AN INTRODUCTION TO p-ADIC L-FUNCTIONS II: MODULAR FORMS

by

Chris Williams

Contents

This set of notes is a continuation of 'An introduction to p-adic L-functions', written by the author jointly with Joaquín Rodrigues Jacinto. The first notes gave an introduction to p-adic L-functions, with a focus on p-adic L-functions for GL(1), and in particular the p-adic analogue of the Riemann zeta function. The main areas of study were p-adic measures and Iwasawa algebras, cyclotomic units, and the Iwasawa main conjecture for GL(1). The previous notes contained a general overview (section 1), Part I (sections 2–5) and Part II (sections 6–8), as well as an appendix of classical background results. They are not required as a prerequisite to the present notes, though sections 1—3 at least would provide useful motivation for the topics we consider here. Throughout, they are cited as [**RJW17**].

The present notes should be considered as the second half of a first course on p-adic L-functions. In them, we look at the analytic side of this picture for GL(2), studying p-adic L-functions of modular forms. We consider the theory of p-adic distributions (a more general notion of measures), and give a construction of the p-adic L-function of a modular form due to Pollack and Stevens.

Recommended reading: The material on modular forms is explained in far more detail in [**DS05**], particularly in §5, where the properties of the L-function are explored. All of the material on p-adic analysis and distributions can be found in a paper of Colmez [**Col10**], a complete and very readable account of the theory (in French). The construction of the p-adic L-function of a modular form via overconvergent modular symbols is from the original papers of Pollack and Stevens [**PS11, PS12**], and is explained beautifully in their Arizona Winter School lectures [**Pol11**], which can be viewed online through the AWS page. Almost all of the material here, and lots more there was not time to cover, also appears in Bellaïche's excellent (but sadly unfinished) book [**Bel**].

General overview, continued

In the first half of these notes, we studied only the very simplest kinds of L-functions, those attached to Dirichlet characters, whilst alluding to the more general picture. It is natural to ask in what generality L-functions, and the results of Iwasawa theory, should live. We now sketch some of the more general aspects of the theory.

I. Adelic automorphic forms

The philosophy of the *Langlands program* says that 'every L-function should come from an automorphic form[(1)].' Such objects are analytic functions on adelic groups that are highly symmetric for a group action.

I.1. Dirichlet characters as automorphic forms for $\mathrm{GL}(1)$**.** — The most basic examples of automorphic forms, again, are Dirichlet characters. We would like a uniform way to consider all such characters, which – in their standard definition – are all defined on different finite multiplicative groups. With that in mind, let $D = \prod_{p \text{ prime}} p^{r_p}$ be a positive integer, noting that for all but finitely many primes, $r_p = 0$. Consider a primitive Dirichlet character

$$\chi : (\mathbf{Z}/D\mathbf{Z})^\times \longrightarrow \mathbf{C}^\times$$

modulo D. Decomposing, one can consider this as a product of characters

$$\chi = \left(\prod_{p \text{ prime}} \chi_p\right) : \prod (\mathbf{Z}/p^{r_p}\mathbf{Z})^\times \longrightarrow \mathbf{C}^\times;$$

and then, lifting under the natural maps $\mathbf{Z}_p^\times \to (\mathbf{Z}/p^{r_p}\mathbf{Z})^\times$, as a character

$$\chi : \prod_p \mathbf{Z}_p^\times \longrightarrow \mathbf{C}^\times.$$

Ultimately, this means we can consider every Dirichlet character as an element

$$\chi \in \mathrm{Hom}_{\mathrm{cts}}\left(\prod_p \mathbf{Z}_p^\times, \mathbf{C}^\times\right).$$

We now have a contribution from every finite place of $\mathbf{Q}$. In the spirit of L-functions, we usually go further, and include the infinite place as well. Recall the identification

$$\begin{aligned} \mathbf{C} &\xrightarrow{\sim} \mathrm{Hom}_{\mathrm{cts}}(\mathbf{R}_{>0}, \mathbf{C}^\times) \\ s &\longmapsto [x \mapsto x^s]. \end{aligned}$$

We may then consider elements

$$(s, \chi) \in \mathrm{Hom}_{\mathrm{cts}}\left(\mathbf{R}_{>0} \times \prod_p \mathbf{Z}_p^\times,\ \mathbf{C}^\times\right).$$

Observe that this is exactly the input one gives an L-function! In particular, we can consider *all* Dirichlet L-functions at once as a single measure on this space $\mathbf{R}_{>0} \times \prod_p \mathbf{Z}_p^\times$. Such a viewpoint was outlined in Tate's thesis.

This is usually packaged into a nicer form by introducing the *ideles*

$$\begin{aligned} \mathbf{A}^\times &= \mathbf{R}^\times \times \prod_p{}' \mathbf{Q}_p^\times \\ &:= \{(x_\infty, x_2, x_3, x_5, ...) : x_p \in \mathbf{Z}_p^\times \text{ for all but finitely many } p\}, \end{aligned}$$

the $\prod'$ denoting 'restricted product'. Note that there is a unique rational number q such that $x_\infty/q \in \mathbf{R}_{>0}$ and $x_p/q \in \mathbf{Z}_p^\times$ for all p. Indeed, any rational number is determined by its valuation at every prime p and its sign; the valuation of q at p is exactly $v_p(x_p)$, and the sign is equal to the sign of x_∞. Note that this is well-defined by the condition that $x_p \in \mathbf{Z}_p^\times$ for almost all p. We thus get a decomposition

$$\mathbf{A}^\times \cong \mathbf{Q}^\times \times \mathbf{R}_{>0} \times \prod_p \mathbf{Z}_p^\times, \tag{I.1}$$

(1) Or more properly, an *automorphic representation*, where one considers the space of all such automorphic forms under an adelic group action.

and we can consider Dirichlet characters as functions

$$\chi : \mathbf{A}^\times \longrightarrow \mathbf{C}^\times$$

which are invariant under pre-multiplication by $\mathbf{Q}^\times$, where the multiplication is by

$$q \cdot (x_\infty, x_2, x_3, ...) = (qx_\infty, qx_2, qx_3, ...).$$

To complete this transition to automorphic forms, now observe that $\mathbf{Q}^\times = \mathrm{GL}_1(\mathbf{Q})$. Further, the notation $\mathbf{A}^\times$ is suggestive, and indeed this is the group of units in a ring

$$\begin{aligned}\mathbf{A} &:= \mathbf{R} \times {\prod_p}' \mathbf{Q}_p \\ &= \{(x_\infty, x_2, x_3, x_5, ...) : x_p \in \mathbf{Z}_p \text{ for all but finitely many } p\}.\end{aligned}$$

In this regime, we then see the Dirichlet character χ as a function

$$\chi : \mathrm{GL}_1(\mathbf{A}) \longrightarrow \mathbf{C}^\times$$

which is:

- invariant under $\mathrm{GL}_1(\mathbf{Q})$;
- invariant under $\mathbf{R}_{>0}$;
- and invariant under the action of a finite index subgroup $K(D) \subset \prod_p \mathbf{Z}_p^\times$.

Here $K(D)$ is defined place by place to be

$$K(D)_p = \begin{cases} 1 + p^{r_p}\mathbf{Z}_p & : r_p > 0 \\ \mathbf{Z}_p^\times & : r_p = 0. \end{cases}$$

We normally again parcel this up by defining

$$\widehat{\mathbf{Z}} = \varprojlim_{N \geq 1} (\mathbf{Z}/N\mathbf{Z}) = \prod_p \mathbf{Z}_p,$$

then seeing $K(D)$ as an open compact subgroup of $\mathrm{GL}_1(\widehat{\mathbf{Z}}) = \prod_p \mathbf{Z}_p^\times$.

This leads us to consider χ as an *automorphic form for $G = \mathrm{GL}_1$ of level D*, that is, a complex function

$$\chi : G(\mathbf{A}) \longrightarrow \mathbf{C}$$

which is (left-)invariant under $G(\mathbf{Q})$ and (right-)invariant under an open compact subgroup $K \subset G(\widehat{\mathbf{Z}})$.

***Remark* (Weights and the idelic norm).** — The Dirichlet characters we consider are finite order, and thus are trivial on the component $\mathbf{R}_{>0}$. These correspond to automorphic forms of 'weight 0'. More generally, the weight of an automorphic form is always encoded in its archimedean part. Automorphic forms for GL_1 of weight k are those functions whose restriction to $\mathbf{R}_{>0}$ is of the form

$$\begin{aligned}\chi_\infty : \mathbf{R}_{>0} &\longrightarrow \mathbf{C} \\ x &\longmapsto x^k.\end{aligned}$$

Note, however, that the function

$$\begin{aligned}\chi_k : \mathbf{A}^\times &\longrightarrow \mathbf{C}^\times \\ (x_\infty; x_f) &\longmapsto x_\infty^k \cdot \chi(x_f),\end{aligned}$$

where $x_f = (x_2, x_3, x_5, ...)$ denotes the *finite* part of an idele x, is not automorphic in the sense above: it is not invariant under pre-multiplication by $\mathbf{Q}$. If we multiply by the prime 5, for example, then

$$\begin{aligned}\chi_k(5 \cdot x) &= 5^k \cdot \chi_k(x) \\ &= |5|_5^{-k} \cdot \chi_k(x).\end{aligned}$$

We can fix this, then, by also multiplying by $|\cdot|_p^k$ at every finite prime. This translates into multiplying by a power of the *idelic norm* function

$$|\cdot|_{\mathbf{A}^\times} : \mathbf{A}^\times \longrightarrow \mathbf{R}_{>0},$$
$$(x_\infty; x_2, x_3, ...) \longmapsto |x_\infty|_{\mathbf{R}} \times \prod_p |x_p|_p.$$

One checks that $|\mathbf{Q}^\times|_{\mathbf{A}^\times} = 1$, and hence that the function

$$\chi|\cdot|_{\mathbf{A}^\times}^k : \mathbf{A}^\times \longrightarrow \mathbf{C}^\times$$

preserves the property of invariance under $\mathbf{Q}^\times$, that is, it is a weight k automorphic form for GL(1).

It turns out that all algebraic weight k automorphic forms for GL(1) are a power of the norm times a finite-order character.

***Remark* (Further conditions at infinity).** — For a more general group G, the infinite part $\mathbf{R}_{>0}$ should be replaced by the connected component $G^+(\mathbf{R})$ of the identity in $G(\mathbf{R})$. We should then also impose a symmetry condition under the maximal compact subgroup $K_\infty \subset G^+(\mathbf{R})$. Note that the maximal compact subgroup of $\mathbf{R}_{>0}$ is just $\{1\}$, so that for $G = \mathrm{GL}_1$, this is an empty condition.

Finally, we should more generally also consider an analyticity condition at the infinite place, which we ignore for now.

I.2. Automorphic forms for GL(2)**: modular forms.** — In the second half of these notes, we turn our attention to what is perhaps the next most natural (and most studied!) case, that of GL_2. The natural generalisation of the above is to consider complex functions

$$f : \mathrm{GL}_2(\mathbf{A}) \longrightarrow \mathbf{C}$$

that are:

- left-invariant under $\mathrm{GL}_2(\mathbf{Q})$,
- right-invariant under an open compact subgroup $K \subset \mathrm{GL}_2(\widehat{\mathbf{Z}})$,
- transforms like $x \mapsto x^{-k}$ on the centre $\mathbf{A}^\times \subset \mathrm{GL}_2(\mathbf{A})$ of diagonal matrices,
- and satisfies a symmetry condition under the maximal compact subgroup

$$K_\infty = \mathrm{SO}_2(\mathbf{R}) \subset \mathrm{GL}_2^+(\mathbf{R}).$$

Here the connected component $\mathrm{GL}_2^+(\mathbf{R})$ is just the group of real matrices of positive determinant.

It turns out these (algebraic) adelic automorphic forms admit a much simpler description. Indeed, the *strong approximation theorem* for GL_2 tells us that

$$\mathrm{GL}_2(\mathbf{A}) = \mathrm{GL}_2(\mathbf{Q}) \cdot \mathrm{GL}_2^+(\mathbf{R}) \cdot K,$$

a higher-dimensional analogue of (I.1). Now, we cut down our space.

– The left-invariance under $\mathrm{GL}_2(\mathbf{Q})$, and the right-invariance under K, means these functions are uniquely determined by their values on $\mathrm{GL}_2^+(\mathbf{R})$.
– These functions have specified transformation properties under the centre $\mathbf{R}_{>0}$ and the maximal compact $\mathrm{SO}_2(\mathbf{R})$, so are uniquely determined by their values on the quotient $\mathrm{GL}_2^+(\mathbf{R})/[\mathbf{R}_{>0} \cdot \mathrm{SO}_2(\mathbf{R})$.

Lemma. — *Let* $\mathcal{H} := \mathbf{R} \times \mathbf{R}_{>0} = \{z = x + iy \in \mathbf{C} : y > 0\}$. *Then we have*

$$\mathcal{H} \cong \mathrm{GL}_2^+(\mathbf{R}) \,/\, \big[\mathbf{R}_{>0} \cdot \mathrm{SO}_2(\mathbf{R})\big]$$

via the map $x + iy \mapsto \left(\begin{smallmatrix} y & x \\ 0 & 1 \end{smallmatrix}\right)$.

In particular, any function f as above descends to a function

$$f : \mathcal{H} \longrightarrow \mathbf{C}$$

with induced transformation properties under a matrix group. One can check that the combination of being right-invariant under K, left-invariant under $G(\mathbf{Q})$ and weight k symmetric under $\mathbf{R}_{>0} \cdot \mathrm{SO}_2(\mathbf{R})$ translates into the condition that this function f satisfies

$$f(\gamma z) = (cz+d)^{k+2} f(z)$$

for all

$$\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma := K \cap \mathrm{SL}_2(\mathbf{Z}).$$

In particular, it becomes exactly the transformation condition defining weight $k+2$ modular forms of level Γ. Of course, the analyticity condition we have been ignoring translates in this formulation to exactly the statement that f is holomorphic on $\mathcal{H}$ and bounded at the cusps. This is all explained in [**Wei71**].

The upshot, then, of all of the above calculations is that *modular forms* are (algebraic) automorphic forms for GL(2), and are the natural 2-dimensional generalisation of Dirichlet characters. For the rest of these lectures, we turn to this case.

II. Iwasawa theory for modular forms

Suppose now that we have a modular form f with attached L-function $L(f,s)$ (which we recap in §9). As we hopefully made clear in [**RJW17**], Iwasawa theory is founded on the study of special values of L-functions. It is natural to ask how much of the theory we described for GL(1) has has an analogue for modular forms.

II.1. Recapping GL(1). — Ultimately, in [**RJW17**] we described three different constructions of the Kubota–Leopoldt p-adic L-function ζ_p.

