Iwasawa Theory for Modular Forms at Supersingular Primes

Antonio Lei

Trinity College
Department of Pure Mathematics and Mathematical Statistics
University of Cambridge

Dissertation submitted to the University of Cambridge
for the degree of Doctor of Philosphy

April 2010

Declaration

The research presented in this thesis was performed in the Department of Pure Mathematics and Mathematical Statistics, Cambridge University between October 2007 and March 2010. The work contained in this thesis is original, except where explicit reference to the results of others is made. Parts of this work (Chapter 7) were performed in collaboration with Sarah Zerbes in Michaelmas term 2009 and Lent term 2010, with the exception of Proposition 7.4.5, which was joint work with David Loeffler. The proofs in this chapter are either entirely mine or those to which I have contributed. Most of the work contained in this thesis has been submitted for publication and preprints are available on the arXiv website:

- *Iwasawa Theory for Modular Forms at Supersingular Primes*,
  arXiv:0904.3938v2 [math.NT]
- *Coleman Maps for Modular Forms at Supersingular Primes over Lubin-Tate Extensions*,
  arXiv:0908.0091v2 [math.NT]
- *Wach Modules and Iwasawa Theory for Modular Forms* (with David Loeffler and Sarah Zerbes),
  arXiv:0912.1263v2 [math.NT]

This dissertation is not substantially the same as any I have submitted for a degree or diploma or other qualification.

Summary

Let $f = \sum a_n q^n$ be a normalised eigen-newform of weight $k \geq 2$ and p an odd prime which does not divide the level of f. We study a reformulation of Kato's main conjecture for f over the $\mathbb{Z}_p$-cyclotomic extension of $\mathbb{Q}$. In particular, we generalise Kobayashi's main conjecture on p-supersingular elliptic curves over $\mathbb{Q}$ with $a_p = 0$, which asserts that Pollack's p-adic L-functions generate the characteristic ideals of some $\pm$-Selmer groups which are cotorsion over the Iwasawa algebra $\Lambda = \mathbb{Z}_p[[\mathbb{Z}_p]]$.

We begin by studying the p-adic Hodge theory for the p-adic representation associated to f in the case when $a_p = 0$. It allows us to give analogous definitions of Kobayashi's $\pm$-Coleman maps and $\pm$-Selmer groups. The Coleman maps are used to show that the Pontryagin duals of these new Selmer groups are torsion over Λ as in the elliptic curve case. As a consequence, we formulate a main conjecture stating that Pollack's p-adic L-functions generate their characteristic ideals. Similar to Kobayashi's works, we prove one inclusion of the main conjecture using an Euler system constructed by Kato.

We then prove the other inclusion of the main conjecture for CM modular forms, generalising works of Pollack and Rubin on CM elliptic curves. As a key step of the proof, we generalise the reciprocity law of Coates-Wiles and Rubin.

Next, we study Wach modules associated to positive crystalline p-adic representations in general and generalise the construction of the Coleman maps. By applying this to modular forms with much more general a_p, we define two Coleman maps and decompose the classical p-adic L functions of f into linear combinations of two power series of bounded coefficients generalising works of Pollack (in the case $a_p = 0$) and Sprung (when f corresponds to an elliptic curve over $\mathbb{Q}$ with $a_p \neq 0$). Once again, this leads to a reformulation of Kato's main conjecture involving cotorsion Selmer groups and p-adic L-functions of bounded coefficients. One inclusion of this new main conjecture is proved in the same way as the $a_p = 0$ case.

Finally, we explain how the $\pm$-Coleman maps can be extended to Lubin-Tate extensions of height 1 in place of the $\mathbb{Z}_p$-cyclotomic extension. This generalises works of Iovita and Pollack for elliptic curves over $\mathbb{Q}$.

Acknowledgements

First and foremost, I offer my deepest gratitude to my supervisor, Prof Tony Scholl, without whom this thesis would not have been possible. Not only is he extremely helpful whenever I encounter any problems, but he also constantly offers me his invaluable encouragements and advice. What I have learnt from him will no doubt benefit me for the rest of my life.

I am also indebted to all the members of the Number Theory group in the University of Cambridge, with whom I have had many fruitful mathematical discussions. Tobias Berger has been a very kind mentor and has given me his great support whenever I needed it. I was lucky enough to have Alex Bartel as my officemate for the last three years. In addition to tolerating my eccentric behaviour in the office, he has been a great friend to talk to, both mathematically and personally.

I was fortunate enough to have the opportunity to work with Sarah Zerbes and David Loeffler. They have been extremely patient with me during our collaboration and helped me tremendously in understanding many aspects of p-adic Hodge theory and p-adic analysis.

I am grateful to Laurent Berger, Byoung Du Kim, Shinichi Kobayashi, Masato Kurihara, Bernadette Perrin-Riou, Robert Pollack, Karl Rubin and Ian Sprung for answering my questions and/or pointing out to me many mistakes I have made. Their works have been great inspirations for me and many results presented in this thesis rely heavily on them.

During my studies in Cambridge, I have encountered many people who have helped me in one way or another for which I am extremely thankful. I would like to thank all my undergraduate and Part III lecturers, my supervisors and my supervision partners for having taught me so much throughout the years. I would also like to thank all my friends for having supported me in so many ways: Volker, Michael, Dirk, Kris, Prim, Lilian, Peter A, Peter T, Thomas, Hao, Keith, Yuan, Mira, just to name a few.

On to my family, I am extremely grateful for having such supportive parents. They are always firmly behind me for whatever I decide to do in life. I am lucky enough to have João as my brother, as he always looks out for me and has taught me many things in life.

It is a great pleasure to be a member of Trinity College Cambridge. I have benefited hugely from their generous financial supports during both my undergraduate and my postgraduate studies. The excellent facilities in the college have made my experience in Cambridge as enjoyable as possible.

Finally, I owe all the staff in the Centre for Mathematical Sciences, Cambridge for providing such a wonderful environment to work in and to the hospitality of l'Institut Henri Poincaré during my stay in Lent term 2010 when a large part of this thesis is written.

Contents

Chapter 1

Introduction

1.1 Background

Let p be an odd prime and let G_∞ be the Galois group of the extension $\mathbb{Q}_\infty$ of $\mathbb{Q}$ by p power roots of unity. We denote by $\Lambda(G_\infty)$ the Iwasawa algebra of G_∞ over $\mathbb{Z}_p$. If Δ denotes the torsion subgroup of G_∞ and γ is a fixed topological generator of the $\mathbb{Z}_p$-part of G_∞, then $\Lambda(G_\infty) \cong \mathbb{Z}_p[\Delta][[\gamma - 1]]$.

Let E be an elliptic curve defined over $\mathbb{Q}$ which has good ordinary reduction at p. The p-adic L-function $L_{p,E} \in \mathbb{Q} \otimes \Lambda(G_\infty)$ of Mazur and Swinnerton-Dyer interpolates complex L-values of E. It is conjectured that $L_{p,E}$ is in fact an element of $\Lambda(G_\infty)$.

The p-Selmer group of E over any number field F is defined to be

$$\mathrm{Sel}_p(E/F) = \ker\left(H^1(F, E[p^\infty]) \to \prod_v \frac{H^1(F_v, E[p^\infty])}{E(F_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right),$$

where the product is taken over all places of F. If we let $\mathrm{Sel}_p(E/\mathbb{Q}_\infty) = \varinjlim \mathrm{Sel}_p(E/F)$ where F runs through the finite extensions of $\mathbb{Q}$ in $\mathbb{Q}_\infty$, then $\mathrm{Sel}_p(E/\mathbb{Q}_\infty)$ is equipped with an action of $\Lambda(G_\infty)$. It turns out that the Pontryagin dual

$$\mathrm{Sel}_p(E/\mathbb{Q}_\infty)^\vee = \mathrm{Hom}_{\mathrm{cts}}(\mathrm{Sel}_p(E/\mathbb{Q}_\infty), \mathbb{Q}_p/\mathbb{Z}_p)$$

is finitely generated over $\Lambda(G_\infty)$, and a theorem of Kato-Rohrlich (conjectured by Mazur) states that it is in fact $\Lambda(G_\infty)$-torsion. If η is a character on Δ, we can associate to the η-isotypical component of $\mathrm{Sel}_p(E/\mathbb{Q}_\infty)^\vee$ a characteristic ideal, and the main conjecture of cyclotomic Iwasawa theory for E at p asserts that this ideal is generated by the η-component of $L_{p,E}$ (written as $L^{\eta}_{p,E}$), i.e. there is a pseudo-isomorphism (a homomorphism with finite kernel and cokernel)

$$\mathrm{Sel}_p(E/\mathbb{Q}_\infty)^{\vee,\eta} \to \prod_{i=1}^{r} \mathbb{Z}_p[[\gamma-1]]/(f_i)$$

for some $f_i \in \mathbb{Z}_p[[\gamma-1]]$ such that $f_1 \cdots f_r = L^{\eta}_{p,E}$.

The construction of p-adic L-functions has been generalised to more general primes and modular forms in [AV75, MTT86]. Let $f = \sum a_n q^n$ be a normalised eigen-newform of weight $k \geq 2$, level N and character ϵ. Fix an odd prime p such that $p \nmid N$. If α is a root of $X^2 - a_p X + \epsilon(p)p^{k-1}$ such that $v_p(\alpha) < k-1$ where v_p is the p-adic valuation of $\mathbb{C}_p$ with $v_p(p) = 1$, then there exists a p-adic L-function $L_{p,\alpha}$ interpolating complex L-values of f. Perrin-Riou [PR95] has established a theory of p-adic L-functions for p-adic representations coming from motives and formulated a main conjecture for such representations. When the motive corresponds to a modular form, Perrin-Riou's main conjecture has been reformulated by Kato [Kat04] using the theory of Euler systems. If f is ordinary at p (i.e. a_p is a p-adic unit) and α is the unique unit root of the quadratic above, then $L_{p,\alpha} \in \mathbb{Q} \otimes \Lambda(G_\infty)$, and the main conjecture again asserts that $L_{p,\alpha}$ generates the characteristic ideal of $\mathrm{Sel}_p(f/\mathbb{Q}_\infty)^\vee$. In *op.cit.*, Kato has shown that $L_{p,\alpha}$ is contained in the characteristic ideal of $\mathrm{Sel}_p(f/\mathbb{Q}_\infty)^\vee$ under some technical assumptions; his proof relies on the interpolating property of an Euler system associated to f (which we refer to as the *Kato zeta elements*).

When f is supersingular at p (i.e. $p|a_p$), two problems arise: on the one hand, the p-adic L-functions obtained in [AV75, MTT86] are no longer elements of $\mathbb{Q} \otimes \Lambda(G_\infty)$ (they have unbounded coefficients), and on the other hand, $\mathrm{Sel}_p(f/\mathbb{Q}_\infty)^\vee$ is no longer $\Lambda(G_\infty)$-torsion. Perrin-Riou's (and hence Kato's) main conjecture can therefore not be translated into a statement relating $L_{p,\alpha}$ and $\mathrm{Sel}_p(f/\mathbb{Q}_\infty)$ as in the ordinary case. When $a_p = 0$, a remedy was made possible by the works of Pollack [Pol03]: If α_1 and α_2 are the roots of $X^2 + \epsilon(p)p^{k-1}$, Pollack showed that there is a decomposition

$$L_{p,\alpha_i} = \log^{+}_{p,k} L^{+}_{p,f} + \alpha_i \log^{-}_{p,k} L^{-}_{p,f}$$

for $i = 1, 2$, where $L^{\pm}_{p,f} \in \Lambda(G_\infty) \otimes \mathbb{Q}$ and $\log^{\pm}_{p,k}$ are some fixed power series which only depend on k. When f corresponds to an elliptic curve E over $\mathbb{Q}$, Kobayashi formulates a main conjecture giving an arithmetic interpretation of these new p-adic L-functions in [Kob03]. In analogy to the ordinary reduction case, he defines the plus and minus Selmer groups $\mathrm{Sel}_p^{\pm}(E/\mathbb{Q}_\infty)$ by modifying the local conditions at p in the definition of the usual Selmer group. Let T_pE be the Tate module of E. Kobayashi shows that $\mathrm{Sel}_p^{\pm}(E/\mathbb{Q}_\infty)^\vee$ is $\Lambda(G_\infty)$-torsion by defining the so-called plus and minus Coleman maps

$$\mathrm{Col}^{\pm} : H^1_{\mathrm{Iw}}(\mathbb{Q}_p, T_pE) \to \Lambda(G_\infty),$$

which construction depends on the structure of the formal group attached to E. Kobayashi's modified main conjecture then asserts that $L_{p,f}^{\pm,\eta}$ generate the respective characteristic ideals of $\mathrm{Sel}_p^{\pm}(E/\mathbb{Q}_\infty)^{\vee,\eta}$ with η as above and it is equivalent to Kato's and Perrin-Riou's main conjectures. On proving that $\mathrm{Col}^{\pm}$ send the localisation of the Kato zeta elements to $L_{p,f}^{\pm}$, Kobayashi proved one inclusion of the main conjecture as in the ordinary case. When the elliptic curve has complex multiplication, the full conjecture has been proved by Pollack and Rubin [PR04].

Sprung [Spr09] has extended the results of Pollack and Kobayashi to p-supersingular elliptic curves with $a_p \neq 0$ (which forces p to be 2 or 3). He constructed a matrix M whose entries are functions of logarithmic growth depending only on a_p such that

$$\begin{pmatrix} L_{p,\alpha} \\ L_{p,\beta} \end{pmatrix} = M \begin{pmatrix} L_p^{\vartheta} \\ L_p^{\upsilon} \end{pmatrix}$$

with $L_p^{\vartheta}, L_p^{\upsilon} \in \Lambda(G_\infty) \otimes \mathbb{Q}$. He also constructed the associated Coleman maps

$$\mathrm{Col}^{\vartheta}, \mathrm{Col}^{\upsilon} : H^1_{\mathrm{Iw}}(\mathbb{Q}_p, T_pE) \to \Lambda(G_\infty),$$

which send Kato's zeta elements to L_p^{ϑ} and L_p^{υ} respectively. Using these Coleman maps, Sprung defined two Selmer groups $\mathrm{Sel}_p^{\vartheta}(E/\mathbb{Q}_\infty)$ and $\mathrm{Sel}_p^{\upsilon}(E/\mathbb{Q}_\infty)$ and formulated the corresponding main conjectures.

1.2 Main results

The Taniyama-Shimura conjecture, proved by Wiles et al, asserts that elliptic curves over $\mathbb{Q}$ correspond to modular forms of weight 2. Therefore, it is natural to ask which results on elliptic curves can be generalised to modular forms of higher weights. In this thesis, we discuss how this can be done for the results of p-supersingular elliptic curves we stated above.

Since the p-adic L-functions of Pollack are defined for any modular forms (by which we mean normalised eigen-newform) f of any weights $k \geq 2$ with $a_p = 0$, one expects that it should be possible to generalise works of Kobayashi to higher weight forms formulating a main conjecture involving $L_{p,f}^{\pm}$. By Kurihara [Kur02], we can interpret Kobayashi's Coleman maps for an elliptic curve $E/\mathbb{Q}$ as pairings with some special points of the formal group associated to E under the exponential map. For an arbitrary f, Deligne [Del69] showed that there exists a p-adic representation V_f of $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ associated to f, which generalises the definition of Tate modules for elliptic curves, whereas the exponential map of Bloch and Kato from [BK90], which is a map on $\mathbb{D}_{\mathrm{cris}}(V_f)$, generalises the exponential map for a formal group. These observations suggest the possibility of defining $\mathrm{Col}^{\pm}$ for general f by p-adic Hodge theory in place of formal groups.

Indeed, in this thesis, we show that the $\pm$-Coleman maps

$$\mathrm{Col}^{\pm} : H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V_f) \to \Lambda(G_\infty) \otimes \mathbb{Q},$$

can be constructed by studying $\mathbb{D}_{\mathrm{cris}}(V_f)$ and the Perrin-Riou exponential [PR94] associated to V_f, which interpolates values of Bloch-Kato's exponential. This is the content of Chapter 2. We first review some properties of Perrin-Riou's exponential and relate them to the Kato zeta elements. We then establish a divisibility property, namely that the images of the Perrin-Riou map of certain elements are divisible by Pollack's $\pm$-logarithms. This allows us to define $\mathrm{Col}^{\pm}$ to be the quotient of the Perrin-Riou map by $\log_{p,k}^{\pm}$. Using the same machinery, we show that the Coleman maps of Sprung can be defined using the Perrin-Riou map also. As a consequence, we show that Sprung's works can be generalised to general weight 2 modular forms.

In Chapter 3, we study the kernels of the Coleman maps. In particular, we assume $p \geq k-1$ so that V_f is Fontaine-Laffaille. In this case, there is a structure theorem for V_f, which allows us to establish a few elementary properties of the cohomology H^1 of V_f and generalise the description of the kernels given in [Kob03]. Under the same assumption, we study the images of the Coleman maps in Chapter 4. We prove a necessary and sufficient condition for the divisibility by $\log^{\pm}_{p,k}$, which allows us to give a fairly explicit description of the images.

In Chapter 5, we generalise Kobayashi's definition of $\mathrm{Sel}_p^{\pm}$. By studying Poitou-Tate exact sequences, we relate $\mathrm{Sel}_p^{\pm}$ to the kernel of $\mathrm{Col}^{\pm}$ as described in Chapter 3. We then show that $\mathrm{Sel}_p^{\pm}(f/\mathbb{Q}_\infty)$ is indeed $\Lambda(G_\infty)$-cotorsion and the $\mathbb{Z}_p[[\gamma-1]]$-characteristic ideals at an isotypical component of Δ contain the respective Pollack's p-adic L-functions by applying our Coleman maps to the Kato zeta elements. In particular, we show that $L_{p,f}^{\pm} \neq 0$ by a simple application of the non-vanishing results for the complex L-values of f by Rohrlich [Roh88] and Shimura [Shi76]. This gives a reformulation of the main conjectures of Kato and Perrin-Riou stating that $L_{p,f}^{\pm,\eta}$ generates the characteristic ideal of $\mathrm{Sel}_p^{\pm}(f/\mathbb{Q}_\infty)^{\vee,\eta}$ where η is a character on Δ.

In Chapter 6, we generalise works of Pollack and Rubin [PR04] for elliptic curves to show that the main conjecture holds for CM modular forms (under some technical conditions). The main ingredient of the proof is a generalisation the reciprocity law of Coates-Wiles and Rubin, which we prove by studying properties of elliptic units associated to a CM form.

We remove the assumption $a_p = 0$ in Chapter 7. We study the (φ, G_∞)-module associated to V_f. By Fontaine, for any $\mathbb{Z}_p$-linear representation T of $G_{\mathbb{Q}_p}$ there is a canonical isomorphism $H^1_{\mathrm{Iw}}(\mathbb{Q}_p, T) \cong D(T)^{\psi=1}$, where $D(T)$ denotes the (φ, G_∞)-module of T, a module over the p-adic completion $\mathbb{A}_{\mathbb{Q}_p}$ of the power series ring $\mathbb{Z}_p[[\pi]][\pi^{-1}]$ and ψ is a certain left inverse of φ. It therefore suffices to define our Coleman maps on $D(T)^{\psi=1}$ instead of $H^1_{\mathrm{Iw}}(\mathbb{Q}_p, T)$.

We do this via Berger's theory of Wach modules [Ber03], which is a refined version of (φ, G_∞)-modules for crystalline representations, originally studied by Wach in [Wac96]. Wach modules have the advantage that they are finitely generated modules over the simpler ring $\mathbb{Z}_p[[\pi]]$, and if V is a d-dimensional positive crystalline representation of $G_{\mathbb{Q}_p}$ satisfying a mild technical condition, then $D(V)^{\psi=1} = \mathbb{N}(V)^{\psi=1}$. For any such representation and a basis of $\mathbb{N}(V)$, we construct in Section 7.1 a family of Coleman maps

$$\mathrm{Col}_i : \mathbb{N}(V)^{\psi=1} \to \Lambda(G_\infty) \otimes \mathbb{Q} \quad (1 \leq i \leq d)$$

by showing that $(1-\varphi)\left(\mathbb{N}(V)^{\psi=1}\right)$ is contained in a free $\Lambda(G_\infty) \otimes \mathbb{Q}$-module of rank d, say with basis $n_1, \ldots, n_d$. We then define Col_i by the relation

$$(1-\varphi)x = \sum_{i=1}^{d} \mathrm{Col}_i(x) n_i$$

for $x \in \mathbb{N}(V)^{\psi=1}$.

Let f be a normalised new eigenform of level N with $p \nmid N$ as above (either ordinary or supersingular). We pick a 'good basis' of $\mathbb{D}_{\mathrm{cris}}(V_f)$ and lift it to a basis of $\mathbb{N}(V_f)$. This gives two Coleman maps

$$\mathrm{Col}_i : H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V_f) \to \Lambda(G_\infty) \otimes \mathbb{Q},$$

$i = 1, 2$. We define the Selmer groups $\mathrm{Sel}^i_p(f/\mathbb{Q}_\infty)$ by modifying the local condition of the usual Sel_p at p using $\ker(\mathrm{Col}_i)$ and define the p-adic L-functions $L_{p,i} \in \Lambda(G_\infty) \otimes \mathbb{Q}$ as the image of the Kato zeta element under Col_i.

When f is supersingular at p, we show that there is a decomposition

$$\begin{pmatrix} L_{p,\alpha} \\ L_{p,\beta} \end{pmatrix} = M \begin{pmatrix} \tilde{L}_{p,1} \\ \tilde{L}_{p,2} \end{pmatrix} \tag{1.1}$$

for some 2×2-matrix M with entries of logarithmic growths. When p is large compared to k, there is a canonical choice of M depending on k and a_p only. This generalises the decompositions of $L_{p,\alpha}, L_{p,\beta}$ given by Pollack when $a_p = 0$ and by Sprung when f corresponds to an elliptic curve defined over $\mathbb{Q}$. In order to show that the two approaches are compatible, we prove that the Perrin-Riou map used in Chapter 2 is related to $(1-\varphi)$ by a simple formula.

When f is ordinary at p, our Coleman maps also give rise to two p-adic L-functions in $\Lambda(G_\infty) \otimes \mathbb{Q}$. Let α and β be the unit and non-unit eigenvalues of the Frobenius respectively. The Kato zeta element gives rise to two p-adic L-functions $L_{p,\alpha}$ and $L_{p,\beta}$. The analogue of (1.1) becomes

$$\begin{pmatrix} L_{p,\alpha} \\ L_{p,\beta} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ * & * \end{pmatrix} \begin{pmatrix} \tilde{L}_{p,1} \\ \tilde{L}_{p,2} \end{pmatrix}, \tag{1.2}$$

which is a generalisation of a result of Perrin-Riou [PR93] for p-ordinary elliptic curves. Note that the first Coleman map gives the usual p-adic L-function of f and the corresponding Selmer group is simply $\mathrm{Sel}_p(f/\mathbb{Q}_\infty)$ as constructed in [Kat04], whereas the second Coleman map gives a new p-adic L-function $\tilde{L}_{p,2}$ and a new Selmer group. which we show is $\Lambda(G_\infty)$-cotorsion and its Pontryagin dual is annihilated by $\tilde{L}_{p,2}$ at each Δ-isotypical component.

The decompositions (1.1) and (1.2) allow us to show that $\tilde{L}_{p,1}, \tilde{L}_{p,2} \neq 0$ and the respective Selmer groups are $\Lambda(G_\infty)$-cotorsion. We then reformulate Kato's and Perrin-Riou's main conjectures relating these p-adic L-functions to the characteristic ideals of $\mathrm{Sel}_p^i(f/\mathbb{Q}_\infty)^\vee$. As above, we prove that one inclusion holds.

There are two appendices in this thesis. We prove some elementary linear algebra results on Lubin-Tate extensions in Appendix A. They are used to give the description of $\ker(\mathrm{Col}^\pm)$ given in Chapter 3 and that of $\mathrm{Im}(\mathrm{Col}^\pm)$ in Chapter 4. In Appendix B, in place of the cyclotomic extension of $\mathbb{Q}_p$, we extend the construction of the $\pm$-Coleman maps to Lubin-Tate extensions of height 1 by studying a generalisation of Perrin-Riou's exponential given by Zhang [Zha04b].

Roughly speaking, Chapters 2 to 6 are based on [Lei09b], Chapter 7 is based on [LLZ10] and the two appendices are mainly taken from [Lei09a].

1.3 Notation and basic properties

1.3.1 Extensions by p power roots of unity

Throughout this thesis, p is an odd prime. If K is a field of characteristic 0, either local or global, G_K denotes its absolute Galois group, χ the p-cyclotomic character on G_K and $\mathcal{O}_K$ the ring of integers of K. For an integer $n \geq 0$, we write K_n for the extension $K(\mu_{p^n})$ where μ_{p^n} is the set of p^nth roots of unity and K_∞ denotes $\cup_{n\geq 1} K_n$. The $\mathbb{Z}_p$-cyclotomic extension of K is denoted by K_c and $K^{(n)}$ denotes the p^n-subextension inside K_c.

For $n \geq m$, we write $\mathrm{Tr}_{n/m}$ for the trace map from $\mathbb{Q}_{p,n}$ to $\mathbb{Q}_{p,m}$. Let G_n denote the Galois group $\mathrm{Gal}(\mathbb{Q}_{p,n}/\mathbb{Q}_p)$ for $0 \leq n \leq \infty$. Then, $G_\infty \cong \Delta \times \Gamma$ where $\Delta = G_1$ is a finite group of order $p-1$ and $\Gamma = \mathrm{Gal}(\mathbb{Q}_{p,\infty}/\mathbb{Q}_{p,1}) \cong \mathbb{Z}_p$. We fix a topological generator γ of Γ and write $u = \chi(\gamma)$. In particular, u is a topological generator of $1 + p\mathbb{Z}_p$.

Given a finite extension K of $\mathbb{Q}_p$, $\Lambda_{\mathcal{O}_K}$ (respectively $\Gamma_{\mathcal{O}_K}$) denotes the Iwasawa algebra of G_∞ (respectively Γ) over $\mathcal{O}_K$. We further write $\Lambda_K = \Lambda_{\mathcal{O}_K} \otimes \mathbb{Q}$ and $\Gamma_K = \Gamma_{\mathcal{O}_K} \otimes \mathbb{Q}$. When $K = \mathbb{Q}_p$ (so $\mathcal{O}_K = \mathbb{Z}_p$), we simply write Λ for $\Lambda_{\mathbb{Z}_p}$. If M is a finitely generated $\Gamma_{\mathcal{O}_K}$-torsion (respectively Γ_K-torsion) module, we write $\mathrm{Char}_{\Gamma_{\mathcal{O}_K}}(M)$ (respectively $\mathrm{Char}_{\Gamma_K}(M)$) for its characteristic ideal.

Given a module M over $\Lambda_{\mathcal{O}_K}$ (respectively Λ_K) and a character $\delta : \Delta \to \mathbb{Z}_p^\times$,

M^δ denotes the δ-isotypical component of M. For any $m \in M$, we write m^δ for the projection of m into M^δ. The Pontryagin dual of M is written as $M^\vee$.

1.3.2 Fontaine rings

Let $\tilde{\mathbb{E}} = \left\{(x^{(0)}, x^{(1)}, \dots) \in \mathbb{C}_p^{\mathbb{N}} : (x^{(i+1)})^p = x^{(i)}\right\}$ and write $\tilde{\mathbb{A}}$ for its Witt vectors and $\tilde{\mathbb{B}} = \tilde{\mathbb{A}}[p^{-1}]$. For each n, we fix a primitive p^nth root of unity ζ_{p^n} such that $\zeta_{p^{n+1}}^p = \zeta_{p^n}$. We write ε for the lift of $(\zeta_{p^n})_n \in \tilde{\mathbb{E}}$ in $\mathbb{A}$ and $\pi = \varepsilon + 1$. We have $g \cdot \pi = (1+\pi)^{\chi(g)} - 1$ for all $g \in G_{\mathbb{Q}_p}$ and $t = \log(\varepsilon) \in \mathbb{B}_{\mathrm{dR}}$. We also have the following rings:

$$\mathbb{A}_{\mathbb{Q}_p}^+ = \mathbb{Z}_p[[\pi]] \subset \mathbb{A}_{\mathbb{Q}_p} = \mathbb{Z}_p\widehat{[[\pi]][\pi^{-1}]} \subset \tilde{\mathbb{A}},$$
$$\mathbb{B}_{\mathbb{Q}_p}^+ = \mathbb{A}_{\mathbb{Q}_p}^+[p^{-1}] \subset \mathbb{B}_{\mathbb{Q}_p} = \mathbb{A}_{\mathbb{Q}_p}[p^{-1}] \subset \tilde{\mathbb{B}}$$

where $\hat{}$ denotes the p-adic completion.

Let $\mathbb{B}_{\mathrm{rig},\mathbb{Q}_p}^+$ be the set of $f(\pi) \in \mathbb{Q}_p[[\pi]]$ such that $f(X)$ converges everywhere on the open unit p-adic disc. In particular, $t \in \mathbb{B}_{\mathrm{rig},\mathbb{Q}_p}^+$. We have a derivation $\partial : \mathbb{B}_{\mathrm{rig},\mathbb{Q}_p}^+ \to \mathbb{B}_{\mathrm{rig},\mathbb{Q}_p}^+$ with $\partial = (1+\pi)\frac{d}{d\pi}$.

The Frobenius is written as φ, so $\varphi(\pi) = (1+\pi)^p - 1$ and ψ denotes its left inverse that satisfies

$$\varphi \circ \psi(f(\pi)) = \frac{1}{p} \sum_{\zeta^p = 1} f(\zeta(\pi+1) - 1).$$

We write q for $\varphi(\pi)/\pi$.

1.3.3 Crystalline representations

Let V be a p-adic representation of $G_{\mathbb{Q}_p}$ which is crystalline. We denote the Dieudonné module by $\mathbb{D}(V) = \mathbb{D}_{\mathrm{cris}}(V)$. If $j \in \mathbb{Z}$, $\mathbb{D}^j(V)$ denotes the jth de Rham filtration of $\mathbb{D}(V)$. If $z \in \mathbb{Q}_{p,n}((t)) \otimes_{\mathbb{Q}_p} \mathbb{D}(V)$, denote the constant coefficient of z by $\partial_V(z) \in \mathbb{Q}_{p,n} \otimes_{\mathbb{Q}_p} \mathbb{D}(V)$.

We write $\mathbb{D}_\infty(V) = \mathbb{B}_{\mathbb{Q}_p}^{+,\psi=0} \underset{\mathbb{Q}_p}{\otimes} \mathbb{D}(V)$, which is contained in $\mathbb{B}_{\mathrm{rig},\mathbb{Q}_p}^+ \otimes \mathbb{D}(V)$. The map $\varphi \otimes \varphi$ on $\mathbb{B}_{\mathrm{rig},\mathbb{Q}_p}^+ \otimes \mathbb{D}(V)$ is simply written as φ and the map $\partial \otimes 1$ is written as ∂. Note that ∂ acts on $\mathbb{D}_\infty(V)$ bijectively, so ∂^j makes sense for any $j \in \mathbb{Z}$.

Let T be a lattice of V which is stable under $G_{\mathbb{Q}_p}$. For integers $m \geq n$, we write $\mathrm{cor}_{m/n}$ for the corestriction map

$$H^1(\mathbb{Q}_{p,m}, A) \to H^1(\mathbb{Q}_{p,n}, A)$$

where $A = V$ or T. Let $\mathbb{H}^1_{\mathrm{Iw}}(T)$ denote the inverse limit $\varprojlim H^1(\mathbb{Q}_{p,n}, T)$ with respect to the corestriction and $\mathbb{H}^1_{\mathrm{Iw}}(V) = \mathbb{Q} \otimes \mathbb{H}^1_{\mathrm{Iw}}(T)$. Moreover, if V arises from the restriction of a p-adic representation of $G_{\mathbb{Q}}$ and T is a lattice stable under $G_{\mathbb{Q}}$, we write

$$\begin{aligned} \mathbb{H}^1(T) &= \varprojlim_n H^1(\mathbb{Z}[\zeta_{p^n}, 1/p], T), \\ \mathbb{H}^1(V) &= \mathbb{Q} \otimes \mathbb{H}^1(T). \end{aligned}$$

The (φ, G_∞)-module of V is denoted by $D(V)$. The canonical Λ-module isomorphism defined by Fontaine is written as

$$h^1_{\mathrm{Iw}} : D(V)^{\psi=1} \to \mathbb{H}^1_{\mathrm{Iw}}(V) \tag{1.3}$$

and we write $h^1_{\mathbb{Q}_{p,n},V}$ for its composition with the projection from $\mathbb{H}^1_{\mathrm{Iw}}(V)$ to $H^1(\mathbb{Q}_{p,n}, V)$.

Let $V(j)$ denote the jth Tate twist of V, i.e. $V(j) = V \otimes \mathbb{Q}_p e_j$ where $G_{\mathbb{Q}_p}$ acts on e_j via χ^j. We have

$$\mathbb{D}(V(j)) = t^{-j}\mathbb{D}(V) \otimes e_j.$$

For any $v \in \mathbb{D}(V)$, $v_j = v \otimes t^{-j} e_j$ denotes its image in $\mathbb{D}(V(j))$. We write

$$\mathrm{Tw}_{j,V} : \mathbb{H}^1_{\mathrm{Iw}}(V) \to \mathbb{H}^1_{\mathrm{Iw}}(V(j))$$

for the isomorphism defined in [PR93, Section A.4], which depends on our choice of ζ_{p^n}. For each n and j, we write

$$\exp_{n,j} : \mathbb{Q}_{p,n} \otimes \mathbb{D}(V(j)) \to H^1(\mathbb{Q}_{p,n}, V(j))$$

for Bloch-Kato's exponential defined in [BK90].

1.3.4 Power series

Let $r \in \mathbb{R}_{\geq 0}$. We define

$$\mathcal{H}_r = \left\{ \sum_{n \geq 0, \sigma \in \Delta} c_{n,\sigma} \cdot \sigma \cdot X^n \in \mathbb{C}_p[\Delta][[X]] : \sup_n \frac{|c_{n,\sigma}|_p}{n^r} < \infty \ \forall \sigma \in \Delta \right\}$$

where $|\cdot|_p$ is the p-adic norm on $\mathbb{C}_p$ such that $|p|_p = p^{-1}$ (the corresponding valuation is written as v_p). We write $\mathcal{H}_\infty = \cup_{r \geq 0} \mathcal{H}_r$ and

$$\mathcal{H}_r(G_\infty) = \{ f(\gamma - 1) : f \in \mathcal{H}_r \}$$

for $r \in \mathbb{R}_{\geq 0} \cup \{\infty\}$. In other words, the elements of $\mathcal{H}_r$ (respectively $\mathcal{H}_r(G_\infty)$) are the power series in X (respectively $\gamma - 1$) over $\mathbb{C}_p[\Delta]$ with growth rate $O(\log_p^r)$. If $F, G \in \mathcal{H}_\infty$ are such that $F = O(G)$ and $G = O(F)$, we write $F \sim G$.

We write the additive Fourier transform on $\mathcal{H}_\infty(G_\infty)$ as

$$\begin{aligned} \mathfrak{M} : \mathcal{H}_\infty(G_\infty) &\to \mathbb{C}_p \otimes \mathbb{B}^{\psi=0}_{\mathrm{rig},\mathbb{Q}_p} \\ f(\gamma - 1) &\mapsto f(\gamma - 1) \cdot (1 + \pi). \end{aligned}$$

We identify $\mathcal{H}_\infty(G_\infty)$ with its image under $\mathfrak{M}$. In particular, Λ is identified with $\mathbb{A}^{+,\psi=0}_{\mathbb{Q}_p}$, $\Lambda_{\mathbb{Q}_p}$ with $\mathbb{B}^{+,\psi=0}_{\mathbb{Q}_p}$, etc.

1.3.5 Modular forms

Let $f = \sum a_n q^n$ be a normalised eigen-newform of weight $k \geq 2$, level N and character ϵ. Write $F_f = \mathbb{Q}(a_n : n \geq 1)$ for its coefficient field. Let $\bar{f} = \sum \bar{a}_n q^n$ be the dual form to f, we have $F_f = F_{\bar{f}}$.

We write $L(f, s)$ for the complex L-function of f. If θ is a finite character of G_∞, we write $L(f_\theta, s)$ for the twisted L-function of f by θ.

We assume that $p \nmid N$ and fix a prime of F above p. We denote the completion of F_f at this prime by E and fix a uniformiser ϖ. We write V_f for the 2-dimensional E-linear representation of $G_\mathbb{Q}$ associated to f from [Del69]. When restricted to $G_{\mathbb{Q}_p}$, V_f is crystalline and its de Rham filtration is given by

$$\mathbb{D}^i(V_f) = \begin{cases} \mathbb{D}(V_f) & \text{if } i \leq 0 \\ E\omega & \text{if } 1 \leq i \leq k-1 \\ 0 & \text{if } i \geq k \end{cases} \tag{1.4}$$

for some $0 \neq \omega \in \mathbb{D}(V_f)$. Hence, the Hodge-Tate weights of V_f are 0 and $1 - k$. The action of φ on $\mathbb{D}(V_f)$ satisfies $\varphi^2 - a_p\varphi + \epsilon(p)p^{k-1} = 0$.

If $v \in V_f$, we write $v^\pm$ for the component of v on which the complex conjugation acts by ± 1.

Chapter 2

Construction of the Coleman maps

In this chapter, we define the plus and minus Coleman maps for a modular form f as in Section 1.3.5 under the following condition:

- **Assumption (1)**: $a_p = 0$ and the eigenvalues of φ on $\mathbb{D}(V_f)$ are not integral powers of p.

We first review the definition of Perrin-Riou's exponential from [PR94] for general crystalline representations and results of Kato [Kat04] on general modular forms. We then prove a divisibility property of the image of the Perrin-Riou pairing under assumption (1) in order to define $\mathrm{Col}^{\pm}$.

2.1 Perrin-Riou's exponential

Throughout this section, we fix V a crystalline p-adic representation of $G_{\mathbb{Q}_p}$ such that the action of φ on $\mathbb{D}(V)$ has no eigenvalues which are integral powers of p. Let j be an integer. Since φ acts on t via multiplication by p and

$$\mathbb{D}(V(j)) = t^{-j}\mathbb{D}(V) \otimes e_j,$$

the eigenvalues of φ on $\mathbb{D}(V(j))$ are not integral powers of p either.

Since $V(j)^{G_{\mathbb{Q}_{p,\infty}}}$ is also a crystalline representation, it is a sum of characters. But a character is crystalline iff it is the product of an unramified character and a power of χ (see for example [Bre01, Example 3.1.4]). Therefore, our assumption on the eigenvalues of φ implies that $V(j)^{G_{\mathbb{Q}_{p,\infty}}} = 0$.

