Stable lattices in p-adic families of residually reducible ordinary modular Galois representations

Dong Yan

Acknowledgements

It is an honor to thank Professor Tadashi Ochiai for his guidance. In my 4th year in my undergraduate studies in 2012, Professor Tadashi Ochiai became my supervisor. During these years, he led me in the right direction during moments of confusion and he also gave me fruitful suggestions and encouragements to study this topic. My appreciation is more than words that I can say. Thanks are also due to Kenji Sakugawa and Makoto Kawashima for valuable discussion, reading the manuscript and correcting several mistakes. I wish to thank to my parents who gave me a lot of supports and encouragements during these ten years when I studied in Japan. Finally, I would like to thank to my fiancée Lifan Liu, I am so thankful that I met you and thanks to your patience in everything.

Contents

Chapter 1

Introduction

1.1 History

Let $p \geq 3$ be a fixed odd prime. We fix a complex embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and a p-adic embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ of an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ throughout the paper, where $\mathbb{C}$ is the field of complex numbers and $\overline{\mathbb{Q}}_p$ an algebraic closure of the field $\mathbb{Q}_p$ of p-adic numbers. For an integer n, we denote by μ_n the group of n-th roots of unity. In 1976, Ribet [Ri] proved the converse of Herbrand's theorem as follows:

Theorem (Ribet)**.** Let k be an even integer satisfying $2 \leq k \leq p-3$ and B_k the k-th Bernoulli number. We denote by $\mathrm{Cl}(\mathbb{Q}(\mu_p))[p]$ the p-part of the ideal class group of $\mathbb{Q}(\mu_p)$ on which the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts by functoriality. Suppose p divides B_k. Then $\mathrm{Cl}(\mathbb{Q}(\mu_p))[p]^{\omega^{1-k}} \neq 0$, where $\omega : (\mathbb{Z}/p\mathbb{Z})^{\times} \to \mu_{p-1}$ is the Teichmüller character such that $\omega(a) \mod p = a$ for all $a \in (\mathbb{Z}/p\mathbb{Z})^{\times}$ and we also denote by the same symbol ω the corresponding character of $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^{\times}$.

The main ideas of Ribet's proof is to construct a normalized Hecke eigen cusp form $f = \sum_{n=1}^{\infty} a(n,f)\, q^n$ of weight 2 at level p which is congruent to Eisenstein series and to consider the Galois representation ρ_f over $K = \mathbb{Q}_p\left(\{a(n,f)\}_{n\geq 1}\right)$ attached to f due to Deligne and Shimura. The following key proposition enables us to take a $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$-stable lattice T of ρ_f such that $T/\varpi T$ is not a semi-simple $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$-module, where $\mathcal{O}$ is the ring of integers of K and ϖ is a fixed uniformizer of $\mathcal{O}$. Then by considering the action of $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_p)\right)$ on $T/\varpi T$, Ribet constructed an unramified p-extension L of $\mathbb{Q}(\mu_p)$ and $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ acts on $\mathrm{Gal}(L/\mathbb{Q}(\mu_p))$ via ω^{1-k}. Thus the converse of Herbrand's theorem follows by class field theory. By extending Ribet's method, Mazur-Wiles [MW1] and Wiles [Wi2] proved the Iwasawa main conjecture for $\mathbb{Q}$ and for totally real fields.

Now we introduce a key lemma in Ribet's proof (which is called "Ribet's lemma") as follows:

Proposition A (Ribet's lemma)**.** Let $(\mathcal{O}, \varpi, \mathcal{O}/(\varpi))$ be the ring of integers of a finite extension of $\mathbb{Q}_p$ where ϖ is a fixed uniformizer of $\mathcal{O}$. Let $K = \mathrm{Frac}(\mathcal{O})$ be the field of fractions of $\mathcal{O}$ and V a 2-dimensional K-vector space. For a given p-adic representation

$$\rho : G \to \mathrm{Aut}_K(V)$$

of a compact group G, let $\bar{\rho}^{\mathrm{ss}}$ be the semi-simplification of the mod (ϖ) representation (see Section 2.1 below). Suppose ρ is irreducible and $\bar{\rho}^{\mathrm{ss}} \cong \vartheta_1 \oplus \vartheta_2$, where $\vartheta_1, \vartheta_2 : G \to (\mathcal{O}/(\varpi))^{\times}$ are characters. Then there exists a G-stable lattice $T \subset V$ for which $\bar{\rho}_T$ is the form $\begin{pmatrix} \vartheta_1 & * \\ 0 & \vartheta_2 \end{pmatrix}$ but is not semi-simple.

In this thesis, we study Ribet's lemma in a more general way. Let us keep the assumptions and the notations of Proposition A. For each positive integer m, we consider the following condition:

(Ext_m) There exist a G-stable lattice T of ρ and two characters $\nu_i : G \to \mathcal{O}/(\varpi)^m$ $(i = 1, 2)$ such that

$$0 \to \mathcal{O}/(\varpi)^m(\nu_1) \to T/\varpi^m T \to \mathcal{O}/(\varpi)^m(\nu_2) \to 0$$

is a non-split exact sequence of G-modules.

Ribet's lemma claims that there exists an integer $m \geq 1$ for which (Ext_m) holds. Since ρ is irreducible, the number of isomorphic classes of G-stable lattices is finite by Proposition 2.4.2. Thus we are interested in the determination of the largest value of m with which (Ext_m) holds and we denote it by $m(\rho)$. Furthermore, we consider the following condition:

(RMF) The semi-simplification of the mod (ϖ) representation is decomposed into two different characters.

Assume the condition (RMF), then we have $m(\rho) = \sharp\mathscr{L}(\rho) - 1$ by the proof of Proposition 3.3.1 at the end of §3 and Proposition 6.1.4, where $\mathscr{L}(\rho)$ is the set of the isomorphic classes of G-stable lattices.

Now assume ρ is a Galois representation attached to a normalized Hecke eigen cusp form with residually reducible representation. Since the determinant $\det \rho$ is an odd character, the condition (RMF) holds. We introduce a result on $\sharp\mathscr{L}(\rho)$ where ρ comes from a modular form. The following known result is obtained by Greenberg and Monsky for the Ramanujan's cusp form $\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24}$ and $p = 691$:

Proposition B (Greenberg, Monsky)**.** Let $\rho_\Delta : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Q}_{691})$ be the 691-adic representation attached to Δ. Then $\sharp\mathscr{L}(\rho_\Delta) = 2$.

Remark. The work of Greenberg and Monsky is unpublished. See [Maz, Section 12, Proposition 1] for the statement. For the proof of more general settings, see Proposition 6.1.5 and the table after it.

1.2 Hida deformation

Before we state our main result, let us prepare some notations on Hida deformation. From now on to the end of this paper, we fix a topological generator u of $1 + p\mathbb{Z}_p$. Let $\mathcal{O} \subset \overline{\mathbb{Q}}_p$ be a commutative ring which is finite flat over $\mathbb{Z}_p$ and let ψ be a Dirichlet character modulo M. We denote by $S_k(\Gamma_0(M), \psi, \mathcal{O})$ the space of cusp forms of weight k, level M, Neben character ψ and Fourier coefficients in $\mathcal{O}$. A normalized Hecke eigen cusp form f is called p-ordinary if its p-th Fourier coefficient $a(p, f)$ is a p-adic unit. Now we prepare some notations on Hida deformation. We fix a positive integer N prime to p and let χ be a Dirichlet character modulo Np. If $\zeta \in \mu_{p^r}(r \geq 0)$ is a p^r-th root of unity, we denote by ψ_ζ the Dirichlet character as follows:

$$\psi_\zeta : \left(\mathbb{Z}/p^{r+1}\mathbb{Z}\right)^{\times} \to \overline{\mathbb{Q}}_p^{\times},\ u \bmod p^{r+1} \mapsto \zeta.$$

Now let $\mathbb{I}$ be an integrally closed local domain which is finite flat over $\Lambda_\chi = \mathbb{Z}_p[\chi][[X]]$ and $\mathfrak{X}_{\mathrm{arith}}(\mathbb{I})$ the set of homomorphisms defined as follows:

$$\mathfrak{X}_{\mathrm{arith}}(\mathbb{I}) = \left\{ \varphi : \mathbb{I} \to \overline{\mathbb{Q}}_p \;\middle|\; \varphi(1+X) = \zeta_\varphi u^{k_\varphi - 2}, (k_\varphi, \zeta_\varphi) \in \mathbb{Z}_{\geq 2} \times \mu_{p^\infty} \right\}.$$

We call an element of $\mathfrak{X}_{\mathrm{arith}}(\mathbb{I})$ an arithmetic specialization of $\mathbb{I}$. Let $\mathcal{F} = \sum_{n=1}^{\infty} a(n,\mathcal{F}) q^n \in \mathbb{I}[[q]]$ be an $\mathbb{I}$-adic normalized Hecke eigen cusp form with character χ. That is,

$$f_\varphi := \sum_{n=1}^{\infty} \varphi(a(n,\mathcal{F})) q^n \in S_{k_\varphi}\left(\Gamma_0(Np^{r_\varphi+1}), \chi\psi_\varphi\omega^{1-k_\varphi}, \varphi(\mathbb{I})\right)$$

is a p-ordinary normalized Hecke eigen cusp form for all $\varphi \in \mathfrak{X}_{\mathrm{arith}}(\mathbb{I})$, where p^{r_φ} is the order of ζ_φ and $\psi_\varphi = \psi_{\zeta_\varphi}$.

Let $\mathcal{F}$ be an $\mathbb{I}$-adic normalized Hecke eigen cusp form and $\mathrm{Frac}(\mathbb{I})$ the field of fraction of $\mathbb{I}$. Hida [Hi2] (see also Theorem 5.4.6 below) proved that there is a continuous representation

$$\rho_{\mathcal{F}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathrm{Frac}(\mathbb{I}))$$

such that for any $\varphi \in \mathfrak{X}_{\mathrm{arith}}(\mathbb{I})$, the residual representation $\rho_{\mathcal{F}}(\mathrm{Ker}\varphi)$ (see Definition 5.4.7 below) is isomorphic to ρ_{f_φ}.

1.3 Statement of the main result

In this thesis, we determine whether the variation of $\sharp\mathscr{L}(\rho)$ is bounded or not when ρ varies in a Hida deformation. From now on throughout the paper, we denote by ϕ the Euler function and we fix a positive integer N prime to p. Let χ be a Dirichlet character modulo Np. Let $\mathbb{I}$ be the same as above with $\mathfrak{m}$ the maximal ideal of $\mathbb{I}$. Let $\mathcal{F}$ be an $\mathbb{I}$-adic normalized Hecke eigen cusp form. We denote by $\mathbb{Q}(\mu_{Np^\infty})$ the union of all cyclotomic fields $\mathbb{Q}(\mu_{Np^r})$ $(r \in \mathbb{Z}_{\geq 1})$ and by $\mathbb{Q}_\infty$ the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Now we are going to determine $\sharp\mathscr{L}(\rho_{f_\varphi})$ when φ varies in $\mathfrak{X}_{\mathrm{arith}}(\mathbb{I})$. Our result is the following theorem:

Theorem 1.3.1 ([Y, Theorem 1.5])**.** Suppose $p \nmid \phi(N)$ and $\rho_{\mathcal{F}}(\mathfrak{m}) \cong \vartheta_1 \oplus \vartheta_2$ such that ϑ_1 (resp. ϑ_2) is unramified (resp. ramified) at p. Let $W(\mathbb{I}/\mathfrak{m})$ be the Witt ring of $\mathbb{I}/\mathfrak{m}$ and $\chi_i : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \to W(\mathbb{I}/\mathfrak{m})^\times$ the composition of ϑ_i with the Teichmüller lift: $(\mathbb{I}/\mathfrak{m})^\times \hookrightarrow W(\mathbb{I}/\mathfrak{m})^\times$. Assume the following conditions:

(Co-prime) The conductors of χ_1 and χ_2 are relatively prime and $\chi_1 \neq \chi_2\omega$.

(Conductor) Every prime factor l of N divides the conductor of χ.

We enlarge $\mathbb{I}$ such that $\mathbb{I}$ is also finite flat over $\Lambda_{\chi_1\chi_2^{-1}}$.

(1) For any $\varphi \in \mathfrak{X}_{\mathrm{arith}}(\mathbb{I})$ such that $\varphi(1+X) = \zeta_\varphi u^{k_\varphi - 2}$, we have

$$\sharp\mathscr{L}(\rho_{f_\varphi}) \leq \mathrm{ord}_{\varpi_\varphi}(L_p(1-k_\varphi, \chi_1^{-1}\chi_2\psi_\varphi\omega)) + 1,$$

where ϖ_φ is a fixed uniformizer of $\varphi(\mathbb{I})$ and $L_p(s, \chi_1^{-1}\chi_2\psi_\varphi\omega)$ is the Kubota-Leopoldt p-adic L-function.

(2) Assume that

(Rank one) $N = 1$ and $h^{\mathrm{ord}}(\chi, \Lambda_\chi)$ (see Definition 5.3.2 below) is isomorphic to Λ_χ.

Then for any $\varphi \in \mathfrak{X}_{\mathrm{arith}}(\mathbb{I})$ such that $\varphi(1+X) = \zeta_\varphi u^{k_\varphi - 2}$, we have

$$\sharp\mathscr{L}(\rho_{f_\varphi}) = \mathrm{ord}_{\varpi_\varphi}(L_p(1-k_\varphi, \chi\psi_\varphi\omega)) + 1.$$

(3) Let $L_\infty, L_\infty^{(Np)}$ be the maximal unramified abelian p-extension of $\mathbb{Q}(\mu_{Np^\infty})$ and the maximal abelian p-extension unramified outside Np of $\mathbb{Q}(\mu_{Np^\infty})$. We denote by $X_\infty = \mathrm{Gal}(L_\infty/\mathbb{Q}(\mu_{Np^\infty}))$ and by $Y_\infty = \mathrm{Gal}\left(L_\infty^{(Np)}/\mathbb{Q}(\mu_{Np^\infty})\right)$ on which $\mathrm{Gal}(\mathbb{Q}(\mu_{Np^\infty})/\mathbb{Q}_\infty)$ acts by conjugation. We denote by $X_\infty^{\chi_1\chi_2^{-1}} = X_\infty \otimes_{\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\mu_{Np^\infty})/\mathbb{Q}_\infty)]} \mathbb{Z}_p[\chi_1\chi_2^{-1}]$ and by $Y_\infty^{\chi_1^{-1}\chi_2} = Y_\infty \otimes_{\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\mu_{Np^\infty})/\mathbb{Q}_\infty)]} \mathbb{Z}_p[\chi_1^{-1}\chi_2]$. Assume the following conditions:

(Cyclic) The $\Lambda_{\chi_1\chi_2^{-1}}$-modules $X_\infty^{\chi_1\chi_2^{-1}}$ and $Y_\infty^{\chi_1^{-1}\chi_2}$ are cyclic.
(Prime ideal) The ideal generated by $\mathcal{L}_p\left(\chi_1^{-1}\chi_2\right)$ (see Theorem 4.2.1 below) is a prime ideal in $\mathbb{I}$.

Then for any $\varphi \in \mathfrak{X}_{\mathrm{arith}}(\mathbb{I})$ such that $\varphi(1+X) = \zeta_\varphi u^{k_\varphi - 2}$, we have

$$\sharp\mathscr{L}(\rho_{f_\varphi}) = \mathrm{ord}_{\varpi_\varphi}(L_p(1-k_\varphi, \chi_1^{-1}\chi_2\psi_\varphi\omega)) + 1.$$

Theorem 1.3.1 will be proved at the end of Section 6.2. Now we discuss the boundedness of $\sharp\mathscr{L}\left(\rho_{f_\varphi}\right)$ when the weight and the level vary. When we fix an $r \in \mathbb{Z}_{\geq 0}$, we define $\mathfrak{X}_{\mathrm{arith}}^{(>r)}(\mathbb{I})$ as follows:

$$\mathfrak{X}_{\mathrm{arith}}^{(>r)}(\mathbb{I}) = \left\{ \varphi \in \mathfrak{X}_{\mathrm{arith}}(\mathbb{I}) \;\middle|\; \varphi(1+X) = \zeta_\varphi u^{k_\varphi - 2}, (k_\varphi, \zeta_\varphi) \in \mathbb{Z}_{\geq 2} \times (\mu_{p^\infty} \setminus \mu_{p^r}) \right\}.$$

When we fix a $\zeta \in \mu_{p^\infty}$, we define $\mathfrak{X}_{\mathrm{arith}}^{(\zeta)}(\mathbb{I})$ as follows:

$$\mathfrak{X}_{\mathrm{arith}}^{(\zeta)}(\mathbb{I}) = \left\{ \varphi \in \mathfrak{X}_{\mathrm{arith}}(\mathbb{I}) \;\middle|\; \varphi(1+X) = \zeta u^{k_\varphi - 2}, k_\varphi \geq 2 \right\}.$$

When we fix a $k \in \mathbb{Z}_{\geq 2}$, we define $\mathfrak{X}_{\mathrm{arith}}^{(k)}(\mathbb{I})$ as follows:

$$\mathfrak{X}_{\mathrm{arith}}^{(k)}(\mathbb{I}) = \left\{ \varphi \in \mathfrak{X}_{\mathrm{arith}}(\mathbb{I}) \;\middle|\; \varphi(1+X) = \zeta_\varphi u^{k-2}, \zeta_\varphi \in \mu_{p^\infty} \right\}.$$

The bounded case of the variation of $\sharp\mathscr{L}(\rho_{f_\varphi})$ is the following corollary:

Corollary 1.3.2 ([Y, Corollary 1.6 (1)-(3)])**.** Let us keep the assumptions and the notations of Theorem 1.3.1. We denote by $\mathcal{L}_p^*\left(\chi_1^{-1}\chi_2\right)$ the distinguished polynomial associated to $\mathcal{L}_p\left(\chi_1^{-1}\chi_2\right)$. Then we have the following statements:

(1) There exists an integer $r \in \mathbb{Z}_{\geq 0}$ such that $\sharp\mathscr{L}(\rho_{f_\varphi})$ is bounded when φ varies in $\mathfrak{X}_{\mathrm{arith}}^{(>r)}(\mathbb{I})$. Furthermore, we have the following inequality for $\sharp\mathscr{L}(\rho_{f_\varphi})$:

$$\sharp\mathscr{L}(\rho_{f_\varphi}) \leq \mathrm{rank}_{\Lambda_\chi}\mathbb{I} \cdot \deg\mathcal{L}_p^*\left(\chi_1^{-1}\chi_2\right) + 1$$

for every arithmetic specialization $\varphi \in \mathfrak{X}_{\mathrm{arith}}^{(>r)}(\mathbb{I})$, where $\mathrm{rank}_{\Lambda_\chi}\mathbb{I}$ is the rank of the Λ_χ-module $\mathbb{I}$.

(2) For each integer $k \geq 2$, $\sharp\mathscr{L}(\rho_{f_\varphi})$ is bounded when φ varies in $\mathfrak{X}_{\mathrm{arith}}^{(k)}(\mathbb{I})$.

(3) Suppose that $\mathbb{I}$ is isomorphic to $\mathcal{O}[[X]]$ with $\mathcal{O}$ the ring of integers of a finite extension of $\mathbb{Q}_p$. Then there exists an integer $r' \in \mathbb{Z}_{\geq 0}$ such that $\sharp\mathscr{L}(\rho_{f_\varphi})$ is constant when φ varies in $\mathfrak{X}_{\mathrm{arith}}^{(>r')}(\mathbb{I})$.

The unbounded case of the variation of $\sharp\mathscr{L}(\rho_{f_\varphi})$ is the following corollary:

Corollary 1.3.3 ([Y, Corollary 1.6 (4)])**.** Let us keep the assumptions and the notations of Theorem 1.3.1. Assume the condition (Rank one) or both of the conditions (Cyclic) and (Prime ideal). For each $\zeta \in \mu_{p^\infty}$, $\sharp\mathscr{L}(\rho_{f_\varphi})$ is unbounded when φ varies in $\mathfrak{X}_{\mathrm{arith}}^{(\zeta)}(\mathbb{I})$ if and only if $L_p(1-s, \chi_1^{-1}\chi_2\psi_\zeta\omega)$ has a zero in $\mathbb{Z}_p$.

Corollary 1.3.2 and 1.3.3 will be proved in Section 6.3. Let $\mathscr{L}(\rho_{\mathcal{F}})$ be the set of the isomorphic classes of stable lattices of Hida deformation $\rho_{\mathcal{F}}$. Now we give a result of $\sharp\mathscr{L}(\rho_{\mathcal{F}})$ answering Question 4.5 1 of [Oc1].

Corollary 1.3.4 ([Y, Corollary 1.7])**.** Let us keep the assumptions and the notations of Theorem 1.3.1. Assume the conditions (Co-prime), (Cyclic) and (Prime ideal). Further assume the following condition

(Free lattice) There exists a stable lattice $\mathbb{T}$ which is free over $\mathbb{I}$.

Suppose that there exists a $\zeta \in \mu_{p^\infty}$ such that $L_p(1-s, \chi_1^{-1}\chi_2\psi_\zeta\omega)$ has a zero in $\mathbb{Z}_p$. Then $\sharp\mathscr{L}(\rho_{\mathcal{F}}) = \infty$.

Corollary 1.3.4 will be proved in Section 6.4.

Outline of this thesis

The outline of this thesis is as follows. In section 2, we recall the definition and some properties of lattices and G-stable lattices. We prove that for a given p-adic Galois representation ρ, $\sharp\mathscr{L}(\rho)$ is unique under the assumption that the residue representation is irreducible and $\sharp\mathscr{L}(\rho)$ is finite under the assumption that ρ is irreducible.

In section 3, we recall the Ribet's proof of the converse of the Herbrand's theorem and we give two proofs of Ribet's lemma: the original proof based on matrix operation and the proof based on the Bruhat-Tits tree of GL_2. The latter proof illustrates us to counting $\sharp\mathscr{L}(\rho)$ by means of the reducibility ideal.

In section 4, we recall the classical Iwasawa theory of ideal class groups, especially the Iwasawa's construction of the Kubota-Leopoldt p-adic L-function and the main conjecture. We normalize the Iwasawa's construction slightly different from Iwasawa's original paper for the compatibility of the arithmetic specialization in Hida deformation ring.

In section 5, we recall Hida theory: the freeness of the space of Λ-adic forms, Hida's control theorem, duality and the construction of the Galois representation attached to an $\mathbb{I}$-adic normalized Hecke eigen cusp form by using the pseudo representation theory. In section 6, we prove our main theorem.

Notations

$\mathrm{Frac}\,(A)$: the field of fractions of a commutative domain A

K : a finite extension of $\mathbb{Q}_p$

$\mathcal{O}$: the ring of integers of a finite extension of $\mathbb{Q}_p$

ϖ : a fixed uniformizer of a discrete valuation ring

$\mathbb{F}$: the residue field of a discrete valuation ring

$\mathscr{L}\,(\rho)$: the set of the isomorphic classes of $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$-stable lattices of a given p-adic representation ρ

χ_{cyc} : the p-adic cyclotomic character, i.e.

$$\chi_{\mathrm{cyc}} : \mathrm{Gal}\left(\mathbb{Q}\left(\mu_{p^\infty}\right)/\mathbb{Q}\right) \xrightarrow{\sim} \mathbb{Z}_p^\times$$

κ_{cyc} : $\mathrm{Gal}\left(\mathbb{Q}_\infty/\mathbb{Q}\right) \xrightarrow{\sim} \mathrm{Gal}\left(\mathbb{Q}\left(\mu_{p^\infty}\right)/\mathbb{Q}\left(\mu_p\right)\right) \xrightarrow{\chi_{\mathrm{cyc}}} 1+p\mathbb{Z}_p$

ω : the Teichmüller character, i.e.

$$\omega : \mathrm{Gal}\left(\mathbb{Q}\left(\mu_{p^\infty}\right)/\mathbb{Q}_\infty\right) \xrightarrow{\sim} \mathrm{Gal}\left(\mathbb{Q}\left(\mu_p\right)/\mathbb{Q}\right) \xrightarrow{\chi_{\mathrm{cyc}}} \mu_{p-1}$$

By abuse of notation, we sometimes denote by χ_{cyc} and κ_{cyc} the characters of $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ composed with $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \twoheadrightarrow \mathrm{Gal}\left(\mathbb{Q}\left(\mu_{p^\infty}\right)/\mathbb{Q}\right)$ and $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \twoheadrightarrow \mathrm{Gal}\left(\mathbb{Q}_\infty/\mathbb{Q}\right)$ respectively.

D_l (resp. I_l) : the decomposition subgroup (resp. inertia subgroup) of $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ at a prime l

Frob_l : the geometric Frobenius at l

$\Lambda_{\mathcal{O}}$: the power series ring $\mathcal{O}[[X]]$

Λ : $= \Lambda_{\mathbb{Z}_p}$.

Λ_ψ : the power series ring $\Lambda_{\mathbb{Z}_p[\psi]}$ for a Dirichlet character ψ

For an integer d which is prime to p, write $d = \omega(d)\langle d\rangle$ under the isomorphism

$$\mathbb{Z}_p^\times \xrightarrow{\sim} \mu_{p-1} \times 1 + p\mathbb{Z}_p$$

and we denote by s_d such that $\langle d\rangle = u^{s_d}$.

Let ψ be a Dirichlet character modulo M, we also denote by the same symbol ψ the corresponding character of $\mathrm{Gal}(\mathbb{Q}(\mu_M)/\mathbb{Q}) \cong (\mathbb{Z}/M\mathbb{Z})^\times$. We denote by $\mathbf{1}$ the trivial Dirichlet character.

For an arithmetic specialization φ which is defined in §1.2, we denote by $(\zeta_\varphi, k_\varphi, r_\varphi)$ the data such that $\varphi(1+X) = \zeta_\varphi u^{k_\varphi - 2}$ and $r_\varphi \in \mathbb{Z}_{\geq 0}$ such that $\zeta_\varphi \in \mu_{p^{r_\varphi}} \setminus \mu_{p^{r_\varphi - 1}}$ i.e. ζ_φ is a primitive p^{r_φ}-th root of unity and. Furthermore, we write $\psi_\varphi = \psi_{\zeta_\varphi}$ (cf. §1.2) for simplicity.

Chapter 2

Lattices and G-stable lattices

2.1 Lattices

Definition 2.1.1. Let A be a commutative Noetherian integral domain with field of fractions K. Let V be a finite dimensional $\mathrm{Frac}\,(A)$-vector space with $\dim_{\mathrm{Frac}(A)} V = n$. We say that an A-submodule T of V is a lattice of V if and only if T is finitely generated and $T \otimes_A \mathrm{Frac}\,(A) = V$.

Remark 2.1.2. If A is a discrete valuation ring, any lattice of V is free over A.

Propostion 2.1.3 ([Bo, Chap. 7, §4.1, Proposition 2])**.** Let A be a commutative Noetherian integral domain and V a finite dimensional $\mathrm{Frac}\,(A)$-vector space. Let T be a lattice of V and T' an A-submodule of V.

(1) Assume there exist $x, y \in \mathrm{Frac}\,(A)^\times$ such that $xT \subset T' \subset yT$, then T' is a lattice.

(2) Conversely, assume T' is a lattice of V, then there exist $a, b \in A$ such that $aT \subset T' \subset b^{-1}T$.

Proof. (1) Since $T' \subset yT$ and T is finitely generated, T' is also finitely generated. Under the assumption of (1), we also have

$$V = xT \otimes_A \mathrm{Frac}\,(A) \subset T' \otimes_A \mathrm{Frac}\,(A) \subset yT \otimes_A \mathrm{Frac}\,(A) = V$$

hence T' is a lattice of V.

(2) We denote by $\{ e_1, \cdots, e_r \}$ the set of generators of T. Since $T \otimes_A \mathrm{Frac}\,(A) = T' \otimes_A \mathrm{Frac}\,(A)$, there exists an element $a \in A$ such that $ae_i \in T'$ for all i. Hence $aT \subset T'$. By changing the roles of T and T' there exists an $b \in A$ such that $bT' \subset T$.

□

Propostion 2.1.4 ([Bo, Chap. 7, §4.1, Proposition 3])**.** Let A be a commutative Noetherian integral domain and V a finite dimensional $\mathrm{Frac}\,(A)$-vector space. If T_1 and T_2 are lattices of V, so are $T_1 \cap T_2$ and $T_1 + T_2$.

Proof. Since there exist $a, b \in A$ such that $aT_1 \subset T_2 \subset b^{-1}T_1$ by (2) of Proposition 2.1.3, we have

$$aT_1 \subset T_1 \cap T_2, T_1 + T_2 \subset b^{-1}T_1.$$

Then the proposition follows by (1) of Proposition 2.1.3.

□

Propostion 2.1.5 ([Bo, Chap. 7, §4.1, Proposition 4])**.** Let B be a commutative Noetherian integral domain and A a sub ring of B. Let V be a finite dimensional $\mathrm{Frac}\,(A)$-vector space.

(1) For any lattice T of V, $T \otimes_A B$ is a lattice of $V \otimes_{\mathrm{Frac}(A)} \mathrm{Frac}\,(B)$.

(2) Suppose B is a faithfully flat A-module. Then the following map

$$\phi : \{ \text{ lattices of } V \} \to \{ \text{ lattices of } V \otimes_{\mathrm{Frac}(A)} \mathrm{Frac}\,(B) \}, T \mapsto T \otimes_A B$$

is injective.

Proof. (1) We have the following equalities:

$$\mathrm{Frac}\,(B) \otimes_B (B \otimes_A T) = (\mathrm{Frac}\,(B) \otimes_B B) \otimes_A T = \mathrm{Frac}\,(B) \otimes_A T. \tag{2.1}$$

Since $T \otimes_A \mathrm{Frac}\,(A) = V$ and $\mathrm{Frac}\,(B) = \mathrm{Frac}\,(B) \otimes_{\mathrm{Frac}(A)} \mathrm{Frac}\,(A)$, the last term of the above equalities becomes to $\mathrm{Frac}\,(B) \otimes_{\mathrm{Frac}(A)} V$. Hence $T \otimes_A B$ is a lattice of $V \otimes_{\mathrm{Frac}(A)} \mathrm{Frac}\,(B)$.

(2) Let T_1 and T_2 be lattices of V such that $B \otimes_A T_1 = B \otimes_A T_2$. First we assume $T_1 \subset T_2$. Then $B \otimes_A (T_2/T_1) = 0$. Since B is a faithfully flat A-module, we have $T_2 = T_1$. Now we consider the general case. We have the following equalities:

$$(B \otimes_A T_1) \cap (B \otimes_A T_2) = B \otimes_A (T_1 \cap T_2)$$

hence $T_1 \cap T_2 = T_1 = T_2$ by the above argument.

□

Propostion 2.1.6 ([Bo, Chap. 7, §4.1, Corollary to Proposition 4])**.** Let A be a discrete valuation ring and V a finite dimensional $\mathrm{Frac}\,(A)$-vector space. Let

$$\rho : G \to \mathrm{Aut}_{\mathrm{Frac}(A)}(V)$$

be a linear representation of a group G. We denote by $\hat{A}$ the completion of A and by $\hat{V} = V \otimes_K \mathrm{Frac}(\hat{A})$. Let $\hat{\rho}$ be the following linear representation:

$$\hat{\rho} : G \to \mathrm{Aut}_{\mathrm{Frac}(\hat{A})}(\hat{V}), g \mapsto \hat{\rho}(g)\,(v \otimes \alpha \mapsto \rho(g)\,v \otimes \alpha).$$

Then the following map

$$\{ \text{ lattices of } V \} \to \{ \text{ lattices of } \hat{V} \}, T \mapsto T \otimes_A \hat{A} \tag{2.2}$$

is bijective and the inverse map is given by maps $\hat{T}$ to $\hat{T} \cap V$, the same holds for the set of G-stable lattices.

Proof. Note that $T \otimes_A \hat{A}$ is the completion of T i.e $T \otimes \hat{A} = \varprojlim_n T/\varpi^n T$, where ϖ is a fixed uniformizer of A. Thus T is dense in $\hat{T}$. Since $T \otimes_A \hat{A}$ is open in $V \otimes_{\mathrm{Frac}(A)} \mathrm{Frac}(\hat{A})$ and T is open in V, we have $(T \otimes_A \hat{A}) \cap V = T$. This implies that the map (2.2) is injective. Now we prove the surjection. Let us take a lattice L of V. For any lattice $\hat{T}$ of $\hat{V}$, there exist two elements α and β of $\hat{A}$ such that $\alpha(L \otimes_A \hat{A}) \subset \hat{T} \subset \beta^{-1}(L \otimes_A \hat{A})$ by (2) of Proposition 2.1.3. Since every element of $\hat{A}$ can be writen by a product of a power of ϖ and an invertible element of $\hat{A}$, there exist two elements a and b of A such that

$$a(L \otimes_A \hat{A}) \subset \hat{T} \subset b^{-1}(L \otimes_A \hat{A}),$$

hence

$$aL \subset \hat{T} \cap V \subset b^{-1}L.$$

Thus $\hat{T} \cap V$ is a lattice of V by (1) of Proposition 2.1.3 and so $\hat{T} \cap V$ is open in V. Since V is dense in $\hat{V}$, $\hat{T} \cap V$ is dense in $\hat{T}$. Hence $\hat{T}$ is the completion of $\hat{T} \cap V$. Further if T is a G-stable lattice, we have

$$\rho(g)(T \otimes_A \hat{A}) = \rho\,(g)\, T \otimes_A \hat{A} = T \otimes_A \hat{A}$$

for any $g \in G$ and hence $T \otimes_A \hat{A}$ is also G-stable. If $\hat{T}$ is G-stable, we have

$$\rho\,(g)\,(\hat{T} \cap V) \subset (\hat{T} \cap V)$$

for any $g \in G$ and hence $\hat{T} \cap V$ is also G-stable. □

Remark 2.1.7. If we consider the lattice over a discrete valuation ring A. Proposition 2.1.6 permits us to confine to the case where A is complete.