(1) In §2-4, we gave an *analytic* construction, a p-adic measure ζ_p^{an} interpolating special values $L(\chi, -k)$ of Dirichlet L-functions attached to characters of p-power conductor.

(2) In §6, we gave an *arithmetic* construction. We defined the Coleman map

$$\mathrm{Col} : \varprojlim \left(\mathcal{O}^\times_{\mathbf{Q}_p(\zeta_{p^n})}\right) \longrightarrow \Lambda(\mathbf{Z}_p^\times)$$

from p-adic towers of local units into measures on $\mathbf{Z}_p^\times$, and defined ζ_p^{arith} as the image under Col of the family of *cyclotomic units*.

(3) Finally, in §7 we gave an *algebraic* construction. We defined a Galois group $\mathscr{X}_\infty^+$, and explained that it was a torsion $\Lambda(\mathbf{Z}_p^\times)$ module, which thus has a well-defined characteristic ideal $\zeta_p^{\mathrm{alg}} \subset \Lambda(\mathbf{Z}_p^\times)$ by the structure theory of Λ-modules.

We showed in §6 that the analytic and arithmetic constructions agree, that is, that $\zeta_p^{\mathrm{an}} = \zeta_p^{\mathrm{arith}}$. The Iwasawa main conjecture is exactly the statement that the algebraic construction agrees with the others, that is, that

$$\zeta_p^{\mathrm{alg}} = \zeta_p^{\mathrm{an}} I(\mathbf{Z}_p^\times) \subset \Lambda(\mathbf{Z}_p^\times).$$

II.2. Analogues for GL(2). — Ultimately, versions of all of the above theory are known for sufficiently nice modular forms. Let f be a cuspidal Hecke eigenform of weight $k+2$ and level $\Gamma_0(N)$, with $p|N$, and let $L(f,s)$ be its attached L-function. There are three ways of associating a p-adic L-function to f.

II.2.1. *Analytic.* — There exists a range of 'critical' values of the complex L-function $L(f,s)$, namely the values $L(f,\chi,j+1)$ for χ any Dirichlet character and $0 \leq j \leq k$. These values are those that the Bloch–Kato conjecture suggests should relate to arithmetic information arising from f.

The analytic p-adic L-function is an element $L_p^{\mathrm{an}}(f)$ in a p-adic analytic space $\mathcal{D}(\mathbf{Z}_p^\times)$ which interpolates these critical values. In particular, we have the following:

Theorem A. — *Let α_p denote the U_p eigenvalue of f. If $v_p(\alpha_p) < k+1$, then there exists a unique locally analytic distribution $L_p^{\mathrm{an}}(f)$ on $\mathbf{Z}_p^\times$ such that*

– *$L_p^{\mathrm{an}}(f)$ has growth of order $v_p(\alpha_p)$,*

– *and for all Dirichlet characters χ of conductor p^n, and for all $0 \leq j \leq k$, we have*

$$L_p^{\mathrm{an}}(f,\overline{\chi},j+1) = \int_{\mathbf{Z}_p^\times} \chi(x)x^j \cdot L_p^{\mathrm{an}}(f)$$
$$= -\alpha_p^{-n} \cdot \left(1 - \chi(p)\frac{p^j}{\alpha_p}\right) \cdot \frac{G(\chi)\cdot j! \cdot p^{nj}}{(2\pi i)^{j+1}} \cdot \frac{L(f,\overline{\chi},j+1)}{\Omega_f^\pm}.$$

The proof of this theorem is the main aim of these notes. In particular, over the course of the lectures we will explain all of the concepts and terms appearing in the theorem. The interpolating constant, whilst significantly more involved than the analogous constant for GL(1), is very natural, and largely corresponds to 'completing the L-function at infinity.' For now, the important thing to take from this theorem is that there exists a single p-adic analytic object which should 'see' the data predicted by the Bloch–Kato conjecture.

II.2.2. *Arithmetic.* — The arithmetic side hinges on Galois representations and Euler systems. In [**RJW17**, §6.6], we explained that:

– The Kubota–Leopoldt p-adic L-function is attached to the Galois representation $\mathbf{Q}_p(1)$, the cyclotomic character.

– The tower of cyclotomic units forms an *Euler system* for $\mathbf{Q}_p(1)$, a norm-compatible family of Galois cohomology classes.

– The Coleman map is the *Perrin-Riou big logarithm map* $\mathrm{Log}_{\mathbf{Q}_p(1)}$ for $\mathbf{Q}_p(1)$, which takes values in p-adic measures.

Attached to a modular form f, we have a Galois representation V_f, in which we can pick a Galois-stable integral lattice T_f. The arithmetic p-adic L-function is then given by the following deep theorem of Kato, proved in his magisterial paper [**Kat04**].

Theorem B. — *There exists an Euler system*

$$\mathbf{z}_m(f) \in \mathrm{H}^1(\mathbf{Q}(\mu_m), T_f)$$

attached to T_f.

In the yoga described in [**RJW17**, §6.6], we then consider the system of classes over $\mathbf{Q}(\mu_{p^n})$, localise to get classes over $\mathbf{Q}_p(\mu_{p^n})$, and then take the inverse limit to obtain an attached element of the Iwasawa cohomology

$$\mathbf{z}_{\mathrm{Iw}}(f) \in \mathrm{H}^1_{\mathrm{Iw}}(\mathbf{Q}_p, V_f).$$

The arithmetic p-adic L-function is then the image of $\mathbf{z}_{\mathrm{Iw}}$ under the Perrin-Riou big logarithm map

$$\mathrm{Log}_{V_f} : \mathrm{H}^1_{\mathrm{Iw}}(\mathbf{Q}_p, V_f) \longrightarrow \mathcal{D}(\mathbf{Z}_p^\times)$$
$$\mathbf{z}_{\mathrm{Iw}} \longmapsto L_p^{\mathrm{arith}}(f).$$

Here $\mathcal{D}(\mathbf{Z}_p^\times)$ is the space of locally analytic distributions from Theorem A in which $L_p^{\mathrm{an}}(f)$ lives.

The second deep theorem of [**Kat04**] in this setting is the following *explicit reciprocity law.*

Theorem C. — *There is an equality*

$$L_p^{\mathrm{an}}(f) = L_p^{\mathrm{arith}}(f)$$

of distributions on $\mathbf{Z}_p^\times$.

For more on the theory of Euler systems, [**Rub00**] is a comprehensive account. The reader is also encouraged to use the resources from Loeffler and Zerbes' course at the 2018 Arizona Winter School; there are video recordings of their lectures in addition to their lecture notes [**LZ18**].

II.2.3. *Algebraic.* — In the case of GL(1), the group $\mathscr{X}_\infty^+$ is a *Selmer group* for ρ, a Galois cohomology group cut out by a family of local conditions. This is described in [**Gre89**, §1]. We may make an analogous definition in general, defining a Selmer group $\mathscr{X}_{p^\infty}(V_f)$ attached to the representation V_f at p.

When f is a *p-ordinary* modular form, that is, when the eigenvalue α_p has $v_p(\alpha_p) = 0$, then $\mathscr{X}_{p^\infty}(V_f)$ is naturally a module over the Iwasawa algebra $\Lambda(\mathbf{Z}_p^\times)$ of $\mathbf{Z}_p^\times$. Again, in [**Kat04**], Kato proved that this is a *torsion* Λ-module, and thus has a characteristic ideal

$$L_p^{\mathrm{alg}}(f) := \mathrm{ch}_{\Lambda(\mathbf{Z}_p^\times)}(\mathscr{X}_{p^\infty}(V_f)),$$

the *algebraic p-adic L-function of f*.

When f is p-ordinary, the analytic/arithmetic p-adic L-function is actually a measure on $\mathbf{Z}_p^\times$, and hence lives in the subspace $\Lambda(\mathbf{Z}_p^\times) \subset \mathcal{D}(\mathbf{Z}_p^\times)$. The Iwasawa main conjecture for such f is then the following theorem.

***Theorem D* (Iwasawa main conjecture for f).** — *Under some mild additional technical hypotheses, we have*

$$L_p^{\mathrm{alg}}(f) = (L_p^{\mathrm{an}}(f)) \subset \Lambda(\mathbf{Z}_p^\times).$$

This is a theorem of Kato [**Kat04**] and Skinner–Urban [**SU14**]. Kato proves one divisibility, that $L_p^{\mathrm{alg}}|(L_p^{\mathrm{an}})$, without requiring the additional hypotheses. These hypotheses were used in Skinner–Urban's proof of the other divisibility; they involve conditions like residual irreducibility of the Galois representation V_f and technical conditions on ramified primes. There has since been much further work weakening the required hypotheses, including analogues for non-ordinary modular forms.

II.3. Iwasawa theory for elliptic curves. — Perhaps the most important aspects of the Iwasawa theory of modular forms come through the applications to elliptic curves. The Taniyama–Shimura conjecture, now a theorem due to the ground-breaking work of Wiles [**Wil95**], Taylor–Wiles [**TW95**] and Breuil–Conrad–Diamond–Taylor [**BCDT01**], is the statement that every rational elliptic curve is *modular* in the sense that its L-function is equal to the L-function of a weight 2 modular form. In this sense, the Iwasawa theory of elliptic curves is a proper subset of the Iwasawa theory of modular forms, and indeed almost everything we know today about L-functions of elliptic curves goes through the modular interpretation.

As we outlined in the introduction of [**RJW17**], Iwasawa theory has really provided the best available results towards the Birch and Swinnerton-Dyer (BSD) conjecture. In particular, the Iwasawa main conjecture for elliptic curves can be viewed as a p-adic version of BSD.

Loosely, an application to classical BSD takes the following, extremely vague, shape. Suppose $L(E,1) \neq 0$. Then through the connection between the classical L-function and the analytic p-adic L-function, this gives a lower bound on the size of the ideal (L_p^{an}) in $\Lambda(\mathbf{Z}_p^\times)$. For this ideal to be big causes the corresponding Selmer group $\mathscr{X}_{p^\infty}(E)$ to be small. But this Selmer group can be thought of as a proxy for the $\mathbf{Q}(\mu_{p^\infty})$-rational points on E, via the Kummmer exact sequence for elliptic curves. In particular, at finite level m over a number field F we have a short exact sequence

$$0 \to E(F)/mE(F) \longrightarrow \mathrm{Sel}_m(E/F) \longrightarrow Ш(E/F)[m] \to 0,$$

where $Ш(E/F)$ is the (conjecturally finite) Tate–Shafarevich group. From this, we deduce that the rank of E in the tower $\mathbf{Q}(\mu_{p^n})$ is *bounded*, a theorem of Mazur. We also get even finer control at all stages, which allows us to deduce that $E(\mathbf{Q})$ itself is small, and in particular that the rank is 0, giving 'weak BSD in analytic rank 0'.

By being more precise, one may also deduce the p-part of the leading term formula in strong BSD. There are also results in analytic rank 1, and partial results in analytic rank 2, that arise directly from knowledge of the Iwasawa main conjecture (see, for example, [**JSW17**]).

More details on all of this, and the more general Iwasawa theory of modular forms, are contained in Skinner's 2018 Arizona Winter School lectures [**Ski18**].

II.4. Further generalisations. — The three constructions above, and the equalities between them, are expected to go through in very wide generality, but there are very few cases in which the whole picture has been completed. We sketch this here. Suppose ρ is a Galois representation, arising from a motive M, and corresponding under Langlands to an automorphic representation.

(1) **(Analytic)**. There should be an element $L_p^{\mathrm{an}}(\rho)$ in a p-adic analytic space $\mathcal{D}$ which interpolates special values of $L(\rho, s)$. The criterion to be a 'special value' was predicted by Deligne [**Del79**], and the exact form of this analytic p-adic L-function is subject to a precise conjecture of Coates–Perrin-Riou [**Coa89, CPR89**].

In practice, this is already difficult, and there are many fundamental cases where such a construction is not known. For example, we've seen the cases GL(1) and GL(2); but at present, there is no construction that works for GL(3). Much more is known for generalisations in other directions (for example, working over number fields, or working with different algebraic groups such as unitary or symplectic groups).

(2) **(Arithmetic)**. We also expect Euler systems to exist in great generality, but known examples are scarcer still. Until very recently, Kato's Euler system and the cyclotomic units were two of only three examples of Euler systems, the other being the system of *elliptic units* (though the system of *Heegner points* is closely related). There has been a recent increase of activity in the area, stemming from Lei, Loeffler and Zerbes' construction of the Euler system of Beilinson–Flach elements [**LLZ14**], for ρ the Rankin–Selberg convolution of two modular forms.

Where an Euler system exists, one can apply a Perrin-Riou logarithm map and extract an arithmetic p-adic L-function; but proving an explicit reciprocity law is harder still, and at present the only known examples of the equality $L_p^{\mathrm{an}} = L_p^{\mathrm{arith}}$ are those presented above and the Rankin–Selberg case [**KLZ17**].

Examples of Euler systems where the explicit reciprocity laws are not yet known are given in [**LLZ15, LLZ18, LSZ17**]. For the p-adic L-function, one may also try and construct the Iwasawa cohomology class $\mathbf{z}_{\mathrm{Iw}}$ directly, without constructing a full Euler system; this is the approach taken in [**CRJ18**].

(3) **(Algebraic)**. One also expects Iwasawa main conjectures to hold in wide generality, at least in ordinary settings, and there are many partial results towards this too. Whenever one has an Euler system with the equality $L_p^{\mathrm{an}} = L_p^{\mathrm{arith}}$, for example, one has that the corresponding Selmer group is torsion and the divisibility $L_p^{\mathrm{alg}} | (L_p^{\mathrm{an}})$.

II.5. What do we cover in these lectures? — Since the case of GL(2) is significantly more involved than that of GL(1), in these lectures a treatment of the Iwasawa main conjecture for modular forms will be out of reach. Instead, we focus on proving the existence of the *analytic* p-adic L-function $L_p(f)^{\mathrm{an}}$ for modular eigenforms f. In particular, we will give a proof of Theorem A above, as well as developing the 'right' p-adic analytic framework – that of p-adic distributions – in which this result lives. We hope this will provide motivation to explore further aspects of the Iwasawa theory of modular forms, or the analytic theory in more general settings.

II.6. Prerequisites. — In [**RJW17**], we attempted to make the treatment as self-contained as possible, and included relevant background material in a series of appendices. The resulting notes should have been accessible to a student with a thorough grounding in undergraduate algebraic number theory. In the second half of these notes, we necessarily assume that the reader is comfortable with the theory of modular forms, including the theory of Hecke operators; a standard first course in the subject should be sufficient.

