An n-dimensional representation of G_K is a continuous homomorphism of groups

$$\rho : G_K \to \mathrm{GL}_n(k)$$

with the topology on G_K the Krull topology and the topology on $\mathrm{GL}_n(k)$ the one induced by the inclusion $\mathrm{GL}_n(k) \hookrightarrow K^{n^2}$.

We also have an equivalent definition as follows.

Definition 2.5.2. Let k be a topological field. An n-dimensional Galois representation of G_K is an $k[G_K]$-module V which is n-dimensional as a k-vector space such that the action

$$\begin{aligned} G_K \times V &\to V \\ (\sigma, v) &\mapsto v^\sigma \end{aligned}$$

is continuous.

Two representations V and V' are said to be equivalent if there exists a continuous $k[G_K]$-modules isomorphism $V \to V'$.

Let $W \subseteq V$ be subspace of V. We say that W is invariant or stable under G_K if it is preserved under the inducded action of G_K on W, i.e., for all $w \in W$ we have $w^\sigma \in W$ for all $\sigma \in G$.

Definition 2.5.3. Let V be an n-dimensional Galois representation. We say that V is irreducible or simple if V has only 0 and V as invariant subspaces. If V is isomorphic to a direct sum of irreducible Galois representation, then we say V is semi-simple.

Let L/K be a finite Galois extension of number fields and let $\mathfrak{B}/\mathfrak{p}$ be primes ideals in these fields. The decomposition group of $\mathfrak{B}$ is defined as

$$D(\mathfrak{B}/\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(L/K) | \sigma(\mathfrak{B}) = \mathfrak{B}\}$$

It is isomorphic to the local Galois group

$$D(\mathfrak{B}/\mathfrak{p}) \cong \mathrm{Gal}(L_{\mathfrak{B}}/K_{\mathfrak{p}})$$

We consider the reduction modulo $\mathfrak{B}$

$$\pi(L_{\mathfrak{B}}/K_{\mathfrak{p}}) = \pi(\mathfrak{B}/\mathfrak{p}) : \mathrm{Gal}(L_{\mathfrak{B}}/K_{\mathfrak{p}}) \to \mathrm{Gal}(\mathbb{F}(\mathfrak{B})/\mathbb{F}(\mathfrak{p}))$$

This map is surjective. The group $\mathrm{Gal}\left(\mathbb{F}(\mathfrak{B})/\mathbb{F}(\mathfrak{p})\right)$ is canonically generated by the Frobenius endomorphism $\mathrm{Frob}(\mathfrak{B}/\mathfrak{p})$ which is given by $x \mapsto x^q$ with $q = \#\mathbb{F}(p)$. The kernel of the reduction map is called the inertia group $I(\mathfrak{B}/\mathfrak{p})$. Hence we have the exact sequence

$$0 \to I(\mathfrak{B}/\mathfrak{p}) \to \mathrm{Gal}(L_{\mathfrak{B}}/K_{\mathfrak{p}}) \to \mathrm{Gal}(\mathbb{F}(\mathfrak{B})/\mathbb{F}(\mathfrak{p}))$$

The field extension $L_{\mathfrak{B}}/K_{\mathfrak{p}}$ is unramified if and only if $I(\mathfrak{B}/\mathfrak{p})$ is trivial, i.e., the reduction map $\pi(\mathfrak{B}/\mathfrak{p})$ is an isomorphism.

We can pass to infinite Galois extensions. Let $K_{\mathfrak{p}} \subset L_{\mathfrak{B}} \subset M_{\widetilde{\mathfrak{B}}}$ be finite subfield of $\overline{\mathbb{Q}_p}$. We obtain a projective system of short exact sequences

$$\begin{array}{ccccccccc}
0 & \longrightarrow & I(M_{\widetilde{\mathfrak{B}}}/K_{\mathfrak{p}}) & \longrightarrow & \mathrm{Gal}(M_{\widetilde{\mathfrak{B}}}/K_{\mathfrak{p}}) & \longrightarrow & \mathrm{Gal}(\mathbb{F}(\widetilde{\mathfrak{B}})/\mathbb{F}(\mathfrak{p})) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & I(L_{\mathfrak{B}}/K_{\mathfrak{p}}) & \longrightarrow & \mathrm{Gal}(L_{\mathfrak{B}}/K_{\mathfrak{p}}) & \longrightarrow & \mathrm{Gal}(\mathbb{F}(\mathfrak{B})/\mathbb{F}(\mathfrak{p})) & \longrightarrow & 0
\end{array}$$

Taking projective limit over compact sets is exact, hence, we obtain the exact sequence

$$0 \to I_{K_\mathfrak{p}} \to G_{K_\mathfrak{p}} \xrightarrow{\pi_p} G_{\mathbb{F}(\mathfrak{p})} \to 0$$

where $\mathrm{Gal}_{K_\mathfrak{p}} = \mathrm{Gal}(\overline{K_\mathfrak{p}}/K_\mathfrak{p})$ and $I_{K_\mathfrak{p}}$ is the projective limit over iniertia groups.

Definition 2.5.4. Let $K_\mathfrak{p}$ be a finite extension of $\mathbb{Q}_p$ and let k be any topological field. Consider a local Galois representation $\rho : G_{K_\mathfrak{p}} \to \mathrm{GL}_n(k)$. We call it unramified if $\rho(I_{K_\mathfrak{p}}) = 0$

We call $I_{K_\mathfrak{p}} := I_\mathfrak{p}$ the inertia group of $K_\mathfrak{p}$

Definition 2.5.5. Let K be a number field, and k any topological field. Consider the Galois representation $\rho : G_K \to \mathrm{GL}_n(k)$. Let $\mathfrak{p}$ be a prime of K corresponding to an embedding $\iota_\mathfrak{p} : K \hookrightarrow \overline{\mathbb{Q}_p}$. Choose any embedding $\iota : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}$ extending $\iota_\mathfrak{p}$, giving rise to an embedding of $G_{K_\mathfrak{p}}$ into G_K. The Galois representation ρ is called unramified at $\mathfrak{p}$ if the restriction of ρ to $G_{K_\mathfrak{p}}$ is unramified.

The cyclotomic character

Let K be a field of characteristic 0 and $\overline{K}$ an algebraic closure. Let

$$\mu_m(\overline{K}) = \overline{K}^\times[m] = \ker\left(\overline{K}^\times \xrightarrow{x\mapsto x^m} \overline{K}^\times\right)$$

be the m-torsion points of $\overline{K}^\times$, i.e. the m-th roots of unity. By choosing a compatible system of roots of unity ξ_{ℓ^n} we obtain the isomorphism of projective systems

$$\begin{array}{ccc} \mathbb{Z}/\ell^n\mathbb{Z} & \longrightarrow & \mu_{\ell^n}(\overline{K}) \\ \downarrow & & \downarrow \\ \mathbb{Z}/\ell^{n-1}\mathbb{Z} & \longrightarrow & \mu_{\ell^{n-1}}(\overline{K}) \end{array}$$

giving rise to an isomorphism as groups

$$\mathbb{Z}_\ell \simeq \varprojlim_n \mu_{\ell^n}(\overline{K}^\times)$$

The object on the right is called the ℓ-adic Tate module of $\overline{K}^\times$ denoted by $T_\ell(\overline{K}^\times)$ or $\mathbb{Z}_\ell(1)$ with the emphasised Galois action.

Hence we have a Galois representation so called ℓ-adic cyclotomic character over $\overline{K}$.

$$\chi_0 : G_K \xrightarrow{\sigma\mapsto(x\mapsto\sigma(x))} Aut(\mathbb{Z}_\ell(1)) \simeq \mathbb{Z}_\ell^\times = GL_1(\mathbb{Z}_\ell) \hookrightarrow GL_1(\mathbb{Q}_\ell)$$

Proposition 2.5.6. *Let χ_0 be the cyclotomic character over $\overline{\mathbb{Q}}$. Then χ_0 is a 1-dimensional global Galois representation, which is unramified at all prime $p \neq \ell$ and*

$$\chi_0(\mathrm{Frob}_p) = p$$

Moreover, χ_0 is an odd representation.

The Tate module of an elliptic curve

Let E be an elliptic curve over a field K of characteristic 0. For every prime p, we denote the subgroup of the p^n-torsion points over $\overline{K}$ by $E(\overline{K})[p^n]$. The group G_K acts on $E(\overline{K})[p^n]$; moreover, for all n we have a group homomorphism

$$E(\overline{K})[p^{n+1}] \to E(\overline{K})[p^n]$$

given by the multiplication by p. It turns out that $\{E(\overline{K})[p^n]\}_{n\in\mathbb{N}}$ is a projective system. Since the action of G_K is compatible with the transition maps, we obtain by the universal property of the inverse limit a continuous action of G_K over $\varprojlim E(\overline{K})[p^n] := Ta_p(E)$, which is called the p-adic Tate module of E.

Note that $E(\overline{K})[p^n] \simeq (\mathbb{Z}/p^n\mathbb{Z})^2$, we have that $Ta_p(E) \simeq \mathbb{Z}_p^2$. By this way we get a 2-dimensional p-adic Galois representation associated to E.

Proposition 2.5.7. *Let k be a finite extension of $\mathbb{Q}_\ell$ for some prime ℓ and let $\rho : G_\mathbb{Q} \to GL_n(k)$ be a Galois representation. Then ρ is equivalent to a Galois representation $\rho' : G_\mathbb{Q} \to GL_n(\mathcal{O}_k)$, where $\mathcal{O}_k$ is the valuation ring of k.*

Proof. Refer [DS05] □

Definition 2.5.8. Let $c \in G_\mathbb{Q}$ be a complex conjugate. A Galois representation $\rho : G_\mathbb{Q} \to \mathrm{GL}_n(\mathbb{C})$ is said to be odd if $\det(\rho(c)) = -1$ for all c.

The following is a celebrated result in ℓ-adic Galois representation due to Deligne.

Theorem 2.5.9. *Let $k \geq 2$, $N \geq 1$, and ℓ a prime not dividing N. Let $\epsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ a Dirichlet character. Then for any normalised eigenform $f \in S_k(\Gamma_0(N), \epsilon)$ with $f = \sum_{n\geq 1} a_n q^n$ one can attach a Galois representation*

$$\rho_f : G_\mathbb{Q} \to GL_2(\overline{\mathbb{Q}}_p)$$

such that

1. *ρ_f is irreducible*

2. *ρ_f is odd*

3. *for all primes $p \nmid N\ell$ the representation ρ_f is unramified at p and the characteristic polynomial of Frobenius of ρ has the form*

$$X^2 - a_p(f)X + \epsilon(p)p^{k-1}$$

Proof. Refer [DS05]. □

We have the corresponding Galois representation for Hida's family.

Theorem 2.5.10. *Let E be an elliptic curve over $\mathbb{Q}$ of tame conductor N with good ordinary or multiplicative reduction at the prime $p \geq 5$. Then there is an open disk $U \subset \mathbb{Z}_p$ about 2, a formal q-expansion $f = \sum_{n=1}^{\infty} \alpha_n q^n \in \mathcal{A}_U[[q]]$ and a Galois representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{A}_U)$ satisfying the following properties*

1. *For each integer $k \geq 2$ in U, the Galois representation $\rho_k : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p)$, obtained by composing ρ with the specialization map $\alpha \mapsto \alpha(k)$, is equivalent to Deligne's representation associated to f_k.*

   In particular, ρ_2 is equivalent to the Galois representation attached to the p-adic Tate module of E.

2. *For all $k \in \mathbb{Z}_p$ the local Galois representation $\rho_k|_{G_{\mathbb{Q}_p}} : G_{\mathbb{Q}_p} \to \mathrm{GL}_2(\mathbb{Z}_p)$ has the form*

$$\rho|_{G_{\mathbb{Q}_p}} = \begin{pmatrix} \chi_0 \langle \chi_0 \rangle^{k-2} \varphi_k^{-1} & * \\ 0 & \varphi_k \end{pmatrix}$$

   where φ_k is the unramified character sending a Frobenius element to $\alpha_p(k)$ and $\langle \chi_0 \rangle : G_{\mathbb{Q}_p} \to \mathbb{Z}_p^{\times}$ is the local Galois character obtained by composing the cyclotomic character χ_0 with projection to the principal units.

Proof. Refer [Wi88]. □

2.6 Ordinary Tate Modules

We define the modular curve $X_0(N)$ as a compact Riemann surface

$$X_0(N) := \Gamma_0(N) \setminus \mathbb{H}^*$$

This modular curve admits the structure of a smooth projective variety over $\mathbb{Q}$.

Theorem 2.6.1. *There exists a smooth projective curve $C/\mathbb{Q}$ and a bihilomorphic mapping $\phi : X_0(N) \to C(\mathbb{Q})$ such that*

$$\phi^*(\mathbb{C}(C)) = \mathbb{C}(X_0(N)) = \mathbb{C}(j, j_N)$$

and

$$\phi^*(\mathbb{Q}(C)) = \mathbb{Q}(j, j_N)$$

The curve $C/\mathbb{Q}$ is unique up to isomorphism over $\mathbb{Q}$, and ϕ is uniquely determined by the isomorphism of $\mathbb{Q}(C)$ with $\mathbb{Q}(j, j_N)$

We refer to (ϕ, C) as a model for $X_0(N)$ over $\mathbb{Q}$. We identify $C(\mathbb{Q})$ with $X_0(N)$ and refer to $X_0(N)/\mathbb{Q}$ as a $\mathbb{Q}$-structure on $X_0(N)$.

Definition 2.6.2. Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$. The Jacobian of the corresponding modular curve $X(\Gamma)$ is

$$J(X(\Gamma)) = S_2(\Gamma)^*/H_1(X(\Gamma), \mathbb{Z})$$

where $*$ denotes the dual space.

The double coset operator induces a pullback on dual spaces, hence it descends to a map on Jacobians

$$\begin{aligned}[\Gamma_1 \alpha \Gamma_2] : J(X_2) &\to J(X_1) \\ \psi &\mapsto [\psi \circ [\Gamma_1 \alpha \Gamma_2]]\end{aligned}$$

where the bracket denote equivalence class modulo homology.

Definition 2.6.3. For each integer $r > 0$, let $X_{r/\mathbb{Q}}$ be the complete modular curve associated to $\Gamma_0(N) \cap \Gamma_1(p^r)$ and endowed with canonical $\mathbb{Q}$-structure in which the 0-cusp is rational.

Let $J_{r/\mathbb{Q}}$ be the Jacobian of X_r and let $Ta_p(J_r)$ be the p-adic Tate module of J_r.

Remark 2.6.4. the Hecke algebra $\mathcal{H}$ acts on J_r, and hence also on $Ta_p(J_r)$, by letting $\mathbb{Z}_p^\times$ act via the Nebentype operators and T_n act via the nth (covariant) Hecke correspondence. For each pair of integers $r_1 \geq r_2 > 0$, the natural projection $X_1(Np^{r_1}) \to X_1(Np^{r_2})$ induces a Galois equivariant map of Tate modules $Ta_p(J_{r_1}) \to Ta_p(J_{r_2})$ which commutes with the action of $\mathcal{H}$, hence we may form the projective limit and obtain an $\mathcal{H}[G_\mathbb{Q}]$-module

$$Ta_p(J_\infty) := \varprojlim_r T_p(J_r)$$

Proposition 2.6.5. *There is a canonical decomposition into $\mathcal{H}[G_\mathbb{Q}]$-modules*

$$Ta_p(J_\infty) = Ta_p(J_\infty)^0 \oplus Ta_p(J_\infty)^{nil}$$

such that the Hecke operator T_p acts invertibly on $Ta_p(J_\infty)^0$ and topologically nilpotently on $Ta_p(J_\infty)^{nil}$.

Moreover, $Ta_p(J_\infty)^0$ is a free Λ-module of finite rank.

If we set $t = [1+p] - 1 \in \Lambda$ or any other generator of the augmentation ideal then the following sequence is exact

$$0 \to Ta_p(J_\infty)^0 \xrightarrow{t} Ta_p(J_\infty)^0 \to Ta_p(J_1)^0 \to 0$$

Suppose that E is a modular elliptic curve of tame conductor N with either good ordinary or multiplicative reduction at the prime p and let $f_E = \sum_{n=1}^{\infty} a_n q^n$ be the associated p-stabilized ordinary newform, normalized so that $a_1 = 1$. Now define $\lambda_E : \mathcal{H} \to \mathbb{Z}_p$ by mapping $\mathbb{Z}_p^\times$ to 1 and each Hecke operator T_n to a_n. Let $\mathcal{H}$ act on the Tate module $Ta_p(E)$ via λ_E. Fix a modular parametrization $X_1 \to E$ and let $Ta_p(J_1)^0 \to Ta_p(E)$ be the induced homomorphism on Tate modules. This map commutes with the action of $G_\mathbb{Q}$ as well as with the action just defined for $\mathcal{H}$.

The following theorem due to Hida says that $Ta_p(E)$ can be lifted to an $\mathcal{H}$-eigenspace in $Ta_p(J_\infty)^0$.

Theorem 2.6.6. *There is an integral domain $\mathcal{R}_E$ finite and flat over Λ and a surjective Λ-homomorphism $h_E : \mathcal{H} \to \mathcal{R}_E$ as in the theorem 2.4.3. Let $\mathbb{T}_E \subset Ta_p(J_\infty)^0 \otimes_\Lambda \mathcal{R}_E$ be the $\mathcal{R}_E$-submodule consisting of elements on which $\mathcal{H}$ acts via h_E. Then $\mathbb{T}_E$ has rank 2 as an $\mathcal{R}_E$-module (i.e. if $\mathcal{K}_E$ is the fraction field of $\mathcal{R}_E$, then $\mathbb{T}_E \otimes_{\mathcal{R}_E} \mathcal{K}_E$ has dimension 2 over $\mathcal{K}_E$).*

CHAPTER 3

$\mathcal{L}$-invariant

Let E be a modular elliptic curve with split multiplicative reduction at the prime $p \geq 5$. Let $\mathbf{f} = \sum_{n=1}^{\infty} \alpha_n(k) q^n \in \mathcal{A}_U[[q]]$ be the analytic family of q-expansions given by Hida's theorem deforming the modular form f_E of weight 2 associated to E. In this chapter we prove the result establishing a connection between the pth coefficient of $\mathbf{f}$ and the $\mathcal{L}$-invariant of E, using local deformation theory.

3.1 Galois Cohomology

We recall the basics of Galois Cohomology without proof which are used frequently in this chapter and the next one. The main references for this topic are [Ser97] and [Neu08]

Let G be a profinite group and A a topological G-module, i.e., a topological abelian group with a continuous action of G, compatible with the abelian group structure. Let B be another G-module, then a map $f : A \to B$ is called a morphism of G-modules if f is both a countinuous group homomorphism and G-equivariant, i.e.,

$$f(a + a') = f(a) + f(a'), \quad \forall a, a' \in A$$
$$f(a^\sigma) = f(a)^\sigma, \quad \forall \sigma \in G, a \in A$$

For every $n \in \mathbb{N}$, define $C^n = C^n(G, A)$ to be the set of continuous maps from G^n to A, where G^0 is the trivial group, so $C^0 = A$. The elements in C^n are called n-cochains. Let

$$d^n : C^n \to C^{n+1}$$

be given by

$$\begin{aligned} d^n(f)(\sigma_1,...,\sigma_{n+1}) = \sigma_1 f(\sigma_2,..,\sigma_{n+1}) + \\ + \sum_{i=1}^{n}(-1)^i f(\sigma_1,...,\sigma_i\sigma_{i+1},...,\sigma_{n+1}) \\ + (-1)^{n+1} f(\sigma_1,...,\sigma_n) \end{aligned}$$

for all $n \geq 1$, we have $d^n \circ d^{n-1} = 0$, therefore $Im(d^n) \subseteq \ker(d^{n+1})$, that is, we get a complex $C^\bullet(G, A)$.

Definition 3.1.1. For $n \in \mathbb{N}$, the n-th continuous cohomology group of G with coefficients in A is the quotient group

$$H^n(G, A) = \ker(d^n)/\mathrm{Im}(d^{n-1})$$

where we set $\mathrm{Im}(d^{-1}) = 0$. Elements in $\ker(d^n)$ are called continuous cocycles, while elements of $\mathrm{Im}(d^{n-1})$ are called continuous coboundaries.

We can give explicit description for $H^n(G, A)$ with $n = 0, 1$.

$$H^0(G, A) = A^G = \{a \in A | \sigma a = a, \ \ \forall \sigma \in G\}$$
$$H^1(G, A) = \frac{\{f : G \to A \text{ continuous} | f(\sigma\tau) = f(\sigma) + f(\tau)^\sigma, \ \ \forall \sigma, \tau \in G\}}{\{f : G \to A | f(\sigma) = \sigma a - a \ \text{ for a fixed } a \in A\}}$$

Remark 3.1.2. When the action of G on A is trivial, i.e., $\sigma a = a$ for all $\sigma \in G$ and $a \in A$, then $H^0(G, A) = A$ and $H^1(G, A) = \mathrm{Hom}(G, A)$, where the homomorphisms between topological groups are always assumed to be continuous.