2.2 Reflexive lattices

In this section, we recall some properties of reflexive lattices which will be used in Hida deformation (cf. Proposition 5.4.10).

Propostion 2.2.1 ([Bo, Chap. 7, §4.1, (iv) of Proposition 3])**.** Let A be a commutative Noetherian integral domain and V, W finite dimensional $\mathrm{Frac}\,(A)$-vector spaces. Let T_V be a lattice of V and T_W a lattice of W. We denote by $\mathrm{Hom}_{\mathrm{Frac}(A),T_V,T_W}\,(V,W)$ the A-submodule of $\mathrm{Hom}_{\mathrm{Frac}(A)}\,(V,W)$ as follows:

$$\mathrm{Hom}_{\mathrm{Frac}(A),T_V,T_W}\,(V,W) = \{\, f \in \mathrm{Hom}_{\mathrm{Frac}(A)}\,(V,W) \mid f\,(T_V) \subset T_W \,\}\,.$$

Then $\mathrm{Hom}_{\mathrm{Frac}(A),T_V,T_W}\,(V,W)$ is a lattice of $\mathrm{Hom}_{\mathrm{Frac}(A)}\,(V,W)$.

Proof. By Proposition 2.1.3 we have that there exist A-free lattices L_V, L'_V of V and L_W, L'_W of W such that

$$L'_V \subset T_V \subset L_V, L'_W \subset T_W \subset L_W.$$

Then

$$\mathrm{Hom}_{\mathrm{Frac}(A),L_V,L'_W}\,(V,W) \subset \mathrm{Hom}_{\mathrm{Frac}(A),T_V,T_W}\,(V,W) \subset \mathrm{Hom}_{\mathrm{Frac}(A),L'_V,L_W}\,(V,W)\,.$$

Since $\mathrm{Hom}_{\mathrm{Frac}(A),L_V,L'_W}\,(V,W)$ is isomorphic to $\mathrm{Hom}_A\,(L_V, L'_W)$, which is free of rank $\dim_{\mathrm{Frac}(A)}V \cdot \dim_{\mathrm{Frac}(A)}V$. Hence $\mathrm{Hom}_{\mathrm{Frac}(A),L_V,L'_W}\,(V,W)$ is a lattice of $\mathrm{Hom}_{\mathrm{Frac}(A)}\,(V,W)$ and the same holds for $\mathrm{Hom}_{\mathrm{Frac}(A),L'_V,L_W}\,(V,W)$. Thus $\mathrm{Hom}_{\mathrm{Frac}(A),T_V,T_W}\,(V,W)$ is a lattice of $\mathrm{Hom}_{\mathrm{Frac}(A)}\,(V,W)$. □

From now on to the end of this section, we denote by A a commutative Noetherian integrally closed domain and by V a finite dimensional $\mathrm{Frac}\,(A)$-vector space. We denote by $V^* = \mathrm{Hom}_{\mathrm{Frac}(A)}\,(V, \mathrm{Frac}\,(A))$ the dual of V and by $V^{**} = (V^*)^*$. Let T be a lattice of V. We denote by $T^* = \mathrm{Hom}_{\mathrm{Frac}(A),T,A}\,(V, \mathrm{Frac}\,(A))$ and by $T^{**} = (T^*)^*$. We may regard T is contained in T^{**} under the canonical isomorphism $V \xrightarrow{\sim} V^{**}$. We say that T is a reflexive lattice if $T = T^{**}$.

Propostion 2.2.2. Let the assumptions and the notations be as above. We have T^* and T^{**} are reflexive lattices for any T.

Proof. Note that $T \subset T^{**}$ implies $T^* \subset T^{***}$. On the other hand, we have $T^* \subset (T^*)^{**} = T^{***}$. Thus $T^* = T^{***}$ and $T^{**} = T^{****}$.

□

Theorem 2.2.3. Let the assumptions and the notations be as above. Then we have the following statements:

(1) $(T^*)_{\mathfrak{p}} = (T_{\mathfrak{p}})^*$ for any prime ideal $\mathfrak{p}$ ([Bo, Chap. 7, §4.1, Proposition 5]).

(2) $T^* = \bigcap_{\mathfrak{p} \in P^1(A)} (T^*)_{\mathfrak{p}}$, where $P^1\,(A)$ is the set of all height 1 prime ideal of A ([Bo, Chap. 7, §4.2, Theorem 1]).

(3) $T^{**} = \bigcap_{\mathfrak{p} \in P^1(A)} T_{\mathfrak{p}}$ ([Bo, Chap 7, §4.2, Corollary to Theorem 1]).

Proof. (1) We have $(T^*)_{\mathfrak{p}} \subset (T_{\mathfrak{p}})^*$ by definition. Conversely, let f be an element of $(T_{\mathfrak{p}})^*$ and $\{\, v_1, \cdots, v_r \,\}$ be a set of generators of T. Then there exists an element $s \in A \setminus \mathfrak{p}$ such that $f\,(v_i) \in s^{-1}A$ for any v_i and hence $sf \in T^*$.

(2) We have $T^* \subset \bigcap_{\mathfrak{p} \in P^1(A)} (T^*)_{\mathfrak{p}}$ by definition. Let us take an element $f \in \bigcap_{\mathfrak{p} \in P^1(A)} (T^*)_{\mathfrak{p}}$. Since $(T^*)_{\mathfrak{p}} = (T_{\mathfrak{p}})^*$ by (1), we have $f\,(v) \in \bigcap_{\mathfrak{p} \in P^1(A)} A_{\mathfrak{p}}$ for any $v \in T$. Under the assumption that A is a Noetherian integrally closed domain, we have $A = \bigcap_{\mathfrak{p} \in P^1(A)} A_{\mathfrak{p}}$.

(3) We have the following equalities by (1) and (2) :

$$T^{**} = (T^*)^* = \bigcap_{\mathfrak{p} \in P^1(A)} \left((T^*)_{\mathfrak{p}}\right)^* = \bigcap_{\mathfrak{p} \in P^1(A)} T_{\mathfrak{p}}^{**}.$$

Since $A_{\mathfrak{p}}$ is a principal ideal domain, we have that $T_{\mathfrak{p}}$ is free over $A_{\mathfrak{p}}$ and hence $T_{\mathfrak{p}}^{**} = T_{\mathfrak{p}}$. This completes the proof of Theorem 2.2.3.

□

The following theorem ensures us the existence of $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$-stable $\mathbb{I}$-free lattice in a Hida deformation under the assumption that $\mathbb{I}$ is a regular local ring (cf. Proposition 5.4.10).

Theorem 2.2.4 ([Oc2, Theorem 2.34])**.** Let the assumptions and the notations be as above. Let T be a lattice of V. Assume that A is a regular local ring with Krull dimension ≤ 2. Then T is free over A.

Proof. First we assume that the Krull dimension of A is 1. Since every regular local ring with Krull dimension 1 is a discrete valuation ring, we have every lattice is free over A.

Now we assume that the Krull dimension of A is 2. Under the assumption that A is a regular local ring, there exists an element $x \in A$ such that the quotient A/xA is a discrete valuation ring. We may regard $T^{**} \otimes_A A/xA$ as an A-submodule of $\mathrm{Hom}_A(T^*, A/xA)$ under the injection $T^{**} \otimes_A A/xA \hookrightarrow \mathrm{Hom}_A(T^*, A/xA)$. Since the module $\mathrm{Hom}_A(T^*, A/xA)$ is A-torsion free, so is $T^{**} \otimes_A A/xA$.

Let s be the number of a minimal basis (cf. [Mat, Theorem 2.3]) of T. Then we have the following exact sequence of A-modules:

$$0 \to \mathrm{Ker}\, h \to A^{\oplus s} \xrightarrow{h} T \to 0. \tag{2.3}$$

Since $T^{**} \otimes_A A/xA$ is A-torsion free and T is a reflexive lattice, we have that $T \otimes_A A/xA$ is also A-torsion free. Then the exact sequence (2.3) induces the following exact sequence of A/xA-modules:

$$0 \to \mathrm{Ker}\, h/\, x\mathrm{Ker}\, h \to (A/xA)^{\oplus s} \to T/xT \to 0. \tag{2.4}$$

We have that s is also the number of a minimal basis of the A/xA-module T/xT by Nakayama's lemma. Furthermore, since A/xA is a discrete valuation ring, T/xT is free over A/xA and hence $\mathrm{Ker}\, h/\, x\mathrm{Ker}\, h = 0$. Then $\mathrm{Ker}\, h = 0$ also by Nakayama's lemma. This completes the proof of Theorem 2.2.4. □

2.3 G-stable lattices

Definition 2.3.1. Let A be a commutative Noetherian integral domain and V be finite dimensional $\mathrm{Frac}(A)$-vector space with $\dim_{\mathrm{Frac}(A)} V = n$. For a linear representation

$$\rho : G \to \mathrm{Aut}_{\mathrm{Frac}(A)}(V)$$

of a group G, we say that a lattice T is a G-stable if $\rho(G)\, T = T$.

Propostion 2.3.2 ([Se2, Chap. 2, §1.3, Proposition 2])**.** Let A be a discrete valuation and V a finite dimensional $\mathrm{Frac}(A)$-vector space with $\dim_{\mathrm{Frac}(A)} V = n$. For a linear representation

$$\rho : G \to \mathrm{Aut}_{\mathrm{Frac}(A)}(V)$$

of a group G, the following are equivalent:

(1) There exists a G-stable lattice of V.

(2) There exists a basis $V = \otimes_{i=1}^{n} \mathrm{Frac}(A)\, e_i$ such that

$$\mathrm{Im}\left(\rho : G \to \mathrm{Aut}_{\mathrm{Frac}(A)}(V) \cong \mathrm{GL}_n(\mathrm{Frac}(A))\right) \subset \mathrm{GL}_n(A).$$

(3) Let us take any basis of V and regard ρ as the following homomorphism:

$$\rho : G \to \mathrm{GL}_n(\mathrm{Frac}(A)).$$

Then $\rho(G)$ is bounded in $\mathrm{GL}_n(\mathrm{Frac}(A))$ i.e. there exists an integer d such that $\mathrm{ord}_{\varpi}(s_{ij}) \geq d$ for any $s = (s_{ij}) \in \rho(G)$.

Proof. (1) implies (2) and (2) implies (3) are obvious. Let us prove (3) implies (1). Let T be a lattice of V. We denote by ϖ a fixed uniformizer of A. Since $\rho(G)$ is bounded, there exists an integer n such that $\rho(g)T \subset \varpi^n T$ for all $g \in G$. Then $\sum_{g\in G} \rho(g)T$ is a lattice by Proposition 2.1.4 and it is G-stable by definition.

□

We introduce the Brauer-Nesbitt theorem as follows, for the proof see [CR, 30.16].

Theorem 2.3.3 (Brauer-Nesbitt)**.** Let k be a field and F a k-algebra. Let M and M' be the semi-simple F-modules such that $\dim_k M = \dim_k M' < \infty$. Suppose for any $f \in F$, the characteristic polynomial of f acting on M and M' coincide. Then M and M' are isomorphic as F-modules.

Let A be a discrete valuation ring. We denote by ϖ a fixed uniformizer of A, $\mathbb{F} = A/(\varpi)$ the residue field. Let V be a finite dimensional $\mathrm{Frac}(A)$-vector space such that $\dim_K V = n$ and $\rho : G \to \mathrm{Aut}_{\mathrm{Frac}(A)}(V)$ a linear representation of a group G such that ρ has a G-stable lattice T. Then we denote by ρ_T the representation

$$\rho_T : G \to \mathrm{Aut}_A(T)$$

and by $\bar{\rho}_T$ the representation $\rho_T \bmod \varpi$ as follows:

$$\rho_T \bmod \varpi : G \xrightarrow{\rho_T} \mathrm{Aut}_{\mathcal{O}}(T) \xrightarrow{\bmod \varpi} \mathrm{Aut}_{A/(\varpi)}(T/\varpi T).$$

Corollary 2.3.4. Let the assumptions and the notations be as above. We have $\overline{\rho}_T^{\mathrm{ss}} \cong \overline{\rho}_{T'}^{\mathrm{ss}}$ for any G-stable lattice T and T', where $\overline{\rho}_T^{\mathrm{ss}}$ (resp. $\overline{\rho}_{T'}^{\mathrm{ss}}$) is the semi-simplification of the $\mathbb{F}[G]$-module $T/\varpi T$ (resp. $T'/\varpi T'$).

Proof. Let us take an element $g \in G$. Note that the characteristic polynomial of $\rho(g)$ is an element of $A[X]$ under the assumption that ρ has a G-stable lattice. The characteristic polynomial of $\overline{\rho}_T(g)$ and $\overline{\rho}_{T'}(g)$ is the mod ϖ reduction of the characteristic polynomial of $\rho(g)$. Then the corollary follows by applying Theorem 2.3.3 (we let $k = \mathbb{F}, F = \mathbb{F}[G], M = T/\varpi T$ and $M' = T'/\varpi T'$).

□

We see that the semi-simplification of mod ϖ representation is independent of the choices of G-stable lattice. Hence we denote by $\overline{\rho}^{\mathrm{ss}}$ the semi-simplification of $\overline{\rho}_T$.

At the end of this section we introduce a condition which makes the G-stable lattice unique up to multiplications by elements of $K^\times$:

Propostion 2.3.5 ([Oc3, Lemma 5.11])**.** Let the assumptions and the notations be as above. Assume $\overline{\rho}_T$ is irreducible. Then for any G-stable lattice T', there exists an element $x \in \mathrm{Frac}(A)^\times$ such that $T' = xT$.

Proof. We prove this proposition by contradiction. By (2) of Proposition 2.1.3 we may assume that there exists a G-stable lattice T' such that $\varpi T \subsetneq T' \subsetneq T$. Since $T/\varpi T$ is an irreducible $\mathbb{F}[G]$-module we have $T'/\varpi T = T/\varpi T$ and hence $T' + \varpi T = T$. Thus $T' = T$ by Nakayama's lemma. This contradicts to our assumption that $T' \subsetneq T$.

□

2.4 p-adic Galois representation and $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$-stable lattices

Let K be a finite extension of $\mathbb{Q}_p$. We denote by $(\mathcal{O}, \varpi, \mathbb{F})$ the ring of integers of K, a fixed uniformizer of $\mathcal{O}$ and the residue field $\mathbb{F} = \mathcal{O}/(\varpi)$. Let V be a finite dimensional K-vector space with $\dim_K V = n$. We induce the product topology on $\mathrm{Aut}_K(V) \cong \mathrm{GL}_n(K)$.

Definition 2.4.1. A p-adic Galois representation of $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ is a continuous homomorphism $\rho : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \to \mathrm{Aut}_K(V)$.

Propostion 2.4.2 ([Se1, pp.1-2])**.** Let $\rho : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \to \mathrm{Aut}_K(V)$ be a p-adic representation. Then there exists a $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$-stable lattice.

Proof. Since ρ is continuous and $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ is compact, we have $\rho\left(\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)\right)$ is bounded in $\mathrm{Aut}_K(V) \cong \mathrm{GL}_n(K)$. Then the proposition follows by Proposition 2.3.2.

□

The following proposition tells us that the number of the isomorphic classes of $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$-stable lattices is finite in an irreducible p-adic representation:

Propostion 2.4.3 ([Oc3, Proposition 5.13])**.** Let $\rho : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \to \mathrm{Aut}_K(V)$ be a p-adic representation. Assume ρ is irreducible, then $\sharp\mathscr{L}(\rho) < \infty$.

Proof. We prove this proposition by contradiction. Assume $\sharp\mathscr{L}(\rho) = \infty$. Then there are infinitely many $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$-stable lattices up to multiplications by elements of $K^\times$. Let us take a $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$-stable lattice T. We have $T/\varpi T$ is a reducible $\mathcal{O}[G]$-module by Proposition 2.3.5. For any $n \in \mathbb{Z}_{>0}$, we denote by $\mathscr{L}_n$ the set of $\mathcal{O}[G]$-submodules M of $T/\varpi^n T$ for which the following conditions hold:

(i) $\{0\} \subsetneq M \subsetneq T/\varpi^n T$.

(ii) $M \nsubseteq \varpi T/\varpi^n T$.

(iii) $\varpi^{n-1}T/\varpi^n T \nsubseteq M$.

For any $n \in \mathbb{Z}_{\geq 1}$, since $\mathcal{O}$ is profinite, there exists a $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$-stable lattice $T' \subsetneq T$ such that $\varpi^n \subset\neq T', T' \nsubseteq \varpi T$ and $\varpi^{n-1}T \nsubseteq T'$. Thus the set $\mathcal{L}_n$ is non-empty for any n.

For any $M_{n+1} \in \mathcal{L}_{n+1}$, we denote by M_n the image of M_{n+1} under the homomorphism $T/\varpi^{n+1}T \twoheadrightarrow T/\varpi^n T$. Now we prove $M_n \in \mathcal{L}_n$. We denote by L the inverse image of M_{n+1} under $T \twoheadrightarrow T/\varpi^{n+1}T$. Then L is a $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$-stable lattice. The conditions (i), (ii) and (iii) in $\mathscr{L}_{n+1}$ is equivalent to the following conditions:

(I) $\varpi^{n+1}T \subsetneq L \subsetneq T$.

(II) $L \subsetneq \varpi T$.

(III) $\varpi^n T \nsubseteq L$.

The conditions (I) and (III) imply $\varpi^n T \subsetneq L + \varpi^n T \subsetneq T$. The condition (II) implies $L + \varpi^n T \subsetneq \varpi T$. Furthermore, we also have $\varpi^{n-1}T \nsubseteq L + \varpi^n T$ by the condition (III). The above arguments tell us that $M_n = L + \varpi^n T/\varpi^n T$ satisfy the condition (i), (ii) and (iii) in $\mathscr{L}_n$.

For any $i < j$, the homomorphism $T/\varpi^j T \twoheadrightarrow T/\varpi^i T$ induces a map from $\mathcal{L}_j$ to $\mathcal{L}_i$. The above argument tells us that $\{\mathcal{L}_n\}_{n\in\mathbb{Z}_{\geq 1}}$ is an inverse system. We have $\varprojlim_n \mathcal{L}_n \neq \varnothing$. Let us take an element $M = (M_1, M_2, \cdots) \in \varprojlim_n \mathscr{L}_n$. Clearly we have $M \subset T$ and M is $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$-stable. Assume M is a lattice of V. Then there exists an element $m \in \mathbb{Z}_{\geq 1}$ such that $\varpi^m T \subset M \subset T$ by (2) of Proposition 2.1.3. This contradicts to the condition (iii) in $\mathcal{L}_{m+1}$ and hence M is not a lattice of V. Thus $\mathrm{rank}_{\mathcal{O}} M < \mathrm{rank}_{\mathcal{O}} T$ and $M \otimes_{\mathcal{O}} K$ is a proper nontrivial $K[G]$-submodule of V. This contradicts to the assumption that ρ is irreducible and we finish the proof of Proposition 2.4.3.

□

2.5 Modular forms and their p-adic Galois representations

In this section, we summary some preliminaries and results on modular forms and their Galois representations. For more details and the proof, the reader can refer to [Hi3, Chap.5] and [Sh] for example. We fix a positive integer M and ψ a Dirichlet character modulo M in this section. We denote by $\Gamma_0(M)$ and $\Gamma_1(M)$ the following subgroup of $\mathrm{SL}_2(\mathbb{Z})$:

$$\Gamma_0(M) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \middle| \, c \equiv 0 \pmod{M} \right\},$$

$$\Gamma_1(M) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \middle| \, c \equiv 0 \pmod{M}, d \equiv 1 \pmod{M} \right\}.$$

Note that we have $\Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$. We denote by

$$\mathfrak{h} = \{ z \in \mathbb{C} | \, \mathrm{Im}(z) > 0 \}$$

the complex upper half plane. Let f be a $\mathbb{C}$-valued function, $k \in \mathbb{Z}$ and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{R})$. We define the weight k action of γ on f as follows:

$$f|_k \gamma : \mathfrak{h} \to \mathbb{C}, z \mapsto \det(\gamma)^{k/2} (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right).$$

For any $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(M)$, we denote by $\psi(\gamma) = \psi(d)$.

Definition 2.5.1. Let

$$f : \mathfrak{h} \to \mathbb{C}$$

be a function. We say that f is a modular form of weight k, level M with Neben character ψ if f satisfies the following conditions:

(i) $f|_k \gamma = f$ for all $\gamma \in \Gamma_1(M)$.

(ii) $f|_k \gamma = \psi(\gamma) f$ for all $\gamma \in \Gamma_0(M)$.

(iii) For any $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, $f|_k \alpha$ is holomorphic at ∞.

Since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_1(M)$, if f is a modular form we have $f(z+1) = f(z)$ by the condition (i). Then by the condition (iii), $f(z)$ has the Fourier expansion $f(z) = \sum_{n \geq 0} a(n, f) q^n$ with $q = \exp\left(2\pi\sqrt{-1}z\right)$. We say that f is a cusp form of weight k, level M with Neben character ψ if f is a modular form and further $a(0, f|_k \alpha) = 0$ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$. We denote by $M_k(\Gamma_0(M), \psi)$ (resp. $S_k(\Gamma_0(M), \psi)$ the space of modular forms (resp. cusp forms) of weight k, level M, Neben character ψ.

Example 2.5.2. We define $E_{k,\psi}(z)$ as follows:

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

where $\sigma_{k-1,\psi}(n) = \sum_{d|n} \psi(d) d^{k-1}$. Then we have $E_{k,\psi}(z) \in M_k(\Gamma_0(M), \psi)$ for $k \geq 2$ (cf. [Hi3, §5.1]). We call $E_{k,\psi}(z)$ the Eisenstein series of weight k and Neben character ψ.

Example 2.5.3. We define $\Delta(z)$ as follows:

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

Then $\Delta(z) \in S_{12}(\mathrm{SL}_2(\mathbb{Z}))$ which is called the Ramanujan's cusp form.

Definition 2.5.4 (Hecke operators)**.** Let $n \in \mathbb{Z}_{>0}$, we denote by

$$T(n) : M_k(\Gamma_0(M), \psi) \to M_k(\Gamma_0(M), \psi), f \mapsto T(n) f$$

a linear map such that

$$a(m, T(n) f) = \sum_{b|(m,n)} \psi(b) b^{k-1} a\left(\frac{mn}{b^2}, f\right)$$

with $\psi(b) := 0$ if $(b, M) > 1$.

Note that if we decompose an integer $n \in \mathbb{Z}_{>0}$ into the production of prime numbers: $n = \prod_i l_i^{e_{l_i}}$, then $T(n)$ is generated by all $T(l_i)$ (cf. [Hi3, §5.3]).

Definition 2.5.5. Let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbb{Q}_p$ the Hecke algebra $H_k(\Gamma_0(M), \psi, \mathcal{O})$ (resp. $h_k(\Gamma_0(M), \psi, \mathcal{O})$) is the $\mathcal{O}$ sub-algebra of $\mathrm{End}_{\mathcal{O}}(M_k(\Gamma_0(M), \psi, \mathcal{O}))$ (resp. $\mathrm{End}_{\mathcal{O}}(S_k(\Gamma_0(M), \psi, \mathcal{O}))$) which is generated by all Hecke operators $T(n)$.

We have the following duality theorem between the Hecke algebra $h_k(\Gamma_0(M), \psi, \mathcal{O})$ and the space of cusp forms $S_k(\Gamma_0(M), \psi, \mathcal{O})$. For the proof, see [Hi3, §5.3, Theorem 1].

Theorem 2.5.6 (Duality)**.** The following pairing

$$h_k(\Gamma_0(M), \psi, \mathcal{O}) \times S_k(\Gamma_0(M), \psi, \mathcal{O}) \to \mathcal{O}, (h, f) \mapsto a(1, h \cdot f) \tag{2.5}$$

is perfect i.e. we have the following isomorphisms:

$$S_k(\Gamma_0(M), \psi, \mathcal{O}) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{O}}(h_k(\Gamma_0(M), \psi, \mathcal{O}), \mathcal{O}),$$

$$h_k(\Gamma_0(M), \psi, \mathcal{O}) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{O}}(S_k(\Gamma_0(M), \psi, \mathcal{O}), \mathcal{O}).$$

We call that a cusp form f is a normalized Hecke eigen cusp form if $a(1,f)=1$ and $T(n)f=a(n,f)f$ for all $T(n)$. For example the Ramanujan's cusp form Δ is a normalized Hecke eigen cusp form.

Definition 2.5.7. We say that a Galois representation ρ is unramified at a prime l if $\rho(I_l)=\{1\}$, otherwise we say that ρ is ramified at l.

Theorem 2.5.8 (Deligne-Shimura)**.** Let $k\in\mathbb{Z}_{\geq 2}$ and $f\in S_k(\Gamma_0(M),\psi,\mathcal{O})$ a normalized Hecke eigen cusp form, where $\mathcal{O}$ is the ring of integers of a finite extension of $\mathbb{Q}_p$. Then there exists a p-adic Galois representation

$$\rho_f:\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)\to \mathrm{GL}_2(\mathrm{Frac}(\mathcal{O}))$$

such that

(1) The representation ρ_f is irreducible and unramified outside the primes dividing Mp.

(2) For the geometric Frobenius element Frob_l at $l\nmid Mp$,

$$\mathrm{tr}\,\rho_f(\mathrm{Frob}_l)=a(l,f),$$

$$\det\rho_f(\mathrm{Frob}_l)=\psi(l)\,l^{k-1}.$$

At the end of this section we recall the Chebotarev density theorem (cf. [Se1, §2.2] for our later use

Theorem 2.5.9 (Chebotarev density theorem)**.** We denote by Σ a finite set of primes and G_Σ the Galois group of the largest algebraic extension of $\mathbb{Q}$ unramified outside Σ. Then $\{\mathrm{Frob}_l \mid l\notin\Sigma\}$ is a density subset of G_Σ.

Chapter 3

Ribet's lemma

3.1 Ribet's proof of the converse of Herbrand theorem

In 1976, Ribet [Ri] proved the converse of Herbrand theorem as follows:

Theorem 3.1.1 (Ribet)**.** Let k be an even integer satisfying $2 \leq k \leq p-3$. We denote by $\mathrm{Cl}(\mathbb{Q}(\mu_p))[p]$ the p-part of the ideal class group of $\mathbb{Q}(\mu_p)$ on which the Galois group $\mathrm{Gal}\left(\mathbb{Q}\left(\mu_p\right)/\mathbb{Q}\right)$ acts by functoriality. Suppose p divides $L\left(1-k,\mathbf{1}\right)$. Then $\mathrm{Cl}(\mathbb{Q}(\mu_p))[p]^{\omega^{1-k}} \neq 0$.

We prove Theorem 3.1.1 in this section. However the tools we used is slightly different from Ribet's original proof. These tools also illustrates the proof of our main theorem.

First we recall the following theorem (see [Da, §6] for example).

Theorem 3.1.2. Let the assumptions and the notations be as in Theorem 3.1.1. Under the assumption that p divides $L\left(1-k,\mathbf{1}\right)$, there exists a normalized Hecke eigen cusp form $f \in S_k\left(\mathrm{SL}_2\left(\mathbb{Z}\right)\right)$ such that $f \equiv E_k \pmod{(\varpi)}$, where $E_k = E_{k,\mathbf{1}}$ (cf. Example 2.5.2) and ϖ is a fixed uniformizer of the ring of integers of $K = \mathbb{Q}_p\left(\left\{a\left(n,f\right)\right\}_{n\geq 1}\right)$.

By class field theory we see that to prove Theorem 3.1.1, it is equivalent to construct an unramified abelian p-elementary extension L (i.e. $\mathrm{Gal}\left(L/\mathbb{Q}\left(\mu_p\right)\right) \cong \left(\mathbb{Z}/p\mathbb{Z}\right)^{\oplus n}$) of $\mathbb{Q}\left(\mu_p\right)$ on which $\mathrm{Gal}\left(\mathbb{Q}\left(\mu_p\right)/\mathbb{Q}\right)$ acts via ω^{1-k}. We construct the field L by using the Galois representation ρ_f attached to f (cf. Theorem 2.5.8). We denote by $\Sigma = \{\, p, \infty \,\}$. Since ρ_f is unramified outside Σ, ρ_f must factor through G_Σ. From now on to the end of this section, we write

$$\rho_f : G_\Sigma \to \mathrm{GL}_2\left(K\right).$$

We denote by $\mathcal{O}$ the ring of integers of K and by $\mathbb{F}$ the residue field.

Lemma 3.1.3. The mod (ϖ) representation of ρ_f is reducible, Furthermore we have $\overline{\rho}_f^{\mathrm{ss}} \cong \mathbb{F}[\mathbf{1}] \oplus \mathbb{F}[\omega^{k-1}]$.

Proof. Let us take a $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$-stable lattice T of ρ_f. Since $f \equiv E_k \pmod{(\varpi)}$ by Theorem 3.1.2, we have $\mathrm{tr}\,\rho_f\left(\mathrm{Frob}_l\right) \equiv 1 + l^{k-1} \pmod{(\varpi)}$ for all $l \neq p$. Thus $\mathrm{tr}\,\rho_f\left(g\right) \equiv 1 + \omega^{k-1}\left(g\right) \pmod{\varpi}$ for all $g \in G_\Sigma$ by Theorem 2.5.9. Since

$$\det \rho_f\left(g\right) = 2^{-1}\left(\mathrm{tr}\,\rho_f\left(g\right)^2 - \mathrm{tr}\,\rho_f\left(g^2\right)\right),$$

we also have $\det \rho_f(g) \equiv \omega^{k-1}(g) \pmod{\varpi}$ for all $g \in G_\Sigma$. Thus the lemma follows by applying Theorem 2.3.3 to $M = (T/\varpi T)^{\mathrm{ss}}$ and $M' = \mathbb{F}(\mathbf{1}) \oplus \mathbb{F}\left(\omega^{k-1}\right)$.

□

Since $f \equiv E_k \pmod{(\varpi)}$, we have $a(p,f) \equiv 1 \pmod{\varpi}$ and hence $a(p,f)$ is a p-adic unit. By a theorem of Mazur-Wiles (see Theorem 5.4.9 for the statement in more general case), there exists a basis of ρ_f such that

$$\rho_f|_{D_p} = \begin{pmatrix} \varepsilon_1 & 0 \\ * & \varepsilon_2 \end{pmatrix}$$

with ε_1 unramified and $\varepsilon_1(\mathrm{Frob}_p) = a(p,f)$. Thus

$$(X - \varepsilon_1(g))(X - \varepsilon_2(g)) \equiv (X-1)\left(X - \omega^{k-1}(g)\right) \pmod{\varpi}$$

for any $g \in D_p$ by Lemma 3.1.3. Since k is an even integer, we have $\overline{\varepsilon}_2 = \overline{\omega}^{k-1}$ is ramified at p. Choose an element $g_0 \in I_p$ such that $1 \not\equiv \varepsilon_2(g_0) \pmod{\varpi}$ and choose a basis of ρ_f such that

$$\rho_f|_{D_p} = \begin{pmatrix} \varepsilon_1 & 0 \\ * & \varepsilon_2 \end{pmatrix} \text{ and } \rho_f(g_0) = \begin{pmatrix} 1 & 0 \\ 0 & \varepsilon_2(g_0) \end{pmatrix}. \tag{3.1}$$

Write $\rho_f(g) = \begin{pmatrix} a(g) & b(g) \\ c(g) & d(g) \end{pmatrix}$ for any $g \in G_\Sigma$. By the following equalities

$$\begin{cases} \mathrm{tr}\rho_f(g_0 g) = a(g) + \varepsilon_2(g_0)\, d(g) \in \mathcal{O} \\ \mathrm{tr}\rho_f(g) = a(g) + d(g) \in \mathcal{O}. \end{cases} \tag{3.2}$$

we have $\varepsilon_2(g_0) - 1 \in \mathcal{O}^\times$. Thus $a(g), d(g) \in \mathcal{O}$ for any $g \in G_\Sigma$. By modulo (ϖ), we have $\overline{a}(g)$ and $\overline{d}(g)$ are the solution for x and y of the following equation:

$$\begin{cases} x + \overline{\varepsilon}_2(g_0)\, y = 1 + \overline{\varepsilon}_2(g_0)\, \omega^{k-1}(g) \\ x + y = 1 + \omega^{k-1}(g). \end{cases} \tag{3.3}$$

Thus we have $a(g) \equiv 1 \pmod{\varpi}$ and $d(g) \equiv \omega^{k-1}(g) \pmod{\varpi}$ for any $g \in G_\Sigma$ by the equality (3.1). Furthermore, we have the following equality

$$b(g)\, c(g') = a(gg') - a(g)\, a(g') \in (\varpi) \tag{3.4}$$

for any $g, g' \in G_\Sigma$.

We denote by B (resp. C) the $\mathcal{O}$-submodule of V which is generated by $b(g)$ (resp. $c(g)$) for all $g \in G_\Sigma$. Since ρ_f has a G_Σ-stable lattice by Proposition 2.4.2, B and C are bounded by Proposition 2.3.2. Also by the irreducibility of ρ_f we have B and C are non-zero ideals. We introduce two operations as follows:

Operation 1. Let $B = (\varpi^n)$ with $n \in \mathbb{Z}$. We replace ρ_f to

$$\begin{pmatrix} 1 & 0 \\ \varpi^n & 1 \end{pmatrix} \rho_f \begin{pmatrix} 1 & 0 \\ \varpi^n & 1 \end{pmatrix}^{-1}$$

and we use the same symbol $\rho_f(g) = \begin{pmatrix} a(g) & b(g) \\ c(g) & d(g) \end{pmatrix}$ and B as above. Then by a matrix calculation we have $B = \mathcal{O}$ after this operation.

Then $B = \mathcal{O}$ by Operation 1. Thus we have $C \subset (\varpi)$ by the equality (3.4). Let e_1, e_2 be $\mathcal{O}$-basis corresponding to this representation and we denote by $T = \mathcal{O}e_1 \oplus \mathcal{O}e_2$. Then we have that $\overline{\rho}_T$ is of the form $\begin{pmatrix} 1 & * \\ 0 & \omega^{k-1} \end{pmatrix}$ and is not semi-simple.