For each $j \in \mathbb{Z}$ and $n \geq 0$, under our assumptions on the eigenvalues of φ, the exponential map $\exp_{n,j}$ induces an isomorphism

$$\exp_{n,j} : \mathbb{Q}_{p,n} \otimes \mathbb{D}(V(j))/\mathbb{D}^0(V(j)) \to H^1_f(\mathbb{Q}_{p,n}, V(j)).$$

When $n \geq 1$, there is a well-defined map

$$\begin{array}{rcl} \Xi_{n,V(j)} : \mathbb{D}_\infty(V(j)) & \to & \mathbb{Q}_{p,n} \otimes \mathbb{D}(V(j)) \\ g & \mapsto & (p \otimes \varphi)^{-n} G(\zeta_{p^n} - 1) \end{array}$$

where $G \in \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p} \otimes \mathbb{D}(V(j))$ is such that $(1-\varphi)G = g$ (see [PR94, Section 3.2.2]). Moreover, $(\exp_{n,j} \circ \Xi_{n,V(j)})_{n \geq 1}$ are compatible with the corestriction maps. In other words, the following diagram commutes:

$$\begin{tikzcd} \mathbb{D}_\infty(V(j)) \arrow[r, "\exp_{n+1,j} \circ \Xi_{n+1,V(j)}"] \arrow[dr, "\exp_{n,j} \circ \Xi_{n,V(j)}"'] & H^1(\mathbb{Q}_{p,n+1}, V(j)) \arrow[d, "\mathrm{cor}_{n+1/n}"] \\ & H^1(\mathbb{Q}_{p,n}, V(j)). \end{tikzcd}$$

The definition of the Perrin-Riou exponential is given by the following theorem, which is the main result of [PR94].

Theorem 2.1.1. *Let h be a positive integer such that $\mathbb{D}^{-h}(V) = \mathbb{D}(V)$. Then, for all integers $j \geq 1 - h$, there is is a unique family of Λ-homomorphisms*

$$\Omega_{V(j),h+j} : \mathbb{D}_\infty(V(j)) \to \mathcal{H}_\infty(G_\infty) \underset{\Lambda}{\otimes} \mathbb{H}^1_{\mathrm{Iw}}(T(j))$$

such that the following diagram commutes:

$$\begin{tikzcd} \mathbb{D}_\infty(V(j)) \arrow[r, "\Omega_{V(j),h+j}"] \arrow[d, "\Xi_{n,V(j)}"'] & \mathcal{H}_\infty(G_\infty) \underset{\Lambda}{\otimes} \mathbb{H}^1_{\mathrm{Iw}}(T(j)) \arrow[d, "\mathrm{pr}"] \\ \mathbb{Q}_{p,n} \otimes \mathbb{D}(V(j)) \arrow[r, "(h+j-1)! \exp_{n,j}"] & H^1(\mathbb{Q}_{p,n}, V(j)) \end{tikzcd}$$

where $n \geq 1$ and pr *stands for projection. Moreover, we have*

$$\mathrm{Tw}_{1,V(j)} \circ \Omega_{V(j),h+j} \circ (\partial \otimes te_{-1}) = -\Omega_{V(j+1),h+j+1}.$$

Proof. [PR94, Section 3.2.3] □

Remark 2.1.2. *By [PR94, Section 3.2.4], if $g \in \mathbb{B}^{+,\psi=0}_{\mathbb{Q}_p} \otimes \mathbb{D}_\alpha(V(j))$ where $\mathbb{D}_\alpha(V(j))$ is the subspace of $\mathbb{D}(V(j))$ in which φ has slope α, then $\Omega_{V(j),h+j}(g)$ is $O(\log_p^{h+\alpha})$, i.e. contained in $\mathcal{H}_{h+\alpha}(G_\infty) \otimes \mathbb{H}^1_{\mathrm{Iw}}(T(j))$.*

Remark 2.1.3. *The theorem also implies the following congruence for $r \geq 0$:*

$$(-1)^r \operatorname{Tw}_{r,V(j)}(\Omega_{V(j),h+j}(g)) \equiv$$
$$(h+j+r-1)! \exp_{n,j+r} \circ \Xi_{n,V(j+r)} \circ (\partial^{-r} \otimes t^{-r} e_r)(g) \mod (\gamma^{p^{n-1}} - 1).$$

2.2 Perrin-Riou's pairing

Let M be a finite extension of $\mathbb{Q}_p$ and we further assume that V is a vector space over M and the action of $G_{\mathbb{Q}_p}$ is compatible with the multiplication by M, i.e. V is a M-linear representation of $G_{\mathbb{Q}_p}$.

We fix T an $\mathcal{O}_M$-lattice of V which is stable under $G_{\mathbb{Q}_p}$. We write V^* for the M-linear dual of V and T^* for the $\mathcal{O}_M$-linear dual of T. Since $H^1(\mathbb{Q}_{p,n}, T)$ and $H^1(\mathbb{Q}_{p,n}, T^*(1))$ are $\mathcal{O}_M[G_n]$-modules, $\mathbb{H}^1_{\mathrm{Iw}}(T)$ and $\mathbb{H}^1_{\mathrm{Iw}}(T^*(1))$ are Λ_M-modules. By [PR94, Section 3.6.1], there is a non-degenerate pairing

$$\begin{array}{rcl} <,>: \mathbb{H}^1_{\mathrm{Iw}}(T) \times \mathbb{H}^1_{\mathrm{Iw}}(T^*(1)) & \to & \Lambda_{\mathcal{O}_M} \\ ((x_n)_n, (y_n)_n) & \mapsto & \left(\sum_{\sigma \in G_n} [x_n^\sigma, y_n]_n \cdot \sigma \right)_n \end{array}$$

where $[,]_n$ is the natural pairing

$$H^1(\mathbb{Q}_{p,n}, T) \times H^1(\mathbb{Q}_{p,n}, T^*(1)) \to \mathcal{O}_M.$$

The pairing $<,>$ extends to

$$\left(\mathcal{H}_\infty(G_\infty) \underset{\Lambda_{\mathcal{O}_M}}{\otimes} \mathbb{H}^1_{\mathrm{Iw}}(T) \right) \times \left(\mathcal{H}_\infty(G_\infty) \underset{\Lambda_{\mathcal{O}_M}}{\otimes} \mathbb{H}^1_{\mathrm{Iw}}(T^*(1)) \right) \to \mathcal{H}_\infty(G_\infty),$$

which we also denote by $<,>$. Let j and h be integers satisfying conditions of Theorem 2.1.1. If $\eta \in \mathbb{D}(V(j))$, then $(1+\pi) \otimes \eta \in \mathbb{D}_\infty(V(j))$. Using the pairing $<,>$, we define a map:

$$\begin{array}{rcl} \mathcal{L}^{h,j}_\eta : \mathbb{H}^1_{\mathrm{Iw}}(T(j)^*(1)) & \to & \mathcal{H}_\infty(G_\infty) \\ \mathbf{z} & \mapsto & < \Omega_{V(j),h+j}((1+\pi) \otimes \eta), \mathbf{z} > . \end{array}$$

Note that $\mathcal{L}^{h,j}_\eta$ modulo $\Gamma^{p^{n-1}} - 1$ induces a map into $M[G_n]$, which we denote by $\mathcal{L}^{h,j}_{\eta,n}$. Also, $\mathcal{L}^{h,j}_\eta$ extends naturally to a map on $\mathbb{H}^1_{\mathrm{Iw}}(V(j)^*(1))$, which we write as $\mathcal{L}^{h,j}_\eta$ also.

2.2.1 Explicit formulae of $\mathcal{L}_{\eta,n}^{h,j}$

The following result is possibly well-known. Due to the lack of reference, we include the proof here for completeness.

Lemma 2.2.1. *Under the notation above, let $\eta \in \mathbb{D}(V(j))$. Then, the projection of*

$$\frac{1}{(h+j-1)!}\Omega_{V(j),h+j}((1+\pi)\otimes\eta)$$

into $H^1(\mathbb{Q}_{p,n}, V(j))$ is given by

$$\begin{cases} p^{-n}\exp_{n,j}\left(\sum_{m=0}^{n-1}\zeta_{p^{n-m}}\otimes\varphi^{m-n}(\eta)+(1-\varphi)^{-1}(\eta)\right) & \text{if } n \geq 1 \\ \exp_{0,j}\left(\left(1-\frac{\varphi^{-1}}{p}\right)(1-\varphi)^{-1}(\eta)\right) & \text{if } n = 0. \end{cases} \tag{2.1}$$

Proof. Let $g \in \mathbb{D}_\infty(V(j))$. We write $\Delta_i(g) = \partial^i(g)(0)$ for $i \in \mathbb{Z}$ and

$$\tilde{g} = g - \sum_{i=0}^{h}\frac{1}{i!}\log_p^i(1+\pi)\otimes\Delta_i(g).$$

By [PR94, Section 2.2], the sum $\sum_{n=0}^{\infty}\varphi^n(\tilde{g})$ converges. Let

$$G = \sum_{n=0}^{\infty}\varphi^n(\tilde{g}) + \sum_{i=0}^{h}\frac{1}{i!}\log_p^i(1+\pi)\otimes v_i$$

where $v_i \in \mathbb{D}(V(j))$ is such that $\Delta_i(g) = (1-p^i\varphi)v_i$ (such v_i exist by our assumption on the eigenvalues of φ), then $(1-\varphi)G = g$. For $g = (1+\pi)\otimes\eta$, we have $\Delta_i(g) = \eta$ and $v_i = (1-p^i\varphi)^{-1}\eta$ for all i. If n is a positive integer, a simple calculation shows that

$$\varphi^m(\tilde{g})(\zeta_{p^n}-1) = \begin{cases} (\zeta_{p^{n-m}}-1)\otimes\varphi^m(\eta) & \text{if } m < n \\ 0 & \text{otherwise.} \end{cases} \tag{2.2}$$

Therefore, we have

$$\begin{aligned} G(\zeta_{p^n}-1) &= \sum_{m=0}^{n-1}(\zeta_{p^{n-m}}-1)\otimes\varphi^m(\eta)+(1-\varphi)^{-1}(\eta) \\ &= \sum_{m=0}^{n-1}\zeta_{p^{n-m}}\otimes\varphi^m(\eta)+(1-\varphi)^{-1}\varphi^n(\eta) \end{aligned}$$

Hence, by Theorem 2.1.1, the nth projection of $\Omega_{V(j),h+j}(g)/(h+j-1)!$ is given by the image of

$$(p\otimes\varphi)^{-n}G(\zeta_{p^n}-1) = \frac{1}{p^n}\left(\sum_{m=0}^{n-1}\zeta_{p^{n-m}}\otimes\varphi^{m-n}(\eta)+(1-\varphi)^{-1}(\eta)\right) \tag{2.3}$$

under the exponential map $\exp_{n,j}$. For the 0th level, it is given by the image of

$$\begin{aligned}
\mathrm{Tr}_{1/0}\left(\frac{1}{p}\varphi^{-1}G(\zeta_p-1)\right) &= \frac{1}{p}\mathrm{Tr}_{1/0}\left(\zeta_p\otimes\varphi^{-1}(\eta)+(1-\varphi)^{-1}(\eta)\right)\\
&= \frac{1}{p}\left(-1\otimes\varphi^{-1}(\eta)+(p-1)(1-\varphi)^{-1}(\eta)\right)\\
&= \left(1-\frac{\varphi^{-1}}{p}\right)(1-\varphi)^{-1}(\eta)
\end{aligned}$$

under the map $\exp_{0,j}$, so we are done. $\square$

For $n\geq 1$ and $\eta\in\mathbb{D}(V(j))$, we write

$$\gamma_{n,j}(\eta):=p^{-n}\left(\sum_{i=0}^{n-1}\zeta_{p^{n-i}}\otimes\varphi^{i-n}(\eta)+(1-\varphi)^{-1}(\eta)\right).$$

Remark 2.1.3 and properties of the twist map (see e.g. [PR94, Sections 3.6.1 and 3.6.5]) implies that for $\mathbf{z}\in\mathbb{H}^1_{\mathrm{Iw}}(T(j)^*(1))$ and $r\geq 0$,

$$\begin{aligned}
&\frac{1}{(h+j+r-1)!}\mathrm{Tw}_r(\mathcal{L}_\eta^{h,j}(\mathbf{z}))\\
\equiv&\sum_{\sigma\in G_n}\left[\exp_{n,j+r}(\gamma_{n,j+r}(\eta_r)^\sigma),z_{-r,n}\right]_n\cdot\sigma\mod(\gamma^{p^{n-1}}-1)
\end{aligned}\tag{2.4}$$

where Tw_r acts on $\mathcal{H}_\infty(G_\infty)$ via $\sigma\mapsto\chi(\sigma)^r\sigma$ for $\sigma\in G_\infty$ and $z_{-r,n}$ is the image of $\mathbf{z}$ under the composition

$$\mathbb{H}^1_{\mathrm{Iw}}(T(j)^*(1))\xrightarrow{(-1)^r\,\mathrm{Tw}_{-r}}\mathbb{H}^1_{\mathrm{Iw}}(T(j+r)^*(1))\xrightarrow{\mathrm{pr}}H^1(\mathbb{Q}_{p,n},T(j+r)^*(1)).$$

By [Kat93, Chapter II, Section 1.4], we also have

$$\left[\exp_{n,j+r}(\cdot),\cdot\right]_n=\mathrm{Tr}_{n/0}\otimes\mathrm{id}\left(\left[\cdot,\exp^*_{n,j+r}(\cdot)\right]'_n\right)$$

where $\exp^*_{n,j+r}$ is the dual exponential map

$$\exp^*_{n,j+r}:H^1(\mathbb{Q}_{p,n},V(j+r)^*(1))\to\mathbb{D}^0(V(j+r)^*(1))$$

and the pairing

$$[,]'_n:\mathbb{Q}_{p,n}\otimes\mathbb{D}(V(j+r))\times\mathbb{Q}_{p,n}\otimes\mathbb{D}(V(j+r)^*(1))\to\mathbb{Q}_{p,n}\otimes M\tag{2.5}$$

is induced by the natural pairing

$$\mathbb{D}(V(j+r))\times\mathbb{D}(V(j+r)^*(1))\to M.$$

To ease notation, we simply write $[,]_n$ for $[,]'_n$ when it does not cause confusion. We can now rewrite (2.4) as:

$$
\begin{aligned}
&\frac{1}{(h+j+r-1)!}\,\mathrm{Tw}_r(\mathcal{L}^h_\eta(\mathbf{z}))\\
\equiv\ &\sum_{\sigma\in G_n}\mathrm{Tr}_{n,0}\left[\gamma_{n,j+r}(\eta_r)^\sigma,\exp^*_{n,j+r}(z_{-r,n})\right]_n\cdot\sigma \mod (\gamma^{p^{n-1}}-1)\\
\equiv\ &\left[\sum_{\sigma\in G_n}\gamma_{n,j+r}(\eta_r)^\sigma\sigma,\ \sum_{\sigma\in G_n}\exp^*_{n,j+r}(z^\sigma_{-r,n})\sigma^{-1}\right]_n \mod (\gamma^{p^{n-1}}-1).
\end{aligned}
\tag{2.6}
$$

Note that we have recovered the pairing P_n of [Kur02]. We write the quantity in (2.6) as $P_{n,r}(\eta, z_{-r,n})$. Following the calculations of [Kur02], we can deduce the following special values of $\mathcal{L}^{h,j}_\eta$:

Lemma 2.2.2. *For an integer $r \geq 0$, we have*

$$
\begin{aligned}
&\frac{1}{(h+j+r-1)!}\chi^r\left(\mathcal{L}^{h,j}_\eta(\mathbf{z})\right)\\
=\ &\left[\left(1-\frac{\varphi^{-1}}{p}\right)(1-\varphi)^{-1}(\eta_r),\exp^*_{0,r+j}(z_{-r,0})\right]_0.
\end{aligned}
$$

Let θ be a character of G_n which does not factor through G_{n-1} with $n \geq 1$, then

$$
\begin{aligned}
&\frac{1}{(h+j+r-1)!}\chi^r\theta\left(\mathcal{L}^{h,j}_\eta(\mathbf{z})\right)\\
=\ &\frac{1}{\tau(\theta^{-1})}\sum_{\sigma\in G_n}\theta^{-1}(\sigma)\left[\varphi^{-n}(\eta_r),\exp^*_{n,r+j}(z^\sigma_{-r,n})\right]_n
\end{aligned}
$$

where τ denotes the Gauss sum.

2.3 Modular forms and Kato zeta elements

The details of the results in this section can be found in [Kat04].

2.3.1 L-functions and p-adic L-functions

Let f be as in Section 1.3.5. For any $v \in V_f$ such that $v^\pm \neq 0$, it determines a lattice $\mathcal{O}_E$-lattice T_f of V_f. We choose v such that T_f is stable under $G_\mathbb{Q}$. Note that as a representations of $G_\mathbb{Q}$, $V_f^* \cong V_{\bar{f}}(k-1)$. Hence, T_f determines a lattice $T_{\bar{f}}$ of $V_{\bar{f}}$ naturally.

Let

$$\mathrm{per}: \mathbb{D}^1(V_f) \to V_f$$

be the period map defined in [Kat04]. Fix $0 \neq \omega \in \mathbb{D}^1(V_f)$ and let $\Omega_\pm \in \mathbb{C}^\times$ such that $\mathrm{per}(\omega) = \Omega_+ v^+ + \Omega_- v^-$. The p-adic L-functions associated to f are given by the following.

Theorem 2.3.1. *Let α be a root of $X^2 - a_p X + \epsilon(p)p^{k-1}$ such that $v_p(\alpha) < k-1$. Under the notation above, there exists a unique $L_{p,\alpha} \in \mathcal{H}_\infty(G_\infty)$ (depending on the choice of ω and v) such that for any integer $0 \leq r \leq k-2$ and any character θ of G_n which does not factor through G_{n-1} with $n \geq 1$,*

$$\chi^r\theta(L_{p,\alpha}) = \frac{c_{n,r}\alpha^{-n}}{\tau(\theta)\Omega_\pm} L(f, \theta, r)$$

where $c_{n,r}$ is some constant, only dependent on n and r and $\pm = (-1)^{k-r}\theta(-1)$.

Proof. [AV75], [MTT86] or [Kat04, Theorem 16.2]. □

If f corresponds to an elliptic curve E_f over $\mathbb{Q}$, there is a canonical choice of ω and T_f, namely, the Néron differential and $T_p(E_f)(-1)$ (see [Kur02, Section 2.2.2]) where $T_p(E_f)$ denotes the Tate module of E_f at p.

2.3.2 Kato's main conjecture

In order to state Kato's main conjecture, we have to review two important results from [Kat04] first.

Theorem 2.3.2. *Under the notation above, we have:*

(a) $\mathbb{H}^2(T_f)$ *is a torsion* $\Lambda_{\mathcal{O}_E}$*-module.*

(b) $\mathbb{H}^1(T_f)$ *is a torsion free* $\Lambda_{\mathcal{O}_E}$*-module and* $\mathbb{H}^1(V_f)$ *is a free* Λ_E*-module of rank 1.*

Proof. [Kat04, Theorem 12.4] □

Theorem 2.3.3. *Fix a character $\delta : \Delta \to \mathbb{Z}/(p-1)\mathbb{Z}$.*

(a) Let θ be a character of G_n and $\pm = (-1)^{k-r}\theta(-1)$ where r is an integer such that $1 \leq r \leq k-1$. Write

$$\begin{aligned} \kappa_\theta : \mathbb{Q}_{p,n} \otimes \mathbb{D}^0(V_f(k-r)) &\to V_f \\ x \otimes y &\mapsto \sum_{\sigma \in G_n} \theta(\sigma)\sigma(x)\mathrm{per}(y)^\pm. \end{aligned}$$

There exists a unique E-linear map (independent of θ and r)

$$V_f \to \mathbb{H}^1(V_f); \qquad v \mapsto \mathbf{z}_v$$

such that κ_θ sends the image of $\mathbf{z}_v$ in $\mathbb{Q}_{p,n} \otimes \mathbb{D}^0(V_f(k-r))$ (under the composition of the localisation, the twist map and the dual exponential) to

$$d_r \cdot L(\bar{f}, \theta, r) \cdot v^{\pm}$$

and d_r is a constant which only depends on r.

(b) Let $\mathbb{Z}(T_f) \subset \mathbb{H}^1(V_f)$ denote the $\Lambda_{\mathcal{O}_E}$-module generated by $\mathbf{z}_{v^\pm} \in T_f$ and write $\mathbb{Z}(V_f) = \mathbb{Z}(T_f) \otimes \mathbb{Q}$. Then, the quotient $\mathbb{H}^1(V_f)/\mathbb{Z}(V_f)$ is a torsion Λ_E-module and

$$\mathrm{Char}_{\Gamma_E}(\mathbb{H}^1(V_f)^\delta/\mathbb{Z}(V_f)^\delta) \subset \mathrm{Char}_{\Gamma_E}(\mathbb{H}^2(V_f)^\delta).$$

(c) If the homomorphism $G_{\mathbb{Q}} \to GL_{\mathcal{O}_E}(T_f)$ is surjective, then $\mathbb{Z}(T_f) \subset \mathbb{H}^1(T_f)$. Moreover, $\mathbb{H}^1(T_f)$ is a free $\Lambda_{\mathcal{O}_E}$-module of rank 1 and

$$\mathrm{Char}_{\Gamma_{\mathcal{O}_E}}(\mathbb{H}^1(T_f)^\delta/\mathbb{Z}(T_f)^\delta) \subset \mathrm{Char}_{\Gamma_{\mathcal{O}_E}}(\mathbb{H}^2(T_f)^\delta).$$

Proof. [Kat04, Theorem 12.5] □

Kato's main conjecture states that:

Conjecture 2.3.4. *The inclusion $\mathbb{Z}(T_f) \subset \mathbb{H}^1(T_f)$ holds. Moreover, if $\delta : \Delta \to \mathbb{Z}/(p-1)\mathbb{Z}$ is a character, then*

$$\mathrm{Char}_{\Gamma_{\mathcal{O}_E}}(\mathbb{H}^1(T_f)^\delta/\mathbb{Z}(T_f)^\delta) = \mathrm{Char}_{\Gamma_{\mathcal{O}_E}}(\mathbb{H}^2(T_f)^\delta).$$

We call elements of $\mathbb{Z}(V_f)$ Kato zeta elements. In particular, we write $\mathbf{z}_f^{\mathrm{Kato}}$ for the one corresponding to our choice of $v \in V_f$ fixed in Section 2.3.1 and call it *the* Kato zeta element associated to f.

We fix $\bar{v} \in V_{\bar{f}}$ and $\bar{\omega} \in \mathbb{D}^{-1}(V_{\bar{f}}(k))$ for the dual form $\bar{f}$ similarly. Below, we relate the Kato zeta element $\mathbf{z}_{\bar{f}}^{\mathrm{Kato}}$ associated to $\bar{f}$ to the p-adic L-functions of f defined by Theorem 2.3.1 via the map $\mathcal{L}_\eta^{h,j}$. For simplicity, we write $\mathbf{z}^{\mathrm{Kato}} = \mathbf{z}_{\bar{f}}^{\mathrm{Kato}}$ from now on.

Let $V = V_f(1)$, then we can take $h = 1$ and $j \geq 0$ in Theorem 2.1.1 by (1.4). For $\eta \in \mathbb{D}(V_f)$, we simply write

$$\mathcal{L}_\eta = \mathcal{L}_{\eta_1}^{1,0} : \mathbb{H}^1_{\mathrm{Iw}}(T_{\bar{f}}(k-1)) \to \mathcal{H}_\infty(G_\infty) \tag{2.7}$$

for the map we defined in Section 2.2, with $M = E$.

Theorem 2.3.5. *For α as in Theorem 2.3.1, there exists η_α, an eigenvector of φ on $\mathbb{D}(V_f)$ with eigenvalue α such that $[\eta_\alpha, \bar{\omega}] = 1$. Moreover, the image of $\mathbf{z}^{\mathrm{Kato}}$ under the composition*

$$\mathbb{H}^1(V_{\bar{f}}) \to \mathbb{H}^1_{\mathrm{Iw}}(V_{\bar{f}}) \xrightarrow{\mathrm{Tw}_{k-1}} \mathbb{H}^1_{\mathrm{Iw}}(V_{\bar{f}}(k-1)) \xrightarrow{\mathcal{L}_{\eta_\alpha}} \mathcal{H}_\infty(G_\infty)$$

is the p-adic L-function $L_{p,\alpha}$ where the first map is just the localisation and Tw_{k-1} denotes $\mathrm{Tw}_{k-1,V_{\bar{f}}}$.

Proof. [Kat04, Theorem 16.6] □

We sometimes abuse notation and write the above composition as $\mathcal{L}_{\eta_\alpha}$ also.

Remark 2.3.6. *Let α_1 and α_2 be the roots of $X^2 - a_pX + \epsilon(p)p^{k-1}$. Then, the slope of φ on $\mathbb{D}(V_f)$ is equal to $t = \max(v_p(\alpha_1), v_p(\alpha_2))$. Since $h = 1$ and the slope of φ on $\mathbb{D}(V_f(1))$ is $t-1$, all elements of $\mathrm{Im}(\mathcal{L}_\eta)$ are $O(\log_p^t)$ by Remark 2.1.2.*

It follows immediately from Lemma 2.2.2 that, with the same notation as in the lemma, we have:

$$\begin{aligned} \chi^r(\mathcal{L}_\eta((z)) &= r!\left[\left(1 - \frac{\varphi^{-1}}{p}\right)(1-\varphi)^{-1}(\eta_{r+1}), \exp^*_{0,r+1}(z_{-r,0})\right]_0, \\ \chi^r\theta(\mathcal{L}_\eta((z)) &= \frac{r!}{\tau(\theta^{-1})}\sum_{\sigma\in G_n}\theta^{-1}(\sigma)\left[\varphi^{-n}(\eta_{r+1}), \exp^*_{n,r+1}(z^\sigma_{-r,n})\right]_n. \end{aligned} \tag{2.8}$$

2.4 The ±-Coleman maps

2.4.1 ±-logarithms

Let f be as above such that assumption (1) holds. If α_1 and α_2 are the roots of $X^2 - a_pX + \epsilon(p)p^{k-1}$, then $\alpha_1 = -\alpha_2$. Moreover, $v_p(\alpha_1) = v_p(\alpha_2) = (k-1)/2$, so Remark 2.3.6 implies that $\mathrm{Im}(\mathcal{L}_\eta) \subset \mathcal{H}_{(k-1)/2}(G_\infty)$ for any $\eta \in \mathbb{D}(V_f)$.

In [Pol03], Pollack defines:

$$\begin{aligned}\log_{p,k}^{+} &= \prod_{j=0}^{k-2}\frac{1}{p}\prod_{n=1}^{\infty}\frac{\Phi_{2n}(u^{-j}\gamma)}{p},\\ \log_{p,k}^{-} &= \prod_{j=0}^{k-2}\frac{1}{p}\prod_{n=1}^{\infty}\frac{\Phi_{2n-1}(u^{-j}\gamma)}{p},\end{aligned}$$

where Φ_m denotes the p^mth cyclotomic polynomial.

By considering the special values of L_{p,α_1} and L_{p,α_2} as given by Theorem 2.3.1, Pollack shows that we have the following divisibility properties over $\mathcal{H}_\infty(G_\infty)\cap E[\Delta][[\gamma-1]]$:

$$\begin{aligned}\log_{p,k}^{+} &\mid \alpha_2 L_{p,\alpha_1}-\alpha_1 L_{p,\alpha_2},\\ \log_{p,k}^{-} &\mid L_{p,\alpha_2}-L_{p,\alpha_1}.\end{aligned}$$

This enables him to define

$$L_{p,f}^{+} = \frac{\alpha_2 L_{p,\alpha_1}-\alpha_1 L_{p,\alpha_2}}{(\alpha_2-\alpha_1)\log_{p,k}^{+}}, \tag{2.9}$$

$$L_{p,f}^{-} = \frac{L_{p,\alpha_2}-L_{p,\alpha_1}}{(\alpha_2-\alpha_1)\log_{p,k}^{-}}. \tag{2.10}$$

It is easy to see that this gives a decomposition of L_{p,α_i}, namely

$$L_{p,\alpha_i}=\log_{p,k}^{+}L_{p,f}^{+}+\alpha_i\log_{p,k}^{-}L_{p,f}^{-} \tag{2.11}$$

for $i\in\{1,2\}$.

To ease notation, we suppress the subscript f and write $L_p^{\pm}$ for $L_{p,f}^{\pm}$. The growth rates of these elements are given by:

Theorem 2.4.1. *$\log_{p,k}^{+}\sim\log_{p,k}^{-}\sim\log_p^{\frac{k-1}{2}}$ and $L_p^{\pm}=O(1)$.*

Proof. [Pol03, Lemma 4.5 and Theorem 5.1] □

2.4.2 Definition of the Coleman maps

Recall that $\mathcal{L}_{\eta_{\alpha_i}}(\mathbf{z}^{\mathrm{Kato}})=L_{p,\alpha_i}$ for $i=1,2$ by Theorem 2.3.5. Hence, if we write

$$\eta^{+}=\frac{\alpha_2\eta_{\alpha_1}-\alpha_1\eta_{\alpha_2}}{\alpha_2-\alpha_1}\qquad\text{and}\qquad\eta^{-}=\frac{\eta_{\alpha_2}-\eta_{\alpha_1}}{\alpha_2-\alpha_1},$$

then $\mathcal{L}_{\eta^{\pm}}(\mathbf{z}^{\mathrm{Kato}})=\log_{p,k}^{\pm}L_p^{\pm}$ by (2.9), (2.10) and the linearity of $\mathcal{L}$. In fact, more is true:

Proposition 2.4.2. *If $\mathbf{z} \in \mathbb{H}^1_{\mathrm{Iw}}(T_{\bar{f}})$, then we have the divisibility $\log^{\pm}_{p,k} | \mathcal{L}_{\eta^{\pm}}(\mathbf{z})$ over $\mathcal{H}_\infty(G_\infty) \cap E[\Delta][[\gamma-1]]$.*

Proof. Recall that $[\omega, \bar{\omega}] = 0$, $[\eta_{\alpha_i}, \bar{\omega}] = 1$ and $\varphi^2 = \alpha_i^2$ on $\mathbb{D}(V_f)$. Therefore, explicit calculation shows that

$$\eta_{\alpha_i} = (\varphi(\omega) + \alpha_i \omega)/[\varphi(\omega), \bar{\omega}]$$

for $i \in \{1, 2\}$. Hence,

$$\eta^+ = \frac{\varphi(\omega)}{[\varphi(\omega), \bar{\omega}]} \qquad \text{and} \qquad \eta^- = \frac{\omega}{[\varphi(\omega), \bar{\omega}]}.$$

Let r be an integer. Since $\varphi^2 = -\epsilon(p)p^{k-2r-3}$ on $\mathbb{D}(V_f(r+1))$, we have

$$\begin{aligned} \varphi^{-n}(\eta^+_{r+1}) &\equiv 0 \mod \omega \qquad \text{if } n \text{ is odd,} \\ \varphi^{-n}(\eta^-_{r+1}) &\equiv 0 \mod \omega \qquad \text{if } n \text{ is even.} \end{aligned}$$

For $0 \leq r \leq k-2$, we have

$$\mathrm{Im}(\exp^*_{n,r+1}) = \mathbb{Q}_{p,n} \otimes E \cdot \bar{\omega}_{-r-1} = \mathbb{Q}_{p,n} \otimes \mathbb{D}^0(V_{\bar{f}}(k-1-r))$$

and

$$\mathbb{D}^0(V_f(r+1)) = E \cdot \omega_{r+1}.$$

Hence, the fact that $\mathbb{D}^0(V_f(r+1))$ and $\mathbb{D}^0(V_{\bar{f}}(k-1-r))$ are orthogonal complements of each other under $[,]$ and (2.8) implies

$$\begin{aligned} \chi^r\theta(\mathcal{L}_{\eta^+}(\mathbf{z})) &= 0 \qquad \text{if } n \text{ is odd,} \\ \chi^r\theta(\mathcal{L}_{\eta^-}(\mathbf{z})) &= 0 \qquad \text{if } n \text{ is even} \end{aligned}$$

where θ and n are as defined in Lemma 2.2.2. Recall that $\chi(\gamma) = u$, so we have equivalences $\chi^r\theta(\Phi_m(u^{-r}\gamma)) = \Phi_m(\theta(\gamma)) = 0$ iff $\theta(\gamma)$ is a primitive p^mth root of unity iff θ factors through G_{m+1} but not G_m. Hence all the zeros of $\log^{\pm}_{p,k}$, which are all simple, are also zeros of $\mathcal{L}_{\eta^{\pm}}(\mathbf{z})$, so we are done. □

Remark 2.4.3. *An alternative proof for this proposition is given in Section 4.1.*

Recall that $\mathcal{L}_{\eta^{\pm}}(\mathbf{z}) = O(\log_p^{\frac{k-1}{2}})$ and Theorem 2.4.1 says that $\log^{\pm}_{p,k} \sim \log_p^{\frac{k-1}{2}}$, so we have $\mathcal{L}_{\eta^{\pm}}(\mathbf{z})/\log^{\pm}_{p,k} = O(1)$. We define

$$\begin{aligned} \mathrm{Col}^{\pm} : \mathbb{H}^1_{\mathrm{Iw}}(T_{\bar{f}}(k-1)) &\to \Lambda_E \\ \mathbf{z} &\mapsto \frac{\mathcal{L}_{\eta^{\pm}}(\mathbf{z})}{\log^{\pm}_{p,k}}. \end{aligned}$$

We call these two maps the plus and minus Coleman maps. Note that we sometimes abuse notation and write $\mathrm{Col}^{\pm}$ for the composition

$$\mathbb{H}^1(T_{\bar{f}}) \to \mathbb{H}^1_{\mathrm{Iw}}(T_{\bar{f}}) \xrightarrow{\mathrm{Tw}_{k-1}} \mathbb{H}^1_{\mathrm{Iw}}(T_{\bar{f}}(k-1)) \xrightarrow{\mathrm{Col}^{\pm}} \Lambda_E$$

and its natural extension to $\mathbb{H}^1(V_{\bar{f}})$. In particular, we have $\mathrm{Col}^{\pm}(\mathbf{z}^{\mathrm{Kato}}) = L_p^{\pm}$. Similar to $\mathcal{L}_{\eta^{\pm},n}$, we write $\mathrm{Col}_n^{\pm}$ for the map $\mathrm{Col}^{\pm}$ modulo $\Gamma^{p^{n-1}} - 1$.

Remark 2.4.4. *The Coleman maps in [Kob03] are defined using a pairing with points coming from the formal group associated to an elliptic curve, instead of images of the Perrin-Riou exponential. It is not hard to see that the definition given above agrees with the one given by Kobayashi on comparing [Kob03, Proposition 8.25] and* (2.6)*.*

2.5 The case $k = 2$

Let f be a modular form as in Section 1.3.5 with $k = 2$. We temporarily remove the condition $a_p = 0$ in assumption (1) and replace it by $v_p(a_p) \geq 2$ (so that $v_p(\alpha) = v_p(\beta) = 1/2$) in the rest of this section. The aim of this section is to rewrite Sprung's construction of the Coleman maps for elliptic curves over $\mathbb{Q}$ with $a_p \neq 0$ using the Perrin-Riou pairing.

Define for $n \geq 1$

$$\begin{pmatrix} \Theta_n^1 & \Upsilon_n^1 \\ \Theta_n^0 & \Upsilon_n^0 \end{pmatrix} = \begin{pmatrix} 0 & \Phi_n(\gamma) \\ -1 & a_p \end{pmatrix} \cdots \begin{pmatrix} 0 & \Phi_1(\gamma) \\ -1 & a_p \end{pmatrix} \in M(2, \mathcal{H}(G_\infty)).$$

It satisfies the following.

Lemma 2.5.1. *Let $i \in \mathbb{Z}$ and write*

$$A_n^i = \begin{pmatrix} 0 & p \\ -1 & a_p \end{pmatrix}^i \begin{pmatrix} \Theta_n^1 & \Upsilon_n^1 \\ \Theta_n^0 & \Upsilon_n^0 \end{pmatrix}.$$

Then, A_n^{i-n} converges in $M(2, \mathcal{H}(G_\infty))$ as $n \to \infty$ for any fixed i. Write A_∞^i for the limit, then all entries of A_∞^i are $O(\log_p^{1/2})$. Moreover, if θ is a character on G_∞ which factors through G_n but not G_{n-1}, then $\theta(A_\infty^i) = \theta(A_m^{i-m})$ for all $m \geq n-1$.

Proof. [Spr09, Lemma 3.21] ∎

Proposition 2.5.2. *For any* $\mathbf{z} \in \mathbb{H}^1_{\mathrm{Iw}}(V_{\bar{f}}(1))$ *and* $0 \neq \omega \in \mathbb{D}^1(V_f)$*, the entries of the row vector*

$$\begin{pmatrix}\mathcal{L}_{\varphi(\omega)}(\mathbf{z}) & -\mathcal{L}_\omega(\mathbf{z})\end{pmatrix} A_\infty^{-1}$$

are both divisible by $\log_p(\gamma)/(\gamma-1)$*.*

Proof. For $n \in \mathbb{Z}$, write

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

where α and β are the roots of $X^2 - a_pX + \epsilon(p)p$. Then,

$$\varphi^n = u_n\varphi - pu_{n-1} \tag{2.12}$$

on $\mathbb{D}(V_f)$ and

$$\begin{pmatrix}0 & p\\ -1 & a_p\end{pmatrix}^n = \begin{pmatrix}-pu_{n-1} & pu_n\\ -u_n & u_{n+1}\end{pmatrix}.$$

Therefore, if $n > 1$ and θ is a character of G_∞ which factors through G_n but not G_{n-1} (so $\theta(\gamma)$ is a primitive p^{n-1}th root of unity), we have

$$\theta(A_\infty^{-1}) = \theta(A_{n-1}^{-n}) = \begin{pmatrix}-pu_{-n-1} & pu_{-n}\\ -u_{-n} & u_{-n+1}\end{pmatrix}\begin{pmatrix}0 & 0\\ -1 & a_p\end{pmatrix}\theta\begin{pmatrix}\Theta^1_{n-2} & \Upsilon^1_{n-2}\\ \Theta^0_{n-2} & \Upsilon^0_{n-2}\end{pmatrix} \tag{2.13}$$

where the last matrix is the identity if $n = 2$.