Theorem 3.1.3. *Let $0 \to A \to B \to C \to 0$ be a short exact sequence topological of G-modules, split as sequence of topological abelian groups. Then we have a long exact sequence of cohomology groups*

$$\begin{aligned} 0 \to & A^G \to B^G \to C^G \to H^1(G, A) \to \cdots \\ & \cdots \to H^n(G, B) \to H^n(G, C) \to H^{n+1}(G, A) \to \cdots \end{aligned}$$

Suppose that H is a subgroup of G, then any G-module is an H-module. Moreover, if $\xi : G \to A$ is a 1-cochain, then by restricting the domain of ξ to H, we obtain an H-to-A cochain. In this way we obtain a restriction homomorphism

$$\mathrm{res} : H^1(G, A) \to H^1(H, A)$$

We will define a homomorphism $H^i(H,A) \to H^i(G,A)$ in the opposite direction of the restriction, which is a kind of norm map and is called the corestriction. It arises from the standard resolution $A \to X^\bullet = X^\bullet(G,A)$ of the G-module A, which is also an acyclic resolution of A as an H-module,i.e

$$H^n(H,A) = H^n((X^\bullet)^H)$$

For $n \geq 0$, we have for the G-module X^n the norm map

$$N_{G/H} : (X^n)^H \to (X^n)^G$$

It commutes with d, hence we have a morphism of complexes

$$N_{G/H} : (X^\bullet)^H \to (X^\bullet)^G$$

Taking cohomology groups of these complexes, we obtain canonical homomorphisms

$$\text{cores} : H^n(H,A) \to H^n(G,A)$$

Assume further that H is a normal subgroup of G. Then the submodule A^H of A consisting of elements fixed by H has a natural structure as a G/H-module. Let $\xi : G/H \to A^H$ be a 1-cochain, one compose this with the projection $G \to G/H$ and with the inclusion $A^H \subset A$ give a G-to-A cochain

$$G \to G/H \xrightarrow{\xi} A^H \subset A$$

In this way we have an inflation homomorphism

$$\text{inf} : H^1(G/H, A^H) \to H^1(G,A)$$

Theorem 3.1.4. *Let A be a G-module and let H be a normal subgroup of G. Then the following sequence is exact*

$$0 \to H^1(G/H, A^H) \xrightarrow{inf} H^1(G,M) \xrightarrow{res} H^1(H,M)$$

Definition 3.1.5. Let H be a closed subgroup of G. For every H-module A, define the G-module $\text{Ind}_G^H(A)$ consisting of all continuous maps $f : G \to A$ such that $f(\tau\sigma) = \tau f(\sigma)$ for all $\tau \in H$. The action of $\rho \in G$ on $\text{Ind}_G^H(A)$ is given by

$$f(\sigma) \mapsto (\rho f)(\sigma) = f(\sigma\rho)$$

We have a canonical projection

$$\pi : \mathrm{Ind}_G^H(A) \to A$$
$$f \mapsto f(1)$$

This is a homomorphism of H-modules, which maps the H-submodule

$$A' = \{f : G \to A | f(\tau) = 0];\ \forall \tau \notin H\} \simeq A$$

If A is a G-module, then $\mathrm{Ind}_G^H(A)$ is canonically isomorphic to the G-module $Map(G/H, A)$ of all continuous functions $g : G/H \to A$. The isomorphism

$$\mathrm{Ind}_G^H(A) \simeq Map(G/H, A)$$

We have the following well-known result due to Shapiro

Theorem 3.1.6. *(Shapiro's Lemma) Let H be a closed subgroup of G and let A be an H-module . Then for all $i \geq 0$ we have a canonical isomorphism*

$$H^i(G, \mathrm{Ind}_G^H(A)) \simeq H^1(H, A)$$

Proposition 3.1.7. *Let K be a local field and $G = \mathrm{Gal}(K_S/K)$. If A is a G-module which is finite (resp. finitely generated over $\mathbb{Z}_p$), then $H^n(G, A)$ is finite (resp. finitely generated over $\mathbb{Z}_p$).*

Theorem 3.1.8. *Let G be a profinite group and A a G-module. Suppose that $A = \varinjlim A_i$, where each A_i is a finite (discrete) G-module. If $H^{n-1}(G, A_i)$ is finite for every i, then there is an isomorphism*

$$H^n(G, A) \simeq \varprojlim H^n(G, A_i)$$

Definition 3.1.9. Given G-modules A, A' and B, a map

$$A \times A' \xrightarrow{\phi} B$$

is a G-pairing if it is bilinear and it respects the action of G:

$$\phi(a^\sigma, a'^\sigma) = \phi(a, a')^\sigma$$

for all $\sigma \in G, a \in A, a' \in A'$.

If A and A' are two G-modules, then $A \otimes_{\mathbb{Z}} A'$ is also a G-module by $\sigma(a \otimes b) = \sigma a \otimes \sigma b$. The bilinear map $A \times A' \to A \otimes_{\mathbb{Z}} A'$ is a G-paring. Note that by the universal property of tensor products, any bilinear paring of G-modules $A \times A' \to B$ factors through $A \otimes A'$.

Such a pairing induces a map

$$\cup : C^r(G, A) \times C^s(G, A') \to C^{r+s}(G, B)$$

as follows: given $f \in C^r(G, A)$ and $f' \in C^r(G, A')$, the cochain $f \cup f' \in C^{r+s}(G, A)$ is defined by

$$(f \cup f')(\sigma_1, ..., \sigma_{r+s}) = \phi\left(f(\sigma_1, .., \sigma_r), f'(\sigma_{r+1}, ..., \sigma_{r+s})\right)$$

We see that

$$d^{r+s}(f \cup f') = d^r(f) \cup f' + (-1)^r f \cup d^s(f')$$

hence it yields a bilinear cup product, again denoted by $\cup$

$$\cup : H^r(G, A) \times H^s(G, A') \to H^{r+s}(G, B)$$

Proposition 3.1.10. *For two homomorphisms $A \to B$ and $A' \to B'$ of G-modules, we have the commutative diagram*

$$\begin{array}{ccccc} H^r(G, A) & \times & H^s(G, A') & \xrightarrow{\cup} & H^{r+s}(G, A \otimes A') \\ \downarrow & & \downarrow & & \downarrow \\ H^r(G, B) & \times & H^s(G, B') & \xrightarrow{\cup} & H^{r+s}(G, B \otimes B') \end{array}$$

Proposition 3.1.11. *Let $0 \to A' \to A \to A'' \to 0$ and $0 \to B' \to B \to B'' \to 0$ be exact sequences of G-modules. Suppose that we are given a pairing*

$$\varphi : A \times B \to C$$

into a G-module C such that $\varphi(A' \times B') = 0$. Then we have the following commutative diagram

$$\begin{array}{ccccc} H^r(G, A'') & \times & H^s(G, B') & \xrightarrow{\cup} & H^{r+s}(G, C) \\ \downarrow{\scriptstyle \delta} & & \uparrow{\scriptstyle \delta} & & \downarrow{\scriptstyle (-1)^{r+1}} \\ H^{r+1}(G, A') & \times & H^{s-1}(G, B'') & \xrightarrow{\cup} & H^{r+s}(G, C) \end{array}$$

where δ is the connecting homomorphism.

3.2 Main Correspondence

Definition 3.2.1. A $\mathbb{Q}_p$-vector space W is called a $\mathbb{Q}_p[G_{\mathbb{Q}_p}]$-module if $G_{\mathbb{Q}_p}$ acts continuously on W.

Theorem 3.2.2. *For any $\mathbb{Q}_p[G_{\mathbb{Q}_p}]$-module W, there is a one-to-one correspondence*

$$\left\{\textit{non-trivial continuous extensions of } \mathbb{Q}_p \textit{ by } W\right\} \leftrightarrow \left\{\textit{one-dimensional subspaces of } H^1(W)\right\}$$

where $H^n(-)$ denotes cohomology with respect to the group $G_{\mathbb{Q}_p}$.

Proof. Suppose that we have an extension X of $\mathbb{Q}_p$ by W, i.e, a short exact sequence of $G_{\mathbb{Q}_p}$-modules

$$0 \to W \to X \to \mathbb{Q}_p \to 0 \tag{3.2.1}$$

Note that $\mathbb{Q}_p^{G_{\mathbb{Q}_p}} = \mathbb{Q}_p$, taking Galois cohomology we obtain

$$0 \to W^{G_{\mathbb{Q}_p}} \xrightarrow{\phi} X^{G_{\mathbb{Q}_p}} \xrightarrow{\psi} \mathbb{Q}_p \xrightarrow{d} H^1(G_{\mathbb{Q}_p}, W) \to \cdots \tag{3.2.2}$$

$\Rightarrow$ Suppose that we have a non-split extension X of $\mathbb{Q}_p$ by W. If $d \neq 0$, then the image of d is an one-dimensional subspace in $H^1(G_{\mathbb{Q}_p}, W)$. Assume that $d = 0$, we have the following exact sequence

$$0 \to W^{G_{\mathbb{Q}_p}} \to X^{G_{\mathbb{Q}_p}} \to \mathbb{Q}_p \to 0$$

It follows that there exits $x \in X^{G_{\mathbb{Q}_p}}$ such that $\psi(x) = 1 \in \mathbb{Q}_p$, so we can define $s : \mathbb{Q}_p \to X$ by $s(q) = qx$. We see that s is $G_{\mathbb{Q}_p}$-homomorphism: for all $\sigma \in G_{\mathbb{Q}_p}$ we have

$$s(q^\sigma) = q^\sigma x = q^\sigma x^\sigma = (qx)^\sigma = s(q)^\sigma$$

and $\psi \circ s = Id_{\mathbb{Q}_p}$: for all $q\mathbb{Q}_p$ we have

$$\psi \circ s(q) = \psi(qx) = q\psi(x) = q \cdot 1 = q$$

Hence the exact sequence 3.2.1 is split.

$\Leftarrow$ Suppose that $\xi : G_{\mathbb{Q}_p} \to W$ be a non-zero 1-cocycle, i.e., a continuous map $G_{\mathbb{Q}_p} \to W$ satisfying $\xi(\sigma\tau) = \xi(\sigma) + \xi(\tau)^\sigma$ for all $\sigma, \tau \in G(\mathbb{Q}_p)$. We define $X = W \oplus \mathbb{Q}_p$ together with the action of $G_{\mathbb{Q}_p}$ given by

$$(w, q)^\sigma = (w^\sigma + q\xi(\sigma), q)$$

We see that this is indeed an act of $G_{\mathbb{Q}_p}$ on X: note that $\xi(Id) = 0$ by the equation determined the 1-cocycle

$$(w, q)^{Id} = (w^{Id} + q\xi(Id), q) = (w, q)$$

and for all $\sigma_1, \sigma_2 \in G_{\mathbb{Q}_p}$ we have

$$\begin{aligned}
\big((w, q)^{\sigma_1}\big)^{\sigma_2} &= \big((w^{\sigma_1} + q\xi(\sigma_1), q)\big)^{\sigma_2} \\
&= \big((w^{\sigma_1} + q\xi(\sigma_1))^{\sigma_2} + q\xi(\sigma_2), q\big) \\
&= \big(w^{\sigma_1\sigma_2} + q^{\sigma_2}\xi(\sigma_1)^{\sigma_2} + q\xi(\sigma_2), q\big) \\
&= \big(w^{\sigma_1\sigma_2} + q\xi(\sigma_1)^{\sigma_2} + q\xi(\sigma_2), q\big) \\
&= \big(w^{\sigma_1\sigma_2} + q\xi(\sigma_1\sigma_2), q\big) \\
&= (w, q)^{\sigma_1\sigma_2}
\end{aligned}$$

We define the $G_{\mathbb{Q}_p}$-homomorphisms $\phi : W \to X$ by $w \mapsto (w, 0)$ and $\psi : X \to \mathbb{Q}_p$ by $(w, q) \mapsto q$. Then we have an exact sequence of $G_{\mathbb{Q}_p}$-modules

$$0 \to W \to X \to \mathbb{Q}_p \to 0$$

Assume that the class $[\xi]$ of ξ in $H^1(G_{\mathbb{Q}_p}, W)$ is nonzero. If the exact sequence is non-split then we are done. Otherwise, suppose that the sequence is split, then there is a section $s : \mathbb{Q}_p \to X$ such that $\psi \circ s = Id_{\mathbb{Q}_p}$ as $G_{\mathbb{Q}_p}$-homomorphism. Let $s(1) = (w, q) \in X$ we have $1 = \psi \circ s(1) = \psi(w, q) = q$. Moreover,

$$(w, 1) = s(1) = s(1^\sigma) = s(1)^\sigma = (w, 1)^\sigma = (w^\sigma + \xi(\sigma), 1)$$

Hence $\xi(\sigma) = w - w^\sigma$ implies $[\xi] = 0$ a contradiction.

We have constructed two maps between non-trivial extensions of $\mathbb{Q}_p$ by W and one-dimensional subspaces of $H^1(W)$. We claim that they are inverse of each other.

Suppose that we have a non-split exact sequence

$$0 \to W \to X \to \mathbb{Q}_p \to 0$$

we obtain a one-dimensional subspace of $H^1(G_{\mathbb{Q}_p}, W)$ given by the image of the connecting homomorphism $d : \mathbb{Q}_p \to H^1(G_{\mathbb{Q}_p}, W)$. Let $\xi : G_{\mathbb{Q}_p} \to W$ be the 1-cocycle generating this line in $H^1(G_{\mathbb{Q}_p}, W)$. Then we can construct the non-split exact sequence of $G_{\mathbb{Q}_p}$-modules by ξ

$$0 \to W \to W \oplus \mathbb{Q}_p \to \mathbb{Q}_p \to 0$$

with the action on $W \oplus \mathbb{Q}_p$ given by $(w^\sigma + q\xi(\sigma), q)$. We claim that this exact sequence is isomorphic to the given one. That is the following diagram is commutative as $G_{\mathbb{Q}_p}$-homomorphism

$$\begin{array}{ccccccccc} 0 & \longrightarrow & W & \longrightarrow & X & \longrightarrow & \mathbb{Q}_p & \longrightarrow & 0 \\ & & \downarrow Id & & \downarrow f & & \downarrow Id & & \\ 0 & \longrightarrow & W & \longrightarrow & W \oplus \mathbb{Q}_p & \longrightarrow & \mathbb{Q}_p & \longrightarrow & 0 \end{array}$$

and $f : X \to W \oplus \mathbb{Q}_p$ defined by $f(x) = \big(\phi^{-1}(x), \psi(x)\big)$ is an isomorphism as $G_{\mathbb{Q}_p}$-homomorphism. Indeed, for all $w \in W$ we have

$$f \circ \phi(w) = \big(\phi^{-1}(\phi(w))^\sigma, \psi(\phi(w))\big) = \big(w^\sigma, 0) = \phi' \circ Id(w)\big)$$

Also, we see that $f(x^\sigma) = \big(\phi^{-1}(x^\sigma), \psi(x^\sigma)\big)$ and $f(x)^\sigma = \big(\phi^{-1}(x)^\sigma + \psi(x)\xi(\sigma), \psi(x)\big)$. Note that

$$\phi\left(\phi^{-1}(x)^\sigma + \psi(x)\xi(\sigma)\right) = \phi(\phi^{-1}(x)^\sigma) + \phi(\psi(x)\xi(\sigma)) = x^\sigma + \psi(x)\phi(\xi(\sigma)) = x^\sigma$$

as $\phi(\xi(\sigma)) = 0$. Hence f is a $G_{\mathbb{Q}_p}$-homomorphism. Moreover, it follows the injectivity of ϕ and surjectivity of ψ we obtain that f is a bijection.

Conversely, suppose that we have a non-zero 1-cocycle $\xi : G_{\mathbb{Q}_p} \to W$ representing a non-zero class in $H^1(G_{\mathbb{Q}_p}, W)$. We can construct a non-split exact sequence

$$0 \to W \to X \to \mathbb{Q}_p \to 0$$

where $X = W \oplus \mathbb{Q}_p$ with the action defined above. Then we have a connecting homomorphism $d : \mathbb{Q}_p \to H^1(G_{\mathbb{Q}_p}, W)$ defines one-dimensional subspace of $H^1(G_{\mathbb{Q}_p}, W)$. Since the exact sequence $0 \to W \to X \to \mathbb{Q}_p \to 0$ is non-split, by the claim of the previous part we have seen that there is no $w \in W$ such that $\xi(\sigma) = w^\sigma - w$, i.e., $0 \neq \xi \in Im\ d$. Thus the subspace determined by ξ and the subspace given by d are the same. □

3.3 Kummer Theory

3.3.1 Kummer Classes

Theorem 3.3.1. *(Hilbert 90) Let L/K be a Galois extension with Galois group* $\mathrm{Gal}(L/K)$ *and $L^\times$ be the multiplicative group of L. Then*

$$H^1(\mathrm{Gal}(L/K), L^\times) = \{1\}$$

Proof. Refer [Bir67] □

Consider the map $\psi : (\overline{\mathbb{Q}_p})^\times \to (\overline{\mathbb{Q}_p})^\times$ given by $q \mapsto q^{p^n}$. The kernel of this map is the group of the p^n-th roots of unity μ_{p^n}. Here we have the action of $G_{\mathbb{Q}_p}$ on μ_{p^n} given by $\epsilon^\sigma = \sigma(\epsilon)$ for $\epsilon \in \mu_{p^n}$ and $\sigma \in G_{\mathbb{Q}_p}$. Hence we have the following exact sequence of $G_{\mathbb{Q}_p}$-modules

$$1 \to \mu_{p^n} \to (\overline{\mathbb{Q}_p})^\times \xrightarrow{p^n} (\overline{\mathbb{Q}_p})^\times \to 1$$

Using Hilbert 90 theorem and observing that $\mu_{p^n}^{G_{\mathbb{Q}_p}} = \{1\}$, we obtain the following exact sequence

$$1 \to \mathbb{Q}_p^\times \xrightarrow{p^n} \mathbb{Q}_p^\times \to H^1(G_{\mathbb{Q}_p}, \mu_{p^n}) \to 1$$

Hence the connecting homomorphism $d : \mathbb{Q}_p^\times \to H^1(G_{\mathbb{Q}_p}, \mu_{p^n})$ induces an isomorphism

$$\mathbb{Q}_p^\times / \left(\mathbb{Q}_p^\times\right)^{p^n} \simeq H^1(G_{\mathbb{Q}_p}, \mu_{p^n}).$$

Hence for every $q \in \mathbb{Q}_p^\times$ we can define a class in $H^1(G_{\mathbb{Q}_p}, \mu_{p^n})$ via this isomorphism. More precisely choosing a compatible sequence $(q^{1/p^n})_n$ of p-power root of q, by the definition of connecting map, we have $\xi_n : G_{\mathbb{Q}_p} \to \mu_{p^n}$ given by $\sigma \mapsto (q^{1/p^n})_n^{\sigma-1}$.

Proposition 3.3.2. *We have* $\mathbb{Q}_p^\times \simeq \mathbb{Z} \times \mathbb{Z}_p^\times \simeq \mathbb{Z} \times \mu_{p-1} \times (1 + p\mathbb{Z}_p)$

Proof. Refer [Ser79] □

It follows that $(\mathbb{Q}_p^\times)^{p^n} \simeq p^n\mathbb{Z} \times \mu_{p-1} \times (1 + p^n\mathbb{Z}_p)$. Note that $1 + p^n\mathbb{Z}_p \simeq p^n\mathbb{Z}_p$, hence

$$\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^{p^n} \simeq \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^{n-1}\mathbb{Z}$$

Taking projective limit we obtain

$$H^1(G_{\mathbb{Q}_p}, \varprojlim \mu_{p^n}) \simeq \varprojlim H^1(G_{\mathbb{Q}_p}, \mu_{p^n}) \simeq \varprojlim \mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^{p^n} \simeq \mathbb{Z}_p \times \mathbb{Z}_p$$

Remark 3.3.3. We have $\mu_{p^n} \simeq \mathbb{Z}/p^n\mathbb{Z}$ as abelian groups but with different actions of $G_{\mathbb{Q}_p}$ ($G_{\mathbb{Q}_p}$ acts trivially on $\mathbb{Z}/p^n\mathbb{Z}$). Hence $\varprojlim \mu_{p^n} \simeq \mathbb{Z}_p$ as abelian group and we denote $\varprojlim \mu_{p^n}$ by $\mathbb{Z}_p(1)$ with the defined action.

Tensoring with $\mathbb{Q}_p$ and denoting $\mathbb{Z}_p(1) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p := \mathbb{Q}_p(1)$ we obtain the following isomorphism

$$H^1(G_{\mathbb{Q}_p}, \mathbb{Q}_p(1)) \simeq (\mathbb{Z}_p \times Z_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

Thus each $q \in \mathbb{Q}_p^\times$ determines a cohomology class $\gamma_q \in H^1(\mathbb{Q}_p(1))$ by taking projective limit of ξ_n, i.e.,

$$\gamma_q(\sigma) = \varprojlim \xi_n(\sigma)$$

We call the class γ_q the Kummer class associated to $q \in \mathbb{Q}_p^\times$.

3.3.2 Tate Module

Definition 3.3.4. Let E an elliptic curve and $E[p^n]$ be the kernel of $[p^n] : E \to E$. We define the Tate module of E is the inverse limit $Ta_p(E) := \varprojlim E[p^n]$.