By using the arguments above in more general settings, we can prove the following proposition :

Propostion 3.1.4 ([Ri, Proposition 2.1])**.** Let K be a finite extension of $\mathbb{Q}_p$ and V a K-vector space of dimension 2. Let $\rho : G \to \mathrm{Aut}_K(V)$ be a linear representation of a group G such that ρ has a G-stable lattice. Suppose ρ is irreducible and $\overline{\rho}^{\mathrm{ss}} \cong \vartheta_1 \oplus \vartheta_2$, where ϑ_1 and ϑ_2 are characters. Then there exists a G-stable lattice T such that $\overline{\rho}_T$ is of the form $\begin{pmatrix} \vartheta_1 & * \\ 0 & \vartheta_2 \end{pmatrix}$ but is not semi-simple.

Under the above preparation we are ready to prove Theorem 3.1.1

Proof of Theorem 3.1.1. By the above arguments we have that there exists a G_Σ-stable lattice T such that $\rho_T : G \to \mathrm{GL}_2(\mathcal{O}), g \mapsto \begin{pmatrix} a(g) & b(g) \\ c(g) & d(g) \end{pmatrix}$ has the following properties:

(i) $\rho_T|_{D_p} = \begin{pmatrix} \varepsilon_1 & 0 \\ * & \varepsilon_2 \end{pmatrix}$.

(ii) $\overline{\rho}_T = \begin{pmatrix} 1 & * \\ 0 & \omega^{k-1} \end{pmatrix}$ and $\overline{\rho}_T$ is not semi-simple.

By restriction $\overline{\rho}_T$ to $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}(\mu_p))$, we get the following homomorphism:

$$\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}(\mu_p)) \to B/\varpi B = \mathbb{F}, g \mapsto \overline{b}(g).$$

Since the group $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ has order prime to p, we have that the above homomorphism is surjective. Let L be the abelian extension of $\mathbb{Q}(\mu_p)$ corresponding to

$$\mathrm{Ker}(\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}(\mu_p)) \to \mathbb{F})$$

and we denote by $\overline{b}$ the following isomorphism:

$$\overline{b} : G := \mathrm{Gal}(L/\mathbb{Q}(\mu_p)) \xrightarrow{\sim} \mathbb{F}, g \mapsto \overline{b}(g).$$

We have ρ_f is unramified outside Σ. Furthermore by the condition (i) we have $\overline{b}(I_p) = 0$. Thus the extension $L/\mathbb{Q}(\mu_p)$ is unramified everywhere. By a matrix calculation we have that $\overline{b}(sgs^{-1}) = \omega^{1-k}(s)\overline{b}(g)$ for any $g \in \mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}(\mu_p))$ and $s \in G_\Sigma$. Thus L is the desired field and this completes the proof of Theorem 3.1.1.

3.2 The Bruhat-Tits tree of GL_2

In this section, we introduce the tree structure of the homothetic classes of G-stable lattices in a linear representation of dimension 2 over a discrete valuation ring. This tree structure also gives us another proof of Ribet's lemma. For more details on this theory, the reader can refer to [Be], [BC3] and [Se2].

From now on to the end of this chapter, we fix a discrete valuation ring A with ϖ a fixed uniformizer of A and $\mathbb{F} = A/(\varpi)$ the residue field. Let V be a finite-dimensional $\mathrm{Frac}(A)$-vector space.

Definition 3.2.1. Let T and T' be lattices of V. We say that T and T' are homothetic if there exists an element $\lambda \in \mathrm{Frac}\,(A)^{\times}$ such that $T' = \lambda T$.

Let $\mathscr{X}$ be the set of lattices in V up to homotheties. For a lattice T, we denote by $[T]$ its equivalence class up to homotheties.

Definition 3.2.2. Let x and x' be the points of $\mathscr{X}$. We say that x is a neighbor of x' if $x \neq x'$ and there exist lattices T, T' of V such that $x = [T], x' = [T']$ and $\varpi T \subset T' \subset T$.

Lemma 3.2.3. Let x and x' be the points of $\mathscr{X}$. Suppose x is a neighbor of x', then x' is also a neighbor of x.

Proof. Let T, T' be the lattices of V such that $x = [T], x' = [T']$ and $\varpi T \subset T' \subset T$. Then $\varpi T' \subset \varpi T \subset T'$. □

We recall the definition of graph as follows:

Definition 3.2.4. A graph Γ is consisted by a data $(\mathrm{vert}\,\Gamma, \mathrm{edge}\,\Gamma, (o,t), i)$ such that

(1) $\mathrm{vert}\,\Gamma$ is a set which is called the vertex set of Γ.

(2) $\mathrm{edge}\,\Gamma$ is a set which is called the edge set of Γ.

(3) (o,t) and i are the following maps

$$(o,t) : \mathrm{edge}\,\Gamma \to \mathrm{vert}\,\Gamma \times \mathrm{vert}\,\Gamma, y \mapsto (o(y), t(y,)),$$

$$i : \mathrm{edge}\,\Gamma \to \mathrm{edge}\,\Gamma, y \mapsto i(y)$$

which satisfy $i(y) \neq y, i(i(y)) = y$ and $o(y) = t(i(y))$.

An element in $x \in \mathrm{vert}\,\Gamma$ is called a vertex of Γ. An element $y \in \mathrm{edge}\,\Gamma$ is called an edge and $i(y)$ is called the inverse edge of y. The vertex $o(y)$ is called the origin of y and $t(y)$ is called the terminus of y.

We endow $\mathscr{X}$ a graph structure as follows:

(vert) The vertex set is $\mathscr{X}$.

(edge) We draw an edge from x to x' if x is a neighbor of x' for the points $x, x' \in \mathscr{X}$.

Then $\mathscr{X}$ is a graph by Lemma 3.2.3. In $\mathscr{X}$, a path from x to x', which is denoted by $\mathrm{Path}_{x,x'}$ is a sequence $x = x_0, x_1, ..., x_n = x'$ of points in $\mathscr{X}$ such that x_i is a neighbor of x_{i+1}. The integer n is the length of the path. Define $d(x,x')$ the distance form x to x' which is the minimal length of a path from x to x'. We call $\mathrm{Path}_{x,x'}$ a path without backtracking if $x_i \neq x_j$ for any $i \neq j$.

Theorem 3.2.5 ([Se2, Chapter II, Theorem 1])**.**

(1) The graph $\mathscr{X}$ is connected i.e. for $x \neq x' \in \mathscr{X}$, there exists a path without backtracking $\mathrm{Path}_{x,x'}$ from x to x'.

(2) Suppose $n = 2$. Then the graph $\mathscr{X}$ is a tree i.e. for $x \neq x' \in \mathscr{X}$, there exists a unique path $\mathrm{Path}_{x,x'}$ without backtracking from x to x'.

Proof. We denote by $x = [T]$ and $x' = [T']$ such that $T' \subset T$ and $T' \not\subset \varpi T$. We have the sequence of lattices

$$T' = T_n \subset T_{n-1} \subset \cdots \subset T_0 = T$$

such that $T_{i-1}/T_i \cong A/(\varpi)$ as A-modules $(i = 1, \cdots, n)$ by the Jordan-Hölder sequence for T/T'. This implies T_{i-1} is a neighbor of T_i and hence $[T_n], [T_{n-1}], \cdots, [T_0]$ is a path form x to x'. Assume $[T_i] = [T_j]$ for some $i < j$, then $T' \subset \varpi T$ which contradicts to our assumption. This completes the proof of (1).

We keep the notations as above and consider the case $n = 2$. By the arguments above we have $d(x, x') = n$. We prove that there exists a unique path without backtracking form x to x' by induction on n. It is obvious if $n = 1$ and hence it is suffices to show that there exists a unique lattice T_{n-1} such that $T_n \subset T_{n-1} \subset T_0$ and $[T_{n-1}]$ is a neighbor of $[T_n]$. Suppose we have two distinct neighbors $[T_{n-1}]$ and $[T'_{n-1}]$ of $[T_n]$ such that T_{n-1} and T'_{n-1} lives between T_n and T_0 under inclusion. Since T_n is free of rank 2 and $T_{n-1} \neq T'_{n-1}$ we have $T_n/\varpi T_n = \varpi T_{n-1}/\varpi T_n \oplus \varpi T'_{n-1}/\varpi T_n$. Hence $T_n = \varpi T_{n-1} + \varpi T'_{n-1}$ by Nakayama's lemma. Then $T_n \subset \varpi T_0$ which contradicts to our assumption. This completes the proof of Theorem 3.2.5. □

From now on to the end of this section we assume $n = 2$.

Propostion 3.2.6 ([BC3, §2.1])**.** Let $x = [T]$ and $n \in \mathbb{Z}_{>0}$ be a fixed integer. Then there is a bijection between the set of the points x' in $\mathscr{X}$ such that $d(x, x') = n$ and the set of lattices $\varpi^n T \subset T' \subset T$ such that $T/T' \cong A/(\varpi)^n$ as an A-module.

Proof. Let $x' = [T']$ such that $d(x, x') = n$ and $T' \not\subset T$. Then there exists a basis $\{e_1, e_2\}$ such that $T = Ae_1 \oplus Ae_2$ and $T' = Ae_1 \oplus A\varpi^n e_2$. Hence $T/T' \cong A/(\varpi)^n$.

For the converse let us choose a lattice T' satisfying $\varpi^n T \subset T' \subset T$ and $T/T' \cong A/(\varpi)^n$. Then there exists a basis $\{e_1, e_2\}$ such that $T = Ae_1 \oplus Ae_2$ and $T' = Ae_1 \oplus A\varpi^n e_2$. For $0 \leq i \leq n$ we denote by $T_i = Ae_1 \oplus A\varpi^i e_2$ and by $x_i = [T_i]$. Then $x_n = [T'], x_{n-1}, \cdots, x_0 = [T]$ is a path without backtracking from x to x'. Thus $d(x, x') = n$.

□

Definition 3.2.7. In the tree $\mathscr{X}$, we define the segment $[x, x']$ as follows:

$$[x, x'] = \begin{cases} \{x\} & (x = x') \\ \mathrm{Path}_{x,x'} & (x \neq x'), \end{cases}$$

where $\mathrm{Path}_{x,x'}$ is the unique path without backtracking form x to x'.

Definition 3.2.8. A subset C of $\mathscr{X}$ is called a convex if the segment $[x, x'] \subset C$ for any $x, x' \in C$.

Definition 3.2.9. Let $x = [T]$ be a point in $\mathscr{X}$. A half-line L_x with origin x is a union of segments $\cup_{n=1}^{\infty}[x, x_n]$, where $H \subsetneq T$ is a direct summand of T and $x_n = [H + \varpi^n T]$.

3.3 Another proof of Ribet's lemma

We keep our notation as in the previous section and we assume $\dim_K V = 2$. First we reformulate Ribet's lemma for more general setting as follows:

Propostion 3.3.1. Let $\rho : G \to \mathrm{Aut}_K V$ be an irreducible linear representation of a group G such that ρ has a G-stable lattice. Assume $\overline{\rho}^{\mathrm{ss}} \cong \vartheta_1 \oplus \vartheta_2$, where $\vartheta_i : G \to \mathbb{F}^\times$ are characters $(i = 1, 2)$. Then there exists a G-stable lattice T such that $\overline{\rho}_T$ is of the form $\begin{pmatrix} \vartheta_1 & * \\ 0 & \vartheta_2 \end{pmatrix}$ but not semi-simple.

Let us keep the assumptions and the notations of Proposition 3.3.1 from now on to the end of this section. We denote by $\mathscr{C}(\rho)$ the set of $x \in \mathscr{X}$ satisfying $\rho(g)\, x = x$ for any $g \in G$.

Lemma 3.3.2 ([BC3, Proposition 11-(a)])**.** Let $x = [T] \in \mathscr{C}(\rho)$. Then T is a G-stable lattice and hence $\mathscr{C}(\rho)$ is non-empty.

Proof. For any $g \in G$, we have $\rho(g)\, T = \varpi^{n(g)} T$. Since $\rho(G)$ is bounded by Proposition 2.3.2, we have $n(g) = 0$.

□

Lemma 3.3.2 implies that $\mathscr{C}(\rho)$ is exactly the set of the homothetic (cf. Definition 3.2.1) class of G-stable lattice.

Lemma 3.3.3 ([BC3, §3.1])**.** The tree $\mathscr{C}(\rho)$ is a convex.

Proof. Let $x, x' \in \mathscr{C}(\rho)$ then $\rho(g)\,[x, x']$ is also a segment with extremities x and x' for any $g \in G$. Since there is only one segment with extremities x and x', we have $\rho(g)\,[x, x'] = [x, x']$.

□

Lemma 3.3.4 ([BC3, Lemme 10])**.** The representation ρ is irreducible if and only if the tree $\mathscr{C}(\rho)$ is bounded.

Proof. We may assume K is complete by Proposition 2.1.6. Assume $\mathscr{C}(\rho)$ is unbounded. Since $\mathscr{C}(\rho)$ is a convex it contains a half-line L_x with origin $x = [T]$. Then there a sequence of points $\{\,[T_n]\,\}_{n \geq 1}$ such that $\varpi^n T \subset T_n \subset T$ and $T/T_n \cong A/\varpi^n A$ as an A-module. Under the assumption that K is complete, we have that $\cap_{n=0}^{\infty} T_n$ is a free A-submodule of T of rank 1 and $\cap_{n=0}^{\infty} T_n$ is stable by G. Hence ρ is reducible.

Assume ρ is reducible. There exists a K-subspace W of dimension 1. Let us take an element $x = [T] \in \mathscr{C}(\rho)$ and we denote by $H = T \cap W$. Then H is an A-submodule of rank 1 and H is a direct summand of T. Then there exists a half line L_x in $\mathscr{C}(\rho)$ by Definition 3.2.9. This implies $\mathscr{C}(\rho)$ is unbounded.

□

Propostion 3.3.5 ([BC3, Proposition 11-(d)])**.** Let $x = [T]$ be an element of $\mathscr{C}(\rho)$ and we denote by $\overline{\rho}_x$ the mod ϖ representation $\overline{\rho}_T$. Then we have the following statements:

(1) The point x has no neighbor in $\mathscr{C}(\rho)$ if and only if the representation $\overline{\rho}_x$ is irreducible.

(2) The point x has exactly one neighbor in $\mathscr{C}(\rho)$ if and only if the representation $\overline{\rho}_x$ is reducible but indecomposable.

(3) The point $x \in \mathscr{C}(\rho)$, then x has exactly two neighbors in $\mathscr{C}(\rho)$ if and only if the representation $\overline{\rho}_x$ is decomposed into two distinct characters.

Proof. Let $x = [T]$. Since (1) is proved in Proposition 2.3.5 we begin with (2). Assume x has two distinct neighbors $[T_1]$ and $[T_2]$ such that $\varpi T \subset T_i \subset T$ for $i = 1, 2$. Then $T/\varpi T = T_1/\varpi T \oplus T_2/\varpi T$ as $\mathbb{F}[G]$-modules. Then $\overline{\rho}_x$ is decomposable. For the converse assume $T/\varpi T = X_1 \oplus X_2$ as $\mathbb{F}[G]$-modules. We denote by T_i the inverse image of X_i in $T \twoheadrightarrow T/\varpi T$ $(i = 1, 2)$. Then $[T_1]$ and $[T_2]$ are distinct neighbors of $x = [T]$.

Now we prove (3). Assume Assume x has more than two distinct neighbors in $\mathscr{C}(\rho)$. Let T_1, T_2, T_3 be the representatives of three neighbors such that $\varpi T \subset T_i \subset T$ $(i = 1, 2, 3)$. Then we have

$$\begin{aligned} T/\varpi T &= T_1/\varpi T \oplus T_2/\varpi T \\ &= T_2/\varpi T \oplus T_3/\varpi T \\ &= T_1/\varpi T \oplus T_3/\varpi T \end{aligned}$$

as $\mathbb{F}[G]$-modules. Since the Jordan-Hölder components of $T/\varpi T$ is unique up to $\mathbb{F}[G]$-isomorphism there exist $i, j \in \{1, 2, 3\}$ such that $i \neq j, T/\varpi T = T_i/\varpi T \oplus T_j/\varpi T$ and $T_i/\varpi T \cong T_j/\varpi T$ as $\mathbb{F}[G]$-modules. Then we have $\overline{\rho}_x$ is decomposed into two equal characters. Now we assume $\overline{\rho}_x$ is decomposed into two equal characters i.e. $T/\varpi T = X_1 \oplus X_2$ such that $X_1 \cong X_2$ as $\mathbb{F}[G]$-modules. We denote by T_i the inverse image of X_i in $T \twoheadrightarrow T/\varpi T$ and by $X_i = \mathbb{F}v_i (i = 1, 2)$. Since $X_1 \cong X_2$, $X_3 := \mathbb{F}(v_1 + v_2)$ is also a G-stable $\mathbb{F}$-vector subspace of $T/\varpi T$. We denote by T_3 the inverse image of X_3 in $T \twoheadrightarrow T/\varpi T$. Then $[T_3]$ is a also a neighbor of x which is distinct from $[T_1]$ and $[T_2]$. Thus x has more than two distinct neighbors in $\mathscr{C}(\rho)$.

□

Under above preparations we are ready to prove Ribet's lemma.

Proof of Proposition 3.3.1. We have that $\mathscr{C}(\rho)$ is a convex and bounded by Lemma 3.3.3 and Lemma 3.3.4 respectively. Thus there exists a point $x \in \mathscr{C}(\rho)$ such that x has exactly one neighbor. This implies that $\overline{\rho}_x$ is decomposable but not semi-simple by (2) of Proposition 3.3.5. This completes the proof if we assume $\vartheta_1 = \vartheta_2$. Now we assume $\vartheta_1 \neq \vartheta_2$. Then every point of $\mathscr{C}(\rho)$ has at most two neighbors by (3) of Proposition 3.3.5. Since $\mathscr{C}(\rho)$ is bounded and convex, we have that $\mathscr{C}(\rho)$ a segment. Let x and x' be the extremities of $\mathscr{C}(\rho)$. Then one of $\{\overline{\rho}_x, \overline{\rho}_{x'}\}$ is of the form $\begin{pmatrix} \vartheta_1 & * \\ 0 & \vartheta_2 \end{pmatrix}$ the other is $\begin{pmatrix} \vartheta_2 & * \\ 0 & \vartheta_1 \end{pmatrix}$ and both of them are not semi-simple. This completes the proof of Proposition 3.3.1.

Chapter 4

Kubota-Leopoldt p-adic L-function and Iwasawa main conjecture

In this section, we introduce the Iwasawa theory for ideal class groups. For more details on this theory, the reader can refer to [Iw1], [Iw2], [MW1], [Oc2] and [Wi2].

4.1 Iwasawa-Serre isomorphism

Let Γ be a multiplicative topological group which is isomorphic to $1+p\mathbb{Z}_p$ and γ a fixed topological generator of Γ. Let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbb{Q}_p$. Then we have the following theorem:

Theorem 4.1.1 (Iwasawa-Serre isomorphism)**.** Let the notations be the same as above. Then we have the following isomorphism of $\mathcal{O}$-algebras:

$$\mathcal{O}[[\Gamma]] \xrightarrow{\sim} \Lambda_{\mathcal{O}}, \gamma \mapsto 1+X.$$

Proof. Let $\Gamma_n = \Gamma/\Gamma^{p^n}$ for any $n \in \mathbb{Z}_{\geq 1}$. Then Γ_n is cyclic of order p^n, generated by $\gamma \bmod \Gamma^{p^n}$. We denote by $\omega_n(X) = (1+X)^{p^n} - 1$ for any $n \in \mathbb{Z}_{\geq 1}$. Then we have the following isomorphism:

$$\mathcal{O}[\Gamma_n] \xrightarrow{\sim} \mathcal{O}[X]/(\omega_n(X))$$

$$\gamma \bmod \Gamma^{p^n} \mapsto 1+X \bmod (\omega_n(X))$$

and the following commutative diagram:

$$\begin{array}{ccc} \mathcal{O}[\Gamma_m] & \longrightarrow & \mathcal{O}[X]/(\omega_m(X)) \\ \downarrow & & \downarrow \\ \mathcal{O}[\Gamma_n] & \longrightarrow & \mathcal{O}[X]/(\omega_n(X)) \end{array}$$

for $m \geq n$. We finish the proof by the following lemma.

□

Lemma 4.1.2. Let the notations be the same as the beginning of this section, then we have the following isomorphism:

$$\Lambda_{\mathcal{O}} \xrightarrow{\sim} \varprojlim_{n} \mathcal{O}[X]/\left(\omega_n\left(X\right)\right).$$

Proof. Let ϖ be a fixed uniformizer of $\mathcal{O}$. Since $\mathcal{O} = \varprojlim_{m} \mathcal{O}/\left(\varpi\right)^m$, we have

$$\varprojlim_{n} \mathcal{O}[X]/\left(\omega_n\left(X\right)\right) = \varprojlim_{m,n} \mathcal{O}[X]/\left(\varpi^m, \omega_n\left(X\right)\right). \tag{4.1}$$

On the other hand, we also have the following equality:

$$\Lambda_{\mathcal{O}} = \varprojlim_{n'} \mathcal{O}[X]/(X^{n'}) = \varprojlim_{m',n'} \mathcal{O}[X]/(\varpi^{m'}, X^{n'}). \tag{4.2}$$

Let us admit the following claim for a while.

Claim 1. (1) When we fix m and n, there exist integers m_0' and n_0' such that $(\varpi^{m'}, X^{n'}) \subset (\varpi^m, \omega_n\left(X\right))$ for any $m' \geq m_0'$ $n' \geq n_0'$.

(2) When we fix m' and n', there exist integers m_0 and n_0 such that $(\varpi^m, \omega_n\left(X\right)) \subset (\varpi^{m'}, X^{n'})$ for any $m \geq m_0$, $n \geq n_0$.

Thus $\varprojlim_{m,n} \mathcal{O}[X]/\left(\varpi^m, \omega_n\left(X\right)\right)$ is isomorphic to $\varprojlim_{m',n'} \mathcal{O}[X]/(\varpi^{m'}, X^{n'})$ by the following claim. Combine the equalities (4.1) and (4.2), we finish the proof of Lemma 5.4.10.

We will show Claim 1 in the rest of the proof. We denote by e the ramification index of K over $\mathbb{Q}_p$ i.e. $\left(\varpi\right)^e = (p)$. First let us fix the integers fix m and n. Let $r = \max\{m, n\}$, $n_0' = p^r$ and $m_0' = m$. Then $\omega_r\left(X\right) \in \left(\omega_n\left(X\right)\right)$. Since $\omega_r\left(X\right) = X^{p^r} + p^r \cdot f\left(X\right)$ with $f\left(X\right) \in \Lambda_{\mathcal{O}}$, we have $X^{p^r} \in \left(\omega_r\left(X\right), \varpi^{er}\right) \subset \left(\varpi^m, \omega_n\left(X\right)\right)$. Now we fix the integers m' and n'. Let n_0 be a integer such that $en_0 > m'$ and $p^{n_0} > n'$. Then $p^{n_0} \subset (\varpi^{m'})$ and $X^{p^{n_0}} \subset (X^{n'})$. This implies $\omega_{n_0}\left(X\right) \in (\varpi^{m'}, X^{n'})$. We finish the proof of Calin 1 by letting $m_0 = m'$.

□

At the end of this section, we introduce a lemma on the ring $\Lambda_{\mathcal{O}}$ for our later use.

Lemma 4.1.3 ([Hi3, §7.1, Lemma 1])**.** Let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbb{Q}_p$ with ϖ a fixed uniformizer of $\mathcal{O}$. Let $a \in \mathcal{O}^{\times}$ and $b \in (\varpi)$. Then the following ring isomorphism is an isomorphism

$$\Lambda_{\mathcal{O}} \to \Lambda_{\mathcal{O}}, A\left(X\right) \mapsto A\left(aX + b\right).$$

Proof. Let $A\left(X\right) = \sum_{m=0}^{\infty} c_n X^n$. Then we have the following expansion of $A\left(aX + b\right)$:

$$A\left(aX + b\right) = \sum_{m=0}^{\infty} \left(\sum_{n=m}^{\infty} c_n a^m b^{n-m} \binom{n}{m} \right) X^m.$$

Since $b \in (\varpi)$, the coefficient $\sum_{n=m}^{\infty} c_n a^m b^{n-m} \binom{n}{m}$ is p-adically absolutely convergent and hence the map is well-definied. The inverse map is given by sending $A\left(X\right)$ to $A\left(a^{-1}X - a^{-1}b\right)$.

□

4.2 Iwasawa's construction of Kubota-Leopoldt p-adic L-function

Let ψ be an arbitrary Dirichlet character. Kubota-Leopoldt (see [Iw2, §3, Theorem 2]) showed that there exists a p-adic continuous function $L_p(s,\psi)$ for $s \in \mathbb{Z}_p - \{1\}$ (also continuous at $s=1$ if ψ is non-trivial) with the following interpolation property for $k \in \mathbb{Z}_{\geq 1}$:

$$L_p(1-k,\psi) = (1-\psi\omega^{-k}(p)p^{k-1})L(1-k,\psi\omega^{-k}),$$

where $L(s,\psi\omega^{-k})$ is the Dirichlet L-function. In this subsection, we introduce the following theorem of Iwasawa's construction (cf. [Iw1]) of $L_p(s,\psi)$:

Theorem 4.2.1 (Iwasawa)**.** Let χ be a primitive Dirichlet character modulo Np with $(N,p)=1$. Then there exists a unique power series $\mathcal{L}_p(\chi)$ such that

$$\varphi(\mathcal{L}_p(\chi)) = \begin{cases} L_p(1-k_\varphi, \chi\psi_\varphi\omega) & (\chi \neq \omega^{-1}) \\ \left(\psi_\varphi(u)\,u^{k_\varphi}-1\right)L_p(1-k_\varphi,\psi_\varphi) & (\chi=\omega^{-1}) \end{cases}$$

for any arithmetic specialization $\varphi \in \mathfrak{X}_{\mathrm{arith}}(\Lambda_\chi)$.

Let K be a finite extension of $\mathbb{Q}_p$ such that K contains the field $\mathbb{Q}_p(\chi)$. We denote by $\mathcal{O}$ the ring of integers of K. We denote by $\Gamma = 1+p\mathbb{Z}_p$ and by $\Gamma_n = {1+p\mathbb{Z}_p}\Big/{1+p^{n+1}\mathbb{Z}_p}$ for any $n \in \mathbb{Z}_{\geq 1}$. For any $a \in \mathbb{Z}$ with $(a,Np)=1$, we denote by $\gamma_n(a)$ the image of a mod Np in Γ_n under the following isomorphism:

$$\left(\mathbb{Z}/Np^{n+1}\mathbb{Z}\right)^\times \xrightarrow{\sim} \Gamma_n \times \left(\mathbb{Z}/Np\mathbb{Z}\right)^\times.$$

We denote by $\xi_n(\chi) \in K[\Gamma_n]$ as follows:

$$\xi_n(\chi) = \frac{1}{Np^{n+1}} \sum_{\substack{0\leq a<Np^{n+1} \\ (a,Np)=1}} a\chi(a)\,\gamma_n(a).$$

Lemma 4.2.2. For $m \geq n \geq 1$, $\xi_m(\chi)$ maps to $\xi_n(\chi)$ under the projection map $K[\Gamma_m] \twoheadrightarrow K[\Gamma_n]$.

Proof. It is sufficient to show $\xi_{n+1}(\chi)$ maps to $\xi_n(\chi)$. Recall that

$$\xi_{n+1}(\chi) = \frac{1}{Np^{n+2}} \sum_{\substack{0\leq a<Np^{n+2} \\ (a,Np)=1}} a\chi(a)\,\gamma_{n+1}(a).$$

For any $0 \leq a < Np^{n+1}$, note that the set $\left\{a+kNp^{n+1}\right\}_{0\leq k\leq p-1}$ maps to $\{a\}$ under the map $\left(\mathbb{Z}/Np^{n+2}\right)^\times \twoheadrightarrow \left(\mathbb{Z}/Np^{n+1}\right)^\times$, then the image of $\xi_{n+1}(\chi)$ under $K[\Gamma_{n+1}] \twoheadrightarrow K[\Gamma_n]$ is

$$\frac{p}{Np^{n+2}} \sum_{\substack{0\leq a<Np^{n+1} \\ (a,Np)=1}} a\chi(a)\,\gamma_n(a) = \xi_n(\chi).$$

□

We fix an integer $c \neq \pm 1$ such that $(c,Np)=1$. For any $n \in \mathbb{Z}_{\geq 1}$, we denote by $\eta_n(\chi)$ as follows:

$$\eta_n(\chi) = (1-c\chi(c)\,\gamma_n(c))\,\xi_n(\chi).$$

For any $a \in \mathbb{Z}$, we denote by $a_n \in [0, Np^{n+1})$ the unique integer such that $a_n \equiv ac \pmod{Np^{n+1}}$ and let $r_n(a)$ be the integer such that

$$a_n = ac + r_n(a) Np^{n+1}. \tag{4.3}$$

Lemma 4.2.3. We have the following equalities:

$$\eta_n(\chi) = \chi(c)\gamma_n(c) \sum_{\substack{0 \le a < Np^{n+1} \\ (a,Np)=1}} r_n(a)\chi(a)\gamma_n(a) \tag{4.4}$$

for all $n \geq 1$.

Proof. Since we have $\chi(a_n) = \chi(ac)$ and $\gamma_n(a_n) = \gamma_n(ac)$,

$$\begin{aligned}
\eta_n(\chi) &= \frac{1}{Np^{n+1}} \sum_{\substack{0 \le a < Np^{n+1} \\ (a,Np)=1}} a\chi(a)\gamma_n(a) - \frac{1}{Np^{n+1}} \sum_{\substack{0 \le a < Np^{n+1} \\ (a,Np)=1}} (ac)\chi(ac)\gamma_n(ac) \\
&= \frac{1}{Np^{n+1}} \sum_{\substack{0 \le a < Np^{n+1} \\ (a,Np)=1}} a\chi(a)\gamma_n(a) - \frac{1}{Np^{n+1}} \sum_{\substack{0 \le a < Np^{n+1} \\ (a,Np)=1}} \left(a_n - r_n(a) Np^{n+1}\right)\chi(a_n)\gamma_n(a_n).
\end{aligned}$$

Note that the map $\left(\mathbb{Z}/Np^{n+1}\mathbb{Z}\right)^\times \xrightarrow{\times c} \left(\mathbb{Z}/Np^{n+1}\mathbb{Z}\right)^\times$ is bijective. Then the above equalities becomes to

$$\begin{aligned}
\eta_n(\chi) &= \sum_{\substack{0 \le a < Np^{n+1} \\ (a,Np)=1}} r_n(a)\chi(a_n)\gamma_n(a_n) \\
&= \chi(c)\gamma_n(c) \sum_{\substack{0 \le a < Np^{n+1} \\ (a,Np)=1}} r_n(a)\chi(a)\gamma_n(a).
\end{aligned}$$

□

We have $\eta_n(\chi) \in \mathcal{O}[\Gamma_n]$ for all $n \geq 1$ by Lemma 4.2.3. Furthermore, since $\eta_m(\chi)$ maps to $\eta_n(\chi)$ under $\mathcal{O}[\Gamma_m] \twoheadrightarrow \mathcal{O}[\Gamma_n]$ for all $m \geq n$. Therefore we can define an element $\eta(\chi) \in \mathcal{O}[[\Gamma]]$ which is the limit of $\eta_n(\chi)$

For any $n, k \in \mathbb{Z}_{\geq 1}$, we denote by $\upsilon_{k,n}$ the homomorphism of $\mathcal{O}$-algebras as follows:

$$\upsilon_{k,n} : \mathcal{O}[\Gamma_n] \to \mathcal{O}/Np^{n+1}\mathcal{O}, \gamma_n(a) \mapsto \langle a \rangle^{k-1} \bmod Np^{n+1}\mathcal{O}. \tag{4.5}$$

By Lemma 4.2.3, we have the following equalities:

$$\upsilon_{k,n}(\eta_n(\chi)) = \chi\omega^{1-k}(c) \sum_{\substack{0 \le a < Np^{n+1} \\ (a,Np)=1}} r_n(a)\chi\omega^{1-k}(a) a^{k-1}c^{k-1} \bmod Np^{n+1}\mathcal{O}. \tag{4.6}$$

Lemma 4.2.4. We have the following equality:

$$k \cdot \upsilon_{k,n}(\eta_n(\chi)) = \left(\chi\omega^{1-k}(c)\, c^k - 1\right) \frac{-1}{Np^{n+1}} \sum_{\substack{0 \le a < Np^{n+1} \\ (a,Np)=1}} \chi\omega^{1-k}(a)\, a^k \bmod Np^{n+1}\mathcal{O}. \tag{4.7}$$

Proof. By the equality (4.3) we have

$$a_n^k \equiv a^k c^k + k a^{k-1} c^{k-1} r_n(a) N p^{n+1} \bmod \left(N p^{n+1}\right)^2.$$

By multiplying $\chi\omega^{1-k}(a)$ to both sides of the congruence above, we have

$$\chi\omega^{1-k}(a) a_n^k \equiv \chi\omega^{1-k}(a) a^k c^k + \chi\omega^{1-k}(a) k a^{k-1} c^{k-1} r_n(a) N p^{n+1} \bmod \left(N p^{n+1}\right)^2. \tag{4.8}$$

On the other hand by the equality (4.6), we have

$$k \cdot \upsilon_{k,n}(\eta_n(\chi)) = \chi\omega^{1-k}(c) \sum_{\substack{0 \le a < N p^{n+1} \\ (a, Np)=1}} \chi\omega^{1-k}(a) k a^{k-1} c^{k-1} r_n(a) \bmod N p^{n+1}\mathcal{O}. \tag{4.9}$$

Combine the equality (4.8) and (4.9), we have

$$\begin{aligned} k \cdot \upsilon_{k,n}(\eta_n(\chi)) &= \chi\omega^{1-k}(c) \sum_{\substack{0 \le a < N p^{n+1} \\ (a, Np)=1}} \frac{\chi\omega^{1-k}(a) a_n^k - \chi\omega^{1-k}(a) a^k c^k}{N p^{n+1}} \bmod N p^{n+1}\mathcal{O} \\ &= \frac{1}{N p^{n+1}} \left(\sum_{\substack{0 \le a < N p^{n+1} \\ (a, Np)=1}} \chi\omega^{1-k}(ac) a_n^k - \chi\omega^{1-k}(c) c^k \sum_{\substack{0 \le a < N p^{n+1} \\ (a, Np)=1}} \chi\omega^{1-k}(a) a^k \right) \\ &\quad \bmod N p^{n+1}\mathcal{O}. \end{aligned}$$

Using the equalities $\chi\omega^{1-k}(ac) = \chi\omega^{1-k}(a_n)$ and $\sum_{\substack{0 \le a < N p^{n+1} \\ (a, Np)=1}} \chi\omega^{1-k}(a_n) a_n^k = \sum_{\substack{0 \le a < N p^{n+1} \\ (a, Np)=1}} \chi\omega^{1-k}(a) a^k$, we have

$$k \cdot \upsilon_{k,n}(\eta_n(\chi)) = \left(1 - \chi\omega^{1-k}(c) c^k\right) \frac{1}{N p^{n+1}} \sum_{\substack{0 \le a < N p^{n+1} \\ (a, Np)=1}} \chi\omega^{1-k}(a) a^k \bmod N p^{n+1}\mathcal{O}.$$

□

Lemma 4.2.5. We have the following equality

$$\lim_{n \to \infty} \frac{-1}{N p^{n+1}} \sum_{\substack{0 \le a < N p^{n+1} \\ (a, Np)=1}} \chi\omega^{1-k}(a) a^k = \left(1 - \chi\omega^{1-k}(p) p^{k-1}\right) L\left(1-k, \chi\omega^{1-k}\right).$$

Proof. Let us consider an integer a such that $0 \le a < N p^{n+1}$ and $(a, N) > 1$. Since the conductor of χ is Np with $(N, p) = 1$ and the conductor of ω is p, we must have the integer a is not prime to the conductor of $\chi\omega^{1-k}$ and hence $\chi\omega^{1-k}(a) = 0$. Thus

$$\begin{aligned} \frac{1}{N p^{n+1}} \sum_{\substack{0 \le a < N p^{n+1} \\ (a, Np)=1}} \chi\omega^{1-k}(a) a^k &= \frac{1}{N p^{n+1}} \sum_{0 \le a < N p^{n+1}} \chi\omega^{1-k}(a) a^k - \frac{1}{N p^{n+1}} \sum_{\substack{0 \le a < N p^{n+1} \\ (a, p) > 1}} \chi\omega^{1-k}(a) a^k \\ &= \frac{1}{N p^{n+1}} \sum_{0 \le a < N p^{n+1}} \chi\omega^{1-k}(a) a^k - \frac{1}{N p^{n+1}} \chi\omega^{1-k}(p) p^k \sum_{0 \le a < N p^n} \chi\omega^{1-k}(a) a^k \\ &= \frac{1}{N p^{n+1}} \sum_{0 \le a < N p^{n+1}} \chi\omega^{1-k}(a) a^k - \frac{1}{N p^n} \chi\omega^{1-k}(p) p^{k-1} \sum_{0 \le a < N p^n} \chi\omega^{1-k}(a) a^k. \end{aligned}$$

By [Iw2, §2.3, Lemma 1] and [Iw2, §2.2, Theorem 1], we have

$$\lim_{n\to\infty}\frac{1}{Np^{n+1}}\sum_{0\le a<Np^{n+1}}\chi\omega^{1-k}(a)\,a^k=-k\cdot L\left(1-k,\chi\omega^{1-k}\right).$$

This completes the proof of Lemma 4.2.5.