To prove the proposition, it is equivalent to proving that

$$\theta\Big(\begin{pmatrix}\mathcal{L}_{\varphi(\omega)}(\mathbf{z}) & -\mathcal{L}_\omega(\mathbf{z})\end{pmatrix} A_\infty^{-1}\Big) = 0 \tag{2.14}$$

for any θ as above. By Lemma 2.2.2, we have

$$\theta(\mathcal{L}_v(\mathbf{z})) = \frac{1}{\tau(\theta^{-1})}\sum_{\sigma\in G_n}\theta^{-1}(\sigma)[\varphi^{-n}(v_1), \exp^*_{n,1}(z_n^\sigma)]_n$$

for any $v \in \mathbb{D}(V_f)$ and $\mathbf{z} \in \mathbb{H}^1_{\mathrm{Iw}}(V_{\bar{f}}(1))$. Hence, by (2.13) and the proof of Proposition 2.4.2, in order to show that (2.14) holds, it suffices to show that

$$\begin{pmatrix}\varphi^{-n}(\varphi(\omega)_1) & -\varphi^{-n}(\omega_1)\end{pmatrix}\begin{pmatrix}-pu_{-n-1} & pu_{-n}\\ -u_{-n} & u_{-n+1}\end{pmatrix}\begin{pmatrix}0 & 0\\ -1 & a_p\end{pmatrix}$$

is congruent to 0 modulo $\mathbb{D}^0(V_f(1))$. But this follows easily from the fact that

$$\begin{pmatrix}\frac{1}{p}u_{-n+1} & -u_{-n}\end{pmatrix}\begin{pmatrix}-pu_{-n-1} & pu_{-n}\\ -u_{-n} & u_{-n+1}\end{pmatrix}\begin{pmatrix}0 & 0\\ -1 & a_p\end{pmatrix} = 0$$

and (2.12), so we are done. $\square$

By Remark 2.3.6, the image of $\mathcal{L}_\upsilon$ is $O(\log_p^{1/2})$ for any $\upsilon \in \mathbb{D}(V_f)$, so we obtain two Coleman maps:

Definition 2.5.3. *For $* = \vartheta, \upsilon$ and $\mathbf{z} \in \mathbb{H}^1_{\mathrm{Iw}}(V_{\bar{f}}(1))$, $\mathrm{Col}^*(\mathbf{z}) \in \Lambda_E$ is defined by*

$$\begin{pmatrix}\mathrm{Col}^\vartheta(\mathbf{z}) & \mathrm{Col}^\upsilon(\mathbf{z})\end{pmatrix} \cdot \log_p(\gamma)/(\gamma - 1) = \begin{pmatrix}\mathcal{L}_{\varphi(\omega)}(\mathbf{z}) & -\mathcal{L}_\omega(\mathbf{z})\end{pmatrix} A_\infty^{-1}. \tag{2.15}$$

In particular, we can define two p-adic L-functions

$$L_p^* = \mathrm{Col}^*(\mathbf{z}^{\mathrm{Kato}}) \in \Lambda_E$$

where $* = \vartheta, \upsilon$.

On choosing $[\varphi(\omega), \bar{\omega}] = 1$ for simplicity, we have, under the notation of Theorem 2.3.5,

$$\eta_\alpha = \varphi(\omega) - \beta\omega \qquad \text{and} \qquad \eta_\beta = \varphi(\omega) - \alpha\omega.$$

Note that $\det(A_\infty^{-1}) = \log_p(\gamma)/(\gamma - 1)$, we therefore obtain a decomposition:

$$L_{p,\alpha} = (\Upsilon_\infty^0 - \beta\Upsilon_\infty^1)L_p^\vartheta - (\Theta_\infty^0 - \beta\Theta_\infty^1)L_p^\upsilon \tag{2.16}$$

$$L_{p,\beta} = (\Upsilon_\infty^0 - \alpha\Upsilon_\infty^1)L_p^\vartheta - (\Theta_\infty^0 - \alpha\Theta_\infty^1))L_p^\upsilon \tag{2.17}$$

where $A_\infty^{-1} = \begin{pmatrix}\Theta_\infty^1 & \Upsilon_\infty^1 \\ \Theta_\infty^0 & \Upsilon_\infty^0\end{pmatrix}$. This generalises (2.11).

Remark 2.5.4. *The results above hold for any modular forms of weight 2. This setting is slightly more general than that in [Spr09].*

Chapter 3

Kernels of the Coleman maps

In addition to assumption (1), we assume the following holds.

- **Assumption (2)**: $p \geq k-1$.

Under these two conditions (which we assume to hold until the end of Chapter 6), we give an explicit description of the kernels of the plus and minus Coleman maps defined in Chapter 2. In particular, we generalise [Kob03, Proposition 8.18], which describe the kernels of $\mathrm{Col}^{\pm}$ in the case of elliptic curves defined over $\mathbb{Q}$.

3.1 Properties of H^1

Recall that when f corresponds to an elliptic curve E_f over $\mathbb{Q}$ and $T_f(1)$ is the Tate module of E_f, we have $E_f[p^\infty] \cong V_f/T_f(1)$ as $G_{\mathbb{Q}}$-modules. Therefore, the following lemma generalises [Kob03, Proposition 8.7], which says that E_f has no p-torsion defined over $\mathbb{Q}_\infty$.

Lemma 3.1.1. *For all $j \in \mathbb{Z}$ and $n \geq 0$, $(V_f/T_f)(j)^{G_{\mathbb{Q}_{p,n}}} = 0$.*

Proof. It is enough to show that $(V_f/T_f)^{G_{\mathbb{Q}_{p,\infty}}} = 0$. Since $V_f/T_f = \varinjlim_{\times\varpi} T_f/\varpi^n T_f$, it in fact suffices to show that $(T_f/\varpi T_f)^{G_{\mathbb{Q}_{p,\infty}}} = 0$.

By assumption (2), a result of Fontaine (a proof can be found in [Edi92]) says that

$$\rho_f|I = \begin{pmatrix} \psi^{k-1} & 0 \\ 0 & \psi'^{k-1} \end{pmatrix}$$

where ρ_f is the representation $G_{\mathbb{Q}} \to \mathrm{GL}(T_f/\varpi T_f)$, I is the inertia group of $G_{\mathbb{Q}_p}$ and ψ and ψ' are fundamental characters of level 2, i.e.

$$\ker\psi = \ker\psi' = G_{\mathbb{Q}_p^{\mathrm{ur}}(\sqrt[p^2-1]{p})}.$$

Hence, if $\sigma \in \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}(\sqrt[p^2-1]{p})/\mathbb{Q}_p^{\mathrm{ur}}(\sqrt[p-1]{p}))$, 1 is not an eigenvalue of $\rho_f(\sigma)$, as $p+1 \nmid k-1$ by assumption (2). Hence, there exists an element in the above Galois group which lifts to $G_{\mathbb{Q}_{p,\infty}}$ and $(T_f/\varpi T_f)^{G_{\mathbb{Q}_{p,\infty}}} = 0$ as required. □

We now give two immediate corollaries.

Corollary 3.1.2. *The projection $\mathbb{H}^1_{\mathrm{Iw}}(T_{\bar{f}}(j)) \to H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(j))$ is surjective for all j and n.*

Proof. It is enough to show that

$$\mathrm{cor}_{n/m} : H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(j)) \to H^1(\mathbb{Q}_{p,m}, T_{\bar{f}}(j))$$

is surjective for all $n \geq m$. On taking Pontryagin dual, it is equivalent to showing that

$$\mathrm{res}_{m/n} : H^1(\mathbb{Q}_{p,m}, V_f/T_f(k-1-j)) \to H^1(\mathbb{Q}_{p,n}, V_f/T_f(k-1-j))$$

is injective. But this immediately follows from the inflation-restriction exact sequence and Lemma 3.1.1, which says that $V_f/T_f(k-1-j)^{G_{\mathbb{Q}_{p,\infty}}} = 0$. □

Corollary 3.1.3. *For all n and j as above, $H^1(\mathbb{Q}_{p,n}, T_f(j)) \hookrightarrow H^1(\mathbb{Q}_{p,n}, V_f(j))$.*

Proof. From the short exact sequence $0 \to T_f(j) \to V_f(j) \to V_f/T_f(j) \to 0$, we obtain a long exact sequence

$$\cdots \to (V_f/T_f(j))^{G_{\mathbb{Q}_{p,n}}} \to H^1(\mathbb{Q}_{p,n}, T_f(j)) \to H^1(\mathbb{Q}_{p,n}, V_f(j)) \to \cdots.$$

Hence the result by Lemma 3.1.1. □

In particular, $H^1(\mathbb{Q}_{p,n}, T_f(j))$ can be identified as an $\mathcal{O}_E$-lattice of the E-vector space $H^1(\mathbb{Q}_{p,n}, V_f(j))$.

Another property of H^1 which we need is the injectivity of the restriction

$$H^1(\mathbb{Q}_{p,m}, V_f(j)) \xrightarrow{\mathrm{res}} H^1(\mathbb{Q}_{p,n}, V_f(j))$$

for $n \geq m$. But this follows easily from the inflation-restriction sequence and the fact that $V_f(j)^{G_{\mathbb{Q}_{p,\infty}}} = 0$ (immediate from Lemma 3.1.1). In particular, the same can be said about H^1_f. We regard $H^1_f(\mathbb{Q}_{p,m}, A)$ as a subgroup of $H^1_f(\mathbb{Q}_{p,n}, A)$ for $A = T_f(j)$ or $V_f(j)$ in the next section.

3.2 Some subgroups of H^1_f

Let $\eta^\pm$ be as defined in Chapter 2. For $1 \le j \le k-1$, we define two $E[G_n]$-modules

$$\begin{aligned} R^+_{n,j} &= \sum_{\sigma \in G_n} E \cdot \gamma_{n,j}(\eta_j^+)^\sigma \mod \omega \subset \mathbb{Q}_{p,n} \otimes \mathbb{D}(V_f(j))/\mathbb{D}^0(V_f(j)), \\ R^-_{n,j} &= \sum_{\sigma \in G_n} E \cdot \gamma_{n,j}(\eta_j^-)^\sigma \mod \omega \subset \mathbb{Q}_{p,n} \otimes \mathbb{D}(V_f(j))/\mathbb{D}^0(V_f(j)). \end{aligned} \tag{3.1}$$

Remark 3.2.1. *For $1 \le j \le k-1$, we have isomorphisms of $E[G_n]$-modules*

$$H^1_f(\mathbb{Q}_{p,n}, V_f(j)) \cong \mathbb{Q}_{p,n} \underset{\mathbb{Q}_p}{\otimes} \mathbb{D}(V_f(j))/\mathbb{D}^0(V_f(j)) \cong \mathbb{Q}_{p,n} \otimes E.$$

Under this identification, the corestriction map

$$\mathrm{cor}_{n/m} : H^1_f(\mathbb{Q}_{p,n}, V_f(j)) \to H^1_f(\mathbb{Q}_{p,m}, V_f(j))$$

corresponds to the trace map

$$\mathrm{Tr}_{n/m} \otimes \mathrm{id} : \mathbb{Q}_{p,n} \otimes E \to \mathbb{Q}_{p,m} \otimes E.$$

By Remark 3.2.1, we can identify $R^\pm_{n,j}$ with subsets of $\mathbb{Q}_{p,n} \otimes E$ and we have the following description.

Lemma 3.2.2. *By identifying $\mathbb{Q}_{p,n} \otimes \mathbb{D}(V(j))/\mathbb{D}^0(V(j))$ with $\mathbb{Q}_{p,n} \otimes E$, we have*

$$\begin{aligned} R^+_{n,j} &= \sum_{m \text{ even}} \sum_{\sigma \in G_m} E \cdot \zeta_{p^m}^\sigma + E, \\ R^-_{n,j} &= \sum_{m \text{ odd}} \sum_{\sigma \in G_m} E \cdot \zeta_{p^m}^\sigma + E \end{aligned} \tag{3.2}$$

where $m \le n$ in the summands.

Proof. Recall that

$$\gamma_{n,j} = p^{-n} \left(\sum_{i=0}^{n-1} \zeta_{p^{n-i}} \otimes \varphi^{i-n} + (1-\varphi)^{-1} \right)$$

and $\eta^\pm$ are given by the following:

$$\eta^+ = \frac{\varphi(\omega)}{[\varphi(\omega), \bar{\omega}]} \qquad \text{and} \qquad \eta^- = \frac{\omega}{[\varphi(\omega), \bar{\omega}]}.$$

Hence, we can apply Corollary A.2.1 to $R^\pm_{n,j}$ provided that

$$(p-1)(1-\varphi)^{-1}(\eta_j^\pm) \not\equiv \varphi^{-1}(\eta_j^\pm) \mod \omega,$$

which can be checked under assumption (1) (see the proof of Proposition B.5.1 for details in a more general setting). The result then follows from the fact that $\varphi^m(\omega) \equiv 0 \mod \omega$ iff m is an even integer (c.f. proof of Proposition 2.4.2). $\square$

In particular, on applying Lemmas A.1.1 and A.1.2 to (3.2), we have

$$R_{n,j}^+ + R_{n,j}^- = \mathbb{Q}_{p,n} \otimes E \quad \text{and} \quad R_{n,j}^+ \cap R_{n,j}^- = E$$

under the identification given by Remark 3.2.1. Let

$$\mathbb{Q}_{p,n}^{\pm} = \{x \in \mathbb{Q}_{p,n} : \mathrm{Tr}_{n/m+1}(x) \in \mathbb{Q}_{p,m}\ \forall m \in S_n^{\pm}\}$$

where $S_n^{\pm}$ are defined by

$$\begin{aligned} S_n^+ &= \{m \in [0, n-1] : m \text{ even}\}, \\ S_n^- &= \{m \in [0, n-1] : m \text{ odd}\}. \end{aligned}$$

Then, $R_{n,j}^{\pm}$ can be identified with $\mathbb{Q}_{p,n}^{\pm} \otimes E$:

Lemma 3.2.3. *For j and n as above, $\mathbb{Q}_{p,n}^{\pm} \otimes E = R_{n,j}^{\pm}$.*

Proof. By (3.2), it is easy to check that $R_{n,j}^{\pm} \subset \mathbb{Q}_{p,n}^{\pm} \otimes E$, so

$$\dim_E R_{n,j}^{\pm} \leq \dim_E \left(\mathbb{Q}_{p,n}^{\pm} \otimes E\right).$$

Since $R_{n,j}^+ + R_{n,j}^- = \mathbb{Q}_{p,n} \otimes E$, we have

$$\mathbb{Q}_{p,n}^+ \otimes E + \mathbb{Q}_{p,n}^- \otimes E = R_{n,j}^+ + R_{n,j}^- = \mathbb{Q}_{p,n} \otimes E.$$

If $x \in \mathbb{Q}_{p,n}^+ \cap \mathbb{Q}_{p,n}^-$, then $\mathrm{Tr}_{n/m+1}(x) \in \mathbb{Q}_{p,m}$ for all $m \leq n-1$, hence $x \in \mathbb{Q}_p$. Therefore, we have $\mathbb{Q}_{p,n}^+ \cap \mathbb{Q}_{p,n}^- = \mathbb{Q}_p$.

Hence, by the formula

$$\dim A + \dim B = \dim(A+B) + \dim(A \cap B),$$

we have

$$\dim_E \left(\mathbb{Q}_{p,n}^{\pm} \otimes E\right) = \dim_E R_{n,j}^{\pm}$$

and we are done. $\square$

Let $H_f^1(\mathbb{Q}_{p,n}, V_f(j))^{\pm}$ denote the image of $R_{n,j}^{\pm}$ under $\exp_{n,j}$, then Remark 3.2.1 and Lemma 3.2.3 implies that it is equal to

$$\left\{x \in H_f^1(\mathbb{Q}_{p,n}, V_f(j)) : \mathrm{cor}_{n/m+1}(x) \in H_f^1(\mathbb{Q}_{p,n}, V_f(j))\ \forall m \in S_n^{\pm}\right\}.$$

By Corollary 3.1.3, if we define

$$H^1_f(\mathbb{Q}_{p,n}, T_f(j))^{\pm} = H^1_f(\mathbb{Q}_{p,n}, V_f(j))^{\pm} \cap H^1_f(\mathbb{Q}_{p,n}, T_f(j)),$$

then it is equal to

$$\left\{x \in H^1_f(\mathbb{Q}_{p,n}, T_f(j)) : \mathrm{cor}_{n/m+1}(x) \in H^1_f(\mathbb{Q}_{p,m}, T_f(j)) \ \forall m \in S_n^{\pm}\right\}$$

generalising the definition of $E^{\pm}$ in [Kob03].

3.3 Description of the kernels

Let $\mathbf{z} \in \mathbb{H}^1_{\mathrm{Iw}}(T_{\bar{f}}(k-1))$. Under the notation of Chapter 2, we have

$$\mathcal{L}_{\eta^{\pm}}(\mathbf{z}) = O(\log_p^{\frac{k-1}{2}}),$$

so $\mathcal{L}_{\eta^{\pm}}(\mathbf{z}) = 0$ iff

$$P_{n,r}(\eta^{\pm}, z_{-r,n}) = 0$$

for all $n \geq 0$ and more than $(k-1)/2$ different values of r with $0 \leq r \leq k-2$. Recall that

$$P_{n,r}(\cdot, z_{-r,n}) = r! \sum_{\sigma \in G_n} \left[\exp_{n,r+1}(\gamma_{n,r+1}(\cdot)^{\sigma}), z_{-r,n}\right]_n \sigma.$$

Therefore, $\ker P_{n,r}(\eta^{\pm}, \cdot)$ is just the annihilator of

$$\left\{\exp_{n,r+1}(\gamma_{n,r+1}(\eta^{\pm})^{\sigma}) : \sigma \in G_n\right\}$$

under the pairing

$$H^1(\mathbb{Q}_{p,n}, V_f(r+1)) \times H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1-r)) \to E$$

which coincides with the annihilator of $H^1_f(\mathbb{Q}_{p,n}, T_f(r+1))^{\pm}$ under the pairing

$$H^1(\mathbb{Q}_{p,n}, T_f(r+1)) \times H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1-r)) \to \mathcal{O}_E. \tag{3.3}$$

We denote this annihilator by $H^1_{\pm}(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1-r))$.

Define

$$\mathbb{H}^1_{\mathrm{Iw},\pm}(T_{\bar{f}}(k-1-r)) = \varprojlim H^1_{\pm}(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1-r)).$$

As $\log_{p,k}^{\pm} \neq 0$ and $\mathcal{L}_{\eta^\pm} = \log_{p,k}^{\pm} \mathrm{Col}^{\pm}$, we have

$$\ker \mathcal{L}_{\eta^\pm} = \ker\left(\mathrm{Col}^{\pm}\right) = \bigcap_{r=0}^{k-2} \mathrm{Tw}_r\left(\mathbb{H}^1_{\mathrm{Iw},\pm}\left(T_{\bar{f}}(k-1-r)\right)\right)$$

by Corollary 3.1.2.

In fact, by the proposition below, it suffices to take just one term in the intersection.

Proposition 3.3.1. $\mathrm{Tw}_r\left(\mathbb{H}^1_{\mathrm{Iw},\pm}\left(T_{\bar{f}}(k-1-r)\right)\right) = \mathbb{H}^1_{\mathrm{Iw},\pm}(T_{\bar{f}}(k-1))$ *for all integers r such that $0 \leq r \leq k-2$.*

Proof. Since $\mathrm{Col}^{\pm}(\mathbf{z}) = O(1)$ for all $\mathbf{z} \in \mathbb{H}^1_{\mathrm{Iw}}(T_{\bar{f}}(k-1))$, it is uniquely determined by its values at an infinite number of characters (see e.g. [Pol03, Lemma 3.2]). Hence, if there exists a fixed r such that $P_{n,r}(\eta^{\pm}, z_{n,-r}) = 0$ for all n, then $\mathrm{Col}^{\pm}(\mathbf{z}) = 0$. Therefore, we have

$$\ker(\mathrm{Col}^{\pm}) = \mathrm{Tw}_r\left(\mathbb{H}^1_{\mathrm{Iw},\pm}\left(T_{\bar{f}}(k-1-r)\right)\right)$$

and we are done. □

Corollary 3.3.2. *We have*

$$\ker \mathcal{L}_{\eta^\pm} = \ker\left(\mathrm{Col}^{\pm}\right) = \mathrm{Tw}_r\left(\mathbb{H}^1_{\mathrm{Iw},\pm}\left(T_{\bar{f}}(k-1-r)\right)\right)$$

for any integer $0 \leq r \leq k-2$.

3.4 Properties of the kernels

We have seen that $\ker(\mathrm{Col}^{\pm})$ can be written in terms of $H^1_{\pm}$, about which we now say a little bit more.

3.4.1 A description using the dual exponential

Proposition 3.4.1. *Let $0 \leq r \leq k-2$. For any $x \in H^1_f(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1-r))$ and $m \leq n$, write $x_m = \exp^*_{m,r+1}(\mathrm{cor}_{n/m}(x))$. Then, $H^1_{\pm}(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1-r))$ coincides with the following set:*

$$\left\{x \in H^1_f(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1-r)) : x_0 = 0 \text{ and } x_m = \frac{x_{m-1}}{p} \forall m \in S_n^{\mp}\right\}.$$

Proof. On the one hand, (3.3) factors through

$$H^1_f(\mathbb{Q}_{p,n}, T_f(1)) \times \frac{H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))}{H^1_f(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))} \to \mathbb{Z}_p.$$

On the other hand, the pairing defined by (2.5) factors through

$$\Big(\mathbb{Q}_{p,n} \otimes \mathbb{D}(V_f(r+1))/\mathbb{D}^0(V_f(r+1))\Big) \times \Big(\mathbb{Q}_{p,n} \otimes \mathbb{D}^0(V_{\bar{f}}(k-1-r))\Big) \to \mathbb{Q}_{p,n} \otimes E.$$

Hence, the compatibility of the two pairings, namely

$$[\exp_{n,r+1}(\cdot), \cdot]_n = \mathrm{Tr}_{n/0} \otimes \mathrm{id}[\cdot, \exp^*_{n,r+1}(\cdot)]'_n,$$

implies that $H^1_\pm(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))$ is the $\exp^*_{n,r+1}$-preimage of

$$\Big(\mathbb{Q}^\pm_{p,n} \otimes \mathbb{D}(V_f(r+1))/\mathbb{D}^0(V_f(r+1))\Big)^\perp$$

But we have:

$$\Big(\mathbb{Q}^\pm_{p,n} \otimes \mathbb{D}(V_f(r+1))/\mathbb{D}^0(V_f(r+1))\Big)^\perp = \Big(\mathbb{Q}^\pm_{p,n}\Big)^\perp \otimes \mathbb{D}^0(V_{\bar{f}}(k-1-r))$$

where $\Big(\mathbb{Q}^\pm_{p,n}\Big)^\perp$ is the orthogonal complement of $\mathbb{Q}^\pm_{p,n}$ under the pairing

$$\begin{array}{rcl} \mathbb{Q}_{p,n} \times \mathbb{Q}_{p,n} & \to & \mathbb{Q}_p \\ (x,y) & \mapsto & \mathrm{Tr}_{n/0}(xy). \end{array}$$

By Corollary A.2.1, it is easy to check that

$$\{x \in \mathbb{Q}_{p,n} : \mathrm{Tr}_{n/0}(x) = 0 \text{ and } \mathrm{Tr}_{n/m+1}(x) \in \mathbb{Q}_{p,m}\ \forall m \in S^\mp_n\} \subset \Big(\mathbb{Q}^\pm_{p,n}\Big)^\perp.$$

By comparing dimensions of the two subspaces (see the proof of Lemma 4.3.1 below for some explicit calculations), we see that equality holds and we are done. □

Hence, on combining this with Proposition 3.3.1, we have:

Corollary 3.4.2. *Let* $\mathbf{z} = (z_n)_n \in \mathbb{H}^1_{\mathrm{Iw}}(T_{\bar{f}}(k-1))$, *then* $\mathrm{Col}^\pm(\mathbf{z}) = 0$ *iff*

$$\exp^*_{0,k-1}(z_0) = 0 \text{ and } \exp^*_{m,1}(z_m) = \frac{1}{p}\exp^*_{m-1,1}(z_{m-1}) \forall m \in S^\mp_\infty$$

where $S^\pm_\infty = \cup_{n\geq 1} S^\pm_n$.

3.4.2 Pontryagin duality

The Pontryagin duality gives a pairing:

$$H^1(\mathbb{Q}_{p,n}, V_f/T_f(r+1)) \times H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1-r)) \to E/\mathcal{O}_E. \tag{3.4}$$

We can describe the annihilator of $H^1_{\pm}(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1-r))$ under this pairing explicitly:

Lemma 3.4.3. *$H^1_f(\mathbb{Q}_{p,n}, T_f(r+1))^{\pm} \otimes E/\mathcal{O}_E \hookrightarrow H^1(\mathbb{Q}_{p,n}, V_f/T_f(r+1))$ and it can be identified as the annihilator of $H^1_{\pm}(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1-r))$ under (3.4).*

Proof. By definitions, we have an exact sequence

$$0 \to H^1_{\pm}(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1-r)) \to H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1-r)) \to \mathrm{Hom}(H^1_f(\mathbb{Q}_{p,n}, T_f(r+1))^{\pm}, \mathcal{O}_E).$$

Taking Pontryagin duals, we have

$$H^1_f(\mathbb{Q}_{p,n}, T_f(r+1))^{\pm} \otimes E/\mathcal{O}_E \to H^1(\mathbb{Q}_{p,n}, V_f/T_f(r+1)) \to H^1_{\pm}(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1-r))^{\vee} \to 0.$$

Therefore, the second part of the lemma follows from the first. Recall that $(V_f/T_f(r+1))^{G_{\mathbb{Q}_{p,n}}} = 0$ by Lemma 3.1.1, so we have

$$H^1_f(\mathbb{Q}_{p,n}, T_f(r+1)) \otimes E/\mathcal{O}_E \hookrightarrow H^1_f(\mathbb{Q}_{p,n}, V_f/T_f(r+1)) \subset H^1(\mathbb{Q}_{p,n}, V_f/T_f(r+1)).$$

Hence, it suffices to show that we have inclusion

$$H^1_f(\mathbb{Q}_{p,n}, T_f(r+1))^{\pm} \otimes E/\mathcal{O}_E \hookrightarrow H^1_f(\mathbb{Q}_{p,n}, T_f(r+1)) \otimes E/\mathcal{O}_E.$$

But this follows from [Kob03, Lemma 8.17]. $\square$

We write $H^1_f(\mathbb{Q}_{p,n}, V_f/T_f(j))^{\pm}$ for $H^1_f(\mathbb{Q}_{p,n}, T_f(j))^{\pm} \otimes E/\mathcal{O}_E$, which is identified as a subgroup of $H^1_f(\mathbb{Q}_{p,n}, V_f/T_f(j))$. Note that it corresponds to the definition of $E^{\pm}(\mathbb{Q}_{p,n}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ given in [Kob03] and this is used to define $\mathrm{Sel}_p^{\pm}$ in Chapter 5.

Chapter 4

Images of the Coleman maps

In this chapter, we describe the images of $\mathrm{Col}^{\pm}$ (under assumptions (1) and (2)). By Corollary 3.1.2, any elements of $H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))$ can be lifted to a global element of $\mathbb{H}^1_{\mathrm{Iw}}(T_{\bar{f}}(k-1))$. Hence, we can in fact think of $\mathcal{L}_{\eta^{\pm},n}$ and $\mathrm{Col}^{\pm}_n$ as maps from $H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))$ to $E[G_n]$. This allows us to give a description of $\mathrm{Im}(\mathrm{Col}^{\pm})$ by studying $\mathrm{Im}(\mathrm{Col}^{\pm}_n)$.

In [Kob03, Section 8], the images of the plus and minus Coleman maps for elliptic curves over $\mathbb{Q}$ are shown to be the following:

$$\begin{aligned}
\mathrm{Im}(\mathrm{Col}^{+}) &= (\gamma - 1)\Lambda_{\mathcal{O}_E} + \left(\sum_{\sigma\in\Delta} \sigma\right)\Lambda_{\mathcal{O}_E},\\
\mathrm{Im}(\mathrm{Col}^{-}) &= \Lambda_{\mathcal{O}_E}.
\end{aligned}$$

In particular, the Δ-invariant part of $\mathrm{Im}(\mathrm{Col}^{\pm})$ is the whole of $\Gamma_{\mathcal{O}_E}$. For a general f, we unfortunately do not know whether the images of the Coleman maps are inside $\Lambda_{\mathcal{O}_E}$ or not. However, after multiplying by a power of ϖ, we will show that the Δ-invariant part of $\mathrm{Im}(\mathrm{Col}^{\pm})$ agree with the above descriptions and the same can be said for the whole of $\mathrm{Im}(\mathrm{Col}^{-})$.

4.1 Divisibility by $\Phi_m(\gamma)$

We have seen that the image of $\mathcal{L}_{\eta^{\pm}}$ is divisible by $\log^{\pm}_{p,k}$. We give a necessary and sufficient condition for such divisibility at the finite level below.

Recall that $G_\infty = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \Delta \times \Gamma$ where Δ is a finite group of order

$p-1$, $\Gamma \cong \mathbb{Z}_p$ and γ is a fixed topological generator of Γ. We have

$$\mathcal{O}_E[G_n] \cong \mathcal{O}_E[\Delta][\gamma]/(\gamma^{p^{n-1}}-1)$$

and

$$\Phi_m(\gamma) = 1 + \gamma^{p^{m-1}} + \gamma^{2p^{m-1}} + \cdots + \gamma^{(p-1)p^{m-1}}.$$

Therefore, if $m \geq n$, then $\Phi_m(\gamma) = p$ in $\mathcal{O}_E[G_n]$, so we only consider $m < n$ here.

Lemma 4.1.1. *Let $m < n$ and*

$$f = \sum_{\substack{r \bmod p^{n-1} \\ \sigma \in \Delta}} c_{r,\sigma} \cdot \sigma \cdot \gamma^r \in \mathcal{O}_E[G_n].$$

For each $\sigma \in \Delta$ and $r \mod p^m$, write

$$b_{r,\sigma} = c_{r,\sigma} + c_{r+p^m,\sigma} + \cdots + c_{r-p^m,\sigma}.$$

Then, f is divisible by $\Phi_m(\gamma)$ in $\mathcal{O}_E[G_n]$ iff $b_{r,\sigma} = b_{s,\sigma}$ whenever $r \equiv s \mod p^{m-1}$.

Proof. Let $f = g\Phi_m(\gamma)$ and $g = \sum a_{r,\sigma} \cdot \sigma \cdot \gamma^r \in \mathcal{O}_E[G_n]$. Then the coefficient of $\sigma\gamma^r$ in f is given by

$$a_{r,\sigma} + a_{r-p^{m-1},\sigma} + \cdots + a_{r-(p-1)p^{m-1},\sigma}.$$

Hence, $b_{r,\sigma}$ as defined in the statement of the lemma is just the sum of the coefficients $a_{s,\sigma}$ of g with $s \equiv r \mod p^{m-1}$. Hence $b_{r,\sigma} = b_{s,\sigma}$ whenever $r \equiv s \mod p^{m-1}$.

Conversely, let $\sum c_{r,\sigma} \cdot \sigma \cdot \gamma^r \in \mathcal{O}_E[G_n]$ and define $b_{r,\sigma}$ as in the statement of the lemma. Assume that $b_{r,\sigma} = b_{s,\sigma}$ for all $r \equiv s \mod p^{m-1}$. Let $f_\sigma(\gamma) = \sum_r c_{r,\sigma} \cdot \gamma^r$, so $f = \sum f_\sigma \cdot \sigma$. We have

$$\begin{aligned} f_\sigma(\zeta_{p^m}) &= \sum_{r \bmod p^m} \left(\sum_{s \equiv r (p^m)} c_{s,\sigma} \right) \zeta_{p^m}^r \\ &= \sum_{r \bmod p^m} b_{r,\sigma} \zeta_{p^m}^r \\ &= \sum_{s \bmod p^{m-1}} b_{s,\sigma} \sum_{r \equiv s (p^{m-1})} \zeta_{p^m}^r \\ &= 0. \end{aligned}$$

Hence, $\Phi_m(\gamma)$ divides f and we are done. $\square$

Applying this to the image of $\mathcal{L}_{\eta^\pm,n}$, we have:

Corollary 4.1.2. *For any $z \in H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))$, $\mathcal{L}_{\eta^\pm,n}(z)$ is divisible by $\Phi_m(\gamma)$ over $E[G_n]$ if $m \in S_n^\pm$.*

Proof. The image of $\mathcal{L}_{\eta^\pm,n}(z)$ is given by the following composition

$$H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1)) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{O}_E}\left(H^1(\mathbb{Q}_{p,n}, T_f(1)), \mathcal{O}_E\right) \to E[G_n]$$

where the first isomorphism is induced by the pairing (3.3) and the second map is given by

$$\begin{aligned} \mathrm{Hom}_{\mathcal{O}_E}\left(H^1(\mathbb{Q}_{p,n}, T_f(1)), \mathcal{O}_E\right) &\to E[G_n] \\ \theta &\mapsto \sum_{\tau \in G_n} \theta(\exp_{n,1}(\gamma_{n,1}(\eta_1^\pm)^\tau)\tau, \end{aligned} \tag{4.1}$$

with θ extended to an element of $\mathrm{Hom}_E(H^1(\mathbb{Q}_{p,n}, V_f(1)), E)$ in the natural way. Therefore, it is enough to show that $\gamma_{n,1}(\eta_1^\pm)^\tau \mod \omega$, $\tau \in G_n$ satisfy the relations described in Lemma 4.1.1. Let $\sigma \in \Delta$. For $\eta = \eta^\pm$, we write

$$\begin{aligned} \eta_{r,\sigma} &= \sum_{s \equiv r (p^m)} \gamma_{n,1}(\eta_1)^{\sigma\gamma^s} \\ &= p^{-m-1}\left((1-\varphi)^{-1}(\eta_1) + \zeta_p \otimes \varphi^{-1}(\eta_1) + \cdots + \zeta_{p^{m+1}} \otimes \varphi^{-m-1}(\eta_1)\right)^{\sigma\gamma^r}. \end{aligned}$$

Therefore, if $\varphi^{-m-1}(\eta_1) \equiv 0 \mod \omega$, then $\eta_{r,\sigma} = \eta_{s,\sigma}$ for $r \equiv s \mod p^{m-1}$, as $(\zeta_{p^m})^{\sigma\gamma^r} = (\zeta_{p^m})^{\sigma\gamma^s}$. Hence, by the definitions of $\eta^\pm$ as given in the proof of Proposition 2.4.2, we are done. $\square$

By considering its image modulo $(u^{-j}\gamma)^{p^{n-1}} - 1$ similarly, one can deduce Proposition 2.4.2. We can in fact say a bit more about the image of $\mathcal{L}_{\eta^+,n}$.

Lemma 4.1.3. *With the notation above, if $\mathcal{L}_{\eta^+,n}(z) = \sum c_{r,\sigma} \cdot \sigma \cdot \gamma^r$, then $\sum_r c_{r,\sigma}$ is independent of σ.*

Proof. For each $\sigma \in \Delta$, we have

$$\sum_r \gamma_{n,1}(\eta_1^+)^{\sigma\gamma^r} = p^{-1}\left((1-\varphi)^{-1}(\eta_1^+) + \zeta_p \otimes \varphi^{-1}(\eta_1^+)\right)^\sigma.$$

But $\varphi^{-1}(\eta_1^+) \equiv 0 \mod \omega$, so we are done. $\square$

We will see later on that these conditions in fact characterise the images of $\mathcal{L}_{\eta^\pm,n}$ completely.

4.2 Images of $\log_{p,k}^{\pm}$ in $\mathcal{O}_E[G_n]$

We now fix an integer j such that $0 < j \leq k-2$.

Lemma 4.2.1. *Let $x \in 1 + p\mathbb{Z}_p$. There exists a constant c such that for any positive integer n, $v_p(x^{p^n} - 1) = n + c$.*

Proof. Let $x = 1 + m$ where $m \in p\mathbb{Z}_p$, so $v_p(m) \geq 1$. We have expansion

$$x^{p^n} - 1 = (1+m)^{p^n} - 1 = m^{p^n} + \binom{p^n}{p^n - 1} m^{p^n - 1} + \cdots + \binom{p^n}{1} m.$$

For $r > 0$, $v_p(\binom{p^n}{r}) = n - v_p(r)$, so

$$v_p\left(\binom{p^n}{r} m^r\right) = r v_p(m) - v_p(r) + n.$$

If $r = p^s a$ where $p \nmid a$ and $a > 1$, then

$$v_p\left(\binom{p^n}{r} m^r\right) > v_p\left(\binom{p^n}{p^s} m^{p^s}\right).$$

Therefore, the set $\left\{v_p\left(\binom{p^n}{r} m^r\right) : r > 0\right\}$ takes its minimum value at $r = p^s$ for some s.