Even then, the treatment will not be entirely self-contained, and at times we borrow deep theorems from automorphic representation theory. Most notably, among results that might not typically appear in a first course on modular forms, we do not prove algebraicity of Hecke eigenvalues, and we do not include a proof of the Eichler–Shimura isomorphism between modular forms and cohomology/modular symbols.

II.7. Organisation of lectures. — These notes are organised as follows.

– In §9 we recall basic facts about modular forms, define their L-functions, and derive integral formulae for them in terms of their period integrals.

– In §10 we recast all of this more algebraically through the theory of (classical) modular symbols, discarding the analytic data inherent in the definition of modular forms in favour of a purely algebraic definition.

– In §11, we describe the Eichler–Shimura isomorphism between spaces of modular forms and modular symbols, and prove that certain 'special/critical values' of the L-function of a modular form are algebraic multiples of complex periods.

– In §12, we describe the theory of overconvergent modular symbols, infinite-dimensional spaces of p-adic modular symbols built using spaces of distributions from p-adic analysis. We state Stevens' control theorem, which controls the space of classical modular symbols as a quotient of the space of overconvergent modular symbols.

– In §13, we give Greenberg's proof of Stevens' control theorem. The proof is computationally effective and uses filtrations on distributions.

– In §14, we use all of the above to construct the p-adic L-function attached to a small slope modular form f as a locally analytic distribution on $\mathbf{Z}_p^\times$, and prove that it interpolates algebraic parts of the critical L-values of f.

– In §15, we define growth properties of locally analytic distributions, and prove that the p-adic L-function has growth of order equal to its slope. As a corollary, we deduce that the p-adic L-function is uniquely determined by its interpolation property.

II.8. Acknowledgements. — I am grateful to Timo Keller, Marc Masdeu and Rob Rockwood for pointing out a number of corrections on earlier drafts of these notes. Further comments and corrections are welcome: please send them to `christopher.d.williams@warwick.ac.uk`.

Part III: p-adic L-functions for Modular Forms

9. The L-function of a modular form

9.1. Modular forms 101. — We start Part III by recalling some relevant facts about modular forms. We treat this only briefly, as it is a vast topic in its own right; an excellent reference for much of this material is [**DS05**], particularly chapters 1 and 5.

Definition 9.1. — Define the *upper half-plane* to be

$$\begin{aligned}\mathcal{H} &:= \{x+iy \in \mathbf{C} : y > 0\}\\ &= \mathbf{R}\times\mathbf{R}_{>0}.\end{aligned}$$

The boundary of $\mathcal{H}$ is the set of cusps $\mathbf{P}^1(\mathbf{Q})$, where a cusp $r \in \mathbf{Q}$ is viewed inside $\mathbf{C}$ as $r + 0i$ on the real line, and where ∞ is viewed to be at the 'end' of the positive imaginary axis in $\mathbf{C}$.

Thoughout, we will work with the congruence subgroup $\Gamma_0(N) \subset \mathrm{SL}_2(\mathbf{Z})$, and for convenience will henceforth always denote this by Γ. The reader should consider N to be fixed through the rest of these notes. When considering the p-adic behaviour, we will impose the additional condition that N is divisible by p. We have the standard action of $\mathrm{SL}_2(\mathbf{Z})$ on $\mathcal{H}\cup\mathbf{P}^1(\mathbf{Q})$ by

$$\begin{pmatrix} a & b\\ c & d\end{pmatrix}\cdot z = \frac{az+b}{cz+d},$$

noting that this preserves both $\mathcal{H}$ and $\mathbf{P}^1(\mathbf{Q})$.

Definition 9.2. — A *modular form* of weight k and level Γ is a holomorphic function

$$f : \mathcal{H} \longrightarrow \mathbf{C}$$

which:

(1) satisfies the invariance property

$$f(\gamma z) = (cz+d)^k f(z)$$

for all $\gamma \in \Gamma$,

(2) and is holomorphic (has bounded growth) as z tends to any cusp.

We write $M_k(\Gamma, \mathbf{C})$ for the (finite-dimensional) complex vector space of modular forms of weight k and level Γ.

We say f is a *cusp form* if it vanishes at every cusp, and write $S_k(\Gamma,\mathbf{C}) \subset M_k(\Gamma,\mathbf{C})$ for the sub-vector-space of cusp forms.

Proposition 9.3. — *There is a direct sum decomposition*

$$M_k(\Gamma,\mathbf{C}) \cong S_k(\Gamma,\mathbf{C}) \oplus \mathcal{E}(\Gamma,\mathbf{C}),$$

where $\mathcal{E}_k(\Gamma,\mathbf{C})$ is the space of Eisenstein series (see [**DS05**, §4]*).*

Since $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right) \in \Gamma$, any modular form satisfies

$$f(z+1) = f(z),$$

and thus admits a Fourier expansion

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

in the variable $q = e^{2\pi i z}$. We call this the *q-expansion* of f. If f is a cusp form, then $a_0(f) = 0$. More precisely, this is the Fourier expansion at the cusp $\infty \in \mathbf{P}^1(\mathbf{Q})$; there are analogous Fourier expansions around any other cusp $r \in \mathbf{P}^1(\mathbf{Q})$, and f is a cusp form if and only if the constant term of the Fourier expansion at r vanishes for each cusp $r \in \mathbf{P}^1(\mathbf{Q})$.

The notion of q-expansions allow us to define natural algebraic structures on the space of modular forms.

Definition 9.4. — For $F \subset \mathbf{C}$, let

$$M_k(\Gamma, F) = \{f \in M_k(\Gamma, \mathbf{C}) : f(z) \in F[[q]]\},$$

a finite-dimensional F-vector space. As before, we have a decomposition

$$M_k(\Gamma, F) = S_k(\Gamma, F) \oplus \mathcal{E}_k(\Gamma, F)$$

into cuspidal and Eisenstein series.

Remark 9.5. — As $F[[q]] \otimes_F \mathbf{C} \subset \mathbf{C}[[q]]$, we clearly have

$$M_k(\Gamma, F) \otimes_F \mathbf{C} \hookrightarrow M_k(\Gamma, \mathbf{C}).$$

From the definition, it is far from obvious that this space is non-zero for *any* F. One remarkable consequence of the theory of Hecke operators, as recalled in the next section, is that there is always a number field F (which depends on Γ and k) such that this is an isomorphism, that is, all modular forms of weight k and level Γ are defined over F.

9.2. Hecke operators and algebraic structure. — The definition of modular forms is inherently analytic, and appears to be implicitly transcendental in nature. One of the major reasons modular forms are so important is that they admit an incredibly rich algebraic structure, arising from the action of *Hecke operators*, a collection of commuting operators built from arithmetic. The space of modular forms admits a basis of eigenforms for these operators, each with algebraic eigenvalues. We say that $M_k(\Gamma, \mathbf{C})$ has a good *spectral theory* under the Hecke operators.

For a full definition of Hecke operators, see [**DS05**, §5]. For our purposes, we recall only the very basics.

Definition 9.6. — For $\gamma \in \mathrm{GL}_2^+(\mathbf{Q})$, define the *weight k operator*

$$f|_k\gamma := \det(\gamma)^{k-1}(cz+d)^{-k} f(\gamma z).$$

Define Hecke operators as follows:

– Let q be a prime not dividing N. There is an operator

$$T_q : M_k(\Gamma, \mathbf{C}) \to M_k(\Gamma, \mathbf{C})$$

defined by

$$T_q f(z) = \sum_{a=0}^{q-1} f \bigg|_k \begin{pmatrix} 1 & a \\ 0 & p \end{pmatrix} (z) \; + f \bigg|_k \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} (z).$$

– For $q|N$, we have an analogous operator

$$U_q f(z) = \sum_{a=0}^{q-1} f \bigg|_k \begin{pmatrix} 1 & a \\ 0 & p \end{pmatrix} (z).$$

These definitions extend in a natural way to composite n; there is a recurrence formula for T_{q^n} [**DS05**, §5.3], and for m, n coprime to N and each other, we have $T_{mn} = T_m T_n$. For $q|N$, we have $U_{q^n} = U_q^n$. All of these operators commute [**DS05**, Prop. 5.2.4].

Definition 9.7. — Let $\mathbf{H}_N$ denote the *Hecke algebra*, the free $\mathbf{Z}$-algebra generated by the T_q and U_q operators.

Definition 9.8. — An *eigenform* for $\mathbf{H}_N$ is $f \in M_k(\Gamma, \mathbf{C})$ such that

$$Tf = \lambda(T)f \qquad \text{for all } T \in \mathbf{H}_N,$$

where $\lambda : \mathbf{H}_N \to \mathbf{C}$ is a homomorphism. We call λ an *eigenpacket*.

The following theorems encode the algebraicity of modular forms. Recall that an eigenform is a *newform* at level N if it 'does not come from any lower level $M|N$'; see [**DS05**, §5.6] for further details.

Theorem 9.9. — (1) *Let f be an eigenform for the Hecke operators, corresponding to an eigenpacket λ. There exists a number field K_f such that*

$$\lambda : \mathbf{H}_N \longrightarrow K_f \subset \mathbf{C}$$

factors, that is, λ is valued in K_f.

(2) *$S_k(\Gamma, \mathbf{C})$ has a basis of eigenforms.*

(3) *Let f be a newform, and let*

$$S_k(\Gamma, \mathbf{C})[f] := \{g \in S_k(\Gamma, \mathbf{C}) : Tg = \lambda(f)g \text{ for all } T \in \mathbf{H}_N\},$$

the f-eigenspace for $\mathbf{H}_N$ in $S_k(\Gamma, \mathbf{C})$. This eigenspace is 1-dimensional over $\mathbf{C}$.

Proof. — Part (1) is proved (in the case of weight 2) in [**DS05**, §6.5]. The idea is to use the *Jacobian* J_Γ of the modular curve $X_\Gamma = \Gamma\backslash[\mathcal{H} \cup \mathbf{P}^1(\mathbf{Q})]$; in particular, there is an identification between J_Γ and the quotient of the dual space $S_2(\Gamma)^\vee$ by the integral homology $\mathrm{H}_1(X_\Gamma, \mathbf{Z})$. The Jacobian – and hence this quotient – admits a natural Hecke action, which is compatible with the action on cusp forms under the above identification; but then the Hecke operators stabilise $\mathrm{H}_1(X_\Gamma, \mathbf{Z})$, which forces their characteristic polynomials to be integral, and the eigenvalues to be algebraic integers. The higher weight case is more involved.

For (2), see [**DS05**, Thm. 5.8.3]. For (3), see [**DS05**, Thm. 5.8.2]. □

Theorem 9.10. — *Let (f, λ) be a cuspidal eigenform that is* normalised *in the sense that $a_1(f) = 1$. Then*

$$\lambda(T_q) = a_q(f),$$
$$\lambda(U_p) = a_p(f).$$

In particular, $f \in M_k(\Gamma, K_f)$.

Proof. — The action of Hecke operators on q-expansions can be computed (see [**DS05**, (5.3)]), and reduces to

$$a_1(T_q f) = a_q(f).$$

But f is an eigenform, so

$$a_1(T_q f) = a_1(\lambda(T_q) \cdot f) = \lambda(T_q)a_1(f) = \lambda(T_q).$$ □

Corollary 9.11. — *There exists a number field F such that $M_k(\Gamma, F) \otimes_F \mathbf{C} \cong M_k(\Gamma, \mathbf{C})$.*

Proof. — Take a (finite) basis of eigenforms $\{f_i\}_{i \in I}$, and let F be the compositum of the number fields K_{f_i} for $i \in I$. □

9.3. p-stabilisation. — In the theory of p-adic variation later on, we will always take p to divide the level N, and the U_p operator will be of central importance. Indeed, if p does not divide the level, then there can be no theory of p-adic variation: we will return to this theme in Remark 12.11. Fortunately it is always possible to force p into the level by passing to an appropriate oldform. All of this is explained in [**DS05**, §5.6].

Suppose now we have a newform $g \in S_k(\Gamma_0(N))$, with N prime to p, with associated eigenpacket λ_g. Note that we have two modular forms

$$g(z), \quad g(pz) \quad \in S_k(\Gamma_0(Np));$$

these functions are both holomorphic on $\mathbf{C}$ and at the cusps, and it is simple to see that they transform as expected under $\Gamma_0(Np)$. The characteristic polynomial of U_p on the span of $g(z)$ and $g(pz)$ is $X^2 - a_p(g)X + p^{k-1}$. When the roots α, β of this polynomial are distinct, then we may diagonalise U_p on this space, and obtain two U_p-eigenforms

$$f_\alpha(z) := g(z) - \beta g(pz), \qquad f_\beta := g(z) - \alpha g(pz);$$

then $U_p f_\alpha = \alpha f_\alpha$ and $U_p f_\beta = \alpha f_\beta$. Since U_p commutes with the other Hecke operators, and $g(z), g(pz)$ are easily seen to be Hecke eigenforms for all the T_q, U_q with $q \neq p$, we obtain two eigenforms f_α, f_β, and corresponding eigenpackets $\lambda_\alpha, \lambda_\beta$ respectively, where

$$\begin{aligned}\lambda_\alpha(T_q) &= \lambda_g(T_q), \quad q \nmid Np;\\ \lambda_\alpha(U_q) &= \lambda_g(U_q), \quad q|N;\\ \lambda_\alpha(U_p) &= \alpha\end{aligned}$$

(and similarly for λ_β).

Recall Theorem 9.9(iii), which said that $S_k(\Gamma_0(N))[f]$ is one-dimensional (for the newform g). When $\alpha \neq \beta$, then using strong multiplicity one we can deduce the analogous statement for the p-stabilisations.

Proposition 9.12. — *Let g be a newform of level N, and let α, β be the roots of $X^2 - a_p(g)X + p^{k-1}$. If $\alpha \neq \beta$, then*

$$\dim_{\mathbf{C}} S_k(\Gamma_0(Np))[f_\alpha] = \dim_{\mathbf{C}} S_k(\Gamma_0(Np))[f_\beta] = 1. \tag{9.1}$$

Proof. — The subspace of $S_k(\Gamma_0(Np))$ on which the Hecke operators T_q for $q \nmid Np$ act as $\lambda_g(T_q)$ is 2-dimensional, spanned by $g(z)$ and $g(pz)$, by the results of [**DS05**, §5]. But then U_p is diagonal with distinct eigenvalues on this 2-dimensional space, so decomposes into the two one-dimensional eigenspaces claimed. □

If $k \geq 2$, then conjecturally $\alpha \neq \beta$ always; this is a form of Maeda's conjecture.