□

Under the above preparation, we are ready to prove Theorem 4.2.1.

Proof of Theorem 4.2.1. Note that the limit of $\upsilon_{k,n}$ for $n\to\infty$, defines a continuous homomorphism of $\mathcal{O}$-algebras as follows:

$$\upsilon_k:\mathcal{O}[[\Gamma]]\to\mathcal{O},\gamma(a)\mapsto\langle a\rangle^{k-1} \tag{4.10}$$

for every $(a,Np)=1$. Let d be element in $\mathbb{Z}_p$ such that $\langle c\rangle=u^d$. Combine Lemma 4.2.4 and Lemma 4.2.5, we have

$$\upsilon_k(\eta(\chi))=\left(\chi\omega(c)\,u^{kd}-1\right)L_p(1-k,\chi\omega) \tag{4.11}$$

for all $k\in\mathbb{Z}_{\geq 1}$. On the other hand, we have the following isomorphism

$$\mathcal{O}[[\Gamma]]\xrightarrow{\sim}\Lambda_{\mathcal{O}},u\mapsto u(1+X) \tag{4.12}$$

of $\mathcal{O}$-algebras by Theorem 4.1.1.

- If $\chi=\omega^{-1}$. Choose $c=u$ and we denote by $\mathcal{L}_p(\chi)$ the element in $\Lambda_{\mathcal{O}}$ corresponding to $\eta(\chi)$ under (4.12).
- If $\chi\neq\omega^{-1}$. We denote by $\mathcal{Q}(\chi)$ the element in $\Lambda_{\mathcal{O}}$ corresponding to $\eta(\chi)$ under (4.12) and by $\mathcal{U}(\chi)=\chi\omega(c)\,u^{2d}(1+X)^d-1$. Choose an element c such that $\mathcal{U}(\chi)$ is a unit in $\Lambda_{\mathcal{O}}$ and we denote by $\mathcal{L}_p(\chi)=\dfrac{\mathcal{Q}(\chi)}{\mathcal{U}(\chi)}$.

Since the equality (4.11) holds for infinitely many $u^k-1\in p\mathbb{Z}_p$, $\mathcal{L}_p(\chi)$ is unique. This completes the proof of Theorem 4.2.1.

At the end of this section, we introduce the following theorem for later use:

Theorem 4.2.6 (Ferrero-Washington [FW])**.** Let us keep the assumptions and the notations of Theorem 4.2.1. Then the element $\mathcal{L}_p(\chi)$ is not divisible by ϖ, where ϖ is a uniformizer of $\mathbb{Z}_p[\chi]$.

4.3 The main conjecture of ideal class groups

First we recall some properties of Fitting ideals and characteristic ideals to obtain the Mazur-Wiles' theorem (the Iwasawa main conjecture for ideal class groups). The reader can refer to [No], [Nu] and [OS, Appendix] for more details.

Let R be a Noetherian integrally closed domain and M a finitely generated R-module. Let $\mathbf{v}=\{v_1,\cdots,v_r\}$ be a set of generators of M. We say that an element $(a_1,\cdots,a_r)\subset R^r$ is a relation for $\{v_1,\cdots,v_r\}$ if $a_1v_1+\cdots+a_rv_r=0$. Let $\mathrm{Fitt}_R(M)$ be the ideal of R which is generated by $\det A$ for all $r\times r$ matrix satisfying the following condition:

($\mathrm{Rel}_{\mathbf{v}}$) Every rows of A is a relation of $\{ v_1, \cdots, v_r \}$.

It may be shown that $\mathrm{Fitt}_R(M)$ is independent of the choices of the generators of M (cf. [Nu, Proposition 3]), hence depends only on M. We call $\mathrm{Fitt}_R(M)$ the R-Fitting ideal of M.

Assume M is R-torsion, we define the characteristic ideal $\mathrm{char}_R(M) \subset R$ of M as follows:

$$\mathrm{char}_R(M) \{ a \in R \mid \mathrm{ord}_P(a) \geq \mathrm{length}_{R_P} M_P, \text{for all height one prime ideal of } R \},$$

where $\mathrm{length}_{R_P} M_P$ is the length of the R_P-module M_P. We define $\mathrm{char}_R(M) = (0)$ if M is R-torsion free.

We have the following properties for Fitting ideal and characteristic ideal:

Propostion 4.3.1. Let R be a Noetherian integrally closed domain. Then we have the following statements:

(1) Let $M \twoheadrightarrow M'$ be a surjective homomorphism of finitely generated R-modules. Then we have $\mathrm{Fitt}_R(M) \subset \mathrm{Fitt}_R(M')$ ([Nu, Lemma 5]).

(2) Let R' be a Noetherian R-algebra and M be a finitely generated R-module. Then we have $\mathrm{Fitt}_{R'}(M \otimes_R R') = \mathrm{Fitt}_R(M) R'$ ([OS, Proposition A.2]).

(3) Let I be an ideal of R and M a faithful R-module. Then we have Then we have $\mathrm{Fitt}_R(M/IM) \subset I$ ([Nu, Corollary 14]).

(4) Assume R is a unique factorization domain and let M be a finitely generated R-module. Then we have $\mathrm{Fitt}_R(M) \subset \mathrm{char}_R(M)$ ([OS, Proposition A.6]).

Now we recall the Theorem of Mazur and Wiles at the end of this section. Let ψ be a Dirichlet character. We assume the conductor of ψ is Np with $(N, p) = 1$. Let L_∞ be the maximal unramified abelian p-extension of $\mathbb{Q}(\mu_{Np^\infty})$ and $X_\infty = \mathrm{Gal}(L_\infty / \mathbb{Q}(\mu_{Np^\infty}))$. Then X_∞^ψ is a $\mathbb{Z}_p[\psi][[\mathrm{Gal}(\mathbb{Q}(\mu_{Np}) / \mathbb{Q}(\mu_{Np^\infty}))]] \cong \mathbb{Z}_p[\psi][[1 + p\mathbb{Z}_p]]$-module. The following map

$$\mathbb{Z}_p[\psi][[\mathrm{Gal}(\mathbb{Q}(\mu_{Np^\infty}) / \mathbb{Q}(\mu_{Np}))]] \to \Lambda_\psi, \tilde{\gamma} \mapsto u^{-1}(1+X)^{-1}$$

is an isomorphism by Theorem 4.1.1 . We fix this isomorphism to the end this section and we consider X_∞^ψ as a Λ_ψ-module.

Theorem 4.3.2 (Iwasawa [Iw3])**.** Let the assumptions and the notations be as above. Then X_∞^ψ is a finitely generated torsion Λ_ψ-module.

The Iwasawa main conjecture for ideal class group claims that the characteristic ideal of X_∞^ψ is generated by Kubota-Leopoldt p-adic L-function as follows:

Conjecture 4.3.3 (Iwasawa main conjecture)**.** Let the assumptions and the notations be as above. Then we have the following equality:

$$\mathrm{char}_{\Lambda_\psi}(X_\infty^\psi) = \left(\mathcal{L}_p\left(\psi^{-1}\right)\right).$$

Conjecture 4.3.3 is proved by Mazur-Wiles [MW1] for $\mathbb{Q}$ and Wiles [Wi2] for totally real fields:

Theorem 4.3.4 (Mazur-Wiles [Wi2, Theorem 1.2])**.** Let the assumptions and the notations be as above. Then we have the following equalities:

$$\mathrm{char}_{\Lambda_\psi}(X_\infty^\psi) = \mathrm{Fitt}_{\Lambda_\psi}(X_\infty^\psi) = \left(\mathcal{L}_p\left(\psi^{-1}\right)\right)$$

i.e. Conjecture 4.3.3 is true.

Let us give some remarks on the proof of Mazur-Wiles. To prove Conjecture 4.3.3, it is sufficient to prove either $\left(\mathcal{L}_p\left(\psi^{-1}\right)\right) \subset \mathrm{char}_{\Lambda_\psi}(X_\infty^\psi)$ or $\mathrm{char}_{\Lambda_\psi}(X_\infty^\psi) \subset \left(\mathcal{L}_p\left(\psi^{-1}\right)\right)$ by the analytic class number formula. Mazur-Wiles proved that $\left(\mathcal{L}_p\left(\psi^{-1}\right)\right) \subset \mathrm{Fitt}_{\Lambda_\psi}(X_\infty^\psi)$. Hence Theorem 4.3.4 follows by (4) of Proposition 4.3.1.

Chapter 5

Hida deformation

In this chapter, we review some fundamental results on Hida theory. For more details on this theory, the reader can refer to Chapter 7 of [Hi3].

5.1 The ordinary part of the space of modular forms

In this section, we construct the ordinary part of the space of modular forms.

Lemma 5.1.1. [Hi3, §7.2, Lemma 1] Let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbb{Q}_p$. For the pair $(\mathcal{M}, h)$ such that $\mathcal{M}$ is a finitely generated free $\mathcal{O}$-module and h is an element of $\mathrm{End}_{\mathcal{O}}(\mathcal{M})$, we have the following statements:

(1) The limit $\lim_{n\to\infty} h^{n!}(x)$ converges in $\mathcal{M}$ for any $x \in \mathcal{M}$ and $\lim_{n\to\infty} h^{n!}$ is an idempotent of $\mathrm{End}_{\mathcal{O}}(\mathcal{M})$.

(2) For an element $x \in \mathcal{M}$ such that there exists an element $\alpha \in \mathcal{O}$ such that $h(x) = \alpha x$, we have the following equality:

$$\lim_{n\to\infty} h(x)^{n!} = \begin{cases} x & (\alpha \in \mathcal{O}^{\times}) \\ 0 & (\alpha \notin \mathcal{O}^{\times}). \end{cases}$$

Proof. Let d be the rank of the $\mathcal{O}$-module $\mathcal{M}$ and $\{a_1, \cdots, a_d\}$ the set of all eigenvalues of h. We may enlarge $\mathcal{O}$ such that $\mathcal{O}$ contains $\{a_1, \cdots, a_d\}$. Since $\mathcal{O}$ is a discrete valuation ring, there exists a basis of $\mathcal{M}$ such that $h = A + B$ where

$$A = \begin{pmatrix} a_1 & & & & 0 \\ & a_2 & & & \\ & & \ddots & & \\ & & & \ddots & \\ 0 & & & & a_d \end{pmatrix}, B = \begin{pmatrix} 0 & & & & \\ & 0 & & & * \\ & & \ddots & & \\ & & & \ddots & \\ 0 & & & & 0 \end{pmatrix}$$

and B is a nilpotent element. Since $\mathcal{O}^{\times} \xrightarrow{\sim} \mathcal{O}/(\varpi) \times (1+\varpi\mathcal{O})$ and $\mathcal{O}/(\varpi)$ is finite, we have the following equality for every eigenvalue a_i:

$$\lim_{n\to\infty} a_i^{n!} = \begin{cases} 1 & (a_i \in \mathcal{O}^{\times}) \\ 0 & (a_i \notin \mathcal{O}^{\times}). \end{cases} \tag{5.1}$$

Combine the equality (5.1) and the equality $h^{n!} = (A+B)^{n!} = A^{n!} + n!A^{n!-1}B + \cdots$, We have the following equality:

$$\lim_{n\to\infty} h^{n!} = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & 0 \\ & & 1 & & & \\ & & & 0 & & \\ & & & & \ddots & \\ 0 & & & & & 0 \end{pmatrix}$$

after change the order of $a_1, \cdots, a_d$. This completes the proof of Lemma 5.1.1

□

We apply Lemma 5.1 to the pair $(T(p), M_k(\Gamma_0(M), \psi, \mathcal{O}))$. Define

$$e := \lim_{n\to\infty} T(p)^{n!}$$

and

$$M_k^{\mathrm{ord}}(\Gamma_0(M), \psi, \mathcal{O}) := eM_k^{\mathrm{ord}}(\Gamma_0(M), \psi, \mathcal{O}).$$

We also define $S_k^{\mathrm{ord}}(\Gamma_0(M), \psi, \mathcal{O}) := eS_k^{\mathrm{ord}}(\Gamma_0(M), \psi, \mathcal{O})$ in the same way. We call an element $f \in M_k^{\mathrm{ord}}(\Gamma_0(M), \psi, \mathcal{O})$ (resp. $f \in S_k^{\mathrm{ord}}(\Gamma_0(M), \psi, \mathcal{O})$) a p-ordinary modular form (resp. p-ordinary cusp form). By (2) of Lemma 5.1, we have the following corollary:

Corollary 5.1.2. Let $f \in M_k^{\mathrm{ord}}(\Gamma_0(M), \psi, \mathcal{O})$ be a normalized Hecke eigen form. Then f is p-ordinary if and only if the p-th Fourier coefficient $a(p, f)$ of f is a p-adic unit.

5.2 $\mathbb{I}$-adic forms

Let N be a positive integer which is prime to p and χ a Dirichlet character modulo Np throughout this chapter. Recall that $\mathbb{I}$ is an integrally closed local domain which is finite flat over Λ_{χ}. We refer to the notations of the arithmetic specialization.

Definition 5.2.1. We call $\mathcal{F} = \sum_{n=0}^{\infty} a(n, \mathcal{F}) q^n \in \mathbb{I}[[q]]$ an $\mathbb{I}$-adic modular form (resp. $\mathbb{I}$-adic cusp form) with Dirichlet character χ if for each $\varphi \in \mathfrak{X}_{\mathrm{arith}}(\mathbb{I})$,

$$f_{\varphi} := \sum_{n=0}^{\infty} \varphi(a(n, \mathcal{F})) q^n \in M_{k_{\varphi}}^{\mathrm{ord}}\left(\Gamma_0\left(Np^{r_{\varphi}+1}\right), \chi\psi_{\varphi}\omega^{1-k_{\varphi}}, \varphi(\mathbb{I})\right)$$

(resp. $f_{\varphi} \in S_{k_{\varphi}}^{\mathrm{ord}}\left(\Gamma_0\left(Np^{r_{\varphi}+1}\right), \chi\psi_{\varphi}\omega^{1-k}, \varphi(\mathbb{I})\right)$) is the q-expansion of a p-ordinary modular form (resp. p-ordinary cusp form).

We denote by $M^{\mathrm{ord}}(\chi,\mathbb{I})$ (resp. $S^{\mathrm{ord}}(\chi,\mathbb{I})$) the $\mathbb{I}$-module of all $\mathbb{I}$-adic modular forms (resp. $\mathbb{I}$-adic cusp forms) with Dirichlet character χ.

Example 5.2.2 (Λ_χ-adic Eisenstein series)**.** First we define the p-stabilization of the Eisenstein series $E_{k,\psi}(z)$ (cf. Example 2.5.2) as follows :

$$\begin{aligned} E_{k,\psi}^{(p)}(z) &= E_{k,\psi}(z) - \psi(p)\, p^{k-1} E_{k,\psi}(pz) \\ &= \frac{\left(1-\psi(p)\, p^{k-1}\right) L(1-k,\psi)}{2} + \sum_{n=1}^{\infty} \sigma_{k-1,\psi}^{(p)}(n)\, q^n, \end{aligned}$$

where $\sigma_{k-1,\psi}^{(p)}(n) = \sum_{\substack{d|n \\ (d,p)=1}} \psi(d)\, d^{k-1}$.

We denote by

$$\mathcal{H}(\chi) = \begin{cases} 1 & (\chi \neq \omega^{-1}) \\ \\ u^2(1+X) - 1 & (\chi = \omega^{-1}). \end{cases}$$

and by $\mathcal{E}_\chi = \sum_{n=1}^{\infty} a(n,\mathcal{E}_\chi)\, q^n \in \mathrm{Frac}(\Lambda_\chi)[[q]]$ where

$$a(n,\mathcal{E}_\chi) = \begin{cases} 2^{-1}\mathcal{L}_p(\chi)/\mathcal{H}(\chi) & (n=0) \\ \\ \sum_{\substack{d|n \\ (d,p)=1}} \chi(d)\, u^{s_d} (1+X)^{s_d} & (n>0). \end{cases}$$

Then for any $\varphi \in \mathfrak{X}_{\mathrm{arith}}(\Lambda_\chi)$,

$$\begin{aligned} \varphi(a(n,\mathcal{E}_\chi)) &= \sum_{\substack{d|n \\ (d,p)=1}} \chi(d)\, u^{s_d} \left(\zeta_\varphi u^{k_\varphi - 2}\right)^{s_d} \\ &= \sum_{\substack{d|n \\ (d,p)=1}} \chi(d)\, \frac{d}{\omega(d)} \psi_\varphi(u)^{s_d} \left(\frac{d}{\omega(d)}\right)^{k_\varphi - 2} \\ &= \sum_{\substack{d|n \\ (d,p)=1}} \chi(d)\, \psi_\varphi(d)\, \omega^{1-k_\varphi}(d)\, d^{k_\varphi - 1} \\ &= a\left(n, E_{k_\varphi, \chi\psi_\varphi\omega^{1-k_\varphi}}^{(p)}\right). \end{aligned}$$

Furthermore we have

$$\begin{aligned} \varphi(a(0,\mathcal{E}_\chi)) &= 2^{-1} L_p(1-k_\varphi, \chi\psi_\varphi\omega) \\ &= 2^{-1}\left(1-\chi\psi_\varphi\omega(p)\, p^{k_\varphi - 1}\right) L\left(1-k_\varphi, \chi\psi_\varphi\omega^{1-k_\varphi}\right) \\ &= a\left(0, E_{k_\varphi, \chi\psi_\varphi\omega^{1-k_\varphi}}^{(p)}\right) \end{aligned}$$

by Theorem 4.2.1. If $\chi \neq \omega^{-1}$, we have $\mathcal{E}_\chi$ is a Λ_χ-adic form. When $\chi = \omega^{-1}$, we have $\left(u^2(1+X)-1\right)\mathcal{E}_{\omega^{-1}}$ is a $\Lambda_{\omega^{-1}}$-adic form.

We introduce the following structure theorem of the $\mathbb{I}$-modules $M^{\mathrm{ord}}(\chi,\mathbb{I})$ and $S^{\mathrm{ord}}(\chi,\mathbb{I})$:

Theorem 5.2.3 ([Hi3, §7.3, Theorem 1])**.**

(1) The $\mathbb{I}$-modules $M^{\mathrm{ord}}(\chi,\mathbb{I})$ and $S^{\mathrm{ord}}(\chi,\mathbb{I})$ are finitely generated and torsion-free $\mathbb{I}$.

(2) Assume $\mathbb{I} = \Lambda_{\mathcal{O}}$ where $\mathcal{O}$ is the ring of integers of a finite extension of $\mathbb{Q}_p$, then the $\Lambda_{\mathcal{O}}$-modules $M^{\mathrm{ord}}(\chi,\mathbb{I})$ and $S^{\mathrm{ord}}(\chi,\mathbb{I})$ are also free over $\Lambda_{\mathcal{O}}$.

Proof. Since the proof are the same for $M^{\mathrm{ord}}(\chi,\mathbb{I})$ and $S^{\mathrm{ord}}(\chi,\mathbb{I})$, we prove only for $M^{\mathrm{ord}}(\chi,\mathbb{I})$. By definition, $M^{\mathrm{ord}}(\chi,\mathbb{I})$ is an $\mathbb{I}$-submodule of the ring of power series $\mathbb{I}[[q]]$. Hence $M^{\mathrm{ord}}(\chi,\mathbb{I})$ is $\mathbb{I}$-torsion free.

Let M be an arbitrary finitely generated free $\mathbb{I}$-submodule of $M^{\mathrm{ord}}(\chi,\mathbb{I})$. First we prove that the $\mathbb{I}$-rank of M is bounded. Write $M = \oplus_{j=1}^{r}\mathbb{I}\mathcal{F}_j$. Then there exist integers $n_1,\cdots,n_r \in \mathbb{Z}_{>0}$ such that the determinant of the $r\times r$ matrix $(a(n_i,\mathcal{F}_j))_{1\leq i,j\leq r}$ is non-zero. We denote by $\mathcal{D}$ the above determinant. Notice that $\mathbb{I}$ is isomorphic to $\varprojlim_j I\Big/\cap_{i=1}^{j}\mathcal{P}_i$, where $\{\mathcal{P}_i\}_i$ is a countable collection of height 1 primes of $\mathbb{I}$ by Lemma 5.5.4. Then there exists an element $\varphi \in \mathfrak{X}_{\mathrm{arith}}(\mathbb{I})$ with $\zeta_\varphi = 1$ such that $\varphi(\mathcal{D}) \neq 0$ by the Weierstrass preparation theorem. We denote by $f_{\varphi,j} \in M_{k_\varphi}^{\mathrm{ord}}\left(\Gamma_0(Np),\chi\omega^{1-k_\varphi},\mathcal{O}\right)$ the specialization $\sum_{n=1}^{\infty}\varphi(a(n,\mathcal{F}_j))q^n$ for each j. Then we have $\varphi(\mathcal{D})$ is the determinant of the $r\times r$ matrix $(a(n_i,f_j))_{1\leq i,j\leq r}$. Thus we have the following inclusion:

$$\oplus_{j=1}^{r}\mathcal{O}f_{\varphi,j} \subset M_{k_\varphi}^{\mathrm{ord}}\left(\Gamma_0(Np),\chi\omega^{1-k_\varphi},\mathcal{O}\right).$$

Since the $\mathcal{O}$-rank of $M_{k_\varphi}^{\mathrm{ord}}\left(\Gamma_0(Np),\chi\omega^{1-k_\varphi},\mathcal{O}\right)$ is bounded independently of the integer k_φ by [Hi3, §7.2, Theorem 1], we have $\mathrm{rank}_{\mathbb{I}}M$ is bounded.

Now let r be the maximal number of linearly independent elements of $M^{\mathrm{ord}}(\chi,\mathbb{I})$ and $\{\mathcal{F}_1,\cdots,\mathcal{F}_r\}$ a set consisted by linearly independent elements of $M^{\mathrm{ord}}(\chi,\mathbb{I})$. We denote by $n_1,\cdots,n_r$ and $\mathcal{D}$ the same symbol as above. Then $\{\mathcal{F}_1,\cdots,\mathcal{F}_r\}$ is a basis of $M^{\mathrm{ord}}(\chi,\mathbb{I})\otimes_{\mathbb{I}}\mathrm{Frac}(\mathbb{I})$. Let us take an element $\mathcal{F} \in M^{\mathrm{ord}}(\chi,\mathbb{I})$. Then there exist elements $x_1,\cdots,x_r \in \mathrm{Frac}(\mathbb{I})$ such that $\mathcal{F} = \sum_{j=1}^{r}x_j\mathcal{F}_j$ and hence

$$(a(n_i,\mathcal{F}_j))_{1\leq i,j\leq r}\cdot {}^t(x_1,\cdots,x_r) = (a(n_i,\mathcal{F}))_{1\leq i\leq r}. \tag{5.2}$$

The equality (5.2) implies $\mathcal{D}x_i \in \mathbb{I}$ and hence

$$\mathcal{D}M^{\mathrm{ord}}(\chi,\mathbb{I}) \subset \oplus_{j=1}^{r}\mathbb{I}\mathcal{F}_j.$$

Thus

$$M^{\mathrm{ord}}(\chi,\mathbb{I}) \xrightarrow{\sim} \mathcal{D}M^{\mathrm{ord}}(\chi,\mathbb{I})$$

is a finitely generated $\mathbb{I}$-module.

Now assume $\mathbb{I} = \Lambda_{\mathcal{O}}$ and we prove the freeness of $M^{\mathrm{ord}}(\chi,\Lambda_{\mathcal{O}})$. We fix an integer $k \in \mathbb{Z}_{\geq 2}$ and we denote by $\mathfrak{p}$ the principal ideal generated by $X - \left(u^{k-2}-1\right)$. Let φ be an element of $\mathfrak{X}_{\mathrm{arith}}(\Lambda_{\mathcal{O}})$ such

that $k_\varphi = k$ and $\zeta_\varphi = 1$. Under the assumption that $\mathbb{I} = \Lambda_{\mathcal{O}}$, we have $\mathfrak{p}M^{\mathrm{ord}}(\chi, \Lambda_{\mathcal{O}}) = \mathrm{Ker}\ \varphi$ and hence $M^{\mathrm{ord}}(\chi, \Lambda_{\mathcal{O}})/\mathfrak{p}M^{\mathrm{ord}}(\chi, \Lambda_{\mathcal{O}})$ can be embedded into $M_k^{\mathrm{ord}}\left(\Gamma_0(Np), \chi\omega^{1-k}, \mathcal{O}\right)$. Let us take elements $\mathcal{F}_1, \cdots, \mathcal{F}_r$ of $M^{\mathrm{ord}}(\chi, \Lambda_{\mathcal{O}})$ such that $\{\mathcal{F}_j \bmod \mathfrak{p}M^{\mathrm{ord}}(\chi, \Lambda_{\mathcal{O}})\}$ is an $\mathcal{O}$-basis of $M^{\mathrm{ord}}(\chi, \Lambda_{\mathcal{O}})/\mathfrak{p}M^{\mathrm{ord}}(\chi, \Lambda_{\mathcal{O}})$ and we denote by $M = \oplus_{j=1}^r \Lambda_{\mathcal{O}}\mathcal{F}_j$. By the following commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M & \xrightarrow{\iota} & M^{\mathrm{ord}}(\chi, \Lambda_{\mathcal{O}}) & \longrightarrow & \mathrm{Coker}(\iota) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \times\mathfrak{p}} & & \downarrow{\scriptstyle \times\mathfrak{p}} & & \downarrow{\scriptstyle \times\mathfrak{p}} & & \\
0 & \longrightarrow & M & \xrightarrow{\iota} & M^{\mathrm{ord}}(\chi, \Lambda_{\mathcal{O}}) & \longrightarrow & \mathrm{Coker}(\iota) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & M/\mathfrak{p}M & \xrightarrow{\sim} & M^{\mathrm{ord}}(\chi, \Lambda_{\mathcal{O}})/\mathfrak{p}M^{\mathrm{ord}}(\chi, \Lambda_{\mathcal{O}}) & \longrightarrow & \mathrm{Coker}(\iota)/\mathfrak{p}\mathrm{Coker}(\iota). & &
\end{array}$$

we have $\mathrm{Coker}(\iota)/\mathfrak{p}\mathrm{Coker}(\iota) = 0$. Thus $\mathrm{Coker}(\iota) = 0$ by Nakayama's lemma and $M^{\mathrm{ord}}(\chi, \Lambda_{\mathcal{O}}) = M = \oplus_{j=1}^r \Lambda_{\mathcal{O}}\mathcal{F}_j$. □

We introduce the following control theorem:

Theorem 5.2.4 (Hida [Hi3, §7.3, Theorem 3])**.** Assume $\mathbb{I} = \Lambda_{\mathcal{O}}$, then we have the following equalities:

$$\varphi\left(M^{\mathrm{ord}}(\chi, \mathbb{I})\right) = M_{k_\varphi}^{\mathrm{ord}}\left(\Gamma_0\left(Np^{r_\varphi+1}\right), \chi\psi_\varphi\omega^{1-k_\varphi}, \varphi(\mathbb{I})\right),$$
$$\varphi\left(S^{\mathrm{ord}}(\chi, \mathbb{I})\right) = S_{k_\varphi}^{\mathrm{ord}}\left(\Gamma_0\left(Np^{r_\varphi+1}\right), \chi\psi_\varphi\omega^{1-k_\varphi}, \varphi(\mathbb{I})\right)$$

for any $\varphi \in \mathfrak{X}_{\mathrm{arith}}(\mathbb{I})$.

Proof. Let us fix an element $\varphi \in \mathfrak{X}_{\mathrm{arith}}(\mathbb{I})$ which we denote by φ_0. Let $k_0 = k_{\varphi_0}, \zeta_0 = \zeta_{\varphi_0}, r_0 = r_{\varphi_0}$ and $\psi_0 = \psi_{\varphi_0}$ for simplicity. We have $\varphi_0\left(S^{\mathrm{ord}}(\chi, \mathbb{I})\right) \subset S_{k_0}^{\mathrm{ord}}\left(\Gamma_0\left(Np^{r_0+1}\right), \chi\psi_0\omega^{1-k_0}, \mathcal{O}[\zeta_0]\right)$ by the definition of $\mathbb{I}$-adic cusp form. Let us take an element $f \in S_{k_0}^{\mathrm{ord}}\left(\Gamma_0\left(Np^{r_0+1}\right), \chi\psi_0\omega^{1-k_0}, \mathcal{O}[\zeta_0]\right)$. We may enlarge $\mathbb{I}$ such that $\zeta_0 \in \mathbb{I}$. Write $\mathcal{E}_\chi(X) = \mathcal{E}_\chi$ in Example 5.2.2 and we denote by $\mathcal{H}'(\chi)$ the image of $\mathcal{H}(\chi)$ under the following isomorphism:

$$\mathbb{I} \xrightarrow{\sim} \mathbb{I}, X \mapsto \zeta_0^{-1}u^{-k_0}X + \zeta_0^{-1}u^{-k_0} - 1.$$

Let

$$\mathcal{F} = f \times \mathcal{H}'\left(\omega^{-1}\right) \times \mathcal{E}_{\omega^{-1}}\left(\zeta_0^{-1}u^{-k_0}X + \zeta_0^{-1}u^{-k_0} - 1\right) \times \left\{2^{-1}\log(u)\left(p^{-1}-1\right)\right\}^{-1}.$$

Then for any φ such that $k_\varphi > k_0$ and $r_\varphi > r_0$, we have

$$\begin{aligned}
\varphi(\mathcal{F}) &= f \times \left(\zeta_\varphi\zeta_0^{-1}u^{k_\varphi-k_0-1} - 1\right) \times \mathcal{E}_{\omega^{-1}}\left(\zeta_\varphi\zeta_0^{-1}u^{k_\varphi-k_0-2} - 1\right) \times \left\{2^{-1}\log(u)\left(p^{-1}-1\right)\right\}^{-1} \\
&\in S_{k_0}^{\mathrm{ord}}\left(\Gamma_0\left(Np^{r_0+1}\right), \chi\psi_0\omega^{1-k_0}, \mathcal{O}[\zeta_0]\right) \times M_{k_\varphi-k_0}^{\mathrm{ord}}\left(\Gamma_0\left(p^{r_\varphi+1}\right), \psi_\varphi\psi_0^{-1}\omega^{-k_\varphi+k_0}, \mathcal{O}[\zeta_\varphi]\right) \\
&\subset S_{k_\varphi}^{\mathrm{ord}}\left(\Gamma_0\left(Np^{r_\varphi}\right), \chi\psi_\varphi\omega^{1-k_\varphi}, \mathcal{O}[\zeta_\varphi]\right).
\end{aligned}$$

The above equalities tell us that $\varphi(\mathcal{F})$ is a p-ordinary cusp form for almost all φ, hence $\mathcal{F}$ is a $\mathbb{I}$-adic cusp form by [Wi2, Lemma 3.1]. Furthermore if $\varphi = \varphi_0$, we have the following equality:

$$\varphi_0(\mathcal{F}) = f \times \left\{2^{-1}\log(u)\left(p^{-1}-1\right)\right\}^{-1} \times \left\{2^{-1}\left(u^s-1\right)\zeta_p(1-s)|_{s=0}\right\}.$$

Since $2^{-1}\left(u^s-1\right)\zeta_p(1-s)|_{s=0} = 2^{-1}\log(u)\left(p^{-1}-1\right)$ by [Hi3, §3.5, Theorem 2], we have $\varphi_0(\mathcal{F}) = f$. □

5.3 Duality between $\mathbb{I}$-adic forms and their Hecke algebras

.