Consider the curve

$$f(t) = p^t v_p(m) - t, \text{ for } t \in \mathbb{R}.$$

It has a unique global minimum when $p^t = (v_p(m) \log p)^{-1}$, so the curve is strictly increasing on $t \geq 0$. Therefore, for a fixed n, the minimum of the values

$$v_p\left(\binom{p^n}{p^s} m^{p^s}\right) = p^s v_p(m) - s + n$$

is just $v_p(m) + n$, which is attained at a unique s, hence the result. □

Corollary 4.2.2. *If $m \geq n$, then $\Phi_m(u^{-j}\gamma)/p$ is congruent to a unit of $\mathbb{Z}_p$ modulo $\gamma^{p^{n-1}} - 1$.*

Proof. By definition,

$$\Phi_m(u^{-j}\gamma) = \frac{(u^{-j}\gamma)^{p^m} - 1}{(u^{-j}\gamma)^{p^{m-1}} - 1},$$

so as elements of $\mathcal{O}_E[G_n]$, we have

$$\frac{1}{p}\Phi_m(u^{-j}\gamma) = \frac{u^{-jp^m} - 1}{p(u^{-jp^{m-1}} - 1)}.$$

But $u \in 1 + p\mathbb{Z}_p$ by definition, so we are done by Lemma 4.2.1. □

Remark 4.2.3. *We have* $\log^{\pm}_{p,k} \equiv p^{1-k}\lambda_{\pm}\prod_{j=0}^{k-2}\omega_n^{\pm}(u^{-j}\gamma) \mod (\gamma^{p^{n-1}}-1)$ *where* $\lambda_{\pm}$ *is a unit of* $\mathbb{Z}_p$ *and* $\omega_n^{\pm}$ *is defined by*

$$\begin{aligned}\omega_n^{+}(1+X) &= \prod_{1\le m<n/2}\Phi_{2m}(1+X)/p,\\ \omega_n^{-}(1+X) &= \prod_{1\le m<(n+1)/2}\Phi_{2m-1}(1+X)/p.\end{aligned}$$

4.3 The images of $\mathrm{Col}_n^{\pm}$

Let $R^{\pm}_{n,j}$ be the vector spaces defined by (3.1). We have:

Lemma 4.3.1. *The dimensions of the* E*-vector spaces* $R^{\pm}_{n,j}$ *are given by*

$$\begin{aligned}\dim_E R^{+}_{n,j} &= 1+\sum_{1\le m\le n/2}p^{2m-2}(p-1)^2\\ \dim_E R^{-}_{n,j} &= p-1+\sum_{1\le m\le (n-1)/2}p^{2m-1}(p-1)^2\end{aligned}$$

Proof. By Lemmas A.1.1 and A.1.2 and (3.2), we have

$$\begin{aligned}\dim_E R^{+}_{n,j} &= \dim_{\mathbb{Q}_p}\mathbb{Q}_p+\sum_{1\le m\le n/2}\dim_{\mathbb{Q}_p}\mathbb{Q}_p^{(2m)}\\ \dim_E R^{-}_{n,j} &= \dim_{\mathbb{Q}_p}\mathbb{Q}_p+\sum_{1\le m\le (n-1)/2}\dim_{\mathbb{Q}_p}\mathbb{Q}_p^{(2m+1)}\end{aligned}$$

where $\mathbb{Q}_p^{(m)}$ denotes the $\mathbb{Q}_p$-vector space generated by $\{\zeta_{p^m}^{\sigma} : \sigma\in G_m\}$. For $m>1$,

$$\begin{aligned}\dim_{\mathbb{Q}_p}\mathbb{Q}_p^{(m)} &= \dim_{\mathbb{Q}_p}\mathbb{Q}_{p,m}-\dim_{\mathbb{Q}_p}\mathbb{Q}_{p,m-1}\\ &= p^{m-1}(p-1)-p^{m-2}(p-1)\\ &= p^{m-2}(p-1)^2\end{aligned}$$

and $\dim_{\mathbb{Q}_p}\mathbb{Q}_p^{(1)}=p-2$, so we are done. $\square$

The dimensions of these vector spaces enables us to obtain the following:

Proposition 4.3.2. *Let* $f=\sum_{\sigma\in\Delta}\sum_{r=0}^{p^{n-1}-1}a_{r,\sigma}\cdot\sigma\cdot u^r\in E[G_n]$. *If* $\omega_n^{\pm}$ *is as defined in Remark 4.2.3, then:*

(a) There exists $z\in H^1(\mathbb{Q}_{p,n},V_{\bar f}(k-1))$ *such that* $\mathrm{Col}_n^{-}(z)\equiv f \mod \omega_n^{+}(\gamma)$.

(b) If moreover $\sum_r a_{r,\sigma_1} = \sum_r a_{r,\sigma_2}$ *for all* $\sigma_1, \sigma_2 \in \Delta$*, then there exists* $z \in H^1(\mathbb{Q}_{p,n}, V_{\bar{f}}(k-1))$ *such that* $\mathrm{Col}_n^+(z) \equiv f \mod \omega_n^-(\gamma)$*.*

Proof. We only prove (b), as (a) can be proved in the same way. Define

$$U_n = \left\{ g = \sum c_{r,\sigma} \cdot \sigma \cdot \gamma^r \in E[G_n] : \log_{p,k}^+ |g, \sum_r c_{r,\sigma_1} = \sum_r c_{r,\sigma_1} \forall \sigma_1, \sigma_2 \in \Delta \right\}.$$

Then U_n is a vector subspace of $E[G_n]$ over E. By remark 4.2.3,

$$\log_{p,k}^+ \equiv p^{1-k} \lambda_+ \prod_{j=0}^{k-2} \omega_n^+(u^{-j}\gamma) \mod (\gamma^{p^{n-1}} - 1)$$

for some $\lambda_+ \in \mathcal{O}_E^\times$. Since $\omega_n^+(u^{-j}(1+X))$ and $(1+X)^{p^{n-1}} - 1$ are coprime for $j > 0$, $\log_{p,k}^+ |g$ iff $\omega_n^+(\gamma)|g$. But Φ_{m_1} and Φ_{m_2} are coprime if $m_1 \neq m_2$, so $\omega_n^+(\gamma)|g$ iff $\Phi_m(\gamma)|g$ for all even $m < n$.

Let $g = \sum c_{r,\sigma} \cdot \sigma \cdot u^r$. For each even $m < n$, let

$$b_{r,\sigma}^{(m)} = c_{r,\sigma} + c_{r+p^m,\sigma} + \cdots + c_{r-p^m,\sigma}.$$

Then, by Lemma 4.1.1, $\Phi_m(\gamma)|g$ iff $b_{r,\sigma}^{(m)} = b_{s,\sigma}^{(m)}$ for all $\sigma \in \Delta$ and $r \equiv s \mod p^{m-1}$. For each such m and $\sigma \in \Delta$, there are p^{m-1} values of modulo p^{m-1}, each is equated to $p-1$ different values. Since $|\Delta| = p-1$, there are $p^{m-1}(p-1)^2$ linearly independent equations for each m. Together with the equations of $\sum_r c_{r,\sigma}$, there are in total

$$p - 2 + \sum_{1 \leq m \leq n/2} p^{2m-1}(p-1)^2$$

equations describing the coefficients of elements of the U_n, which gives the codimension of U_n over E in $E[G_n]$.

By Corollary 4.1.2 and Lemma 4.1.3, for $z \in H^1(\mathbb{Q}_{p,n}, V_{\bar{f}}(k-1))$, $\mathcal{L}_{\eta^+,n}(z)$ lies inside the above subspace. But the dimension of the image is given by $\dim_E R_{n,1}^+$ which is the same as the dimension of U_n by Lemma 4.3.1, so

$$\mathcal{L}_{\eta^+,n}\left(H^1(\mathbb{Q}_{p,n}, V_{\bar{f}}(k-1))\right) = U_n$$

as E-vector spaces and there exists some z such that $\mathcal{L}_{\eta^+,n}(z) = g$. This implies

$$\log_{p,k}^+ \mathrm{Col}_n^+(z) \equiv f \log_{p,k}^+ \mod (\gamma^{p^{n-1}} - 1).$$

The factors of $\omega_n^+(u^{-j}\gamma)$ on both sides can be cancelled out for $j > 0$ as $\omega_n^+(u^{-j}\gamma)$ is coprime to $\omega_n^+(\gamma)$. Since

$$p^{n-1}(\gamma-1)\omega_n^+(\gamma)\omega_n^-(\gamma) = \gamma^{p^{n-1}} - 1,$$

we deduce that

$$\mathrm{Col}_n^+(z) \equiv f \mod ((\gamma-1)\omega_n^-(\gamma)),$$

which implies (b). □

4.4 The images of $\mathrm{Col}^\pm$

In the previous section, we studied the images of $H^1(\mathbb{Q}_{p,n}, V_{\bar{f}}(k-1))$ under $\mathrm{Col}_n^\pm$. To understand the images of $\mathrm{Col}^\pm$, we have to understand those of $H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))$ as well.

Lemma 4.4.1. *For all n, there exist $r_n^\pm \in \mathbb{Z}$ such that*

$$\mathcal{L}_{\eta^\pm,n}(H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))) = \mathcal{L}_{\eta^\pm,n}(H^1(\mathbb{Q}_{p,n}, V_{\bar{f}}(k-1))) \cap \varpi^{r_n^\pm}\mathcal{O}_E[G_n].$$

Proof. Note that $\exp_{n,1}(\gamma_{n,1}(\eta_1^\pm)) \neq 0$. As an element of $H^1(\mathbb{Q}_{p,n}, T_f(1))$, it lifts to a cocycle on $G_{\mathbb{Q}_{p,n}}$. By considering the image of this cocycle in $V_f(1)$, which is invariant under the action of G_n, there exists $r_n^\pm$ such that

$$\varpi^{-r_n^\pm}\exp_{n,1}(\gamma_{n,1}(\eta^\pm)^\tau) \in H^1(\mathbb{Q}_{p,n}, T_f(1)) \setminus \varpi H^1(\mathbb{Q}_{p,n}, T_f(1))$$

for all $\tau \in G_n$.

Recall from (4.1) that $\mathcal{L}_{\eta^\pm,n}$ is given by:

$$\begin{aligned} &\mathrm{Hom}_E\left(H^1(\mathbb{Q}_{p,n}, V_f(1)), E\right) \to E[G_n] \\ &\qquad\qquad \theta \mapsto \sum_{\tau\in G_n} \theta(\exp_{n,1}(\gamma_{n,1}(\eta_1^\pm)^\tau)\tau, \end{aligned}$$

where we have identified $\mathrm{Hom}_E\left(H^1(\mathbb{Q}_{p,n}, V_f(1)), E\right)$ with $H^1(\mathbb{Q}_{p,n}, V_{\bar{f}}(k-1))$. Under this identification, $H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))$ corresponds to the set of maps which send $H^1(\mathbb{Q}_{p,n}, T_f(1))$ (which is identified as a subset of $H^1(\mathbb{Q}_{p,n}, V_f(1))$ as discussed in Chapter 3) to $\mathcal{O}_E$. Therefore, we have

$$\left\{\theta(\exp_{n,1}(\gamma_{n,1}(\eta_1^\pm)^\tau) : \theta \in H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))\right\} = \varpi^{r_n^\pm}\mathcal{O}_E$$

for all $\tau \in G_n$. This implies that the LHS of the equation in the statement of the lemma is contained in the RHS.

Conversely, if $x \in$RHS, then there exists $\theta \in H^1(\mathbb{Q}_{p,n}, V_{\bar{f}}(k-1))$ such that $\sum_{\tau \in G_n} \theta(\exp_{n,1}(\gamma_{n,1}(\eta_1^{\pm})^{\tau})\tau = x$ by Proposition 4.3.2. In particular,

$$\theta\left(\varpi^{-r_n^{\pm}} \exp_{n,1}(\gamma_{n,1}(\eta_1^{\pm})^{\tau}\right) \in \mathcal{O}_E$$

for all $\tau \in G_n$. Hence, there exists $\tilde{\theta} \in H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))$ such that θ and $\tilde{\theta}$ agree on $\varpi^{-r_n^{\pm}} \exp_{n,1}(\gamma_{n,1}(\eta_1^{\pm})^{\tau})$ which shows that $x \in$LHS. □

Lemma 4.4.2. *Let $r_n^{\pm}$ be the integers defined in Lemma 4.4.1, then there exist $c_{\pm}$ such that $r_n^{\pm} = -e(k-1)\lfloor n/2 \rfloor + c_{\pm}$ for n sufficiently large where e is the ramification degree of E.*

Proof. By Remark 2.3.6,

$$\Omega_{V_f(1),1}((1+\pi) \otimes \eta_1^{\pm}) = O(\log_p^{(k-1)/2}),$$

which implies that the nth component of $\Omega_{V_f(1),1}((1+\pi) \otimes \eta_1^{\pm})$, which is $\exp_{n,1}\left(\gamma_{n,1}(\eta_1^{\pm})\right)$ satisfies

$$\exp_{n,1}\left(\gamma_{n,1}(\eta_1^{\pm})\right) \in \varpi^{-e(k-1)\lfloor n/2 \rfloor + c_{\pm}} H^1(\mathbb{Q}_{p,n}, T_f(1))$$

for some constant $c_{\pm}$ independent of n.

Recall that $\mathbb{H}^1_{\mathrm{Iw}}(T_f(1))$ is free of rank 2 over $\Lambda_{\mathcal{O}_E}$. Fix a basis z_1, z_2, say. Note that $(1+\pi) \otimes \eta_1^{\pm}$ form a Λ_E-basis for $\mathbb{D}_{\infty}(V_f)$. The determinant of

$$\Omega_{V_f(1),1} : \mathcal{H}_{\infty}(G_{\infty}) \underset{\Lambda_E}{\otimes} \mathbb{D}_{\infty}(V_f(1)) \to \mathcal{H}_{\infty}(G_{\infty}) \underset{\Lambda_{\mathcal{O}_E}}{\otimes} \mathbb{H}^1_{\mathrm{Iw}}(T_f(1))$$

with respect to these bases, as a $\mathcal{H}_{\infty}(G_{\infty})$-homomorphism, is given by

$$\prod_{j=0}^{k-2} \log_p(u^j \gamma) \sim \log_p^{k-1}$$

up to a unit of Λ_E (this is the $\delta(V)$-conjecture of [PR94], which can be deduced from the explicit reciprocity law of Colmez [Col98]). But Theorem 2.4.1 says that $\log_{p,k}^{\pm} \sim \log_p^{(k-1)/2}$. Hence, we in fact have

$$\Omega_{V_f(1),1}((1+\pi) \otimes \eta^{\pm}) \sim \log_p^{(k-1)/2}.$$

Therefore, we can choose $c_{\pm}$ such that

$$\exp_{n,1}\left(\gamma_{n,1}(\eta_1^{\pm})\right) \notin \varpi^{-e(k-1)\lfloor n/2 \rfloor + c_{\pm} + 1} H^1(\mathbb{Q}_{p,n}, T_f(1)),$$

so $r_n^{\pm} = -e(k-1)\lfloor n/2 \rfloor + c_{\pm}$, for n sufficiently large. □

On combining these two lemmas, we have:

Corollary 4.4.3. *If θ is the trivial character on Δ, then there exist $s^\pm$ such that*

$$\mathrm{Col}^\pm\left(\mathbb{H}^1_{\mathrm{Iw}}(T_{\bar{f}}(k-1))\right)^\theta = \varpi^{s^\pm}\Gamma_{\mathcal{O}_E}.$$

Proof. By Proposition 4.3.2 and Lemma 4.4.1, for sufficiently large n,

$$\varpi^{r_n^\pm}\left(\sum_{\sigma\in\Delta}\sigma\right)\cdot\prod_{j=0}^{k-2}\tilde{\omega}_n^\pm(u^{-j}\gamma)\in\mathcal{L}_{\eta^\pm,n}\left(H^1(\mathbb{Q}_{p,n},T_{\bar{f}}(k-1))\right)$$

where

$$\begin{aligned}
\tilde{\omega}_n^+(1+X) &= \prod_{1\le m<n/2}\Phi_{2m}(1+X),\\
\tilde{\omega}_n^-(1+X) &= \prod_{1\le m<(n+1)/2}\Phi_{2m-1}(1+X).
\end{aligned}$$

Hence, by Remark 4.2.3 and Lemma 4.4.2, there exist constants $s^\pm$ (independent of n) such that

$$\varpi^{s^\pm}\left(\sum_{\sigma\in\Delta}\sigma\right)\cdot\log_{p,k}^\pm\in\mathcal{L}_{\eta^\pm,n}\left(H^1(\mathbb{Q}_{p,n},T_{\bar{f}}(k-1))\right)$$

and

$$\mathcal{L}_{\eta^\pm,n}\left(H^1(\mathbb{Q}_{p,n},T_{\bar{f}}(k-1))\right)\subset\varpi^{s^\pm}\log_{p,k}^\pm\mathcal{O}_E[G_n].$$

But $\log_{p,k}^\pm\mathrm{Col}^\pm=\mathcal{L}_{\eta^\pm}$, so we have

$$\varpi^{s^\pm}\sum_{\sigma\in\Delta}\sigma\in\mathrm{Col}^\pm\left(H^1(\mathbb{Q}_{p,n},T_{\bar{f}}(k-1)\right)\mod\tilde{\omega}_n^\mp(\gamma).$$

Therefore, we are done since

$$\varprojlim\Lambda_{\mathcal{O}_E}/\tilde{\omega}_n^\pm(\gamma)=\Lambda_{\mathcal{O}_E}\quad\text{and}\quad\Lambda_{\mathcal{O}_E}^\theta=\left(\sum_{\sigma\in\Delta}\sigma\right)\Lambda_{\mathcal{O}_E}.$$

□

Remark 4.4.4. *It is clear that we can replace θ by an arbitrary character on Δ for the minus map in the corollary.*

Chapter 5

$\pm$-Selmer groups

Throughout this chapter, with the exception of Sections 5.3.2 and 5.4, assumptions (1) and (2) are not necessary.

Let f be a modular form as in Section 1.3.5, K a number field, the p-Selmer groups of f over K are defined by the following:

$$\begin{aligned}\mathrm{Sel}_p^0(f/K) &= \ker\left(H^1(K,V_f/T_f(1)) \to \prod_v H^1(K_v,V_f/T_f(1))\right)\\ \mathrm{Sel}_p(f/K) &= \ker\left(H^1(K,V_f/T_f(1)) \to \prod_v \frac{H^1(K_v,V_f/T_f(1))}{H^1_f(K_v,V_f/T_f(1))}\right)\end{aligned}$$

where v runs through the places of K.

We write k_n for $\mathbb{Q}$ adjoining all the p^nth roots of unity and $\mathbb{Q}_\infty = \cup k_n$. Since there is a unique place above p in k_n, we write this place as p as well. Note that the completion of k_n at p is isomorphic to $\mathbb{Q}_{p,n}$. For f satisfying assumptions (1) and (2), let $H^1_f(\mathbb{Q}_{p,n},V_f/T_f(1))^\pm$ be as defined in Section 3.4.2. For all $n\geq 0$, we define the plus and minus Selmer groups by

$$\mathrm{Sel}_p^\pm(f/k_n) = \ker\left(\mathrm{Sel}_p(f/k_n) \to \frac{H^1(\mathbb{Q}_{p,n},V_f/T_f(1))}{H^1_f(\mathbb{Q}_{p,n},V_f/T_f(1))^\pm}\right).$$

In this chapter, we show that $\mathrm{Sel}_p(f/\mathbb{Q}_\infty)$ is not $\Lambda_{\mathcal{O}_E}$-cotorsion when f is supersingular at p. When f satisfies assumptions (1) and (2), we show that $\mathrm{Sel}_p^\pm(f/\mathbb{Q}_\infty)$, the direct limit of $\mathrm{Sel}_p^\pm(f/k_n)$, is $\Lambda_{\mathcal{O}_E}$-cotorsion.

5.1 Restricted ramification

We now describe the Selmer groups defined above using restricted ramification. Let S be a finite set of places of a number field K containing all infinite places, all primes above p and those dividing N. Then, by [Rub00, Lemma I.5.3],

$$H^1(G_{S,K}, V_f/T_f(1)) = \ker\left(H^1(K, V_f/T_f(1)) \to \prod_{v\notin S} \frac{H^1(K_v, V_f/T_f(1))}{H^1_f(K_v, V_f/T_f(1))}\right) \tag{5.1}$$

where $G_{S,K}$ is the Galois group of the maximal extension of K unramified outside S. Therefore, we can rewrite Sel_p as

$$\mathrm{Sel}_p(f/K) = \ker\left(H^1(G_{S,K}, V_f/T_f(1)) \to \bigoplus_{v\in S} \frac{H^1(K_v, V_f/T_f(1))}{H^1_f(K_v, V_f/T_f(1))}\right). \tag{5.2}$$

If f satisfies assumptions (1) and (2), we write

$$H^1_f(k_{n,v}, V_f/T_f(1))^{\pm} = H^1_f(k_{n,v}, V_f/T_f(1))$$

for $v \nmid p$. Then,

$$\mathrm{Sel}_p^{\pm}(f/k_n) = \ker\left(H^1(G_{S,k_n}, V_f/T_f(1)) \to \bigoplus_{v\in S} \frac{H^1(k_{n,v}, V_f/T_f(1))}{H^1_f(k_{n,v}, V_f/T_f(1))^{\pm}}\right). \tag{5.3}$$

The next lemma enables us to give a similar alternative description of Sel_p^0 as well.

Lemma 5.1.1. *With notation above, we have $H^1_f(K_v, V_f/T_f(1)) = 0$ for $v \nmid pN$.*

Proof. If v is an infinite place, we in fact have $H^1(K_v, V_f/T_f(1)) = 0$ as p is odd (see e.g. [Rub00, Section I.3.7]).

We now assume that v is a finite place not dividing pN. Since $v \nmid p$,

$$H^1_f(K_v, V_f(1)) = H^1_{\mathrm{ur}}(K_v, V_f(1))$$

by definition and $H^1_f(K_v, V_f/T_f(1))$ is defined to be the image of $H^1_{\mathrm{ur}}(K_v, V_f(1))$ in $H^1(K_v, V_f/T_f(1))$ under the natural map

$$H^1(K_v, V_f(1)) \to H^1(K_v, V_f/T_f(1)).$$

By [Rub00, Section I.3.2],

$$H^1_{\mathrm{ur}}(K_v, V_f(1)) \cong V_f(1)^I/(\mathrm{Fr}-1)V_f(1)^I$$

where I is the inertia group of K_v and Fr is the Frobenius of K_v^{ur}/K_v. Hence, it suffices to show that 1 is not an eigenvalue of Fr. But v is a good prime (i.e. $v \nmid N$), so the eigenvalues have absolute value $q_v^{(k-1)/2}$ where q_v is the rational prime lying below v. Hence we are done. □

If S is as above, Lemma 5.1.1 and (5.1) implies that

$$H^1(G_{S,K}, V_f/T_f(1)) = \ker\left(H^1(K, V_f/T_f(1)) \to \prod_{v \notin S} H^1(K_v, V_f/T_f(1))\right).$$

Therefore, by the definition of Sel_p^0, we have:

$$\mathrm{Sel}_p^0(f/K) = \ker\left(H^1(G_{S,K}, V_f/T_f(1)) \to \bigoplus_{v \in S} H^1(K_v, V_f/T_f(1))\right). \quad (5.4)$$

As stated in the proof of Lemma 5.1.1, $H^1(K_v, V_f/T_f(1)) = 0$ if v is an infinite place. We can therefore simplify (5.4) further:

$$\mathrm{Sel}_p^0(f/K) = \ker\left(H^1(G_{S,K}, V_f/T_f(1)) \to \bigoplus_{v \in S_f} H^1(K_v, V_f/T_f(1))\right). \quad (5.5)$$

where S_f denotes the set of finite places in S.

5.2 Poitou-Tate exact sequences

Here, we briefly review results on Poitou-Tate exact sequences. Details can be found in [PR95, Section A.3].

With the above notation, let S be a finite set of places of K containing those above p and the infinite places, then we have an exact sequence

$$\begin{aligned} \bigoplus_{v \in S_f} H^0(K_v, V_f/T_f(1)) \to H^2(G_{S,K}, T_{\bar{f}}(k-1))^\vee \to H^1(G_{S,K}, V_f/T_f(1)) \\ \to \bigoplus_{v \in S_f} H^1(K_v, V_f/T_f(1)) \end{aligned} \quad (5.6)$$

where S_f is again the set of finite places in S. On combining (5.6) and (5.5), we have

$$\bigoplus_{v \in S_f} H^0(K_v, V_f/T_f(1)) \to H^2(G_{S,K}, T_{\bar{f}}(k-1))^\vee \to \mathrm{Sel}_p^0(f/K).$$

By taking duals and the fact that

$$H^0(K_v, V_f/T_f(1))^\vee = H^2(K_v, T_{\bar{f}}(k-1)),$$

we obtain

$$\mathrm{Sel}_p^0(f/K)^\vee = \ker\left(H^2(G_{S,K}, T_{\bar{f}}(k-1)) \to \bigoplus_{v \in S_f} H^2(K_v, T_{\bar{f}}(k-1))\right) \quad (5.7)$$

For each $v \in S_f$, let

$$A_v \subset H^1(K_v, T_{\bar{f}}(k-1)) \quad \text{and} \quad B_v \subset H^1(K_v, V_f/T_f(1))$$

be $\mathcal{O}_E$-modules so that they are orthogonal complements to each other under the Pontryagin duality. Define

$$H^1_B(K, V_f/T_f(1)) = \ker \left(H^1(G_{S,K}, V_f/T_f(1)) \to \bigoplus_{v \in S_f} \frac{H^1(K_v, V_f/T_f(1))}{B_v} \right).$$

Then [PR95, Proposition A.3.2] says that we have an exact sequence

$$\begin{aligned} H^1(G_{S,K}, T_{\bar{f}}(k-1)) \to \bigoplus_{v \in S_f} \frac{H^1(K_v, T_{\bar{f}}(k-1))}{A_v} \to H^1_B(K, V_f/T_f(1))^\vee \\ \to H^2(G_{S,K}, T_{\bar{f}}(k-1)) \to \bigoplus_{v \in S_f} H^2(K_v, T_{\bar{f}}(k-1)). \end{aligned} \tag{5.8}$$

Hence, we can combine (5.7) and (5.8) to obtain:

$$\begin{aligned} H^1(G_{S,K}, T_{\bar{f}}(k-1)) \to \bigoplus_{v \in S_f} \frac{H^1(K_v, T_{\bar{f}}(k-1))}{A_v} \to H^1_B(K, V_f/T_f(1))^\vee \\ \to \mathrm{Sel}^0_p(f/K)^\vee \to 0. \end{aligned} \tag{5.9}$$

5.3 Cotorsionness

5.3.1 $\mathrm{Sel}_p(f/\mathbb{Q}_\infty)$ is not $\Lambda_{\mathcal{O}_E}$-cotorsion

We now prove our claim about $\mathrm{Sel}_p(f/\mathbb{Q}_\infty)^\vee$ in the introduction. Let $K = k_n$. Take

$$B_v = H^1_f(k_{n,v}, V_f/T_f(1))$$

for $v \in S_f$ in (5.9), then

$$A_v = H^1_f(k_{n,v}, T_{\bar{f}}(k-1))$$

by [BK90, Proposition 3.8]. Hence, on combining (5.2) and (5.9), we have

$$\begin{aligned} H^1(G_{S,k_n}, T_{\bar{f}}(k-1)) \to \frac{H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))}{H^1_f(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))} \oplus \bigoplus_{v \mid N} \frac{H^1(k_{n,v}, T_{\bar{f}}(k-1))}{H^1_f(k_{n,v}, T_{\bar{f}}(k-1))} \\ \to \mathrm{Sel}_p(f/k_n)^\vee \to \mathrm{Sel}^0_p(f/k_n)^\vee \to 0. \end{aligned} \tag{5.10}$$

We are interested in taking inverse limit over n. For the terms coming from places dividing N, we can apply the following.

Lemma 5.3.1. *For each integer $n \geq 0$, fix a prime $v(n)$ of $\mathbb{Q}_{p,n}$ not dividing p such that $v(n+1)$ lies above $v(n)$, then*

$$\varprojlim_{n,\mathrm{cor}} \frac{H^1(k_{n,v(n)}, T_{\bar{f}}(k-1))}{H^1_f(k_{n,v(n)}, T_{\bar{f}}(k-1))} = 0.$$

Proof. The Pontryagin dual of the said inverse limit is $\varinjlim H^1_f(k_{n,v(n)}, V_f/T_f(1))$, so the result follows immediately from Lemma 5.1.1 if $v(n) \nmid N$. The general case is proved in [Kat04, Section 17.10] by considering p-cohomological dimensions. □

Therefore, on taking inverse limits in (5.10), we have

$$\mathbb{H}^1_S(T_{\bar{f}}(k-1)) \to \frac{\mathbb{H}^1_{\mathrm{Iw}}(T_{\bar{f}}(k-1))}{\mathbb{H}_f(T_{\bar{f}}(k-1))} \to \mathrm{Sel}_p(f/\mathbb{Q}_\infty)^\vee \to \mathrm{Sel}^0_p(f/\mathbb{Q}_\infty)^\vee \to 0 \tag{5.11}$$

where $\mathbb{H}_f(\cdot) = \varprojlim_n H^1_f(\mathbb{Q}_{p,n}, \cdot)$ and $\mathbb{H}^1_S(\cdot) = \varprojlim_n H^1(G_{k_n,S}, \cdot) \cong \mathbb{H}^1(\cdot)$ (see [Kob03, Proposition 7.1]).

Proposition 5.3.2. $\mathrm{Sel}_p(f/\mathbb{Q}_\infty)^\vee$ *is not torsion over* $\Lambda_{\mathcal{O}_E}$.

Proof. We actually know more or less everything about the terms appearing in the exact sequence (5.11) now.

By Theorem 2.3.2, $\mathbb{H}^1_S(T_{\bar{f}}(k-1))$ is a torsion-free $\Lambda_{\mathcal{O}_E}$-module of rank 1. By [PR00, Theorem 0.6], $\mathbb{H}_f(T_{\bar{f}}(k-1)) = 0$. By [PR94, Proposition 3.2.1], $\mathbb{H}^1_{\mathrm{Iw}}(T_{\bar{f}}(k-1))$ is of rank 2 over $\Lambda_{\mathcal{O}_E}$. By [Kob03, proof of Proposition 7.1], which is a purely algebraic proof and generalises to modular forms directly, $\mathrm{Sel}^0_p(f/\mathbb{Q}_\infty)^\vee$ is $\Lambda_{\mathcal{O}_E}$-torsion. Therefore, $\mathrm{Sel}_p(f/\mathbb{Q}_\infty)^\vee$ has $\Lambda_{\mathcal{O}_E}$-rank at least 1 and we are done. □

5.3.2 $\mathrm{Sel}^\pm_p(f/\mathbb{Q}_\infty)$ is $\Lambda_{\mathcal{O}_E}$-cotorsion

We again set $K = k_n$. Let

$$B_v = \begin{cases} H^1_f(k_{n,v}, V_f/T_f(1)) & \text{if } v|N \\ H^1(\mathbb{Q}_{p,n}, V_f/T_f(1))^\pm & \text{if } v = p. \end{cases}$$

By [BK90, Proposition 3.8] and Lemma 3.4.3, we have

$$A_v = \begin{cases} H^1_f(k_{n,v}, T_{\bar{f}}(k-1)) & \text{if } v|N \\ H^1_\pm(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1)) & \text{if } v = p. \end{cases}$$

Hence, on combining (5.3) with (5.9), we obtain the following exact sequence:

$$H^1(G_{S,k_n}, T_{\bar{f}}(k-1)) \to \frac{H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))}{H^1_{\pm}(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))} \oplus \bigoplus_{v|N} \frac{H^1(k_{n,v}, T_{\bar{f}}(k-1))}{H^1_f(k_{n,v}, T_{\bar{f}}(k-1))} \\ \to \mathrm{Sel}_p^{\pm}(f/k_n)^\vee \to \mathrm{Sel}_p^0(f/k_n)^\vee \to 0. \tag{5.12}$$

Therefore, on taking inverse limits in (5.12) and applying Lemma 5.3.1, we have

$$\mathbb{H}^1_S(T_{\bar{f}}(k-1)) \to \frac{\mathbb{H}^1_{\mathrm{Iw}}(T_{\bar{f}}(k-1))}{\mathbb{H}^1_{\mathrm{Iw},\pm}(T_{\bar{f}}(k-1))} \to \mathrm{Sel}_p^{\pm}(f/\mathbb{Q}_\infty)^\vee \to \mathrm{Sel}_p^0(f/\mathbb{Q}_\infty)^\vee \to 0 \tag{5.13}$$

where $\mathbb{H}^1_{\mathrm{Iw},\pm}(T_{\bar{f}}(k-1))$ is as defined in Chapter 3, i.e.

$$\varprojlim H^1_{\pm}(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1)).$$

Proposition 5.3.3. $\mathrm{Sel}_p^{\pm}(f/\mathbb{Q}_\infty)$ *is* $\Lambda_{\mathcal{O}_E}$*-cotorsion.*

Proof. Recall that $\ker(\mathrm{Col}^{\pm}) = \mathbb{H}^1_{\mathrm{Iw},\pm}(T_{\bar{f}}(k-1))$ and $\mathrm{Col}^{\pm}(\mathbf{z}^{\mathrm{Kato}}) = L_p^{\pm}$. Therefore, if $L_p^{\pm} \neq 0$, it would imply that the cokernel of the first map in (5.13) is $\Lambda_{\mathcal{O}_E}$-torsion and the result would follow from the fact that $\mathrm{Sel}_p^0(f/\mathbb{Q}_\infty)^\vee$ is $\Lambda_{\mathcal{O}_E}$-torsion. Hence, we are done by the following lemma. □

Lemma 5.3.4. $L_p^{\pm} \neq 0$.

Proof. The case when f corresponds to an elliptic curve is proved in [Pol03, Corollary 5.11]. The general case can be proved similarly.

By [Pol03], if θ is a character on G_n which does not factor through G_{n-1} and $0 \le r \le k-2$, then

$$\chi^r\theta(L_p^+) = C^+_{n,r}(\theta)L(f,\theta,r+1) \qquad \text{if } n \text{ is even,}$$
$$\chi^r\theta(L_p^-) = C^-_{n,r}(\theta)L(f,\theta,r+1) \qquad \text{if } n \text{ is odd}$$

where $C^{\pm}_{n,r}(\theta)$ are nonzero constants. By [Roh88], $L(f,\theta,1) = 0$ for finitely many θ if $k = 2$. If $k \ge 3$, $L(f,\theta,r+1) \neq 0$ for $r+1 \le (k-1)/2$ by [Shi76, Proposition 2]. Hence we are done. □

Corollary 5.3.5. *The first map in* (5.13) *is injective.*

Proof. It follows from Theorem 2.3.2 and Lemma 5.3.4. □

Remark 5.3.6. *It is clear from the proof of Lemma 5.3.4 that* $L_p^{\pm,\theta} \neq 0$ *for any character* θ *on* Δ. *Therefore,* $\mathrm{Sel}_p^{\pm}(f/\mathbb{Q}_\infty)^\theta$ *is* $\Gamma_{\mathcal{O}_E}$*-cotorsion and we can associate to it a characteristic ideal, namely*

$$\mathrm{Char}_{\Gamma_{\mathcal{O}_E}}\left(\mathrm{Sel}_p^{\pm}(f/\mathbb{Q}_\infty)^{\vee,\theta}\right).$$

5.4 Main conjectures

We now formulate a main conjecture and relate it to that of Kato.

By Corollary 5.3.5 and the fact that $\mathrm{Sel}_p^0(f/\mathbb{Q}_\infty)^\vee \cong \mathbb{H}^2(T_{\bar{f}}(k-1))$ (see [Kur02]), we have an exact sequence

$$0 \to \mathbb{H}_S^1(T_{\bar{f}}(k-1)) \to \mathrm{Im}(\mathrm{Col}^{\pm}) \to \mathrm{Sel}_p^{\pm}(f/\mathbb{Q}_\infty)^\vee \to \mathbb{H}^2(T_{\bar{f}}(k-1)) \to 0. \quad (5.14)$$

If θ is a character on Δ, then

$$\mathrm{Char}_{\Gamma_{\mathcal{O}_E}}(\mathbb{H}_S^1(T_{\bar{f}}(k-1))^\theta/\mathbb{Z}(T_{\bar{f}}(k-1))^\theta) = \mathrm{Char}_{\Gamma_{\mathcal{O}_E}}(\mathbb{H}^2(T_{\bar{f}}(k-1))^\theta)$$

if and only if

$$\mathrm{Char}_{\Gamma_{\mathcal{O}_E}}(\mathrm{Sel}_p^{\pm}(f/\mathbb{Q}_\infty)^{\vee,\theta}) = \mathrm{Char}_{\Gamma_{\mathcal{O}_E}}(\mathrm{Im}(\mathrm{Col}^{\pm,\theta})/L_p^{\pm,\theta}).$$

In other words, Kato's main conjecture (for $\bar{f}$) is equivalent to the following conjecture.

Conjecture 5.4.1. $\mathrm{Char}_{\Gamma_{\mathcal{O}_E}}(\mathrm{Sel}_p^{\pm}(f/\mathbb{Q}_\infty)^{\vee,\theta}) = \mathrm{Char}_{\Gamma_{\mathcal{O}_E}}(\mathrm{Im}(\mathrm{Col}^{\pm,\theta})/L_p^{\pm,\theta})$.

Moreover, by Corollary 4.4.3 and Remark 4.4.4, we have:

Corollary 5.4.2. *Let* $\delta = \pm$. *When* $\theta = 1$ *or* $\delta = -$, *Conjecture 5.4.1 is equivalent to*

$$\mathrm{Char}_{\Gamma_{\mathcal{O}_E}}(\mathrm{Sel}_p^{\pm}(f/\mathbb{Q}_\infty)^{\vee,\theta}) = (\varpi^{-s^{\pm}} L_p^{\pm,\theta}).$$

Remark 5.4.3. *It is clear that the RHS in Conjectures 5.4.1 and 5.4.2 are contained in the LHS if we replace* $\Gamma_{\mathcal{O}_E}$ *by* Γ_E *by Theorem 2.3.3.*

Chapter 6

CM forms

We now follow the strategy of [PR04] to prove that equality holds in Corollary 5.4.2 (with $\theta = 1$) for CM forms.

6.1 Generality of CM forms

We first briefly review the theory of CM modular forms. Details can be found in [Kat04, Section 15].

Let K be an imaginary quadratic field with idele class group C_K. A Hecke character of K is simply a continuous homomorphism $\phi : C_K \to \mathbb{C}^\times$ with complex L-function

$$L(\phi, s) = \prod_v (1 - \phi(v)N(v)^{-s})^{-1}$$

where the product runs through the finite places v of K at which ϕ is unramified, $\phi(v)$ is the image of the uniformiser of K_v under ϕ and $N(v)$ is the norm of v.

Let f be a modular form as defined in Section 1.3.5 with complex multiplication, i.e. $L(f, s) = L(\phi, s)$ for some Hecke character ϕ of an imaginary quadratic field K. Then, for a good prime p,

$$1 - a_p p^{-s} + \epsilon(p)p^{k-1-2s} = \begin{cases} 1 - \phi(p)p^{-2s} & \text{if } p \text{ is inert in } K \\ (1 - \phi(\mathfrak{P})p^{-s})(1 - \phi(\bar{\mathfrak{P}})p^{-s}) & \text{if } (p) = \mathfrak{P}\bar{\mathfrak{P}} \text{ in } K. \end{cases}$$

Therefore, $a_p = 0$ if p is inert in K. If p splits into $\mathfrak{P}\bar{\mathfrak{P}}$, $a_p = \phi(\mathfrak{P}) + \phi(\bar{\mathfrak{P}})$. It is known that $\phi(\mathfrak{P}) + \phi(\bar{\mathfrak{P}})$ is a p-adic unit, hence f is ordinary at p. Therefore, for a good prime $p \nmid N$, $a_p = 0$ iff f is supersingular at p. We fix such a p which is odd.

Let $\mathcal{O}$ be the ring of integers of K. We denote the conductor of ϕ by $\mathfrak{f}$. For an ideal $\mathfrak{a}$ of K, $K(\mathfrak{a})$ denotes the ray class field of K of conductor $\mathfrak{a}$. We write $\mathcal{K}$ for the union $\cup_n K(p^n\mathfrak{f})$. Then, the action of $G_{\mathbb{Q}}$ on V_f factors through $\mathrm{Gal}(\mathcal{K}/\mathbb{Q})$. The same is then true for $V_f(j)$ for all j as $\mathbb{Q}_\infty \subset \mathcal{K}$.