We denote by $V(E) := Ta_p(E) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

Suppose that $E/\mathbb{Q}_p$ has the split reduction at p, then we have the isomorphism

$$E(\overline{\mathbb{Q}_p}) \simeq \overline{\mathbb{Q}_p}^\times / q_E^{\mathbb{Z}}$$

Since $1 = q_E^0 \in q_E^{\mathbb{Z}}$, by this isomorphism we see that $\mu_{p^n} \subset E[p^n]$. On the other hand, if $z \in E[p^n]$ then $z^{p^n} \in q_E^{\mathbb{Z}}$. That is there is $c \in \mathbb{Z}$ such that $z^{p^n} = q_E^c$. We associate to z the image of $c \mod \mathbb{Z}/p^n\mathbb{Z}$. Note that $z_1^{p^n} \cdot z_2^{p^n} = q_E^{c_1} \cdot q_E^{c_2} = q_E^{c_1+c_2}$. Furthermore, for all $\bar{c} \in \mathbb{Z}/p^n\mathbb{Z}$, let $c \in \mathbb{Z}$ be its representative. By the isomorphism $E(\overline{\mathbb{Q}_p}^\times) \simeq \overline{\mathbb{Q}_p}^\times / q_E^{\mathbb{Z}}$, we see that $q_E^c = 1$ in $E(\overline{\mathbb{Q}_p})$. Hence, there exits $z \in E[p^n]$ such that $z^{p^n} = (q_E^c)$. Thus, we have the following exact sequence

$$1 \to \mu_{p^n} \to E[p^n] \to \mathbb{Z}/p^n\mathbb{Z} \to 0$$

Note that $\{\mu_{p^n}\}_{n\in\mathbb{N}}$ is a surjective system, taking projective limit we have

$$1 \to \mathbb{Z}_p(1) \to Ta_p(E) \to \mathbb{Z}_p \to 0$$

Tensoring with $\mathbb{Q}_p$, since $\mathbb{Q}_p$ is a flat $\mathbb{Z}_p$-module we obtain the following exact sequence

$$1 \to \mathbb{Q}_p(1) \to V(E) \to \mathbb{Q}_p \to 0$$

Theorem 3.3.5. *Let E be an elliptic curve over $\mathbb{Q}_p$. Suppose that E has a split mutiplicative reduction at p. Let $q \in \mathbb{Q}_p^\times$ be any nontrivial element of the group $q_E^{\mathbb{Z}}$ of Tate period. Then the Kummer class γ_q associated to q spans the line in $H^1(\mathbb{Q}_p(1))$ associated to the extension*

$$1 \to \mathbb{Q}_p(1) \to V(E) \to \mathbb{Q}_p \to 0$$

Proof. Recall that for all $q \in q_E^{\mathbb{Z}}$, we have the 1-cocycle associated to q given by

$$\begin{aligned} q = q_E^c \mapsto &(\xi_n : G_{\mathbb{Q}_p} \to \mu_{p^n}) \\ &\sigma \mapsto \left(((q_E^c)^{1/p^n})_n\right)^{\sigma-1} \end{aligned}$$

The Kummer class, by definition, is $\gamma_q = \varprojlim \xi_n$.

On the other hands, the line in $H^1(G_{\mathbb{Q}_p}, \mu_{p^n})$ corresponding to the exact sequence

$$1 \to \mu_{p^n} \to E[p^n] \to \mathbb{Z}/p^n\mathbb{Z} \to 0$$

is given as follows: for all $\bar{c} \in \mathbb{Z}/p^n\mathbb{Z}$, let c be its representative. Then there exist $z = (q_E^c)^{1/p^n} \in E[p^n]$ such that $z^{p^n} = q_E^c$. The class in $H^1(G_{\mathbb{Q}_p}, \mu_{p^n})$ associated to this extension is hence given by

$$\begin{aligned} \psi_c : &G_{\mathbb{Q}_p} \to \mu_{p^n} \\ &\sigma \mapsto z^{\sigma-1} = \left((q_E^c)^{1/p^n}\right)^{\sigma-1} \end{aligned}$$

Thus we see that Kummer class γ_q associated to q spans the line in $H^1(\mathbb{Q}_p(1))$ associated to the extension

$$1 \to \mathbb{Q}_p(1) \to V(E) \to \mathbb{Q}_p \to 0$$

□

3.4 Infinitesimal Deformations

Let $\widetilde{\mathbb{Q}} := \mathbb{Q}_p[t]/t^2$ be the ring of polyomials over $\mathbb{Q}_p$ modulo t^2. We see that

$$\widetilde{\mathbb{Q}}_p = \{a + bt + (t^2) | a, b \in \mathbb{Q}_p\}$$

The valuation on $\tilde{\mathbb{Q}}_p$ is induced by the valuation v_p on $\mathbb{Q}_p$

$$v_{\widetilde{\mathbb{Q}}_p} : \widetilde{\mathbb{Q}}_p \to \mathbb{Z} \cup \{\infty\}$$
$$v_{\widetilde{\mathbb{Q}}_p}(a + bt) = \min(v_p(a), v_p(b))$$

Definition 3.4.1. Let V be a finite dimensional $\mathbb{Q}_p$-vector space with continuous $G_{\mathbb{Q}_p} := \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ action. We will say that a $\widetilde{\mathbb{Q}_p}$-module, $\widetilde{V}$, with $G_{\mathbb{Q}_p}$ action is an infinitesimal deformation of V if $\widetilde{V}$ is free as a $\widetilde{\mathbb{Q}_p}$-module and $\widetilde{V}/t\widetilde{V} \simeq V$ as a $G_{\mathbb{Q}_p}$-module.

It follows that $\widetilde{V}$ is a $\widetilde{\mathbb{Q}}_p$-flat module. Using the flatness of $\widetilde{V}$, we will show that $t\widetilde{V}$ is isomorphic to V.

Theorem 3.4.2. *Let A be a commutative ring and let M be an A-module. Then M is flat over A if and only if $I \otimes_A M \to A \otimes_A M$ is an injective homomorphism for every finitely generated ideal I of A.*

Proof. Refer [Ei95], theorem 6.1. □

Corollary 3.4.3. *Let k be a field and let $R := k[t]/(t^2)$ be the quotient ring of polynomials over k modulo (t^2). Let M be an R-module, then M is flat over R if and only if the map $M/tM \simeq tM$, $m + tM \mapsto tm$ is isomorphism.*

Proof. The only non-trivial ideal of A is (t), which is isomorphic as an R-module to $R/(t)$. Indeed, consider the R-homomorphism

$$f : R/(t) \to tR$$
$$r \mapsto rt$$

Since $(t^2) = 0$ in R, f is well-defined. Let $a+bt+(t^2) \in R$ and assume that $(a+bt+(t^2))t = 0$ then $at = 0 \in R$ as $t^2 = 0$ in R. It follows that $a \in (t)$, i.e., f is injective and hence bijective. Thus, by the above theorem, M is flat over R if and only if

$$M/tM \simeq R/(t) \otimes_R M \simeq (t) \otimes_R M \to R \otimes_R M = M$$

is injective, hence isomorphic. □

Proposition 3.4.4. *If $\widetilde{V}$ is an infinitesimal deformation of V, then $\widetilde{V}/t\widetilde{V}$ and $t\widetilde{V}$ are isomorphic to V. Hence $\widetilde{V}$ is an extension of V by V.*

Proof. By definition $\widetilde{V}/t\widetilde{V} \simeq V$. Since $\tilde{V}$ is free over $\widetilde{\mathbb{Q}}_p$, $\widetilde{V}$ is a $\widetilde{\mathbb{Q}}_p$-flat module, hence

$$V \simeq \widetilde{V}/t\widetilde{V} \simeq t\widetilde{V}$$

So we have an exact sequence of $G_{\mathbb{Q}_p}$-modules

$$0 \to V \to \widetilde{V} \to V \to 0$$

□

Lemma 3.4.5. *Let k be a field. Then $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + (x^n)$ is an unit of the quotient $k[x]/(x^n)$ if and only if $a_0 \neq 0$.*

Proof. If $a_0 = 0$ then $f(x) \in (x)$, so $f(x)$ is not a unit in $k[x]/(x^n)$. Conversely, suppose

$$f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}\ , \quad a_0 \neq 0$$

so $\gcd(x^n,\, f(x)) = 1$. Thus there exist $p(x),\, q(x) \in k[x]$ with $p(x)x^n + q(x)f(x) = 1$, and then

$$(f(x) + (x^n))(q(x) + (x^n)) = 1 + (x^n)$$

Thus $f(x)$ is a unit in $k[x]/(x^n)$. □

It follows that $\widetilde{\mathbb{Q}}_p^{\times} = \{a + bt + (t^2) | a, b \in \mathbb{Q}_p, a \neq 0\} = \mathbb{Q}_p^{\times} \cdot (1 + t\mathbb{Q}_p)$.

Definition 3.4.6. Let $\psi : G_{\mathbb{Q}_p} \to \widetilde{\mathbb{Q}_p}^{\times}$ be a nontrivial continuous Galois character. We denote by $\widetilde{\mathbb{Q}_p}(\psi)$ the vector space $\widetilde{\mathbb{Q}_p}$ with the action via ψ. That is

$$(a + bt)^{\sigma} := \psi(\sigma) \cdot (a + bt)$$

We will emphasis a nontrivial continuous Galois character $\psi : G_{\mathbb{Q}_p} \to \widetilde{\mathbb{Q}}_p^{\times}$ satisfying the congruence $\psi(\sigma) \equiv 1 \mod t$ for every $\sigma \in G_{\mathbb{Q}_p}$. That is the image of ψ lies inside $1 + t\mathbb{Q}_p$.

$$\psi(G_{\mathbb{Q}_p}) \subseteq 1 + t\mathbb{Q}_p$$

It follows that $\psi(\sigma) \cdot (a + bt) \equiv 1 \cdot a = a \mod t$. Note that the multiplicative group $(1 + t\mathbb{Q}_p, \cdot)$ is isomorphic to the additive group $(\mathbb{Q}_p, +)$ as topological groups.

Define the projection

$$\pi : \widetilde{\mathbb{Q}}_p(\psi) \to \mathbb{Q}_p$$
$$a + bt \mapsto a$$

We claim that π is a $G_{\mathbb{Q}_p}$-homomorphism. Indeed, we have

$$\pi((a+bt)^\sigma) = \pi(\psi(\sigma)\cdot(a+bt)) = a$$

On the other hand,

$$\pi(a+bt)^\sigma = a^\sigma = a$$

π is obviously surjective and its kernel is $t\mathbb{Q}_p$. Note that $G_{\mathbb{Q}_p}$ acts trivially on $t\mathbb{Q}_p$ because

$$(tx)^\sigma = \psi(\sigma)\cdot(tx) = tx$$

It follows that $t\mathbb{Q}_p \simeq \mathbb{Q}_p$ as $G_{\mathbb{Q}_p}$-modules via $tx \mapsto x$. Thus, we have an exact sequence as $G_{\mathbb{Q}_p}$- modules

$$0 \to t\mathbb{Q}_p \simeq \mathbb{Q}_p \longrightarrow \widetilde{\mathbb{Q}_p}(\psi) \xrightarrow{\pi} \mathbb{Q}_p \to 0$$
$$x \mapsto tx$$

We obtain $\widetilde{\mathbb{Q}}_p(\psi)$ is an infinitesimal deformation of $\mathbb{Q}_p$.

Proposition 3.4.7. *If $\psi : G_{\mathbb{Q}_p} \to \widetilde{\mathbb{Q}_p}^\times$ is a nontrivial continuous Galois character satisfying the congruence $\psi(\sigma) \equiv 1 \mod t$ for every $\sigma \in G_{\mathbb{Q}_p}$ then $\widetilde{\mathbb{Q}_p}(\psi)$ is an infinitesimal deformation of $\mathbb{Q}_p$. In particular, $\widetilde{\mathbb{Q}_p}(\psi)$ is a nonsplit extension of $\mathbb{Q}_p$ by $\mathbb{Q}_p$.*

Proof. We claim that the extension

$$0 \to \mathbb{Q}_p \longrightarrow \widetilde{\mathbb{Q}_p}(\psi) \xrightarrow{\pi} \mathbb{Q}_p \to 0$$

is non-split. Otherwise, let $s : \mathbb{Q}_p \to \widetilde{\mathbb{Q}_p}(\psi)$ be the section of π, i.e., a $G_{\mathbb{Q}_p}$-homomorphism satisfying $\pi \circ s = Id_{\mathbb{Q}_p}$. Let $s(1) \equiv a + bt$ then

$$1 = \pi(s(1)) = \pi(a+bt) = a$$

Moreover, since s is $G_{\mathbb{Q}_p}$-equivariant we obtain

$$1 + bt = s(1) = s(1^\sigma) = s(1)^\sigma = \psi(\sigma)\cdot(1+bt), \quad \forall \sigma \in G_{\mathbb{Q}_p}$$

As $1 + bt \in \widetilde{\mathbb{Q}_p}^\times$ we see that $\psi(\sigma) = 1$ for all $\sigma \in G_{\mathbb{Q}_p}$, a contradiction with the nontrivial property of ψ. Thus this extension is nonsplit as $G_{\mathbb{Q}_p}$-modules. □

This extension hence determines a line in $H^1(\mathbb{Q}_p)$. Note that $\psi(\sigma)\cdot(a+bt)=(a+bt)$ for all $\sigma\in G_{\mathbb{Q}_p}$ if only if $a=0$. It follows that

$$\widetilde{\mathbb{Q}_p}(\psi)^{G_{\mathbb{Q}_p}}=t\mathbb{Q}_p$$

Thus we obtain the following long exact sequence

$$0\to\mathbb{Q}_p\to\widetilde{\mathbb{Q}_p}(\psi)^{G_{\mathbb{Q}_p}}=t\mathbb{Q}_p\to\mathbb{Q}_p\xrightarrow{d}H^1(G_{\mathbb{Q}_p},\mathbb{Q}_p)\to\cdots$$

Note that the $G_{\mathbb{Q}_p}$-homomorphism $x\mapsto tx$ gives us $\mathbb{Q}_p\simeq t\mathbb{Q}_p$, so we have an inclusion $d:\mathbb{Q}_p\hookrightarrow H^1(G_{\mathbb{Q}_p},\mathbb{Q}_p)$ in which we obtain a 1-dimensional subspace in $H^1(\mathbb{Q}_p)$.

Differentiation with respect to t induces a continuous isomorphism

$$\begin{aligned}\frac{d}{dt}:1+t\mathbb{Q}_p&\to\mathbb{Q}_p\\ 1+bt&\mapsto b\end{aligned}$$

from the multiplicative subgroup $1+t\mathbb{Q}_p\subseteq\widetilde{\mathbb{Q}_p}$ to the additive group $\mathbb{Q}_p$. The composition of ψ with $\dfrac{d}{dt}$ is an nonzero additive character

$$\begin{aligned}\frac{d\psi}{dt}:G_{\mathbb{Q}_p}&\to\mathbb{Q}_p\\ \sigma&\mapsto\frac{d}{dt}(\psi(\sigma))=\frac{d}{dt}(1+bt)=b\end{aligned}$$

Since $G_{\mathbb{Q}_p}$ acts trivially on $\mathbb{Q}_p$, we have $H^1(G_{\mathbb{Q}_p},\mathbb{Q}_p)=\mathrm{Hom}(G_{\mathbb{Q}_p},\mathbb{Q}_p)$. Hence we may consider $\dfrac{d\psi}{dt}$ as a cohomology class in $H^1(G_{\mathbb{Q}_p},\mathbb{Q}_p)$.

Proposition 3.4.8. *The line $\mathbb{Q}_p\dfrac{d\psi}{dt}\subseteq H^1(G_{\mathbb{Q}_p},\mathbb{Q}_p)$ corresponds to the nontrivial extension*

$$0\to t\mathbb{Q}_p\to\widetilde{\mathbb{Q}_p}(\psi)\to\mathbb{Q}_p\to 0$$

Proof. We describe the image of the inclusion $d:\mathbb{Q}_p\hookrightarrow H^1(G_{\mathbb{Q}_p},\mathbb{Q}_p)$. Consider $1\in\mathbb{Q}_p$, then choose $1+bt\in\widetilde{\mathbb{Q}_p}$, then the image of 1 in $H^1(G_{\mathbb{Q}_p},\mathbb{Q}_p)$ is given by

$$\begin{aligned}d(1):G_{\mathbb{Q}_p}&\to t\mathbb{Q}_p\\ \sigma&\mapsto(1+bt)^\sigma-(1+bt)\end{aligned}$$

Let $\psi(\sigma)=1+b't\in 1+t\mathbb{Q}_p$ we have

$$(1+bt)^\sigma-(1+bt)\equiv(1+b't)(1+bt)-(1+bt)\equiv b't=\frac{d}{dt}(\psi(\sigma))\cdot t$$

Thus the line $d(\mathbb{Q}_p)$ is generated by $\dfrac{d\psi}{dt}$. □

Theorem 3.4.9. *The correspondence* $\widetilde{\mathbb{Q}_p}(\psi) \leftrightarrow \mathbb{Q}_p \dfrac{d\psi}{dt}$ *induces a one-one correspondence*

$$\begin{array}{c} \left\{ \textit{Nontrivial infinitesimal deformations of } \mathbb{Q}_p \right\} \\ \updownarrow \\ \left\{ \textit{One-dimensional subspaces of } H^1(\mathbb{Q}_p) \right\} \end{array}$$

Proof. We have seen that every nontrivial infinitesimal deformation of $\mathbb{Q}_p$ induces a 1-dimensional subspace of $H^1(G_{\mathbb{Q}_p}, \mathbb{Q}_p)$ via the connecting homomorphism.

Suppose we have a 1-dimensional $\mathbb{Q}_p$ vector space in $H^1(G_{\mathbb{Q}_p}, \mathbb{Q}_p)$ generated by $0 \neq [\gamma] \in H^1(G_{\mathbb{Q}_p}, \mathbb{Q}_p)$. Let γ denote the 1-cocycle representive of $[\gamma]$, then $\gamma : G_{\mathbb{Q}_p} \to \mathbb{Q}_p$ is a continuous group homomorphism since $G_{\mathbb{Q}_p}$ act trivially on $\mathbb{Q}_p$. Compose this homomorphism with the continuous group isomorphism $(\mathbb{Q}_p, +) \simeq (1 + t\mathbb{Q}_p, \cdot)$ we obtain a character

$$\psi : G_{\mathbb{Q}_p} \xrightarrow{\gamma} \mathbb{Q}_p \xrightarrow{\simeq} 1 + t\mathbb{Q}_p$$

It gives rise an infinitesimal deformation $\widetilde{\mathbb{Q}_p}(\psi)$ of $\mathbb{Q}_p$

$$0 \to \mathbb{Q}_p \to \widetilde{\mathbb{Q}_p}(\psi) \to \mathbb{Q}_p \to 0$$

Let X be a nontrivial infinitesimal deformation of $\mathbb{Q}_p$. Then we have the following extension

$$0 \to \mathbb{Q}_p \to X \to \mathbb{Q}_p \to 0$$

Then X is isomorphic to $\widetilde{\mathbb{Q}_p}(\psi)$ in the sense that we have the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Q}_p & \longrightarrow & X & \longrightarrow & \mathbb{Q}_p & \longrightarrow & 0 \\ & & \downarrow Id & & \downarrow \simeq & & \downarrow Id & & \\ 0 & \longrightarrow & \mathbb{Q}_p & \longrightarrow & \tilde{\mathbb{Q}}_p(\psi) & \longrightarrow & \mathbb{Q}_p & \longrightarrow & 0 \end{array}$$

□

3.5 Tate Duality

3.5.1 The Brauer Group

Before we state Tate's local duality, we study the Brauer group following [Ser67].

Definition 3.5.1. Let k be a field with absolute Galois group $G_k = \mathrm{Gal}(\overline{k}/k)$. The Brauer group of k is the cohomology group $H^2(G_k, \overline{k}^\times)$. We denote it by $\mathrm{Br}(k)$

Thus $Br(k)$ is the inductive limit of the groups $\mathrm{Br}(L/k) := H^2(\mathrm{Gal}(L/k), L^\times)$ for L/k a finite Galois extension. Note that if K is an extension of k, we have a homomorphism $\mathrm{Br}(k) \to \mathrm{Br}(K)$, induced by the natural morphism $G_K \to G_k$ and the inclusion $\overline{k}^\times \to \overline{K}^\times$.

Recall the Kummer exact sequence

$$1 \to \mu_n \to \overline{k}^\times \xrightarrow{\cdot^n} \overline{k}^\times \to 1$$

Using Hilber90 theorem we obtain

Proposition 3.5.2. *Let n be an integer which is invertible in k. Then*

$$H^2(k, \mu_n) = (\mathrm{Br}\, k)[n]$$

where $(\mathrm{Br}\, k)[n] := \ker\left(H^2(G_k, \overline{k}^\times) \xrightarrow{\cdot^n} \ker(H^2(G_k, \overline{k}^\times\right)$

Let K be a local field and K_{nr} be its maximal unramified extension. The Galois group $G_{nr} := \mathrm{Gal}(K_{nr}/K)$ is isomorphic to $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$ which is topologically generated by the Frobenius. We can identify the Brauer group of K with the cohomology group $H^2(G_{nr}, K_{nr}^\times)$.