Remark 9.13. — If $\alpha = \beta$ – the so-called 'p-irregular' case – then it is still always possible to take a p-stabilisation f_α of f to level Np which is an eigenform. Morevoer, Proposition 9.12 can be seen to be true as well. This is far more subtle: the *generalised* eigenspace is now 2-dimensional, but a simple calculation (see [**RS17**, §9.2]) shows that the U_p-action on this is not semisimple, and hence the *actual* eigenspace is only 1-dimensional.

9.4. The L-function of a modular form. — The central object in Part III of these notes is the L-function of a modular form, which we now define.

Definition 9.14. — Let $f = \sum_{n\geq 1} a_n(f)q^n \in S_k(\Gamma, \mathbf{C})$. For $\mathrm{Re}(s) > k/2+1$, define the *L-function of f* to be

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

If χ is a Dirichlet character, then define the *twist of $L(f,s)$ by χ* to be

$$L(f,\chi,s) = \sum_{n\geq 1} a_n(f)\chi(n)n^{-s}.$$

To see that this makes sense in the region of definition, we use:

Lemma 9.15. — *There exists a constant C such that $|a_n| \leq Cn^{k/2}$ for all n. Thus $L(f,s)$ is absolutely convergent for* $\mathrm{Re}(s) > k/2+1$.

Proof. — See [**DS05**, Prop. 5.9.1]. This is essentially a consequence of f being holomorphic at the cusp infinity. □

9.4.1. *An integral formula.* — Recall we described the Γ-function in [**RJW17**, Intro.] as

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

Previously, we used the transformation $t \leftrightarrow nt$ to extract an integral description of n^{-s}. In this setting, given the variable $q = e^{2\pi i z}$, it is more convenient to normalise differently. We obtain:

Lemma 9.16. — *We have*

$$n^{-s} = \frac{(2\pi)^s}{\Gamma(s)} \int_0^\infty e^{-2\pi n t} t^{s-1} dt.$$

Proof. — Make the substitution $t \leftrightarrow 2\pi n t$, and rearrange. □

Proposition 9.17. — *Let $f \in S_k(\Gamma)$ be a cusp form, and define*

$$g(s) = \int_0^{i\infty} f(z) z^{s-1} dz.$$

Then for $\mathrm{Re}(s) \gg 0$*, we have*

$$g(s) = \frac{\Gamma(s)}{(-2\pi i)^s} L(f,s).$$

Proof. — We compute directly that

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

using the expression for n^{-s} in Lemma 9.16. For $\mathrm{Re}(s) \gg 0$, this converges absolutely, and we may swap the sum and product. We also write $-t = i \times (it)$, so as to recover the exponent $2\pi i$, and obtain

$$\begin{aligned} &= \frac{(2\pi)^s}{\Gamma(s)} \int_0^\infty \sum_{n\geq 1} a_n(f) e^{2\pi n i (it)} t^{s-1} dt \\ &= \frac{(2\pi)^s}{\Gamma(s)} \int_0^\infty f(it) t^{s-1} dt \\ &= \frac{(-2\pi i)^s}{\Gamma(s)} \int_0^\infty f(it)(it)^{s-1} d(it), \end{aligned}$$

where in the last step we multiply by $(-i)^s i^s = 1$ and make a basic change of variables. We conclude by setting $z = it$. □

Corollary 9.18. — *The L-function $L(f,s)$ has an analytic continuation to the whole complex plane $\mathbf{C}$. It admits a functional equation relating the values at s and $k-s$.*

Proof. — To prove the analytic continuation, one shows that the integral is everywhere convergent, and thus gives the extension of the Dirichlet series to all of $\mathbf{C}$. See the accompanying exercise sheets for further details. □

By specialising at the value $s = j+1$, we immediately obtain the following special value formula, recalling that the integer values $\Gamma(j+1) = j!$ of Γ are the factorials.

Corollary 9.19. — *Let $j \in \mathbf{Z}_{\geq 0}$. We have*

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

We also have twisted versions of this. Let $\chi : (\mathbf{Z}/D\mathbf{Z})^\times \to \overline{\mathbf{Q}}^\times$ be a Dirichlet character of conductor D, and recall the Gauss sums from [**RJW17**, §4.1].

Lemma 9.20. — *We have*

$$\overline{\chi}(n) n^{-s} = \frac{(-2\pi i)^s}{\Gamma(s) G(\chi)} \sum_{a \in (\mathbf{Z}/D\mathbf{Z})^\times} \chi(a) \int_{a/D}^\infty e^{2\pi i n z} \left(z - \frac{a}{D}\right)^{s-1} dz.$$

Proof. — We have the identity

$$\frac{1}{G(\chi)}\sum_{a\in(\mathbf{Z}/D\mathbf{Z})^\times}\chi(a)e^{2\pi i n a/D} = \begin{cases} \chi^{-1}(n)=\overline{\chi}(n) & : (n,D)=1 \\ 0 & : \text{otherwise}\end{cases}$$

of Gauss sums, which we used in [**RJW17**, Rem. 4.3] when studying Dirichlet p-adic L-functions. We may consider this uniformly by extending $\overline{\chi}$ to $\mathbf{Z}$ in the natural way, that is, letting $\overline{\chi}(n)=0$ if n is not coprime to the conductor D. Multiplying the expression of Lemma 9.16 by this identity, we obtain

$$\begin{aligned}\overline{\chi}(n)n^{-s} &= \frac{(2\pi)^s}{\Gamma(s)G(\chi)}\sum_{a\in(\mathbf{Z}/D\mathbf{Z})^\times}\chi(a)e^{2\pi i n a/D}\int_0^\infty e^{-2\pi n t}t^{s-1}dt\\ &= \frac{(2\pi)^s}{\Gamma(s)G(\chi)}\sum_{a\in(\mathbf{Z}/D\mathbf{Z})^\times}\chi(a)\int_0^\infty e^{2\pi i n\left(it+\frac{a}{D}\right)}t^{s-1}dt\\ &= \frac{(-2\pi i)^s}{\Gamma(s)G(\chi)}\sum_{a\in(\mathbf{Z}/D\mathbf{Z})^\times}\chi(a)\int_0^\infty e^{2\pi i n\left(it+\frac{a}{D}\right)}(it)^{s-1}d(it),\end{aligned}$$

multiplying by $1=(-i)^s\cdot i^{s-1}\cdot i$. This is

$$= \frac{(-2\pi i)^s}{\Gamma(s)G(\chi)}\sum_{a\in(\mathbf{Z}/D\mathbf{Z})^\times}\chi(a)\int_{a/D}^\infty e^{2\pi i n z}\left(z-\frac{a}{D}\right)^{s-1}dz$$

after making the substitution $z=it+a/D$. □

Corollary 9.21. — *We have*

$$L(f,\overline{\chi},s) = \frac{(-2\pi i)^s}{\Gamma(s)G(\chi)}\sum_{a\in(\mathbf{Z}/D\mathbf{Z})^\times}\chi(a)\int_{a/D}^\infty f(z)\left(z-\frac{a}{D}\right)^{s-1}dz.$$

In particular, the twisted L-function also admits analytic continuation to all of $\mathbf{C}$, *and satisfies a functional equation.*

Proof. — We argue almost exactly as in the proof of Proposition 9.17, only now with twisted coefficients. □

The following will not be used during these lectures, but the statement is included for completeness.

Theorem 9.22. — *f is a normalised eigenform if and only if*

$$L(f,s) = \prod_{p\ prime}(1-a_pp^{-s}+p^{k-1-2s})^{-1}.$$

Proof. — [**DS05**, Thm. 5.9.2]. □

10. Modular symbols

As we've seen, modular forms are defined in an inherently analytic way, but via Hecke operators, they turn out to have deep underlying algebraic structure. Further than that, via the q-expansion, we can recover a cuspidal eigenform f purely from its Hecke eigenvalues, as $a_p(f)=\lambda(T_p)$. Moreover, the L-function is then also defined in terms of the Hecke eigenvalues. It is natural to ask: was it possible to define this algebraic structure directly, without resorting the analytic definitions at all?

The theory of *modular symbols*, which we now describe, does exactly this, by algebraically encoding values of integrals of f (sometimes called periods of f). In particular, the space of modular symbols can be viewed as 'throwing away' all the analytic properties of the modular form, leaving only the algebraic skeleton underneath.

10.1. Modular symbols in weight 2. — Let $f \in S_2(\Gamma)$ be a modular form. We saw in the previous section that the integrals

$$\int_r^s f(z)dz, \quad r, s \in \mathbf{P}^1(\mathbf{Q})$$

are interesting, and linear combinations of them give twisted values $L(f, \chi, 1)$ of the L-function attached to f. Let us now consider them all at once.

Definition 10.1. — Let $\Delta = \mathrm{Div}(\mathbf{P}^1(\mathbf{Q})) = \mathbf{Z}[\mathbf{P}^1(\mathbf{Q})]$ be the free abelian group generated by symbols $[r]$ for $r \in \mathbf{P}^1(\mathbf{Q})$ a cusp. There is a natural degree map

$$\begin{aligned} \deg : \Delta &\longrightarrow \mathbf{Z}, \\ \sum_r c_r[r] &\longmapsto \sum_r c_r, \end{aligned}$$

and we define

$$\Delta_0 = \ker(\deg)$$

to be its kernel. Then Δ_0 is generated by terms of the form $[r] - [s]$ for $r, s \in \mathbf{P}^1(\mathbf{Q})$.

We view $[r] - [s]$ as (any) simple path $r \to s$ in $\mathcal{H}$, and then Δ_0 as the (additive) space of such paths. We will encode this principle in notation by writing $[r] - [s]$ as $\{r \to s\}$.

Definition 10.2. — Define

$$\mathrm{Symb}(\mathbf{C}) = \mathrm{Hom}(\Delta_0, \mathbf{C}).$$

By analogy with our motivation, a homomorphism $\phi \in \mathrm{Symb}(\mathbf{C})$ should be viewed as a 'system of integrals over paths $r \to s$'.

Example 10.3. — Let $f \in S_2(\Gamma, \mathbf{C})$. Then

$$\phi_f : \{r \to s\} \mapsto \int_r^s f(z)dz$$

gives an element of $\mathrm{Symb}(\mathbf{C})$. Note that this integral is well-defined by the properties of f: in particular, it is independent of the choice of simple path $r \to s$ since f holomorphic, and converges as f is a cusp form, hence has exponential decay at every cusp.

This construction gives a map $S_2(\Gamma, \mathbf{C}) \to \mathrm{Symb}(\mathbf{C})$. But $\mathrm{Symb}(\mathbf{C})$ is far too big to maintain a nice spectral theory of Hecke operators: in particular, it is infinite dimensional. We need to build in the remaining property satisfied by modular forms, that is, a notion of Γ-invariance.

Lemma 10.4. — *Let $f \in S_2(\Gamma, \mathbf{C})$. Then*

$$\phi_f\{\gamma r \to \gamma s\} = \phi_f\{r \to s\}.$$

for all $\gamma \in \Gamma$.

Proof. — We compute directly that

$$\begin{aligned} \frac{d(\gamma z)}{dz} &= \frac{d}{dz}\left(\frac{az+b}{cz+d}\right) \\ &= \frac{a(cz+d) - c(az+b)}{(cz+d)^2} \\ &= \frac{1}{(cz+d)^2}, \end{aligned}$$

as $ad - bc = 1$. Thus under the change of variables $z \leftrightarrow \gamma z$, we have

$$d(\gamma z) = (cz+d)^{-2}dz.$$

Then since f has weight 2, we get $f(\gamma z)d(\gamma z) = f(z)dz$, and

$$\phi_f\{\gamma r \to \gamma s\} = \int_{\gamma r}^{\gamma s} f(z)dz = \int_r^s f(\gamma z)d(\gamma z)$$
$$= \int_r^s f(z)dz = \phi_f\{r \to s\}.$$

□

Definition 10.5. — The space of $\mathbf{C}$-*valued modular symbols for* Γ is the space

$$\mathrm{Symb}_\Gamma(\mathbf{C}) := \mathrm{Hom}_\Gamma(\Delta_0, \mathbf{C})$$

of Γ-invariant homomorphisms (that is, homomorphisms satisfying $\phi\{\gamma r \to \gamma s\} = \phi\{r \to s\}$).

In particular, Lemma 10.4 shows that

$$\phi_f \in \mathrm{Symb}_\Gamma(\mathbf{C}).$$

This is now a *purely algebraic* space, containing elements corresponding to f. Moreover, the symbol ϕ_f (more or less by definition) computes special values of the L-function of f; by Corollary 9.19 we have

$$\phi_f\{0 \to \infty\} = -\frac{1}{2\pi i}L(f,1).$$

Remark 10.6. — The -1 here appears because we are considering $\int_0^\infty$ rather than $\int_\infty^0$, as in [**Pol11**].

Moreover, ϕ_f also sees all the twisted L-values at 1.

Definition 10.7. — Let $\chi : (\mathbf{Z}/D\mathbf{Z})^\times \to \overline{\mathbf{Q}}^\times$ be a (primitive) Dirichlet character. Define

$$\begin{aligned}\mathrm{Ev}_\chi : \mathrm{Symb}_\Gamma(\mathbf{C}) &\longrightarrow \mathbf{C}\\ \phi &\longmapsto \sum_{a \in (\mathbf{Z}/D\mathbf{Z})^\times} \chi(a)\phi_f \Big| \begin{pmatrix} 1 & a \\ 0 & D\end{pmatrix} \{0 \to \infty\}\\ &= \sum_{a \in (\mathbf{Z}/D\mathbf{Z})^\times} \chi(a)\phi_f\left\{\frac{a}{D} \to \infty\right\}.\end{aligned}$$

We abuse notation here, and henceforth, and write "$a \in (\mathbf{Z}/D\mathbf{Z})^\times$" to mean a set of integer representatives of the unit classes modulo D.

(We will define a more general version of this map, with general coefficients, in Definition 10.16 below).

Proposition 10.8. — *Let $f \in S_2(\Gamma, \mathbf{C})$, and $\chi : (\mathbf{Z}/D\mathbf{Z})^\times \to \overline{\mathbf{Q}}^\times$ be a Dirichlet character. Then*

$$\mathrm{Ev}_\chi(\phi_f) = -\frac{G(\chi)}{2\pi i}L(f, \overline{\chi}, 1).$$

Proof. — This follows directly by specialising the integral formula for $L(f, \overline{\chi}, s)$ given in Corollary 9.21; since $s = 1$, the polynomial term $z - a/D$ does not appear. □

10.2. Abstract modular symbols. — All of the above was valid only for weight 2. We want an analogous theory for higher weight modular forms.