We keep our notation as in the previous section. First we define $\mathbb{I}$-adic Hecke operators acting on $M^{\mathrm{ord}}(\chi, \Lambda_\chi)$ and $S^{\mathrm{ord}}(\chi, \Lambda_\chi)$. Let n be a positive integer. We define $T(n)$ the following $\mathbb{I}$-module homomorphism:

$$\mathbb{I}[[q]] \to \mathbb{I}[[q]], \mathcal{F} \mapsto T(n)\mathcal{F} = \sum_{m=0}^{\infty} a(m, T(n)\mathcal{F}) q^n$$

such that

$$a(m, T(n)\mathcal{F}) = \sum_{b|(m,n)} \langle b \rangle (1+X)^{s_b} \chi(b) b^{-1} a\left(\frac{mn}{b^2}, \mathcal{F}\right),$$

with $\chi(l) = 0$ if $(b, Np) > 1$. If $\mathcal{F}$ is an element in $M^{\mathrm{ord}}(\chi, \mathbb{I})$, we have the following equalities:

$$\begin{aligned}
\varphi(a(m, T(n)\mathcal{F})) &= \sum_{b|(m,n)} \zeta_\varphi^{s_b} u^{s_b(k_\varphi - 1)} \chi(b) a\left(\frac{mn}{b^2}, f_\varphi\right) \\
&= \sum_{b|(m,n)} \psi_\varphi(u)^{s_b} \left(\frac{b}{\omega(b)}\right)^{k_\varphi - 1} \chi(b) a\left(\frac{mn}{b^2}, f_\varphi\right) \\
&= \sum_{b|(m,n)} \chi\psi_\varphi\omega^{1-k_\varphi}(b) a\left(\frac{mn}{b^2}, f_\varphi\right) \\
&= a(m, T(n) f_\varphi).
\end{aligned}$$

for any $\varphi \in \mathfrak{X}_{\mathrm{arith}}(\mathbb{I})$. The last equality follows by Definition 2.5.4. This shows that $\varphi(T(n)\mathcal{F}) = T(n)(\varphi(\mathcal{F}))$. Therefore $T(n)$ acts on $M^{\mathrm{ord}}(\chi, \mathbb{I})$ and $S^{\mathrm{ord}}(\chi, \mathbb{I})$.

Definition 5.3.1. We say that an $\mathbb{I}$-adic cusp form $\mathcal{F}$ is a Hecke eigen cusp form if there exists a sequence $\{C_n\}_{n \in \mathbb{Z}_{\geq 1}}$ such that $T(n)\mathcal{F} = C_n \mathcal{F}$. We say that a Hecke eigen cusp form $\mathcal{F}$ is normalized if $a(1, \mathcal{F}) = 1$.

We denote by $S^{\mathrm{ord}}(\chi, \mathrm{Frac}(\mathbb{I})) = S^{\mathrm{ord}}(\chi, \mathbb{I}) \otimes_{\mathbb{I}} \mathrm{Frac}(\mathbb{I})$. Since $S^{\mathrm{ord}}(\chi, \mathbb{I})$ is a finitely generated torsion-free $\mathbb{I}$-module by Theorem 5.2.3, $S^{\mathrm{ord}}(\chi, \mathrm{Frac}(\mathbb{I}))$ is a finitely dimensional $\mathrm{Frac}(\mathbb{I})$-vector space.

Definition 5.3.2. The Hecke algebra $h^{\mathrm{ord}}(\chi, \mathbb{I})$ (resp. $h^{\mathrm{ord}}(\chi, \mathrm{Frac}(\mathbb{I}))$) is a $\mathbb{I}$-subalgebra (resp. $\mathrm{Frac}(\mathbb{I})$-subalgebra) of $\mathrm{End}_{\mathbb{I}}\left(S^{\mathrm{ord}}(\chi, \mathbb{I})\right)$ (resp. $\mathrm{End}_{\mathrm{Frac}(\mathbb{I})}\left(S^{\mathrm{ord}}(\chi, \mathrm{Frac}(\mathbb{I}))\right)$) which is generated by $T(n)$ for all $n \in \mathbb{Z}_{>0}$.

We define the following pairing:

$$<,>: h^{\mathrm{ord}}(\chi, \mathrm{Frac}(\mathbb{I})) \times S^{\mathrm{ord}}(\chi, \mathrm{Frac}(\mathbb{I})) \to \mathrm{Frac}(\mathbb{I}), (h, \mathcal{F}) \mapsto a(1, h\mathcal{F}). \tag{5.3}$$

Theorem 5.3.3 (Hida [Hi3, §7.3, Theorem 5])**.**

(1) The pairing (5.3) induces the following isomorphism of $\mathbb{I}$-modules:

$$S^{\mathrm{ord}}(\chi, \mathbb{I}) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{I}}\left(h^{\mathrm{ord}}(\chi, \mathbb{I}), \mathbb{I}\right). \tag{5.4}$$

(2) When $\mathbb{I}=\Lambda_{\mathcal{O}}$, (5.3) also induces the following isomorphism of $\Lambda_{\mathcal{O}}$-modules:

$$h^{\mathrm{ord}}(\chi,\Lambda_{\mathcal{O}})\xrightarrow{\sim}\mathrm{Hom}_{\Lambda_{\mathcal{O}}}\left(S^{\mathrm{ord}}(\chi,\Lambda_{\mathcal{O}}),\Lambda_{\mathcal{O}}\right).$$

Thus the Hecke algebra $h^{\mathrm{ord}}(\chi,\Lambda_{\mathcal{O}})$ is also a $\Lambda_{\mathcal{O}}$-free module of finite rank.

Proof. (1) First we prove that the pairing (5.3) is non-degenerated. Assume $\langle h,\mathcal{F}\rangle=0$ for all h. We have

$$a(n,\mathcal{F})=a(1,T(n)\mathcal{F})=0,$$

thus $\mathcal{F}=0$. Assume $\langle h,\mathcal{F}\rangle=0$ for all $\mathcal{F}$. We have the following equalities:

$$0=\langle h,T(n)\mathcal{F}\rangle=a(1,hT(n)\mathcal{F})=a(1,T(n)h\mathcal{F})=a(n,h\mathcal{F}),$$

for all n and $\mathcal{F}$. Thus $h=0$ and (5.3) is a non-degeneracy pairing.

Now let us take an element $\lambda\in\mathrm{Hom}_{\Lambda_\chi}\left(h^{\mathrm{ord}}(\chi,\Lambda_\chi),\Lambda_\chi\right)$. Then λ induces the following homomorphism:

$$\tilde{\lambda}:h^{\mathrm{ord}}(\chi,\mathrm{Frac}(\Lambda_\chi))\to\mathrm{Frac}(\Lambda_\chi),\alpha T(n)\mapsto\alpha\lambda(T(n)).$$

By the non-degeneracy of the pairing (5.3), we have $\mathcal{F}=\sum_{n=1}^{\infty}\tilde{\lambda}(T(n))q^n\in S^{\mathrm{ord}}(\chi,\mathrm{Frac}(\Lambda_\chi))$ satisfies $\langle h,\mathcal{F}\rangle=\tilde{\lambda}(h)$. Furthermore we have $\tilde{\lambda}(T(n))=\lambda(T(n))\in\Lambda_\chi$, thus $\mathcal{F}\in S^{\mathrm{ord}}(\chi,\mathbb{I})$.

(2) Write $h^{\mathrm{ord}}=h^{\mathrm{ord}}(\chi,\Lambda_{\mathcal{O}})$ and $S^{\mathrm{ord}}=S^{\mathrm{ord}}(\chi,\Lambda_{\mathcal{O}})$ for simplicity. We denote by $\left(h^{\mathrm{ord}}\right)^{**}$ the following $\Lambda_{\mathcal{O}}$-module:

$$\left(h^{\mathrm{ord}}\right)^{**}:=\mathrm{Hom}_{\Lambda_{\mathcal{O}}}\left(\mathrm{Hom}_{\Lambda_{\mathcal{O}}}\left(h^{\mathrm{ord}},\Lambda_{\mathcal{O}}\right),\Lambda_{\mathcal{O}}\right).$$

By (1), we see that to prove (1), it is sufficient to show $h^{\mathrm{ord}}=\left(h^{\mathrm{ord}}\right)^{**}$.

We have $\left(h^{\mathrm{ord}}\right)^{**}_{\mathfrak{p}}=h^{\mathrm{ord}}_{\mathfrak{p}}$ for each height 1 prime ideal $\mathfrak{p}$ of $\Lambda_{\mathcal{O}}$ by (3) of Theorem 2.2.3. Thus $Z:=\left(h^{\mathrm{ord}}\right)^{**}/h^{\mathrm{ord}}$ is a finite module by [NSW, Remark after Definition 5.1.4]. Since $\Lambda_{\mathcal{O}}$ is a regular local ring of Krull dimension 2, $\left(h^{\mathrm{ord}}\right)^{**}$ is $\Lambda_{\mathcal{O}}$-free by Proposition 2.2.2 and Theorem 2.2.4. Thus we have the following isomorphism:

$$\left(h^{\mathrm{ord}}\right)^{***}\Big/\mathfrak{p}\left(h^{\mathrm{ord}}\right)^{***}\xrightarrow{\sim}\mathrm{Hom}_{\mathcal{O}}\left(\left(h^{\mathrm{ord}}\right)^{**}\Big/\mathfrak{p}\left(h^{\mathrm{ord}}\right)^{**},\mathcal{O}\right),\tag{5.5}$$

where $\mathfrak{p}$ is the prime ideal of $\Lambda_{\mathcal{O}}$ which is generated by $X-\left(u^{k-2}-1\right)$ for a fixed integer $k\in\mathbb{Z}_{\geq 2}$. On the other hand since S^{ord} is $\Lambda_{\mathcal{O}}$-free, by the isomorphism (5.4) and Theorem 5.2.4, we have the following isomorphism of $\mathcal{O}$-modules:

$$\left(h^{\mathrm{ord}}\right)^{***}\Big/\mathfrak{p}\left(h^{\mathrm{ord}}\right)^{***}\xrightarrow{\sim}S^{\mathrm{ord}}/\mathfrak{p}S^{\mathrm{ord}}\xrightarrow{\sim}S_k^{\mathrm{ord}}\left(\Gamma_0(Np),\chi\omega^{1-k},\mathcal{O}\right).\tag{5.6}$$

We denote by $h_k^{\mathrm{ord}}\left(\Gamma_0(Np),\chi\omega^{1-k},\mathcal{O}\right)=eh_k\left(\Gamma_0(Np),\chi\omega^{1-k},\mathcal{O}\right)$ as in §5.1. Then the pairing (2.5) defined in Theorem 2.5.6 also induces the following isomorphism of $\mathcal{O}$-modules:

$$S_k^{\mathrm{ord}}\left(\Gamma_0(Np),\chi\omega^{1-k},\mathcal{O}\right)\xrightarrow{\sim}\mathrm{Hom}_{\mathcal{O}}\left(h_k^{\mathrm{ord}}\left(\Gamma_0(Np),\chi\omega^{1-k},\mathcal{O}\right),\mathcal{O}\right)\tag{5.7}$$

Combine (5.5), (5.6) and (5.7), we have the following isomorphism:

$$\mathrm{Hom}_{\mathcal{O}}\left(\left(h^{\mathrm{ord}}\right)^{**}\Big/\mathfrak{p}\left(h^{\mathrm{ord}}\right)^{**},\mathcal{O}\right)\xrightarrow{\sim}\mathrm{Hom}_{\mathcal{O}}\left(h_k^{\mathrm{ord}}\left(\Gamma_0(Np),\chi\omega^{1-k},\mathcal{O}\right),\mathcal{O}\right).\tag{5.8}$$

Since we have the following exact sequence

$$0 \to h^{\mathrm{ord}} \to \left(h^{\mathrm{ord}}\right)^{**} \to Z \to 0,$$

by tensor $\Lambda_{\mathcal{O}}/\mathfrak{p}\Lambda_{\mathcal{O}}$ we have

$$\mathrm{Tor}^1_{\Lambda_{\mathcal{O}}}\left(Z, \Lambda_{\mathcal{O}}/\mathfrak{p}\Lambda_{\mathcal{O}}\right) \to h^{\mathrm{ord}}/\mathfrak{p}h^{\mathrm{ord}} \to \left(h^{\mathrm{ord}}\right)^{**} \Big/ \mathfrak{p}\left(h^{\mathrm{ord}}\right)^{**} \to Z/\mathfrak{p}Z \to 0. \tag{5.9}$$

Since Z is finite, so is $\mathrm{Tor}^1_{\Lambda_{\mathcal{O}}}\left(Z, \Lambda_{\mathcal{O}}/\mathfrak{p}\Lambda_{\mathcal{O}}\right)$. Then the exact sequence (5.9) implies

$$0 \to h^{\mathrm{ord}}_k\left(\Gamma_0\left(Np\right), \chi\omega^{1-k}, \mathcal{O}\right) \to \left(h^{\mathrm{ord}}\right)^{**} \Big/ \mathfrak{p}\left(h^{\mathrm{ord}}\right)^{**} \to Z/\mathfrak{p}Z \to 0 \tag{5.10}$$

since the image of $h^{\mathrm{ord}}/\mathfrak{p}h^{\mathrm{ord}}$ is the sub-algebra of the $\mathcal{O}$-free algebra $\left(h^{\mathrm{ord}}\right)^{**} \Big/ \mathfrak{q}\left(h^{\mathrm{ord}}\right)^{**}$ generated by all $T\left(n\right)$. The exact sequence (5.10) induces the following exact sequence:

$$0 \to \mathrm{Hom}_{\mathcal{O}}\left(\left(h^{\mathrm{ord}}\right)^{**} \Big/ \mathfrak{p}\left(h^{\mathrm{ord}}\right)^{**}, \mathcal{O}\right) \to \mathrm{Hom}_{\mathcal{O}}\left(h^{\mathrm{ord}}_k\left(\Gamma_0\left(Np\right), \chi\omega^{1-k}, \mathcal{O}\right), \mathcal{O}\right) \to \mathrm{Ext}^1_{\mathcal{O}}\left(Z/\mathfrak{p}Z, \mathcal{O}\right) \to 0.$$

Since $\mathrm{Ext}^1_{\mathcal{O}}\left(Z/\mathfrak{p}Z, \mathcal{O}\right) = 0$ by (5.8), we have $Z/\mathfrak{p}Z = 0$. Thus $h^{\mathrm{ord}} = \left(h^{\mathrm{ord}}\right)^{**}$ by Nakayama's lemma.

□

Remark 5.3.4.

(1) By the proof of Theorem 5.3.3, there is a one-to-one correspondence between the set of $\mathbb{I}$-algebra homomorphisms $h^{\mathrm{ord}}\left(\chi, \mathbb{I}\right) \to \mathbb{I}$ and the set of all normalized Hecke eigen cusp form of $S^{\mathrm{ord}}\left(\chi, \mathbb{I}\right)$.

(2) Note that the freeness of $h^{\mathrm{ord}}\left(\chi, \Lambda_{\mathcal{O}}\right)$ is also proved in [Hi1, Theorem 3.1] without using $\Lambda_{\mathcal{O}}$-adic forms. Also notice that Hida's papers [Hi1, Corollary 3.2] and [Hi2, Theorem 1.2] give us two different proofs of the control theorem for the Hecke algebra $h^{\mathrm{ord}}\left(\chi, \Lambda_{\mathcal{O}}\right)$.

By Theorem 5.2.4 we know that a normalized Hecke eigen cusp form can be lifted to a Λ_{χ}-adic cusp form. However we do not know if it is a Hecke eigen form. We have the following lifting theorem:

Theorem 5.3.5 (Hida [Hi3, §7.4, Theorem 7])**.** Let $\zeta \in \mu_{p^r}(r \geq 0)$ be a primitive p^r-th root of unity and $f \in S_k\left(\Gamma_0\left(Np^{r+1}\right), \chi\psi\omega^{1-k}, \mathcal{O}\right)$ a p-ordinary normalized Hecke eigen cusp form of weight $k \geq 2$. Then there exist an integrally closed local domain $\mathbb{I}$ which is finite flat over Λ_{χ}, an $\mathbb{I}$-adic normalized Hecke eigen cusp form $\mathcal{F} \in S^{\mathrm{ord}}\left(\chi, \mathbb{I}\right)$ and an element $\varphi \in \mathfrak{X}_{\mathrm{arith}}\left(\mathbb{I}\right)$ such that $\varphi(\mathcal{F}) = f$.

Proof. We may assume $\zeta \in \mathcal{O}$. We have already known that f can be lifted into a Λ_{χ}-adic cusp form by Theorem 5.2.4. Let $h^{\mathrm{ord}}_k\left(\Gamma_0\left(Np^{r+1}\right), \chi_{\zeta}\chi\omega^{1-k}, \mathcal{O}\right)$ be the Hecke algebra of $S^{\mathrm{ord}}_k\left(\Gamma_0\left(Np^{r+1}\right), \chi\psi_{\zeta}\omega^{1-k}, \mathcal{O}\right)$. Let λ_f be the following $\mathcal{O}$-algebra homomorphism

$$\lambda_f : h^{\mathrm{ord}}_k\left(\Gamma_0\left(Np^{r+1}\right), \chi\psi_{\zeta}\omega^{1-k}, \mathcal{O}\right) \to \mathcal{O}, T\left(n\right) \mapsto a\left(n, f\right)$$

by the duality theorem of classical modular form (cf. [Hi3, §5.3, Theorem 1]). By definition we have that there exists an canonical homomorphism $h^{\mathrm{ord}}\left(\chi, \Lambda_{\mathcal{O}}\right) \to h^{\mathrm{ord}}_k\left(\Gamma_0\left(Np^{r+1}\right), \chi\psi_{\zeta}\omega^{1-k}, \mathcal{O}\right)$ which sends $T\left(n\right)$ to $T\left(n\right)$ of $h^{\mathrm{ord}}_k\left(\Gamma_0\left(Np^{r+1}\right), \chi\psi_{\zeta}\omega^{1-k}, \mathcal{O}\right)$. Then we have the following $\Lambda_{\mathcal{O}}$-algebra homomorphism:

$$\lambda : h^{\mathrm{ord}}\left(\chi, \Lambda_{\mathcal{O}}\right) \to h^{\mathrm{ord}}_k\left(\Gamma_0\left(Np^{r+1}\right), \chi_{\zeta}\chi\omega^{1-k}, \mathcal{O}\right) \xrightarrow{\lambda_f} \mathcal{O}, T\left(n\right) \mapsto a\left(n, f\right).$$

Note that if we regard λ as a $\Lambda_{\mathcal{O}}$-module homomorphism, λ factors through $\Lambda_{\mathcal{O}}$.

Let $\mathfrak{p} \subset \mathrm{Ker}\,\lambda$ be a minimal prime ideal of $h^{\mathrm{ord}}(\chi, \Lambda_{\mathcal{O}})$. Then $\mathbb{H} := h^{\mathrm{ord}}(\chi, \Lambda_{\mathcal{O}})/\mathfrak{p}$ is a finite extension of $\Lambda_{\mathcal{O}}$ and let $\mathbb{I}$ be the integral closure of $\Lambda_{\mathcal{O}}$ in $\mathrm{Frac}(\mathbb{H})$. We denote by $\lambda_{\mathbb{H}}$ the surjective homomorphism $h^{\mathrm{ord}}(\chi, \Lambda_{\mathcal{O}}) \otimes_{\Lambda_{\mathcal{O}}} \mathbb{H} \twoheadrightarrow \mathbb{H}$. Then there exists an algebra homomorphism $\varphi : \mathbb{H} \to \mathcal{O}$ such that $\lambda = \varphi \circ \lambda_{\mathbb{H}}$. Let $\mathcal{F} = \sum_{n=1}^{\infty} \lambda_{\mathbb{H}}(T(n)) q^n$. Then Theorem 5.3.5 follows by letting $\mathbb{I}$ be the integral closure of $\Lambda_{\mathcal{O}}$ in $\mathrm{Frac}(\mathbb{H})$ and by extending φ to $\mathbb{I}$.

□

Example 5.3.6. Let $\Delta \in S_{12}(\mathrm{SL}_2(\mathbb{Z}))$ be the Ramanujan's cusp form (cf. Example 2.5.3). Suppose that Δ is p-ordinary. We denote by $\Delta^* = \Delta(q) - \beta\Delta(q^p) \in S_{12}(\Gamma_0(p), \mathbb{Z}_p)$, where β is the unique root of $x^2 - \tau(p)x + p^{11}$ with p-adic absolute $|\beta| < 1$. The $\mathbb{Z}_p$-module $S_{12}^{\mathrm{ord}}(\Gamma_0(p), \mathbb{Z}_p)$ is of rank 1 which is generated by Δ^* by [Mi, Theorem 4.6.17 (2)], thus

$$h_{12}^{\mathrm{ord}}(\Gamma_0(p), \mathbb{Z}_p) \xrightarrow{\sim} \mathbb{Z}_p, \tag{5.11}$$

where $h_{12}^{\mathrm{ord}}(\Gamma_0(p), \mathbb{Z}_p) = e h_{12}^{\mathrm{ord}}(\Gamma_0(p), \mathbb{Z}_p)$ with $e = \lim_{n\to\infty} T(p)^{n!}$ (cf. §5.1). We denote by $\mathfrak{p}_{12}$ the ideal of Λ which is generated by $X - (u^{10} - 1)$. Since the Λ-module $S^{\mathrm{ord}}(\omega^{11}, \Lambda)$ is free of finite rank by Theorem 5.2.3 and

$$S^{\mathrm{ord}}(\omega^{11}, \Lambda)/\mathfrak{p}_{12} S^{\mathrm{ord}}(\omega^{11}, \Lambda) \xrightarrow{\sim} S_{12}(\Gamma_0(p), \mathbb{Z}_p)$$

by Theorem 5.2.4, we have

$$\begin{aligned} h^{\mathrm{ord}}(\omega^{11}, \Lambda)/\mathfrak{p}_{12} h^{\mathrm{ord}}(\omega^{11}, \Lambda) &\xrightarrow{\sim} \mathrm{Hom}_{\Lambda}(S^{\mathrm{ord}}(\omega^{11}, \Lambda), \Lambda)/\mathfrak{p}_{12}\mathrm{Hom}_{\Lambda}(S^{\mathrm{ord}}(\omega^{11}, \Lambda), \Lambda) \\ &\xrightarrow{\sim} h_{12}^{\mathrm{ord}}(\Gamma_0(p), \mathbb{Z}_p) \end{aligned} \tag{5.12}$$

by (2) of Theorem 5.3.3.

Since h^{ord} is a Λ-algebra, let $\iota : \Lambda \to h^{\mathrm{ord}}(\omega^{11}, \Lambda)$ be the structural homomorphism. We have ι is surjective by (5.11), (5.12) and Nakayama's lemma. Furthermore, ι is injective since $h^{\mathrm{ord}}(\omega^{11}, \Lambda)$ is Λ-torsion free. Thus $h^{\mathrm{ord}}(\omega^{11}, \Lambda)$ is isomorphic to Λ as a Λ-algebra and there exists a unique Λ-adic normalized Hecke eigen cusp form $\mathcal{F}_\Delta \in S^{\mathrm{ord}}(\omega^{11}, \Lambda)$ such that $\varphi(\mathcal{F}_\Delta) = \Delta^*$, where $k_\varphi = 12$ and $\zeta_\varphi = 1$.

5.4 Galois representation attached to $\mathbb{I}$-adic normalized Hecke eigen cusp forms

We keep the notations of the previous section. We denote by $\mathfrak{m}$ the maximal ideal of $\mathbb{I}$ and by $\mathbb{K} = \mathrm{Frac}(\mathbb{I})$.

Definition 5.4.1. A Galois representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{K})$ is continuous if there exists a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$- stable lattice $\mathbb{T} \subset \mathbb{K}^{\oplus 2}$ such that $\rho_{\mathbb{T}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}_{\mathbb{I}}(\mathbb{T})$ is continuous with respect to the $\mathfrak{m}$-adic topology on $\mathrm{Aut}_{\mathbb{I}}(\mathbb{T})$.

Remark 5.4.2. Since $\mathbb{I}$ is a ring of Krull dimension 2, $\mathbb{K}$ is not locally compact in any non-discrete topology on $\mathbb{K}$ ([Bo, VI, §9.3]). This implies that the image of a continuous representation $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{K})$, with non-discrete topology on $\mathbb{K}$, is very small. Hence one takes the $\mathfrak{m}$-adic topology on $\mathrm{Aut}_{\mathbb{I}}(\mathbb{T})$.

Lemma 5.4.3. If the $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$-stable lattice $\mathbb{T}$ in Definition 5.4.1 is free over $\mathbb{I}$. Then $\mathrm{Aut}_{\mathbb{I}}\left(\mathbb{T}\right)$ is topologically isomorphic to $\mathrm{GL}_2\left(\mathbb{I}\right)$, where we take the topology on $\mathrm{GL}_2\left(\mathbb{I}\right) \hookrightarrow \mathbb{I}^{\oplus 4}$.

Proof. We have $\left(\mathbb{I}/\mathfrak{m}^i\right)^{\oplus 2} \cong \mathbb{T}/\mathfrak{m}^i\mathbb{T}$, hence $\mathrm{End}_{\mathbb{I}/\mathfrak{m}^i}\left(\mathbb{T}/\mathfrak{m}^i\mathbb{T}\right)$ is topologically isomorphic to $\left(\mathbb{I}/\mathfrak{m}^i\right)^{\oplus 4}$. Thus $\mathrm{End}_{\mathbb{I}}\left(\mathbb{T}\right) = \varprojlim_i \mathrm{End}_{\mathbb{I}/\mathfrak{m}^i}\left(\mathbb{T}/\mathfrak{m}^i\mathbb{T}\right)$ is topologically isomorphic to $\mathbb{I}^{\oplus 4}$.

□

We recall the Artin-Rees lemma for proving Lemma 5.4.5.

Theorem 5.4.4 (Artin-Rees lemma)**.** Let M be a module which is finitely generated over a Noetherian ring A and N a submodule of M. Let I be an ideal of A. Then there exists an integer $c \in \mathbb{Z}_{>0}$ such that for any integer $n > c$,

$$I^n M \cap N = I^{n-c}\left(I^c M \cap N\right).$$

The following lemma tells us that the continuity of ρ in Definition 5.4.1 is independent on the choice of $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$-stable lattice $\mathbb{T}$:

Lemma 5.4.5. Let us keep the notations of Definition 5.4.1. Let $\mathbb{T}$ and $\mathbb{T}'$ be the $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$-stable lattices of $\mathbb{K}^{\oplus 2}$. Then if $\rho_{\mathbb{T}}$ is continuous so is $\rho_{\mathbb{T}'}$.

Proof. We may regard $\mathrm{End}_{\mathbb{I}}\left(\mathbb{T}\right)$ (resp. $\mathrm{End}_{\mathbb{I}}\left(\mathbb{T}'\right)$) the set of $\mathbb{K}$-homomorphisms $f : \mathbb{K}^{\oplus 2} \longrightarrow \mathbb{K}^{\oplus 2}$ such that $f\left(\mathbb{T}\right) \subset \mathbb{T}$ (resp. $f\left(\mathbb{T}'\right) \subset \mathbb{T}'$). Then $\mathrm{End}_{\mathbb{I}}\left(\mathbb{T}\right)$ and $\mathrm{End}_{\mathbb{I}}\left(\mathbb{T}'\right)$ are lattices of $\mathrm{End}_{\mathbb{K}}\left(\mathbb{K}^{\oplus 2}\right)$ by [Bo, Chap. 7, §4.1, (iv) of Proposition 3]. Then by multiplication an element in $\mathbb{K}^{\times}$ we may assume that $\mathrm{End}_{\mathbb{I}}\left(\mathbb{T}'\right) \subset \mathrm{End}_{\mathbb{I}}\left(\mathbb{T}\right)$ by Proposition 2.1.3. By Theorem 5.4.4 we have that there there exists a $c \in \mathbb{Z}_{>0}$ such that for any $n > c$,

$$\mathfrak{m}^n \mathrm{End}_{\mathbb{I}}\left(\mathbb{T}\right) \cap \mathrm{End}_{\mathbb{I}}\left(\mathbb{T}'\right) = \mathfrak{m}^{n-c}\left(\mathfrak{m}^c \mathrm{End}_{\mathbb{I}}\left(\mathbb{T}\right) \cap \mathrm{End}_{\mathbb{I}}\left(\mathbb{T}'\right)\right). \tag{5.13}$$

Furthermore we may assume that $\mathrm{End}_{\mathbb{I}}\left(\mathbb{T}'\right) \subset \mathfrak{m}^c \mathrm{End}_{\mathbb{I}}\left(\mathbb{T}\right)$, thus the induced topology on $\mathrm{End}_{\mathbb{I}}\left(\mathbb{T}'\right)$ from $\mathrm{End}_{\mathbb{I}}\left(\mathbb{T}\right)$ coincide with the $\mathfrak{m}$-adic topology on $\mathrm{End}_{\mathbb{I}}\left(\mathbb{T}'\right)$. □

Let $\mathcal{F}$ be an $\mathbb{I}$-adic normalized Hecke eigen cusp form. Hida associates a continuous Galois representation over $\mathbb{K}$ to $\mathcal{F}$ as follows:

Theorem 5.4.6 (Hida [Hi2, Theorem 2.1])**.** There exists a continuous irreducible representation $\rho_{\mathcal{F}} : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \longrightarrow \mathrm{GL}_2\left(\mathbb{K}\right)$ satisfying following properties:

1. $\rho_{\mathcal{F}}$ is unramified outside Np.
2. For the geometric Frobenius element Frob_l at $l \nmid Np$, we have:

$$\mathrm{tr}\,\rho_{\mathcal{F}}(\mathrm{Frob}_l) = a\left(l, \mathcal{F}\right),$$

$$\det \rho_{\mathcal{F}}(\mathrm{Frob}_l) = \chi(l)\langle l\rangle\left(1+X\right)^{s_l}.$$

We prove Theorem 5.4.6 in the next section. Now let us introduce the residual representation of the representation modulo a prime ideal of $\mathbb{I}$:

Definition 5.4.7. For a prime ideal $\mathcal{P}$ of $\mathbb{I}$, a Galois representation

$$\rho_{\mathcal{F}}(\mathcal{P}) : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \longrightarrow \mathrm{GL}_2\left(\mathrm{Frac}\left(\mathbb{I}/\mathcal{P}\right)\right)$$

is called a residual representation of $\rho_{\mathcal{F}}$ modulo $\mathcal{P}$ if $\rho_{\mathcal{F}}(\mathcal{P})$ is semi-simple, continuous under the $\mathfrak{m}$-adic topology of $\mathrm{Frac}\left(\mathbb{I}/\mathcal{P}\right)$ and satisfies the following properties:

1. $\rho_{\mathcal{F}}(\mathcal{P})$ is unramified outside Np.
2. For the geometric Frobenius element Frob_l at $l \nmid Np$,

$$\mathrm{tr}\,\rho_{\mathcal{F}}(\mathcal{P})(\mathrm{Frob}_l) = a\left(l, \mathcal{F}\right) \bmod \mathcal{P},$$

$$\det \rho_{\mathcal{F}}(\mathcal{P})(\mathrm{Frob}_l) = \chi(l)\langle l\rangle \left(1+X\right)^{s_l} \bmod \mathcal{P}.$$

Although $\rho_{\mathcal{F}}$ may not have $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$-stable lattice which is isomorphic to $\mathbb{I}^{\oplus 2}$, we have the following proposition (see [Hi3, §7.5, Corollary 1] and see also [MW2, §9]).

Propostion 5.4.8 (Hida, Mazur-Wiles)**.** For every prime ideal $\mathcal{P}$, the residual representation $\rho_{\mathcal{F}}(\mathcal{P})$ exists and is unique up to isomorphism over an algebraic closure of $\mathrm{Frac}(\mathbb{I}/\mathcal{P})$.