Theorem 3.5.3. *Let K be a local field. Then we have an isomorphism*

$$\mathrm{Br}(K) \simeq H^2(G_{nr}, K_{nr}^\times)$$

Theorem 3.5.4. *The valuation map $v : K_{nr}^\times \to \mathbb{Z}$ defines an isomorphism*

$$H^2(G_{nr}, K_{nr}^\times) \simeq H^2(\widehat{\mathbb{Z}}, \mathbb{Z})$$

Now consider the exact sequence of G-modules

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

The module $\mathbb{Q}$ has trivial cohomology since it is uniquely divisible (i.e., $\mathbb{Z}$-injective). Hence the coboundary $\delta : H^1(\mathbb{Q}/\mathbb{Z}) \to H^2(\mathbb{Z})$ yields an isomorphism

$$\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \simeq H^1(\mathbb{Q}/\mathbb{Z}) \simeq H^2(G, \mathbb{Z})$$

Let $\phi \in \mathrm{Hom}(\widehat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z})$ and define a map

$$\begin{aligned} \gamma : \mathrm{Hom}(\widehat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) &\to \mathbb{Q}/\mathbb{Z} \\ \phi &\mapsto \phi(1) \end{aligned}$$

Thus we have isomorphisms

$$H^2(G_{nr}, K_{nr}^\times) \xrightarrow{v} H^2(\widehat{\mathbb{Z}}, \mathbb{Z}) \xrightarrow{\delta^{-1}} \mathrm{Hom}(\widehat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\gamma} \mathbb{Q}/\mathbb{Z}$$

The map $\mathrm{inv}_K : H^2(G_{nr}, K_{nr}^\times) \to \mathbb{Q}/\mathbb{Z}$ is defined by $\mathrm{inv}_K = \gamma \circ \delta^{-1} \circ v$.

Theorem 3.5.5. *Let K be a local field. Then we have an isomorphism*

$$\mathrm{inv}_K : \mathrm{Br}\, K \to \mathbb{Q}/\mathbb{Z}$$

Recall the Kummer sequence in local case

$$1 \to \mu_{p^n} \to \overline{\mathbb{Q}_p}^\times \xrightarrow{p^n} \overline{\mathbb{Q}}_p^\times \to 1$$

Note that the $G_{\mathbb{Q}_p}$ is of strict cohomological dimension 2, so $H^i(G_{\mathbb{Q}_p}, \overline{\mathbb{Q}_p}^\times) = 1$ for all $i \geq 2$. By Hilbert90, we have $H^1(G_{\mathbb{Q}_p}, \overline{\mathbb{Q}}_p^\times) = \{1\}$ and have already proved that $H^1(G_{\mathbb{Q}_p}, \mu_{p^n}) = \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^n$. Taking cohomology we obtain the following exact sequence

$$1 \to \mathbb{Q}_p^\times \to \mathbb{Q}_p^\times \to H^1(G_{\mathbb{Q}_p}, \mu_{p^n}) \to H^1(G_{\mathbb{Q}_p}, \overline{\mathbb{Q}_p}) \to H^1(G_{\mathbb{Q}_p}, \overline{\mathbb{Q}_p}) \to H^2(G_{\mathbb{Q}_p}, \mu_{p^n}) \to 1$$

Now we can use the Brauer group to compute $H^2(G_{\mathbb{Q}_p}, \mu_{p^n})$.

Proposition 3.5.6. *We have $H^2(G_{\mathbb{Q}_p}, \mu_n) = \mathbb{Z}/n\mathbb{Z}$ and hence $H^2(G_{\mathbb{Q}_p}, \mathbb{Q}_p(1)) = \mathbb{Q}_p$.*

Proof. It follows that

$$H^2(G_{\mathbb{Q}_p}, \mu_{p^n}) = (Br\mathbb{Q}_p)[p^n] \simeq \mathbb{Z}/n\mathbb{Z}$$

Taking projective limit we obtain $H^2(\mathbb{Q}_p(1)) = \mathbb{Q}_p$ □

3.5.2 Tate Duality

Theorem 3.5.7. *(Tate local duality) The cup product induces a pairing*

$$\langle , \rangle : H^{2-i}(G_{\mathbb{Q}_p}, \mathbb{Q}_p(1)) \times H^i(, G_{\mathbb{Q}_p}\mathbb{Q}_p(1)^*) \to H^2(G_{\mathbb{Q}_p}, \mathbb{Q}_p(1)) = \mathbb{Q}_p$$

where $\mathbb{Q}_p(1)^* = \mathrm{Hom}(\mathbb{Q}_p(1), \mathbb{Q}_p(1))$.

The multiplication induces a perfect pairing

$$\begin{aligned} \mathbb{Q}_p(1) \times \mathbb{Q}_p &\to \mathbb{Q}_p(1) \\ (a, b) &\mapsto a \cdot b \end{aligned}$$

It follows that Tate duality gives us a perfect pairing

$$\langle , \rangle : H^{2-i}(G_{\mathbb{Q}_p}, \mathbb{Q}_p(1)) \times H^i(G_{\mathbb{Q}_p}, \mathbb{Q}_p) \to H^2(G_{\mathbb{Q}_p}, \mathbb{Q}_p(1)) = \mathbb{Q}_p$$

Hence a line in either one of the cohomology groups $H^1(\mathbb{Q}_p(1))$, $H^1(\mathbb{Q}_p)$ determines a line in the other one- namely, its orthogonal complement.

$$\begin{array}{ccc} \left\{\begin{array}{c}\text{Nontrivial infinitesimal deformations}\\ \mathbb{Q}_p(\psi) \text{ of } \mathbb{Q}_p\end{array}\right\} & \longleftrightarrow & \left\{\begin{array}{c}\text{One-dimensional subspaces}\\ \text{of } H^1(\mathbb{Q}_p)\end{array}\right\} \\ \updownarrow & & \updownarrow \\ \left\{\begin{array}{c}\text{Nontrivial extensions of}\\ \mathbb{Q}_p \text{ by } \mathbb{Q}_p(1)\end{array}\right\} & \longleftrightarrow & \left\{\begin{array}{c}\text{One-dimensional subspaces}\\ \text{of } H^1(\mathbb{Q}_p(1))\end{array}\right\} \end{array}$$

The main result in local class field theory is the following theorem.

Definition 3.5.8. Let L/K be a finite Galois extension of degree n. We call fundamental class of the extension L/K the unique element $u_{L/K}$ of $\mathrm{Br}(L/K) = H^2(Gal(L/K), L^*)$ such that $\mathrm{inv}_K(u_{L/K}) = 1/n \in \mathbb{Q}/\mathbb{Z}$.

Theorem 3.5.9. *Let L be a finite Galois extension of a local field K. Then the cup product with $u_{L/K}$ defines an isomorphism*

$$\theta_{L/K} : G^{ab} \to K^\times / N_{L/K}(L^\times)$$

where $G := \mathrm{Gal}(L/K)$. The isomorphism

$$\omega_{L/K} := \theta_{L/K}^{-1} : K^\times / N_{L/K}(L^\times) \to G^{ab}$$

is called the reciprocity map associated to the extension L/K.

The map $\sigma_{L/K} : K^\times \to K^\times/N_{L/K}(L^\times) \to G^{ab}$ given by $\alpha \mapsto \overline{\alpha} \mapsto \omega_{L/K}(\overline{\alpha})$ is called local Artin symbol associated to the extension L/K. We start with an $\alpha \in K^\times$ and will seek the image $\sigma_{L/K}(\alpha) \in G^{ab}$.

Let G be a finite group. The norm element of $\mathbb{Z}[G]$ is $N_G := \sum_{g\in G} g$. Let A be a G-module and let $N_G : A \to A$ be the G-module endomorphism $a \mapsto N_G a$. We then have $I_G A \subset \ker N_G$ where I_G is the augmentation ideal of $\mathbb{Z}[G]$. Moreover, $\operatorname{im} N_G \subseteq A^G$, thus N_G induces a morphism of trivial G-modules

$$\widehat{N}_G : A_G := A/I_G A \to A^G$$

Set $H_0(G, A) = A_G$, the functor $A \mapsto H_0(G, A)$ is covariant and right exact. We define the homology groups $H_i(G, A)$ as its left derived functor.

Definition 3.5.10. Let A be a G-module. For $n \geq 0$ the Tate cohomology and homology are defined by

$$\widehat{H}^n(G,A) := \begin{cases} \operatorname{coker} \widehat{N}_G & \text{for } n = 0 \\ H^n(G,A) & \text{for } n > 0 \end{cases} \quad \widehat{H}_n(G,A) := \begin{cases} \ker \widehat{N}_G & \text{for } n = 0 \\ H_n(G,A) & \text{for } n > 0 \end{cases}$$

and $\widehat{H}^{-n}(G, A) := \widehat{H}_{n-1}(G, A)$, $\widehat{H}_{-n}(G, A) := \widehat{H}^{n-1}(G, A)$

By definition $\widehat{H}^{-2}(G, \mathbb{Z}) = H_1(G, \mathbb{Z})$. Moreover, it is remarkable that $\widehat{H}^0(\mathrm{Gal}(L/K), L^\times) = K^\times/N_{L/K}L^\times$ and the homology group $H_1(G, \mathbb{Z})$ is the abelianisation $G^{ab} = G/[G, G]$ of G.

Proposition 3.5.11. *Let $\chi \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) = H^2(G, \mathbb{Z})$ be a character of degree 1 of G and let $\delta_\chi \in H^2(G, \mathbb{Z})$ be the image of χ by the coboundary map $\delta : H^1(G, \mathbb{Q}/\mathbb{Z}) \to H^2(G, \mathbb{Z})$. Let*

$$\overline{\alpha} \in K^\times/N_{L/K}(L^\times) = \widehat{H}^0(G, L^\times)$$

be the image of α. The cup product $\overline{\alpha} \cup \delta_\chi$ is an element of $H^2(G, L^\times) \subset \mathrm{Br}(K)$. We have the formula

$$\chi(\sigma_{L/K}(\alpha)) = \mathrm{inv}_K(\overline{\alpha} \cup \delta_\chi)$$

Proof. By definition

$$\sigma_{L/K}(\alpha) \cup u_{L/K} = \overline{\alpha} \in \hat{H}^0(G, L^\times)$$

here $\sigma_{L/K}(\alpha)$ is identified with an element of $H^{-2}(G,\mathbb{Z})$. Using the associativity of the cup product, this gives us

$$\overline{\alpha} \cup \delta_\chi = u_{L/K} \cup \sigma_{L/K}(\alpha) \cup \delta_\chi = u_{L/K} \cup (\delta(\sigma_{L/K}(\alpha) \cup \chi)$$

with $\sigma_{L/K}(\alpha) \cup \chi \in \hat{H}^{-1}(G,\mathbb{Q}/\mathbb{Z})$. Now

$$\hat{H}^{-1}(G,\mathbb{Q}/\mathbb{Z}) \xrightarrow{\delta} \hat{H}^{0}(G,\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$$

and we identify $\hat{H}^{-1}(G,\mathbb{Q}/\mathbb{Z})$ with $\mathbb{Z}/n\mathbb{Z}$. Moreover, the identification between $H^{-2}(G,\mathbb{Z})$ and G^{ab} ensure that $\sigma_{L/K}(\alpha) \cup \chi = \chi(\sigma_{L/K}\alpha)$. Now write $\sigma_{L/K}(\alpha) \cup \chi = r/n$, $r \in \mathbb{Z}$. Then $\delta(r/n) \in \hat{H}^{0}(G,\mathbb{Z})$ and $\delta(r/n) = r$. Hence

$$u_{L/K} \cup (\sigma_{L/K} \cup \delta_\chi) = r \cup u_{L/K}$$

and the invariant of this cohomology class is just $r/n = \chi(x_\alpha)$. □

Now consider a tower of Galois extensions $K \subset L' \subset L$ with $G = \mathrm{Gal}(L/K)$ and $H = G(L/L')$. Then, if χ' is a character of $(G/H)^{ab}$ and χ is the corresponding character of G^{ab}, and if $\alpha \in K^\times$ induces $\sigma_{L/K}(\alpha) \in G^{ab}$ and $\sigma'_{L'/K}(\alpha) \in (G/H)^{ab}$ under the natural map $G^{ab} \to (G/H)^{ab}$. It follows from the proposition and the inflation map transforms χ' (resp. $\delta_{\chi'}$) into χ (resp. δ_χ), we have $\chi(\sigma_{L/K}(\alpha)) = \chi'(\sigma'_{L'/K}(\alpha))$. This compatibility allows us to define σ_α for any abelian extension; in particular, taking $L = K^{ab}$, the maximal abelian extension of K, we get a homomorphism

$$\sigma_K : K^\times \to \mathrm{Gal}(K^{ab}/K)$$

Note that $H^1(G_{\mathbb{Q}_p},\mathbb{Q}_p) = \mathrm{Hom}_{cont}(G^{ab}_{\mathbb{Q}_p},\mathbb{Q}_p)$ as every group homomorphism factors through its abelization. We can reinterpret the Tate local duality as follows.

Theorem 3.5.12. *Let $G^{ab}_{\mathbb{Q}_p}$ be the abelianized Galois group and let $\sigma : \mathbb{Q}_p^\times \to G^{ab}_{\mathbb{Q}_p}$ be a local Artin symbol, normalized so that σ_p is the inverse of a Frobenius element. Then the Tate pairing*

$$\langle , \rangle : H^1(\mathbb{Q}_p(1)) \times H^1(\mathbb{Q}_p) \to \mathbb{Q}_p$$

is explicitly given by the formula

$$\big\langle \gamma_q, \xi \big\rangle = \xi(\sigma_q)$$

for arbitrary $q \in \mathbb{Q}_p^\times$ and $\xi \in H^1(\mathbb{Q}_p)$, where $\gamma_q \in H^1(\mathbb{Q}_p(1))$ is the Kummer class of q.

Recall that the cyclotomic character $\xi_0 : G_{\mathbb{Q}_p} \to \mathbb{Z}_p^\times$ is characterized by $\xi_{p^n}^\sigma = \xi_{p^n}^{\xi_0(\sigma)}$ for all $\sigma \in G$ and $\xi_{p^n} \in \mu_{p^n}$. Note that ξ_0 is alternatively obtained by lifting $I_{\mathbb{Q}_p} \to I_{\mathbb{Q}_p}^{ab} \simeq \mathbb{Z}_p^\times$ to $G_{\mathbb{Q}_p}$. Hence ξ_0 is given by $\xi_0(\sigma_u) = u$ for $u \in \mathbb{Z}_p^\times$.

Theorem 3.5.13. *Let $E_{/\mathbb{Q}_p}$ be an elliptic curve with split multiplicative reduction with Tate p-adic period q_E and let $\psi : G_{\mathbb{Q}_p} \to \widetilde{\mathbb{Q}}_p^\times$ be a nontrivial character which is $\equiv 1$ modulo t. Then the following statements are equivalent:*

1. *$\dfrac{d\psi}{dt}(\sigma_{q_E}) = 0$ with $\sigma : \mathbb{Q}_p^\times \to G_{\mathbb{Q}_p}^{ab}$ the local Artin symbol.*
2. *Tate's module $V(E)$ corresponds to $\widetilde{\mathbb{Q}}_p(\psi)$ under*

$$\begin{array}{c} \{\textit{Nontrivial infinitesimal deformations } \mathbb{Q}_p(\psi) \textit{ of } \mathbb{Q}_p\} \\ \updownarrow \\ \{\textit{Nontrivial extensions of } \mathbb{Q}_p \textit{ by } \mathbb{Q}_p(1)\} \end{array}$$

3. *There is an indinitesimal deformation $\widetilde{V}$ of Tate's module $V(E)$ and a commutative diagram*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \widetilde{\mathbb{Q}}_p(1) & \longrightarrow & \widetilde{V} & \longrightarrow & \widetilde{\mathbb{Q}}_p(\psi) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathbb{Q}_p(1) & \longrightarrow & V(E) & \longrightarrow & \mathbb{Q}_p & \longrightarrow & 0 \end{array}$$

   in which the top row is an exact sequence of $\widetilde{\mathbb{Q}}_p[G_{\mathbb{Q}_p}]$-modules and the vertical maps are reduction modulo t.

Proof. (1) $\Leftrightarrow$ (2) By the Tate's local duality formula $\langle \gamma_q, \xi \rangle = \xi(\sigma_q)$, we see that $\dfrac{d\psi}{dt}(\sigma_{q_E}) = 0$ if and only if $\left\langle \gamma_{q_E}, \dfrac{d\psi}{dt} \right\rangle = 0$, i.e., γ_{q_E} is orthogonal to $\dfrac{d\psi}{dt}$ with respect to the Tate pairing. On the other hand, the Kummer class γ_{q_E} spans the line in $H^1(\mathbb{Q}_p(1))$ determined by $V(E)$ and $\dfrac{d\psi}{dt}$ spans the line in $H^1(\mathbb{Q}_p)$ determined by the infinitesimal deformation $\widetilde{\mathbb{Q}_p}(\psi)$.

(2) $\Rightarrow$ (3) Suppose that the Tate module $V(E)$ corresponds to $\widetilde{\mathbb{Q}_p}(\psi)$. Then we can provide an explicit construction of $\widetilde{V}$ as follows. Let γ denote a cocycle representing the cohomology class of γ_{q_E}. Then the function

$$\zeta : G_{\mathbb{Q}_p} \times G_{\mathbb{Q}_p} \to \mathbb{Q}_p(1)$$

$$(g_1, g_2) \mapsto \gamma(g_1) \cdot \frac{d\psi}{dt}(g_2)$$

is a 2-cocycle representing the cup product of γ_{q_E} and $\dfrac{d\psi}{dt}$.

Since this cup product vanishes by Tate duality, there is a 1-cochain $\xi : G_{\mathbb{Q}_p} \to \mathbb{Q}_p(1)$ whose coboundary is the ζ. Hence, for all $(g_1, g_2) \in G_{\mathbb{Q}_p} \times G_{\mathbb{Q}_p}$, we have

$$\xi(g_1 g_2) - \xi_0(g_1)\xi(g_2) - \xi(g_1) = \gamma(g_1)\frac{d\psi}{dt}(g_2)$$

Now define for each $g \in G$

$$\rho(g) = \begin{pmatrix} \xi_0(g) & \gamma(g) + t\xi(g) \\ 0 & \psi(g) \end{pmatrix} \in \mathrm{GL}_2(\overline{\mathbb{Q}_p})$$

We can check that $\rho : G_{\mathbb{Q}_p} \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ is a group homomorphism. Let $\widetilde{V} =: \widetilde{\mathbb{Q}_p}^2$ equipped with the Galois action induced by ρ, i.e., for all $(q_1, q_2) \in \widetilde{\mathbb{Q}_p}^2$ and $g \in G$

$$(q_1, q_2)^g = (\xi_0(g)q_1, \psi(g)q_2)$$

Define

$$\begin{aligned} \Psi : \widetilde{V} &\to \widetilde{\mathbb{Q}_p}(\psi) \\ (q_1, q_2) &\mapsto q_2 \end{aligned}$$

We see that Ψ is $G_{\mathbb{Q}_p}$-equivariant

$$\Psi((q_1, q_2)^g) = \Psi((\xi_0(g)q_1, \psi(g)q_2)) = \psi(g)q_2 = q_2^g = \Psi(q)^g$$

Moreover, its kernel is $\widetilde{\mathbb{Q}_p}(\xi_0) = \widetilde{\mathbb{Q}_p}(1)$. Reduce modulo t we obtain the maps $\theta_1 : \widetilde{\mathbb{Q}_p}(1) \to \mathbb{Q}_p(1)$ and $\theta_2 : \widetilde{\mathbb{Q}_p}(\psi) \to \mathbb{Q}_p$. Now define $\theta = (\theta_1, \theta_2) : \widetilde{V} \to V(E)$ we obtain

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \widetilde{\mathbb{Q}}_p(1) & \longrightarrow & \widetilde{V} & \longrightarrow & \widetilde{\mathbb{Q}}_p(\psi) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathbb{Q}_p(1) & \longrightarrow & V(E) & \longrightarrow & \mathbb{Q}_p & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

By Snake lemma we get the diagram in 3.