Remark 10.9. — Henceforth, it will be convenient to always consider forms to have weight $k+2$, instead of weight k. (One always has to contend with this shift by 2; some authors choose to continue to work with weight k forms, at the cost of introducing coefficients of index $k-2$). We remark that this shift by 2 arises because weight 2 is the lowest weight for which modular forms are cohomological, that is, weight 2 modular forms have trivial – or 'weight 0' – cohomological coefficients.

Let $f \in S_{k+2}(\Gamma, \mathbf{C})$. Then the computations above show that

$$f(\gamma z)d(\gamma z) = (cz+d)^k f(z)dz. \tag{10.1}$$

Thus the same definition of modular symbol does not work, as we no longer have invariance under the action of Γ. To fix this, we need to consider *modular symbols with coefficients*, so that we can kill the additional action of $(cz+d)^k$ through the coefficients.

Definition 10.10. — Let V be a right Γ-module. Then define an action of Γ on $\mathrm{Hom}(\Delta_0, V)$ by

$$\phi|\gamma\{r \to s\} = \phi\{\gamma r \to \gamma s\}|\gamma.$$

The space of *V-valued modular symbols for* Γ is

$$\mathrm{Symb}_\Gamma(V) := \mathrm{Hom}_\Gamma(\Delta_0, V).$$

The following turns out to be a good choice of V.

Definition 10.11. — For a commutative ring R, let $V_k(R)$ be the space of polynomials in X over R of degree $\leq k$.

Equivalently, we could see this as homogeneous polynomials in two variables X, Y of degree k, which can be identified with the symmetric kth power $\mathrm{Sym}^k(R^2)$. In this sense, it is apparent that this carries a plethora of natural actions of $\mathrm{GL}_2(R)$ through its actions on R^2. It is important for us to choose a very specific action, which will not be the most natural, but *will* translate into precisely cancelling the factor $(cz+d)^k$ from (10.1).

We will consider the function

$$\begin{aligned} \phi_f : \Delta_0 &\longrightarrow V_k(\mathbf{C}), \\ \{r \to s\} &\longmapsto \int_r^s f(z)(zX+1)^k dz. \end{aligned}$$

To equip $V_k(\mathbf{C})$ with an action that renders this Γ-invariant, we consider the polynomial $(zX+1)^k$, and compute that

$$\begin{aligned} (\gamma(z)X+1)^k &= \left(\frac{az+b}{cx+d}X+1\right)^k \\ &= \Big[(az+b)X + (cz+d)\Big]^k (cz+d)^{-k}. \end{aligned}$$

In particular, up to some action on X that we are yet to define, this cancels off the errant factor $(cz+d)^k$. To determine the action on X, note that ϕ_f is an element of $\mathrm{Symb}_\Gamma(V_k(\mathbf{C}))$ if and only if $\phi_f\{\gamma r \to \gamma s\} = \phi_f\{r \to s\}|\gamma^{-1}$ for all $\gamma \in \Gamma$. Our computations show that

$$\begin{aligned} \phi_f\{\gamma r \to \gamma s\} &= \int_{\gamma r}^{\gamma s} f(z)(zX+1)^k dz \\ &= \int_r^s f(\gamma z)(\gamma(z)X+1)^k d(\gamma z) \\ &= \int_r^s f(z)\Big[(az+b)X + (cz+d)\Big]^k dz \\ &= \int_r^s f(z)\Big[(aX+c)z + (bX+d)\Big]^k dz \end{aligned}$$

So γ^{-1} sends X to $aX+c$, and 1 to $bX+d$. Then γ should send X to $dX-c$, and 1 to $-bX+a$.

Definition 10.12. — Equip V_k with an action of $\mathrm{GL}_2(R)$ by

$$P\left|\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right.(X) = (-bX+a)^k P\left(\frac{dX-c}{-bX+a}\right).$$

From the way we've defined this action, the following is immediate.

Proposition 10.13. — *We have* $\phi_f \in \mathrm{Symb}_\Gamma(V_k(\mathbf{C}))$.

Moreover, we retain the connection to L-values: and indeed, we see a wider range L-values.

Proposition 10.14. — *We have*

$$\phi_f\{0\to\infty\} = \sum_{j=0}^{k}\binom{k}{j}\left[\frac{j!}{(-2\pi i)^{j+1}}\cdot L(f,j+1)\right]X^j \ \in V_k(\mathbf{C}).$$

Proof. — Expanding out $(zX+1)^k$, we obtain

$$\phi_f\{0\to\infty\} = \sum_{j=0}^{k}\binom{k}{j}\left[\int_0^\infty f(z)z^j dz\right]X^j.$$

The result follows from Corollary 9.19. □

Remark 10.15. — Unlike in Part I, when we considered values of the Riemann zeta function at negative integers, we see only a *finite* range of 'critical' values here namely, the values $s = j+1$ for $0 \leq j \leq k$. In particular, for weight 2 forms, the modular symbol sees only one value, namely $s = 1$. This is not surprising, and in fact tallies exactly with expectations surrounding these L-values going back to Deligne [**Del79**]. He predicted that any L-function that is *motivic* (which, conjecturally, is all L-functions) should admit a set J of *critical integers*, defined in terms of 'Euler factors at infinity', and a controlled set of complex *periods* such that the values of the L-function at $j \in J$ are algebraic multiples of one of the periods.

– In the case of the Riemann zeta function, the critical values are all the negative odd integers, and the period can be taken to be $1 \in \mathbf{C}$, since the values are already algebraic (in fact, rational).

– For a modular form of weight k, Deligne's conjecture translates into the statement that $J = \{j+1 : 0 \leq j \leq k\}$, and thus the modular symbol is seeing all of these critical values. In the next section, we use the modular symbol to show that these L-values are algebraic multiples of periods.

There are, naturally, analogous results computing the twisted L-values – in the critical strip – through values of the modular symbol. The following map Ev_χ is a direct generalisation of that given for trivial coefficients in Definition 10.7.

Definition 10.16. — Let χ be a Dirichlet character of conductor D. Define a twisting map

$$\mathrm{Symb}_\Gamma(V_k(\mathbf{C})) \longrightarrow \mathrm{Symb}_\Gamma(V_k(\mathbf{C}))$$

by

$$\phi \longmapsto \phi_\chi := \sum_{a\in(\mathbf{Z}/D\mathbf{Z})^\times}\chi(a)\phi\left|\begin{pmatrix}1 & a\\ 0 & D\end{pmatrix}\right..$$

Define the evaluation at χ map by

$$\begin{aligned}\mathrm{Ev}_\chi : \mathrm{Symb}_\Gamma(V_k(\mathbf{C})) &\longrightarrow V_k(\mathbf{C})\\ \phi &\longmapsto \phi_\chi\{0\to\infty\}\\ &= \sum_{a\in(\mathbf{Z}/D\mathbf{Z})^\times}\chi(a)\phi\left|\begin{pmatrix}1 & a\\ 0 & D\end{pmatrix}\right.\{0\to\infty\}.\end{aligned}$$

Remark 10.17. — This twisting map is very closely related to the one we defined on measures in [**RJW17**, §4]. Indeed, we relate the two twisting maps in §14 below.

We have the following.

Proposition 10.18. — *Let $f \in S_2(\Gamma, \mathbf{C})$, and $\chi : (\mathbf{Z}/D\mathbf{Z})^\times \to \overline{\mathbf{Q}}^\times$ be a Dirichlet character. Then*

$$\mathrm{Ev}_\chi(\phi_f) = \sum_{j=0}^{k} \binom{k}{j} \left[\frac{G(\chi)\cdot j!\cdot D^j}{(-2\pi i)^{j+1}} \cdot L(f, \overline{\chi}, j+1)\right] X^j.$$

Proof. — We compute:

$$\begin{aligned}
\phi_f \left| \begin{pmatrix} 1 & a \\ 0 & D \end{pmatrix} \{0 \to \infty\} \right. &= \phi_f \left\{\frac{a}{D} \to \infty\right\} \left| \begin{pmatrix} 1 & a \\ 0 & D \end{pmatrix} \right. \\
&= \left[\int_{a/D}^{\infty} f(z)(zX+1)^k dz\right] \left| \begin{pmatrix} 1 & a \\ 0 & D \end{pmatrix} \right. \\
&= \int_{a/D}^{\infty} f(z) \left(z\frac{DX}{-aX+1} + 1\right)^k (-aX+1)^k dz \\
&= \int_{a/D}^{\infty} f(z) \left(zDX + (-aX+1)\right)^k dz \\
&= \int_{a/D}^{\infty} f(z) \Big[(zD-a)X + 1\Big]^k dz \\
&= \sum_{j=0}^{k} \binom{k}{j} \left[\int_{a/D}^{\infty} f(z) \left((Dz-a)^j\right) dz\right] X^j \\
&= \sum_{j=0}^{k} \binom{k}{j} D^j \left[\int_{a/D}^{\infty} f(z) \left(z - \frac{a}{D}\right)^j dz\right] X^j.
\end{aligned}$$

Multiplying by $\chi(a)$ and summing over all $a \in (\mathbf{Z}/D\mathbf{Z})^\times$, then, the coefficient of X^j in $\mathrm{Ev}_\chi(\phi_f)$ is therefore

$$\begin{aligned}
&\binom{k}{j} D^j \sum_{a \in (\mathbf{Z}/D\mathbf{Z})^\times} \chi(a) \left[\int_{a/D}^{\infty} f(z) \left(z - \frac{a}{D}\right)^j dz\right] \\
&\qquad\qquad = \binom{k}{j} D^j \cdot \frac{G(\chi)\Gamma(j+1)}{(-2\pi i)^{j+1}} \cdot L(f, \overline{\chi}, j+1),
\end{aligned}$$

where the last equality follows from specialising Corollary 9.21 at $s = j+1$. $\square$

Definition 10.19. — We define

$$\mathrm{Ev}_{\chi,j} : \mathrm{Symb}_\Gamma(V_k(\mathbf{C})) \longrightarrow \mathbf{C}$$

to be the composition of Ev_χ, as defined in Definition 10.16, with projection to the jth co-ordinate.

In particular, we've shown:

Corollary 10.20. — *We have*

$$\mathrm{Ev}_{\chi,j}(\phi_f) = C_{\chi,j} \cdot L(f, \overline{\chi}, j+1),$$

where

$$C_{\chi,j} := \binom{k}{j} D^j \cdot \frac{G(\chi)\cdot j!}{(-2\pi i)^{j+1}}.$$

For later use, we summarise all of this in the following diagram:

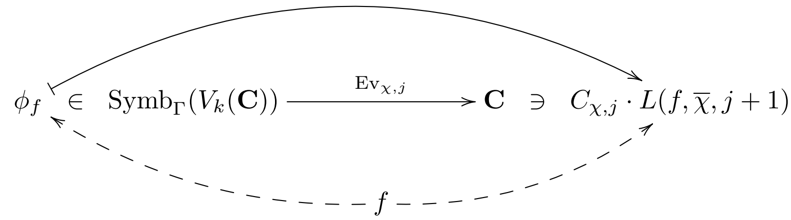

Figure 10.1. L-values from modular symbols: complex coefficients

11. Algebraicity of L-values

By analogy with the Kubota–Leopoldt p-adic L-function, to study the Iwasawa theory of a modular form we wish to construct a p-adic version of $L(f,s)$. The most natural generalisation is to look for a 'p-adic measure' $L_p(f)$ on $\mathbf{Z}_p^\times$ satisfying an interpolation property of the shape

$$\int_{\mathbf{Z}_p^\times} \chi(x)x^j \cdot L_p(f) = (*)L(f,\overline{\chi},j+1),$$

where $(*)$ is some explicit factor including Euler factors at p.

The values of this integral, however, will be p-adic numbers; and the L-function $L(f,s)$ is valued in $\mathbf{C}$. Whilst it is possible to fix an isomorphism $\mathbf{C} \cong \overline{\mathbf{Q}}_p$, to do so renders such an interpolation formula essentially meaningless from an arithmetic standing. Instead, we want to view the right-hand side *algebraically*. That this is possible is the main result of this section. In particular, we will explain the following theorem.

***Theorem 11.1* (Manin, Shimura).** — *Let $f \in S_{k+2}(\Gamma,\mathbf{C})$ be an eigenform. There exist complex periods $\Omega_f^+,\Omega_f^- \in \mathbf{C}^\times$ such that for any Dirichlet character χ, and any $0 \leq j \leq k$, we have*

$$\frac{L(f,\chi,j+1)}{(2\pi i)^{j+1}\cdot \Omega_f^\pm} \in \overline{\mathbf{Q}}.$$

Here the sign is determined by $\chi(-1)(-1)^j = \pm 1$.

In other words, at certain special values, the L-function can only be transcendental in a very controlled manner. It is then meaningful to p-adically interpolate the 'algebraic parts' of these L-values.

We will prove this first for newforms, where we have tight control on the dimensions of Hecke eigenspaces. At the end of the section we will describe the generalisation to arbitrary eigenforms via p-stabilisation.

Remark 11.2. — If we take the periods $\Omega_f^\pm$ to be defined by this property, then they are only well-defined as elements of $\mathbf{C}^\times/\overline{\mathbf{Q}}^\times$. The question of normalising these periods correctly is an important one, particularly for Iwasawa theory, where one is particularly interested in the p-adic valuation of the algebraic part of the L-value. Without further input, renormalising the period by an arbitrary power of p will change this p-adic valuation to any specified value, and render its study meaningless. Since the aim of these lectures is to *construct* $L_p(f)$, rather than describe its Iwasawa-theoretic properties, we will not look at this in detail.

When f is weight 2, and attached to an elliptic curve, then one may construct canonical periods $\Omega_f^\pm$ from the usual period of the elliptic curve.

11.1. Motivation: a proof strategy.

— We outline a strategy for the proof.