More specifically, $V_f \cong V(\phi) \oplus \tau V(\phi)$ where $V(\phi)$ is the one-dimensional E-representation of G_K associated to ϕ and τ is the complex conjugation. The action of $G_{\mathbb{Q}}$ is given by

$$\sigma(x,y) = \begin{cases} (\sigma(x), \tau(\tau\sigma\tau)(y)) & \text{if } \sigma \in G_K, \\ ((\tau\sigma\tau)(y), \tau\sigma(x)) & \text{otherwise.} \end{cases}$$

In addition to assumptions (1) and (2), we assume:

- **Assumption (3)**: f is defined over $\mathbb{Q}$, $\epsilon = 1$ and K has class number 1.

Then, as a $\mathbb{Q}_p$-vector space, V_f is isomorphic to K_p (where K_p denotes the completion of K at p) and we can take T_f to be the lattice corresponding to $\mathcal{O}_p$. We write ρ for the character given by

$$\rho : G_K \to \mathrm{Aut}(V_f/T_f(1)) \cong \mathcal{O}_p^\times.$$

For simplicity, we write A for $V_f/T_f(1)$ from now on.

Recall that K_c denote the $\mathbb{Z}_p$-cyclotomic extension of K. We write K_m for the unique $\mathbb{Z}_p^2$-extension of K and $\mathfrak{L}$ denotes $\mathcal{O}_p[[\mathrm{Gal}(K_m/K)]]$. Given a $\mathbb{Z}_p[[\mathrm{Gal}(\mathcal{K}/K)]]$-module Y, we write Y_F for

$$Y \otimes_{\mathbb{Z}_p[[\mathrm{Gal}(\mathcal{K}/K)]]} \mathbb{Z}_p[[\mathrm{Gal}(F/K)]]$$

and $Y_F^\rho = Y_F(\rho^{-1})$ where $F = K_c$ or K_m.

Let F be an extension of $\mathbb{Q}$. Following [Rub85], we define a modified Selmer group:

$$\mathrm{Sel}'_p(f/F) = \ker\left(H^1(F, A) \to \prod_{v \nmid p} \frac{H^1(F_v, A)}{H^1_f(F_v, A)} \right).$$

For a finite abelian extension F of K, we define groups C_F, E_F and U_F as in [PR04]: U_F is the pro-p part of the local unit group $(\mathcal{O}_F \otimes \mathbb{Z}_p)^\times$, E_F is the closure of the projection of the global units $\mathcal{O}_F^\times$ into U_F and C_F is the closure of the projection of the subgroup of elliptic units (as defined in [Rub91, Section 1], see also Section 6.1.1 below) into U_F. We then define

$$\mathcal{C} = \varprojlim C_F, \ \mathcal{E} = \varprojlim E_F \ \text{ and } \ \mathcal{U} = \varprojlim U_F$$

where the inverse limits are taken over finite extensions F of K inside $\mathcal{K}$ and the connecting map is the norm map.

Finally, let M be the maximal abelian p-extension of $\mathcal{K}$ which is unramified outside p and write $\mathcal{X}$ for the Galois group of M over $\mathcal{K}$.

6.1.1 Elliptic units

We now briefly review the definition of elliptic units associated to K. Let $\mathfrak{a}$ and $\mathfrak{b}$ be non-zero ideals of $\mathcal{O}_K$ such that $\mathfrak{a}$ is prime to $6\mathfrak{b}$ and the natural map $\mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{b})^\times$ is injective. There exists an elliptic function on $\mathbb{C}/\mathfrak{b}$ with zeros and poles given by 0 (with multiplicity $N(\mathfrak{a})$) and the $\mathfrak{a}$-division points respectively. There exists a unique such function if we impose some norm compatibility condition on its values as $\mathfrak{a}$ varies. We write ${}_\mathfrak{a}\theta_\mathfrak{b}$ for this unique function and let ${}_\mathfrak{a}z_\mathfrak{b} ={}_\mathfrak{a} \theta_\mathfrak{b}(1)^{-1}$. Then, ${}_\mathfrak{a}z_\mathfrak{b} \in K(\mathfrak{b})^\times$ for any $\mathfrak{a}$ and $\mathfrak{b}$ as above. For a fixed $\mathfrak{b}$, the group of elliptic units in $K(\mathfrak{b})$ is defined to be the group generated by ${}_\mathfrak{a}z_\mathfrak{b}^\sigma$ where $\sigma \in \mathrm{Gal}(K(\mathfrak{b})/K)$ and the roots of unity in $K(\mathfrak{b})$.

6.2 Properties of Sel'_p

In this section, we generalise [PR04, Theorem 2.1]. We do this by generalising three results of [Rub85].

Lemma 6.2.1. *There is an isomorphism* $\mathrm{Sel}'_p(f/K_c) \cong \mathrm{Sel}_p(f/K_c)$.

Proof. By definitions, we have the following exact sequence:

$$0 \to \mathrm{Sel}_p(f/K_c) \to \mathrm{Sel}'_p(f/K_c) \to \frac{H^1(K_{c,p}, A)}{H^1_f(K_{c,p}, A)}.$$

Therefore, it suffices to show that $H^1(K_{c,p}, A) = H^1_f(K_{c,p}, A)$. By [BK90, Proposition 3.8],

$$\left(\frac{H^1(K_{c,p}, A)}{H^1_f(K_{c,p}, A)}\right)^\vee = \varprojlim H^1_f(K_p^{(n)}, T_{\bar{f}}(k-1)).$$

Hence, it suffices to show that the said inverse limit is 0.

Note that $\mathrm{Gal}\left(K_{p,n}/K_p^{(n-1)}\right) \cong \Delta$, we have the inflation-restriction exact sequence

$$0 \to H^1(\Delta, T_{\bar{f}}(k-1)^{G_{K_{p,n}}}) \to H^1(K_p^{(n-1)}, T_{\bar{f}}(k-1)) \to H^1(K_{p,n}, T_{\bar{f}}(k-1))^\Delta \to H^2(\Delta, T_{\bar{f}}(k-1)^{G_{K_{p,n}}}).$$

As $K_p/\mathbb{Q}_p$ is unramified, the proof of Lemma 3.1.1 implies

$$T_{\bar{f}}(k-1)^{G_{K_{p,n}}} = 0$$

for all n. Therefore,

$$H^1(K_p^{(n-1)}, T_{\bar{f}}(k-1)) \cong H^1(K_{p,n}, T_{\bar{f}}(k-1))^{\Delta}.$$

By [PR00, Theorem 0.6], we have

$$\varprojlim H^1_f(K_{n,p}, T_{\bar{f}}(k-1)) = 0,$$

hence we are done. $\square$

This corresponds to [Rub85, Theorem 2.1], which holds for any infinite extensions of K contained in $\mathcal{K}$. Since we have used a result on the inverse limit of H^1_f over $K_{p,n}$, the proof above would unfortunately not work in such generality.

We now generalise [Rub85, Proposition 1.1].

Lemma 6.2.2. *There is an isomorphism* $\mathrm{Sel}'_p(f/\mathcal{K}) \cong \mathrm{Hom}(\mathcal{X}, A)$.

Proof. Since the action of G_K on A factors through $\mathrm{Gal}(\mathcal{K}/K)$, we have

$$H^1(\mathcal{K}, A) \cong \mathrm{Hom}(G_{\mathcal{K}}, A).$$

We can therefore identify $\mathrm{Sel}'_p(f/\mathcal{K})$ with a subgroup of $\mathrm{Hom}(G_{\mathcal{K}}, A)$. Also, the triviality of the action implies that A is unramified at all places of $\mathcal{K}$. Therefore, $H^1_f(\mathcal{K}_v, A) = H^1_{\mathrm{ur}}(\mathcal{K}_v, A)$ for all $v \nmid p$ by [Rub00, Lemma 3.5(iv)]. Hence, $\mathrm{Sel}'_p(f/\mathcal{K})$ corresponds to the subgroup $\mathrm{Hom}(\mathcal{X}, A) \subset \mathrm{Hom}(G_{\mathcal{K}}, A)$. $\square$

Before we continue, we state a result of Rubin:

Lemma 6.2.3. *For* $i = 1, 2$, $H^i(\mathcal{K}/K_c, A) = 0$.

Proof. See [Rub85, proof of Proposition 1.2]. $\square$

Now, we can generalise [Rub85, Proposition 1.2].

Lemma 6.2.4. *There is an isomorphism* $\mathrm{Sel}'_p(f/K_c) \cong \mathrm{Sel}'_p(f/\mathcal{K})^{\mathrm{Gal}(\mathcal{K}/K_c)}$.

Proof. We have the inflation-restriction exact sequence

$$0 \to H^1(\mathcal{K}/K_c, A) \to H^1(K_c, A) \xrightarrow{r} H^1(\mathcal{K}, A)^{\mathrm{Gal}(\mathcal{K}/K_c)} \to H^2(\mathcal{K}/K_c, A)$$

where r is the restriction map. Consider the following commutative diagram:

$$\begin{tikzcd} H^1(K_c, A) \arrow[r, "r"] \arrow[d] & H^1(\mathcal{K}, A) \arrow[d] \\ H^1(K_{c,v}, A)/H^1_f(K_{c,v}, A) \arrow[r] & H^1(\mathcal{K}_{v'}, A)/H^1_f(\mathcal{K}_{v'}, A) \end{tikzcd}$$

where $v \nmid p$ is a place of K_c and v' is a place of $\mathcal{K}$ above v. It clearly implies that

$$r\left(\mathrm{Sel}'_p(f/K_c)\right) \subset \mathrm{Sel}'_p(f/\mathcal{K}).$$

Write v' for the place of $K_c(\mathfrak{f})$ below v', then v' is unramified in $\mathcal{K}/K_c(\mathfrak{f})$. Therefore, the map

$$r_{v'} : H^1(I_{K_c(\mathfrak{f})_{v'}}, A) \to H^1(I_{\mathcal{K}_{v'}}, A)$$

where I denotes the inertia group is injective. This implies that

$$H^1(K_c(\mathfrak{f})_{v'}, A)/H^1_f(K_c(\mathfrak{f})_{v'}, A) \to H^1(\mathcal{K}_{v'}, A)/H^1_f(\mathcal{K}_{v'}, A)$$

is injective because the H^1_f coincide with H^1_{ur}. But $\mathrm{Gal}(K_c(\mathfrak{f})/K_c)$ has trivial Sylow p-subgroup, hence the bottom row of the commutative diagram above is injective. Therefore, we have

$$r^{-1}(\mathrm{Sel}'_p(f/\mathcal{K})) \subset \mathrm{Sel}'_p(f/K_c).$$

Hence, we have an exact sequence:

$$0 \to H^1(\mathcal{K}/K_c, A) \to \mathrm{Sel}'_p(f/K_c) \xrightarrow{r} \mathrm{Sel}'_p(f/\mathcal{K})^{\mathrm{Gal}(\mathcal{K}/K_c)} \to H^2(\mathcal{K}/K_c, A).$$

Hence, we are done by Lemma 6.2.3. □

We can now give a generalisation of [PR04, Theorem 2.1]:

Corollary 6.2.5. $\mathrm{Sel}_p(f/K_c) \cong \mathrm{Hom}_{\mathcal{O}}(\mathcal{X}^{\rho}_{K_c}, K_p/\mathcal{O}_p)$.

Proof. Combining the Lemmas 6.2.1, 6.2.2 and 6.2.4, we have

$$\begin{aligned} \mathrm{Sel}_p(f/K_c) &\cong \mathrm{Sel}'_p(f/K_c) \\ &\cong \mathrm{Sel}'_p(f/\mathcal{K})^{\mathrm{Gal}(\mathcal{K}/K_c)} \\ &\cong \mathrm{Hom}(\mathcal{X}, A)^{\mathrm{Gal}(\mathcal{K}/K_c)} \end{aligned}$$

But $A|_{G_K} \cong K_p/\mathcal{O}_p(\rho)$, hence the result. □

6.3 Reciprocity law

In this section, we generalise the reciprocity law given by [PR04, Theorem 5.1]. We first review a result of Rubin.

Theorem 6.3.1 (Rubin)**.** *The $\mathfrak{L}$-module $\mathcal{C}^{\rho}_{K_m}$ is free of rank* 1*.*

Proof. By [Rub91, Theorem 7.7], $\mathcal{C}_{K_m} \cong \mathfrak{I}(K_m)\mathfrak{I}_\mu$ where $\mathfrak{I}(K_m)$ is the augmentation ideal of $\mathfrak{L}$ and $\mathfrak{I}_\mu$ is the annihilator of the roots of unity of K_m in $\mathfrak{L}$. But since $\rho \neq 1$ and $\rho \neq \chi$, we have

$$\mathfrak{I}(K_m)(\rho^{-1}) = \mathfrak{I}_\mu(\rho^{-1}) = \mathfrak{L}(\rho^{-1}),$$

hence the result. □

We now generalise [PR04, Proposition 4.1]:

Lemma 6.3.2. $H^1_f(K_{c,p}, A) \cong \mathrm{Hom}_{\mathcal{O}}(\mathcal{U}^{\rho}_{K_c}, K_p/\mathcal{O}_p)$.

Proof. As in the proof of Lemma 6.2.2, we have

$$H^1(\mathcal{K}_p, A) \cong \mathrm{Hom}(G_{\mathcal{K}_p}, A).$$

But we also have an isomorphism

$$H^1(K_{c,p}, A) \cong H^1(\mathcal{K}_p, A)^{\mathrm{Gal}(\mathcal{K}_p/K_{c,p})}$$

by the inflation-restriction sequence and Lemma 6.2.3.

Hence, by local class field theory, we have

$$\begin{aligned} H^1(K_{c,p}, A) &\cong \mathrm{Hom}(G_{\mathcal{K}_p}, A)^{\mathrm{Gal}(\mathcal{K}_p/K_{c,p})} \\ &\cong \mathrm{Hom}_{\mathcal{O}_p}(\mathcal{U}, A) \end{aligned}$$

(see [Rub87, Proposition 5.2]). By the proof of Lemma 6.2.1, we have

$$H^1_f(K_{c,p}, A) \cong H^1(K_{c,p}, A),$$

hence we are done. □

In particular, we have a pairing $<,>$: $H^1_f(K_{c,p}, A) \times \mathcal{U}^{\rho}_{K_c} \to K_p/\mathcal{O}_p$. We now prove the explicit reciprocity law.

Proposition 6.3.3. *There exists a generator ξ of $\mathcal{C}^{\rho}_{K_m}$ over $\mathfrak{L}$ such that for any finite extension F of K contained in K_c, θ a character on $G = \mathrm{Gal}(F/K)$, $x \in H^1_f(F_p, A)$ and r a non-negative integer, we have*

$$\sum_{\sigma\in G} \theta(\sigma) < x^{\sigma} \otimes p^{-r}, \xi >= p^{-r} \frac{L(f_{\theta^{-1}}, 1)}{\Omega_f^{\pm}} \left[\sum_{\sigma\in G} \theta(\sigma) \exp^{-1}_{F_p, V_f(1)}(x^{\sigma}), \bar{\omega}_{-1} \right] \tag{6.1}$$

where $\theta(-1) = \pm$ and $\exp^{-1}_{F_p,V_f(1)}$ is the inverse of the exponential map

$$\exp_{F_p,V_f(1)} : F_p \otimes \mathbb{D}(V_f(1))/\mathbb{D}^0(V_f(1)) \xrightarrow{\sim} H^1_f(F_p, V_f(1)).$$

Proof. Let $z_{p^\infty\mathfrak{f}} = (z_{p^n\mathfrak{f}})_n$ be the system of norm-compatible elliptic units in $\varprojlim K(p^n\mathfrak{f})$ defined in [Kat04, Section 16.5], then ${}_{\mathfrak{a}}z_{p^n\mathfrak{f}}$ is a multiple of $z_{p^n\mathfrak{f}}$ for all $\mathfrak{a}$ and $p^n\mathfrak{f}$ satisfying the conditions in Section 6.1.1. Therefore, if we write ξ as its image in $\mathcal{C}^{\rho}_{K_m}$, it must be a generator of $\mathcal{C}^{\rho}_{K_m}$ over $\mathfrak{L}$ by Theorem 6.3.1.

Let $x \in H^1_f(F_p, T_f(1))$ and $y \in H^1(F_p, T_{\bar{f}}(k-1))$, we have

$$\begin{aligned}
\sum_{\sigma\in G} \theta(\sigma)[x^{\sigma}, y] &= \sum_{\sigma\in G} \theta(\sigma)\mathrm{Tr}_{F/K} \left[\exp^{-1}_{F_p,V_f(1)}(x^{\sigma}), \exp^*_{F_p,V_{\bar{f}(k-1)}}(y)\right] \\
&= \sum_{\sigma,\tau\in G} \theta(\sigma) \left[\exp^{-1}_{F_p,V_f(1)}(x^{\sigma\tau}), \exp^*_{F_p,V_{\bar{f}(k-1)}}(y^{\tau})\right] \\
&= \sum_{\sigma,\tau\in G} \theta(\sigma\tau)\theta^{-1}(\tau) \left[\exp^{-1}_{F_p,V_f(1)}(x^{\sigma\tau}), \exp^*_{F_p,V_{\bar{f}(k-1)}}(y^{\tau})\right] \\
&= \left[\sum_{\sigma\in G} \theta(\sigma) \exp^{-1}_{F_p,V_f(1)}(x^{\sigma}), \sum_{\tau\in G} \theta^{-1}(\tau) \exp^*_{F_p,V_{\bar{f}(k-1)}}(y^{\tau})\right].
\end{aligned}$$

Consider the Kummer exact sequences:

$$\begin{tikzcd}
\mathcal{C} \arrow[r] \arrow[d] & \mathcal{U} \arrow[d] \\
\varprojlim H^1(\mathcal{O}_{K'}[1/p], \mathcal{O}_p(1)) \arrow[r] \arrow[d, "\otimes\rho\chi^{k-2}"] & \varprojlim H^1(K'_p, \mathcal{O}_p(1)) \arrow[d, "\otimes\rho\chi^{k-2}"] \\
\varprojlim H^1(\mathcal{O}_{K'}[1/p], T_{\bar{f}}(k-1)) \arrow[r] & \varprojlim H^1(K'_p, T_{\bar{f}}(k-1)).
\end{tikzcd}$$

By [Kat04, Proposition 15.9 and (15.16.1)], the image of $z_{p^\infty\mathfrak{f}}$ in

$$\varprojlim H^1(\mathcal{O}_{K'}[1/p], T_{\bar{f}}(k-1))$$

is $\mathbf{z}^{\mathrm{Kato}}$ (up to a twist) and so ξ satisfies

$$\sum_{\tau\in G} \theta^{-1}(\tau) \exp^*_{F_p,V_{\bar{f}(k-1)}}(\xi^{\tau}) = \frac{L(f_{\theta^{-1}}, 1)\bar{\omega}_{-1}}{\Omega_f^{\pm}}.$$

Therefore, we have:

$$\sum_{\sigma\in G}\theta(\sigma) < x^\sigma \otimes p^{-r}, \xi >= p^{-r}\left[\sum_{\sigma\in G}\theta(\sigma)\exp^{-1}_{F,V_f(1)}(x^\sigma), \frac{L(f_{\theta^{-1}},1)\bar{\omega}_{-1}}{\Omega_f^\pm}\right]$$

as required. □

6.4 Proof of the main conjecture

On replacing $\mathbb{Q}_{p,n}$ by $K_{p,n}$, we define $H^1_f(K_{p,n},W)^\pm$ and hence $\mathrm{Sel}_p^\pm(f/K_\infty)$ as in Chapter 5 where $W = A$ or $T_f(1)$. Let $\mathcal{G} = \mathrm{Gal}(K/\mathbb{Q})$. As in the proof of Lemma 6.2.1, the inflation-restriction exact sequence implies that

$$H^1(\mathbb{Q}_{p,n},W) \cong H^1(K_{p,n},W)^{\mathcal{G}}$$

for $W = A$ or $T_f(1)$, so we recover $\mathrm{Sel}_p^\pm(f/\mathbb{Q}_\infty)$ on taking $\mathcal{G}$-invariant. Similarly, on replacing $\mathbb{Q}_{p,n}$ and $K_{p,n}$ by $\mathbb{Q}_p^{(n-1)}$ and $K_p^{(n-1)}$ respectively, we define the $\pm$-Selmer groups $\mathrm{Sel}_p^\pm(f/\mathbb{Q}_c)$ and $\mathrm{Sel}_p^\pm(f/K_c)$. Under our assumptions, they coincide with the Δ-invariants of $\mathrm{Sel}_p^\pm(f/\mathbb{Q}_\infty)$ and $\mathrm{Sel}_p^\pm(f/K_\infty)$ respectively. Analogously, we have $H^1_\pm(F, T_{\bar{f}}(k-1))$ for $F = K_{p,n}$, $K_p^{(n-1)}$ or $\mathbb{Q}_p^{(n-1)}$. Since $K_p/\mathbb{Q}_p$ is unramified, all the results from the previous chapters generalise directly on replacing $\mathbb{Q}_p$ by K.

Via the isomorphism defined in Lemma 6.3.2, we define $\mathcal{V}^\pm \subset \mathcal{U}^\rho_{K_c}$ to be the subgroup corresponding to the elements of $\mathrm{Hom}_{\mathcal{O}}\left(H^1_f(K_{c,p},A), K_p/\mathcal{O}_p\right)$ which factor through $H^1_f(K_{c,p},A)^\pm$. Then, by [PR04, Theorem 4.3],

$$\mathrm{Sel}_p^\pm(f/K_c) \cong \mathrm{Hom}_{\mathcal{O}}\left(\mathcal{X}^\rho_{K_c}/\alpha(\mathcal{V}^\pm), K_p/\mathcal{O}_p\right)$$

where α is the Artin map on $\mathcal{U}$, which enables us to generalise [PR04, Theorem 7.2]:

Theorem 6.4.1. *Let $s^\pm$ be the integer from Corollary 4.4.3, then*

$$\mathrm{Char}_{\Gamma_{\mathcal{O}_p}}\left(\mathrm{Hom}_{\mathcal{O}}\left(\mathrm{Sel}_p^\pm(f/K_c), K_p/\mathcal{O}_p\right)\right) = \left(p^{-s^\pm}L_p^\pm\right).$$

Proof. By the above isomorphism and [PR04, Theorem 6.3], we have:

$$\begin{aligned}
& \mathrm{Char}_{\Gamma_{\mathcal{O}_p}}\left(\mathrm{Hom}_{\mathcal{O}}\left(\mathrm{Sel}_p^\pm(f/K_c), K_p/\mathcal{O}_p\right)\right) \\
= \; & \mathrm{Char}_{\Gamma_{\mathcal{O}_p}}\left(\mathcal{X}^\rho_{K_c}/\alpha(\mathcal{V}^\pm)\right) \\
= \; & \mathrm{Char}_{\Gamma_{\mathcal{O}_p}}\left(\mathcal{U}^\rho_{K_c}/(\mathcal{V}^\pm + \mathcal{C}^\rho_{K_c})\right).
\end{aligned}$$

By Corollary 4.4.3, the quotient

$$H^1(\mathbb{Q}_{c,p}, T_{\bar{f}}(k-1))/H^1_{\pm}(\mathbb{Q}_{c,p}, T_{\bar{f}}(k-1))$$

is free of rank one over $\Gamma_{\mathbb{Z}_p}$. Hence, by (4.1) and the proofs of Lemma 4.4.1 and Corollary 4.4.3, the $\Gamma_{\mathbb{Z}_p}$-module

$$\mathrm{Hom}\left(H^1_f(\mathbb{Q}_{c,p}, T_f(1))^{\pm}, \mathbb{Z}_p\right)$$

is also free of rank one and it has a generator $f_{\pm}$ such that

$$\sum_{\sigma \in G_n} f_{\pm}(\exp_{n,1}(\gamma_{n,1}(\eta_1^{\pm})^{\sigma}))\sigma \equiv p^{s^{\pm}} \log^{\pm}_{p,k} \mod (\gamma^{p^{n-1}} - 1). \tag{6.2}$$

Note that we have abused notation by writing $\exp_{n,1}(\gamma_{n,1}(\eta_1^{\pm}))$ for its image in $H^1(\mathbb{Q}_p^{(n-1)}, T_f(1))$ under the corestriction.

As in [PR04, Theorems 7.1 and 7.2], we have

$$\begin{aligned}
\mathrm{Hom}\left(H^1_f(\mathbb{Q}_{c,p}, A)^{\pm}, \mathbb{Q}_p/\mathbb{Z}_p\right) &\cong \mathrm{Hom}\left(H^1_f(\mathbb{Q}_{c,p}, T_f(1))^{\pm}, \mathbb{Z}_p\right), \\
\mathrm{Hom}_{\mathcal{O}}\left(H^1_f(K_{c,p}, A)^{\pm}, K_p/\mathcal{O}_p\right) &\cong \mathrm{Hom}\left(H^1_f(\mathbb{Q}_{c,p}, A)^{\pm}, \mathbb{Q}_p/\mathbb{Z}_p\right) \otimes \mathcal{O}_p.
\end{aligned}$$

Let $\mu^{\pm}$ (resp. $\vartheta^{\pm}$) be the image of $f_{\pm}$ (resp. ξ from Proposition 6.3.3) in $\mathrm{Hom}_{\mathcal{O}}\left(H^1_f(K_{c,p}, A)^{\pm}, K_p/\mathcal{O}_p\right)$. Then $\vartheta^{\pm} = h^{\pm}\mu^{\pm}$ for some $h^{\pm} \in \Gamma_{\mathcal{O}_p}$. As in [PR04, proof of Theorem 7.2], there is an isomorphism

$$\mathcal{U}^{\rho}_{K_c}/(\mathcal{V}^{\pm} + \mathcal{C}^{\rho}_{K_c}) \cong \Gamma_{\mathcal{O}_p}/h^{\pm}\Gamma_{\mathcal{O}_p}.$$

Hence we have:

$$\mathrm{Char}_{\Gamma_{\mathcal{O}_p}}\left(\mathrm{Hom}_{\mathcal{O}}\left(\mathrm{Sel}^{\pm}_p(f/K_c), K_p/\mathcal{O}_p\right)\right) = h^{\pm}\Gamma_{\mathcal{O}_p}.$$

Let F be a finite extension of K contained in K_c, θ a character of G, the Galois group of F over K, $x \in H^1_f(F_p, A)$, r and integer, then $\vartheta^{\pm} = h^{\pm}\mu^{\pm}$ implies

$$\sum_{\sigma \in G} \theta(\sigma)\vartheta^{\pm}(x^{\sigma} \otimes p^{-r}) = \theta(h^{\pm}) \sum_{\sigma \in G} \theta(\sigma)\mu^{\pm}(x^{\sigma} \otimes p^{-r}) \tag{6.3}$$

We now take $x = \exp_{n,1}(\gamma_{n,1}(\eta_1^{\pm}))$. By (6.2), the RHS of (6.3) is just $p^{-r+s^{\pm}}\theta(h^{\pm})\theta(\log^{\pm}_{p,k})$. Hence, (6.1) implies that the LHS of (6.3) equals to the following:

$$p^{-r} \frac{L(f_{\theta^{-1}}, 1)}{\Omega_f^{\delta}} \left[\sum_{\sigma \in G} \theta(\sigma)\gamma_{n,1}(\eta_1^{\pm})^{\sigma}, \bar{\omega}_{-1}\right]$$

where $\delta = \theta(-1)$. We now compute $\sum_{\sigma\in G}\theta(\sigma)\gamma_{n,1}(\eta_1^{\pm})^{\sigma}$.

Take F to be $K_p^{(n-1)}$ and θ a character of conductor p^n. Then

$$\begin{aligned}\sum_{\sigma\in G}\theta(\sigma)\gamma_{n,1}(\eta^{\pm})^{\sigma} &= \sum_{\sigma\in G}\frac{\theta(\sigma)}{p^n}\left(\sum_{i=0}^{n-1}\zeta_{p^{n-i}}^{\sigma}\otimes\varphi^{i-n}(\eta_1^{\pm})+(1-\varphi)^{-1}(\eta_1^{\pm})\right)\\ &= p^{-n}\sum_{\sigma\in G}\theta(\sigma)\zeta_{p^n}^{\sigma}\otimes\varphi^{-n}(\eta_1^{\pm})\\ &= p^{-n}\tau(\theta)\varphi^{-n}(\eta_1^{\pm})\end{aligned}$$

where $\tau(\theta)$ denotes the Gauss sum of θ. Since $\varphi^2+\epsilon(p)p^{k-3}=0$ on $\mathbb{D}(V_f(1))$, we have

$$\begin{aligned}\varphi^{-n}(\eta_1^{-}) &= (-\epsilon(p)p^{k-3})^{\frac{-n-1}{2}}p^{-1}\varphi(\omega)_1/[\varphi(\omega),\bar{\omega}]\quad(\text{for } n \text{ odd}),\\ \varphi^{-n}(\eta_1^{+}) &= (-\epsilon(p)p^{k-3})^{\frac{-n}{2}}\varphi(\omega)_1/[\varphi(\omega),\bar{\omega}]\quad(\text{for } n \text{ even}).\end{aligned}$$

Hence, (6.3) implies:

$$\begin{aligned}p^{s^-}\theta(h^-)\theta(\log_{p,k}^{-}) &= (-\epsilon(p)p^{k-1})^{\frac{-n-1}{2}}\tau(\theta)\frac{L(f_{\theta^{-1}},1)}{\Omega_f^{\delta}}\quad(\text{for } n \text{ odd}),\\ p^{s^+}\theta(h^+)\theta(\log_{p,k}^{+}) &= (-\epsilon(p)p^{k-1})^{\frac{-n}{2}}\tau(\theta)\frac{L(f_{\theta^{-1}},1)}{\Omega_f^{\delta}}\quad(\text{for } n \text{ even}).\end{aligned}$$

Therefore, by the interpolating properties of $L_p^{\pm}$ at these characters, we have:

$$\begin{aligned}p^{s^-}\theta(h^-) &= \theta(L_p^-)\quad(\text{for } n \text{ odd}),\\ p^{s^+}\theta(h^+) &= \theta(L_p^+)\quad(\text{for } n \text{ even}).\end{aligned}$$

But $h^{\pm}$ and $L_p^{\pm}$ are both $O(1)$ and the above holds for infinitely many n, so $h^{\pm}=p^{-s^{\pm}}L_p^{\pm}$. Hence we are done. □

By taking $\mathcal{G}$-invariants, we have the following.

Corollary 6.4.2. $\mathrm{Char}_{\Gamma_{\mathbb{Z}_p}}\left(\mathrm{Sel}_p^{\pm}(f/\mathbb{Q}_c)^{\vee}\right)=\left(p^{-s^{\pm}}L_p^{\pm}\right)$.

Chapter 7

Wach modules and modular forms

Let f be a modular form as in Section 1.3.5. In this chapter, we explain how some of our earlier results can be generalised for more general a_p. In particular, we construct Coleman maps for f at an arbitrary good prime - either ordinary or supersingular. When $v_p(a_p)$ is large in a precise sense, we give a reformulation of Kato's main conjecture as in Chapter 5 by carrying out some explicit calculations.

7.1 Positive crystalline representations

7.1.1 Generality of Wach modules

We first review some results on Wach modules. Proofs can be found in [Ber03, Ber04, BB10].

Let E be a finite extension of $\mathbb{Q}_p$ and V a crystalline representation of $G_{\mathbb{Q}_p}$ which is E-linear, with Hodge-Tate weights in $[a, b]$. The Wach module of V is the unique $E \otimes_{\mathbb{Q}_p} \mathbb{B}^+_{\mathbb{Q}_p}$-module $\mathbb{N}(V)$ in $D(V)$ such that the following conditions are satisfied:

1. $\mathbb{N}(V)$ is free of rank $d = \dim_E(V)$ over $E \otimes_{\mathbb{Q}_p} \mathbb{B}^+_{\mathbb{Q}_p}$;
2. the action of G_∞ preserves $\mathbb{N}(V)$ and is trivial on $\mathbb{N}(V)/\pi\mathbb{N}(V)$;
3. $\varphi(\pi^b\mathbb{N}(V)) \subset \pi^b\mathbb{N}(V)$ and $\pi^b\mathbb{N}(V)/\varphi^*(\pi^b\mathbb{N}(V))$ is killed by q^{b-a}, where $\varphi^* M$ denotes the R-module generated by $\varphi(M)$ if M is a R-module equipped with an action of φ.

When V is positive, we endow $\mathbb{N}(V)$ with the filtration

$$\mathrm{Fil}^i\,\mathbb{N}(V) = \{x \in \mathbb{N}(V) \mid \varphi(x) \in q^i\mathbb{N}(V)\}.$$

Then, $\mathbb{N}(V)/\pi\mathbb{N}(V)$ is a filtered E-linear φ-module, and there is an isomorphism $\mathbb{N}(V)/\pi\mathbb{N}(V) \cong \mathbb{D}(V)$. Moreover, we can recover $\mathbb{D}(V)$ from $\mathbb{N}(V)$ as

$$\mathbb{D}(V) = \left(\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p} \otimes_{\mathbb{B}^+_{\mathbb{Q}_p}} \mathbb{N}(V)\right)^{G_\infty}.$$

If T is an $\mathcal{O}_E$-lattice in V stable under $G_{\mathbb{Q}_p}$, then $\mathbb{N}(T) = \mathbb{N}(V) \cap D(T)$ is an $\mathcal{O}_E \otimes_{\mathbb{Z}_p} \mathbb{A}^+_{\mathbb{Q}_p}$-lattice in $\mathbb{N}(V)$, and the functor $T \mapsto \mathbb{N}(T)$ gives a bijection between the $G_{\mathbb{Q}_p}$-stable lattices T in V and the $\mathcal{O}_E \otimes_{\mathbb{Z}_p} \mathbb{A}^+_{\mathbb{Q}_p}$-lattices in $\mathbb{N}(V)$ satisfying

1. $\mathbb{N}(T)$ is free of rank $d = \dim_E(V)$ over $\mathcal{O}_E \otimes_{\mathbb{Z}_p} \mathbb{A}^+_{\mathbb{Q}_p}$;
2. the action of G_∞ preserves $\mathbb{N}(T)$;
3. $\varphi(\pi^b\mathbb{N}(T)) \subset \pi^b\mathbb{N}(T)$ and $\pi^b\mathbb{N}(T)/\varphi^*(\pi^b\mathbb{N}(T))$ is killed by q^{b-a}.

Let m be an integer. For the Tate twist $T(m)$ of T, its Wach module is related to that of T by

$$\mathbb{N}(T(m)) = \pi^{-m}\mathbb{N}(T) \otimes e_m.$$

Theorem 7.1.1 (Berger). *Let T be as above, then $(\varphi^*\mathbb{N}(T))^{\psi=0}$ is a free $\Lambda_{\mathcal{O}_E}$-module of rank d. Moreover, if $n_1^0, \ldots, n_d^0$ is a basis of $\mathbb{N}(T)$, then there exists a basis $n_1, \ldots, n_d$ such that $n_i \equiv n_i^0 \mod \pi$ for all i and*

$$(1+\pi)\varphi(n_1 \otimes \pi^{-m}e_m), \ldots, (1+\pi)\varphi(n_d \otimes \pi^{-m}e_m)$$

form a $\Lambda_{\mathcal{O}_E}$-basis of $(\varphi^*\mathbb{N}(T(m)))^{\psi=0}$ for all integers m.

7.1.2 Construction of Coleman maps

Assume that V is a positive d-dimensional E-linear representation of $G_{\mathbb{Q}_p}$ with Hodge-Tate weights $-r_d \le -r_{d-1} \le \cdots \le -r_1 \le 0$ and it has no quotient isomorphic to $E(-r_d)$. Fix an $\mathcal{O}_E$-lattice T in V stable under $G_{\mathbb{Q}_p}$ and a basis $n_1, \ldots, n_d$ of $\mathbb{N}(T)$ given by Theorem 7.1.1 and write P for the matrix of φ with respect to this basis. Then, as column vectors,

$$\begin{pmatrix} \varphi(n_1) \\ \vdots \\ \varphi(n_d) \end{pmatrix} = P^T \begin{pmatrix} n_1 \\ \vdots \\ n_d \end{pmatrix}.$$

Moreover, the determinant of P is $q^{r_1+\cdots+r_d}$ up to a unit.

Let $m = \sum_{i=1}^{d} r_i$, then $D(T(m))^{\psi=1} = \mathbb{N}(T(m))^{\psi=1}$ by [Ber03, Theorem A.3]. So, if $x \in D(T(m))^{\psi=1}$, there exist unique $x_1, \ldots, x_d \in \mathcal{O}_E \otimes \mathbb{A}^+_{\mathbb{Q}_p}$ such that

$$x = \pi^{-m} \begin{pmatrix} x_1 & \cdots & x_d \end{pmatrix} \begin{pmatrix} n_1 \\ \vdots \\ n_d \end{pmatrix} \otimes e_m. \tag{7.1}$$

Let $\nu_1, \ldots, \nu_d$ be a basis of $\mathbb{D}(V)$ over E and write A_φ for the matrix of φ with respect to this basis. We have

$$\mathbb{D}(V) \subset (E \otimes \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}) \otimes \mathbb{N}(V)$$

and there exists a matrix $M \in M(d, E \otimes \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})$ such that

$$\begin{pmatrix} \nu_1 \\ \vdots \\ \nu_d \end{pmatrix} = M \begin{pmatrix} n_1 \\ \vdots \\ n_d \end{pmatrix}.$$

The determinant of M is equal to $(t/\pi)^m$ up to a unit in $E \otimes \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}$. Moreover, the isomorphism $\mathbb{N}(V)/\pi\mathbb{N}(V) \cong \mathbb{D}(V)$ means that we may assume $M|_{\pi=0} = I$, the identity matrix. The compatibility of the action of φ implies that

$$\varphi(M)P^T = A_\varphi^T M. \tag{7.2}$$

We can now rewrite (7.1):

$$x = \begin{pmatrix} x_1 & \cdots & x_d \end{pmatrix} \cdot \left(\frac{t}{\pi}\right)^m M^{-1} \begin{pmatrix} \nu_{1,m} \\ \vdots \\ \nu_{d,m} \end{pmatrix} \tag{7.3}$$

with $(t/\pi)^m M^{-1} \in M(d, E \otimes \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p})$ and $\{\nu_{i,m} = \nu_i \otimes t^{-m} e_m : i = 1, \ldots, d\}$ gives a basis of $\mathbb{D}(V(m))$.

Lemma 7.1.2. *For any x as above, the entries of the row vector*

$$\mathbf{Col}(x) := \begin{pmatrix} x_1 & \cdots & x_d \end{pmatrix} q^m (P^T)^{-1} - \begin{pmatrix} \varphi(x_1) & \cdots & \varphi(x_d) \end{pmatrix}$$

are elements of $\left(\mathcal{O}_E \otimes \mathbb{A}^+_{\mathbb{Q}_p}\right)^{\psi=0}$.