(3) $\Rightarrow$ (2) Suppose that we have a commutative diagram as in (c). We show that γ_E is orthogonal to $\dfrac{d\psi}{dt}$ with respect to the Tate pairing. From the diagram in c we obtain a commutative diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathbb{Q}_p(1) & \longrightarrow & V(E) & \longrightarrow & \mathbb{Q}_p & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \widetilde{\mathbb{Q}}_p(1) & \longrightarrow & \widetilde{V} & \longrightarrow & \widetilde{\mathbb{Q}}_p(\psi) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathbb{Q}_p(1) & \longrightarrow & V(E) & \longrightarrow & \mathbb{Q}_p & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

in which the rows and columns are exact. We see there exits a section $\mathbb{Q}_p(1) \to \widetilde{\mathbb{Q}_p}(1)$, the leftmost vertical row splits, the connecting homomorphism $H^1(\mathbb{Q}_p(1)) \to H^2(\mathbb{Q}_p(1))$ vanishes (the galois cohomology functor is additive). On the other hand, let $\delta_\psi : H^0(\mathbb{Q}_p) \to H^1(\mathbb{Q}_p)$ be the connecting homomorphism of degree 0 attached to the rightmost vertical row, and let $\delta_i : H^1(\mathbb{Q}_p) \to H^{i+1}(\mathbb{Q}_p(1))$ $(i = 0, 1)$ be the connecting homomorphism of degree i associated to the bottom row, we obtain a commutative diagram

$$\begin{array}{ccc}
H^0(\mathbb{Q}_p) = \mathbb{Q}_p & \xrightarrow{\delta_0} & H^1(\mathbb{Q}_p(1)) \\
\downarrow{\scriptstyle \delta_\psi} & & \downarrow{\scriptstyle =0} \\
H^1(\mathbb{Q}_p) & \xrightarrow{\delta_1} & H^2(\mathbb{Q}_p(1))
\end{array}$$

Since $\delta_1(\dfrac{d\psi}{dt}) = \delta_1 \circ \psi(1) = 0 \circ \delta_0(1) = 0$, $\dfrac{d\psi}{dt} \in \operatorname{Ker} \delta_1$. On the other hand, the Kummer class γ_{q_E} is in the image of δ_0. We will show that the kernel of δ_1 is orthogonal to the image of δ_0.

The multiplication induces a perfect pairing

$$\begin{aligned} P : \mathbb{Q}_p(1) \times \mathbb{Q}_p &\to \mathbb{Q}_p(1) \\ (q_1, q_2) &\mapsto q_1 q_2 \end{aligned}$$

Indeed, $\mathbb{Q}_p \to \mathrm{Hom}(\mathbb{Q}_p(1), \mathbb{Q}_p(1))$, $q_2 \mapsto P(-, q_2)$. Moreover, the Weil pairing

$$V(E) \times V(E) \to \mathbb{Q}_p(1)$$

with respect to which the homomorphisms $i : \mathbb{Q}_p(1) \to V(E)$ and $\pi : V(E) \to \mathbb{Q}_p$ are transpose of each other. It follow that

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Q}_p(1) & \longrightarrow & V(E) & \longrightarrow & \mathbb{Q}_p & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathbb{Q}_p(1)^* = \mathbb{Q}_p & \longrightarrow & V(E)^* = V(E) & \longrightarrow & \mathbb{Q}_p^* = \mathbb{Q}_p(1) & \longrightarrow & 0 \end{array}$$

Hence the fundamental exact sequence

$$0 \to \mathbb{Q}_p(1) \to V(E) \to \mathbb{Q}_p \to 0$$

is self dual with respect to these pairings. By duality, the connecting homomorphisms $\delta_0 : H^0(\mathbb{Q}_p) \to H^1(\mathbb{Q}_p(1))$ and $\delta_1 : H^1(\mathbb{Q}_p) \to H^2(\mathbb{Q}_p(1))$ are transposes under the Tate pairing. In particular, the image of δ_0 is orthogonal to the kernel of δ_1 □

3.6 L-invariant

Theorem 3.6.1. *Let $\alpha_p(k)$ be the p-adic analytic function attached to the p-th coefficient of Hida's Λ-adic modular form. Then*

$$\alpha_p'(2) = -\frac{1}{2}\mathcal{L}_p(E)$$

Proof. Let $f = \sum_{n=1}^{\infty} \alpha_n(k) q^n \in \mathcal{A}_U[[q]]$ be the formal q-expansion given by Hida's theorem, where U is a suitable p-adic neighborhood of 2. Consider the representation $\rho : G_{\mathbb{Q}_p} \to \mathrm{GL}_2(\mathcal{A}_U)$ given in the theorem 2.5.10. Then we obtain a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{A}_U(\chi_0 \langle \chi_0 \rangle^{k-2} \varphi_k^{-1}) & \longrightarrow & \mathcal{A}_U^2 & \longrightarrow & \mathcal{A}_U(\varphi_k) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathbb{Q}_p(1) & \longrightarrow & V(E) & \longrightarrow & \mathbb{Q}_p & \longrightarrow & 0 \end{array}$$

of $G_{\mathbb{Q}_p}$-representations where $\varphi_k : G_{\mathbb{Q}_p} \to \mathcal{A}_U^\times$ is the unramified character with $\varphi_k(\mathrm{Frob}_p) = \alpha_p(k)$, the bottom row is the fundamental sequence associated to E, and the vertical arrows are given by specialization to $k = 2$.

Twisting each term of the above diagram by $\varphi_k \langle\chi_0\rangle^{2-k}$ so that the leftmost term is $\mathcal{A}_U(\chi_0)$. Since this character specializes to the trivial character at $k = 2$, we obtain a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{A}_U(\chi_0) & \longrightarrow & \mathcal{A}_U^2(\varphi\langle\chi_0\rangle^{2-k}) & \longrightarrow & \mathcal{A}_U(\varphi_k^2\langle\chi_0\rangle^{2-k}) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathbb{Q}_p(1) & \longrightarrow & V(E) & \longrightarrow & \mathbb{Q}_p & \longrightarrow & 0 \end{array}$$

Let $t := k - 2 \in \mathcal{A}_U$ we have $\mathcal{A}_U/(t^2) \simeq \widetilde{\mathbb{Q}}_p$. Hence, reducing the terms modulo t^2 and setting $\widetilde{V} := \widetilde{\mathbb{Q}}_p^2(\varphi_k\langle\chi_0\rangle^{2-k})$ we obtain a diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \bar{\mathbb{Q}}_p(1) & \longrightarrow & \bar{V} & \longrightarrow & \bar{\mathbb{Q}}_p(\psi) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathbb{Q}_p(1) & \longrightarrow & V(E) & \longrightarrow & \mathbb{Q}_p & \longrightarrow & 0 \end{array}$$

where $\psi = \varphi_k^2\langle\chi_0\rangle^{2-k}$ considered modulo t^2. It follows that

$$\frac{d\psi}{dk}(\sigma_{p_E}) = 0$$

Writing $q_E = p^n u$ where $n = \mathrm{ord}_p(q_E)$ and $u \in \mathbb{Z}_p^\times$ and noting that $\varphi_k(\sigma_p) = \varphi(\mathrm{Frob}_p)^{-1}$ and $\varphi_k(\mathrm{Frob}_p) = \alpha_p(k)$ we obtain

$$\psi(\sigma_{q_E}) = \alpha_p(k)^{-2n}\langle u\rangle^{2-k}$$

Differentiate this with respect to k and set $k = 2$. Note that $\alpha_p(2) = 1$ since E has split multiplicative reduction at p, we have the equality

$$\alpha_p'(2) = -\frac{1}{2}\frac{\log_p(q_E)}{\mathrm{ord}_p(q_E)}$$

□

CHAPTER 4

Two-variable p-adic L-function

In this chapter, we will construct the Mazur-Kitagawa p-adic L-function following Greenberg and Stevens [GS94] by conceptual study the measure -valued modular symbols. In chaoter 1, we have seen that classical modular symbol encodes special values of L-function. It is well-known that the classical modular symbols can be interpreted in the sense of cohomology. One of the remarkable things is that the measure-valued module of modular symbols has the structure of a Λ-module, to which we can apply Hida's theory.

Given an elliptic curve E over $\mathbb{Q}$, we constructed the p-adic L-function attached to E in chapter 1. It will turn out that we can lift a classical modular symbol to a measure-valued modular symbol which can be viewed as a family of p-adic L-functions whose weight 2 specialization agrees with the p-adic L-function attached to E.

4.1 Modular Symbols

4.1.1 Modular Symbols

Definition 4.1.1. Let $\mathcal{D} := Div(\mathbb{P}^1(\mathbb{Q}))$ be the group of divisors supported on the rational cusps $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$ of the upper half plane $\mathbb{H}$. Denote

$$\mathcal{D}_0 := \big\{\{c_1\} - \{c_2\} | \text{where } \{c_1\}, \{c_2\} \in \mathbb{P}^1(\mathbb{Q})\big\} \subset \mathcal{D}$$

the subgroup of divisors of degree zero.

The group $\mathrm{GL}_2(\mathbb{Q})$ acts by fractional linear transformations on $\mathcal{D}$ and also on $\mathcal{D}_0$, i.e,

for all $z \in \mathcal{D}$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}$$

Also, we define the action of the multiplicative semigroup $M_2(\mathbb{Z})$ of 2×2 integral matrices on $\mathcal{D}$ and $\mathcal{D}_0$.

Definition 4.1.2. If $\sum$ is a subsemigroup of the multiplicative semigroup $M_2(\mathbb{Z})$ and if A is a right $\mathbb{Z}\left[\sum\right]$-module, then we define a right action of $\sum$ on $\mathrm{Hom}_{\mathbb{Z}}(\mathcal{D}_0, A)$ by $\Phi \mapsto \Phi|_\sigma$, for $\sigma \in \sum$, where

$$(\Phi|_\sigma)(D) = \Phi(\sigma D)|_\sigma$$

for all $D \in \mathcal{D}$.

Note that the action on the right hand side is the module action on A. Also, we see that if $\sigma_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \in \sum$ then

$$\left(\Phi|_{\sigma_1}\right)|_{\sigma_2}(D) = \left((\Phi|_{\sigma_1})(\sigma_2 D)\right)|_{\sigma_2} = \left(\Phi(\sigma_1\sigma_2 D)\right)|_{\sigma_2\sigma_1} = (\Phi)|_{\sigma_1\sigma_2}(D)$$

Hence the action defined is indeed a right action of $\sum$ on $\mathrm{Hom}_{\mathbb{Z}}(\mathcal{D}_0, A)$.

Definition 4.1.3. An element $\Phi \in \mathrm{Hom}_{\mathbb{Z}}(\mathcal{D}_0, A)$ is called an A-valued modular symbol if the stabilizer of Φ in $\sum$ contains a congruence subgroup of $SL_2(\mathbb{Z})$. That is, there is a congruence subgroup $\Gamma \subset SL_2(\mathbb{Z})$ sucht that

$$\Gamma \subseteq \{\sigma \in \sum | \Phi_\sigma = \Phi\}$$

We say that Φ is a modular symbol over Γ.

Notation: The module of all A-valued modular symbols is denoted $\mathrm{Symb}(A)$. The module of modular symbols over Γ is denoted $\mathrm{Symb}_\Gamma(A) \subset \mathrm{Symb}(A)$

Definition 4.1.4. We denote $L_k(R)$ the R-module of homogeneous polynomials of degree $k-2$ in two variables X, Y with coefficients in a commutative ring R.

We let $\sum$ act on $L_k(R)$ by the following formula

$$(F|g)(X,Y) = F((X,Y)g^*)$$

where $g \in \sum$ and $F \in L_k(R)$ and $*$ is the main involution $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$

Claim: Let $g_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$ and $g_2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$ we have

$$g_1 g_2 = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix}$$

and

$$\begin{pmatrix} d_1 & -c_1 \\ -b_1 & a_1 \end{pmatrix} \begin{pmatrix} d_2 & -c_2 \\ -b_2 & a_2 \end{pmatrix} = \begin{pmatrix} d_1d_2 + c_1b_2 & -d_1c_2 - c_1a_2 \\ -b_1d_2 - a_1b_2 & b_1c_2 + a_1a_2 \end{pmatrix}$$

Definition 4.1.5. Fix an integer $k \geq 2$ and a commutative ring R. Then $\mathrm{Symb}(L_k(R))$ is called the module of modular symbols of weight k over R.

The main modular symbol I use throughout my thesis is due to Eicher-Shimura. Let $S_k(\overline{\mathbb{Q}})$ be the space of weight k cusp forms of all levels having algebraic q-expansions and let $\mathrm{GL}_2^+(\mathbb{Q})$ act on $S_k(\overline{\mathbb{Q}})$ via the standard weight k action: for any $\sigma \in \mathrm{GL}_2^+(\mathbb{Q})$ and z in the upper half-plane we define

$$(f|_\sigma)(z) := \frac{\det(\sigma)^{k-1}}{(cz+d)^k} f(\sigma z)$$

Definition 4.1.6. For each $f \in S_k(\overline{\mathbb{Q}})$ we associate the unique $\mathbb{Z}$-linear function $\psi_f : \mathcal{D}_0 \to L_k(\mathbb{C})$ whose value on divisors of the form $\{c_2\} - \{c_1\} \in \mathcal{D}_0$, with $c_1, c_2 \in \mathbb{P}^1(\mathbb{Q})$ is given by

$$\psi_f\left(\{c_2\} - \{c_1\}\right) = 2\pi i \int_{c_1}^{c_2} f(z)(zX+Y)^{k-2} dz \tag{4.1.1}$$

Remark 4.1.7. For any $\sigma \in \mathrm{GL}_2^+(\mathbb{Q})$ we have

$$(\psi_f|\sigma)\left(\{c_2\} - \{c_1\}\right) = 2\pi i \int_{\sigma c_1}^{\sigma c_2} f(z)(zX+Y)^{k-2} dz = 2\pi i \int_{c_1}^{c_2} f(\sigma z)((\sigma z)X+Y)^{k-2} d(\sigma z)$$

We have

$$\big(\sigma(z)X+Y\big)^{k-2}=\left(\frac{az+b}{cz+d}X+Y\right)^{k-2}=\big((az+b)X+(cz+d)Y\big)^{k-2}(cz+d)^{2-k}$$

And

$$\frac{d}{dz}(\sigma z)=\frac{d}{dz}(\frac{az+b}{cz+d})=\frac{ad-bc}{(cz+d)^2}$$

Hence

$$(\psi_f|\sigma)\big(\{c_2\}-\{c_1\}\big)=2\pi i\int_{c_1}^{c_2}\frac{(ad-bc)^{k-1}}{(cz+d)^k}f(\sigma z)(zX+Y)^{k-2}dz$$

4.1.2 Modular Symbols and Hecke Operators

We define operators via the action of double cosets.

Definition 4.1.8. Let Γ and Γ' be two congruence subgroups and let $\Delta\subset \mathrm{GL}_2^+(\mathbb{Q})$ be a semigroup. We denote by $H(\Gamma,\Gamma',\Delta)$ the free $\mathbb{Z}$-module generated by double cosets $\Gamma\alpha\Gamma'$ with $\alpha\in\Delta$

$$\mathcal{H}(\Gamma,\Gamma',\Delta)=\{\sum_{\alpha\in\Delta}a_\alpha\Gamma\alpha\Gamma'|a_\alpha\in\mathbb{Z},a_\alpha=0 \text{ except for finitly many } \alpha\}$$

We define multiplication of elements of $\mathcal{H}(\Gamma,\Delta):=\mathcal{H}(\Gamma,\Gamma,\Delta)$ so that $\mathcal{H}(\Gamma,\Delta)$ becomes an algebra.

Let $\Gamma_1,\Gamma_2,\Gamma_3$ be congruence subgroups. For two elements $\Gamma_1\alpha\Gamma_2=\sqcup_i\Gamma_1\alpha_i$ and $\Gamma_2\beta\Gamma_3=\sqcup_j\Gamma_2\beta_j$, we define

$$\Gamma_1\alpha\Gamma_2\cdot\Gamma_2\beta\Gamma_3=\sum_\gamma c_\gamma\Gamma_1\gamma\Gamma_3$$

where $c_\gamma=|\{(i,j)|\Gamma_1\alpha_i\beta_j=\Gamma_1\gamma\}|$ and the summation is taken over all double cosets $\Gamma_1\gamma\Gamma_3$ such that $\gamma\in\Delta$. The right hand side is a finite sum because there are only finitely many i's and j's.

Lemma 4.1.9. *The multiplication defined by the equality is independent of the choice of the representatives α_i, β_j and γ.*

Proof. Refer [Mi89] □

The $\mathbb{Z}$-algebra $\mathcal{H}(\Gamma, \Delta)$ is called a Hecke algebra. The unity in $\mathbb{Z}$-algebra $\mathcal{H}(\Gamma, \Delta)$ is Γ.

Definition 4.1.10. For an arbitrary congruence subgroup $\Gamma \subset \sum$, let $H(\Gamma, \sum)$ be the double coset algebra over $\mathbb{Z}$ associated to the pair $(\Gamma, \sum)$. The action of $H(\Gamma, \sum)$ on A-valued modular symbols over Γ is given as follows. If $T(g) \in H(\Gamma, \sum)$ is the element associated to the double coset $\Gamma g \Gamma$, $g \in \sum$, then we can write $\Gamma g \Gamma$ as a finite disjoint union of right cosets, $\bigcup_i \Gamma g_i$. For a modular symbol $\Phi \in \mathrm{Symb}_\Gamma(A)$ we then define

$$\Phi | T(g) = \sum_i \Phi | g_i \in \mathrm{Symb}_\Gamma(A)$$

Proposition 4.1.11. *Let $f \in S_k(\overline{\mathbb{Q}})$ be a weight k cusp form of any level. Recall the action of Hecke operaton on f given by*

$$f|T_p := p^{k/2-1} \left(\sum_u^{p-1} f \left| \begin{pmatrix} 1 & u \\ 0 & p \end{pmatrix} + \epsilon(p) \cdot f \right| \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \right)$$

. Then the map $f \mapsto \psi_f$ is Hecke equivariant.

Proof. Let $\sigma = \begin{pmatrix} 1 & a \\ 0 & p \end{pmatrix}$ for some prime p, then we have

$$\begin{aligned} \psi_{f|\sigma}(\{c_2\} - \{c_1\}) &= 2\pi i \int_{c_1}^{c_2} f(z) | \gamma \cdot (zX + Y)^{k-2} dz \\ &= 2\pi i \int_{c_1}^{c_2} \frac{p^{k-1}}{p^k} f(\frac{z+a}{p})(zX + Y)^{k-2} dz \end{aligned}$$

Substituting $y = \dfrac{z+a}{p}$, so $y = py - a$ and $dz = l dy$ we obtain

$$\psi_{f|\sigma}(\{c_2\} - \{c_1\}) = 2\pi i \int_{c_1}^{c_2} f(y) \cdot ((py - a)X + Y)^{k-2} dy$$

Furthermore, we see that

$$(yX+Y)^{k-2}|\sigma = (1-aX)^{k-2}\left(y\frac{pX}{1-aX}+Y\right)^{k-2} = ((py-a)X+Y)^k$$

Hence $\psi_{f|\sigma}(\{c_2\}-\{c_1\}) = \psi_f|\sigma(\{c_2\}-\{c_1\})$. The U_p operator is a sum of matrices of this form, we deduce that $\psi_{f|U_p} = \psi_f|U_p$. For the T_p operator, it remains to check only the matrix $\gamma = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$. Note that $P|\gamma(X,Y) = p^{k-2}P((X,Y)/p)$ we directly verify that

$$\begin{aligned}
\psi_{f|\gamma}(\{c_2\}-\{c_1\}) &= 2\pi i\int_{c_1}^{c_2} p^{k-1}f(pz)(zX+Y)^{k-2}dz \\
&= 2\pi i\int_{c_1}^{c_2} f(y)\left[p^{k-2}\left(y\frac{X}{p}+Y\right)^{k-2}\right]dy \\
&= \psi_f|\gamma(\{c_2\}-\{c_1\})
\end{aligned}$$

□

4.1.3 Modular Symbols and Cohomology

Definition 4.1.12. Let Γ be a congruence subgroup. We say an element $\gamma \in \Gamma$ is parabolic if γ fixes exactly one point in $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q}\cup\{\infty\}$. Let P denote the set of all parabolic elements of Γ.