Assume first *that f is a newform.* Then by Theorem 9.9(iii), the Hecke eigenspace $S_{k+2}(\Gamma,\mathbf{C})[f]$ is one-dimensional; and normalising to have algebraic coefficients, the same is true of $S_{k+2}(\Gamma, F)[f]$, where $F \subset \mathbf{C}$ is any number field containing the Hecke field K_f over which the eigenpacket λ_f of f is defined.

$$\begin{array}{ccccccc} & \dashrightarrow & S_{k+2}(\Gamma,F)[f] & \overset{?}{\dashrightarrow} : & \mathrm{Symb}_\Gamma(V_k(F)) & \xrightarrow{\mathrm{Ev}_{\chi,j}} & \overline{\mathbf{Q}} \\ \text{1-dimensional} & & \cap & & \cap & & \\ & \dashrightarrow & S_{k+2}(\Gamma,\mathbf{C})[f] & \longrightarrow & \mathrm{Symb}_\Gamma(V_k(\mathbf{C})) & \xrightarrow{\mathrm{Ev}_{\chi,j}} & \mathbf{C} \end{array}$$

Now, suppose we could prove the same result for modular symbols; that is, that we could prove that for a natural Hecke action, we have

$$\dim_{\mathbf{C}}\mathrm{Symb}_\Gamma(V_k(\mathbf{C}))[f] \overset{?}{=} 1 \overset{?}{=} \dim_F \mathrm{Symb}_\Gamma(V_k(F))[f]. \tag{11.1}$$

One would hope that the $\mathbf{C}$-space is spanned by the canonical modular symbol ϕ_f we saw above. If we then choose a generator $\phi_{f,F}$ of the analogous F-space, then necessarily this is also in $\mathrm{Symb}_\Gamma(V_k(\mathbf{C}))$, and hence a complex multiple $\Omega_f^{-1} \cdot \phi_f$ of ϕ_f. In particular, we would then have

$$\mathrm{Ev}_{\chi,j}\left(\frac{\phi_f}{\Omega_f}\right) \sim \frac{L(f,\overline{\chi},j+1)}{(2\pi i)^{j+1}\Omega_f} \in \overline{\mathbf{Q}}.$$

In practice, however, (11.1) ***does not hold***, so this strategy does not work on the nose. Fortunately, it can be salvaged with a little modification: the spaces in (11.1) are each two-dimensional, decomposing into two one-dimensional $\pm$-eigenspaces under a natural involution ι. This is why we end up with *two* periods Ω_f^+, Ω_f^-, one for each ι-eigenspace, and a sign condition on the algebraicity result.

To enact this, we need the following ingredients:

– a Hecke action on modular symbols, for which $f \mapsto \phi_f$ is Hecke-equivariant;
– control on the size of $\mathrm{Symb}_\Gamma(V_k(\mathbf{C}))$ in terms of spaces of modular forms;
– both of the above steps to be defined with coefficients in a sufficiently large number field F.

These steps are the content of the *Eichler–Shimura isomorphism*. In the remainder of this section, we make all of this precise.

11.2. The Eichler–Shimura isomorphism. — We first describe the Hecke action on modular symbols. Each Hecke operator on modular forms has a double coset decomposition, which translates into the sum of the actions of a finite set of matrices. As each of these matrices is an element of the monoid $\Sigma_0(p)$, we can define their action on modular symbols as well; for example, we may define

$$\phi|U_p = \sum_{a=0}^{p-1} \phi \left| \begin{pmatrix} 1 & a \\ 0 & p \end{pmatrix} \right.,$$

and similarly for all the T_ℓ's.

Proposition 11.3. — *The map $f \mapsto \phi_f$ is Hecke equivariant.*

Proof. — This is another computation in change of variables. Recall the weight $k+2$ action of $\mathrm{GL}_2^+(\mathbf{Q})$ on modular forms is by $f|_k\gamma = \det^{k+1}(\gamma)(cz+d)^{-k-2}f(\gamma z)$. Let $\gamma = \left(\begin{smallmatrix} 1 & a \\ 0 & \ell \end{smallmatrix}\right)$ for some prime ℓ, then compute

$$\begin{aligned} \phi_{f|\gamma}\{r \to s\} &= \int_r^s (zX+1)^k f|_k\gamma dz \\ &= \int_r^s (zX+1)^k \ell^{k+1}(0z+\ell)^{-k-2} f\left(\frac{z+a}{\ell}\right) dz \\ &= \ell^{-1}\int_{\gamma r}^{\gamma s} ((\ell y - a)X+1)^k f(y)(\ell dy), \end{aligned}$$

under the substitution $y = \frac{z+a}{\ell}$, with $z = \ell y - a$ and $dz = \ell dy$. We further compute that

$$(yX+1)^k|\gamma = (1-aX)^k\left(y\frac{\ell X}{1-aX}+1\right)^k = ((\ell y - a)X+1)^k,$$

and substituting this in, our expression becomes

$$\begin{aligned} &= \left[\int_{\gamma r}^{\gamma s}(yX+1)^k f(y)dy\right]\Bigg|\gamma \\ &= \phi_f|\gamma\{r\to s\}. \end{aligned}$$

The U_p operator is comprised of a sum of matrices of this form, so we deduce that $\phi_{f|U_p} = \phi_f|U_p$. For the T_ℓ operator, it remains to check only the matrix $\left(\begin{smallmatrix}\ell & 0\\ 0 & 1\end{smallmatrix}\right)$. Let $\gamma = \left(\begin{smallmatrix}\ell & 0\\ 0 & 1\end{smallmatrix}\right)$; we check directly that

$$\begin{aligned} \phi_{f|\gamma}\{r\to s\} &= \int_r^s \ell^{k+1}f(\ell z)(zX+1)^k dz \\ &= \int_{\gamma r}^{\gamma s} f(y)\left[\ell^k\left(y\frac{X}{\ell}+1\right)^k\right]dy \\ &= \phi_f|\gamma\{r\to s\}, \end{aligned}$$

where we use that $P|\gamma(X) = \ell^k P(X/\ell)$. Thus $f\mapsto\phi_f$ is equivariant for each matrix used in the T_ℓ operator as well, and we conclude the desired Hecke equivariance. □

Remark 11.4. — In passing from f (an analytic object) to ϕ_f (a purely algebraic one) we are *a priori* throwing away all the analytic data. However, via its q-expansion and Theorem 9.10, one can always reconstruct f solely from the data of its Hecke eigenvalues. This Hecke-equivariance statement, therefore, can be summarised as saying 'no information is lost in discarding the analytic data': we can reconstruct f from its modular symbol ϕ_f.

This remark means that the map $f\mapsto\phi_f$ is injective. It is natural to ask if it is also surjective. This is not true, but it fails in a controlled manner. As well as the usual space of holomorphic cusp forms, we have modular symbols attached to:

– **Eisenstein series.** If f is an Eisenstein series, then the association $f\mapsto\phi_f$ above needs adapting, as we no longer have absolute convergence of the integrals $\int_r^s$. However, there is still an easily identified Eisenstein subspace in the space of modular symbols. In particular, consider the space $\mathrm{Hom}_\Gamma(\Delta, V_k(\mathbf{C}))$. As a $\mathbf{Z}[\Gamma]$-module, $\Delta = \mathrm{Div}(\mathbf{P}^1(\mathbf{Q}))$ is freely generated by the (finite set of) cusps of Γ, so any such homomorphism is just the data of an element of $V_k(\mathbf{C})$ at each cusp. There is a natural restriction map

$$\mathrm{res}: \mathrm{Hom}_\Gamma(\Delta, V_k(\mathbf{C})) \longrightarrow \mathrm{Hom}_\Gamma(\Delta_0, V_k(\mathbf{C})) = \mathrm{Symb}_\Gamma(V_k(\mathbf{C})),$$

where $\mathrm{res}(\phi)\{r\to s\} := \phi(s) - \phi(r)$. We define

$$\mathrm{BSymb}_\Gamma(V_k(\mathbf{C})) := \mathrm{Im}(\mathrm{res}) \subset \mathrm{Symb}_\Gamma(V_k(\mathbf{C})).$$

The space $\mathrm{BSymb}_\Gamma(V_k(\mathbf{C}))$ can be canonically and Hecke-equivariantly identified with the space of cusp forms of weight $k+2$ and level Γ (see [**Bel**, §III.2.8]); in line with the above, we write ϕ_g for the symbol corresponding to an Eisenstein series g.

– **Antiholomorphic cusp forms.** Every cusp form $f\in S_{k+2}(\Gamma,\mathbf{C})$ has an anti-holomorphic cousin $\overline{f}(z) := \overline{f(z)}$, its complex conjugate. We write $\overline{S_{k+2}}(\Gamma,\mathbf{C})$ for the space of antiholomorphic cusp forms. Each of these antiholomorphic cusp forms also gives a modular symbol $\phi_{\overline{f}}$ by

$$\phi_{\overline{f}}\{r\to s\} := \int_r^s \overline{f}(z)(\overline{z}X+1)^k d\overline{z},$$

and this association is again Hecke-equivariant for the natural Hecke action on $\overline{S_{k+2}}(\Gamma,\mathbf{C})$. Importantly, if f is a (holomorphic) Hecke eigenform, then $\overline{f}$ is also an eigenform, with the same Hecke eigenvalues.

Eichler–Shimura says that the space of modular symbols is exhausted by the contributions of (holomorphic) cusp forms, antiholomorphic cusp forms, and Eisenstein series.

***Theorem 11.5* (Eichler–Shimura).** — *There is a Hecke-equivariant isomorphism*

$$S_{k+2}(\Gamma, \mathbf{C}) \oplus \overline{S_{k+2}(\Gamma, \mathbf{C})} \oplus \mathcal{E}_{k+2}(\Gamma, \mathbf{C}) \cong \mathrm{Symb}_{\Gamma}(V_k(\mathbf{C}))$$

given by the map

$$(f, \overline{f}, g) \mapsto \phi_f + \phi_{\overline{f}} + \phi_g.$$

Proof. — This theorem is very important in the sequel, but its proof is quite involved, and takes us quite far from the p-adic L-functions we are aiming to study. Thus, in these notes, we give only a sketch of the proof. The main steps are as follows:

– Rephrase the theorem in cohomology. Let $Y_\Gamma := \Gamma\backslash\mathcal{H}$ denote the open modular curve. By [**AS86**], there is an isomorphism

$$\mathrm{Symb}_{\Gamma}(V_k(\mathbf{C})) \cong \mathrm{H}^1_{\mathrm{c}}(Y_\Gamma, V_k(\mathbf{C}))$$

between modular symbols and the compactly supported cohomology; this is proved using homological algebra, and identifying $\mathrm{Symb}_\Gamma(V)$ with the degree 0 group cohomology $\mathrm{H}^0(\Gamma, \mathrm{Hom}(\Delta_0, V))$.

– Recall the the Petersson product on modular forms. There is also a natural cup product pairing

$$\mathrm{H}^1_{\mathrm{c}}(Y_\Gamma, V_k(\mathbf{C})) \times \mathrm{H}^1(Y_\Gamma, V_k(\mathbf{C})) \to \mathbf{C}.$$

One finds an explicit relationship between these two pairings.

– Use the relationship between the two pairings, and the properties of the Petersson product, to show that the map is injective.

– Show that both sides have the same dimension, using standard dimension results in the theory of modular forms (for the left-hand side) and algebraic topology (for the right-hand side). Such formulae involve topological invariants of Y_Γ, for example the genus. □

11.3. Plus-minus spaces.

— Let first $f \in S_{k+2}(\Gamma, \mathbf{C})$ be a newform.

Definition 11.6. — Let $\lambda_f : \mathbf{H}_N \to F \subset \mathbf{C}$ be the eigenpacket attached to f. If M is a space with an action of the Hecke algebra $\mathbf{H}_N$, then recall we write

$$\begin{aligned} M[f] &= f\text{-eigenspace of } \mathbf{H}_N \text{ inside } M \\ &= \{m \in M : Tm = \lambda_f(T)m \text{ for all } T \in \mathbf{H}_N\}. \end{aligned}$$

In particular, Theorem 9.9(3) is the statement that

$$\dim_{\mathbf{C}} S_{k+2}(\Gamma, \mathbf{C})[f] = 1 = \dim_{\mathbf{C}} \overline{S_{k+2}}(\Gamma, \mathbf{C})[f], \tag{11.2}$$

where the last equality follows from the fact that f and its antiholomorphic cousin $\overline{f}$ have the same Hecke eigenvalues.

Proposition 11.7. — *We have*

$$\dim_{\mathbf{C}} \mathrm{Symb}_{\Gamma}(V_k(\mathbf{C}))[f] = 2.$$

Proof. — Under Corollary 11.5, we may identify this space with $S_{k+2}(\Gamma, \mathbf{C}) \oplus \overline{S_{k+2}}(\Gamma, \mathbf{C}) \oplus \mathcal{E}_{k+2}(\Gamma, \mathbf{C})$. The eigenpacket λ_f cannot occur in $\mathcal{E}_{k+2}(\Gamma, \mathbf{C})$, since the T_ℓ-eigenvalue of an Eisenstein series at a prime ℓ is of size approximately ℓ^k, whilst for cusp forms, we have the estimate $a_\ell(f) \leq C\ell^{k/2}$ of Lemma 9.15. It appears exactly once in both $S_{k+2}(\Gamma, \mathbf{C})$ and $\overline{S_{k+2}}(\Gamma, \mathbf{C})$ by (11.2), and hence in the space of symbols with multiplicity two. □

We cut this down to a direct sum of two 1-dimensional eigenspaces with the action of a natural involution.

Definition 11.8. — Let ι be the involution given by the action of $\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$ on $\mathrm{Symb}_\Gamma(V_k(\mathbf{C}))$. Note that

$$\iota = [\Gamma \left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right) \Gamma]$$

has the structure of a double coset operator for Γ, and hence ι commutes with the Hecke algebra $\mathbf{H}_N$.

Proposition 11.9. — *We have a Hecke-stable decomposition*

$$\mathrm{Symb}_\Gamma(V_k(\mathbf{C})) \cong \mathrm{Symb}_\Gamma^+(V_k(\mathbf{C})) \oplus \mathrm{Symb}_\Gamma^-(V_k(\mathbf{C}))$$

into the ± 1 *eigenspaces of the involution* ι.

Proof. — Attached to ι, we have projectors $\frac{1\pm\iota}{2}$ which naturally land in the ±1-eigenspaces. This induces the required direct sum decomposition. □

Note that it is not immediately obvious that both components are non-zero at f.

11.4. Connection to L-values. — Recall Proposition 10.14, where we derived the expression

$$\phi_f\{0 \to \infty\} = \sum_{j=0}^{k} \binom{k}{j} \left[\frac{j!}{(-2\pi i)^{j+1}} L(f, j+1)\right] X^j. \tag{11.3}$$

This also decomposes under the involution ι. Let

$$\phi_f^{\pm} := \frac{\iota \pm 1}{2}(\phi_f),$$

so that $\phi_f = \phi_f^+ + \phi_f^- \in \mathrm{Symb}_\Gamma^+(V_k(\mathbf{C})) \oplus \mathrm{Symb}_\Gamma^-(V_k(\mathbf{C}))$.

Proposition 11.10. — *We have*

$$\phi_f^+\{0 \to \infty\} = \sum_{\substack{j=0\\ j \text{ even}}}^{k} \binom{k}{j} \left[\frac{j!}{(-2\pi i)^{j+1}} L(f, j+1)\right] X^j.$$

Similarly, $\phi_f^-\{0 \to \infty\}$ *is the sum of the terms in* (11.3) *for* j *odd.*

Proof. — The involution ι fixes both 0 and ∞, and acts on polynomials by sending

$$X^j|\iota := X^j \left| \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} \right. = (-1)^j X^j.$$

It follows that $\frac{\iota\pm1}{2}$ acts as the identity on the terms X^j where $(-1)^j = \pm1$, and 0 on others, from which the proposition follows immediately. □

As usual, we have an analogous statement for twisted L-values, which (as ever) makes a good exercise. The below should be compared to Proposition 10.18 and Corollary 10.20.