Proof. First suppose that $\mathcal{P}$ is of height 1. Let us take a $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$-stable lattice $\mathbb{T}$. Since $\mathbb{I}$ is a Krull domain by [Bo, Chap 7, §4.1, Corollary to Theorem 2], $\mathbb{I}_{\mathcal{P}}$ is a discrete valuation ring. Hence $\mathbb{T}_{\mathcal{P}} = \mathbb{T} \otimes_{\mathbb{I}} \mathbb{I}_{\mathcal{P}} \cong \mathbb{I}_{\mathcal{P}}^{\oplus 2}$ and we can review $\rho_{\mathcal{F}}$ as $\rho_{\mathcal{F}} : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \longrightarrow \mathrm{GL}_2\left(\mathbb{I}_{\mathcal{P}}\right)$. We denote by $\rho_{\mathcal{F}}(\mathcal{P})$ the semi-simplification of the following representation:

$$\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \xrightarrow{\rho_{\mathcal{F}}} \mathrm{GL}_2\left(\mathbb{I}_{\mathcal{P}}\right) \xrightarrow{\mathrm{mod}\,\mathcal{P}} \mathrm{GL}_2\left(\mathbb{I}_{\mathcal{P}}/\mathcal{P}\mathbb{I}_{\mathcal{P}}\right) = \mathrm{GL}_2\left(\mathrm{Frac}\left(\mathbb{I}/\mathcal{P}\right)\right).$$

Since $\mathbb{T}_{\mathcal{P}}$ is free of rank 2 over $\mathbb{I}_{\mathcal{P}}$, the $\mathfrak{m}$-adic topology of $\mathrm{End}_{\mathbb{I}_{\mathcal{P}}}\left(\mathbb{T}_{\mathcal{P}}\right)$ and $\mathbb{I}_{\mathcal{P}}^{\oplus 4}$ coincide (where we take the product topology on $\mathbb{I} \times \left(\mathbb{I} \setminus \mathcal{P}\right)$ and the $\mathfrak{m}$-adic topology of $\mathbb{I}_{\mathcal{P}} = \left(\mathbb{I} \times \left(\mathbb{I} \setminus \mathcal{P}\right)\right) / \sim$ is the quotient topology on $\mathbb{I} \times \mathbb{I} \setminus \{\,\mathcal{P}\,\}$). Thus $\rho_{\mathcal{F}}(\mathcal{P})$ is continuous.

Now we suppose $\mathcal{P} = \mathfrak{m}$. Let us take a $\varphi \in \mathfrak{X}_{\mathrm{arith}}\left(\mathbb{I}\right)$ and we denote by $\mathcal{P}_\varphi = \mathrm{Ker}\,\varphi$. Since

$$\mathrm{tr}\,\rho_{\mathcal{F}}\left(\mathcal{P}_\varphi\right)\left(\mathrm{Frob}_l\right) = a\left(l, \mathcal{F}\right) \bmod \mathcal{P}_\varphi = a\left(l, f_\varphi\right),$$

$$\det \rho_{\mathcal{F}}\left(\mathcal{P}_\varphi\right)\left(\mathrm{Frob}_l\right) = \chi(l)\langle l\rangle \left(1+X\right)^{s_l} \bmod \mathcal{P}_\varphi = \chi\psi_\varphi\omega^{1-k_\varphi}\left(l\right) l^{k_\varphi - 1}$$

for all $l \nmid Np$ and ρ_{f_φ} is irreducible, we have $\rho_{\mathcal{F}}\left(\mathcal{P}_\varphi\right)$ is isomorphic to ρ_{f_φ} by the Brauer-Nesbitt theorem (Theorem 2.3.3) and the Chebotarev density theorem (Theorem 2.5.9). Thus we denote by $\rho_{\mathcal{F}}\left(\mathfrak{m}\right)$ the representation $\overline{\rho}_{f_\varphi}^{\mathrm{ss}}$. The uniqueness of $\rho_{\mathcal{F}}\left(\mathcal{P}\right)$ follows also by Theorem 2.3.3 and Theorem 2.5.9. □

We introduce the following local property of $\rho_{\mathcal{F}}$ due to Mazur and Wiles:

Theorem 5.4.9 (Wiles [Wi1, Theorem 2.2.2])**.** With the same notations as above, the restriction of $\rho_{\mathcal{F}}$ to D_p is given up to equivalence by

$$\rho_{\mathcal{F}}\mid_{D_p} \sim \begin{pmatrix} \varepsilon_1 & 0 \\ * & \varepsilon_2 \end{pmatrix}$$

with ε_1 unramified and $\varepsilon_1\left(\mathrm{Frob}_p\right) = a\left(p, \mathcal{F}\right)$.

At the end of this section, we introduce the following list of cases where the condition (Free lattice) in Corollary 1.3.4 is known to be true.

Propostion 5.4.10 (Mazur-Wiles, Tilouine, Mazur-Tilouine)**.** The condition (Free lattice) holds if one of the following conditions is satisfied:

(1) The ring $\mathbb{I}$ is regular.

(2) The tame level N of $\mathcal{F}$ is equal to 1 and the ring $\mathbb{I}$ is Gorenstein (Mazur-Wiles [MW2, §9]).

(3) Let $\chi|_{(\mathbb{Z}/p\mathbb{Z})^\times} = \omega^a$. Then $a \not\equiv 0, 1 \pmod{p-1}$ and the ring $\mathbb{I}$ is Gorenstein (Tilouine [Ti, Theorem 4.4]).

(4) The residual representation $\rho_{\mathcal{F}}(\mathfrak{m})$ is irreducible (Mazur-Tilouine [MT, §2 Corollary 6]).

If $\mathbb{I}$ is a regular local ring, then $\mathbb{T}^{**} := \mathrm{Hom}_{\mathbb{I}}(\mathrm{Hom}_{\mathbb{I}}(\mathbb{T}, \mathbb{I}), \mathbb{I})$ (cf. §2.2) of a $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$-stable lattice $\mathbb{T}$ of $\rho_{\mathcal{F}}$ is free over $\mathbb{I}$ by Proposition 2.2.2 and Theorem 2.2.4.

5.5 Pseudo-representations

In this section we prove Theorem 5.4.6 by using pseudo-representations due to Wiles. Let R be a topological algebra and

$$\rho : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \to \mathrm{GL}_2(R), g \mapsto \begin{pmatrix} a(g) & b(g) \\ c(g) & d(g) \end{pmatrix}$$

continuous linear representation such that

(1) ρ is unramified outside a finite set of primes Σ.

(2) $\rho(\sigma) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$, where σ is the complex conjugation.

Then ρ must factors through G the Galois group of the largest algebraic extension of $\mathbb{Q}$ which is unramified outside Σ by the assumption (1). We denote by a, d and x the functions as follows:

$$a : G \to R, g \mapsto a(g),$$

$$d : G \to R, g \mapsto d(g),$$

$$x : G \times G \to R, (g_1, g_2) \mapsto b(g_1) c(g_2).$$

By matrix calculation, we have the following properties:

(P1) a, d and x are continuous.

(P2) $a(g_1 g_2) = a(g_1) a(g_2) + x(g_1, g_2), d(g_1 g_2) = d(g_1) d(g_2) + x(g_2, g_1)$ and

$$\begin{aligned} x(g_1 g_2, g_3 g_4) = {} & a(g_1) a(g_4) x(g_2, g_3) + a(g_4) d(g_2) x(g_1, g_3) \\ & + a(g_1) d(g_3) x(g_2, g_4) + d(g_2) d(g_3) x(g_1, g_4). \end{aligned}$$

(P3) $a(1) = d(1) = d(\sigma) = 1, a(\sigma) = -1$ and $x(g,h) = x(h,g) = 0$ for any $g \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right), h \in \{1, \sigma\}$.

(P4) $x(g_1,g_2)\,x(g_3,g_4) = x(g_1,g_4)\,x(g_3,g_2)$.

Proof. The properties (P1), (P3) and (P4) follow by definition. We prove the property (P2). Since

$$\begin{pmatrix} a(g_1g_2) & b(g_1g_2) \\ c(g_1g_2) & d(g_1g_2) \end{pmatrix} = \begin{pmatrix} a(g_1) & b(g_1) \\ c(g_1) & d(g_1) \end{pmatrix} \begin{pmatrix} a(g_2) & b(g_2) \\ c(g_2) & d(g_2) \end{pmatrix} \tag{5.14}$$

by calculating the right hand of the equality (5.14) we have the following equalities:

$$a(g_1g_2) = a(g_1)\,a(g_2) + b(g_1)\,c(g_2), \tag{5.15}$$

$$d(g_1g_2) = d(g_1)\,d(g_2) + b(g_2)\,c(g_1), \tag{5.16}$$

$$b(g_1g_2) = a(g_1)\,b(g_2) + b(g_1)\,d(g_2), \tag{5.17}$$

$$c(g_1g_2) = a(g_2)\,c(g_1) + c(g_2)\,d(g_1). \tag{5.18}$$

Then the first two assertions of (P2) follows by the equalities (5.15) and (5.16). The last assertion of (P2) follows by replacing the equality (5.18) to $g_1 = g_3, g_2 = g_4$ and by taking the product of the equalities (5.17) and (5.18). □

Definition 5.5.1. Let G be a topological group and R a topological algebra. We denote by $\pi = (a,d,x)$ such that a, d are functions of G into R and x is a function of $G \times G$ into R. We say that π is a pseudo-representation of G into R if a, d and x satisfies the conditions (P1)-(P4).

For a pseudo-representation $\pi = (a,d,x)$ of G into R, we denote by

$$\mathrm{tr}\,\pi : G \to R, g \mapsto a(g) + d(g)$$

the trace of π and by

$$\det \pi : G \to R, g \mapsto a(g)\,d(g) - x(g,g)$$

the determinant of π. The following two propositions are used to prove Theorem 5.4.6:

Propostion 5.5.2. Let $\pi = (a,d,x)$ be a pseudo-representation of a topological group G into a topological integral domain R. Then there exists a continuous representation $\rho_\pi : G \to \mathrm{GL}_2(\mathrm{Frac}(R))$ such that $\mathrm{tr}\,\rho_\pi = \mathrm{tr}\,\pi$ and $\det \rho_\pi = \det \pi$.

Proof. First we assume that $x(g,h) = 0$ for all $g, h \in G$. Then we have $a(gh) = a(g)\,a(h)$ and $d(gh) = d(g)\,d(h)$. We denote by $\rho_\pi : G \mapsto \mathrm{GL}_2(R), g \mapsto \begin{pmatrix} a(g) & 0 \\ 0 & d(g) \end{pmatrix}$. Then the proposition follows.

Next we assume there exist elements $s, t \in G$ such that $x(s,t) \neq 0$. We define

$$\rho_\pi : G \mapsto \mathrm{GL}_2(\mathrm{Frac}(R)), g \mapsto \begin{pmatrix} a(g) & b(g) \\ c(g) & d(g) \end{pmatrix}$$

such that $b(g) = \dfrac{x(g,t)}{x(s,t)}$ and $c(g) = x(s,g)$. Then the remain of the proof is to check that ρ_π is a homomorphism.

(1) Note that $b(g_1)\,c(g_2) = \dfrac{x(g_1,t)\,x(s,g_2)}{x(s,t)}$. By the property (P4), we have $x(g_1,t)\,x(s,g_2) = x(g_1,g_2)\,x(s,t)$. Hence

$$a(g_1g_2) = a(g_1)\,a(g_2) + x(g_1,g_2) = a(g_1)\,a(g_2) + b(g_1)\,c(g_2).$$

We can also prove

$$d(g_1g_2) = d(g_1)\,d(g_2) + b(g_2)\,c(g_1)$$

by the same way.

(2) Note that

$$a(g_1)\,b(g_2) + b(g_1)\,d(g_2) = \frac{a(g_1)\,x(g_2,t) + x(g_1,t)\,d(g_2)}{x(s,t)}. \tag{5.19}$$

By the property (P2) we have the following equality:

$$\begin{aligned} x(g_1g_2,g_3g_4) = {} & a(g_1)\,a(g_4)\,x(g_2,g_3) + a(g_4)\,d(g_2)\,x(g_1,g_3) \\ & + a(g_1)\,d(g_3)\,x(g_2,g_4) + d(g_2)\,d(g_3)\,x(g_1,g_4). \end{aligned} \tag{5.20}$$

Put $g_4 = 1$ and $g_3 = t$. Then the above equality (5.20) becomes to

$$x(g_1g_2,t) = a(g_1)\,x(g_2,t) + d(g_2)\,x(g_1,t) \tag{5.21}$$

by the property (P3). Combine the equalities (5.19) and (5.21), we have

$$a(g_1)\,b(g_2) + b(g_1)\,d(g_2) = \frac{x(g_1g_2,t)}{x(s,t)} = b(g_1g_2).$$

Note that

$$a(g_2)\,c(g_1) + c(g_2)\,d(g_1) = a(g_2)\,x(s,g_1) + x(s,g_2)\,d(g_1). \tag{5.22}$$

Replace $\{g_1,g_2,g_3,g_4\}$ to $\{s,1,g_1,g_2\}$ then the equality (5.20) becomes to

$$x(s,g_1g_2) = a(g_2)\,x(s,g_1) + d(g_1)\,x(s,g_2)$$

by the property (P3). Since $c(g_1g_2) = x(s,g_1g_2)$, this shows that ρ_π is a homomorphism.

□

Propostion 5.5.3. Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of $\mathbb{I}$. We denote by $\pi(\mathfrak{a})$ (resp. $\pi(\mathfrak{b})$) a pseudo-representation into $\mathbb{I}/\mathfrak{a}$ (resp. $\mathbb{I}/\mathfrak{b}$). Suppose there exist a dense subset $\Sigma \subset G$ and functions

$$\mathrm{Tr} : \Sigma \to \mathbb{I}/\mathfrak{a}\cap\mathfrak{b},$$

$$\mathrm{Det} : \Sigma \to \mathbb{I}/\mathfrak{a}\cap\mathfrak{b}$$

such that

$$\mathrm{tr}\,\pi(\mathfrak{c})(g) = \mathrm{Tr}(g) \mod \mathfrak{c}$$

and

$$\det \pi(\mathfrak{c})(g) = \mathrm{Det}(g) \mod \mathfrak{c}$$

for all $g \in \Sigma$ and $\mathfrak{c} \in \{\mathfrak{a}, \mathfrak{b}\}$ (we call that $\pi(\mathfrak{a})$ and $\pi(\mathfrak{b})$ are *compatible* in this situation). Then there exists a pseudo-representation $\pi(\mathfrak{a} \cap \mathfrak{b})$ from G into $\mathbb{I}/\mathfrak{a} \cap \mathfrak{b}$ such that

$$\mathrm{tr}\, \pi(\mathfrak{a} \cap \mathfrak{b})(g) = \mathrm{Tr}(g)$$

and

$$\det \pi(\mathfrak{a} \cap \mathfrak{b})(g) = \mathrm{Det}(g)$$

for all $g \in \Sigma$.

Proof. We consider the following exact sequence:

$$0 \to \mathbb{I}/\mathfrak{a} \cap \mathfrak{b} \xrightarrow{\iota} \mathbb{I}/\mathfrak{a} \oplus \mathbb{I}/\mathfrak{b} \xrightarrow{\alpha} \mathbb{I}/\mathfrak{a} + \mathfrak{b} \to 0 \tag{5.23}$$

such that $\iota(x \bmod \mathfrak{a} \cap \mathfrak{b}) = (x \bmod \mathfrak{a}, x \bmod \mathfrak{b})$ and $\alpha((x \bmod \mathfrak{a}, y \bmod \mathfrak{b})) = x - y \bmod \mathfrak{a} + \mathfrak{b}$. We denote by $\pi := \pi(\mathfrak{a}) \oplus \pi(\mathfrak{b})$ the pseudo-representation with values in $\mathbb{I}/\mathfrak{a} \oplus \mathbb{I}/\mathfrak{b}$. Since $\pi(\mathfrak{a})$ and $\pi(\mathfrak{b})$ are compatible, we have the following equalities:

$$\begin{aligned}
\alpha(\mathrm{tr}\, \pi(g)) &= \alpha(\mathrm{tr}\, \pi(\mathfrak{a})(g), \mathrm{tr}\, \pi(\mathfrak{a})(g)) \\
&= \alpha(\mathrm{Tr}(g) \bmod \mathfrak{a}, \mathrm{Tr}(g) \bmod \mathfrak{b}) \\
&= 0.
\end{aligned}$$

Hence $\mathrm{tr}\, \pi(g) \in \mathrm{Im}\, \iota$ by the equality (5.23). Write $\pi = (a, d, x)$, then we have the following equalities:

$$\begin{aligned}
a(g) &= 2^{-1}(\mathrm{tr}\, \pi(g) - \mathrm{tr}\, \pi(gc)) \in \mathrm{Im}\, \iota, \\
d(g) &= 2^{-1}(\mathrm{tr}\, \pi(g) + \mathrm{tr}\, \pi(gc)) \in \mathrm{Im}\, \iota
\end{aligned}$$

and

$$x(g, h) = a(gh) - a(g)\, a(h) \in \mathrm{Im}\, \iota.$$

Thus π has values in $\mathbb{I}/\mathfrak{a} \cap \mathfrak{b}$. We denote by $\pi(\mathfrak{a} \cap \mathfrak{b}) = \iota^{-1} \circ \pi$. This completes the proof of Proposition 5.5.3.

□

Under the above preparation, we are ready to proof Theorem 5.4.6.

Proof of Theorem 5.4.6. We denote by $\Sigma = \{\mathrm{Frob}_l \mid l \nmid Np\}$ which is dense in G by Theorem 2.5.9. We denote by

$$\mathrm{Tr} : \Sigma \to \mathbb{I}, \mathrm{Frob}_l \mapsto a(l, \mathcal{F})$$

and by

$$\mathrm{Det} : \Sigma \to \mathbb{I}, \mathrm{Frob}_l \mapsto \chi(l)\langle l \rangle (1 + X)^{s_l}.$$

Let $S = \{\mathcal{P}_i\}_{i=1}^{\infty}$ be a countable subset of $\{\mathrm{Ker}\, \varphi \mid \varphi \in \mathfrak{X}_{\mathrm{arith}}(\mathbb{I})\}$. For any $\mathcal{P}_i = \mathrm{Ker}\, \varphi_i \in S$, we denote by $f_i = \varphi_i(\mathcal{F})$ and by ρ_{f_i} the Galois representation attached to f_i due to Deligne and Shimura. Then

ρ_{f_i} are pseudo-representation and compatible. By Proposition 5.5.3 there exists a pseudo-representation $\pi_i = (a_i, d_i, x_i)$ of G into $\mathbb{I}/\cap_{j=1}^{i} \mathcal{P}_i$ such that

$$\operatorname{tr} \pi_i (g) \bmod \cap_{j=1}^{i-1} \mathcal{P}_i = \operatorname{tr} \pi_{i-1} (g)$$

for all $g \in G$.

Since

$$a(g) = 2^{-1} (\operatorname{tr} \pi (g) - \operatorname{tr} \pi (gc)),$$
$$d(g) = 2^{-1} (\operatorname{tr} \pi (g) + \operatorname{tr} \pi (gc))$$

and

$$x(g,h) = a(gh) - a(g) a(h),$$

we have $(\{a_i(g)\}_i, \{d_i(g)\}_i, \{x_i(g,h)\}_i) \in \varprojlim_i \mathbb{I}/\cap_{j=1}^{i} \mathcal{P}_i$ for any $g, h \in G$. Since $\cap_{i=1}^{\infty} \varprojlim_i \mathbb{I}/\cap_{j=1}^{i} \mathcal{P}_i = (0)$ by the following lemma, we have $\mathbb{I} = \varprojlim_i \mathbb{I}/\cap_{j=1}^{i} \mathcal{P}_i$ hence $\pi := \varprojlim_i \pi_i$ is a pseudo-representation of G into $\mathbb{I}$. Then $\rho_{\mathcal{F}}$ is the representation ρ_π in Proposition 5.5.2. This completes the proof of Theorem 5.4.6.

Lemma 5.5.4. Let R be a commutative Noether integral domain and S be a countable collection of height 1 prime ideal of R, then we have $\cap_{P \in S} P = (0)$.

Proof. Let us take a $x \in R$. Since R is Noetherian, primary decomposition exists for ideals ([Mat, Theorem 6.8]). Hence the radical of x is a finite intersection of height 1 prime ideals. Thus there are only finite height 1 prime ideals which contain x. This completes the proof of Lemma 5.5.4. □

Chapter 6

Proof of Theorem 1.3.1 and its corollaries

6.1 The reducibility ideal

We recall the following lemma due to Bellaïche and Chenevier:

Lemma 6.1.1 (Bellaïche-Chenevier [BC1, Lemme 1])**.** Let $(A, \mathfrak{m})$ be a complete local domain such that $\mathrm{char}(A/\mathfrak{m}) \neq 2$, where $\mathfrak{m}$ is the maximal ideal of A. Let $\rho : G \to \mathrm{GL}_2(\mathrm{Frac}(A))$ be a linear representation of a group G satisfying $\mathrm{tr}\,\rho(G) \subset A$ and $\mathrm{tr}\,\rho \bmod \mathfrak{m} = \vartheta_1 + \vartheta_2, \vartheta_1 \neq \vartheta_2$, where $\vartheta_1, \vartheta_2 : G \to (A/\mathfrak{m})^\times$ are characters. Let $g_0 \in G$ be an element satisfying $\vartheta_1(g_0) \neq \vartheta_2(g_0)$ and $\lambda_1, \lambda_2 \in A$ the roots of the characteristic polynomial of $\rho(g_0)$. Choose a basis $\{e_1, e_2\}$ of the representation ρ such that $\rho(g_0)e_i = \lambda_i e_i$ $(i = 1, 2)$. Write $\rho(g) = \begin{pmatrix} a(g) & b(g) \\ c(g) & d(g) \end{pmatrix}$ for any $g \in G$.

Let $I \subsetneq A$ be an ideal such that there exist two characters $\nu_1, \nu_2 : G \to (A/I)^\times$ such that

$$\mathrm{tr}\,\rho(g) \bmod I = \nu_1(g) + \nu_2(g)$$

for any $g \in G$. Assume $\nu_1 \bmod \mathfrak{m} = \vartheta_1, \nu_2 \bmod \mathfrak{m} = \vartheta_2$ without loss of generality. Then for any $g, g' \in G$, we have $a(g), d(g) \in A$, $a(g) \bmod I = \nu_1(g), d(g) \bmod I = \nu_2(g)$, and $b(g)c(g') \in I$.

We omit the proof of the lemma, since it is done in the similar way as the arguments in §3.1.

Remark 6.1.2. If $\mathrm{char}(A/\mathfrak{m}) = 2$, the statement holds assuming an extra condition on the determinate (cf. [BC1, Lemme 1]).

Definition 6.1.3. Let $(A, \mathfrak{m})$ be a complete local domain such that $\mathrm{char}(A/\mathfrak{m}) \neq 2$, where $\mathfrak{m}$ is the maximal ideal of A. Let $\rho : G \to \mathrm{GL}_2(\mathrm{Frac}(A))$ be a linear representation of a group G satisfying $\mathrm{tr}\rho(G) \subset A$ and $\mathrm{tr}\,\rho \bmod \mathfrak{m} = \vartheta_1 + \vartheta_2, \vartheta_1 \neq \vartheta_2$, where $\vartheta_1, \vartheta_2 : G \to (A/\mathfrak{m})^\times$ are characters. For any $g \in G$, write $\rho(g) = \begin{pmatrix} a(g) & b(g) \\ c(g) & d(g) \end{pmatrix}$ with respect to the basis taken as in Lemma 6.1.1. We define $I(\rho)$ the ideal of A which is generated by $b(g)c(g')$ for all $g, g' \in G$.

The ideal $I(\rho)$ is well-defined by Lemma 6.1.1. Under the above preparation, we are ready to determine $\sharp\mathscr{L}(\rho)$ of a p-adic representation ρ.

Propostion 6.1.4. Let $(\mathcal{O}, \varpi, \mathbb{F})$ be the ring of integers of a finite extension of $\mathbb{Q}_p$ with ϖ a fixed uniformizer of $\mathcal{O}$ and $\mathbb{F}$ the residue field. Let V be a vector space of dimension 2 over $K = \mathrm{Frac}(\mathcal{O})$ and $\rho : G \to \mathrm{Aut}_K(V)$ a continuous irreducible representation of a compact group G.

Assume that

$$\mathrm{tr}\,\rho \bmod \varpi = \vartheta_1 + \vartheta_2, \vartheta_1 \neq \vartheta_2,$$

where $\vartheta_1, \vartheta_2 : G \to \mathbb{F}^\times$ are characters. Then we have

$$\mathrm{ord}_\varpi I(\rho) + 1 = \sharp\mathscr{C}(\rho) = \sharp\mathscr{L}(\rho),$$

where $\mathscr{C}(\rho)$ is the set of G-stable lattices up to multiplication by elements of $K^\times$ (cf. §3.3).

Note that the first equality $\mathrm{ord}_\varpi I(\rho) + 1 = \sharp\mathscr{C}(\rho)$ is a special case of Bellaïche-Graftieaux [BG, Théorème 4.1.3] (see also the remark immediately after it).

Proof. We first show $\mathrm{ord}_\varpi I(\rho) + 1 = \sharp\mathscr{C}(\rho)$. Fix a $g_0 \in G$ such that $\vartheta_1(g_0) \neq \vartheta_2(g_0)$. The characteristic polynomial of $\rho(g_0)$

$$X^2 - \mathrm{tr}\,\rho(g_0)X + \det\rho(g_0)$$

has roots $\lambda_1 \neq \lambda_2$ in A such that $\lambda_i \bmod \varpi = \vartheta_i(g_0) (i = 1, 2)$ by Hensel's lemma. Choose a basis $\{e_1, e_2\}$ of the representation ρ such that $\rho(g_0)e_i = \lambda_i e_i$ $(i = 1, 2)$. Write $\rho(g) = \begin{pmatrix} a(g) & b(g) \\ c(g) & d(g) \end{pmatrix}$ for all $g \in G$. Let B be the module of $\mathcal{O}$ generated by $b(g)$ for all $g \in G$. Since ρ is irreducible, we have $B \neq (0)$. Since ρ is continuous and G is compact, there exists a G-stable lattice. Hence Im ρ is bounded in $\mathrm{GL}_2(K)$ by Proposition 2.3.2. We have $B = \mathcal{O}$ and the following properties by Operation 1 (cf. §3.1).

(1) $\rho(g_0) = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$.

(2) There exists a $h \in G$ such that $\varpi \nmid b(h)$.

Since $BC = I(\rho)$ by Lemma 6.1.1, we must have $C = I(\rho) = (\varpi)^n$ for a positive integer n. This also means that we have chosen a G-stable lattice T such that

$$\rho = \rho_T : G \to \mathrm{GL}_2(\mathcal{O})$$

and $T/\varpi T$ is not semi-simple. By reduction mod $(\varpi)^i$ $(i = 1, 2, \ldots, n)$, we obtain the G-stable lattices $T_1, \cdots, T_n$ such that $[T_i] \neq [T_j]$ if $i \neq j$. Then $n + 1 = \mathrm{ord}_\varpi I(\rho) + 1 \leq \sharp\mathscr{C}(\rho)$.

Let $\sharp\mathscr{C}(\rho) = m + 1$. We have $\mathscr{C}(\rho)$ is a segment $[x, x_m]$ by the proof of Proposition 3.3.1 at the end of §3.3. Let T, T_m be the representatives of x, x_m such that $T_m \subset T$ and $T/T_m \cong \mathcal{O}/(\varpi)^m$ as an $\mathcal{O}$-module. Hence there exists a basis of T such that $\rho_T : G \to \mathrm{GL}_2(\mathcal{O}), g \mapsto \begin{pmatrix} a(g) & b(g) \\ c(g) & d(g) \end{pmatrix}$ satisfies $\varpi^m \mid c(g)$ for any $g \in G$. Then

$$a \bmod (\varpi)^m : G \to (\mathcal{O}/(\varpi)^m)^\times, g \mapsto a(g) \bmod (\varpi)^m$$

and

$$d \bmod (\varpi)^m : G \to (\mathcal{O}/(\varpi)^m)^\times, g \mapsto d(g) \bmod (\varpi)^m$$

are two characters. Thus $I(\rho) \subset (\varpi)^m$ by Lemma 6.1.1 and $\sharp\mathscr{C}(\rho) \leq \mathrm{ord}_\varpi I(\rho) + 1$.

Next we prove $\sharp\mathscr{C}(\rho) = \sharp\mathscr{L}(\rho)$. Suppose $\sharp\mathscr{C}(\rho) = n+1$. Since $\mathscr{C}(\rho)$ is a segment, there exist the following representatives of the points in $\mathscr{C}(\rho)$:

$$T_0 \supsetneq \cdots \supsetneq T_n$$

such that

(i) $[T_i]$ is a neighbor of $[T_{i-1}]$ and $T_0/T_i \cong \mathcal{O}/(\varpi)^i$ as an $\mathcal{O}$-module for $i = 1, \cdots, n$.

(ii) T_0, T_n are mod ϖ not semi-simple lattices and the others are not.

Thus it is sufficient to show that for $i \neq j$, T_i and T_j are non-isomorphic as $\mathcal{O}[G]$-modules.

1. Suppose we have $f : T_0 \xrightarrow{\sim} T_n$ as $\mathcal{O}[G]$-modules. Then $\varpi T_n \subset f(T_1) \subset T_n$ since $[T_1]$ is a neighbor of $[T_0]$. Since T_n is a mod ϖ not semi-simple lattice, we have $f(T_1) = \varpi T_{n-1}$ by (2) of Proposition 3.3.5. Thus we have the following isomorphism:

$$T_1/\varpi T_0 \cong \varpi T_{n-1}/\varpi T_n \cong \mathbb{F}[\vartheta_1] \text{ (resp. } \mathbb{F}[\vartheta_2]) \tag{6.1}$$

as an $\mathbb{F}[G]$-module. Since $T_1/\varpi T_0$ (resp. $\varpi T_{n-1}/\varpi T_n$) is the unique $\mathbb{F}[G]$-submodule of $T_0/\varpi T_0$ (resp. $T_n/\varpi T_n$) of dimension 1, the isomorphism (6.1) implies that there is no mod ϖ not semi-simple stable lattice T such that $T/\varpi T$ has a submodule which is isomorphic to $\mathcal{O}/(\varpi)[\vartheta_2]$ (resp. $\mathcal{O}/(\varpi)[\vartheta_1]$). This contradicts to Proposition 3.3.1.

2. Suppose we have $f : T_i \xrightarrow{\sim} T_j$ as $\mathcal{O}[G]$-modules for some $0 < i < j < n$. Since T_0 is a mod ϖ not semi-simple lattice and T_0, T_n are non-isomorphic as $\mathcal{O}[G]$-modules, we have $[f(\varpi^i T_0)] = [T_0]$ i.e. $f(\varpi^i T_0) = \varpi^l T_0$ for some l. Thus

$$\mathcal{O}/(\varpi)^i \cong T_0/T_i \cong T_0/\varpi^{i-l} T_j$$

as an $\mathcal{O}$-module. This implies $d([T_0], [T_j]) = i$ by Proposition 3.2.6. On the other hand, $[T_0]$ is an edge of the segment $\mathscr{C}(\rho)$, there exists an unique point $y \in \mathscr{C}(\rho)$ such that $d([T_0], y) = i$. This contradicts to $i \neq j$.

□

Now we give an example by using Proposition 6.1.4 to determine $\sharp\mathscr{L}(\rho_f)$, where ρ_f is the Galois representation attached to a normalized Hecke eigen cusp form f. Let $\Delta \in S_{12}(\mathrm{SL}_2(\mathbb{Z}))$ be the Ramanujan's cusp form (cf. Example 2.5.3) and

$$\rho_\Delta : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Q}_p)$$

the Galois representation attached to Δ.

Propostion 6.1.5. The ideal $I(\rho_\Delta) \subset \mathbb{Z}_p$ defined as in Definition 6.1.3 is the minimal ideal such that there exists an integer $a \in \mathbb{Z}$ such that for any prime $l \neq p$,

$$\tau(l) \equiv l^a + l^{11-a} \bmod I(\rho_\Delta).$$

Proof. Since ρ_Δ is unramified outside $\{ p, \infty \}$, ρ_Δ must factor through $G_{\{p,\infty\}}$ which is the Galois group of the maximal Galois extension of $\mathbb{Q}$ unramified outside $\{ p, \infty \}$. Let $\nu_1, \nu_2 : G_{\{p,\infty\}} \to (\mathbb{Z}_p / I(\rho_\Delta))^\times$ be the character such that

$$\operatorname{tr} \rho \bmod I(\rho_\Delta) = \nu_1 + \nu_2.$$

Also by the fact that ρ_Δ is unramified outside $\{ p, \infty \}$, ν_1 and ν_2 must factor through $\operatorname{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ by class field theory. Thus ϑ_1 and ϑ_2 must be power $\chi_{cyc} \bmod I(\rho_\Delta)$. For the Frobenius element Frob_l with prime $l \neq p$, we have $\chi_{cyc}(\mathrm{Frob}_l) = l$ and $\det \rho_\Delta(\mathrm{Frob}_l) = l^{11}$. Thus the proposition follows by the Theorem 2.5.9.