Definition 4.1.13. We denote by $C_P^1(\Gamma, M)$ the R-submodule of $C^1(\Gamma, M)$ consisting of elements u with the property that for all $\gamma \in P$ there exists some $m \in M$ such that

$$u(\gamma) = (\gamma - 1)m$$

Setting

$$\begin{aligned}
Z_P^1(\Gamma, M) &= Z_1(\Gamma, M)\cap C_P^1(\Gamma, M) \\
B_P^2(\Gamma, M) &= d^1(C_P^1(\Gamma, M))
\end{aligned}$$

We define the parabolic cohomology groups of Γ with coefficients in M to be

$$\begin{aligned}
H_P^0(\Gamma, M) &= H^0(\Gamma, M) = M^\Gamma \\
H^1(\Gamma, M) &= Z_P^1(\Gamma, M)/B_P^1(\Gamma, M) \\
H_P^2(\Gamma, M) &= Z^2(\Gamma, M)/B_P^2(\Gamma, M)
\end{aligned}$$

Let $\Gamma_1, \Gamma_2 \subset \mathrm{SL}_2(\mathbb{Z})$ be congruence subgroups. For any $\alpha \in \mathrm{GL}_2^+(\mathbb{Z})$, let $R\langle\Gamma_1, \Gamma_2, \alpha^\iota\rangle$ denote the semi-group ring generated by Γ_1, Γ_2, and α^ι over R, where $\alpha^\iota = \det(\alpha)\alpha^{-1}$. We define the action of the double coset operator $[\Gamma_1\alpha\Gamma_2]$ on $H^1(\Gamma, M)$ for an $R\langle\Gamma_1, \Gamma_2, \alpha^\iota\rangle$-module M. Let decompose the double coset $[\Gamma_1\alpha\Gamma_2] = \sqcup\Gamma_1\alpha_i$. For each $\gamma \in \Gamma_2$, we have $\alpha_i\gamma = \gamma_i\alpha_j$ for some $\gamma_i \in \Gamma_1$. Now, for any 1-cocycle $u : \Gamma_1 \to M$ we define

$$v(\gamma) := u|[\Gamma_1\alpha\Gamma_2](\gamma) = \sum_i \alpha_i^\iota u(\gamma_i)$$

The operator $[\Gamma_1\alpha\Gamma_2]$ does not depend on choices of orbit representatives $\{\alpha_i\}$. Furthermore, if $\gamma, \delta \in \Gamma_2$ with $\alpha_i\gamma = \gamma_i\alpha_j$ and $\alpha_i\delta = \delta_i\alpha_j$, we have $\alpha_i\gamma\delta = \gamma_i\delta_j\alpha_j$. It follows that

$$v(\gamma\delta) = \sum_i \alpha_i^\iota u(\gamma_i\delta_j) = \gamma v(\delta) + v(\gamma)$$

Hence, $v = u|[\Gamma_1\alpha\Gamma_2]$ is a 1-cocycle of Γ_2. Suppose u is a 1-coboundary of Γ_1 with $u(\gamma) = (\gamma - 1)m$. Then we have

$$v(\gamma) = \sum_i \alpha_i^\iota(\gamma_i - 1)m = \sum_j (\alpha_j\gamma)^\iota m - \sum_i \alpha_i^\iota m = (\gamma - 1)\sum_i \alpha_i^\iota m$$

which show that v is a 1-coboundary of Γ_2. Thus, the double coset operator $[\Gamma_1\alpha\Gamma_2]$ is a well defined linear operator from $H^1(\Gamma_1, M)$ to $H^1(\Gamma_2, M)$. Furthermore, one can see that it maps $H_P^1(\Gamma_1, M)$ to $H_P^1(\Gamma_2, M)$.

We provide the cohomology interpretation of modular symbols due to Ash and Stevens [AS86]

Definition 4.1.14. A Hecke pair (Γ_0, S_0) is said to be weakly compatible to a Hecke pair (Γ, S) if

1. $(\Gamma_0, S_0) \subseteq (\Gamma, S)$
2. the set $S' = S \setminus \Gamma S_0$ satisfies $SS' \subseteq S'$ and $S'S_0 \subseteq S'$
3. $\Gamma \cap S_0 S_0^{-1} = \Gamma_0$

If $(\Gamma_0, S_0) \subseteq (\Gamma, S)$ are weakly compatible then there is a canonical algebra homomorphism

$$i : \mathcal{H}(\Gamma, S) \to \mathcal{H}(\Gamma_0, S_0)$$

Viewing the Hecke algebras as convolution algebras this map is given by the restriction of functions on S to functions on S_0. The following lemma due to Shapiro allows us to relate systems of Hecke eigenvalues occurring in the cohomology of Γ to those occurring in Γ_0.

Proposition 4.1.15. *Suppose that* $(\Gamma_0, S_0) \subseteq (\Gamma, S)$ *are weakly compatible Hecke pairs*

1. *Let* E *be a right* S*-module,* F *be a right* S_0*-module and* $\phi : E \to F$ *be an* S_0*-morphism. If* $E|\sigma \subseteq \ker(\phi)$ *for every* $\sigma \in S \setminus \Gamma S_0$ *then the composition*

$$H^r(\Gamma, E) \overset{res}{\to} H^r(\Gamma_0, E) \overset{\phi_*}{\to} H^r(\Gamma_0, F)$$

is Hecke equivariant; i.e. if $\xi \in H^r(\Gamma, E)$ *and* $h \in \mathcal{H}(\Gamma, S)$ *then*

$$(\phi_* \circ \mathrm{res})(\xi|h) = (\phi_* \circ \mathrm{res}(\xi))|i(h)$$

2. *If* F *is a right* S_0*-module then the induced module* $\mathrm{Ind}_{\Gamma_0}^{\Gamma}(F)$ *inherits a natural right* S*-action. The Shapiro isomorphism*

$$H^r(\Gamma, \mathrm{Ind}_{\Gamma_0}^{\Gamma}(F)) \to H^r(\Gamma_0, F)$$

is Hecke equivariant.

Definition 4.1.16. Let X be a topological space and K be a compact subset of X, define the compact support cochains

$$\begin{aligned} C_c^i(X) &:= \cup_K C^i(X, X \setminus K) \\ &= \{\varphi : C_i(X) \to R | \exists \text{ a compact subset } K_\varphi \subset X \text{ such that } \varphi = 0 \text{ on chains in } X \setminus K_\varphi\} \end{aligned}$$

For $\varphi \in C_c^i(X)$, define the differential

$$d\varphi(\sigma) := \varphi(d\sigma)$$

for all $\sigma \in C^i(X)$

Note that if $\varphi \in C_c^i(X)$, then $d\varphi$ is also zero on all chains in $X \setminus K_\varphi$ and so $d\varphi \in C_c^{i+1}(X)$. Hence we obtain a cochain subcomplex $C_c^*(X)$ of $C^i(X)$. We define

$$H_c^i(X) := H^i(C_c^*(X))$$

the cohomology of X with compact support.

Theorem 4.1.17. *Let R be a commutative ring in which the order of every torsion element of Γ is invertible. If E is an $R[\Gamma]$-module then we have*

$$\mathrm{Symb}_\Gamma(E) \simeq H^1_c(\Gamma, E)$$

One of the most celebrated result in the subject is the following theorem due to Eicher-Shimura.

Theorem 4.1.18. *There is a Hecke-equivariant isomorphism*

$$S_{k+2}(\Gamma, \mathbb{C}) \oplus \overline{S_{k+2}(\Gamma, \mathbb{C})} \oplus \mathcal{E}_{k+2}(\Gamma, \mathbb{C}) \simeq \mathrm{Symb}_\Gamma(L_k(\mathbb{C})$$

given by the map

$$(f, \overline{f}, g) \mapsto \psi_f + \psi_{\overline{f}} + \psi_g$$

Proof. (Sketch) Firstly we can reinterpret the modular symbols in term of cohomology. Let $Y_\Gamma := \Gamma \setminus \mathbb{H}$ denote the modular curve. We have an isomorphism

$$\mathrm{Symb}_\Gamma(L_k(\mathbb{C})) \simeq H^1_c(Y_\Gamma, L_k(\mathbb{C}))$$

There is a cup product pairing

$$H^1_c(Y_\Gamma, L_k(\mathbb{C})) \times H^1(Y_\Gamma, L_k(\mathbb{C})) \to \mathbb{C}$$

Together with the Petersson product on modular forms, one can use these two pairings to show the injectivity. Using the standard dimension results in the theory of modular forms and algebraic topology, one can show that both sides have the same dimension. □

Let f be an eigenform. Then for all operator T in Hecke algebra $\mathcal{H}$ we have

$$T(f) = \lambda_f(T) f$$

where $\lambda_f(T)$ is the eigenvalue. It gives rise a homomorphism $\lambda_f : \mathcal{H} \to \mathbb{C}$, $T \mapsto \lambda_f(T)$. We call λ_f is the eigenpacket associated to f.

Definition 4.1.19. Let $f \in S^{new}_{k+2}(\Gamma, \mathbb{C})$ be a newform and let $\lambda_f : \mathcal{H} \to \mathbb{C}$ be its eigenpacket. If M is a space with an action of the Hecke algebra $\mathcal{H}$, then define

$$\begin{aligned} M[f] &:= \text{f-eigenvalue of } \mathcal{H} \text{ in } M \\ &= \{m \in M : T(m) = \lambda_f(T)m,\ \forall T \in \mathcal{H}\} \end{aligned}$$

Proposition 4.1.20. *We have*

$$\dim_{\mathbb{C}} \mathrm{Symb}_{\Gamma}(L_k(\mathbb{C})[f] = 2$$

Proof. The eiegenpacket λ_f cannot occur in $\mathcal{E}_{k+2}(\Gamma, \mathbb{C})$, since the T_p-eigenvalue of an Eisenstein series at a prime p is of size approximately p^k, whilst for cusp forms, we have the estimate $a_p(f) \leq Cp^{p/2}$. It appears exactly once in both $S_{k+2}(\Gamma, \mathbb{C})$ and $\overline{S_{k+2}}(\Gamma, \mathbb{C})$, and hence the space of modular symbols is of dimensional two. □

Let $\iota = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ we have the following decomposition.

Proposition 4.1.21. *We have a Hecke-stable decomposition*

$$\mathrm{Symb}_{\Gamma}(L_k(\mathbb{C}) \simeq \mathrm{Symb}^{+}_{\Gamma}(L_k(\mathbb{C}) \oplus \mathrm{Symb}^{-}_{\Gamma}(L_k(\mathbb{C})$$

into the ± 1 *eigenspaces of the involution* ι

More generally, we can consider modular symbol with algebraic coefficients. If multiplication by 2 is invertible on A, then we can decompose any modular symbol $\Phi \in \mathrm{Symb}_{\Gamma_0(N)}(A)$ in a unique way as a sum

$$\Phi = \Phi^{+} + \Phi^{-}$$

where $\Phi^{\pm}|\iota = \pm\Phi^{\pm}$. Let

$$\mathrm{Symb}_{\Gamma_0(N)}(A) = \mathrm{Symb}_{\Gamma(N)}(A)^{+} \oplus \mathrm{Symb}_{\Gamma_0(N)}(A)^{-}$$

be the corresponding decomposition of the space of modular symbols.

Theorem 4.1.22. ***(Manin-Shimura)*** *Let $f \in S_k(\Gamma_0(M))$ be a common eigenform for the operators T_p, p prime, let $\mathcal{O}(f)$ be the ring of algebraic integers generated by the eigenvalues, and let $K(f)$ be the fraction field of $\mathcal{O}(f)$. Then for either choice of sign $\pm$, the Hecke eigen space associated to f in $\mathrm{Symb}_{\Gamma_0(M)}\left(L_k(K(f))\right)^{\pm}$ is one dimensional over $K(f)$.*

Moreover, there are 'periods' $\Omega_f^{\pm} \in \mathbb{C}^{\times}$ such that the modular symbols

$$\varphi_f^{\pm} = (\Omega_f^{\pm})^{-1}\psi_f^{\pm}$$

generates these eigenspaces and are defined over $\mathcal{O}(f)$, i.e. take values in $L_k(\mathcal{O}(f))$

4.2 p-adic Measures

Fix a prime $p > 0$ and $v : \mathbb{Q}_p \to \mathbb{Z} \cup \{\infty\}$ the p-adic valuation.

Definition 4.2.1. Let E be a $\mathbb{Q}_p$-vector space with a valuation $w : E \to \mathbb{R} \cup \{\infty\}$ such that

1. $w(x+y) \geq \min\{w(x), w(y)\}$ for all $x, y \in E$
2. $w(ax) = v(a) + w(x)$ for all $a \in \mathbb{Q}_p$, $x \in E$.

We say E is a $\mathbb{Q}_p$-Banach space if E is complete with respect to the topology defined by the valuation w.

Proposition 4.2.2. *Define*

$$\mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p) := \{f : \mathbb{Z}_p \to \mathbb{Q}_p |\ f \text{ is continuous}\}$$

and $w(f) := \inf_{x \in \mathbb{Z}_p} v(f(x)) \in \mathbb{Z} \cup \{\infty\}$ *(giving rise to the supremum norm). Then* $\mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$ *with the valuation* w *is a* $\mathbb{Q}_p$*-Banach space.*

Proof. Refer [Col] □

Proposition 4.2.3. *For* $k \in \mathbb{N}_{n \geq 1}$ *define*

$$LC_k := \{f : \mathbb{Z}_p \to \mathbb{Q}_p | \forall a \in \mathbb{Z}_p, f|_{U_{a,k}} \text{is constant}\}$$

where $U_{a,k} = a + p^k \mathbb{Z}_p$. *Denote* $LC := \bigcup_{k \geq 1} LC_k$ *all locally constant functions on* $\mathbb{Z}_p$. *Then* $LC \subset \mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$ *is dense.*

Proof. Refer [Col] □

More generally, let X be a profinite abelian group. We denote $\mathcal{C}(X, \mathbb{Q}_p)$ denote the module of $\mathbb{Q}_p$-valued continuous functions on X and $LC(X)$ denote the submodule of locally constant functions.

We equip $\mathcal{C}(X, \mathbb{Q}_p)$ with the topology induced by the supremum norm and we also have $LC(X)$ is dense in $\mathcal{C}(X, \mathbb{Q}_p)$.

Definition 4.2.4. Define the space $\mathrm{Meas}(X)$ of $\mathbb{Q}_p$-valued measures on X to be the dual $\mathrm{Hom}_{cont}(\mathcal{C}(X,\mathbb{Q}_p),\mathbb{Q}_p)$ equipped with the strong topology.

$$\mathrm{Meas}(X) := \mathrm{Hom}_{cont}(\mathcal{C}(X,\mathbb{Q}_p),\mathbb{Q}_p)$$

If $\phi \in \mathcal{C}(X,L)$ and $\mu \in \mathrm{Meas}(X)$ the evaluation of μ at ϕ will be denoted by

$$\int_X \phi(x)\cdot\mu(x) \text{ or shortly } \int_X \phi\cdot d\mu$$

We say that an element $\mu \in \mathrm{Meas}(X)$ is an $\mathbb{Z}_p$-valued measure, and write $\mu \in \mathrm{Meas}(X,\mathbb{Z}_p)$, if μ takes values in $\mathbb{Z}_p$.

Proposition 4.2.5. *We have*

$$\mathrm{Meas}(X,\mathbb{Q}_p) = \mathrm{Meas}(X,\mathbb{Z}_p)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$$

Proof. Since $\mathbb{Z}_p$ is compact and measures are continuous, or equivalently bounded. It follows that for all $\mu \in \mathrm{Meas}(X,\mathbb{Q}_p)$ there is $c \in \mathbb{Z}_p$ such that $c\mu \in \mathrm{Meas}(X,\mathbb{Z}_p)$. Thus we obtain $\mu = c\mu \otimes c^{-1}$

□

Remark 4.2.6. We can think of measures as additive functions

$$\mu : \{\text{compact open subsets of X}\} \to \mathbb{Z}_p$$

Indeed, let $\phi \in \mathcal{C}(X,\mathbb{Z}_p)$. Assume first that ϕ is locally constant. Then there exists some open subgroup U of X such that we can view ϕ as a function on X/U. We define the integral of ϕ against μ to be

$$\int_X \phi\cdot\mu := \sum_{[a]\in X/U} \phi(a)\mu(aU)$$

If ϕ is continuous, we can write $\phi = \lim_{n\to\infty}\phi_n$, where each ϕ_n is locally constant. Then we can define

$$\int_X \phi\cdot\mu := \lim_{n\to\infty}\int_X \phi_n\cdot\mu$$

which exists and is independent of the choice of ϕ_n.

Conversely, if $\mu \in \mathrm{Meas}(X,\mathbb{Z}_p)$ and $U \subset X$ is and open compact set, one defines

$$\mu(U) := \int_X \mathbf{1}_U(x)\cdot\mu(x)$$

the value of μ on the characteristic function of U.

Proposition 4.2.7. *We have an isomorphism*

$$\mathrm{Meas}(X, \mathbb{Z}_p) \simeq \varprojlim_U \mathbb{Z}_p[X/U]$$

where the limit is over all open subgroups of X.

Proof. We define the map from $\mathrm{Meas}(X, \mathbb{Z}_p)$ to $\varprojlim_U \mathbb{Z}_p[X/U]$ as follows. Let μ be a measure in $\mathrm{Meas}(X, \mathbb{Z}_p)$, define an element $\lambda_U \in \mathbb{Z}_p[X/U]$ given by

$$\lambda_U = \sum_{[a] \in X/U} \mu(aU)[a]$$

By the additivity property of μ, we see that $(\lambda_U) \in \varprojlim_U \mathbb{Z}_p[X/U]$.

Conversely, given an element $\lambda \in \varprojlim_U \mathbb{Z}_p[X/U]$, write λ_U for its image in $\mathbb{Z}_p[X/U]$ under the natural projection. Then

$$\lambda_U = \sum_{[a] \in X/U} c_a[a]$$

We define

$$\mu(aH) = c_a$$

Since the λ_U is compatible under the projection maps, this defines an additive function on the open compact subgroups of G. □

In particular, we can determine the structure of $\mathrm{Meas}(\mathbb{Z}_p^\times, \mathbb{Z}_p)$ explicitly via Dirac measure.

Definition 4.2.8. For each $t \in \mathbb{Z}_p^\times$, let $\delta_t \in \mathrm{Meas}(\mathbb{Z}_p^\times)$ be the Dirac measure given by the integral

$$\int f d\delta_t = f(t)$$

for $f \in \mathcal{C}(\mathbb{Z}_p^\times, \mathbb{Q}_p)$, i.e., δ_t is the linear functional evaluation at t.

Under the indentification of measures with additive functions on open compact subsets of $\mathbb{Z}_p^\times$, we find that this corresponds to the function

$$\tilde{\delta}_t(U) = \begin{cases} 1 & \text{if } a \in U \\ 0 & \text{if } a \notin U \end{cases}$$

As an element of the inverse limit, we find that at finite level δ_t corresponds to the the basis element $[a + p^n\mathbb{Z}_p] \in \mathbb{Z}_p[(\mathbb{Z}_p/p^n\mathbb{Z}_p)^\times]$ with $a \neq 0$, denoted by $[a]$.

Proposition 4.2.9. *The map $t \mapsto \delta_t$ defines a continuous map $\mathbb{Z}_p^\times \to \mathrm{Meas}(\mathbb{Z}_p^\times, \mathbb{Z}_p)$. Then it can be uniquely extended to a continuous $\mathbb{Z}_p$-isomorphism*

$$\mathbb{Z}_p[[\mathbb{Z}_p^\times]] \to \mathrm{Meas}(\mathbb{Z}_p^\times, \mathbb{Z}_p)$$

Let $(\mathbb{Z}_p^2)'$ denote the set of primitive vectors in $\mathbb{Z}_p^2$ (i.e. vectors which are not divisible by p) and consider the canonical projection

$$(\mathbb{Z}_p^2)' \to \mathbb{P}^1(\mathbb{Q}_p)$$

sending (x, y) in affine coordinates to $[x, y]$ in projective coordinates. The fibers of this map are just the orbits of the scalar action of $\mathbb{Z}_p^\times$.

Definition 4.2.10. For X a compact open subset of $\mathbb{P}^1(\mathbb{Q}_p)$, we set

$$U(X) := \{(x, y) \in (\mathbb{Z}_p^2)' | [x, y] \in X\}$$

Thus, $U(X)$ is the preimage of X in $(\mathbb{Z}_p^2)'$. Define

$$\mathbb{D}(X) := \mathrm{Meas}(U(X))$$

When $X = \mathbb{P}^1(\mathbb{Q}_p)$, we will simply write $\mathbb{D}$.

Remark 4.2.11. For an arbitrary compact open set $X \subseteq \mathbb{P}^1(\mathbb{Q}_p)$, the scalar action of $\mathbb{Z}_p^\times$ on $U(X)$ induces a continuous action of $\mathbb{Z}_p^\times$ on $\mathbb{D}$. For all $\lambda \in \mathbb{Z}_p^\times$ and $\mu \in \mathbb{D}$

$$\int f(x, y)d(\lambda\mu) := \int f(\lambda x, \lambda y)d\mu$$

Hence $\mathbb{D}(X)$ is endowed with a natural structure as continuous $\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$-module

Denote $M_2(\mathbb{Z}_p)$ the semigroup of 2×2 matrices over $\mathbb{Z}_p$. Consider the elements of $\mathbb{Z}_p^2$ as row vectors, let $M_2(\mathbb{Z}_p)$ act by matrix multiplication on the right. This induces an action of $M_2(\mathbb{Z}_p)$ on $\mathrm{Cont}(\mathbb{Z}_p^2)$ by the formula

$$(\sigma f)(v) = f(v\sigma)$$

for $\sigma \in M_2(\mathbb{Z}_p)$ and $f \in \mathrm{Cont}(\mathbb{Z}_p^2)$.

We can endow $\mathbb{D}$ with a natural structure as $\mathbb{Z}_p[[\mathbb{Z}_p^\times]][M_2(\mathbb{Z}_p)]$-module as follows. Identifying $\mathrm{Cont}((\mathbb{Z}_p^2)')$ with the submodule of $\mathrm{Cont}(\mathbb{Z}_p^2)$ consisting of functions supported on $(\mathbb{Z}_p^2)'$, we have that $\mathrm{Cont}((\mathbb{Z}_p^2)') \subseteq \mathrm{Cont}(\mathbb{Z}_p^2)$ is preserved by the action of $M_2(\mathbb{Z}_p)$. We endow $\mathrm{Cont}((\mathbb{Z}_p^2)')$ with this action of $M_2(\mathbb{Z}_p)$ and endow $\mathbb{D}$ with the dual action. Hence, for $\mu \in \mathbb{D}$, $\sigma \in M_2(\mathbb{Z}_p)$, and $f \in \mathrm{Cont}((\mathbb{Z}_p^2)')$

$$\int f \,\mathrm{d}\,\mu|\sigma = \int (\sigma f)\,\mathrm{d}\,\mu$$

This action commutes with the action of $\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$ on $\mathbb{D}$. Hence $\mathbb{D}$ is endowed with a natural structure as $\mathbb{Z}_p[[\mathbb{Z}_p^\times]][M_2(\mathbb{Z}_p)]$-module.