Proposition 11.11. — *Let* $\chi : (\mathbf{Z}/D\mathbf{Z})^\times \to \overline{\mathbf{Q}}^\times$ *be a Dirichlet character of conductor* D, *and let* $0 \leq j \leq k$. *Then*

$$\mathrm{Ev}_\chi(\phi_f^\pm) = \sum_{\substack{j=0\\ \chi(-1)(-1)^j = \pm1}}^{k} \binom{k}{j} \left[\frac{G(\chi)\cdot j! \cdot D^j}{(-2\pi i)^{j+1}} \cdot L(f, \overline{\chi}, j+1)\right] X^j.$$

In particular, for $C_{\chi,j}$ *as in Corollary 10.20, we see that*

$$\mathrm{Ev}_{\chi,j}(\phi_f^\pm) = \begin{cases} C_{\chi,j}\cdot L(f,\overline{\chi}, j+1) & : \chi(-1)(-1)^j = \pm1\\ 0 & : \textit{else}. \end{cases}$$

Proof. — This is a straightforward calculation. Note that $\iota \cdot a/D = -a/D$. Thus in the calculations that go into the proof of Proposition 10.18, one brings out a factor of $\chi(-1)$ to obtain $\chi(-a/D)$ in the sum, rescaling the choice of representatives for $(\mathbf{Z}/D\mathbf{Z})^\times$. When combined with the action of ι on X^j described above, we find that

$$\text{coefficient of } X^j \text{ in } \mathrm{Ev}_\chi(\phi|\iota) = \chi(-1)(-1)^j \times \text{ coefficient of } X^j \text{ in } \mathrm{Ev}_\chi(\phi).$$

In particular, the projector $\mathrm{pr}^\pm$ acts as the identity on the coefficients where $\chi(-1)(-1)^j = \pm 1$, and kills the others. □

Corollary 11.12. — *For each sign, we have*

$$\dim_{\mathbf{C}} \mathrm{Symb}_\Gamma^\pm(V_k(\mathbf{C}))[f] = 1.$$

Proof. — A theorem of Rohrlich [**Roh91**] says that for all but finitely many Dirichlet characters χ, the L-value

$$L(f, \overline{\chi}, 1) \neq 0.$$

In particular, there exists at *least* one even χ and one odd χ with this non-vanishing property. But if χ is even (resp. odd), then a non-zero multiple of $L(f, \overline{\chi}, 1)$ appears as the coefficient of $\mathrm{Ev}_\chi(\phi_f^+)$, a sum of values of ϕ_f^+ (resp. ϕ_f^-). It follows that $\phi_f^\pm \neq 0$ for both choices of sign. We then conclude since they live in a 2-dimensional ambient space which is the direct sum of the $\pm$-eigenspaces of ι. □

Remark 11.13. — Rohrlich's theorem is a deep result in analytic number theory. If the weight $k+2$ of f is at least 4, then there is a proof that doesn't invoke this. Indeed, in this case the value $L(f, \overline{\chi}, k+1)$ appears as a linear combination of values of ϕ_f. But this is in the region of absolute convergence for the L-function, where we have the Euler product, which converges absolutely to a non-zero value. We then deduce $\phi_f^\pm \neq 0$ as before.

11.5. Eichler–Shimura with algebraic coefficients. — In all of the above, we worked with complex coefficients. We saw in the previous sections that there is a natural algebraic structure on the space of modular forms by looking at q-expansions with algebraic coefficients, and moreover that there exists a number field $F/\mathbf{Q}$ such that

$$M_{k+2}(\Gamma, \mathbf{C}) \cong M_{k+2}(\Gamma, F) \otimes_F \mathbf{C}, \tag{11.4}$$

with the Hecke action defined over F. There is also a natural algebraic structure on modular symbols: we can simply take modular symbols with coefficients in $V_k(F)$. We have the analogy of (11.4) for modular symbols.

***Proposition 11.14* (Shimura).** — *There is a (Hecke-equivariant) isomorphism*

$$\mathrm{Symb}_\Gamma(V_k(F)) \otimes_F \mathbf{C} \cong \mathrm{Symb}_\Gamma(V_k(\mathbf{C})).$$

Remark 11.15. — We omit the proof; this is proved, for example, in [**Hid88**, §7] and [**Hid94**, §8].

Note that this is *not* automatic without appealing to deeper results in algebraic geometry. We have seen that there are canonical one-dimensional Hecke-stable subspaces $\mathrm{Symb}_\Gamma^\pm(V_k(\mathbf{C}))[f]$ attached to f, and moreover we know that the eigenpacket $\lambda : \mathbf{H}_N \to F \subset \mathbf{C}$ takes values in F. It follows easily that we can exhibit a (non-canonical) F-rational structure on $\mathrm{Symb}_\Gamma^\pm(V_k(\mathbf{C}))$; this is purely a linear algebra statement on the abstract vector spaces. Sometimes, it is claimed that this rational structure then coincides with the space $\mathrm{Symb}_\Gamma^\pm(V_k(F))[f]$. To this author, however, this appears far from obvious without further (cohomological) input.

As an example of this, suppose we are in the weight 3 situation, so that we consider the space $\mathrm{Symb}_\Gamma(\mathbf{C}X \oplus \mathbf{C})$. As the complex Eichler–Shimura isomorphism is Hecke-equivariant, the modular symbol ϕ_f attached to any eigenform f is an eigensymbol, and hence the F-line $F \cdot \phi_f$ is preserved by the Hecke operators. We may always scale ϕ_f by a complex scalar such that, for example, $\phi_f\{0 \to \infty\} = aX + b$, with $a \in F$. This process does not *a priori* also control b, however, which without further input may by horribly transcendental. In addition, it says nothing about the other values $\phi_f\{r \to s\}$. It may be possible to say something directly using symmetries under Γ and the Hecke action, but this quickly becomes a fiddly exercise without much conceptual basis.

One may fix this by instead arguing on the identification of modular symbols with cohomology mentioned above. One can prove that the Hecke algebra is naturally dual to modular forms, and also – via complex Eichler–Shimura – to modular symbols. From the study of modular forms, we obtain an F-rational structure on the Hecke algebra, and we may then transfer this to the cohomology, showing that the rational structure outlined above *does* coincide with the F-rational modular symbols. This is the approach taken in the references given above. Alternatively, one may observe that the modular curve has a model over $\mathbf{Q}$ (as in [**DS05**, §7], and hence its cohomology admits $\mathbf{Q}$-rational structure; so $\mathrm{Symb}_\Gamma(V_k(\mathbf{C}))$ admits a $\mathbf{C}$-basis of modular symbols valued in $V_k(\mathbf{Q})$ (though this will *not* in general be a basis of eigensymbols).

Allowing the proposition, we can descend Eichler–Shimura to algebraic coefficients. The argument from here now proceeds via elementary linear algebra.

Lemma 11.16. — *Let M and N be F-vector spaces with actions of the Hecke algebra $\mathbf{H}$. Suppose that $M \otimes_F \mathbf{C} \cong N \otimes_F \mathbf{C}$ as $\mathbf{H}$-modules. Then*

$$M \cong N$$

(non-canonically) as $\mathbf{H}$-modules.

Proof. — Choose bases for M and N over F. A linear map $M \to N$ is determined by its matrix (x_{ij}) in these bases, and since the Hecke action is defined over F (even $\mathbf{Q}$), the x_{ij} are elements of F. Then:

– the statement 'the map is an isomorphism' is determined by a linear equation in the x_{ij} (for example, $\det \neq 0$ for M, N finite dimensional of the same dimension),
– and for each $T \in \mathbf{H}$, the statement 'the map is T-equivariant' cuts out another linear equation in the x_{ij}.

The hypothesis that $M \otimes_F \mathbf{C} \cong N \otimes_F \mathbf{C}$ implies this this system of equations has a simultaneous solution over $\mathbf{C}$. But since every equation in this system is defined over F, this implies there exists a solution (x_{ij}) with each $x_{ij} \in F$; and then by construction the map (x_{ij}) defines the required $\mathbf{H}$-equivariant isomorphism. □

Applying this with M and N the F-rational structures on modular forms and modular symbols respectively, with the $\mathbf{H}_N$-module isomorphism on the complexifications given by Theorem 11.5, we obtain the following.

Corollary 11.17. — *There is a Hecke-equivariant isomorphism*

$$S_{k+2}(\Gamma, F) \oplus \overline{S_{k+2}(\Gamma, F)} \oplus \mathcal{E}_{k+2}(\Gamma, F) \cong \mathrm{Symb}_\Gamma(V_k(F)).$$

Note, however, that this map is now *non-canonical.* This non-canonicity will manifest itself in an ambiguity in complex periods in the next section.

11.6. Periods and algebraic modular symbols for newforms. — The algebraic Eichler–Shimura isomorphism shows that all of the dimension results of §11.3 descend to algebraic coefficients. In particular, we have the following analogue of Corollary 11.12, from which we can enact the strategy of §11.1.

Proposition 11.18. — *For each sign, for the newform f we have*

$$\dim_F \mathrm{Symb}_\Gamma^\pm(V_k(F))[f] = 1.$$

Let $\phi_{f,F}^\pm$ be generators of these two 1-dimensional vector spaces. These are non-canonical, well-defined only up to multiplication by an element of $F^\times$. We clearly have an inclusion

$$\mathrm{Symb}_\Gamma^\pm(V_k(F)) \subset \mathrm{Symb}_\Gamma^\pm(V_k(\mathbf{C})),$$

of 1-dimensional vector spaces, with the F-valued modular symbols spanning an F-line inside $\mathbf{C}$ (see Figure 11.1). In this larger $\mathbf{C}$-space, we have canonical generators, namely $\phi_f^\pm$, the $\pm$-classes projected from the canonical class ϕ_f. As any element of $\mathrm{Symb}_\Gamma^\pm(V_k(F))$ is then in the $\mathbf{C}$-span of $\phi_f^\pm$, we deduce that there exist $\Omega_f^\pm \in \mathbf{C}^\times$ such that

$$\phi_{f,F}^\pm = \frac{\phi_f^\pm}{\Omega_f^\pm} \in \mathrm{Symb}_\Gamma^\pm(V_k(F)).$$

We call the $\Omega_f^\pm$ the $\pm$-*periods* of f.

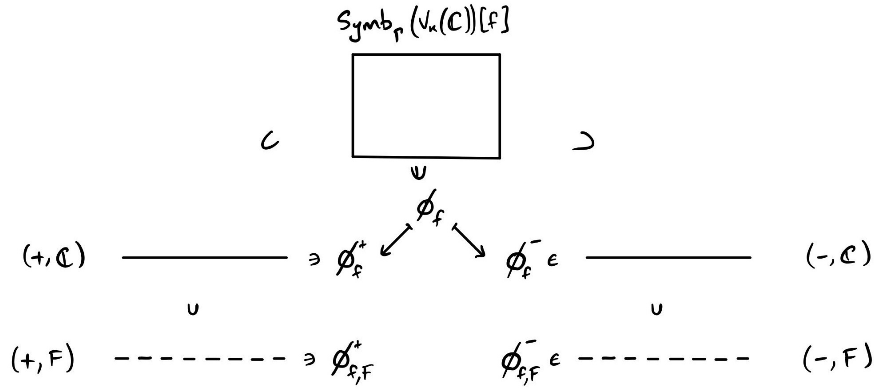

FIGURE 11.1. *Algebraic structures on modular symbols*

We summarise this discussion in the following proposition.

Proposition 11.19. — *For any field $F \subset \mathbf{C}$ containing the Hecke field K_f of the newform f, there exist complex periods $\Omega_f^\pm \in \mathbf{C}^\times$, well-defined up to multiplication by $F^\times$, such that*

$$\frac{\phi_f^\pm}{\Omega_f^\pm} \in \mathrm{Symb}_\Gamma^\pm(V_k(F)).$$

11.7. Algebraic modular symbols for general eigenforms. — Let now $f \in S_{k+2}(\Gamma_0(N))$ be an arbitrary eigenform; we wish to deduce an analogue of this for f. From the general theory of eigenforms, there exists a unique newform $g \in S_{k+2}(\Gamma_0(M))$ (furnished by [**DS05**, Prop. 5.8.4] for some $M|N$ such that f is a linear combination of modular forms of the form $g(mz)$, where m is a divisor of N/M (via [**DS05**, Thm. 5.8.3]).

Proposition 11.20. — *The modular symbol attached to the modular form $h_m(z) := g(mz)$ is*

$$\phi_{h_m} := m^{-k-1}\phi_g \,|\left(\begin{smallmatrix} m & 0 \\ 0 & 1\end{smallmatrix}\right)$$

Proof. — We have $h_m(z) = g(mz) = m^{-k-1}g|\left(\begin{smallmatrix} m & 0 \\ 0 & 1\end{smallmatrix}\right)(z)$. But we already showed in the proof of Proposition 11.3 that the association $g \mapsto \phi_g$ is equivariant for the action of $\left(\begin{smallmatrix} m & 0 \\ 0 & 1\end{smallmatrix}\right)$ on both sides, from which the result follows immediately. □

Let $\varphi_g^\pm := \phi_f^\pm/\Omega_f^\pm \in \mathrm{Symb}_{\Gamma_0(M)}^\pm(V_k(F))$ be the algebraic symbols given by Proposition 11.19. We may trivially consider these symbols as elements of the space $\mathrm{Symb}_\Gamma^\pm(V_k(F))$. Then for any m dividing N/M, attached to $h_m(z) = g(mz)$ we have

$$\frac{\phi_{h_m}^\pm}{\Omega_g^\pm} = \frac{m^{-k-1}\cdot\phi_g^\pm|\left(\begin{smallmatrix} m & 0 \\ 0 & 1\end{smallmatrix}\right)}{\Omega_g^\pm} \in \mathrm{Symb}_\Gamma^\pm(V_k(F)).$$

Write $f = \sum_{m|(N/M)} A_m h_m$ as a linear combination of the h_m's. After possibly renormalising, it is always possible to take the A_m's to be algebraic; and we may enlarge F to contain them. Then:

$$\frac{\phi_f^{\pm}}{\Omega_g^{\pm}} = \sum_{m|(N/M)} A_m \frac{\phi_{h_m}^{\pm}}{\Omega_g^{\pm}} \in \mathrm{Symb}_\Gamma(V_k(F)).$$

So we may define $\Omega_f^{\pm} := \Omega_g^{\pm}$ to be the periods of the associated newform, after which we obtain:

Proposition 11.21. — *Let f be an eigenform. There exists a sufficiently large number field F and complex periods $\Omega_f^{\pm} \in \mathbf{C}^\times$, well-defined up to multiplication by $F^\times$, such that*

$$\frac{\phi_f^{\pm}}{\Omega_f^{\pm}} \in \mathrm{Symb}_\Gamma^{\pm}(V_k(F)).$$

11.8. Algebraicity of L-values. — We are finally in a position to prove Shimura's theorem.

Proof. — *(Theorem 11.1).* Let χ be a Dirichlet character of conductor D, and let $0 \leq j \leq k$, as in the statement of Theorem 11.1. Let $F(\chi)$ be the finite field extension of F obtained by adjoining the values of χ (which will all be roots of unity, since χ has order dividing the totient $\phi(D)$).