□

Serre and Swinnerton-Dyer showed that $\bar{\rho}_\Delta$ is reducible if and only if $p = 2, 3, 5, 7$ and 691 (see [Sw1, Corollary to Theorem 4]). [Sw2] also showed the congruence mod p^n for $p = 3, 5, 7$ and 691 (see [Sw2], page 77 for $p = 691$, Theorem 4 for $p = 5, 7$ and the table after Theorem 6 for $p = 3$). Then combined with our arguments, we have the following table for odd primes.

p	3	5	7	691
$\sharp \mathscr{L}(\rho_\Delta)$	7	4	2	2

6.2 The relation between the reducibility ideal and the Kubota-Leopoldt p-adic L-function

We prove Theorem 1.3.1 in this section. We denote by γ a topological generator of $\operatorname{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ such that $\kappa_{\mathrm{cyc}}(\gamma) = u$ and by κ_{univ} the universal cyclotomic character as follows:

$$\kappa_{\mathrm{univ}} : \operatorname{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \twoheadrightarrow \operatorname{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \xrightarrow{\sim} 1 + p\mathbb{Z}_p \hookrightarrow \Lambda_\chi^\times,$$

where $1 + p\mathbb{Z}_p \hookrightarrow \Lambda_\chi^\times$ is the homomorphism defined by sending u to $1 + X$. By Theorem 5.4.9, we have

$$\rho_{\mathcal{F}} \mid_{D_p} \sim \begin{pmatrix} \varepsilon_1 & 0 \\ * & \varepsilon_2 \end{pmatrix},$$

with ε_1 unramified. Recall that $\rho_{\mathcal{F}}(\mathfrak{m}) \cong \overline{\chi}_1 \oplus \overline{\chi}_2$. Then for any $g \in D_p$, $\{ \bar{\varepsilon}_1(g), \bar{\varepsilon}_2(g) \}$ and $\{ \overline{\chi}_1(g), \overline{\chi}_2(g) \}$ are the set of the roots of the mod $\mathfrak{m}$ characteristic polynomial of $\rho_{\mathcal{F}}(g)$: $X^2 - \mathrm{tr}\rho_{\mathcal{F}}(g)X + \det\rho_{\mathcal{F}}(g) \bmod \mathfrak{m}$, hence they must be coincide. Thus $\bar{\varepsilon}_1 = \overline{\chi}_1 \mid_{D_p}$ and $\bar{\varepsilon}_2 = \overline{\chi}_2 \mid_{D_p}$ under the assumption that $\overline{\chi}_1$ (resp. $\overline{\chi}_2$) is unramified (resp. ramified). We denote by I_p the inertia group of p and we choose a $g_0 \in I_p$ such that $\overline{\chi}_1(g_0) \neq \overline{\chi}_2(g_0)$.

Let $\{e_1, e_2\}$ be a basis of $\operatorname{Frac}(\mathbb{I})^{\oplus 2}$ such that

$$\rho_{\mathcal{F}}(g_0) = \begin{pmatrix} 1 & 0 \\ 0 & \varepsilon_2(g_0) \end{pmatrix}, \rho_{\mathcal{F}} \mid_{D_p} = \begin{pmatrix} \varepsilon_1 & 0 \\ * & \varepsilon_2 \end{pmatrix}. \tag{6.2}$$

Write $\rho_{\mathcal{F}}(g) = \begin{pmatrix} a(g) & b(g) \\ c(g) & d(g) \end{pmatrix}$ for any $g \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. We have $a(g), d(g)$ and $b(g)c(g') \in \mathbb{I}$ for any $g, g' \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ by Lemma 6.1.1. Recall that $I(\rho_{\mathcal{F}})$ is the ideal of $\mathbb{I}$ generated by $b(g)c(g')$ for all $g, g' \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Since $\rho_{\mathcal{F}}(\mathfrak{m})$ is reducible, we have $I(\rho_{\mathcal{F}}) \subset \mathfrak{m}$ by Lemma 6.1.1.

Lemma 6.2.1. Let us take the basis of $\mathrm{Frac}(\mathbb{I})^{\oplus 2}$ to be the same as the beginning of this section. For any $\varphi \in \mathfrak{X}_{\mathrm{arith}}(\mathbb{I})$, let ϖ_φ be a fixed uniformizer of $\varphi(\mathbb{I})$. Then

$$\mathrm{ord}_{\varpi_\varphi}(\varphi(I(\rho_{\mathcal{F}}))) + 1 = \sharp\mathscr{L}(\rho_{f_\varphi}).$$

Proof. For any $\varphi \in \mathfrak{X}_{\mathrm{arith}}(\mathbb{I})$, we denote by $\mathcal{P} = \mathrm{Ker}\,\varphi$ and by $\mathbb{I}_{\mathcal{P}}$ the localization of $\mathbb{I}$ at $\mathcal{P}$. Then $\mathbb{I}_{\mathcal{P}}$ is a discrete valuation ring with κ_{cyc} a fixed uniformizer of $\mathbb{I}_{\mathcal{P}}$. For the Galois representation

$$\rho_{\mathcal{P}} : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \xrightarrow{\rho_{\mathcal{F}}} \mathrm{GL}_2(\mathrm{Frac}(\mathbb{I})) = \mathrm{GL}_2(\mathrm{Frac}(\mathbb{I}_{\mathcal{P}})),$$

let B be the $\mathbb{I}_{\mathcal{P}}$-submodule of $\mathrm{Frac}(\mathbb{I}_{\mathcal{P}})$ generated by $b(g)$ for all $g \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$. Since $\rho_{\mathcal{F}}$ is irreducible, $B \neq (0)$. Since $\rho_{\mathcal{F}}$ is continuous, by Definition 5.4.1 there exists a lattice $\mathbb{T} \subset \mathrm{Frac}(\mathbb{I})^{\oplus 2}$ which is stable under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action. Then $\mathbb{T}_{\mathcal{P}} = \mathbb{T} \otimes_{\mathbb{I}} \mathbb{I}_{\mathcal{P}}$ is a stable lattice of $\rho_{\mathcal{P}}$ and $\mathrm{Im}\,\rho_{\mathcal{P}}$ is bounded by Proposition 2.3.2. Thus we may assume $B = \mathbb{I}_{\mathcal{P}}$ by Operation 1 (cf. §3.1). Then $\mathrm{Im}\,\rho_{\mathcal{P}} \subset \mathrm{GL}_2(\mathbb{I}_{\mathcal{P}})$ for this new $\rho_{\mathcal{P}}$ by Lemma 6.1.1.

We denote by ρ_φ the Galois representation

$$\rho_\varphi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho_{\mathcal{P}}} \mathrm{GL}_2(\mathbb{I}_{\mathcal{P}}) \twoheadrightarrow \mathrm{GL}_2(\varphi(\mathbb{I}_{\mathcal{P}})), g \mapsto \begin{pmatrix} a_\varphi(g) & b_\varphi(g) \\ c_\varphi(g) & d_\varphi(g) \end{pmatrix}$$

and by ρ_{f_φ} the Galois representation associated to f_φ. Since

$$\mathrm{tr}\,\rho_\varphi(\mathrm{Frob}_l) = \mathrm{tr}\,\rho_{f_\varphi}(\mathrm{Frob}_l), \det\rho_\varphi(\mathrm{Frob}_l) = \det\rho_{f_\varphi}(\mathrm{Frob}_l)$$

for all primes $l \nmid Np$, we have the semi-simplification of ρ_φ and ρ_{f_φ} are isomorphic by Theorem 2.3.3 and Theorem 2.5.9. Then by the fact that ρ_{f_φ} is irreducible, we have that the representations ρ_φ and ρ_{f_φ} are isomorphic. Thus $I\left(\rho_{f_\varphi}\right) = \varphi\left(I\left(\rho_{\mathcal{F}}\right)\right)$ by the definition of $I\left(\rho_{f_\varphi}\right)$ and Lemma 6.2.1 follows by Proposition 6.1.4.

□

Lemma 6.2.2. Let us take the basis of $\mathrm{Frac}(\mathbb{I})^{\oplus 2}$ to be the same as the beginning of this section. Let J be the ideal of $\mathbb{I}$ generated by $\mathrm{tr}\rho_{\mathcal{F}}(g) - \chi_1(g) - \chi_2\kappa_{\mathrm{cyc}}\kappa_{\mathrm{univ}}(g)$ for all $g \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ and J' the ideal generated by $a(g) - \chi_1(g)$ for all $g \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$. Then we have the following statements:

(1) $I(\rho_{\mathcal{F}}) = J = J'$.

(2) Suppose $N = 1$. Then $\rho_{\mathcal{F}}(\mathfrak{m}) \cong \overline{\mathbf{1}} \oplus \overline{\chi}$, where $\mathbf{1}$ is the trivial character.

Proof. We first show $J = J'$. Since $\mathrm{tr}\rho_{\mathcal{F}} \equiv \chi_1 + \chi_2\kappa_{\mathrm{cyc}}\kappa_{\mathrm{univ}} \bmod J$, $a(g) \equiv \chi_1(g) \bmod J$ or $a(g) \equiv \chi_2\kappa_{\mathrm{cyc}}\kappa_{\mathrm{univ}}(g) \bmod J$ for all $g \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ by Lemma 6.1.1. By equality (6.2) we have that the character $a \bmod \mathfrak{m} = \overline{\chi}_1$ is unramified at p, thus $a(g) \equiv \chi_1(g) \bmod J$ for all $g \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$. This implies $J' \subset J$. We also have $J \subset J'$ since

$$\mathrm{tr}\,\rho_{\mathcal{F}}(g) - \chi_1(g) - \chi_2\kappa_{\mathrm{cyc}}\kappa_{\mathrm{univ}}(g) = (a(g) - \chi_1(g)) + (a(g^{-1}) - \chi_1(g^{-1}))\det\rho_{\mathcal{F}}(g) \in J'.$$

Now we prove $I(\rho_{\mathcal{F}}) = J'$. We have $b(g)c(g') \in J$ for any $g, g' \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ by Lemma 6.1.1 hence $I(\rho_{\mathcal{F}}) \subset J = J'$. Let K be the abelian extension of $\mathbb{Q}$ corresponding to

$$\mathrm{Ker}\left(\nu : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow (\mathbb{I}/I(\rho_{\mathcal{F}}))^{\times},\ g \mapsto a(g) \bmod I(\rho_{\mathcal{F}})\right).$$

Then ν factors through $\mathrm{Gal}(K/\mathbb{Q})$. Write $a(g) = \chi_1(g)(1 + m(g))$ where $m(g) \in \mathfrak{m}$. Then $\nu(g) = \chi_1(g) \bmod I(\rho_{\mathcal{F}}) \cdot (1 + m(g)) \bmod I(\rho_{\mathcal{F}})$. Note that ν is unramified outside N by the equality (6.2), hence K is a subfield of $\mathbb{Q}(\mu_N)$ by class field theory. On the other hand, the kernel of the map $(\mathbb{I}/I(\rho_{\mathcal{F}}))^{\times} \to (\mathbb{I}/\mathfrak{m})^{\times}$ is a pro-p group, thus $(1 + m(g)) \bmod I(\rho_{\mathcal{F}})$ must be trivial under the assumption $p \nmid \phi(N)$. This implies $\chi_1(g) \equiv a(g) \pmod{I(\rho_{\mathcal{F}})}$, hence $J' \subset I(\rho_{\mathcal{F}})$. Specially when $N = 1$, we have that $a \bmod I(\rho_{\mathcal{F}})$ is an unramified character. Thus $a \bmod I(\rho_{\mathcal{F}})$ is trivial by class field theory (the Galois group of the maximal unramified abelian extension of a number field F is isomorphic to the ideal class group of F). □

Lemma 6.2.2 tells us that $I(\rho_{\mathcal{F}})$ is a closed ideal in $\mathbb{I}$ under the $\mathfrak{m}$-adic topology.

Propostion 6.2.3. Let us take the basis of $\mathrm{Frac}(\mathbb{I})^{\oplus 2}$ to be the same as at the beginning of this section. Let $L_\infty, L_\infty^{(Np)}$ be the maximal unramified abelian p-extension of $\mathbb{Q}(\mu_{Np^\infty})$ and the maximal abelian p-extension unramified outside Np of $\mathbb{Q}(\mu_{Np^\infty})$. We denote by $X_\infty = \mathrm{Gal}(L_\infty/\mathbb{Q}(\mu_{Np^\infty}))$ and by $Y_\infty = \mathrm{Gal}\left(L_\infty^{(Np)}/\mathbb{Q}(\mu_{Np^\infty})\right)$ on which $\Delta_{Np} = \mathrm{Gal}(\mathbb{Q}(\mu_{Np^\infty})/\mathbb{Q}_\infty)$ acts by conjugation. Then we have the following statements:

(1) $\mathcal{L}_p(\chi_1^{-1}\chi_2)\mathbb{I} \subset I(\rho_{\mathcal{F}})$.

(2) Suppose the $\Lambda_{\chi_1\chi_2^{-1}}$-modules $X_\infty^{\chi_1\chi_2^{-1}}$ and $Y_\infty^{\chi_1^{-1}\chi_2}$ are cyclic. Then $I(\rho_{\mathcal{F}})$ is principal.

Proof. (1) We have $\chi_1(g) \equiv a(g) \bmod I(\rho_{\mathcal{F}})$ and $\chi_2\kappa_{\mathrm{cyc}}\kappa_{\mathrm{univ}}(g) \equiv d(g) \bmod I(\rho_{\mathcal{F}})$ for all $g \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ by Lemma 6.1.1 and Lemma 6.2.2. We prove the proposition by using Wiles' construction (cf. [Wi2, Section 6]) of an uramified extension N_∞ of $\mathbb{Q}(\mu_{Np^\infty})$.

Let B (resp. C) be an $\mathbb{I}$-submodule of $\mathrm{Frac}(\mathbb{I})$ generated by $b(g)$ (resp. $c(g)$) for all $g \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then the modules B and C are finitely generated by Lemma 6.1.1. We denote by b the function

$$b : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to B,\ g \mapsto b(g)$$

and we endow B with the $\mathfrak{m}$-adic topology.

Step 1 We show the map b is continuous in this first step. Since $\rho_{\mathcal{F}}$ is continuous, by Definition 5.4.1 there exists a lattice $\mathbb{T} \subset \mathrm{Frac}(\mathbb{I})^{\oplus 2}$ which is stable under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action such that $\rho_{\mathcal{F}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}_{\mathbb{I}}(\mathbb{T})$ is continuous with respect to the $\mathfrak{m}$-adic topology of $\mathrm{Aut}_{\mathbb{I}}(\mathbb{T})$. We denote by $V_i = \mathrm{Frac}(\mathbb{I})e_i$ and by $\mathbb{T}_i = \mathbb{T} \cap V_i$ $(i = 1, 2)$. Then $\rho_{\mathcal{F}}(\mathbb{T}_i) \subset \mathbb{T}$. For any $xe_1 \in \mathbb{T}_1$ and $ye_2 \in \mathbb{T}_2$, we have

$$\rho_{\mathcal{F}}(g)(xe_1) = a(g)\,xe_1 + c(g)\,xe_2,$$

$$\rho_{\mathcal{F}}(g)(ye_2) = b(g)\,ye_1 + d(g)\,ye_2.$$

Since $a(g) \in \mathbb{I}$ by Lemma 6.1.1, $a(g)\,xe_1 \in \mathbb{T} \cap V_1 = \mathbb{T}_1$ and $c(g)\,xe_2 = \rho_{\mathcal{F}}(g)(xe_1) - a(g)\,xe_1 \in \mathbb{T} \cap V_2 = \mathbb{T}_2$. We also have $b(g)\,ye_1 \in \mathbb{T}_1$ by the same argument. This implies that

$\mathbb{T}_1 \oplus \mathbb{T}_2$ is also a stable lattice of $\mathrm{Frac}\,(\mathbb{I})^{\oplus 2}$. We replace $\mathbb{T}$ with $\mathbb{T}_1 \oplus \mathbb{T}_2$. The representation $\rho_{\mathcal{F}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}_{\mathbb{I}}(\mathbb{T})$ is also continuous by Theorem 5.4.4. We may regard B as an $\mathbb{I}$-submodule of $\mathrm{Hom}_{\mathbb{I}}(\mathbb{T}_2, \mathbb{T}_1)$ via the injective homomorphism as follows:

$$B \hookrightarrow \mathrm{Hom}_{\mathbb{I}}\left(\mathbb{T}_2, \mathbb{T}_1\right),\ b(g) \mapsto b(g)(ye_2) = b(g) \cdot ye_1$$

for all $ye_2 \in \mathbb{T}_2$. Then b is the following map:

$$\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \overset{\rho_{\mathcal{F}}}{\to} \mathrm{Aut}_{\mathbb{I}}\left(\mathbb{T}\right) \to \mathrm{Hom}_{\mathbb{I}}(\mathbb{T}_2, \mathbb{T}_1).$$

The homomorphism $\mathrm{Aut}_{\mathbb{I}}(\mathbb{T}) \to \mathrm{Hom}_{\mathbb{I}}(\mathbb{T}_2, \mathbb{T}_1)$ is continuous under the $\mathfrak{m}$-adic topology, hence b is continuous.

Step 2 In this step, we construct an abelian p-extension of $\mathbb{Q}\left(\mu_{Np^\infty}\right)$ by the following homomorphism:

$$\overline{b} : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\left(\mu_{Np^\infty}\right)\right) \overset{b}{\to} B \twoheadrightarrow B/I(\rho_{\mathcal{F}})B.$$

Let N_∞ be the abelian extension of $\mathbb{Q}\left(\mu_{Np^\infty}\right)$ corresponding to $\mathrm{Ker}\ \overline{b}$ and we denote by the same symbol $\overline{b}$

$$\overline{b} : G = \mathrm{Gal}\left(N_\infty/\mathbb{Q}\left(\mu_{Np^\infty}\right)\right) \hookrightarrow B/I(\rho_{\mathcal{F}})B. \tag{6.3}$$

For any $h \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ and $g \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\left(\mu_{Np^\infty}\right)\right)$, a matrix calculation shows that

$$\overline{b}(hgh^{-1}) = \chi_1\chi_2^{-1}\kappa_{\mathrm{cyc}}^{-1}\kappa_{\mathrm{univ}}^{-1}(h)\overline{b}(g).$$

Let $\tilde{\gamma}$ be a topological generator of $\mathrm{Gal}\left(\mathbb{Q}\left(\mu_{Np^\infty}\right)/\mathbb{Q}\left(\mu_{Np}\right)\right)$ which is sent to γ under the canonical isomorphism $\mathrm{Gal}\left(\mathbb{Q}\left(\mu_{Np^\infty}\right)/\mathbb{Q}\left(\mu_{Np}\right)\right) \to \mathrm{Gal}\left(\mathbb{Q}_\infty/\mathbb{Q}\right)$. The above arguments tell us that $\overline{b}\left(G\right)$ is a $\Lambda_{\chi_1\chi_2^{-1}} = \mathbb{Z}_p[\chi_1\chi_2^{-1}][[X]]$-module under the surjection

$$\mathbb{Z}_p[[\mathrm{Gal}\left(\mathbb{Q}\left(\mu_{Np^\infty}\right)/\mathbb{Q}\right)]] \overset{\chi_1\chi_2^{-1}\kappa_{\mathrm{cyc}}^{-1}\kappa_{\mathrm{univ}}^{-1}}{\longrightarrow} \Lambda_{\chi_1\chi_2^{-1}},\ u^{-1}\tilde{\gamma}^{-1} \mapsto 1 + X$$

and $\mathrm{Gal}\left(\mathbb{Q}(\mu_{Np^\infty})/\mathbb{Q}_\infty\right)$ acts on $\overline{b}\left(G\right)$ via $\chi_1\chi_2^{-1}$.

Step 3 In this step, we show that the canonical homomorphism $\overline{b}\left(G\right) \otimes_{\Lambda_{\chi_1\chi_2^{-1}}} \mathbb{I} \to B/I(\rho_{\mathcal{F}})B$ is an isomorphism. The injectivity follows from the assumption that $\mathbb{I}$ is flat over $\Lambda_{\chi_1\chi_2^{-1}}$ by applying the base extension $\otimes_{\Lambda_{\chi_1\chi_2^{-1}}}\mathbb{I}$ to the equality (6.3). For any $g \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$, consider the commutator $[g, g_0] \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\left(\mu_{N^\infty p^\infty}\right)\right)$ we have

$$\overline{b}([g, g_0]) = \frac{\lambda - 1}{\lambda}\left(\chi_2\kappa_{\mathrm{cyc}}\kappa_{\mathrm{univ}}(g)\right)^{-1}\overline{b}(g),$$

where $\lambda = \varepsilon_2(g_0)$. Since $\lambda \not\equiv 1 \bmod \mathfrak{m}$, we have $\overline{b}\left([g, g_0]\right) \otimes \chi_2\kappa_{\mathrm{cyc}}\kappa_{\mathrm{univ}}(g)\dfrac{\lambda}{\lambda - 1} \in \overline{b}\left(G\right) \otimes_{\Lambda_{\chi_1\chi_2^{-1}}} \mathbb{I}$.

Step 4 In this step, we show that the extension $N_\infty/\mathbb{Q}(\mu_{Np^\infty})$ is unramified everywhere. Note that $N_\infty/\mathbb{Q}\left(\mu_{Np^\infty}\right)$ is unramified since all $l \nmid Np$ since the representation $\rho_{\mathcal{F}}$ is unramified at

such l. We have $b(I_p) = 0$ by the equality (6.2) and hence $N_\infty/\mathbb{Q}(\mu_{Np^\infty})$ is also unramified at p.

Let $L_\infty^{(N)}$ be the maximal abelian p-extension of $\mathbb{Q}(\mu_{Np^\infty})$ which is unramified outside N. Let us take a prime $l|N$ and we denote by $L_\infty^{(l)}$ the maximal subfield of $L_\infty^{(N)}$ which is unramified at l. We denote by $K_r = \mathbb{Q}\left(Np^{r+1}\right)$ and by $K_{r,\mathfrak{l}}$ the completion of K_r at a prime $\mathfrak{l}$ dividing l with $\mathcal{O}_{r,\mathfrak{l}}$ its ring of integers. Then there exists an surjective homomorphism

$$\varprojlim_r \prod_{\mathfrak{l}|l} \mathcal{O}_{r,\mathfrak{l}}^\times \twoheadrightarrow \mathrm{Gal}\left(L_\infty^{(N)}/L_\infty^{(l)}\right) \tag{6.4}$$

by class field theory. Note that $L_\infty^{(N)}/L_\infty^{(l)}$ is a p-extension, then the homomorphism (6.4) induces the following surjective homomorphism:

$$\varprojlim_r \prod_{\mathfrak{l}|l} \mathbb{F}_{r,\mathfrak{l}}^\times \twoheadrightarrow \mathrm{Gal}\left(L_\infty^{(N)}/L_\infty^{(l)}\right), \tag{6.5}$$

where $\mathbb{F}_{r,\mathfrak{l}}$ is the residue field of $\mathcal{O}_{r,\mathfrak{l}}$. Now I_l acts trivially on $\varprojlim_r \prod_{\mathfrak{l}|l} \mathbb{F}_{r,\mathfrak{l}}^\times$, hence

$$\mathrm{Gal}\left(L_\infty^{(N)}/L_\infty^{(l)}\right)^{\chi_1\chi_2^{-1}} = \{0\}$$

because we have $\chi_1\chi_2^{-1}$ has conductor divisible by N under the assumptions (Co-prime) and (Conductor). Thus the extension $N_\infty/\mathbb{Q}(\mu_{Np^\infty})$ is also unramified at the primes dividing N.

Step 5 We fix the Iwasawa-Serre isomorphism as follows:

$$\mathbb{Z}_p[\chi_1\chi_2^{-1}][[\mathrm{Gal}\left(\mathbb{Q}\left(\mu_{Np^\infty}\right)/\mathbb{Q}\left(\mu_{Np}\right)\right)]] \xrightarrow{\sim} \Lambda_{\chi_1\chi_2^{-1}}, \tilde{\gamma} \mapsto u^{-1}(1+X)^{-1}. \tag{6.6}$$

Then we have the following $\mathbb{I}$-homomorphisms:

$$X_\infty^{\chi_1\chi_2^{-1}} \otimes_{\Lambda_{\chi_1\chi_2^{-1}}} \mathbb{I} \twoheadrightarrow \overline{b}(G) \otimes_{\Lambda_{\chi_1\chi_2^{-1}}} \mathbb{I} \xrightarrow{\sim} B/I(\rho_{\mathcal{F}})B. \tag{6.7}$$

By (1)-(3) of Proposition 4.3.1, we have the following inclusion relation of Fitting ideals:

$$\mathrm{Fitt}_{\Lambda_{\chi_1\chi_2^{-1}}}(X_\infty^{\chi_1\chi_2^{-1}})\mathbb{I} = \mathrm{Fitt}_{\mathbb{I}}(X_\infty^{\chi_1\chi_2^{-1}} \otimes_{\Lambda_{\chi_1\chi_2^{-1}}} \mathbb{I}) \subset \mathrm{Fitt}_{\mathbb{I}}(B/I(\rho_{\mathcal{F}})B) \subset I(\rho_{\mathcal{F}}).$$

By the Iwasawa main conjecture (Theorem of Mazur-Wiles cf. Theorem 4.3.4) we have

$$\mathrm{Fitt}_{\Lambda_{\chi_1\chi_2^{-1}}}(X_\infty^{\chi_1\chi_2^{-1}}) = \mathcal{L}_p(\chi_1^{-1}\chi_2)\Lambda_{\chi_1\chi_2^{-1}}.$$

Thus $\mathcal{L}_p(\chi_1^{-1}\chi_2)\mathbb{I} \subset I(\rho_{\mathcal{F}})$. This completes the proof of (1) of the proposition.

(2) Similarly, we denote by $M_\infty^{(Np)}$ the abelian extension of $\mathbb{Q}\left(\mu_{Np^\infty}\right)$ corresponding to

$$\mathrm{Ker}\left(\overline{c} : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\left(\mu_{Np^\infty}\right)\right) \to C/I\left(\rho_{\mathcal{F}}\right)C,\ g \mapsto \overline{c}(g)\right)$$

and by $H = \mathrm{Gal}\left(M_\infty^{(Np)}/\mathbb{Q}\left(\mu_{Np^\infty}\right)\right)$. Then $\overline{c}(H)$ is a $\Lambda_{\chi_1^{-1}\chi_2}$-module under the surjection

$$\mathbb{Z}_p[[\mathrm{Gal}\left(\mathbb{Q}\left(\mu_{Np^\infty}\right)/\mathbb{Q}\right)]] \xrightarrow{\chi_1^{-1}\chi_2\kappa_{\mathrm{cyc}}\kappa_{\mathrm{univ}}} \Lambda_{\chi_1\chi_2^{-1}},\ u^{-1}\tilde{\gamma} \mapsto 1+X$$

and the map $\overline{c}(H) \otimes_{\Lambda_{\chi_1^{-1}\chi_2}} \mathbb{I} \to C/I(\rho_{\mathcal{F}})C$ induced by $\overline{c}$ is an isomorphism by the same arguments as in **Step 3**. Hence we have the surjective homomorphism as follows:

$$Y_{\infty}^{\chi_1^{-1}\chi_2} \otimes_{\Lambda_{\chi_1^{-1}\chi_2}} \mathbb{I} \twoheadrightarrow C/I(\rho_{\mathcal{F}})C. \tag{6.8}$$

Note that in the equality (6.8), we endowed $Y_{\infty}^{\chi_1^{-1}\chi_2}$ with the $\Lambda_{\chi_1\chi_2^{-1}}$-module structure under the isomorphism as follows:

$$\mathbb{Z}_p[\chi_1^{-1}\chi_2][[\mathrm{Gal}\left(\mathbb{Q}\left(\mu_{Np^{\infty}}\right)/\mathbb{Q}\left(\mu_{Np}\right)\right)]] \xrightarrow{\sim} \Lambda_{\chi_1^{-1}\chi_2}, \tilde{\gamma} \mapsto u(1+X).$$

By the equalitys (6.7) and (6.8), there exists a $g_B \in X_{\infty}$ (resp. $g_C \in Y_{\infty}$) such that $B/I(\rho_{\mathcal{F}})B$ (resp. $C/I(\rho_{\mathcal{F}})C$) is generated by $\overline{b}(g_B)$ (resp. $\overline{c}(g_C)$). By Nakayama's lemma, B (resp. C) is generated by $b(g_B)$ (resp. $c(g_C)$) over $\mathbb{I}$. This implies $I(\rho_{\mathcal{F}}) = BC = (b(g_B)\, c(g_C))$.

□

Define the Eisenstein ideal $I(\chi, \mathbb{I})$ the ideal of $h^{\mathrm{ord}}(\chi, \mathbb{I})$ which is generated by $T(l) - 1 - \chi(l)\langle l\rangle (1+X)^{s_l}$ for all primes $l \neq p$ and $T(p) - 1$.

Corollary 6.2.4. Let the assumptions and the notations be as in Theorem 1.3.1. Assume the condition (Rank one). We have $I(\rho_{\mathcal{F}}) = \mathcal{L}_p(\chi)\mathbb{I}$.

Proof. We have $\chi_1 = \mathbf{1}$ by Lemma 6.2.2 and hence $\mathcal{L}_p(\chi)\mathbb{I} \subset I(\rho_{\mathcal{F}})$ by Proposition 6.2.3. Thus it is suffices to prove $I(\rho_{\mathcal{F}}) \subset \mathcal{L}_p(\chi)\mathbb{I}$.

Since $h^{\mathrm{ord}}(\chi, \mathbb{I}) = h^{\mathrm{ord}}(\chi, \Lambda_{\chi}) \otimes_{\Lambda_{\chi}} \mathbb{I}$, $h^{\mathrm{ord}}(\chi, \mathbb{I})$ is isomorphic to $\mathbb{I}$ by the assumption (Rank one). Since $N = 1$, $I(\rho_{\mathcal{F}})$ is generated by $a(l, \mathcal{F}) - 1 - \chi(l)\langle l\rangle (1+X)^{s_l}$ for all primes $l \neq p$ by Lemma 6.2.2 and Theorem 2.5.9. We also have $c(p, \mathcal{F}) - 1 = \varepsilon_1(\mathrm{Frob}_p) - 1 = a(\mathrm{Frob}_p) - 1 \in I(\rho_{\mathcal{F}})$ by Theorem 5.4.9 and Lemma 6.2.2. Thus the canonical isomorphism $\mathbb{I} \to h^{\mathrm{ord}}(\chi, \mathbb{I})$ sends $I(\rho_{\mathcal{F}})$ to the Eisenstein ideal $I(\chi, \mathbb{I})$. On the other hand, the canonical homomorphism

$$\mathbb{I} \Big/ \mathcal{L}_p(\chi)\mathbb{I} \to h^{\mathrm{ord}}(\chi, \mathbb{I}) \Big/ (I(\chi, \mathbb{I}), \mathcal{L}_p(\chi))$$

is an isomorphism by [Wi2, Theorem 4.1]. This implies $I(\rho_{\mathcal{F}}) \subset \mathcal{L}_p(\chi)\mathbb{I}$.

□

The next corollary is obviously deduced from (2) of Proposition 6.2.3.

Corollary 6.2.5. Let the assumptions and the notations be as in Theorem 1.3.1. Assume the conditions (Cyclic) and (Prime ideal). We have $I(\rho_{\mathcal{F}}) = \mathcal{L}_p\left(\chi_1^{-1}\chi_2\right)\mathbb{I}$.

Now we prove Theorem 1.3.1.

Proof of Theorem 1.3.1. For any $\varphi \in \mathfrak{X}_{\mathrm{arith}}(\mathbb{I})$, let ϖ_{φ} be a fixed uniformizer of $\varphi(\mathbb{I})$. Then

$$\mathrm{ord}_{\varpi_{\varphi}}(\varphi(I(\rho_{\mathcal{F}})) \leq \mathrm{ord}_{\varpi_{\varphi}}\left(\varphi\left(\mathcal{L}_p(\chi_1^{-1}\chi_2)\right)\right) \tag{6.9}$$

by (1) of Proposition 6.2.3. Under the assumption that $\chi_1 \neq \chi_2\omega$, we have

$$\varphi\left(\mathcal{L}_p(\chi_1^{-1}\chi_2)\right) = L_p(1 - k_{\varphi}, \chi_1^{-1}\chi_2\psi_{\varphi}\omega) \tag{6.10}$$

by Theorem 4.2.1. Furthermore, we have

$$\mathrm{ord}_{\varpi_\varphi}(\varphi(I(\rho_{\mathcal{F}}))) + 1 = \sharp\mathscr{L}(\rho_{f_\varphi}), \tag{6.11}$$

by combining Proposition 6.1.4 and Lemma 6.2.1. Combine the inequality (6.9) and the equalities (6.10), (6.11), we have the following inequality:

$$\sharp\mathscr{L}(\rho_{f_\varphi}) \leq \mathrm{ord}_{\varpi_\varphi}\left(L_p(1-k_\varphi, \chi_1^{-1}\chi_2\psi_\varphi\omega)\right) + 1. \tag{6.12}$$

If we assume the condition (Rank one) or both of the conditions (Cyclic) and (Prime ideal), we have $I(\rho_{\mathcal{F}}) = \mathcal{L}_p(\chi_1^{-1}\chi_2)\mathbb{I}$ by Corollary 6.2.4 and Corollary 6.2.5. Thus the inequality (6.12) becomes equal. Specially when (Rank one) satisfied, $\chi_1 = 1$ and $\chi_2 = \chi$ by Lemma 6.2.2. This completes the proof of Theorem 1.3.1.

6.3 Proof of Corollary 1.3.2 and Corollary 1.3.3

We prove Corollary 1.3.2 and Corollary 1.3.3 by calculating the order of the integral values of Kubota-Leopoldt p-adic L-function in this section. The following lemma is useful to our calculation:

Lemma 6.3.1. Let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbb{Q}_p$ and $F(X) \in \mathcal{O}[X]$ a distinguished polynomial. Then there exists an integer $r \in \mathbb{Z}_{\geq 0}$ such that for any $(k, \zeta) \in \mathbb{Z}_{\geq 0} \times (\mu_{p^\infty} \setminus \mu_{p^r})$,

$$\mathrm{ord}_p\left(F\left(\zeta u^k - 1\right)\right) = \frac{\deg F(X)}{(p-1)\, p^{r_\zeta - 1}},$$

where r_ζ is the order of ζ.

Proof. Decompose

$$F(X) = \prod_{i=1}^{n}(X - \alpha_i)$$

and choose an integer $r \geq 0$ such that $\mathrm{ord}_p(\alpha_i) > \dfrac{1}{(p-1)p^{r-1}}$ for all α_i. Then for any $(k, \zeta) \in \mathbb{Z}_{\geq 0} \times (\mu_{p^\infty} \setminus \mu_{p^r})$, we have the following equality:

$$\begin{aligned}\mathrm{ord}_p(\zeta u^k - 1 - \alpha_i) &= \mathrm{ord}_p\left(\zeta\left(\exp\left(k \cdot \log(u)\right) - 1\right) + (\zeta - 1) - \alpha_i\right) \\ &= \frac{1}{(p-1)p^{r_\zeta - 1}},\end{aligned}$$

where exp and log are the p-adic exponential and logarithm functions. Thus we have the following equality:

$$\mathrm{ord}_p\left(F\left(\zeta u^k - 1\right)\right) = \sum_{i=1}^{n}\mathrm{ord}_p(\zeta u^k - 1 - \alpha_i) = \frac{\deg F(X)}{(p-1)\, p^{r_\zeta - 1}}.$$

□

Let us return to the proof of Corollary 1.3.2.