4.3 p-Ordinary Λ-adic Modular Symbols

We fix N a positive integer that is not divisible by p.

Definition 4.3.1. For an integer $k \geq 2$ we define the specialization map $\phi_k : \mathbb{D} \to L_k(\mathbb{Z}_p)$ by

$$\mu \mapsto \int_{\mathbb{Z}_p^\times \times \mathbb{Z}_p} (xY - yX)^{k-2} \,\mathrm{d}\,\mu(x,y)$$

Remark 4.3.2. The specialization homomorphism $x_k : \Lambda \to \mathbb{Z}_p$, $[u] \mapsto u^{k-2}$ gives $L_k(\mathbb{Z}_p)$ a Λ-module structure.

Let $\Gamma_0(p\mathbb{Z}_p)$ denote the set of matrices in $\mathrm{GL}_2(p\mathbb{Z}_p)$ that are upper triangular modulo p.

Proposition 4.3.3. *The homomorphism ϕ_k induces a morphism $\phi_{k,*}$ by the composition*

$$\mathrm{Symb}_{\Gamma_0(N)}(\mathbb{D}) \to \mathrm{Symb}_{\Gamma(Np)}(L_k(\mathbb{Z}_p))$$

Proof. The map $\phi_{k,*}$ is $\Gamma_0(p\mathbb{Z}_p)$-equivariant since the matrices used to define the Hecke operators are upper triangle. That is,

$$\phi_{k,*}(\mu|\gamma) = \phi_{k,*}(\mu)|\gamma$$

for $\mu \in \mathrm{Symb}_{\Gamma_0(N)}(\mathbb{D})$ and $\gamma \in \Gamma_0(p\mathbb{Z}_p)$.

Hence, for $\mu \in \mathrm{Symb}_{\Gamma_0(N)}(\mathbb{D})$ and $\gamma \in \Gamma_0(Np)$, and $P = (xY - yX)^{k-2}$ we obtain

$$\begin{aligned}\phi_{k,*}(\mu|\gamma)\{c_2-c_2\}(P) &= \int_{\mathbb{Z}_p\times\mathbb{Z}_p^\times} P d(\mu|\gamma)\{c_2-c_1\}\\ &= \int_{\mathbb{Z}_p\times\mathbb{Z}_p^\times} P d\left(\mu\{\gamma c_2-\gamma c_1\}\right)|\gamma\\ &= \int_{\gamma(\mathbb{Z}_p\times\mathbb{Z}_p^\times)} P|\gamma d\mu\{\gamma c_2-\gamma c_1\}\end{aligned}$$

Note that $\gamma(\mathbb{Z}_p\times\mathbb{Z}_p^\times)=\mathbb{Z}_p\times\mathbb{Z}_p^\times$ if γ is upper triangular modulo p. Hence

$$\left(\phi_k(\mu)|\gamma\right)\{c_2-c_1\}(P)=\int_{\mathbb{Z}_p\times\mathbb{Z}_p^\times} P|\gamma d\mu\{\gamma c_2-\gamma c_1\}$$

The proposition follows from $\Gamma_0(N)\cap\Gamma_0(p\mathbb{Z}_p)=\Gamma_0(Np)$. □

The space $\mathrm{Symb}_{\Gamma_0(N)}(\mathbb{D})$ is an infinite dimensional Λ-module. We restrict our attention to the ordinary part we obtain the following exact sequence to get a finite dimensional subspace.

Definition 4.3.4. Let $e_{ord}=\lim_{n\to\infty}U_p^{n!}$ be the Hida's projector and Γ be a congruence subgroup. The ordinary subspace of $\mathrm{Symb}_\Gamma(X)$ is given by

$$\mathrm{Symb}^0_\Gamma(X):=e_{ord}\,\mathrm{Symb}_\Gamma(X)$$

Definition 4.3.5. Let $\kappa\in\mathcal{X}_0:=\mathrm{Hom}(\mathbb{Z}_p[[\mathbb{Z}_p^\times]],\overline{\mathbb{Q}_p})$, we say that a function $\varphi:(\mathbb{Z}_p^2)'\to\overline{\mathbb{Q}_p}$ is homogeneuous of degree κ if $\varphi(t\mathbf{x})=\kappa(t)\varphi(\mathbf{x})$ for every $t\in\mathbb{Z}_p^*$ and every $\mathbf{x}\in(\mathbb{Z}_p^2)'$.

Let $\gamma\in\mathbb{Z}_p^\times$ be a topological generator of $1+p\mathbb{Z}_p$ and let $[\gamma]\in\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$ be the corresponding element of the completed group ring. For each integer $k\geq 2$, consider $\pi_k:=[\gamma]-\gamma^{k-2}\in\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$. Every element in $\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$ can be viewed as a character on $\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$ as obvious way $[\alpha]\mapsto\alpha^{k-2}$.

Lemma 4.3.6. *Let $\gamma\in\mathbb{Z}_p^\times$ be a topological generator of $1+p\mathbb{Z}_p$ and let $\pi_k:=[\gamma]-\gamma^{k-2}\in\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$. Define*

$$P_{\pi_k}=\{a\in\mathbb{Z}_p[[\mathbb{Z}_p^\times]]|\pi_k\cdot a=0\}$$

be the prime ideal associated to π_k. A measure $\mu\in\mathbb{D}$ lies in $P_{\pi_k}\mathbb{D}$ if and only if $\int\varphi d\mu=0$ for every continuous function φ on $(\mathbb{Z}_p^2)'$ which is homogeneous of degree π_k.

Proof. $\Rightarrow$ Assume that $\mu \in P_{\pi_k}\mathbb{D}$, then $\mu = \sum_{i\in I} a_i\mu_i$ with I is finite and $a_i \in P_{\pi_k}$, $\mu_i \in \mathbb{D}$. Note that $\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$ acts as scalar on the integral, it follows that

$$\int \varphi d\mu = \sum_i \int \varphi d\left(a_i\mu_i\right) = \sum_i \mu_i\left(\pi_k \cdot a_i\varphi_i\right) = 0$$

for all continuous function φ which is homogeneous of degree π_k.

Conversely, consider the multiplication by π_k on the ring of continuous functions on $(\mathbb{Z}_p^2)'$ with values on $\overline{\mathbb{Q}_p}$

$$\mathcal{C}((\mathbb{Z}_p^2)') \xrightarrow{\cdot\pi_k} \mathcal{C}((\mathbb{Z}_p^2)').$$

We compute the kernel of this map. Let $f \in \mathcal{C}((\mathbb{Z}_p^2)')$ be a continuous on $\mathbb{Z}_p^2$, we have

$$\pi_k f(\mathbf{x}) = ([\gamma] - \gamma^{k-2})f(\mathbf{x}) = f(\gamma\mathbf{x}) - \gamma^{k-2}f(\mathbf{x})$$

It follows that $f \in \ker(\pi_k)$ precisely when $f(\gamma\mathbf{x}) = \gamma^{k-2}f(\mathbf{x})$. Hence for all $n \in \mathbb{Z}$ we have $f(\gamma^n\mathbf{x}) = (\gamma^n)^{k-2}f(\mathbf{x})$. As γ is the generator of $1 + p\mathbb{Z}_p$ and f is continuous, we obtain for every $\alpha \in 1 + p\mathbb{Z}_p$, we have

$$f(\alpha\mathbf{x}) = \alpha^{k-2}f(\mathbf{x})$$

By definition f is a homogeneous polynomial of degree π_k. By definitions, the measure $\mathbb{D}$ is a dual of $\mathcal{C}((\mathbb{Z}_p^2)', \overline{\mathbb{Q}_p})$, and $P_{\pi_k}\mathbb{D}$ is the dual of homogeneous space of $\mathbb{D}$. Thus, if $\int \varphi d\mu = 0$ for every continuous function φ on $(\mathbb{Z}_p^2)'$ which is homogeneous of degree π_k then $\mu \in P_{\pi_k}\mathbb{D}$. □

For each integer $m > 0$ let $\varphi_{\pi_k}^{(m)}$ be the continuous function on $(\mathbb{Z}_p^2)'$ given by

$$\varphi_{\pi_k}^{(m)}(a,b) = \begin{cases} \pi_k \cdot a & \text{if } b \equiv 0 \mod p^m \\ 0 & \text{otherwise} \end{cases}$$

Lemma 4.3.7. *Let $\Phi \in W = \mathrm{Symb}_{\Gamma_0(N)}(\mathbb{D}) \subset \mathrm{Hom}(\mathcal{D}_0, \mathbb{D})$ be a Λ-adic modular symbol. Then the following are equivalent*

1. $\Phi \in P_{\pi_k}W$
2. $\int_{\pi_k} \varphi d\Phi(D) = 0$ *for all $D \in \mathcal{D}_0$ and all continuous functions φ homogeneous of degree*

3. $\int \varphi_\kappa^{(m)} d\Phi(D) = 0$ *for all* $D \in \mathcal{D}_0$ *and all* $m > 0$

Proof. $1 \Leftrightarrow 2$ Since P_{π_k} is a principal ideal, we have $P_{\pi_k} W = \mathrm{Symb}_\Gamma(P_{\pi_k}\mathbb{D})$. Hence, we have that $\Phi \in P_{\pi_k} W$ if and only if $\Phi(D) \in P_{\pi_k}\mathbb{D}$ for all $D \in \mathcal{D}_0$. So the equivalence follows from the previous lemma.

$2 \Leftrightarrow 3$ The implication follows a priori. Now assume that 3 is true. Then for every $\gamma \in \Gamma_0(N)$

$$\int \gamma\varphi_{\pi_k}^{(m)} d\Phi(D) = \int \varphi_{\pi_k}^{(m)} d\Phi(\gamma D) = 0$$

So 2 follows from the fact that every continuous function φ is homogeneous of degree π_k is the uniform limit of a sequence of linear combinations of the functions $\gamma\varphi_{\pi_k}^{(m)}$. □

Proposition 4.3.8. *The group* $W^0 = \mathrm{Symb}_{\Gamma_0(N)}(\mathbb{D})^0$ *of ordinary* Λ*-adic modular symbols is a free* Λ*-module of finite rank. Then for* $\Phi \in W^0$*, let* $\Phi_{\pi_k} := \phi^0_{k,*}(\Phi) \in \mathrm{Symb}_{\Gamma_0(Np)}(L_k(\mathbb{Z}_p))^0$*. Then we have* $\Phi_{\pi_k} = 0$ *if and only if* $\Phi \in P_{\pi_k} W^0$*.*

Proof. We first prove that $\ker(\phi^0_{k,*}) = P_{\pi_k} W^0$. Recall that for $\Phi \in W$ the specialization Φ_k is the element of $\mathrm{Symb}_\Gamma(L_k(\mathbb{Z}_p))$ whose value on a divisor $D \in \Delta_0$ is given by

$$\Phi_k(D) = \int_{\mathbb{Z}_p^* \times \mathbb{Z}_p} (xY - yX)^{k-2} d\Phi(D)$$

Since the integral is homogeneous of degree π_k, the inclusion $P_{\pi_k} W \subseteq \ker(\phi^0_{k,*})$ follows from the implication (1) ⇒ (2) of the previous lemma.

Conversely, suppose $\Phi \in W^0$ and that Φ_{π_k}. We will show that $\Phi \in P_{\pi_k} W^0$ by using $3 \Rightarrow 1$ from lemma . Fix $m > 0$ and $D \in \mathcal{D}_0$. Since Φ is ordinary, there is a $\Psi \in W^0$ such that $\Psi | T_p^m = \Phi$. The action of the operator T_p and its power T_p^m on W can be described precisely as follows. Consider the reduction map $(\mathbb{Z}_p^2)' \to \mathbb{P}^1(\mathbb{Z}/p^m\mathbb{Z})$. For each $\mathbf{x} \in \mathbb{P}^1(\mathbb{Z}/p^m\mathbb{Z})$ the preimage of $\mathbf{x}$ in $(\mathbb{Z}_p^2)'$ is a compact open set which we denote by $U(\mathbf{x}, p^m)$. Choose a matrix $g_{\mathbf{x},p^m}$ with determinant p^m for which $U(\mathbf{x}, p^m) \subseteq ((\mathbb{Z}_p^2)')g_{\mathbf{x},p^m}$. If $\mathbf{x} = [1, a]$ with $a \in \mathbb{Z}_p/p^m\mathbb{Z}_p = \mathbb{Z}/p^m\mathbb{Z}$, we can choose an element $g_{\mathbf{x},p^m} = \begin{pmatrix} 1 & a \\ 0 & p^m \end{pmatrix}$ mod p^m. The coset $\Gamma g_{\mathbf{x},p^m}$ is independent of the choice of $g_{\mathbf{x},p^m}$ with this property. Then we have the identity

$$\int \varphi_{\pi_k}^{(m)} d\Phi(D) = \sum_{\mathbf{x}\in\mathbb{P}^1(\mathbb{Z}/p^m\mathbb{Z})} \int g_{\mathbf{x},p^m}\varphi_{\pi_k}^{(m)} d\Psi(g_{\mathbf{x},p^m}\cdot D)$$

a sum of modular symbols which are supported on the disjoint compact open sets $U(\mathbf{x}, p^m)$. But $g_{\mathbf{x},p^m}\varphi_{\pi_k}^{(m)} = 0$ unless $\mathbf{x} = [1, 0]$. Hence the above integral is equal to

$$\int g_{[1,0],p^m}\varphi_{\pi_k}^{(m)} d\Psi(g_{[1,0],p^m}\cdot D) = \int_{\mathbb{Z}_p^*\times\mathbb{Z}_p} x^{k-2} d\Psi(g_{[1,0],p^m}\cdot D)$$

But this vanishes since it is the coefficient of Y^r in $\phi_{k,*}^0(\Phi)(g_{[1,0],p^m}\cdot D)$. Therefore $\ker(\phi_{k,*}^0) = P_{\pi_k}W^0$. It follows from this and the compact Nakayama's lemma that W^0 is a free Λ-module of finite rank. □

The following theorem allow us to lift an ordinary symbol from $\mathrm{Symb}_{\Gamma_0(Np)}(L_k(\mathbb{Z}_p))$ to $\mathrm{Symb}_{\Gamma_0(N)}(\mathbb{D})$ via $\phi_{k,*}$.

Theorem 4.3.9. *Fix a topological generator $\gamma \in \mathbb{Z}_p^\times$ and let $[\gamma] \in \mathbb{Z}_p[[\mathbb{Z}_p^\times]]$ be the corresponding element of the completed group ring. For each integer $k \geq 2$, let $\pi_k := [\gamma] - \gamma^{k-2} \in \mathbb{Z}_p[[\mathbb{Z}_p^\times]]$. Then the sequence*

$$0 \to \mathrm{Symb}_{\Gamma_0(N)}(\mathbb{D})^0 \overset{\pi_k}{\to} \mathrm{Symb}_{\Gamma_0(N)}(\mathbb{D})^0 \overset{\phi_{k,*}^0}{\to} \mathrm{Symb}_{\Gamma_0(Np)}(L_k(\mathbb{Z}_p))^0 \to 0$$

is an exact sequence of $\mathcal{H}$-modules.

Proof. By the previous proposition we see that $\mathrm{Symb}_{\Gamma_0(N)}(\mathbb{D})^0$ is a torsion-free Λ-module, so the multiplication by π_k is injective. Furthermore, every polynomial is continuous, we obtain the inclusion $L_k(\mathbb{Z}_p) \subset \mathbb{D}$ and taking duality we get the surjective map $\mathrm{Symb}_{\Gamma_0(N)}(\mathbb{D}) \to \mathrm{Symb}_{\Gamma_0(Np)}(L_k(\mathbb{Z}_p))$. Again, by the previous lemma we get

$$\mathrm{Symb}_{\Gamma_0(N)}(\mathbb{D}^0/\Big(\pi_k \cdot \mathrm{Symb}_{\Gamma_0(N)}(\mathbb{D}^0\Big) \simeq \mathrm{Symb}_{\Gamma_0(Np)}(L_k(\mathbb{Z}_p))$$

□

For each $r \geq 1$, let $\Gamma_r := \Gamma_0(N) \cap \Gamma_1(p^r)$ $(r \geq 1)$. Also, we define

$$\mathbb{D}_r := \{\mu : \big((\mathbb{Z}/p^r\mathbb{Z})^2\big)' \to \mathbb{Z}_p\}$$

the module of $\mathbb{Z}_p$-valued functions on the set of primitive elements of $\big((\mathbb{Z}/p^r\mathbb{Z})^2\big)'$ equipped with the natural action of $\Gamma_0(N)$.

Lemma 4.3.10. *The $\mathbb{Z}_p[[\mathbb{Z}_p^\times]][\Gamma_0(N)]$-module $\mathbb{D}$ is isomorphic to the projective limit $\varprojlim_r \mathbb{D}_r$.*

Proof. Consider the map

$$\begin{aligned}\Gamma_r \setminus \Gamma_0(N) &\to \left((\mathbb{Z}/p^r\mathbb{Z}\right)' \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} &\mapsto (c,d) \mod p^r\end{aligned}$$

is a bijective. Hence, it induces an isomorphism

$$\mathbb{D}_r \simeq \mathrm{Ind}_{\Gamma_r}^{\Gamma_0}(\mathbb{Z}_p)$$

It follows that we can define the projective system $\{\mathbb{D}_r\}$ by

$$\begin{aligned}&\mathbb{D}_{r+1} \longrightarrow \mathbb{D}_r \\ &\mu_{r+1} \mapsto \mu_r : x \mapsto \sum_{y \equiv x \mod p^r} \mu_{r+1}(y)\end{aligned}$$

Taking the projective limit we have $\mathbb{D} \simeq \varprojlim_r \mathbb{D}_r$. □

Proposition 4.3.11. *Let H_* denote either H^1, H^1_c, or H^1_{par} we have*

$$H^1_*(\Gamma_0(N), \mathbb{D}) \cong \varprojlim_r H^1_*(\Gamma_r, \mathbb{Z}_p)$$

Proof. By Sharipo's lemma we have $H^1_*(\Gamma_0(N), \mathbb{D}_{r+1}) \simeq H^1_*(\Gamma_{r+1}, \mathbb{Z}_p)$. Hence, we get the commutative diagram

$$\begin{array}{ccc} H^1_*(\Gamma_0(N), \mathbb{D}_{r+1}) & \longrightarrow & H^1_*(\Gamma_0(N), \mathbb{D}_r) \\ \downarrow \sim & & \downarrow \\ H^1_*(\Gamma_{r+1}, \mathbb{Z}_p) & \xrightarrow{cores} & H^1_*(\Gamma_r, \mathbb{Z}_p) \end{array}$$

Taking the projective limit and by the previous proposition we obtain the isomorphism

$$H^1_*(\Gamma_0(N), \mathbb{D}) \cong \varprojlim_r H^1_*(\Gamma_r, \mathbb{Z}_p)$$

□

Theorem 4.3.12. *There is an isomorphism of covariant Hecke modules*

$$H^1_{par}(\Gamma_r, \mathbb{Z}_p) \cong Ta_p(J_r)$$

for each $r \geq 1$. Hence we obtain an isomorphism of covariant Hecke modules

$$H^1_{par}(\Gamma_0(N), \mathbb{D}) \cong Ta_p(J_\infty)$$

Proof. For each $r \geq 1$, there is an isomorphism of Hecke modules due to Shimura [Shi]

$$H^1_{par}(\Gamma_r, \mathbb{Z}_p) \simeq Ta_p(J_r)$$

Recall that $\varprojlim_r Ta_p(J_r) \simeq Ta_p(J_\infty)$ by Hida's theory, we obtain

$$H^1_{par}(\Gamma_0(N), \mathbb{D}) = \varprojlim_r H^1_{par}(\Gamma_r, \mathbb{Z}_p) \simeq \varprojlim_r Ta_p(J_r) \simeq Ta_p(J_\infty)$$

□

Theorem 4.3.13. *Let E be a modular elliptic curve of tame conductor N with either good ordinary or multiplicative reduction at the prime $p \geq 5$. Assume that Hida's deformation ring $\mathcal{R}_E$ satisfies $\mathcal{R}_E = \Lambda$. Let $h_E : \mathcal{H} \to \Lambda$ be the homomorphism given by Hida's theorem. Then for either choice of sign $\pm$, the submodule $\mathrm{Symb}_{\Gamma_0(N)}(\mathbb{D})^{0,\pm}$ on which $\mathcal{H}$ acts via h_E has rank one as a Λ-module.*

Let $\psi_E \in \mathrm{Symb}_{\Gamma_0(Np)}(\mathbb{C})$ be the modular symbol associated to the p-stabilized newform f_E and fix a choice of period $\Omega_E^{\pm} \in \mathbb{C}^\times$ as in theorem [] so that the modular symbols $\varphi_E^{\pm} := \dfrac{\psi_E^{\pm}}{\Omega_E^{\pm}}$ are defined over $\mathbb{Z}_p$, i.e. $\varphi_E^{\pm} \in \mathrm{Symb}_{\Gamma_0(Np)}(\mathbb{Z}_p^{0,\pm}$. Then there is a Hecke eigensymbol $\Phi_E^{\pm} \in \mathrm{Symb}_{\Gamma_0(N)}(\mathbb{D})^{0,\pm}$ such that

1. *$\phi_{2,*}\Phi_E^{\pm} = \varphi_E^{\pm}$*
2. *the Hecke operators act on $\Phi_E^{\pm}$ via h_E.*

Proof. Applying Hida's theorem to the isomorphism $H^1_{par}(\Gamma_0(N), \mathbb{D}) \cong Ta_p(J_\infty)$ we obtain that for either choice of sign $\pm$, the h_E-eigensubmodule of $H^1_{par}(\Gamma_0(N), \mathbb{D})^{0,\pm}$ has rank one. Since $\mathrm{Symb}_{\Gamma_0(N)}(\mathbb{D}) \cong H^1_c(\Gamma_0(N), \mathbb{D})$, we have a surjective map

$$\mathrm{Symb}_{\Gamma_0(N)}(\mathbb{D}) \to H^1_{par}(\Gamma_0(N), \mathbb{D})$$

whose kernel is Eisenstein, hence the kernel has no nontrivial h_E-eigenvectors. It follows that the above map induces an injective homomorphism

$$\mathrm{Symb}_{\Gamma_0(N)}(\mathbb{D})_{h_E} \to H^1_{par}(\Gamma_0(N), \mathbb{D})_{h_E}$$

on the h_E-eigensubmodules and moreover that the cokernel of this map is a torsion Λ-module whose annihilator is not contained in the augmentation ideal. □

4.4 Two Variable p-adic L-functions

4.4.1 p-adic L-functions

We revisit one variable p-adic L-functions. Now suppose that $M = Np$ where $p \not| N$, and let $f \in S_k(\Gamma_0(Np))$ be a p-ordinary eigenform. For simplicity we assume that the Fourier coefficients of f are rational integers, hence the eigenvalues of the operators T_p are also integral. If $a_p \in \mathbb{Z}_p$ is the eigenvalue of T_p on f, the p-ordinary means a_p is not divisible by p. Now choose a real period Ω_f^+ so that the modular symbol $\varphi_f^+ := \dfrac{1}{\Omega_f^+}\psi_f^+$ is defined over $\mathbb{Z}$.