Proof. Since the determinant of P is q^m up to a unit in $\mathcal{O}_E \otimes \mathbb{A}^+_{\mathbb{Q}_p}$, the entries of $\mathbf{Col}(x)$ are indeed elements of $\mathcal{O}_E \otimes \mathbb{A}^+_{\mathbb{Q}_p}$. It remains to show that $\psi(\mathbf{Col}(x)) = 0$.

But $\varphi(\pi) = \pi q$, (7.1) implies that

$$x = \begin{pmatrix} x_1 & \cdots & x_d \end{pmatrix} q^m (P^T)^{-1} \varphi(\pi^{-m}) \begin{pmatrix} \varphi(n_1) \\ \vdots \\ \varphi(n_d) \end{pmatrix} \otimes e_m.$$

Hence,

$$\psi(x) = \psi\left(\begin{pmatrix} x_1 & \cdots & x_d \end{pmatrix} q^m (P^T)^{-1} \right) \pi^{-m} \begin{pmatrix} n_1 \\ \vdots \\ n_d \end{pmatrix} \otimes e_m.$$

Therefore, $\psi(x) = x$ implies that

$$\psi\left(\begin{pmatrix} x_1 & \cdots & x_d \end{pmatrix} q^m (P^T)^{-1} \right) = \begin{pmatrix} x_1 & \cdots & x_d \end{pmatrix}.$$

Hence the result. □

Definition 7.1.3. *For $1 \leq i \leq d$, we define*

$$\mathrm{Col}_i : D(T(m))^{\psi=1} \to \left(\mathcal{O}_E \otimes \mathbb{A}^+_{\mathbb{Q}_p} \right)^{\psi=0}$$

by sending x to the ith component of $\mathbf{Col}(x)$ as defined in Lemma 7.1.2.

It is clear that Col_i depends on the choice of basis. The precise dependence is given by the following.

Lemma 7.1.4. *Let $n_1, \ldots, n_d$ and $n'_1, \ldots, n'_d$ be two bases of $\mathbb{N}(T)$ with*

$$\begin{pmatrix} n_1 \\ \vdots \\ n_d \end{pmatrix} = \mathcal{M} \begin{pmatrix} n'_1 \\ \vdots \\ n'_d \end{pmatrix}.$$

Then, the respective Coleman maps defined by these two bases, $\mathbf{Col}$ and $\mathbf{Col}'$ are related by $\mathbf{Col}(x)\varphi(\mathcal{M}) = \mathbf{Col}'(x)$ for all $x \in D(T(m))^{\psi=1}$.

Proof. For any $x \in D(T(m))^{\psi=1}$, write $x = x_1 n_1 + \cdots + x_d n_d = x'_1 n'_1 + \cdots + x'_d n'_d$. Then,

$$\begin{pmatrix} x'_1 & \cdots & x'_d \end{pmatrix} = \begin{pmatrix} x_1 & \cdots & x_d \end{pmatrix} \mathcal{M}$$

Let P and P' be the matrices of φ with respect to $n_1, \ldots, n_d$ and $n'_1, \ldots, n'_d$ respectively, then $P^T \mathcal{M} = \varphi(\mathcal{M}) P'^T$. Therefore,

$$\begin{aligned} \mathbf{Col}'(x) &= \begin{pmatrix} x'_1 & \cdots & x'_d \end{pmatrix} q^m (P'^T)^{-1} - \begin{pmatrix} \varphi(x'_1) & \cdots & \varphi(x'_d) \end{pmatrix} \\ &= \begin{pmatrix} x_1 & \cdots & x_d \end{pmatrix} q^m \mathcal{M} (P'^T)^{-1} - \begin{pmatrix} \varphi(x_1) & \cdots & \varphi(x_d) \end{pmatrix} \varphi(\mathcal{M}) \\ &= \begin{pmatrix} x_1 & \cdots & x_d \end{pmatrix} q^m (P^T)^{-1} \varphi(\mathcal{M}) - \begin{pmatrix} \varphi(x_1) & \cdots & \varphi(x_d) \end{pmatrix} \varphi(\mathcal{M}). \end{aligned}$$

Hence the lemma. □

By simple calculations, $\mathbf{Col}(x)$ can be related to $(1-\varphi)(x)$:

$$(1-\varphi)(x) = \mathbf{Col}(x)\varphi(\pi)^{-m}P^T \begin{pmatrix} n_1 \\ \vdots \\ n_d \end{pmatrix} \otimes e_m \tag{7.4}$$

$$= \mathbf{Col}(x)\varphi\left(\begin{pmatrix} n_1 \\ \vdots \\ n_d \end{pmatrix} \pi^{-m} \otimes e_m\right) \tag{7.5}$$

$$= \mathbf{Col}(x)\left(\frac{t}{\pi q}\right)^m P^T M^{-1} \begin{pmatrix} \nu_{1,m} \\ \vdots \\ \nu_{d,m} \end{pmatrix}. \tag{7.6}$$

Remark 7.1.5. *By* (7.5)*, we can prove Lemma 7.1.2 using the fact that* $\psi(x) = x$ *iff* $\psi \circ (1-\varphi)(x) = 0$.

Note that Col_i defined above are not $\Lambda_{\mathcal{O}_E}$-homomorphisms. However, by (7.5), $(1-\varphi)(x) \in (\varphi^*\mathbb{N}(T(m)))^{\psi=0}$ for any $x \in D(T(m))^{\psi=1}$. Therefore, Theorem 7.1.1 allows us to define:

Definition 7.1.6. *For* $i = 1, \ldots, d$*, we define* $\underline{\mathrm{Col}}_i : D(T(m))^{\psi=1} \to \Lambda_{\mathcal{O}_E}$ *by the relation*

$$(1-\varphi)(x) = \sum_{i=1}^{d} \underline{\mathrm{Col}}_i(x) \cdot [(1+\pi)\varphi(n_i \otimes \pi^{-m}e_m)]$$

for $x \in D(T(m))^{\psi=1}$

We are interested in both sets of Coleman maps which arise from a modular form. Although the former is not $\Lambda_{\mathcal{O}_E}$-homomorphism, it has the advantage of being more explicit than the latter. It is clear that these maps can be extended to a map on $D(V(m))^{\psi=1}$ (with images in $\left(E \otimes \mathbb{B}^+_{\mathbb{Q}_p}\right)^{\psi=0}$ and Λ_E respectively). On abusing notation, we write these maps as Col_i and $\underline{\mathrm{Col}}_i$ as well.

7.2 p-supersingular modular forms

Let f be as in Section 1.3.5 with $v_p(a_p) > 0$. On choosing appropriate bases, we obtain two pairs of p-adic L-functions (as elements of $E \otimes B^{+,\psi=0}_{\mathbb{Q}_p}$ and Λ_E respectively) associated to f by applying the Coleman maps from Section 7.1 to the restriction of $V_{\bar{f}}$ to $G_{\mathbb{Q}_p}$. We then study some of their basic properties and consequences.

7.2.1 Construction of p-adic L-functions

For simplicity, we assume that $\epsilon(p) = 1$. In particular $a_p = \bar{a}_p$. Recall that we have de Rham filtration

$$\mathbb{D}^i(V_f) = \begin{cases} E\nu_1 \oplus E\nu_2 & \text{if } i \leq 0 \\ E\nu_1 & \text{if } 1 \leq i \leq k-1 \\ 0 & \text{if } i \geq k \end{cases} \tag{7.7}$$

for some basis ν_1, ν_2 over E. By Theorem 2.3.5, ν_1 is not an eigenvalue of φ and we may choose $\nu_2 = p^{1-k}\varphi(\nu_1)$ so that the matrix A_φ of φ with respect to this basis is given by

$$\begin{pmatrix} 0 & -1 \\ p^{k-1} & a_p \end{pmatrix}$$

as $\varphi^2 - a_p\varphi + p^{k-1} = 0$. We call such a basis a 'good basis' for $\mathbb{D}(V_f)$.

Let $\bar{\nu}_1, \bar{\nu}_2$ be a 'good basis' of $\mathbb{D}(V_{\bar{f}})$. Then, the matrix of φ with respect to this basis is again equal to A_φ also since $a_p = \bar{a}_p$.

Pick a basis n_1, n_2 of $\mathbb{N}(V_{\bar{f}})$ lifting $\bar{\nu}_1, \bar{\nu}_2$ as given by Theorem 7.1.1. It then determines lattices $T_{\bar{f}}$ and T_f as in Section 2.3.1. Note that $V_{\bar{f}}$ is irreducible with Hodge-Tate weights 0 and $-k+1$, so it has no quotient isomorphic to a Tate twist of E. Therefore, we obtain two sets of Coleman maps associated to f, namely

$$\begin{aligned} \mathrm{Col}_i : D(T_{\bar{f}}(k-1))^{\psi=1} &\to \left(\mathcal{O}_E \otimes \mathbb{A}^+_{\mathbb{Q}_p}\right)^{\psi=0}, \\ \underline{\mathrm{Col}}_i : D(T_{\bar{f}}(k-1))^{\psi=1} &\to \Lambda_{\mathcal{O}_E}, \end{aligned}$$

for $i \in \{1, 2\}$. We can then define two pairs of p-adic L-functions:

Definition 7.2.1. *For $i = 1, 2$, define $L_{p,i} = \mathrm{Col}_i(\mathbf{z}) \in (E \otimes \mathbb{B}^+_{\mathbb{Q}_p})^{\psi=0}$ and $\tilde{L}_{p,i} = \underline{\mathrm{Col}}_i(\mathbf{z}) \in \Lambda_E$ where $\mathbf{z}$ is the image of the localisation of $\mathbf{z}^{\mathrm{Kato}}$ (after twisting) under $(h^1_{\mathrm{Iw}})^{-1}$.*

Below is a list of assumptions which we need for establishing some of the properties of these Coleman maps and p-adic L-functions.

- **Assumption (A)**: $k \geq 3$.
- **Assumption (B)**: a_p is not of the form $p^j + p^{k-2-j}$ for some integer j.
- **Assumption (C)**: $v_p(a_p) > \lfloor (k-2)/(p-1) \rfloor$.
- **Assumption (D)**: $p \geq k-1$.

Additionally, we always assume that the eigenvalues of φ on $\mathbb{D}(V_f)$ are not integral powers of p as before.

7.2.2 Properties

Decomposition of p-adic L-functions

Let α and β be the roots of the quadratic $X^2 - a_p X + p^{k-1}$. By Theorem 2.3.1, we can associate to α and β p-adic L-functions $L_{p,\alpha}$ and $L_{p,\beta}$ respectively. We show that there is a decomposition of these p-adic L-functions in terms of $L_{p,i}$ and $\tilde{L}_{p,i}$, $i = 1, 2$. This generalises (2.9) and (2.10) for the case $a_p = 0$ and (2.16) and (2.17) for the case $k = 2$.

Let ν_1, ν_2 and $\bar{\nu}_1, \bar{\nu}_2$ be 'good bases' for $\mathbb{D}(V_f)$ and $\mathbb{D}(V_{\bar{f}})$ respectively. Then, $\nu_{1,1} \in \mathbb{D}^0(V_f(1))$ and $\bar{\nu}_{1,k-1} \in \mathbb{D}^0(V_{\bar{f}}(k-1))$ for $i = 1, 2$. Under the pairing

$$[\ ,\ ] : \mathbb{D}(V_f(1)) \times \mathbb{D}(V_{\bar{f}}(k-1)) \to \mathbb{D}(E(1)) = E \cdot e_1 t^{-1}, \tag{7.8}$$

we have $[\nu_{1,1}, \bar{\nu}_{1,k-1}] = 0$. By applying φ, we have $[\nu_{2,1}, \bar{\nu}_{2,k-1}] = 0$, too. We also have $[\nu_{1,1}, \bar{\nu}_{2,k-1}] = -[\nu_{2,1}, \bar{\nu}_{1,k-1}] \neq 0$. Without loss of generality, we may assume this common quantity is 1.

Proposition 7.2.2. *Let ν_i and $\bar{\nu}_i$ be as above. For all $x \in D(T_{\bar{f}}(k-1))^{\psi=1}$,*

$$\mathfrak{M}\begin{pmatrix} -\mathcal{L}_{\nu_2}(h^1_{\mathrm{Iw}}(x)) & \mathcal{L}_{\nu_1}(h^1_{\mathrm{Iw}}(x)) \end{pmatrix} = \begin{pmatrix} \mathrm{Col}_1(x) & \mathrm{Col}_2(x) \end{pmatrix} M'$$

as row vectors, where $\mathcal{L}_\eta$ is as defined by (2.7) for $\eta = \nu_1, \nu_2$ and $M' = \left(\frac{t}{\pi q}\right)^{k-1} P^T M^{-1}$ and $\mathfrak{M}$ is as defined in Section 1.3.4.

Proof. Proved by S. Zerbes, see [LLZ10, Proposition 3.19]. □

Let η_α and η_β be as in Theorem 2.3.5, then

$$\mathcal{L}_{\eta_\alpha}(\mathbf{z}^{\mathrm{Kato}}) = L_{p,\alpha} \quad \text{and} \quad \mathcal{L}_{\eta_\beta}(\mathbf{z}^{\mathrm{Kato}}) = L_{p,\beta}.$$

By elementary calculations, $\eta_\alpha = \alpha^{-1}\nu_1 - \nu_2$ and $\eta_\beta = \beta^{-1}\nu_1 - \nu_2$. Therefore, on writing

$$M' = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix},$$

Definition 7.2.1 and Proposition 7.2.2 implies

$$\begin{aligned} \mathfrak{M}(L_{p,\alpha}) &= (\alpha^{-1} m_{12} + m_{11}) L_{p,1} + (\alpha^{-1} m_{22} + m_{21}) L_{p,2}, \\ \mathfrak{M}(L_{p,\beta}) &= (\beta^{-1} m_{12} + m_{11}) L_{p,1} + (\beta^{-1} m_{22} + m_{21}) L_{p,2}. \end{aligned}$$

Hence, $L_{p,1}$ and $L_{p,2}$ can be written as

$$L_{p,1} = \frac{(\beta^{-1}m_{22}+m_{21})\mathfrak{M}(L_{p,\alpha})-(\alpha^{-1}m_{22}+m_{21})\mathfrak{M}(L_{p,\beta})}{(\beta^{-1}-\alpha^{-1})\det(M')}, \quad (7.9)$$

$$L_{p,2} = \frac{(\beta^{-1}m_{12}+m_{11})\mathfrak{M}(L_{p,\alpha})-(\alpha^{-1}m_{12}+m_{11})\mathfrak{M}(L_{p,\beta})}{(\alpha^{-1}-\beta^{-1})\det(M')}. \quad (7.10)$$

Let $x \in D(V_{\bar{f}}(k-1))^{\psi=1}$. By Proposition 7.2.2 and (7.6),

$$(1-\varphi)x = \mathfrak{M}\circ\mathcal{L}_{1,\nu_1}\circ h^1_{\mathrm{Iw}}(x)\bar{\nu}_{2,k-1} - \mathfrak{M}\circ\mathcal{L}_{1,\nu_2}\circ h^1_{\mathrm{Iw}}(x)\bar{\nu}_{1,k-1}$$

Therefore, by the definition of $\underline{\mathrm{Col}}_i$,

$$\begin{pmatrix}\underline{\mathrm{Col}}_1 & \underline{\mathrm{Col}}_2\end{pmatrix}\cdot[(1+\pi)M'] = \mathfrak{M}\begin{pmatrix}-\mathcal{L}_{\nu_2}\circ h^1_{\mathrm{Iw}} & \mathcal{L}_{\nu_1}\circ h^1_{\mathrm{Iw}}\end{pmatrix}.$$

Let $\underline{M} = \mathfrak{M}^{-1}[(1+\pi)M'] \in M(2,\mathcal{H}(G_\infty))$, then

$$\begin{pmatrix}\underline{\mathrm{Col}}_1 & \underline{\mathrm{Col}}_2\end{pmatrix}\underline{M} = \begin{pmatrix}-\mathcal{L}_{\nu_2}\circ h^1_{\mathrm{Iw}} & \mathcal{L}_{\nu_1}\circ h^1_{\mathrm{Iw}}\end{pmatrix}. \quad (7.11)$$

Therefore, by exactly the same calculation as above, we have:

$$L_{p,\alpha} = (\alpha^{-1}\underline{m}_{12}+\underline{m}_{11})\tilde{L}_{p,1} + (\alpha^{-1}\underline{m}_{22}+\underline{m}_{21})\tilde{L}_{p,2} \quad (7.12)$$

$$L_{p,\beta} = (\beta^{-1}\underline{m}_{12}+\underline{m}_{11})\tilde{L}_{p,1} + (\beta^{-1}\underline{m}_{22}+\underline{m}_{21})\tilde{L}_{p,2} \quad (7.13)$$

where $\begin{pmatrix}\underline{m}_{ij}\end{pmatrix} = \underline{M}$.

Interpolating properties

Proposition 7.2.3. *Let θ be a primitive character modulo p, then*

$$\theta(\tilde{L}_{p,1}) = \frac{\tau(\theta)}{p^{k-1}}\cdot\frac{L(f_{\theta^{-1}},1)}{\Omega_f^{\theta(-1)}},$$

$$\theta(\tilde{L}_{p,2}) = 0.$$

Similarly, if θ is the trivial character, then

$$\theta(\tilde{L}_{p,1}) = \frac{a_p-p^{k-2}-1}{p^{k-1}}\cdot\frac{L(f,1)}{\Omega_f^+},$$

$$\theta(\tilde{L}_{p,2}) = \left(\frac{1}{p}-1\right)\cdot\frac{L(f,1)}{\Omega_f^+}.$$

Proof. Since

$$M' = (t/\pi q)^{k-1}P^TM^{-1} = (t/\pi q)^{k-1}\varphi(M^{-1})A_\varphi^T$$

and $M|_{\pi=0} = I$, we have $M'|_{\pi=(\zeta-1)} = A_\varphi^T$ for any pth root of unity ζ. By the compatibility of Fourier transforms (see Theorem 7.4.1 below), we have $\theta(\underline{M}) = A_\varphi^T$ for any character θ modulo p. By (7.12) and (7.13), we have

$$\begin{aligned}\theta(\tilde{L}_{p,1}) &= \frac{(\beta^{-1}a_p - 1)\theta(L_{p,\alpha}) - (\alpha^{-1}a_p - 1)\theta(L_{p,\beta})}{(\beta^{-1} - \alpha^{-1})p^{k-1}},\\ \theta(\tilde{L}_{p,2}) &= \frac{(\beta^{-1}p^{k-1})\theta(L_{p,\alpha}) - (\alpha^{-1}p^{k-1})\theta(L_{p,\beta})}{(\alpha^{-1} - \beta^{-1})p^{k-1}}.\end{aligned}$$

Hence, we are done by the values of $\theta(L_{p,\alpha})$ and $\theta(L_{p,\beta})$ as given in [AV75] and [MTT86]. $\square$

Corollary 7.2.4. *If assumption (A) holds, then $\tilde{L}_{p,i} \neq 0$ for $i \in \{1,2\}$. Moreover, if η is a character of Δ, then $\tilde{L}^{\eta}_{p,1} \neq 0$.*

Remark 7.2.5. *We see that the interpolating properties of $\tilde{L}_{p,1}$ and $\tilde{L}_{p,2}$ at characters modulo p are independent of the choice of n_1, n_2 as long as we have fixed a pair of 'good bases' for $\mathbb{D}(V_f)$ and $\mathbb{D}(V_{\bar{f}})$.*

Remark 7.2.6. *It is not hard to see that $\mathfrak{M}^{-1}(L_{p,i})$ has the same interpolating properties as $\tilde{L}_{p,i}$ at characters modulo p for $i = 1, 2$ because the action of G_∞ on $\mathbb{N}(T_{\bar{f}}(k-1))$ is trivial modulo π, so $\mathfrak{M}(L_{p,i}) \equiv \tilde{L}_{p,i} \mod \varphi(\pi)$ by comparing* (7.5) *and Definition 7.1.6.*

7.2.3 Infinitude of zeros

We generalise [Pol03, Theorem 3.5] beyond the case $a_p = 0$ using our decomposition of $L_{p,\alpha}$ and $L_{p,\beta}$.

Proposition 7.2.7. *Let η be a character of Δ, then either $L^{\eta}_{p,\alpha}$ or $L^{\eta}_{p,\beta}$ has infinitely many zeros.*

Proof. Assume the contrary, then [Pol03, Lemma 3.2] implies that $L^{\eta}_{p,\alpha}$ and $L^{\eta}_{p,\beta}$ are $O(1)$.

By [BB10, Lemmas 3.3.5 and 3.3.6], the entries of M are $O(\log_p^m)$ where $m = \max\{v_p(\alpha), v_p(\beta)\} < k-1$. Therefore, with the notation above, $m_{ij} = O(\log_p^m)$ for $i, j \in \{1,2\}$. In particular, the η-component of

$$(\beta^{-1}m_{22} + m_{21})L_{p,\alpha} - (\alpha^{-1}m_{22} + m_{21})L_{p,\beta}$$

is $O(\log_p^m)$. By (7.9), the quantity above is divisible by $(t/\pi q)^{k-1} \sim \log_p^{k-1}$ which forces $L^{\eta}_{p,1} = 0$ contradicting Corollary 7.2.3 and Remark 7.2.6. $\square$

As in [Pol03, Theorem 3.5], we have:

Corollary 7.2.8. *If $\alpha \notin F_f(\eta)$, then both $L^{\eta}_{p,\alpha}$ and $L^{\eta}_{p,\beta}$ have infinitely many zeros.*

7.3 Modular forms with $v_p(a_p) > \lfloor (k-2)/(p-1) \rfloor$

Under assumption (C), a canonical basis for $\mathbb{N}(T_{\bar{f}})$ has been constructed in [BLZ04]. In this section, we study this basis and prove the surjectivity of Col_1 and $\underline{\mathrm{Col}}_1$.

Define

$$\log^+(1+\pi) = \prod_{n\geq 0} \frac{\varphi^{2n+1}(q)}{p} \qquad \text{and} \qquad \log^-(1+\pi) = \prod_{n\geq 0} \frac{\varphi^{2n}(q)}{p}.$$

Write $m = \lfloor (k-2)/(p-1) \rfloor$ and let z_i be elements of $\mathbb{Q}_p$ such that

$$p^m \left(\frac{\log^-(1+\pi)}{\log^+(1+\pi)} \right)^{k-1} = \sum_{i\geq 0} z_i \pi^i,$$

then [BLZ04, Proposition 3.1.1] says that

$$z = \sum_{i=0}^{k-2} z_i \pi^i \in \mathbb{Z}_p[[\pi]].$$

Theorem 7.3.1 (Berger-Li-Zhu)**.** *Under assumption (C), i.e. $v_p(a_p) > m$, there is a canonical basis of $\mathbb{N}(T_{\bar{f}})$ such that the matrix of φ with respect to this basis, P, is given by*

$$\begin{pmatrix} 0 & -1 \\ q^{k-1} & \delta z \end{pmatrix}$$

where $\delta = a_p/p^m$.

It is easy to check that this basis reduces to a 'good basis' of $\mathbb{D}(V_{\bar{f}})$. We define the Coleman maps with respect to this basis. For any $x \in D(T_{\bar{f}}(k-1))^{\psi=1}$ with

$$x = \pi^{1-k} \begin{pmatrix} x_1 & x_2 \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \otimes e_{k-1},$$

we can express $\mathrm{Col}_i(x)$, $i = 1, 2$, in terms of x_1 and x_2:

$$\mathrm{Col}_1(x) = x_2 - \varphi(x_1) + \delta z x_1, \tag{7.14}$$

$$\mathrm{Col}_2(x) = -q^{k-1} x_1 - \varphi(x_2). \tag{7.15}$$

7.3.1 Surjectivity

Image of Col_1

We first give a few preliminary lemmas.

Lemma 7.3.2. *If $n \geq 0$, then $\varphi^n(M^{-1})(A_\varphi^T)^n = \varphi^{n-1}(P^T)\cdots\varphi(P^T)P^TM^{-1}$. Moreover, as $n \to \infty$, the quantity above tends to 0.*

Proof. The equality follows from (7.2) and induction. For the limit, note that $M|_{\pi=0} = I$, hence $\varphi^n(M) \to I$ as $n \to \infty$. Since the eigenvalues of A_φ are α and β and α^n, $\beta^n \to 0$ as $n \to \infty$, we are done. □

Lemma 7.3.3. *Let $x = \pi^{1-k}\begin{pmatrix} x_1 & x_2 \end{pmatrix}\begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \otimes e_{k-1}$. Then, $\psi(x)$ is given by*

$$\begin{pmatrix} \psi(x_1\delta z + x_2) & -\psi(q^{k-1}x_1) \end{pmatrix} \pi^{1-k}\begin{pmatrix} n_1 \\ n_2 \end{pmatrix}$$

Proof. Recall that $\varphi(\pi) = \pi q$, we have

$$\begin{aligned} x &= \pi^{1-k}\begin{pmatrix} x_1 & x_2 \end{pmatrix}(P^T)^{-1}\begin{pmatrix} \varphi(n_1) \\ \varphi(n_2) \end{pmatrix} \\ &= \begin{pmatrix} x_1\delta z + x_2 & -q^{k-1}x_1 \end{pmatrix}\varphi(\pi)^{1-k}\begin{pmatrix} \varphi(n_1) \\ \varphi(n_2) \end{pmatrix}, \end{aligned}$$

hence the result □

Lemma 7.3.4. *For all $n \geq 1$, the constant term of $\psi(q^n)$ is p^{n-1}.*

Proof. Induction. □

Lemma 7.3.5. *If $g(\pi) \in E \otimes \mathbb{B}^+_{\mathbb{Q}_p}$, then there exist unique $a_i \in E$ for $1 \leq i \leq k-1$ such that $g(\pi) = \sum_{i=1}^{k-1} a_i(\pi+1)^i \mod \pi^{k-1}$.*

Proof. Proved by S. Zerbes (see [LLZ10, Lemma 4.5]). □

Proposition 7.3.6. *Under assumption (C), we have $\left(\pi^{k-1}\mathcal{O}_E \otimes \mathbb{A}^+_{\mathbb{Q}_p}\right)^{\psi=0} \subset \mathrm{Col}_1\left(D(T_{\bar{f}}(k-1))^{\psi=1}\right)$.*

Proof. Recall that (7.4) says

$$(1-\varphi)x = \begin{pmatrix} \mathrm{Col}_1(x) & \mathrm{Col}_2(x) \end{pmatrix} \cdot (\pi q)^{1-k}P^T\begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \otimes e_{k-1}.$$

For any $y_1 \in \left(\pi^{k-1}\mathcal{O}_E \otimes \mathbb{A}^+_{\mathbb{Q}_p}\right)^{\psi=0}$, Theorem 7.3.1 implies that

$$y := \begin{pmatrix} y_1 & 0 \end{pmatrix} \cdot (\pi q)^{1-k}P^T\begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \otimes e_{k-1} = \begin{pmatrix} 0 & y_1/\pi^{k-1} \end{pmatrix}\begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \otimes e_{k-1}.$$

If n is a non-negative integer, we have

$$\begin{aligned}\varphi^n(y) &= \begin{pmatrix}0 & \varphi^n(y_1/\pi^{k-1})\end{pmatrix}\varphi^{n-1}(P^T)\cdots\varphi(P^T)P^T\begin{pmatrix}n_1\\n_2\end{pmatrix}\otimes e_{k-1}\\ &= \begin{pmatrix}0 & \varphi^n(y_1/\pi^{k-1})\end{pmatrix}\varphi^n(M^{-1})(A_\varphi^T)^n M\begin{pmatrix}n_1\\n_2\end{pmatrix}\otimes e_{k-1}.\end{aligned}$$

Hence, Lemma 7.3.2 implies that $\varphi^n(y)\to 0$ as $n\to\infty$ and the series $x := \sum_{n\geq 0}\varphi^n(y)$ converges to an element of $D(T_{\bar f}(k-1))^{\psi=1}$ with $(1-\varphi)x = y$. Therefore, $y_1 = \mathrm{Col}_1(x)$. □

Proposition 7.3.7. *Under assumptions (B), (C) and (D), the map* $\mathrm{Col}_1 : D(V_{\bar f}(k-1)) \to \left(E\otimes\mathbb{B}^+_{\mathbb{Q}_p}\right)^{\psi=0}$ *is surjective.*

Proof. By Proposition 7.3.6, if $y_1 \in \left(\pi^{k-1}E\otimes\mathbb{B}^+_{\mathbb{Q}_p}\right)^{\psi=0}$, then $y_1\in\mathrm{Im}(\mathrm{Col}_1)$. For an arbitrary $y_1\in\left(E\otimes\mathbb{B}^+_{\mathbb{Q}_p}\right)^{\psi=0}$, there exists y' in the E-linear span of $\{(1+\pi)^i\}_{1\leq i<k}$ such that $y_1+\varphi(y')$ is divisible by π^{k-1} by Lemma 7.3.5. Then, as in the proof of Proposition 7.3.6,

$$\sum_{n\geq 0}\varphi^n\left(\begin{pmatrix}0 & (y_1+\varphi(y'))/\pi^{k-1}\end{pmatrix}\begin{pmatrix}n_1\\n_2\end{pmatrix}\right)$$

converges to an element $x\in\mathbb{N}(V_{\bar f}(k-1))$. By Lemma 7.3.3 and the fact that $\psi(y_1)=0$, we have

$$\begin{aligned}\psi(x)-x &= \psi\left(\begin{pmatrix}0 & (y_1+\varphi(y'))/\pi^{k-1}\end{pmatrix}\begin{pmatrix}n_1\\n_2\end{pmatrix}\right)\\ &= \pi^{1-k}\begin{pmatrix}y' & 0\end{pmatrix}\begin{pmatrix}n_1\\n_2\end{pmatrix}\end{aligned}$$

Let $x' = x+\pi^{1-k}\begin{pmatrix}x_1 & x_2\end{pmatrix}\begin{pmatrix}n_1\\n_2\end{pmatrix}$ where $x_i\in E\otimes\mathbb{B}^+_{\mathbb{Q}_p}$. Then

$$\psi(x')-x' = \pi^{1-k}\begin{pmatrix}y'-x_1+\psi(x_1\delta z+x_2) & -x_2-\psi(q^{k-1}x_1)\end{pmatrix}\begin{pmatrix}n_1\\n_2\end{pmatrix}.$$

Hence, $x'\in D(V_{\bar f}(k-1))^{\psi=1}$ iff

$$x_2 = -\psi(q^{k-1}x_1), \tag{7.16}$$

$$y' = x_1-\psi(x_1\delta z)+\psi^2(q^{k-1}x_1). \tag{7.17}$$

Let $x_1 = \sum_{i=1}^{k-1}\beta_i(1+\pi)^i$ with $\beta_i\in E$. Since the degrees of δz and q^{k-1} are at most $k-2$ and $(p-1)(k-1)$ respectively, the degrees of $\psi(x_1\delta z)$ and $\psi^2(q^{k-1}x_1)$ are at most $(k-2+k-1)/p$ and $((p-1)(k-1)+k-1)/p^2$ respectively. But we assume that $p \geq k-1$, so both $\psi(x_1\delta z)$ and $\psi^2(q^{k-1}x_1)$ are scalar multiples of $(1+\pi)$. Write

$$y' = \sum_{i=1}^{k-1} \alpha_i(1+\pi)^i \qquad \text{and} \qquad \delta z = \sum_{i=0}^{k-2} \gamma_i(1+\pi)^i$$

where α_i, $\gamma_i \in E$. Then, (7.17) holds iff

$$\begin{aligned} \alpha_i &= \beta_i \qquad \text{for } i \geq 2 \\ \alpha_1 &= \beta_1 - \sum_{i+j=p} \beta_i\gamma_j + \beta_{p^2-(k-1)(p-1)} \end{aligned}$$

where $\gamma_i = \beta_i = 0$ if $i < 0$. But $p^2 - (k-1)(p-1) > 1$ and $p|\gamma_{p-1}$ by definition, so the matrix relating $(\alpha_i)_{1\leq i\leq k-1}$ and $(\beta_i)_{1\leq i\leq k-1}$ is upper triangular with nonzero entries on the diagonal. Therefore, there is a bijection between $(\alpha_i)_{1\leq i\leq k-1} \in E^{k-1}$ and $(\beta_i)_{1\leq i\leq k-1} \in E^{k-1}$. In other words, given any y' as above, there exists a unique x_1 (and hence x_2) such that $x' \in D(V_{\bar{f}}(k-1))^{\psi=1}$. For any $0 \leq j \leq k-2$, we can therefore choose y_1 (and hence y') such that $x_1 \equiv \pi^j \mod \pi^{j+1}$. In this case,

$$\begin{aligned} \mathrm{Col}_1(x') &= y_1 + \varphi(y') - \psi(q^{k-1}x_1) - \varphi(x_1) + x_1\delta z \\ &\equiv -\psi(q^{k-1}x_1) - \varphi(x_1) + x_1\delta z \mod \pi^{k-1} \\ &\equiv (-p^{k-2-j} - p^j + a_p)\pi^j \mod \pi^{j+1}, \end{aligned}$$

where we deduce the last line from the previous one using Lemma 7.3.4 and the fact that $\pi q = \varphi(\pi)$. Therefore, we are done by assumption (B). □

Image of $\underline{\mathrm{Col}}_1$

By Theorem 7.1.1, there is a natural isomorphism of Λ_E-modules

$$\mathfrak{J} : (\varphi^*\mathbb{N}(V_{\bar{f}}(k-1)))^{\psi=0} \to \Lambda_E^{\oplus 2}$$

In particular, $\mathfrak{J}$ is additive and linear over E. We write $n_i' = \varphi(n_i \otimes \pi^{1-k}e_{k-1})$ for $i \in \{1,2\}$.

Proposition 7.3.8. *Let $y \in (\varphi^*\mathbb{N}(T_{\bar{f}}(k-1)))^{\psi=0}$ be of the form $y = y_2n_2'$ for some $y_2 \in \left(\mathcal{O}_E \otimes \mathbb{A}^+_{\mathbb{Q}_p}\right)^{\psi=0}$, then there exists $z \in \Lambda_{\mathcal{O}_E}$ and $\tilde{x} \in \mathbb{N}(T_{\bar{f}}(k-1))^{\psi=1}$ such that*

$$\mathfrak{J}(y) - \mathfrak{J} \circ \mathbf{Col}(\tilde{x}) = (0, z).$$

Proof. Proved by S. Zerbes, see [LLZ10, Corollary 4.31]. □

Theorem 7.3.9. *If assumptions (B), (C) and (D) hold, then the map* $\underline{\mathrm{Col}}_1 : D(V_{\bar{f}}(k-1))^{\psi=1} \to \Lambda_E$ *is surjective.*

Proof. By Proposition 7.3.7, there exists $x \in D(T_{\bar{f}}(k-1))^{\psi=1}$ such that

$$\mathbf{Col}(x) = \varpi^m(1+\pi)n_1' + y_2 n_2'$$

for some $y_2 \in \left(\mathcal{O}_E \otimes \mathbb{A}_{\mathbb{Q}_p}^+\right)^{\psi=0}$ and an integer m. Proposition 7.3.8 says that there exist $z \in \Lambda_{\mathcal{O}_E}(G)$ and $\tilde{x} \in D(T_{\bar{f}}(k-1))^{\psi=1}$ such that

$$\mathfrak{J}(y_2 n_2') - \mathfrak{J} \circ \mathbf{Col}(\tilde{x}) = (0, z).$$

But $\mathfrak{J}(\varpi^m(1+\pi)n_1') = (\varpi^m, 0)$, hence $\mathfrak{J} \circ \mathrm{Col}(x) - \mathfrak{J} \circ \mathrm{Col}(\tilde{x}) = (\varpi^m, z)$ and $\underline{\mathrm{Col}}_1(x - \tilde{x}) = \varpi^m$. In particular, 1 is in the image and we are done. □

7.4 Compatibility of Coleman maps

We now show the compatibility of the definitions of the Coleman maps defined in Chapter 2 and the ones from Section 7.2. We first state a result of D. Loeffler:

Theorem 7.4.1. *If $F \in \mathcal{H}_\infty(G_\infty)$ and $n \geq 2$, then the following are equivalent:*

(1) $\mathfrak{M}(F)$ is divisible by $\Phi_n(1+\pi) = \varphi^{n-1}(q)$.

(2) F is zero at all primitive Dirichlet character modulo p^n.

(3) F is divisible by $\Phi_{n-1}(\gamma)$.

For $n = 1$, the same holds with (2) replaced by

(2') F is zero at all Dirichlet character modulo p.

Proof. Proved by D. Loeffler, see [LLZ10, Theorem 5.4]. □

7.4.1 The case $a_p = 0$

When $a_p = 0$, we can work out the matrix M' defined in Proposition 7.2.2 explicitly.

Lemma 7.4.2. *The matrix M' is given by*

$$\begin{pmatrix} 0 & (\log^+(1+\pi))^{k-1} \\ -(\log^-(1+\pi)/q)^{k-1} & 0 \end{pmatrix}.$$

Proof. With respect to the basis n_1, n_2 of $\mathbb{N}(V_{\bar{f}})$ over $\mathbb{B}^+_{\mathbb{Q}_p}$, as chosen in [BLZ04], the matrices of φ and $g \in G_\infty$ are given by

$$P = \begin{pmatrix} 0 & -1 \\ q^{k-1} & 0 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} \left(\frac{\log^+(1+\pi)}{g(\log^+(1+\pi))}\right)^{k-1} & 0 \\ 0 & \left(\frac{\log^-(1+\pi)}{g(\log^-(1+\pi))}\right)^{k-1} \end{pmatrix}, \tag{7.18}$$

which implies that

$$M = \begin{pmatrix} (\log^+(1+\pi))^{k-1} & 0 \\ 0 & (\log^-(1+\pi))^{k-1} \end{pmatrix}. \tag{7.19}$$

The result then follows from explicit calculations. □

Lemma 7.4.3. *We have* $\varphi(\log^-(1+\pi)) = \log^+(1+\pi)$ *and* $\varphi(\log^+(1+\pi)) = \frac{p}{q}\log^-(1+\pi)$.

Proof. Immediate. □

Lemma 7.4.4. *Let* $F \in \mathcal{H}_\infty(G_\infty)$*. Then* F *is divisible by* $\log^\pm_{p,k}$ *if and only if* $\mathfrak{M}(F)$ *is divisible by* $\varphi\left(\log^\pm(1+\pi)\right)^{k-1}$.