Proof of Corollary 1.3.2. First we prove (1) of Corollary 1.3.2. By (1) of Theorem 1.3.1, it is sufficient to show that there exists an $r \in \mathbb{Z}_{\geq 0}$ such that

$$\mathrm{ord}_{\varpi_\varphi}(L_p(1-k_\varphi, \chi_1^{-1}\chi_2\psi_\varphi\omega)) \leq \mathrm{rank}_{\Lambda_\chi}\mathbb{I} \cdot \mathrm{deg}\mathcal{L}_p^*\left(\chi_1^{-1}\chi_2\right)$$

for any $\varphi \in \mathfrak{X}_{\mathrm{arith}}^{(>r)}(\mathbb{I})$. Since $\mathcal{L}_p(\chi_1^{-1}\chi_2)$ is not divisible by a uniformizer of $\mathbb{Z}_p[\chi_1^{-1}\chi_2]$ by Theorem 4.2.6, the Weierstrass preparation theorem enables one to decompose

$$\mathcal{L}_p(\chi_1^{-1}\chi_2) = \mathcal{L}_p^*\left(\chi_1^{-1}\chi_2\right)\mathcal{U},$$

where $\mathcal{L}_p^*\left(\chi_1^{-1}\chi_2\right)$ is a distinguished polynomial and $\mathcal{U}$ a unit in $\Lambda_{\chi_1^{-1}\chi_2}$. We apply Lemma 6.3.1 to $\mathcal{L}_p^*\left(\chi_1^{-1}\chi_2\right)$. Then there exists an integer $r \in \mathbb{Z}_{\geq 0}$ such that

$$\mathrm{ord}_p\left(\varphi\left(\mathcal{L}_p^*\left(\chi_1^{-1}\chi_2\right)\right)\right) = \frac{\mathrm{deg}\mathcal{L}_p^*\left(\chi_1^{-1}\chi_2\right)}{(p-1)\,p^{r_\varphi-1}} \tag{6.13}$$

for any $\varphi \in \mathfrak{X}_{\mathrm{arith}}^{(>r)}(\mathbb{I})$.

Let us take an element $\varphi \in \mathfrak{X}_{\mathrm{arith}}^{(>r)}(\mathbb{I})$ and consider the extension of the discrete valuation rings $\varphi(\mathbb{I}) \supset \mathbb{Z}_p[\chi][\zeta_\varphi]$. Since $[\mathrm{Frac}(\varphi(\mathbb{I})) : \mathrm{Frac}(\mathbb{Z}_p[\chi][\zeta_\varphi])] \leq \mathrm{rank}_{\Lambda_\chi}\mathbb{I}$, so is the ramification index e_φ. Under the assumption $p \nmid \phi(N)$, the extension of p-adic fields $\mathbb{Q}_p(\chi)/\mathbb{Q}_p$ is unramified. Thus the ramification index in the extension $\mathbb{Z}_p[\chi][\zeta_\varphi] \supset \mathbb{Z}_p$ is $(p-1)\,p^{r_\varphi-1}$. Then by the equality (6.13), we have

$$\begin{aligned}
\mathrm{ord}_{\varpi_\varphi}(L_p(1-k_\varphi, \chi_1^{-1}\chi_2\psi_\varphi\omega)) &= \mathrm{ord}_{\varpi_\varphi}\left(\varphi\left(\mathcal{L}_p^*\left(\chi_1^{-1}\chi_2\right)\right)\right) \\
&= e_\varphi(p-1)p^{r_\varphi-1}\frac{\mathrm{deg}\mathcal{L}_p^*\left(\chi_1^{-1}\chi_2\right)}{(p-1)\,p^{r_\varphi-1}} \\
&= e_\varphi \mathrm{deg}\mathcal{L}_p^*\left(\chi_1^{-1}\chi_2\right) \\
&\leq \mathrm{rank}_{\Lambda_\chi}\mathbb{I} \cdot \mathrm{deg}\hat{G}^*_{\chi_1^{-1}\chi_2}(X).
\end{aligned}$$

This completes the proof of (1) of Corollary 1.3.2 and (2) is easily deduced from (1).

Now we prove (3) of Corollary 1.3.2. Assume that $\mathbb{I}$ is isomorphic to $\mathcal{O}[[X]]$ with $\mathcal{O}$ the ring of integers of a finite extension K of $\mathbb{Q}_p$. Let $f_1(X), \cdots, f_m(X)$ be the generators of $I(\rho_\mathcal{F})$.

(r_1) For each $i = 1, \cdots, m$, decompose

$$f_i(X) = \varpi^{\mu_i}P_i(X)U_i(X),$$

where $P_i(X)$ is a distinguished polynomial and $U_i(X)$ a unit in $\mathcal{O}[[X]]$. Let

$$F(X) = \prod_{i=1}^{m} P_i(X).$$

We apply Lemma 6.3.1 to $F(X)$. Then there exists an integer $r_1 \in \mathbb{Z}_{\geq 0}$ such that

$$\mathrm{ord}_p\varphi(f_i(X)) = \mu_i \mathrm{ord}_p\varpi + \frac{\mathrm{deg}P_i(X)}{(p-1)p^{r_\varphi-1}} \tag{6.14}$$

for any $\varphi \in \mathfrak{X}_{\mathrm{arith}}^{(>r_1)}(\mathbb{I})$.

(r_2) We denote by ζ_m a primitive m-th root of unity for an integer $m > 0$. We denote by r_2 the following integer:

$$r_2 = \max\{\, j \in \mathbb{Z}_{\geq 0} \mid \zeta_{p^j} \in K \,\}.$$

Let us take an element $\varphi \in \mathfrak{X}_{\mathrm{arith}}^{(>r_2)}(\mathbb{I})$. Write $K_\varphi = \mathrm{Frac}(\varphi(\mathbb{I}))$ for short. First we assume $r_2 > 0$. Then we have $K \cap \mathbb{Q}_p(\zeta_\varphi) = \mathbb{Q}_p(\zeta_{p^{r_2}})$ and $\mathrm{Gal}(K_\varphi/\mathbb{Q}_p(\zeta_\varphi)) \xrightarrow{\sim} \mathrm{Gal}(K/\mathbb{Q}_p(\zeta_{p^{r_2}}))$. Since $\mathbb{I}$ is isomorphic to $\mathcal{O}[[X]]$, the residue degree of the extensions $K_\varphi/\mathbb{Q}_p(\zeta_\varphi)$ and $K/\mathbb{Q}_p(\zeta_{p^{r_2}})$ coincide, so are the ramification index. Hence the ramification index of K_φ over $\mathbb{Q}_p$ is $e(p-1)p^{r_\varphi - 1}$, where e is the ramification index of K over $\mathbb{Q}_p(\zeta_{p^{r_2}})$. If $r_2 = 0$, we may enlarge $\mathcal{O}$ to $\mathcal{O}' = \mathcal{O}[\zeta_p]$ since $\mathcal{O}[\zeta_\varphi] = \mathcal{O}'[\zeta_\varphi]$ for $\varphi \in \mathfrak{X}_{\mathrm{arith}}^{(>r_2)}(\mathbb{I})$. Then the argument above also holds, i.e. there exists a constant e such that the ramification index of K_φ over $\mathbb{Q}_p$ is $e(p-1)p^{r_\varphi - 1}$. Note that e is the ramification index of $K(\zeta_p)/\mathbb{Q}_p(\zeta_p)$ if $r_2 = 0$.

(r_3) Since $\mathcal{L}_p(\chi_1^{-1}\chi_2)\mathbb{I} \subset I(\rho_{\mathcal{F}})$ and $\varpi \nmid \mathcal{L}_p(\chi_1^{-1}\chi_2)$, we have the following set

$$\mathcal{Z} = \{\, i = 1, \cdots, m \mid \mu_i = 0 \,\}$$

is nonempty. Let

$$l = \min\{\, \mathrm{deg}P_i(X) \mid i \in \mathcal{Z} \,\}$$

and let us take an integer $r_3 \in \mathbb{Z}_{\geq 0}$ such that

$$(p-1)p^{r_3 - 1}\mu_i \mathrm{ord}_p\varpi + \mathrm{deg}P_i(X) \geq l. \tag{6.15}$$

for any $i \notin \mathcal{Z}$.

Let $r' = \max\{\, r_1, r_2, r_3 \,\}$ and let us take a $\varphi \in \mathfrak{X}_{\mathrm{arith}}^{(>r')}(\mathbb{I})$. Then we have the following equality:

$$\sharp\mathscr{L}(\rho_{f_\varphi}) = \min\{\, \mathrm{ord}_{\varpi_\varphi}\varphi(f_i(X)) \mid 1 \leq i \leq n \,\} + 1. \tag{6.16}$$

Since the ramification index of K_φ over $\mathbb{Q}_p$ is $e(p-1)p^{r_\varphi - 1}$, we have

$$\mathrm{ord}_{\varpi_\varphi}\varphi(f_i(X)) = e(p-1)p^{r_\varphi - 1}\mu_i \mathrm{ord}_p\varpi + e \cdot \mathrm{deg}P_i(X) \tag{6.17}$$

for each $1 \leq i \leq n$ by the equality (6.14). Thus

$$\min\{\, \mathrm{ord}_{\varpi_\varphi}\varphi(f_i(X)) \mid 1 \leq i \leq n \,\} = el \tag{6.18}$$

by the equality (6.15). Combine the equalities (6.16) and (6.18), we have that $\sharp\mathscr{L}(\rho_{f_\varphi}) = el + 1$ is constant. This completes the proof of Corollary 1.3.2.

Proof of Corollary 1.3.3. Now we assume the condition (Rank one) or both of the conditions (Cyclic) and (Prime ideal). We have $\sharp\mathscr{L}(\rho_{f_\varphi}) = \mathrm{ord}_{\varpi_\varphi}\left(L_p\left(1 - k_\varphi, \chi_1^{-1}\chi_2\psi_\varphi\omega\right)\right) + 1$ by (2) and (3) of Theorem 1.3.1. We fix a $\zeta \in \mu_{p^\infty}$. First we assume that $L_p(1-s, \chi_1^{-1}\chi_2\psi_\zeta\omega)$ has a zero $s_0 \in \mathbb{Z}_p$. Let $\{k_n\}$ be the sequence defined as follows:

(i) $k_n = s_0 + p^n$ if $s_0 \in \mathbb{Z}$,

(ii) $k_n = \displaystyle\sum_{i=0}^{n} a_i p^i$ if $s_0 = \sum_{i=0}^{\infty} a_i p^i$ such that $0 \leq a_i \leq p-1$ and $s_0 \notin \mathbb{Z}$.

Then $\sharp\mathscr{L}(\rho_{f_\varphi})$ is unbounded when k_φ runs over the sequence $\{k_n\}$.

Assume $L_p\left(1-s,\chi_1^{-1}\chi_2\psi_\zeta\omega\right)$ has no zero in $\mathbb{Z}_p$ and we show $\mathrm{ord}_{\varpi_\varphi}\left(L_p\left(1-k_\varphi,\chi_1^{-1}\chi_2\psi_\zeta\omega\right)\right)$ is bounded by contradiction. Suppose that $\mathrm{ord}_{\varpi_\varphi}\left(L_p\left(1-k_\varphi,\chi_1^{-1}\chi_2\psi_\zeta\omega\right)\right)$ is unbounded. Then there exists a sequence $\{k_n\}$ such that $k_n\geq 2$ and

$$\lim_{n\to\infty} L_p\left(1-k_n,\chi_1^{-1}\chi_2\psi_\zeta\omega\right)=0.$$

Since $\mathbb{Z}_p$ is compact and L_p is a continuous function, $L_p\left(s,\chi_1^{-1}\chi_2\psi_\zeta\omega\right)$ must have zero in $\mathbb{Z}_p$. This contradicts to our assumption and hence $\sharp\mathscr{L}(\rho_{f_\varphi})$ is bounded. This completes the proof of Corollary 1.3.3.

6.4 Proof of Corollary 1.3.4

We denote by $\mathbb{F}$ the residue field $\mathbb{I}/\mathfrak{m}$. The following lemma is a generalization of the arguments in [Maz, Appendix I] for more general settings.

Lemma 6.4.1. Let the assumptions and the notations be as in Theoren 1.3.1. Assume the conditions (Co-prime), (Cyclic), (Prime ideal) and (Free lattice). Let $\mathbb{T}$ be a $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$-stable lattice which is free over $\mathbb{I}$. Then $\mathbb{T}\otimes_{\mathbb{I}}\varphi(\mathbb{I})$ is a mod ϖ_φ not semi-simple lattice for any $\varphi\in\mathfrak{X}_{\mathrm{arith}}(\mathbb{I})$.

Proof. We have $I(\rho_{\mathcal{F}})=\mathcal{L}_p(\chi_1^{-1}\chi_2)\mathbb{I}$ under the conditions (Co-prime), (Cyclic) and (Prime ideal) by Corollary 6.2.5. Let us take a $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$-stable lattice $\mathbb{T}\cong\mathbb{I}^{\oplus 2}$ and we consider the following representation:

$$\rho=\rho_{\mathcal{F},\mathbb{T}}:\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)\to\mathrm{GL}_2(\mathbb{I}).$$

The condition (Prime ideal) enables us to define $\mathrm{Frac}\left(\mathbb{I}/\mathcal{L}_p(\chi_1^{-1}\chi_2)\mathbb{I}\right)$ and $\mathrm{Frac}\left(\mathbb{I}/\mathcal{L}_p(\chi_1^{-1}\chi_2)\mathbb{I}\right)$ is of characteristic zero by Theorem 4.2.6. We denote by $\rho \bmod \mathcal{L}_p(\chi_1^{-1}\chi_2)\mathbb{I}$ the representation as follows:

$$\rho \bmod \mathcal{L}_p(\chi_1^{-1}\chi_2)\mathbb{I}:\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)\xrightarrow{\rho}\mathrm{GL}_2(\mathbb{I})\overset{\bmod\ \mathcal{L}_p(\chi_1^{-1}\chi_2)\mathbb{I}}{\longrightarrow}\mathrm{GL}_2\left(\mathbb{I}/\mathcal{L}_p(\chi_1^{-1}\chi_2)\mathbb{I}\right).$$

Since $\mathrm{tr}\rho \bmod \mathcal{L}_p(\chi_1^{-1}\chi_2)\mathbb{I}$ is the sum of two characters, we have $\rho \bmod \mathcal{L}_p(\chi_1^{-1}\chi_2)\mathbb{I}$ is reducible by the Theorem 2.3.3. Let $\{v_1,v_2\}$ be a basis corresponding to $\rho \bmod \mathcal{L}_p(\chi_1^{-1}\chi_2)\mathbb{I}$ such that $\left(\mathbb{I}/\mathcal{L}_p(\chi_1^{-1}\chi_2)\mathbb{I}\right)v_1$ is stable under $\rho \bmod \mathcal{L}_p(\chi_1^{-1}\chi_2)\mathbb{I}$. Let $\tilde{v}_i\in\mathbb{T}$ be a lift of v_i $(i=1,2)$ and $\mathbb{M}=\mathbb{I}\tilde{v}_1\oplus\mathbb{I}\tilde{v}_2$. Then by the following commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{M} & \xrightarrow{\iota} & \mathbb{T} & \longrightarrow & \mathrm{Coker}(\iota) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle\times\mathcal{L}_p(\chi_1^{-1}\chi_2)} & & \downarrow{\scriptstyle\times\mathcal{L}_p(\chi_1^{-1}\chi_2)} & & \downarrow{\scriptstyle\times\mathcal{L}_p(\chi_1^{-1}\chi_2)} & & \\
0 & \longrightarrow & \mathbb{M} & \xrightarrow{\iota} & \mathbb{T} & \longrightarrow & \mathrm{Coker}(\iota) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \mathbb{M}/\mathcal{L}_p(\chi_1^{-1}\chi_2)\mathbb{M} & \xrightarrow{\sim} & \mathbb{M}/\mathcal{L}_p(\chi_1^{-1}\chi_2)\mathbb{M} & \longrightarrow & \mathrm{Coker}(\iota)/\mathcal{L}_p(\chi_1^{-1}\chi_2)\mathrm{Coker}(\iota), & &
\end{array}$$

we have $\mathrm{Coker}(\iota)=0$ by Nakayama's lemma and hence $\mathbb{T}=\mathbb{I}\tilde{v}_1\oplus\mathbb{I}\tilde{v}_2$. Since $\left(\mathbb{I}/\mathcal{L}_p(\chi_1^{-1}\chi_2)\mathbb{I}\right)v_1$ is stable under $\rho \bmod \mathcal{L}_p(\chi_1^{-1}\chi_2)\mathbb{I}$, we have that $\mathbb{T}'=\mathbb{I}\tilde{v}_1\oplus\mathcal{L}_p(\chi_1^{-1}\chi_2)\mathbb{I}\tilde{v}_2$ is also a $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$-stable $\mathbb{I}$-free lattice and $\mathbb{T}/\mathbb{T}'\cong\mathbb{I}/\mathcal{L}_p(\chi_1^{-1}\chi_2)\mathbb{I}$.

For any $\varphi \in \mathfrak{X}_{\mathrm{arith}}(\mathbb{I})$, we denote by T and T' the $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$-stable lattice $\mathbb{T} \otimes_{\mathbb{I}} \varphi(\mathbb{I})$ and $\mathbb{T}' \otimes_{\mathbb{I}} \varphi(\mathbb{I})$ respectively. Let $\sharp\mathscr{L}(\rho_{f_\varphi}) = n+1$. Since $I(\rho_{\mathcal{F}}) = \mathcal{L}_p(\chi_1^{-1}\chi_2)\mathbb{I}$, we have the following isomorphism:

$$T/T' = \mathbb{T} \otimes_{\mathbb{I}} \varphi(\mathbb{I}) \Big/ \mathbb{T}' \otimes_{\mathbb{I}} \varphi(\mathbb{I}) \xrightarrow{\sim} (\mathbb{T}/\mathbb{T}') \otimes_{\mathbb{I}} \varphi(\mathbb{I}) \xrightarrow{\sim} \left(\mathbb{I}/\mathcal{L}_p(\chi_1^{-1}\chi_2)\mathbb{I}\right) \otimes_{\mathbb{I}} \varphi(\mathbb{I}) \xrightarrow{\sim} \varphi(\mathbb{I})/(\varpi_\varphi)^n.$$

Thus $d([T],[T']) = n$ by Proposition 3.2.6. We have $\sharp\mathscr{L}\left(\rho_{f_\varphi}\right) = \sharp\mathscr{C}\left(\rho_{f_\varphi}\right)$ Proposition 6.1.4. Furthermore we have $\mathscr{C}\left(\rho_{f_\varphi}\right)$ is a segment by the proof of Proposition 3.3.1. Thus $[T]$ has exactly one neighbor in $\mathscr{L}\left(\rho_{f_\varphi}\right)$. This implies that T is a mod ϖ_φ not semi-simple $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$-stable lattice by (3) of Proposition 3.3.5.

□

Under the above preparation, we return to the proof of Corollary 1.3.4.

Proof of Corollary 1.3.4. Let us take an integer $l \in \mathbb{Z}_{>0}$. By Corollary 1.3.3 we know that there exists an arithmetic specialization $\varphi \in \mathfrak{X}_{\mathbb{I},\zeta}$ such that $\sharp\mathscr{L}(\rho_{f_\varphi}) = n+1 > l$

Now we the above element φ and we denote by $\mathcal{P} = \mathrm{Ker}\,\varphi$. Let $\mathbb{T}$ be the $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$-stable lattice with which (Free lattice) holds. We denote by $T = \mathbb{T} \otimes \varphi(\mathbb{I})$ and let

$$\pi : \mathbb{T} \twoheadrightarrow \mathbb{T} \otimes \varphi(\mathbb{I}) = T$$

be the reduction map. We have T is mod ϖ_φ not semi-simple by Lemma 6.4.1. Let

$$\mathscr{L}\left(\rho_{f_\varphi}\right) = \{\,[T],[T_1],\cdots,[T_n]\,\}$$

such that for any $1 \leq i \leq n$, $T/T_i \cong \varphi(\mathbb{I})/(\varpi_\varphi)^i$ as a $\varphi(\mathbb{I})$-module. We denote by $\mathbb{T}_i = \pi^{-1}(T_i)$. Since $\mathcal{P}\mathbb{T} \subset \mathbb{T}_i \subset \mathbb{T}$, we have that $\mathbb{T}_i$ is a lattice. By the definition of $\mathbb{T}_i$ we have that $\mathbb{T}_i$ is stable under the action of $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$. Thus we have the following chain of $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$-stable $\mathbb{I}$-lattices

$$\mathbb{T} \supset \mathbb{T}_1 \supset \cdots \supset \mathbb{T}_n.$$

For $i \neq j$, if there exists an $\mathbb{I}[\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)]$-isomorphism $\Xi : \mathbb{T}_i \xrightarrow{\sim} \mathbb{T}_j$, then Ξ induces a $\varphi(\mathbb{I})[\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)]$-isomorphism

$$T_i \xrightarrow{\sim} T_j, v \otimes 1 \mapsto \Xi(v) \otimes 1$$

in $\mathbb{T} \otimes_{\mathbb{I}} \varphi(\mathbb{I})$. For $i \neq j$, we have that T_i and T_j are non-isomorphic by Proposition 6.1.4. This contradicts to our assumption and hence $\mathbb{T}_i$ and $\mathbb{T}_j$ are non-isomorphic to each other. This implies that $\sharp\mathscr{L}(\rho_{\mathcal{F}}) \geq n+1 > m$ and completes the proof of Corollary 1.3.4.

Remark 6.4.2. Corollary 1.3.4 is also satisfied if we assume the conditions (Co-prime), (Rank one), (Prime ideal) and (Free lattice) obviously.

6.5 Examples

We give two examples at the end of this paper. Let (p, k_0) be the irregular pair i.e. p divides the numerator of the k_0-th Bernoulli number B_{k_0}. We give two examples as follows:

1. $(p, k_0) = (691, 12)$. Let $\Delta \in S_{12}(\mathrm{SL}_2(\mathbb{Z}))$ be the Ramanujan's cuspform. Since $\dim_{\mathbb{C}} S_{12}(\mathrm{SL}_2(\mathbb{Z})) = 1$, there exists an unique Λ-adic normalized Hecke eigen cusp form $\mathcal{F} \in S^{\mathrm{ord}}(\omega^{11}, \Lambda)$ such that for the arithmetic specialization $\varphi \in \mathfrak{X}_{\mathrm{arith}}(\Lambda)$ with $k_\varphi = 12, \zeta_\varphi = 1$,

$$\varphi(\mathcal{F}) = \Delta^*.$$

By Example 5.3.6 we know that $h^{\mathrm{ord}}(\omega^{11}, \Lambda)$ is isomorphic to Λ. Thus $I(\rho_{\mathcal{F}}) = \mathcal{L}_p(\omega^{11})\mathbb{I}$ by Corollary 6.2.4. The ideal $\left(\mathcal{L}_p(\omega^{11})\right)$ is equal to $(X - a_{\omega^{11}})$ with $a_{\omega^{11}} \in p\mathbb{Z}_p \setminus p^2\mathbb{Z}_p$ which is calculated by Iwasawa-Sims (see [Wa, §1]). Then we have the following statements:

(i) $\sharp\mathscr{L}(\rho_{f_\varphi})$ is unbounded when φ varies in $\mathfrak{X}_{\mathrm{arith}}^{(\zeta=1)}(\Lambda)$ by Corollary 1.3.3.

(ii) $\sharp\mathscr{L}(\rho_{f_\varphi}) = 2$ is constant when φ varies in $\mathfrak{X}_{\mathrm{arith}}^{(>0)}(\Lambda)$ by (1) and (3) of Corollary 1.3.2.

(iii) For each $k \geq 2$, $\sharp\mathscr{L}(\rho_{f_\varphi})$ is bounded with maximum value $\mathrm{ord}_p(L_p(1-k, \chi\omega)) + 1$ when φ varies in $\mathfrak{X}_{\mathrm{arith}}^{(k)}(\Lambda)$ by (i) and (ii).

(iv) Since $\mathbb{I} = \Lambda$ is a regular local ring, for a stable Λ-lattice $\mathbb{T}$, we have that $\mathbb{T}^{**}$ is a Λ-free lattice by (1) of Proposition 5.4.10. Hence the condition (Free lattice) is satisfied and we have $\sharp\mathscr{L}(\rho_{\mathcal{F}}) = \infty$ by Corollary 1.3.4.

Remark 6.5.1. Mazur [Maz, Appendix II] tells us that for the irregular pairs (p, k_0) with $p < 10^7$ and $k_0 < 8000$ such that $p \mid B_{k_0}$, the corresponding Hecke algebra $h^{\mathrm{ord}}(\chi, \Lambda)$ is isomorphic to Λ except for the pair $(p, k_0) = (547, 486)$. Thus we can apply Theorem 1.3.1 (2) for these pairs.

2. $(p, k_0) = (547, 486)$. By [Maz, Appendix II], there is a conjugate pair of newforms of weight 486 with the required Eisenstein congruence condition and the field which generated by the Fourier coefficients over $\mathbb{Q}_p$ is $\mathbb{Q}_p(\sqrt{-p})$ for both of them. Furthermore, the corresponding Hida Hecke algebra $h^{\mathrm{ord}}(\omega^{485}, \Lambda)$ is finite flat of rank two over Λ. We denote by $f_{486}^*, f_{486}'^*$ the corresponding cusp forms.

Let $\mathcal{F}$ (resp. $\mathcal{F}'$) be the $\mathbb{I}$-adic normalized Hecke eigen cusp form associated to f_{486}^* (resp. $f_{486}'^*$). Note that $\mathbb{I}$ is an integral closure of a quotient of $h^{\mathrm{ord}}(\omega^{484}, \Lambda)$ by a minimum prime ideal of Λ by the proof of Theorem 5.3.5. Hence $\mathrm{Frac}(\mathbb{I})$ is a quadratic extension of $\mathrm{Frac}(\Lambda)$. The ideal generated by $\left(\mathcal{L}_p(\omega^{485})\right)$ is equal to $(X - a_{\omega^{485}})$ with $a_{\omega^{485}} \in p\mathbb{Z}_p \setminus p^2\mathbb{Z}_p$ which is calculated by Iwasawa-Sims (see also [Wa, §1]). Then $\sharp\mathscr{L}(\rho_{f_\varphi}) \leq 3$ when we have φ varies in $\mathfrak{X}_{\mathrm{arith}}^{(>0)}(\mathbb{I})$ by (1) of Corollary 1.3.2. Note that the condition (Cyclic) holds for $\mathcal{F}$ (this is because the Vandiver's conjecture is true for $p = 547$), thus $I(\rho_{\mathcal{F}})$ is a principal ideal which is generated by a factor of $X - a_{\omega^{485}}$ in $\mathbb{I}$ by Corollary 6.2.5. The same holds for $\mathcal{F}'$.

Bibliography

[Be] J. Bellaïche, *Ribet's lemma, generalizations, and pseudocharacters.*, available at `http://people.brandeis.edu/~jbellaic/RibetHawaii3.pdf`.

[BC1] J. Bellaïche, G. Chenevier, *Lissité de la courbe de Hecke de GL2 aux points Eisenstein critiques.*, J. Inst. Math. Jussieu 5 (2006), no. 2, 333-349.

[BC2] J. Bellaïche, G. Chenevier, *Families of Galois representations and Selmer groups.*, Astérisque No. 324 (2009).

[BC3] J. Bellaïche, G. Chenevier, *Sous-groupes de GL_2 et arbres.*, J. Algebra 410 (2014), 501-525.

[BG] J. Bellaïche, P. Graftieaux, *Représentations sur un anneau de valuation discrète complet.*, Math. Ann. 334 (2006), no. 3, 465-488.

[Bo] N. Bourbaki, *Commutative algebra. Chapters 1-7.*, Translated from the French. Reprint of the 1989 English translation. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998.

[CR] C. Curtis, I. Reiner, *Representation theory of finite groups and associative algebras.*, Interscience, New York (1962).

[Da] S. Dalawat, *Ribet's modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$.*, Guwahati Workshop on Iwasawa Theory of Totally Real Fields, 67-81, Ramanujan Math. Soc. Lect. Notes Ser., 12, Ramanujan Math. Soc., Mysore, 2010.

[FW] B. Ferrero, L. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields.*, Ann. of Math. (2) 109 (1979), no. 2, 377-395.

[Hi1] H. Hida, *Iwasawa modules attached to congruences of cusp forms.*, Ann. Sci. cole Norm. Sup. (4) 19 (1986), no. 2, 231-273.

[Hi2] H. Hida, *Galois representations into $\mathrm{GL}_2(\mathbb{Z}_p[[X]])$ attached to ordinary cusp forms.*, Invent. Math. 85 (1986), no. 3, 545-613.

[Hi3] H. Hida, *Elementary theory of L-functions and Eisenstein series.*, London Mathematical Society Student Texts, 26. Cambridge University Press, Cambridge, 1993.

[Iw1] K. Iwasawa, *On p-adic L-functions.*, Ann. of Math. (2) 89, 1969, 198-205.

[Iw2] K. Iwasawa, *Lectures on p-adic L-functions.*, Annals of Mathematics Studies, No. 74. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1972.

[Iw3] K. Iwasawa *On $\mathbb{Z}_l$-extensions of algebraic number fields.*, Ann. of Math. (2) 98 (1973), 246-326.

[Mat] H. Matsumura, *Commutative ring theory.*, Translated from the Japanese by M. Reid. Second edition. Cambridge Studies in Advanced Mathematics, 8. Cambridge University Press, Cambridge, 1989.

[Maz] B. Mazur, *How can we construct abelian Galois extensions of basic number fields ?.*, Bull. Amer. Math. Soc. (N.S.) 48 (2011), no. 2, 155-209.

[MW1] B. Mazur, A. Wiles, *Class fields of abelian extensions of $\mathbb{Q}$.*, Invent. Math. 76 (1984), no. 2, 179-330.

[MW2] B. Mazur, A. Wiles, *On p-adic analytic families of Galois representations.*, Compositio Math. 59 (1986), no. 2, 231-264.

[MT] B. Mazur, J. Tilouine, *Représentations galoisiennes, différentielles de Kähler et "conjectures principales".* Inst. Hautes Études Sci. Publ. Math. No. 71 (1990), 65-103.

[Mi] T. Miyake, *Modular forms.*, Translated from the Japanese by Yoshitaka Maeda. Springer-Verlag, Berlin, 1989.

[NSW] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of number fields.*, Second edition. Grundlehren der Mathematischen Wissenschaften, 323. Springer-Verlag, Berlin, 2008.

[No] D. G. Northcott, *Finite free resolutions.*, Cambridge Tracts in Mathematics, No. 71. Cambridge University Press, Cambridge-New York-Melbourne, 1976.

[Nu] F. Nuccio, *Fitting ideals.*, Guwahati Workshop on Iwasawa Theory of Totally Real Fields, 8395, Ramanujan Math. Soc. Lect. Notes Ser., 12, Ramanujan Math. Soc., Mysore, 2010.

[Oc1] T. Ochiai, *The algebraic p-adic L-function and isogeny between families of Galois representations.*, J. Pure Appl. Algebra 212 (2008), no. 6, 1381-1393.

[Oc2] T. Ochiai, *Iwasawa theory and its perspective I (in Japanese)*, Iwanami Studies in Advanced Mathematics, 2014.

[Oc3] T. Ochiai, *Iwasawa theory and its perspective II (in Japanese)*, Iwanami Studies in Advanced Mathematics, 2016.

[OS] T. Ochiai, K. Shimomoto, *Bertini theorem for normality on local rings in mixed characteristic (applications to characteristic ideals).*, Nagoya Math. J. 218 (2015), 125-173.

[Ri] K. Ribet, *A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$.*, Invent. Math. 34 (1976), no. 3, 151-162.

[Se1] J. P. Serre, *Abelian l-adic representations and elliptic curves.*, With the collaboration of Willem Kuyk and John Labute. Second edition. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989.

[Se2] J. P. Serre, *Trees.*, Translated from the French original by John Stillwell. Corrected 2nd printing of the 1980 English translation. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2003.

[Sh] G. Shimura, *Introduction to the arithmetic theory of automorphic functions.*, Princeton University Press, Princeton, N.J., 1971.

[Sw1] H. P. F. Swinnerton-Dyer, *On l-adic representations and congruences for coefficients of modular forms.*, Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972), pp. 1-55. Lecture Notes in Math., Vol. 350, Springer, Berlin, 1973.

[Sw2] H. P. F. Swinnerton-Dyer, *On l-adic representations and congruences for coefficients of modular forms. II.*, Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), pp. 63-90. Lecture Notes in Math., Vol. 601, Springer, Berlin, 1977.

[Ti] J. Tilouine, *Un sous-groupe p-divisible de la jacobienne de $X_1(Np^r)$ comme module sur l'algèbre de Hecke.*, Bull. Soc. Math. France 115 (1987), no. 3, 329-360.

[Wa] S. Wagstaff, *Zeros of p-adic L-functions.*, Math. Comp. 29 (1975), no. 132, 1138-1143.

[Wi1] A. Wiles, *On ordinary λ-adic representations associated to modular forms.*, Invent. Math. 94 (1988), no. 3, 529-573.

[Wi2] A. Wiles, *The Iwasawa conjecture for totally real fields.*, Ann. of Math. (2) 131 (1990), no. 3, 493-540.

[Y] D. Yan, *Stable lattices in modular Galois representations and Hida deformation.*, Jour. of Number theory 197 (2019), 62-88.