Definition 4.4.1. Define a measure $\nu_f \in \mathrm{Meas}(\mathbb{Z}_p^\times)$ by

$$\nu_f(a + p^m\mathbb{Z}_p) = \frac{1}{a_p^{-m}}\varphi_f^+\left(\{\frac{a}{p^m}\} - \{i\infty\}\right)|_{X=0,Y=1}$$

for each $a \in \mathbb{Z}$ prime to p, and each $m > 0$.

It follows from the fact that f is an eigenform for T_p with eigenvalue a_p that this defines a finitely additive function on the compact open subset of $\mathbb{Z}_p^\times$. Since a_p is a p-adic unit, the values of ν_f are p-adic integer, hence $\nu_f \in \mathrm{Meas}(\mathbb{Z}_p^\times)$.

Definition 4.4.2. The p-adic L-function associated to f and the fixed choice of a real period Ω_f^+ is defined by

$$L_p(f, s) = L_p(\nu_f, s) := \int_{\mathbb{Z}_p^\times} \langle t\rangle^{s-1}\, d\nu(t), \quad s \in \mathbb{Z}_p$$

4.4.2 Constructing two-variables p-adic L-function

Let E be a elliptic curve defined over $\mathbb{Q}$ having conductor M and either good ordinary or multiplicative reduction at p. Choose a real period Ω_E for E so that the normalized modular symbol

$$\varphi_E = \Omega_E^{-1} \cdot \psi_E \in \mathrm{Symb}_{\Gamma_0(Np)}(\mathbb{Z}_p)^0$$

takes p-integral values and let $L_p(E,s)$ be the associated p-adic L-function defined as in definition 4.4.2. Assume, for simplicity, that $\mathcal{R}_E \cong \Lambda$ and let $h_E : \mathcal{H} \to \Lambda$ be the homomorphism of theorem 2.4.3.

Let f_E be the p-stabilized ordinary newform associated to E and let N be the tame conductor of f_E. The relationship between M and N is given by

$$M = \begin{cases} N & \text{if E has good reduction at } p \\ Np & \text{if E has multiplicative reduction at } p \end{cases}$$

The Atkin-Lehner operators W_N, W_M act as involution on $S_k(\Gamma_0(Np))$ and preserve the eigenspace spanned by f_E. Hence we have

$$f_E|W_N = \omega_N f_E \text{ and } f_E|W_M = \omega_M f_E$$

where $\omega_N = \pm 1$ and $\omega_M = \pm 1$. We have the functional equation of E

$$\Lambda_\infty(E, 2-s) = -\omega_M \Lambda_\infty(E,s)$$
$$\Lambda_p(E, 2-s) = -\omega_N \Lambda_p(E,s)$$

Hence $\epsilon_\infty = -\omega_M$ and $\epsilon_p = -\omega_N$. The relationship between ϵ_∞ and ϵ_p described in theorem follows easily from this description of ϵ_∞ and ϵ_p. Indeed, if E has good reduction at p, then $M = N$, hence $\omega_M = \omega_N$. We know by Deligne-Rapoport that E has multiplicative reduction at p if and only if $a_p = \pm 1$ and in that case a standard result of Atkin and Lehner tells us $\omega_M = -a_p \omega_N$. Combining these two cases we see that $\omega_M = -\omega_N$ if and only if $a_p = 1$, which is equivalent to saying that E has split multiplicative reduction at p following Deligne-Rapoport.

Theorem 4.4.3. *Let $\alpha_p = h_E(T_p) \in \Lambda$ and let $\alpha_p(k)$, $k \in \mathbb{Z}_p$, be the Iwasawa function associated to α_p. Then there are functions $L_p(k,s)$ with $k, s \in \mathbb{Z}_p$ and $L_p^*(k,1)$, $k \in \mathbb{Z}_p$, which are Iwasawa functions in each of the p-adic variables k and s, and which satisfy the following properties*

1. $L_p(2,s) = L_p(E,s)$ *for all* $s \in \mathbb{Z}_p$
2. $L_p(k,s) = \epsilon_p \cdot \langle N \rangle \frac{k}{2}^{-s} \cdot L_p(k, k-s)$
3. $L_p(k,1) = (1-\alpha_p(k)^{-1}) L_p^*(k,1)$
4. $L_p^*(2,1) = \left(1 - \frac{\beta}{p}\right) \frac{L_\infty(E,1)}{\Omega_E}$

Proof. Let $\nu_E \in \mathrm{Meas}(\mathbb{Z}_p^\times)$ be the p-adic measure associated to the pair (E, Ω_E) as in theorem 4.1.22. Let $\Phi_E = \Phi_E^+ \in \mathrm{Symb}_{\Gamma_0(N)}(\mathbb{D})^{0,+}$ be a Λ-adic modular symbol satisfying the conclusion of theorem 4.3.13.

Let $\mu = \mu_E = \Phi_E(\{0\} - \{i\infty\}) \in \mathbb{D}$ and let $\nu \in Meas(\mathbb{Z}_p^\times)$ be the measure determined by the integration formulas

$$\int f d\nu = \int_{\mathbb{Z}_p^\times \times \mathbb{Z}_p^\times} f(y/x) d\mu(x,y)$$

for $f \in \mathrm{Cont}(\mathbb{Z}_p^\times)$. Now we define the functions $L_p(k,s)$ and $L_p^*(k,1)$ by

$$L_p(k,s) = L_p(\mu, k, s) =$$

and

$$L_p^*(k,1) = L_p^*(\mu, k, 1)$$

1. We claim that $\nu = \nu_E$. So fix $a \in \mathbb{Z}_p^\times$ and $n > 0$. We have

$$\nu(a + p^n\mathbb{Z}_p) = \mu_E(U(a + p^n\mathbb{Z}_p))$$

On the other hand, for each $x \in \mathbb{P}^1(\mathbb{Q}_p)$, we choose a matrix $\beta(x,p^n) \equiv \begin{pmatrix} 1 & * \\ 0 & p^n \end{pmatrix}$ mod p^n one of whose rows is in $U(x,p^n)$ and whose determinant is p^n. Now let

$$\mu_{x,p^n} = \Phi|\beta(x,p^n)\left(\{0\} - \{i\infty\}\right) \in \mathbb{D}$$

It follows from the definitions that μ_{x,p^n} is supported on $U(x,p^n)$. Hence we have $\alpha_p^n \mu = \sum_{x \in \mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})} \mu_{x,p^n}$. Therefore, we obtain

$$a_p^n \nu(a + p^n\mathbb{Z}_p) = a_p^n \cdot \mu(U(a + p^n\mathbb{Z}_p))$$

$$= (\alpha_p^n \mu)(U(a + p^n \mathbb{Z}_p))$$
$$= \mu_{a,p^n}(U(a + p^n \mathbb{Z}_p))$$

But $\mu_{a,p^n} = \Phi\left(\left\{\frac{a}{p^n}\right\} - \{i\infty\}\right)(U(\mathbb{Z}_p)) = \varphi_E\left(\left\{\frac{a}{p^n}\right\} - \{i\infty\}\right)$. Thus

$$\nu(a + p^n \mathbb{Z}_p) = a_p^{-n} \varpi_E\left(\left\{\frac{a}{p^n}\right\} - \{i\infty\}\right) = \nu_E(a + p^n \mathbb{Z}_p)$$

2. We first claim that $\mu\left|\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} = \epsilon\left[\langle N\rangle^{1/2}\right]\mu$. Indeed, since

$$\Phi|W_N^2 = \Phi|[-N] = [\langle N\rangle]\Phi$$

we have $\Phi|W_N = \pm w_N[\langle N\rangle^{1/2}]\Phi$. Applying $\phi_{2,*}$ and using the fact that $\varphi_E|W_N = w_N\varphi_E$, we obtain

$$\Phi|W_N = w_N[\langle N\rangle^{1/2}]\Phi$$

Now evaluate both sides of this identity on the divisor $\{0\} - \{i\infty\} \in \mathcal{D}_0$. Since the action of W_N on Φ is given by the action of $\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$, and since this matrix interchange the cusps 0 and $i\infty$, the identity $\mu\left|\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}\right. = \epsilon_p[\langle N\rangle^{1/2}]\mu$ follows from the equality $\epsilon_p = -w_N$

3. Recall the identity

$$\alpha_p^n \mu = \sum_{x \in \mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})} \mu_{x,p^n}$$

Setting $n = 1$ gives us

$$\alpha_p \mu = \sum_{n \in \mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})} \mu_{x,p}$$

A simple calculation shows that

$$\alpha_p(k) \cdot L_p(k, s) = \sum_{a=1}^{p-1} \int \langle x\rangle^{k-2} \left\langle y/x\right\rangle^{s-1} d\mu_{\alpha,p}(x, y)$$

$$\alpha_p(k)\cdot L_p^*(k,s_0)=\sum_{a=0}^{p-1}\int \langle x\rangle^{k-2}\left\langle y/x\right\rangle^{s_0-1}d\mu_{a,p}(x,y)$$

Hence, $\alpha_p(k)\cdot\Big(L_p^*(k,1)-L_p(k,1)\Big)=\int\langle x\rangle^{k-2}\,d\mu_{0,p}(x,y)$. But $\mu_{0,p}=\mu\Big|\begin{pmatrix}1&0\\0&p\end{pmatrix}$ and the function $(x,y)\mapsto\langle x\rangle^{k-2}$ on $U(\mathbb{Z}_p)$ is fixed by $\begin{pmatrix}1&0\\0&p\end{pmatrix}$. It follows that the last integral is equal to

$$L_p^*(k,1)=\int_{U(\mathbb{Z}_p)}\langle x\rangle^{k-2}\,d\mu(x,y)$$

Thus

$$\alpha_p(k)\cdot\Big(L_p^*(k,1)-L_p(k,1)\Big)=L_p^*(k,1)$$

4. We have

$$L_p^*(2,1)=\mu(\mathbb{Z}_p^\times\times\mathbb{Z}_p)=\phi_2\mu=\varphi_E(\{0\}-\{i\infty\})=\frac{L_\infty(f_E,1)}{\Omega_E}$$

Hence $L_p^*(2,1)=\dfrac{L_\infty(f_E,1)}{\Omega_E}$ and 4 follows from the equality

$$(1-\beta p^{-s})\cdot L_\infty(E,s)=L_\infty(f_E,s)$$

□

CHAPTER 5

Proof of Main Result

Theorem 5.0.1. *Let E be an elliptic curve over $\mathbb{Q}$ with split multiplicative reduction at the prime $p \geq 5$. Let Ω_E be the Neron period of E and let $L_p(E,s)$ be the associated p-adic L-function. Then*

$$\frac{d}{ds}L_p(E,s)|_{s=1} = \mathcal{L}_p(E) \cdot \frac{L_\infty(E,1)}{\Omega_E}$$

Proof. We will give the proof only under the simplifying assumption that $\mathcal{R}_E = \Lambda$. Let $\epsilon_\infty = \pm 1$ denote the sign in the functional equation for $L_\infty(E,z)$. Since E has split multiplicative reduction at p, the p-adic L-function of E has the following functional equation

$$L_p(E, 2-s) = \epsilon_p \langle N \rangle^{s-1} L_p(E,s)$$

where $\epsilon_p = -\epsilon_\infty$, N is the conductor of E and $\langle N \rangle = N\omega^{-1}(N)$ where ω is the Teichmuller character.

In case $\epsilon_p = 1$, the p-adic L-function has an even order zero at $s = 1$ and the complex L-function has an odd order zero at $s = 1$. Hence, in this case, the theorem is true, since both sides of the desired equality vanish.

Now assume that $\epsilon_p = -1$. Let $L_p(k,s)$ be a two variable p-adic L-function satisfying the properties

1. $L_p(2,s) = L_p(E,s)$ for all $s \in \mathbb{Z}_p$
2. $L_p(k,s) = \epsilon_p \cdot \langle N \rangle^{\frac{k}{2}-s} \cdot L_p(k, k-s)$

3. $L_p(k,1) = (1-\alpha_p(k)^{-1})L_p^*(k,1)$
4. $L_p^*(2,1) = \left(1-\dfrac{\beta}{p}\right)\dfrac{L_\infty(E,1)}{\Omega_E}$

From the functional equation (2) it follows that $L_p(k,k/2)=0$ identically for $k\in\mathbb{Z}_p$. In particular, the linear terms in the Taylor expansion of $L_p(k,s)$ around the point $(k,s)=(2,1)$ must vanish along the line $s=k/2$. Hence, there is a constant $c\in\mathbb{Z}_p$, such that

$$L_p(k,s) \sim c\cdot\left((s-1)-\frac{1}{2}(k-2)\right)$$

where $f(k,s)\sim g(k,s)$ means that the Taylor expansions of f and g at $(k,s)=(2,1)$ agree modulo terms of order ≥ 2. The theorem will follow by computing c in two ways.

Setting $k=2$ and applying the equality (1) we obtain $L_p(E,s)\sim c(s-1)$, hence

$$c = \frac{d}{ds}L_p(E,s)|_{s=1}$$

On the other hand, setting $s=1$ and using (3) we obtain

$$(1-\alpha_p(k)^{-1})L_p^*(k,1) \sim -\frac{1}{2}c(k-2)$$

Differentiating this with respect to k at $k=2$ and note that $\alpha_p(2)=1$, we obtain

$$-\frac{1}{2}c = \alpha_p'(s)L_p^*(2,1)$$

We also have $\alpha_p'(2) = -\dfrac{1}{2}\mathcal{L}_p(E)$, and by (4) we have

$$L_p^*(2,1) = \frac{L_\infty(E,1)}{\Omega_E}$$

Hence

$$-\frac{1}{2}c = -\frac{1}{2}\mathcal{L}_p(E)\cdot\frac{L_\infty(E,1)}{\Omega_E}$$

□

Bibliography

[AS86] Ash, A., Stevens, G.: Modular forms in characteristic l and special values of their L-functions, Duke Math. J. 53, no. 3, (1986), 849-868

[AV75] Amice, Y., Velu, J.: Distributions p-adiques associees aux series de Hecke, Asterisque 24-25 (1975), 119-131.

[BD07] Bertolini, M., Darmon, H. : Hida families and rational points on elliptic curves, Inventiones mathematicae 168, pages371–431 (2007)

[BD20] Bruin, P., Dahmen, S.: Modular Forms Lecture Notes, Mastermath Course, Spring 2020

[Bir67] Birch, B. J. : Cyclotomic Fields and Kummer Extensions,In: J. W. S. Cassels and A. Frohlich, Eds., Algebraic Number Theory, Academic Press, London, 1967, pp. 85-93.

[BNG] Banerjee, D., V.G. Narasimha Kumar Ch, Ghate, E., :Λ-adic forms and the Iwasawa main conjecture, Lecture notes from: Advanced Instructional School on Arithmetic Algerbaic Geometry, September 22-30 (2008), IIT Guwahati.

[Col] Colmez, P.: Fontaine's rings and p-adic L-functions

[De68] Deligne, P.: Formes modulaires et representations ℓ-adiques, Sem. Bourbaki, exp. 355, 139-172, (1968-1969)

[DS05] Diamond, F., Shurman,J.: A First Course in Modular Forms, Graduate Texts in Mathematics 228, Springer-Verlag, (2005)

[Ei95] Eisenbud, D.: Commutative Algebra with a View Toward Algebraic Geometry, Graduate Texts in Mathematics 150, Springer-Verlag, (1995)

[GS93] Greenberg, R., Stevens,G.: p-adic L-functions and p-adic periods of modular forms, Invent. Math. 111 (1993), 407-447.

[GS94] Greenberg, R., Stevens, G.: On the conjecture of Mazur, Tate, and Teitelbaum. *Contemporary Mathematics*, 1994, 183-211.

[Hi86a] Hida, H.: Galois representations into $GL_2(\mathbb{Z}_p[[X]])$ attached to ordinary cusp forms, Inventiones mathematicae volume 85, 45–613 (1986)

[Hi86b] Hida, H., Iwasawa modules attached to congruences of cusp forms, Ann. Scient. Ec.Norm. Sup., 19 (1986), 231-273.

[Hi93] Hida, H., Elementary theory of L-functions and Eisenstein series, London Math. Soc.Student Texts 85, Cambridge University Press, 2nd Edition, (1993).

[JW17] Jacinto, J., Williams, C.: An introduction to p-adic L-functions, Lecture Notes, 2017

[JW20] Jacinto, J., Williams, C.: An introduction to p-adic L-functions, Lecture Notes, 2020

[Ko79] Koblitz, N.: A new proof of certain formulas for p-adic L-functions, Duke Math. J. 46(2): 455-468 (1979)

[Ko84] Koblitz, N.: p-adic Numbers, p-adic Analysis, and Zeta-Functions, Springer,(1984)

[Laf] Lafferty, M.: Hida's Theory, Lecture Notes

[Mi89] Miyake, T., Modular forms, Springer-Verlag, (1989).

[MTT] Mazur, B., Tate, J. , Teitelbaum, J. : On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer, Inventiones mathematicae volume 84, pages 1–48 (1986)

[Neu08] Neukirch, J. et al.: Cohomology of Number Fields, Springer, Second Edition (2008)

[Ou] Ouyang, Y.: Introduction to Iwasawa Theory, Lecture Notes

[Ru00] Rubin,K.: Euler Systems, Annals of Mathematics Studies, Princeton University press (2000)

[Sha] Sharif,R.: Iwasawa Theory, Lecture Notes

[Sil94] Silverman,J.: Advanced Topics in the Arithmetic of Elliptic Curves, Graduate Texts in Mathematics 151, Springer-Verlag, 1994

[Sil09] Silverman,J.: The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics 106, Springer-Verlag, 2nd edition, 2009

[Ser67] Serre,J-P.: Local Class Fields, In: J. W. S. Cassels and A. Frohlich, Eds., Algebraic Number Theory, Academic Press, London, 1967, pp.

[Ser79] Serre,J-P.: Local Fields, Graduate Texts in Mathematics 67, Springer-Verlag, 1979

[Ser97] Serre,J-P.: Galois Cohomology,(translated by Ion, P.), Springer Monographs in Mathematics, Springer-Verlag, 1997

[Shi] Shimura, G.: Introduction to Arithmetic Theory of Automorphic Functions, Princeton University Press, 1971

[Vi76] Vishik,M.: Non archimedean measures connected with Dirichlet series, Math. USSR Sbornik 28 (1976), 216-228

[Wi] Wiese,G.: Galois Representations, Lecture Notes, 2008

[Wi88] Wiles, A., On ordinary λ-adic representations associated to modular forms, Inventiones Math., 94 (1988), 529-573.