Proof. Let $m \geq 1$. Since the action of Tw_j on $\mathcal{H}_\infty(G_\infty)$ corresponds to that of ∂^j on $\mathbb{C}_p \otimes \mathbb{B}^{+,\psi=0}_{\mathrm{rig},\mathbb{Q}_p}$ for any j, we have $\Phi_m(u^{-j}\gamma)|F$ iff $\varphi^m(q)|\partial^j(\mathfrak{M}(F))$ by Theorem 7.4.1. But $\varphi^m(q)$ and $\partial(\varphi^m(q))$ are coprime. Hence, by induction on k, we conclude that

$$\prod_{j=0}^{k-2} \Phi_m(u^{-j}\gamma)\Big|F \qquad \text{iff} \qquad (\varphi^m(q))^{k-1}\Big|\mathfrak{M}(F).$$

□

Proposition 7.4.5. *There exists* $a^\pm \in \Lambda_E^\times$ *such that*

$$\underline{M} = \begin{pmatrix} 0 & -a^- \log^-_{p,k} \\ a^+ \log^+_{p,k} & 0 \end{pmatrix}.$$

Proof. As a Λ_E-module, $X^\pm := \varphi(\log^\pm(1+\pi))^{k-1}E \otimes \mathbb{B}^{+,\psi=0}_{\mathbb{Q}_p}$ is generated by $(1+\pi)\varphi(\log^\pm(1+\pi))^{k-1}$. By Lemma 7.4.4 and the fact that $\mathfrak{M}$ preserves orders, $\mathfrak{M}(\log^\pm_{p,k}\Lambda_E) = X^\pm$. Hence the result. □

Recall that the $\pm$-Coleman maps are defined by

$$\log^+_{p,k}\mathrm{Col}^+ = \mathcal{L}_{\nu_1} \quad \text{and} \quad \log^-_{p,k}\mathrm{Col}^- = \mathcal{L}_{\nu_2}.$$

Therefore, by (7.11), we have:

Corollary 7.4.6. *Let $a^{\pm}$ be as in Proposition 7.4.5, then $a^{-}\,\underline{\mathrm{Col}}_1 = \mathrm{Col}^-$ and $a^{+}\,\underline{\mathrm{Col}}_2 = \mathrm{Col}^+$.*

Description of kernels

By the calculations above, we see that Col_1 is related to Col^- by the following:

$$\log^-_{p,k}\mathrm{Col}^- = \mathfrak{M}(\varphi(\log^-(1+\pi))^{k-1}\,\mathrm{Col}_1\circ h^1_{\mathrm{Iw}})$$

In particular, we have $\ker(\mathrm{Col}_1) = h^1_{\mathrm{Iw}}(\ker(\mathrm{Col}^-))$ and a similar statement can be made about Col^+ and Col_2. We now find $\ker(\mathrm{Col}_i)$ for $i = 1, 2$ using (7.14) and (7.15) and show that they do agree with $\ker(\mathrm{Col}^{\pm})$ as described in Chapter 3.

By (7.3) and the formula for M above, we have for any $x \in D(V_{\bar{f}}(k-1))^{\psi=1}$, $x = x_1\bar{\nu}_{1,k-1} + x_2\bar{\nu}_{2,k-1}$ where

$$x_1 = x_1'(\log^-(1+\pi))^{k-1} \quad \text{and} \quad x_2 = x_2'(\log^+(1+\pi))^{k-1}$$

for some $x_1', x_2' \in E\otimes\mathbb{B}^+_{\mathbb{Q}_p}$. We write f_i for the power series such that $f_i(\pi) = x_i$, $i = 1, 2$.

Lemma 7.4.7. *Let x be as above. Then $p^{k-2}f_1(0) + f_2(0) = 0$.*

Proof. By [Ber03, Theorem II.6], we have

$$\exp^*_{0,1}\left(h^1_{\mathbb{Q}_p,V}(x)\right) = (1-p^{-1}\varphi^{-1})\partial_V(x) \tag{7.20}$$

where $V = V_{\bar{f}}(k-1)$. Since $\partial_V(x) = f_1(0)\bar{\nu}_{1,k-1} + f_2(0)\bar{\nu}_{2,k-1}$, we have

$$\left(1-p^{-1}\varphi^{-1}\right)\partial_V(x) = \left(f_1(0) - p^{-1}f_2(0)\right)\nu_{1,k-1} + \left(p^{k-2}f_1(0) + f_2(0)\right)\nu_{2,k-1}.$$

The image of $\exp^*_{0,1}$ is contained in $\mathbb{D}^0(V_{\bar{f}}(k-1))$, so $p^{k-2}f_1(0) + f_2(0) = 0$. □

Lemma 7.4.8. *Let $x \in D(V_{\bar{f}}(k-1))^{\psi=1}$, and write $x = x_1\bar{\nu}_{1,k-1} + x_2\bar{\nu}_{2,k-1}$ as above. Then*

(i) $x \in \ker(\mathrm{Col}_1)$ if and only if $\varphi(x_1) = -p^{k-1}\psi(x_1)$;

(ii) $x \in \ker(\mathrm{Col}_2)$ if and only if $\varphi(x_2) = -p^{k-1}\psi(x_2)$.

Proof. We only prove this for Col_1, as the proof for Col_2 is analogous. Note that the condition that $\psi(x) = x$ translates to $\psi(x_1) = -p^{1-k}x_2$ and $\psi(x_2) = x_1$. But $\mathrm{Col}_1(x) = x_2' - \varphi(x_1') = 0$ iff $x_2 = \varphi(x_1)$. Hence the result. □

Proposition 7.4.9. *Let x be as above, then*

(i) $x \in \ker(\mathrm{Col}_1)$ *if and only if the following equations hold*

$$\begin{aligned} \mathrm{Tr}_{n/n-1}(f_1(\zeta_{p^n}-1)) &= -p^{2-k}f_1(\zeta_{p^{n-2}}-1),\ n\geq 2 && (7.21)\\ \mathrm{Tr}_{1/0}(f_1(\zeta_p-1)) &= -(1+p^{2-k})f_1(0); && (7.22)\end{aligned}$$

(ii) $x \in \ker(\mathrm{Col}_2)$ *if and only if*

$$\begin{aligned} \mathrm{Tr}_{n/n-1}(f_2(\zeta_{p^n}-1)) &= -p^{2-k}f_2(\zeta_{p^{n-2}}-1),\ n\geq 2\\ \mathrm{Tr}_{1/0}(f_2(\zeta_p-1)) &= -(1+p^{k-2})f_2(0).\end{aligned}$$

Proof. We prove the proposition for Col_1. Recall that

$$\varphi\psi(x_1) = p^{-1}\sum_{\zeta^p=1} f_1\big(\zeta(1+\pi)-1\big).$$

Hence, $\varphi(x_1) = -p^{k-1}\psi(x_1)$ implies that

$$\sum_{\zeta^p=1} f_1\big(\zeta(1+\pi)-1\big) = -p^{2-k}\varphi^2\big(f_1(\pi)\big). \tag{7.23}$$

Let $n \geq 2$. On substituting π by $\zeta_{p^n}-1$ in (7.23), we have

$$\mathrm{Tr}_{n/n-1}(f_1(\zeta_{p^n}-1)) = \sum_{\zeta^p=1} f_1(\zeta\zeta_{p^n}-1) = -p^{2-k}f_1(\zeta_{p^{n-2}}-1).$$

Similarly, we obtain the second condition by substituting π by 0 in (7.23).

Conversely, assume that (7.21) holds for all $n\geq 2$, then $\varphi(f_1)+p^{k-1}\psi(f_1) = 0$ at $\zeta_{p^n}-1$. Recall that $x_1 = x_1'(\log^-(1+\pi))^{k-1}$ where $x_1' \in E\otimes\mathbb{B}^+_{\mathbb{Q}_p}$. Since

$$\varphi(x_1)+p^{k-1}\psi(x_1) = (\varphi(x_1')+\psi(q^{k-1}x_1'))(\log^+(1+\pi))^{k-1},$$

the power series in $\mathbb{Q}\otimes\mathbb{Z}_p[[X]]$ corresponding to $(\varphi(x_1')+\psi(q^{k-1}x_1'))$ has infinitely many zeros, so it must be zero itself and we are done. □

Corollary 7.4.10. *For $x \in D(V_{\bar f}(k-1))^{\psi=1}$, write $e_n(x)$ for the image of the nth component of $h^1_{\mathrm{Iw}}(x)$ under the dual exponential $\exp^*_{n,1}$. Let $i=1$ (respectively $i=2$), then $x\in\ker(\mathrm{Col}_i)$ iff*

$$e_0(x) = 0 \text{ and } e_{n+1}(x) = p^{-1}e_n(x)\ \forall n \in S^{\mp}_\infty$$

where $S^{\pm}_\infty$ are as defined in Chapter 3.

Proof. Again, we only prove this for $i = 1$. By [CC99, Théorème IV.2.1], we have $e_n(x) = p^{-n}\partial_V(\varphi^{-n}(x))$ for all $n \geq 1$. But φ^{-2} is the multiplication by $-p^{k-1}$ on $\mathbb{D}(V_{\bar{f}}(k-1))$. Using again that $\mathrm{Im}(\exp^*_{n,1}) \subset \mathbb{D}^0(V)$, we see that

$$\begin{aligned} e_{2n}(x) &= p^{-2n} \cdot (-p)^{n(k-1)} f_1(\zeta_{p^{2n}} - 1)\bar{\nu}_{1,k-1} \\ e_{2n+1}(x) &= p^{-2n-1} \cdot (-p)^{n(k-1)} f_2(\zeta_{p^{2n+1}} - 1)\bar{\nu}_{1,k-1} \end{aligned}$$

and $f_2(\zeta_{p^{2n}} - 1) = f_1(\zeta_{p^{2n-1}} - 1) = 0$ for all $n \geq 1$. Therefore, (7.21) holds for any $2n-1$ and it holds for $2n$ if and only if $e_{2n}(x) = \mathrm{Tr}_{2n+1/2n}(e_{2n+1}(x)) = p^{-1}e_{2n-1}(x)$.

Now $e_0(x) = (f_1(0) - p^{-1}f_2(0))\bar{\nu}_{1,k-1}$ by (7.20) and $p^{k-2}f_1(0) + f_2(0) = 0$ by Lemma 7.4.7, so

$$e_0(x) = (1 + p^{k-3})f_1(0)\bar{\nu}_{1,k-1} = -(p^{2-k} + p^{-1})f_2(0)\bar{\nu}_{1,k-1}.$$

The condition (7.22) is therefore equivalent to $f_1(0) = 0$, which in turns is equivalent to $e_0(x) = 0$. $\square$

Therefore, the two descriptions of the kernels (Corollaries 3.4.1 and 7.4.10) agree via the isomorphism h^1_{Iw}.

7.4.2 The case $k = 2$

We now assume that f is a modular form as in Section 2.5. Since condition (C) holds and $k = 2$, with respect to the canonical basis of $\mathbb{N}(V_f)$ given above, P is simply

$$\begin{pmatrix} 0 & -1 \\ q & a_p \end{pmatrix}. \tag{7.24}$$

Write B^i_∞ (respectively B^i_n) for the matrix obtained from A^i_∞ (respectively A^i_n) by replacing $\Phi_m(\gamma)$ by $\varphi^{m-1}(q)$ for all m. Then, we have:

Lemma 7.4.11. *Under the notation of Section 7.2, $M = B^0_\infty$.*

Proof. By (7.24), $(B^{-n}_n)^T = P\varphi(P)\cdots\varphi^{n-1}(P)A^{-n}_\varphi$. For $g \in G_\infty$, we write $G^{(n)}_g = (B^{-n}_n)^T \cdot g\left((B^{-n}_n)^T\right)^{-1}$. Then,

$$P \cdot \varphi\left(G^{(n)}_g\right) \cdot g(P)^{-1} = G^{(n+1)}_g.$$

Hence, if we write G_g for the limit of $G^{(n)}_g$ as $n \to \infty$, then

$$P \cdot \varphi\left(G_g\right) \cdot g(P)^{-1} = G_g,$$

It is easy to check that G_g satisfies $G_{g_1g_2} = G_{g_1} \cdot g_1(G_{g_2})$ for any $g_1, g_2 \in G_\infty$. Hence, we recover the action of G_∞ on the Wach module $\mathbb{N}(V_f)$. In other words, G_g is the matrix of g with respect to the basis n_1, n_2 chosen in Section 7.3. Since $G_g = (B^0_\infty)^T \cdot g\left((B^0_\infty)^T\right)^{-1}$ and $G_g|_{\pi=0} = I$, we have

$$B^0_\infty \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \left((E \otimes \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}) \otimes \mathbb{N}(V_f)\right)^{G_\infty} = \mathbb{D}(V_f)$$

and $M = B^0_\infty$. □

We write $A^c = \det(A)A^{-1}$ if A is an invertible matrix, then we have:

Corollary 7.4.12. *The matrix M' can be obtained from $(A_\infty^{-1})^c$ by replacing Φ_m by $\varphi(q)^m$.*

Proof. Explicit calculation. □

Recall that (2.15) says that

$$\begin{pmatrix} \mathcal{L}_{\varphi(\omega)}(\mathbf{z}) & -\mathcal{L}_\omega(\mathbf{z}) \end{pmatrix} A_\infty^{-1} = \begin{pmatrix} \mathrm{Col}^\vartheta(\mathbf{z}) & \mathrm{Col}^\upsilon(\mathbf{z}) \end{pmatrix} \log(\gamma)/(\gamma - 1)$$

for any $\mathbf{z} \in \mathbb{H}^1_{\mathrm{Iw}}(V_{\bar{f}}(1))$. Hence, on setting $\nu_1 = -\omega$, (7.11) implies that

$$\begin{pmatrix} \underline{\mathrm{Col}}_1 & \underline{\mathrm{Col}}_2 \end{pmatrix} \underline{M} A_\infty^{-1} = \begin{pmatrix} \mathrm{Col}^\vartheta \circ h^1_{\mathrm{Iw}} & \mathrm{Col}^\upsilon \circ h^1_{\mathrm{Iw}} \end{pmatrix} \log_p(\gamma)/(\gamma - 1). \tag{7.25}$$

By considering the determinant of $\Omega_{V_f(1),1}$ (see the proof of Lemma 4.4.2), we see that the images of

$$\begin{pmatrix} \underline{\mathrm{Col}}_1 & \underline{\mathrm{Col}}_2 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \mathrm{Col}^\vartheta & \mathrm{Col}^\upsilon \end{pmatrix}$$

are isomorphic as Λ_E-modules, so (7.25) implies that there exists $A \in GL_2(\Lambda_E)$ such that $\underline{M} A_\infty^{-1} = [\log_p(\gamma)/(\gamma - 1)]A$. Hence,

$$\begin{pmatrix} \underline{\mathrm{Col}}_1 & \underline{\mathrm{Col}}_2 \end{pmatrix} A = \begin{pmatrix} \mathrm{Col}^\vartheta \circ h^1_{\mathrm{Iw}} & \mathrm{Col}^\upsilon \circ h^1_{\mathrm{Iw}} \end{pmatrix}.$$

We also see that $\underline{M}$ and $(A_\infty^{-1})^c$ agree up to an element in $GL_2(\Lambda_E)$ which is a generalisation of Proposition 7.4.5 because of the description of M' in Corollary 7.4.12.

7.5 p-ordinary modular forms

We now assume that f is ordinary at p. Then, $V_{\bar{f}}$ has no quotient isomorphic to $E(-k+1)$, so results from Section 7.1 hold.

As before, we assume $\epsilon(p) = 1$. Let α be the root of $X^2 - a_pX + p^{k-1}$ which is a p-adic unit and let β be the one with p-adic valuation $k-1$. By [Kat04, Section 17], there exists an 1-dimensional $G_{\mathbb{Q}_p}$-subrepresentation $V'_{\bar{f}}$ in $V_{\bar{f}}$. Moreover, $V'_{\bar{f}}$ has Hodge-Tate weight 0 and $\mathbb{D}(V'_{\bar{f}})$ can be identified with the α-eigenspace of φ in $\mathbb{D}(V_{\bar{f}})$. We fix a nonzero element $\bar{\nu}_1 \in \mathbb{D}(V'_{\bar{f}})$. Then, $\bar{\nu}_1$ is a basis of $\mathbb{N}(V_{\bar{f}})$ over $E \otimes \mathbb{B}^+_{\mathbb{Q}_p}$. Let $\bar{\nu}_2$ be a nonzero β-eigenvector of φ in $\mathbb{D}(V_{\bar{f}})$. We lift $\bar{\nu}_1, \bar{\nu}_2$ to a basis $n_1 = \bar{\nu}_1, n_2$ of $\mathbb{N}(V_{\bar{f}})$, which defines a lattice $T_{\bar{f}}$ in $V_{\bar{f}}$ as in the supersingular case. Then, the change of basis matrix M, with

$$\begin{pmatrix} \bar{\nu}_1 \\ \bar{\nu}_2 \end{pmatrix} = M \begin{pmatrix} n_1 \\ n_2 \end{pmatrix},$$

is lower triangular. By considering determinant, we can choose n_2 so that the diagonal entries of M are 1 and $(t/\pi)^{k-1}$. With respect to this basis, the associated Coleman maps Col_i and $\underline{\mathrm{Col}}_i$, $i \in \{1,2\}$ given in Section 7.1 enable us to define:

Definition 7.5.1. *For $i = 1, 2$, define $L_{p,i} = \mathrm{Col}_i(\mathbf{z}) \in (E \otimes \mathbb{B}^+_{\mathbb{Q}_p})^{\psi=0}$ and $\tilde{L}_{p,i} = \underline{\mathrm{Col}}_i(\mathbf{z}) \in \Lambda_E$ as in Definition 7.2.1.*

Since $\varphi(n_1) = \alpha n_1$, the matrix P as defined in Section 7.1 is upper triangular and there exists a unit u in $E \otimes \mathbb{B}^+_{\mathbb{Q}_p}$ such that

$$P = \begin{pmatrix} \alpha & * \\ 0 & uq^{k-1} \end{pmatrix}.$$

Therefore, (7.6) becomes

$$(1-\varphi)(x) = \begin{pmatrix} \mathrm{Col}_1(x) & \mathrm{Col}_2(x) \end{pmatrix} \begin{pmatrix} \alpha(\frac{t}{\pi q})^{k-1} & 0 \\ * & u \end{pmatrix} \begin{pmatrix} \bar{\nu}_{1,k-1} \\ \bar{\nu}_{2,k-1} \end{pmatrix}. \tag{7.26}$$

Lemma 7.5.2. *Let ν_1, ν_2 be a basis of $\mathbb{D}(V_f)$ such that $\varphi(\nu_1) = \alpha\nu_1$ and $\varphi(\nu_2) = \beta\nu_2$. Then*

$$[\nu_{i,1}, \bar{\nu}_{i,k-1}] = 0$$

for $i = 1, 2$ where $[\ ,\ ]$ is the pairing as in (7.8).

Proof. Assume $m_1 := [\nu_{1,1}, \bar{\nu}_{1,k-1}] \neq 0$. Since $[\ ,\ ]$ is compatible with φ, we have

$$\begin{aligned}\varphi[\nu_{1,1}, \bar{\nu}_{1,k-1}] &= [\varphi(\nu_{1,1}), \varphi(\bar{\nu}_{1,k-1})]\\ p^{-1}m_1 &= [\alpha p^{-1}\nu_{1,1}, \alpha p^{1-k}\bar{\nu}_{1,k-1}]\\ p^{k-1}m_1 &= \alpha^2 m_1.\end{aligned}$$

Hence, $\alpha^2 = p^{k-1}$, which is a contradiction. The proof for $i = 2$ is similar. □

As in Section 7.2.2, we may assume that $[\nu_{1,1}, \bar{\nu}_{2,k-1}] = -[\nu_{2,1}, \bar{\nu}_{1,k-1}] = 1$ and an analogue of Proposition 7.2.2 says that

$$\mathfrak{M}\begin{pmatrix}-\mathcal{L}_{\nu_2}(h^1_{\mathrm{Iw}}(x)) & \mathcal{L}_{\nu_1}(h^1_{\mathrm{Iw}}(x))\end{pmatrix} = \begin{pmatrix}\mathrm{Col}_1(x) & \mathrm{Col}_2(x)\end{pmatrix}\begin{pmatrix}\alpha(\frac{t}{\pi q})^{k-1} & 0\\ * & u\end{pmatrix}.$$

In particular, if we apply this to the Kato zeta element, we have

$$\begin{pmatrix}-\mathfrak{M}(L_{p,\beta}) & \mathfrak{M}(L_{p,\alpha})\end{pmatrix} = \begin{pmatrix}L_{p,1} & L_{p,2}\end{pmatrix}\begin{pmatrix}\alpha(\frac{t}{\pi q})^{k-1} & 0\\ * & u\end{pmatrix}$$

where $L_{p,\beta} = \mathcal{L}_{\nu_2}(\mathbf{z}^{\mathrm{Kato}})$. On applying Theorem 7.4.1, we have

$$\begin{pmatrix}-L_{p,\beta} & L_{p,\alpha}\end{pmatrix} = \begin{pmatrix}\tilde{L}_{p,1} & \tilde{L}_{p,2}\end{pmatrix}\begin{pmatrix}\alpha\tilde{v}\log_{p,k} & 0\\ * & \tilde{u}\end{pmatrix}$$

where $\log_{p,k} = \prod_{j=0}^{k-2}\log_p(\chi(\gamma)^{-j}\gamma)/(\chi(\gamma)^{-j}\gamma - 1)$ and $\tilde{u}, \tilde{v} \in \Lambda_E^\times$.

We now say something about $L_{p,1}$ and $\tilde{L}_{p,1}$. When V_f is not locally split at p, $L_{p,\beta}$ is conjecturally equal to the critical slope p-adic L-function constructed in [PS09]. By [Kat04, Theorems 16.4 and 16.6], $L_{p,\beta}$ has the same interpolating properties as $L_{p,\alpha}$, namely:

$$\chi^r\theta(L_{p,\alpha}) = \frac{c_{\theta,r}}{\beta^n}L(f_{\theta^{-1}}, r+1) \qquad \text{and} \qquad \chi^r\theta(L_{p,\beta}) = \frac{c_{\theta,r}}{\beta^n}L(f_{\theta^{-1}}, r+1) \tag{7.27}$$

where θ is a finite character of conductor $p^n > 1$, $0 \leq r \leq k-2$ and $c_{\theta,r}$ is some constant independent of α and β. Note that the values given by (7.27) do not determine $L_{p,\beta}$ uniquely, but it allows us to show that $L_{p,1}, \tilde{L}_{p,1} \neq 0$.

- **Assumption (A'):** V_f is not locally split at p and $k \geq 3$.

Proposition 7.5.3. *If assumption (A') holds, then $L^\eta_{p,1}, \tilde{L}^\eta_{p,1} \neq 0$ for any character η of Δ.*

Proof. As in the proof of Proposition 7.2.3, the fact that $M|_{\pi=0} = I$ implies that $M'|_{\pi=(\zeta-1)} = A_\varphi^T$ for any $\zeta^p = 1$, where $A_\varphi = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$ is the matrix of φ with respect to $\bar{\nu}_1, \bar{\nu}_2$. Therefore, $\mathfrak{M}(L_{p,\beta})(\zeta-1) = \alpha L_{p,1}(\zeta-1)$. Since V_f is not locally split and $k \geq 3$, by the above discussion, $\eta(L_{p,\beta}) = \frac{\tau(\eta)}{\beta} L(f_{\eta^{-1}}, 1) \neq 0$ for any primitive character η modulo p as in the supersingular case. Therefore, $L_{p,1}^\eta(0) \neq 0$. The result for $\tilde{L}_{p,1}^\eta$ then follows immediately by Remark 7.2.6. □

In particular, we see that the interpolating properties of $\mathfrak{M}^{-1}(L_{p,1})$ and $\tilde{L}_{p,1}$ at characters modulo p are the same as that of $L_{p,\beta}$ after multiplying a constant.

Remark 7.5.4. *If V_f does split locally at p, we can choose $n_2 = \bar{\nu}_2$ and M would be diagonal. Then, we have*

$$L_{p,\beta} = \mathfrak{M}^{-1}\left((t/\pi)^{k-1} L_{p,1}\right) = \tilde{v} \log_{p,k} \tilde{L}_{p,1}.$$

But it is not known that whether $L_{p,\beta}$ is nonzero or not.

7.6 Main conjectures

For $i = 1, 2$, let $\ker(\underline{\mathrm{Col}}_i)_n$ be the image of $\ker(\underline{\mathrm{Col}}_i)$ in $H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))$ under the composition of h^1_{Iw} and the natural projection. We write $H^1_f(\mathbb{Q}_{p,n}, V_f/T_f(1))^i$ for the annihilator of $\ker(\underline{\mathrm{Col}}_i)_n$ under the pairing

$$H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1)) \times H^1(\mathbb{Q}_{p,n}, V_f/T_f(1)) \to E/\mathcal{O}_E.$$

This enables us to define

$$\mathrm{Sel}_p^i(f/\mathbb{Q}(\mu_{p^n})) = \ker\left(\mathrm{Sel}_p(f/\mathbb{Q}(\mu_{p^n})) \to \frac{H^1(\mathbb{Q}_{p,n}, V_f/T_f(1))}{H^1_f(\mathbb{Q}_{p,n}, V_f/T_f(1))^i}\right).$$

and $\mathrm{Sel}_p^i(f/\mathbb{Q}_\infty) = \varinjlim \mathrm{Sel}_p^i(f/\mathbb{Q}(\mu_{p^n}))$. The results in Chapter 5 generalise directly and (5.13) becomes

$$\mathbb{H}^1(T_{\bar{f}}(k-1)) \to \mathrm{Im}(\underline{\mathrm{Col}}_i) \to \mathrm{Sel}_p^i(f/\mathbb{Q}_\infty)^\vee \to \mathbb{H}^2(T_{\bar{f}}(k-1)) \to 0. \tag{7.28}$$

Proposition 7.6.1. *Under assumption (A) (if f is supersingular at p) or assumption (A') (if f is ordinary at p), $\mathrm{Sel}_p^i(f/\mathbb{Q}_\infty)$ is $\Lambda_{\mathcal{O}_E}$-cotorsion for $i = 1, 2$. Moreover, $\mathrm{Sel}_p^i(f/\mathbb{Q}_\infty)^\eta$ is $\Gamma_{\mathcal{O}_E}$-cotorsion and there exists some $n_i \geq 0$ such that*

$$\varpi^{n_i} \tilde{L}_{p,i}^\eta \in \mathrm{Char}_{\Gamma_{\mathcal{O}_E}}(\mathrm{Sel}_p^i(f/\mathbb{Q}_\infty)^{\vee,\eta})$$

where η is any character on Δ unless f is supersingular at p and $i = 2$ in which case η is the trivial character.

Proof. This is exactly the same as the corresponding results from Section 5.4. As in (5.14), the first arrow of (7.28) is now injective by the fact that $\tilde{L}^{\eta}_{p,i} \neq 0$ and there exist $n \in \mathbb{Z}$ such that

$$0 \to \mathbb{H}^1(T_{\bar{f}}(k-1))/\mathbb{Z}(T_{\bar{f}}(k-1)) \to \mathrm{Im}(\underline{\mathrm{Col}}_i)/(\varpi^{n_i}\tilde{L}_{p,i}) \to \mathrm{Sel}_p^i(f/\mathbb{Q}_\infty)^\vee \to \mathbb{H}^2(T_{\bar{f}}(k-1)) \to 0. \tag{7.29}$$

□

Corollary 7.6.2. *Let η be as above. If assumption (A) (or (A') depending on whether f is supersingular or ordinary at p) and the homomorphism $G_{\mathbb{Q}} \to GL_{\mathcal{O}_E}(T_{\bar{f}})$ is surjective, then Kato's main conjecture is equivalent to*

$$\mathrm{Char}_{\Gamma_{\mathcal{O}_E}}\left(\mathrm{Sel}_p^i(f/\mathbb{Q}_\infty)^{\vee,\eta}\right) = \mathrm{Char}_{\Gamma_{\mathcal{O}_E}}\left(\mathrm{Im}(\underline{\mathrm{Col}}_i)^\eta/(\varpi^{n_i}\tilde{L}^{\eta}_{p,i})\right). \tag{7.30}$$

Proof. It follows immediately from (7.29). □

By the surjectivity of $\underline{\mathrm{Col}}_1$, we have:

Corollary 7.6.3. *If assumptions (A)-(D) hold and η is as above, then Kato's main conjecture tensor $\mathbb{Q}$, i.e.*

$$\mathrm{Char}_{\Gamma_E}\left(\mathbb{H}^1(V_f)^\eta/\mathbb{Z}(V_f)^\eta\right) = \mathrm{Char}_{\Gamma_E}\left(\mathbb{H}^2(V_f)^\eta\right),$$

is equivalent to

$$\mathrm{Char}_{\Gamma_E}\left(\mathrm{Sel}_p^1(f/\mathbb{Q}_\infty)^{\vee,\eta}\otimes\mathbb{Q}\right) = \left(\tilde{L}^{\eta}_{p,1}\right) \tag{7.31}$$

As before, one inclusion is immediate for both (7.30) and (7.31).

Appendix A

Results in linear algebra

In this appendix, we prove some elementary results in linear algebra which we have used in the main part of the thesis. Some of them are needed in Appendix B as well.

A.1 Linear algebra over Lubin-Tate extensions

Lemma A.1.1. *Let K be a field of characteristic 0 and $K = K_0 \subset \cdots \subset K_n$ a tower of Galois extensions. Write $K^{(n)} = \ker(\mathrm{Tr}_{n/n-1})$ and $K^{(0)} = K$. Then, as K-vector spaces, we have*

$$K_n = K^{(0)} \oplus K^{(1)} \oplus \cdots \oplus K^{(n)}.$$

Proof. By induction, it is enough to show that $K_n = K_{n-1} \oplus K^{(n)}$. It is clear that $K_{n-1} \cap K^{(n)} = \{0\}$. If $x \in K_n$, $x = (x - r_n \mathrm{Tr}_{n/n-1}(x)) + r_n \mathrm{Tr}_{n/n-1}(x)$ where $r_n = [K_n : K_{n-1}]^{-1}$, so we are done. □

Take $K = \mathbb{Q}_p$. Let π be a uniformiser of $\mathbb{Q}_p$ such that $\pi \equiv p \mod p^2$ and $g_\pi = (1+X)^p + (\pi - p)X - 1$. This is called a good lift of Frobenius in [IP06]. Let K_n be the extension of $\mathbb{Q}_p$ generated by the π^n-torsion of the Lubin-Tate group associated to g_π with Galois group G_n. Let π_n be a primitive π^n-torsion and define

$$\pi_n' = \begin{cases} \pi_n - \frac{1}{p}\mathrm{Tr}_{n/n-1}(\pi_n) = \pi_n + 1 & \text{if } n > 1, \\ \pi_1 - \frac{1}{p-1}\mathrm{Tr}_{1/0}(\pi_1) = \pi_1 + \frac{p}{p-1} & \text{if } n = 1, \\ 1 & \text{if } n = 0. \end{cases}$$

It is then clear that $\pi_n' \in K^{(n)}$.

Lemma A.1.2. *Under the notation of Lemma A.1.1, $\{\pi_n'^\sigma : \sigma \in G_n\}$ generates $K^{(n)}$ over $\mathbb{Q}_p$.*

Proof. By [IP06, Proposition 4.4], we have

$$K_n = \mathbb{Q}_p[G_n]\pi_n + K_{n-1}.$$

Let $x \in K^{(n)}$. Since $\mathrm{Tr}_{n/n-1}\,\pi_n \in K_{n-1}$, we can write $x = \sum_{\sigma \in G_n} a_\sigma \pi_n'^\sigma + y$ for some $a_\sigma \in \mathbb{Q}_p$ and $y \in K_{n-1}$. But $\mathrm{Tr}_{n/n-1}\,x = \mathrm{Tr}_{n/n-1}\,\pi_n'^\sigma = 0$ for all σ, we have $y = 0$. Hence we are done. $\square$

Proposition A.1.3. *Let $n \geq 0$ be an integer and*

$$\alpha = \sum_{i=0}^{n} x_i \pi_i' \text{ for some } x_i \in \mathbb{Q}_p.$$

Then, the $\mathbb{Q}_p$-vector space generated by $\{\alpha^\sigma : \sigma \in G_n\}$ is given by

$$\bigoplus_{i : x_i \neq 0} K^{(i)}.$$

Proof. We proceed by induction on $|S|$. The case $|S| = 1$ follows directly from Lemma A.1.2

Write V for the $\mathbb{Q}_p$-vector space generated by $\{\alpha^\sigma : \sigma \in G_n\}$. Clearly,

$$V \subset \bigoplus_{i : x_i \neq 0} K^{(i)}.$$

Without loss of generality, we assume that $x_n \neq 0$. Let $\beta = \sum_{i=0}^{n-1} x_i \pi_i'$. Then, by induction, $\{\beta^\tau : \tau \in G_{n-1}\}$ generates $\bigoplus_{i \in S \setminus \{n\}} K^{(i)}$ over K. Fix $\tau \in G_{n-1}$, then

$$\sum_{\sigma \in G_n, \sigma|_{K_{n-1}} = \tau} \alpha^\sigma = p\beta^\tau + (\mathrm{Tr}_{n/n-1}\,\pi_n')^\tau = p\beta^\tau.$$

Therefore, for any $\tau \in G_{n-1}$, $\beta^\tau \in V$ and $\pi_n'^\sigma \in V$ for any $\sigma \in G_n$. Hence we are done. $\square$

A.2 Linear algebra of cyclotomic extensions

We now apply results above to the extension $\mathbb{Q}_{p,n}$ of $\mathbb{Q}_p$.

Corollary A.2.1. *Let* $\eta = a_0 + \sum_{i=1}^{n} a_i \zeta_{p^i}$ *where* $a_i \in \mathbb{Q}_p$ *with* $a_1 \neq (p-1)a_0$, *then the* $\mathbb{Q}_p$*-vector space generated by* $\{\eta^\sigma : \sigma \in G_n\}$ *is given by*

$$\mathbb{Q}_p + \sum_{r \in S} \sum_{\sigma \in G_n} \mathbb{Q}_p \cdot \zeta_{p^r}^{\sigma}.$$

where $S = \{r \in [1, n] : a_r \neq 0\}$.

Proof. Take $\pi = p$ and $\pi_n = \zeta_{p^n} - 1$. Then, $\pi'_n = \zeta_{p^n}$ for $n > 1$ and $\pi'_1 = \zeta_p + (p-1)^{-1}$. Therefore, the result is immediate if $a_1 = 0$ by Proposition A.1.3. If $a_1 \neq 0$, then

$$\eta = \left(a_0 - \frac{a_1}{p-1}\right) + a_1 \pi'_1 + \sum_{i>1} a_i \pi'_i.$$

Hence, we can again apply Proposition A.1.3. □

Corollary A.2.2. *Let* $\eta = 1 + \zeta_p + \zeta_{p^2} + \cdots + \zeta_{p^n}$, *then* η *is a normal basis of* $\mathbb{Q}_{p,n}$ *over* $\mathbb{Q}_p$.

Proof. Combine Lemma A.1.1 and Corollary A.2.1. □

Appendix B

Coleman maps over Lubin-Tate extensions

In this appendix, we explain how the construction of $\mathrm{Col}^{\pm}$ can be generalised to Lubin-Tate extensions of height 1 in place of the cyclotomic extension. This is the contents of [Lei09a].

B.1 Perrin-Riou's exponential map over Lubin-Tate extensions

We first review the generalisation of Perrin-Riou's exponential to Lubin-Tate extensions given in [Zha04b]. Fix π a uniformiser of $\mathbb{Z}_p$. Let α be the p-adic unit in $\mathbb{Z}_p^\times$ such that $\pi = \alpha p$. Let g be a lift of Frobenius with respect to π and denote the Lubin-Tate group associated to π (which is independent of g up to isomorphisms over $\mathbb{Z}_p$) by $\mathcal{F}$. We write $[\cdot]_{\mathcal{F}} : \mathbb{Z}_p \to \mathrm{End}(\mathcal{F})$ for the natural ring homomorphism associated to $\mathcal{F}$.

Let K_n denote the extension of $\mathbb{Q}_p$ obtained by adjoining the π^n-torsions of $\mathcal{F}$ and write G_n for the Galois group of K_n over $\mathbb{Q}_p$ for $0 \le n \le \infty$. In particular, $G_n \cong (\mathbb{Z}/p^n)^\times$ and $G_\infty \cong G_1 \times \mathrm{Gal}(K_\infty/K_1) \cong \mathbb{Z}/(p-1) \times \mathbb{Z}_p$. Note that G_n denotes something less general in the main part of the thesis, but since it should not cause confusions, we use the same notation here. We abuse notation in a similar manner for other objects in later parts of the appendix.

Let κ be the character of $G_{\mathbb{Q}_p}$ given by its action on the Tate module of $\mathcal{F}$. Then, $\sigma\omega = [\kappa(\sigma)]_{\mathcal{F}}(\omega)$ for all $\omega \in \mathcal{F}[\pi^\infty]$ and $\sigma \in G_{\mathbb{Q}_p}$. Moreover, $\kappa = \chi\psi$ for some unramified character ψ.

Let Ξ denote the completion of the maximal unramified extension of $\mathbb{Q}_p$ and $\mathcal{O}$ its ring of integers. Let $\eta : \mathbb{G}_m \to \mathcal{F}$ be an isomorphism between the multiplicative group and $\mathcal{F}$, then $\eta \in \mathcal{O}[[X]]$. Moreover,

$$\eta(X) = \Omega X + (\text{higher degree terms})$$

where Ω is a p-adic unit. The lift of Frobenius g satisfies $g \circ \eta = \eta^{\varphi} \circ ((1+X)^p - 1)$ where φ is the Frobenius of $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p)$, which acts on η by acting on its coefficients. In particular, $\Omega^{\varphi} = \alpha\Omega$.

Definition B.1.1. *We define $\Xi[[X]]^{\psi}$ to be the set of power series f over Ξ such that $\sigma f(X) = f((1+X)^{\psi(\sigma)} - 1) \forall \sigma \in G_{\mathbb{Q}_p}$.*

Remark B.1.2. *[Zha04b, (1.13)] says that $\Xi[[X]]^{\psi}$ contains η.*

The significance of $\Xi[[X]]^{\psi}$ is given by the following:

Lemma B.1.3. *Let $f \in \Xi[[X]]^{\psi}$ and ζ a p^nth root of unity. Then $f(\zeta - 1) \in K_n$.*

Proof. By definition, $\sigma f(X) = f((1+X)^{\psi(\sigma)} - 1)$ for any $\sigma \in G_{\mathbb{Q}_p}$. Therefore, we have

$$\begin{aligned} \sigma(f(\zeta - 1)) &= (\sigma f)(\zeta^{\sigma} - 1) \\ &= f(\zeta^{\chi(\sigma)\psi(\sigma)} - 1) \\ &= f(\zeta^{\kappa(\sigma)} - 1). \end{aligned}$$

If, in addition, $\sigma \in G_{K_n}$, then $\kappa(\sigma) \in 1 + p^n\mathbb{Z}_p$. Hence, $\sigma(f(\zeta - 1)) = f(\zeta - 1)$ for any $\sigma \in G_{K_n}$, so we are done. $\square$

Fix a crystalline representation V of $G_{\mathbb{Q}_p}$. We write $r(V)$ for the slope of φ on $\mathbb{D}(V)$. We again assume that the eigenvalues of φ on $\mathbb{D}(V)$ are not integral powers of p. On abusing notation, we write φ for the map $\varphi \otimes \varphi$ on $\Xi \otimes \mathbb{D}(V)$. For $k \in \mathbb{Z}$, we write $V(\kappa^k)$ for the representation of V twisted by κ^k. Then, $\mathbb{D}(V(\kappa^k)) = t_{\pi}^{-k}\mathbb{D}(V)$ where $t_{\pi} = \Omega t$ since $G_{\mathbb{Q}_p}$ acts on t_{π} via κ by [Zha04b, Section 2].

Lemma B.1.4. *The de Rham filtrations satisfy $\mathbb{D}^i(V(\kappa^j)) = t_{\pi}^{-j}\mathbb{D}^{i+j}(V)$.*

Proof. By definitions, we have

$$\begin{aligned}\mathbb{D}^i(V(\kappa^j)) &= (t_\pi^{-j}\mathbb{D}(V)) \cap t^i\mathbb{B}_{\mathrm{dR}}^+ \\ &= t_\pi^{-j}(\mathbb{D}(V) \cap t^{i+j}\Omega^j\mathbb{B}_{\mathrm{dR}}^+) \\ &= t_\pi^{-j}(\mathbb{D}(V) \cap t^{i+j}\mathbb{B}_{\mathrm{dR}}^+) \text{ (since } \Omega \text{ is a } p\text{-adic unit)} \\ &= t_\pi^{-j}\mathbb{D}^{i+j}(V).\end{aligned}$$

Hence we are done. □

Let B be a Banach p-adic space. For $r \in \mathbb{R}_{\geq 0}$, $\mathbb{D}_r(\mathbb{Q}_p, B)$ denotes the set of tempered B-valued distributions of order r (i.e. of order $O(\log_p^r)$) on the locally analytic functions with compact support in $\mathbb{Q}_p$. It is equipped with an action $\varphi_{\mathbb{D}}$, which is defined by $\int f\varphi_{\mathbb{D}}(\mu) = \int f(px)\mu$. Similarly, if A is a compact open subset of $\mathbb{Q}_p$, $\mathbb{D}_r(A, B)$ denotes the set of tempered distributions of order r on A with values in B.

We define $\mathbb{D}_r(\mathbb{Q}_p, \Xi\otimes\mathbb{D}(V))^\psi$ to be the subset of $\mathbb{D}_r(\mathbb{Q}_p, \Xi\otimes\mathbb{D}(V))$ consisting of all the distributions μ satisfying:

$$\sigma\left(\int_{\mathbb{Q}_p} f\mu\right) = \int_{\mathbb{Q}_p} f(\psi(\sigma)x)\mu \ \forall\sigma \in G_{\mathbb{Q}_p}.$$

Remark B.1.5. *Let $\mu \in \mathbb{D}_r(\mathbb{Z}_p, \Xi \otimes \mathbb{D}(V))$. Then, $\mu \in \mathbb{D}_r(\mathbb{Z}_p, \Xi \otimes \mathbb{D}(V))^\psi$ iff its Amice transform $\mathcal{A}_\mu(X) = \int_{\mathbb{Z}_p}(1+X)^x\mu$ is in $\Xi[[X]]^\psi \otimes \mathbb{D}(V)$ (see [Zha04b, Proposition 2.4(i)]).*

We define $\widetilde{\mathbb{D}_r}(\mathbb{Z}_p^\times, \Xi \otimes \mathbb{D}(V))$ to be $\varprojlim_{\mathrm{Tw}} \mathbb{D}_r\left(\mathbb{Z}_p^\times, \Xi \otimes D(V(\kappa^k))\right)$ where Tw is the twist map given by $\mu \mapsto (-tx)^{-1}\mu$. It is well-defined by [Zha04a, Lemma 3.6]. We define $\widetilde{\mathbb{D}_r}(\mathbb{Q}_p, \Xi \otimes \mathbb{D}(V))$ similarly. By [Zha04b, Theorems 3.3 and 3.6], the generalised Perrin-Riou exponential is given by:

Theorem B.1.6. *Let h be a positive integer such that $\mathbb{D}^{-h}(V) = \mathbb{D}(V)$. Then, there is a map*

$$\mathbb{E}_{h,V} : \widetilde{\mathbb{D}_r}(\mathbb{Q}_p, \Xi \otimes \mathbb{D}(V))^{\varphi_{\mathbb{D}}\otimes\varphi=1,\psi} \to H^1\left(K_\infty, \mathbb{D}_{r+r(V)+h}(\mathbb{Z}_p^\times, \mathbb{D}(V))\right)^{G_\infty}$$

such that for $k \geq 1-h$

$$\begin{aligned}\int_{\mathbb{Z}_p^\times} x^k\mathbb{E}_{h,V}(\mu) &= (k+h-1)!\exp_k\left((1-\varphi)^{-1}\left(1-\frac{\varphi^{-1}}{p}\right)\int_{\mathbb{Z}_p^\times}\frac{\mu}{(-tx)^k}\right), \\ \int_{1+p^n\mathbb{Z}_p} x^k\mathbb{E}_{h,V}(\mu) &= (k+h-1)!\exp_k\left(\frac{\varphi^{-n}}{p^n}\int_{\mathbb{Z}_p}\epsilon\left(\frac{x}{p^n}\right)\frac{\mu}{(-tx)^k}\right)\end{aligned}$$

where ϵ is as defined in [Col98, Section V.1] and $\exp_k$ *denotes the exponential map for the p-adic representation* $V(\kappa^k)$ *as defined in [BK90].*

B.2 Distributions on $\mathbb{Z}_p^\times$

Let $\mu \in \mathbb{D}_r(\mathbb{Z}_p, \Xi \otimes \mathbb{D}(V))^\psi$, then $\mu \in \mathbb{D}_r(\mathbb{Z}_p^\times, \Xi \otimes \mathbb{D}(V))^\psi$ iff

$$\sum_{\zeta^p=1} \mathcal{A}_\mu(\zeta(1+X)-1) = 0$$

where $\mathcal{A}_\mu$ is the Amice transform as defined in Remark B.1.5. On the space of power series satisfying this condition, $D = (1+X)\frac{d}{dX}$ acts bijectively. Moreover, for such a μ,

$$D^k \mathcal{A}_\mu(\zeta_{p^n} - 1) = \int_{\mathbb{Z}_p^\times} \epsilon\left(\frac{x}{p^n}\right) x^k \mu, \tag{B.1}$$

see e.g. [Col98, Section I.5].

Lemma B.2.1. *Any* $\mu \in \mathbb{D}_r(\mathbb{Z}_p^\times, \Xi \otimes \mathbb{D}(V))^\psi$ *can be lifted to*

$$\widetilde{\mu} \in \widetilde{\mathbb{D}_r}(\mathbb{Q}_p, \Xi \otimes \mathbb{D}(V))^{\varphi_{\mathbb{D}} \otimes \varphi = 1, \psi}.$$

Moreover, the image of such a lift under $\mathbb{E}_{h,V}$ *is independent of the choice of the lift.*

Proof. [Col98, Lemma IX.2.8 and Remark IX.2.6(iii)] and [Zha04b, Lemma 3.5]. ∎

Given any $\mu \in \mathbb{D}_r(\mathbb{Z}_p^\times, \Xi \otimes \mathbb{D}(V))^\psi$, we abuse notation and write $\mathbb{E}_{h,V}(\mu) = \mathbb{E}_{h,V}(\widetilde{\mu})$ where $\widetilde{\mu}$ is a lift of μ given by Lemma B.2.1. The fact that $\varphi_{\mathbb{D}} \otimes \varphi(\widetilde{\mu}) = \widetilde{\mu}$ implies that

$$\int_{pA} f(x)\widetilde{\mu} = \varphi\left(\int_A f(px)\widetilde{\mu}\right) \tag{B.2}$$

for any f and $A \subset \mathbb{Q}_p$. It allows us to compute some special values of $\widetilde{\mu}$.

Lemma B.2.2. $\int_{\mathbb{Z}_p} x^k \widetilde{\mu} = (1 - p^k\varphi)^{-1}\left(D^k \mathcal{A}_\mu(0)\right)$.

Proof. Since $\widetilde{\mu}$ restricted to $\mathbb{Z}_p^\times$ equals μ, (B.1) implies that

$$\int_{\mathbb{Z}_p^\times} x^k \widetilde{\mu_\xi} = \int_{\mathbb{Z}_p^\times} x^k \mu_\xi = D^k \mathcal{A}_\mu(0).$$

Hence, by applying (B.2) to the decomposition

$$\int_{\mathbb{Z}_p} x^k \widetilde{\mu} = \int_{p\mathbb{Z}_p} x^k \widetilde{\mu} + \int_{\mathbb{Z}_p^\times} x^k \widetilde{\mu},$$

we have

$$\int_{\mathbb{Z}_p} x^k \widetilde{\mu} = p^k \varphi \left(\int_{\mathbb{Z}_p} x^k \widetilde{\mu} \right) + D^k \mathcal{A}_\mu(0),$$

so we are done. □

Lemma B.2.3.

$$\int_{\mathbb{Z}_p} \epsilon\left(\frac{x}{p^n}\right) x^k \widetilde{\mu} = \sum_{i=0}^{n-1} p^{ik} \varphi^i \left(D^k \mathcal{A}_\mu(\zeta_{p^{n-i}} - 1) \right) + p^{nk}(1 - p^k \varphi)^{-1}(D^k \mathcal{A}_\mu(0)).$$

Proof. Since $\mathbb{Z}_p = \mathbb{Z}_p^\times \cup p\mathbb{Z}_p^\times \cup \cdots \cup p^{n-1}\mathbb{Z}_p^\times \cup p^n \mathbb{Z}_p$, we have

$$\begin{aligned} & \int_{\mathbb{Z}_p} \epsilon\left(\frac{x}{p^n}\right) x^k \widetilde{\mu} \\ = & \sum_{i=0}^{n-1} \int_{p^i \mathbb{Z}_p^\times} \epsilon\left(\frac{x}{p^n}\right) x^k \mu + \int_{p^n \mathbb{Z}_p} \epsilon\left(\frac{x}{p^n}\right) x^k \widetilde{\mu} \\ = & \sum_{i=0}^{n-1} p^{ik} \varphi^i \left(\int_{\mathbb{Z}_p^\times} \epsilon\left(\frac{x}{p^{n-i}}\right) x^k \mu \right) + p^{nk} \varphi^n \int_{\mathbb{Z}_p} x^k \widetilde{\mu} \end{aligned}$$

where the last equality follows from repeated applications of (B.2). Hence the result by (B.1) and Lemma B.2.2. □

B.3 Special values of the Perrin-Riou exponential

With the notation above, we define

$$\bar{\eta}(X) = \eta(X) - \frac{1}{p} \sum_{\zeta^p = 1} \eta(\zeta(1+X) - 1).$$

It is then clear that

$$\sum_{\zeta^p = 1} \bar{\eta}(\zeta(1+X) - 1) = 0.$$

Moreover, we have:

Lemma B.3.1. *We have $\bar{\eta} \in \Xi[[X]]^\psi$.*

Proof. Let $\sigma \in G_{\mathbb{Q}_p}$ and ζ a pth root of unity. By [Zha04b, (1.13)], $\eta \in \Xi[[X]]^\psi$, so $\sigma\eta(X) = \eta((1+X)^{\psi(\sigma)} - 1)$. If we replace X by $\zeta^\sigma(1+X) - 1$, we have

$$\begin{aligned} \sigma(\eta(\zeta(1+X) - 1)) &= (\sigma\eta)(\zeta^\sigma(1+X) - 1) \\ &= \eta((\zeta^\sigma(1+X))^{\psi(\sigma)} - 1) \\ &= \eta(\zeta^{\kappa(\sigma)}(1+X)^{\psi(\sigma)} - 1). \end{aligned}$$

Hence, on summing over $\zeta^p = 1$, we have

$$\begin{aligned}
\sigma\left(\sum_{\zeta^p=1} \eta(\zeta(1+X)-1)\right) &= \sum_{\zeta^p=1} \sigma(\eta(\zeta(1+X)-1)) \\
&= \sum_{\zeta^p=1} \eta(\zeta^{\kappa(\sigma)}(1+X)^{\psi(\sigma)}-1) \\
&= \sum_{\zeta^p=1} \eta(\zeta(1+X)^{\psi(\sigma)}-1) \text{ (as } \kappa(\sigma) \in \mathbb{Z}_p^\times).
\end{aligned}$$

Hence, we have

$$\sum_{\zeta^p=1} \eta(\zeta(1+X)-1) \in \Xi[[X]]^\psi.$$

But we already know that $\eta(X) \in \Xi[[X]]^\psi$, so we are done. □

Let $\xi \in \mathbb{D}(V)$, then $\bar{\eta}(X) \otimes \xi$ defines an element $\mu_\xi \in \mathbb{D}_0(\mathbb{Z}_p^\times, \Xi \otimes \mathbb{D}(V))$ with

$$\bar{\eta}(X) \otimes \xi = \int_{\mathbb{Z}_p^\times} (1+X)^x \mu_\xi.$$

By Lemma B.3.1 and Remark B.1.5, $\mu_\xi \in \mathbb{D}_0(\mathbb{Z}_p^\times, \Xi \otimes \mathbb{D}(V))^\psi$. On applying the Perrin-Riou exponential, we have:

Proposition B.3.2. *With the notation above, we have for $n \geq 1$ and $k \geq 1-h$*

$$\int_{1+p^n\mathbb{Z}_p} (-x)^k \mathbb{E}_{h,V}(\mu_\xi) = (k+h-1)! \exp_k(\gamma_{n,k}(\xi))$$

where $\gamma_{n,k}(\xi)$ is defined by

$$\frac{1}{p^n}\left(\sum_{i=0}^{n-i} D^{-k}\bar{\eta}^{\varphi^{i-n}}(\zeta_{p^{n-i}}-1) \otimes \varphi^{i-n}(\xi_k) + (1-\varphi)^{-1}(D^{-k}\bar{\eta}(0) \otimes \xi_k)\right)$$

with $\xi_k = \xi t^{-k}$.

Proof. The result follows from combining Theorem B.1.6 with Lemmas B.2.2, B.2.3 and the fact that $\varphi(t) = pt$. □

Our assumption on the eigenvalues of φ implies that there is an isomorphism

$$\begin{aligned}
H^1(K_\infty, \mathbb{D}_r(Z_p^\times, V))^{G_\infty} &\cong \mathbb{D}_r(G_\infty) \otimes \mathbb{H}^1_{\mathrm{Iw}}(\mathcal{F}, V) \\
\mu &\mapsto \left(\ldots, \int_{1+p^n\mathbb{Z}_p} \mu, \ldots\right)
\end{aligned}$$

where $\mathbb{H}^1_{\mathrm{Iw}}(\mathcal{F}, V) := \varprojlim_{\mathrm{cor}} H^1(K_n, V)$ and $\mathbb{D}_r(G_\infty) = \mathbb{D}_r(G_\infty, \mathbb{Q}_p)$ (see e.g. [Col98, Proposition 2]). Under this identification, we have

$$\mathbb{E}_{h,V}(\mu_\xi) \in \mathbb{D}_{h+r(V)}(G_\infty) \otimes \mathbb{H}^1_{\mathrm{Iw}}(\mathcal{F}, V).$$

Write $\mathrm{Tw}_k : \mathbb{H}^1_{\mathrm{Iw}}(\mathcal{F}, V) \to \mathbb{H}^1_{\mathrm{Iw}}(\mathcal{F}, V(\kappa^k))$ for the twist map. Recall that $\mathrm{Tw}_k(\mu) = (-tx)^{-k}\mu$, so Proposition B.3.2 implies that if $n \geq 1$, the nth component of $\mathrm{Tw}_k(\mathbb{E}_{h,V}(\mu))$ is given by

$$(k+h-1)! \exp_k(\gamma_{n,k}(\xi)) \tag{B.3}$$

where $\exp_k = \exp_{n,k}$ now denotes the exponential map

$$K_n \otimes \mathbb{D}(V(\kappa^k)) \to H^1(K_n, V(\kappa^k)).$$

We have suppressed the subscript n for simplicity, as it should not cause confusions.

Recall that $G_\infty \cong G_1 \times \Gamma$ where $\Gamma \cong \mathbb{Z}_p$. We fix a topological generator γ of Γ, then $\mathbb{D}_r(G_\infty)$ can be identified with the set of power series in $\gamma - 1$ over $\mathbb{Q}_p[G_1]$ which are $O(\log_p^r)$.

We now assume that V is a M-representation of $G_{\mathbb{Q}_p}$ where M is a finite extension of $\mathbb{Q}_p$. Then, as in Section 2.2, we have a pairing

$$<,>: \mathbb{D}_m(G_\infty) \otimes \mathbb{H}^1_{\mathrm{Iw}}(\mathcal{F}, V) \times \mathbb{D}_n(G_\infty) \otimes \mathbb{H}^1_{\mathrm{Iw}}(\mathcal{F}, V^*(1)) \to \mathbb{D}_{m+n}(G_\infty) \otimes M$$

for all $m, n \in \mathbb{R}_{\geq 0}$ and we can define the following.

Definition B.3.3. *For a fixed $\xi \in \mathbb{D}(V)$, we define a map*

$$\begin{aligned} \mathcal{L}^h_\xi : \mathbb{H}^1_{\mathrm{Iw}}(\mathcal{F}, V^*(1)) &\to \mathbb{D}_{r(V)+h}(G_\infty) \\ \mathbf{z} &\mapsto < \mathbb{E}_{h,V}(\mu_\xi), \mathbf{z} > . \end{aligned}$$

The same calculation as that in Section 2.2.1 shows that for $n \geq 1$

$$\begin{aligned} \left(\mathrm{Tw}_k \mathcal{L}^h_\xi(\mathbf{z})\right)_n &= (h+k-1)! \sum_{\sigma \in G_n} [\exp_k(\gamma_{n,k}(\xi)^\sigma), z_{-k,n}]_n \sigma \\ &= (h+k-1)! [\sum_{\sigma \in G_n} \gamma_{n,k}(\xi)^\sigma \sigma, \sum_{\sigma \in G_n} \exp_k^*(z^\sigma_{-k,n}) \sigma^{-1}]_n \end{aligned}$$

where $z_{-k,n}$ denotes the image of $\mathbf{z}$ under

$$\mathbb{H}^1_{\mathrm{Iw}}(\mathcal{F}, V^*(1)) \to \mathbb{H}^1_{\mathrm{Iw}}(\mathcal{F}, V^*(1)(\kappa^{-k})) \to H^1(K_n, V^*(1)(\kappa^{-k}))$$

and Tw_k acts on $\mathbb{D}_{r(V)+h}(G_\infty)$ by $\sigma \mapsto \kappa(\sigma)^k \sigma$ for $\sigma \in G_\infty$.

Let θ be a character on G_n which does not factor through G_{n-1}. Since $D^{-k}\bar{\eta}^{\varphi^{i-n}}(\zeta_{p^{n-i}} - 1) \in K_{n-i}$ by Lemma B.1.3, we have

$$\theta\left(\sum_{\sigma \in G_n} \gamma_{n,k}(\xi)^\sigma \sigma\right) = \frac{1}{p^n} \sum_{\sigma \in G_n} D^{-k}\bar{\eta}^{\varphi^{-n}}(\zeta_{p^n} - 1)^\sigma \theta(\sigma) \otimes \varphi^{-n}(\xi_k).$$

Hence, as in Section 2.2.1, we have for $k \geq 1-h$

$$\begin{aligned}&\frac{1}{(h+k-1)!}\kappa^k\theta(\mathcal{L}_\xi^h(\mathbf{z}))\\ =&\frac{1}{p^n}\left[\sum_{\sigma\in G_n} D^{-k}\bar{\eta}^{\varphi^{-n}}(\zeta_{p^n}-1)^\sigma\theta(\sigma)\otimes\varphi^{-n}(\xi_k),\sum_{\sigma\in G_n}\exp_k^*(z_{-k,n}^\sigma)\theta(\sigma^{-1})\right]_n.\end{aligned} \tag{B.4}$$

B.4 Construction of the ±-Coleman maps

From now on, we fix a modular form f as in Section 1.3.5 with $a_p = 0$ and $\epsilon(p) = 1$ (the latter is solely for simplicity) such that the eigenvalues of φ are not integral powers of p. Let $V = V_f(1)$. In particular, $r(V) = (k-1)/2 - 1$. On taking $h = 1$ in Theorem B.1.6 and writing $\mathcal{L}_\xi$ for $\mathcal{L}_\xi^h$, we have

$$\mathrm{Im}(\mathcal{L}_\xi) \subset \mathbb{D}_{(k-1)/2}(G_\infty) \otimes E \ \forall \xi \in \mathbb{D}(V).$$

Let $u = \kappa(\gamma)$, we modify the ±-logarithms of Pollack to define

$$\begin{aligned}\log_{p,k}^+ &= \prod_{j=0}^{k-2}\prod_{n=1}^{\infty}\frac{\Phi_{2n}(u^{-j}\gamma)}{p},\\ \log_{p,k}^- &= \prod_{j=0}^{k-2}\prod_{n=1}^{\infty}\frac{\Phi_{2n-1}(u^{-j}\gamma)}{p}.\end{aligned}$$

We can now give a generalisation of Proposition 2.4.2:

Lemma B.4.1. *Let $\xi^+ = \varphi(\omega)$ and $\xi^- = \omega$ where $0 \neq \omega \in \mathbb{D}^0(V)$, then $\log_{p,k}^\pm |\mathcal{L}_{\xi^\pm}(\mathbf{z})$ for all $\mathbf{z} \in \mathbb{H}^1_{\mathrm{Iw}}(\mathcal{F}, V^*(1))$.*

Proof. We have $\varphi^{2n}(\omega) \in \mathbb{D}^0(V(\kappa^r))$ for all integers n and $0 \leq r \leq k-2$. Therefore, by (B.4), we have

$$\begin{aligned}\kappa^r\theta(\mathcal{L}_{\xi^+}(\mathbf{z})) &= 0 \quad \text{if } n \text{ is odd},\\ \kappa^r\theta(\mathcal{L}_{\xi^-}(\mathbf{z})) &= 0 \quad \text{if } n \text{ is even}\end{aligned}$$

where θ is a character of G_n which does not factor through G_{n-1}. Hence, the zeros of $\log_{p,k}^\pm$ are also zeros of $\mathcal{L}_{\xi^\pm}(\mathbf{z})$, so we are done. ∎

In particular, since $\mathcal{L}_{\xi^\pm}(\mathbf{z}) \in \mathbb{D}_{(k-1)/2)}(G_\infty) \otimes E$, we have $\mathcal{L}_{\xi^\pm}(\mathbf{z})/\log_{p,k}^\pm = O(1)$. Hence, we have:

Definition B.4.2. *The plus and minus Coleman maps are defined to be*

$$\begin{aligned}\mathrm{Col}^{\pm} : \mathbb{H}^1_{\mathrm{Iw}}(K, V^*(1)) &\to \mathbb{D}_0(G_\infty) \otimes E \\ \mathbf{z} &\mapsto \mathcal{L}_{\xi^{\pm}}(\mathbf{z}) / \log^{\pm}_{p,k} .\end{aligned}$$

B.5 Kernel

For any positive integer n, we write $\pi_n = \eta^{\varphi^{-n}}(\zeta_{p^n} - 1)$. Then, $g^{(n)}(\pi_n) = 0$ where $g^{(n)} = \underbrace{g \circ \cdots \circ g}_{n}$. Moreover, $g(\pi_n) = \pi_{n-1}$ and $K_n = K(\pi_n)$. We from now on assume that g is a good lift of Frobenius as explained in Appendix A.

Fix a lattice T_f in V_f which is stable under $G_{\mathbb{Q}}$. Write

$$T = T_f(1) \subset V = V_f(1).$$

To describe the kernel of $\mathrm{Col}^{\pm}$, we assume $p \geq k - 1$. In this setting, all the results in Section 3.1 carry through.

Let $\mathbf{z} \in \mathbb{H}^1_{\mathrm{Iw}}(K, T^*(1))$. By Proposition 3.3.1, $\mathbf{z} \in \ker(\mathrm{Col}^{\pm})$ iff there exists $0 \leq m \leq k-2$, such that $z_{-m,n}$ is in the annihilator of the E-vector space generated by $\{\exp_m(\gamma_{n,m}(\xi^{\pm})^{\sigma}) : \sigma \in G_n\}$ for all $n > 0$. We take $m = 0$ below.

Proposition B.5.1. *The vector subspace over E of $H^1_f(K_n, V(\kappa))$ generated by the set $\{\exp(\gamma_{n,0}(\xi^{\pm})^{\sigma}) : \sigma \in G_n\}$, is equal to*

$$\left\{x \in H^1_f(K_n, V) : \mathrm{cor}_{n/m+1} x \in H^1_f(K_m, V) \forall m \in S^{\pm}_n\right\}.$$

Proof. Recall that by the proof of Lemma B.1.3, we have $\sigma g(\zeta - 1) = g(\zeta^{\kappa(\sigma)} - 1)$ for any $g \in \Xi[[X]]^{\psi}$, $\sigma \in G_{\mathbb{Q}_p}$ and ζ a p power root of unity. Therefore, for $n > 1$

$$\sum_{\zeta^p = 1} g(\zeta\zeta_{p^n} - 1) = \mathrm{Tr}_{n/n-1}\, g(\zeta_{p^n} - 1).$$

If $n = 1$, then

$$\sum_{\zeta^p = 1} g(\zeta\zeta_p - 1) = g(0) + \mathrm{Tr}_{1/0}\, g(\zeta_p - 1).$$

Hence, under the notation of Appendix A, we have

$$\begin{aligned}
p^n\gamma_{n,0}(\xi) &= \sum_{i=0}^{n-1}\bar{\eta}^{\varphi^{i-n}}(\zeta_{p^{n-i}}-1)\otimes\varphi^{i-n}(\xi)+\bar{\eta}(0)\otimes(1-\varphi)^{-1}(\xi)\\
&= \sum_{i=0}^{n-1}\left(\eta^{\varphi^{i-n}}(\zeta_{p^{n-i}}-1)-\frac{1}{p}\sum_{\zeta^p=1}\eta^{\varphi^{i-n}}(\zeta\zeta_{p^{n-i}}-1)\right)\otimes\varphi^{i-n}(\xi)\\
&\quad+\left(\eta(0)-\frac{1}{p}\sum_{\zeta^p=1}\eta(\zeta-1)\right)\otimes(1-\varphi)^{-1}(\xi)\\
&= \sum_{i=0}^{n}\left(\pi_{n-i}-\frac{1}{p}\operatorname{Tr}(\pi_{n-i})\right)\otimes\varphi^{i-n}(\xi)-\frac{1}{p}\operatorname{Tr}(\pi_1)\otimes(1-\varphi)^{-1}(\xi)\\
&= \sum_{i=0}^{n}\pi'_{n-i}\otimes\varphi^{i-n}(\xi)-\frac{1}{p-1}\otimes\xi+(1-\varphi)^{-1}(\xi).
\end{aligned}$$

Recall that $\varphi^2=-p^{k-3}$ on $\mathbb{D}(V)$, so we have

$$(1-\varphi)^{-1}=\frac{1}{1+p^{k-3}}(1+\varphi).$$

In particular, $-\frac{1}{p-1}\otimes\xi^{\pm}+(1-\varphi)^{-1}(\xi^{\pm})\notin\mathbb{D}^0(V)$. Moreover, $\varphi^r(\omega)\in\mathbb{D}^0(V)$ iff r is even, hence $\{\gamma_{n,0}(\xi^{\pm})^{\sigma}\}$ generates

$$\left(K+\sum_{i\in S_n^{\pm}}K^{(i)}\right)\otimes E\otimes\mathbb{D}(V)/\mathbb{D}^0(V)$$

by Corollary A.1.3. By translating the proof of Lemma 3.2.3, the result follows.

□

We write $H^1_f(K_n,V)^{\pm}$ for the vector space described in the proposition and define $H^1_f(K_n,T)^{\pm}=H^1_f(K_n,T)\cap H^1_f(K_n,V)^{\pm}$. Then,

$$H^1_f(K_n,T)^{\pm}=\left\{x\in H^1_f(K_n,T):\operatorname{cor}_{n/m+1}x\in H^1_f(K_m,T))\forall m\in S_n^{\pm}\right\}$$

and $\ker(\mathrm{Col}^{\pm})$ is given by

$$\mathbb{H}^1_{\mathrm{Iw},\pm}(T^*(1)):=\varprojlim H^1_{\pm}(K_n,T^*(1))$$

where $H^1_{\pm}(K_n,T^*(1))$ is defined to be the annihilator of $H^1_f(K_n,T)^{\pm}$ under the pairing

$$H^1(K_n,T^*(1))\times H^1(K_n,T)\to\mathcal{O}_F.$$

Finally, we state a few possible further generalisations which proofs we omit.

Remark B.5.2. *A generalisation of Proposition 3.4.1 can be proved straightforwardly.*

Remark B.5.3. *The images of* $\mathrm{Col}^{\pm}$ *can be described in the same way as in Chapter 4.*

Remark B.5.4. *The Coleman maps can also be extended to relative Lubin-Tate groups generalising those defined for elliptic curves in [Kim07].*

A detailed discussion about relative Lubin-Tate groups can be found in [Lei09a].

B.6 Selmer groups

We now briefly discuss how the kernels obtained above can be used to define $\pm$-Selmer groups for number fields other than $\mathbb{Q}$.

Let F be a number field with $[F:\mathbb{Q}]=d$. We assume that p splits completely in F. Let $\mathfrak{p}_1,\ldots,\mathfrak{p}_d$ be the primes of F above p and F_∞/F a $\mathbb{Z}_p$-extension such that $\mathfrak{p}_i$ is totally ramified in F_∞ for all i. We write F_n for the nth layer, i.e. the p^n-subextension.

Note that $F_{\mathfrak{p}_i}$ is isomorphic to $\mathbb{Q}_p$ for $i=1,\ldots,d$. By [IP06, Section 4.2], $F_{\infty,\mathfrak{p}_i}/F_{\mathfrak{p}_i}$ is contained in a Lubin-Tate extension for some uniformiser π of $\mathbb{Q}_p$ such that $\pi\in p(1+p\mathbb{Z}_p)$. Therefore, we can define $\mathrm{Col}^{\pm}$ for the corresponding Lubin-Tate extension and they can be restricted to

$$\varprojlim H^1(F_{n,\mathfrak{p}_i},T^*(1)),$$

since we have an isomorphism

$$H^1(F_{n,\mathfrak{p}_i},T^*(1))\cong H^1(K_n,T^*(1))^{G_1},$$

which can be proved as in the proof of Lemma 6.2.1. It is then easy to check that the description of the kernels generalise directly, as discussed in Section 6.4. For each $n\geq 0$, we can define as in [IP06]

$$\mathrm{Sel}_p^{\pm}(f/F_n)=\ker\left(\mathrm{Sel}_p(f/F)\to\prod_i\frac{H^1(F_{n,\mathfrak{p}_i},V/T)}{H^1_f(F_{n,\mathfrak{p}_i},T)^{\pm}\otimes\mathbb{Q}_p/\mathbb{Z}_p}\right)$$

and $\mathrm{Sel}_p^{\pm}(f/F_\infty)=\varinjlim\mathrm{Sel}_p^{\pm}(f/F_n)$.

Unfortunately, unlike the cyclotomic case, $\mathrm{Sel}_p^{\pm}(f/F_\infty)$ is not Λ-cotorsion in general. However, they do satisfy a control theorem (c.f. [Kob03, Theorem 9.3]) and their coranks can be used to describe those of $\mathrm{Sel}_p(f/F_n)$ (c.f. [IP06, Proposition 7.1]). Since the proofs for these results given in [IP06, Kob03] are purely algebraic and do not involve properties of elliptic curves, they generalise to general f with no difficulties.

Bibliography

[AV75] Yvette Amice and Jacques Vélu, *Distributions p-adiques associées aux séries de Hecke*, Journées Arithmétiques de Bordeaux (Conf., Univ. Bordeaux, Bordeaux, 1974), Soc. Math. France, Paris, 1975, pp. 119–131. Astérisque, Nos. 24–25.

[BB10] Laurent Berger and Christophe Breuil, *Sur quelques représentations potentiellement cristallines de* $GL_2(\mathbb{Q}_p)$, Astérisque (2010), no. 330, 155–211.

[Ber03] Laurent Berger, *Bloch and Kato's exponential map: three explicit formulas*, Doc. Math. (2003), no. Extra Vol., 99–129 (electronic), Kazuya Kato's fiftieth birthday.

[Ber04] ———, *Limites de représentations cristallines*, Compos. Math. **140** (2004), no. 6, 1473–1498.

[BK90] Spencer Bloch and Kazuya Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, Vol. I, Progr. Math., vol. 86, Birkhäuser Boston, Boston, MA, 1990, pp. 333–400.

[BLZ04] Laurent Berger, Hanfeng Li, and Hui June Zhu, *Construction of some families of 2-dimensional crystalline representations*, Math. Ann. **329** (2004), no. 2, 365–377.

[Bre01] Christophe Breuil, *p-adic hodge theory, deformations and local langlands*, cours au C.R.M. de Barcelone (http://www.ihes.fr/∼breuil/), 2001.

[CC99] Frédéric Cherbonnier and Pierre Colmez, *Théorie d'Iwasawa des représentations p-adiques d'un corps local*, J. Amer. Math. Soc. **12** (1999), no. 1, 241–268.

[Col98] Pierre Colmez, *Théorie d'Iwasawa des représentations de de Rham d'un corps local*, Ann. of Math. (2) **148** (1998), no. 2, 485–571.

[Del69] Pierre Deligne, *Formes modulaires et représentations l-adiques*, Séminaire Bourbaki (1968/69), no. 21, Exp. No. 355, 139–172.

[Edi92] Bas Edixhoven, *The weight in Serre's conjectures on modular forms*, Invent. Math. **109** (1992), no. 3, 563–594.

[IP06] Adrian Iovita and Robert Pollack, *Iwasawa theory of elliptic curves at supersingular primes over $\mathbb{Z}_p$-extensions of number fields*, J. Reine Angew. Math. **598** (2006), 71–103.

[Kat93] Kazuya Kato, *Lectures on the approach to Iwasawa theory for hasse-weil L-functions via B_{dR}. I*, Arithmetic algebraic geometry (Trento, 1991), Lecture Notes in Math., vol. 1553, Springer, Berlin, 1993, pp. 50–163.

[Kat04] ______, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque (2004), no. 295, ix, 117–290, Cohomologies p-adiques et applications arithmétiques. III.

[Kim07] Byoung Du Kim, *The parity conjecture for elliptic curves at supersingular reduction primes*, Compos. Math. **143** (2007), no. 1, 47–72.

[Kob03] Shin-ichi Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math. **152** (2003), no. 1, 1–36.

[Kur02] Masato Kurihara, *On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction. I*, Invent. Math. **149** (2002), no. 1, 195–224.

[Lei09a] Antonio Lei, *Coleman maps for modular forms at supersingular primes over Lubin-Tate extensions*, arXiv: 0908.0091v2, 2009.

[Lei09b] ______, *Iwasawa theory for modular forms at supersingular primes*, arXiv: 0904.3938v2, 2009.

[LLZ10] Antonio Lei, David Loeffler, and Sarah Zerbes, *Wach modules and Iwasawa theory for modular forms*, arXiv: 0912.1263v2, 2010.

[MTT86] Barry Mazur, John Tate, and Jeremy Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), no. 1, 1–48.

[Pol03] Robert Pollack, *On the p-adic L-function of a modular form at a supersingular prime*, Duke Math. J. **118** (2003), no. 3, 523–558.

[PR93] Bernadette Perrin-Riou, *Fonctions L p-adiques d'une courbe elliptique et points rationnels*, Ann. Inst. Fourier (Grenoble) **43** (1993), no. 4, 945–995.

[PR94] ______, *Théorie d'Iwasawa des représentations p-adiques sur un corps local*, Invent. Math. **115** (1994), no. 1, 81–161.

[PR95] ______, *Fonctions L p-adiques des représentations p-adiques*, Astérisque (1995), no. 229, 198.

[PR00] ______, *Représentations p-adiques et normes universelles. I. Le cas cristallin*, J. Amer. Math. Soc. **13** (2000), no. 3, 533–551.

[PR04] Robert Pollack and Karl Rubin, *The main conjecture for CM elliptic curves at supersingular primes*, Ann. of Math. (2) **159** (2004), no. 1, 447–464.

[PS09] Robert Pollack and Glenn Stevens, *Critical slope p-adic l-functions*, (preprint), 2009.

[Roh88] David E. Rohrlich, *L-functions and division towers*, Math. Ann. **281** (1988), no. 4, 611–632.

[Rub85] Karl Rubin, *Elliptic curves and $\mathbb{Z}_p$-extensions*, Compositio Math. **56** (1985), no. 2, 237–250.

[Rub87] ______, *Local units, elliptic units, Heegner points and elliptic curves*, Invent. Math. **88** (1987), no. 2, 405–422.

[Rub91] ———, *The "main conjecture" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. **103** (1991), no. 1, 25–68.

[Rub00] ———, *Euler systems*, Annals of Mathematics Studies, vol. 147, Princeton University Press, Princeton, NJ, 2000, Hermann Weyl Lectures. The Institute for Advanced Study.

[Shi76] Goro Shimura, *The special values of the zeta functions associated with cusp forms*, Comm. Pure Appl. Math. **29** (1976), no. 6, 783–804.

[Spr09] Ian Sprung, *Iwasawa theory for elliptic curves at supersingular primes: beyond the case* $a_p = 0$, arXiv: 0903.3419, 2009.

[Wac96] Nathalie Wach, *Représentations p-adiques potentiellement cristallines*, Bull. Soc. Math. France **124** (1996), no. 3, 375–400.

[Zha04a] Shaowei Zhang, *On a trivial zero problem*, Int. J. Math. Math. Sci. (2004), no. 5-8, 295–318.

[Zha04b] ———, *On explicit reciprocity law over formal groups*, Int. J. Math. Math. Sci. (2004), no. 9-12, 607–635.