Recall the map $\mathrm{Ev}_{\chi,j}$ from Definitions 10.16 and 10.19. These were composed of a 'twist by χ' map, then evaluation at $\{0 \to \infty\}$, then projection to the jth co-ordinate. In particular, if ϕ is valued in $V_k(F)$, then

$$\mathrm{Ev}_\chi(\phi) \in V_k(F(\chi)), \qquad \text{and} \qquad \mathrm{Ev}_{\chi,j}(\phi) \in F(\chi).$$

We end up with the following commutative diagram:

$$\begin{array}{cccccc} \mathrm{Ev}_{\chi,j}: & \mathrm{Symb}_\Gamma^{\pm}(V_k(\mathbf{C})) & \xrightarrow{\mathrm{Ev}_\chi} & V_k(\mathbf{C}) & \xrightarrow{j\text{th coeff}} & \mathbf{C} \\ & \cup & & \cup & & \cup \\ \mathrm{Ev}_{\chi,j}: & \mathrm{Symb}_\Gamma^{\pm}(V_k(F)) & \xrightarrow{\mathrm{Ev}_\chi} & V_k(F(\chi)) & \xrightarrow{j\text{th coeff}} & F(\chi). \end{array}$$

By Proposition 11.11, we know that

$$\mathrm{Ev}_{\chi,j}(\phi_f^{\pm}) = \binom{k}{j} D^j \cdot \frac{G(\chi)\Gamma(j+1)}{(-2\pi i)^{j+1}} \cdot L(f, \overline{\chi}, j+1)$$

if $\chi(-1)(-1)^j = \pm 1$ (and is equal to 0 otherwise). Since $\phi_f^{\pm}/\Omega_f^{\pm} \in \mathrm{Symb}_\Gamma^{\pm}(V_k(F))$, we deduce that when this sign condition is satisfied, we have

$$\begin{aligned} \mathrm{Ev}_{\chi,j}\left(\frac{\phi_f^{\pm}}{\Omega_f^{\pm}}\right) &= \frac{\mathrm{Ev}_{\chi,j}(\phi_f^{\pm})}{\Omega_f^{\pm}} \\ &= \binom{k}{j} D^j \cdot \frac{G(\chi)\Gamma(j+1)}{(-2\pi i)^{j+1}} \cdot \frac{L(f,\overline{\chi}, j+1)}{\Omega_f^{\pm}} \in F(\chi) \subset \overline{\mathbf{Q}}. \end{aligned}$$

All of the terms in the interpolating factor are algebraic except $(-2\pi i)^{j+1}$ and possibly $\Omega_f^{\pm}$, from which we deduce that

$$\frac{L(f,\overline{\chi}, j+1)}{(2\pi i)^{j+1} \cdot \Omega_f^{\pm}} \in \overline{\mathbf{Q}},$$

as required. (We may always swap χ and $\overline{\chi} = \chi^{-1}$ to get the stated formulation). □

Unlike the complex modular symbol ϕ_f, the algebraic modular symbols ϕ_f^+/Ω_f^+ and ϕ_f^-/Ω_f^- each only see *half* of the critical values. We rectify this by defining:

Definition 11.22. — Define

$$\varphi_f := \frac{\phi_f^+}{\Omega_f^+} + \frac{\phi_f^-}{\Omega_f^-} \in \mathrm{Symb}_\Gamma(V_k(F)).$$

From Proposition 11.11, we immediately have

$$\mathrm{Ev}_{\chi,j}(\varphi_f) = C_{\chi,j} \cdot \frac{L(f,\overline{\chi},j+1)}{\Omega_f^\pm},$$

where the sign of the period is determined by $\chi(-1)(-1)^j = \pm 1$. The left-hand side now has no dependence on the sign: that is, φ_f is algebraic and sees all the critical values, regardless of sign. The following algebraic version of Figure 10.1 is then the starting point for the p-adic theory.

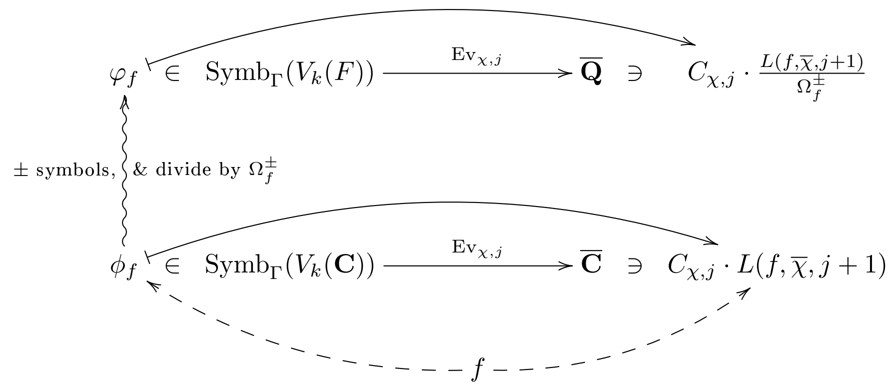

FIGURE 11.2. L-values from modular symbols: algebraic coefficients

Interlude: a change of language

As we saw in [**RJW17**] – where we frequently switched between measures and power series – it sometimes pays to change the language in which you consider an Iwasawa-theoretic problem. As a stand-alone theory, it makes far more sense to introduce modular symbols to be valued in polynomials, as we did above. However, in the context of overconvergent modular symbols and p-adic L-functions, it is more convenient to take the *dual* approach.

Ultimately, our aim is to construct a p-adic "measure"(2) $L_p(f)$ – a function on characters of the form $x \mapsto \chi(x)x^j$ – that interpolates the algebraic L-values above, that is, such that

$$L_p(f,j) = \int_{\mathbf{Z}_p^\times} \chi(x)x^k \cdot L_p(f) = (*)\frac{L(f,\overline{\chi},j+1)}{(2\pi i)^{j+1}\Omega_f^\pm}$$

for all χ of p-power conductor, and for all $0 \leq j \leq k$, where $(*)$ is an explicit algebraic constant (of the form we are already seeing arising in integral formulae).

In this sense, we want:

– an element *dual* to functions,
– such that the measure of z^j – the jth *moment* – computes the L-value at $j+1$.

Currently, our modular symbols are valued in $V_k(F)$, namely:

– a module of (polynomial) functions,
– such that the jth *coefficient* computes the L-value at j.

(2)In fact, the space of measures is not big enough to contain $L_p(f)$ in general, and we must pass to the space of p-adic *distributions*, which we introduce in the next section.

Our change of perspective is to replace $V_k(F)$ with its dual space.

Definition 11.23. — Let $\mathcal{V}_k(R)$ be the space of polynomials over R of degree at most k, with a new (left) action of Γ defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot P(X) = (a+cX)^k P\left(\frac{b+dX}{a+cX}\right).$$

Denote the dual space by

$$\mathcal{V}_k^\vee(R) := \mathrm{Hom}(\mathcal{V}_k(R), R),$$

with the dual right action given by

$$\mu|\gamma(P) := \mu(\gamma \cdot P).$$

This is a space of "polynomial measures".

Note that $\mathcal{V}_k^\vee(F)$ has the (dual) basis $\{\mathcal{X}^j : 0 \leq j \leq k\}$, where $\mathcal{X}^j$ is defined on monomials by

$$\mathcal{X}^j : X^i \mapsto \begin{cases} 1 & : i = j \\ 0 & i \neq j. \end{cases}$$

Lemma 11.24. — *There is an isomorphism*

$$\begin{aligned} \eta : V_k(F) &\xrightarrow{\sim} \mathcal{V}_k^\vee(F) \\ (-1)^j \binom{k}{j} X^j &\longmapsto \mathcal{X}^j \end{aligned}$$

of $\mathrm{GL}_2(F)$*-modules.*

Proof. — The map is obviously an isomorphism of F-vector spaces, so the content of this lemma is entirely in the equivariance of the $\mathrm{GL}_2(F)$-action. One can check this explicitly, for which we give only a simple example by way of illustration. Note that

$$\begin{aligned} \mathcal{X}^j \left| \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right. (X^i) &= \mathcal{X}^j\left((X+1)^i\right) \\ &= \sum_{n=0}^{i} \binom{i}{n} \mathcal{X}^j(X^n) = \binom{i}{j}, \end{aligned} \tag{11.5}$$

so that

$$\mathcal{X}^j \left| \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right. = \sum_{i=j}^{k} \binom{i}{j} \mathcal{X}^i.$$

We also have

$$\begin{aligned} (-1)^j \binom{k}{j} X^j \left| \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right. &= (-1)^j (X-1)^{k-j} X^j \\ &= (-1)^j \binom{k}{j} \sum_{n=0}^{k-j} \binom{k-j}{n} (-1)^{k-j-n} X^{n+j} \\ &= \sum_{i=j}^{k} (-1)^i \binom{k}{i} \binom{i}{j} X^i, \end{aligned} \tag{11.6}$$

where we have used the identity

$$\binom{k}{j}\binom{k-j}{i-j} = \binom{k}{i}\binom{i}{j}$$

in the final step. Under the stated map, (11.6) is sent to (11.5). The general case is similar, just keeping track of additional notation. □

In particular, under this isomorphism we have

$$[j\text{th coefficient of a polynomial } P] = \int X^j \cdot \eta(P).$$

This is visibly closer to our goal. Putting this into the context of modular symbols, we obtain:

Corollary 11.25. — *There is an isomorphism*

$$\eta : \mathrm{Symb}_\Gamma(V_k(F)) \cong \mathrm{Symb}_\Gamma(\mathcal{V}_k^\vee(F))$$

of Hecke-modules, and

$$\int X^j \cdot \eta(\varphi_f)\{0 \to \infty\} = -\frac{j!}{(2\pi i)^{j+1}} \cdot \frac{L(f, j+1)}{\Omega_f^\pm}.$$

Note in particular that as a consequence of this change of language, we have killed the binomial coefficient from the integral formula of Proposition 10.14, as well as (most of) the sign. (The remaining -1 is simply a matter of convention).

From now on:

– we switch notation and replace φ_f with its image $\eta(\varphi_f) \in \mathrm{Symb}_\Gamma(\mathcal{V}_k^\vee(F))$,
– and we redefine

$$\begin{aligned}\mathrm{Ev}_{\chi,j} : \mathrm{Symb}_\Gamma(\mathcal{V}_k^\vee(F)) &\xrightarrow{\varphi \mapsto \varphi_\chi} \mathrm{Symb}_\Gamma(\mathcal{V}_k^\vee(F(\chi)))\\ &\xrightarrow{\{0\to\infty\}} \mathcal{V}_k^\vee(F(\chi))\\ &\xrightarrow{\int z^j} F(\chi).\end{aligned}$$

Corollary 11.26. — *If χ is a Dirichlet character of conductor D, then*

$$\mathrm{Ev}_{\chi,j}(\varphi_f) = \mathcal{C}_{\chi,j} \cdot L(f, \overline{\chi}, j+1),$$

where

$$\mathcal{C}_{\chi,j} = \frac{G(\chi) \cdot j! \cdot D^j}{(2\pi i)^{j+1}\Omega_f^\pm}.$$

There is still a glaring problem to overcome: we cannot compute beyond the kth moment. In the case of GL(1), only when we passed to full measures on $\mathbf{Z}_p$ did we see the correspondence to power series, to local units, and ultimately the statement of the Iwasawa main conjecture. To obtain analogues here, we must rigidify further with p-adic analysis.

12. Overconvergent modular symbols

Let $L/\mathbf{Q}_p$ be a finite extension that contains all possible embeddings of F. We write $\mathcal{O}$ for the ring of integers in L. Henceforth, we consider φ_f as an element of $\mathrm{Symb}_\Gamma(\mathcal{V}_k^\vee(L))$.

We are aiming to construct the element $L_p(f)$ at the top right of the diagram below.

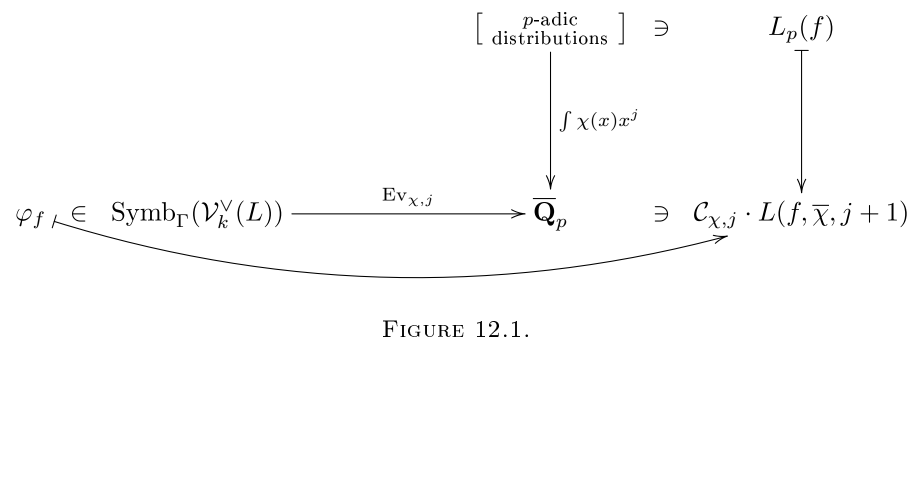

FIGURE 12.1.

The idea behind overconvergent modular symbols, as introduced by Glenn Stevens in [**Ste94**], is to instead produce the analogous objects on the *left-hand* side of the diagram, 'interpolating' the spaces of modular symbols and the maps $\mathrm{Ev}_{\chi,j}$.

12.1. Analytic distributions. — To access higher moments, we pass from polynomial functions to power series.

Definition 12.1. — A function $\psi : \mathbf{Z}_p \to L$ is *rigid analytic* if we can write

$$\psi(x) = \sum_{n\geq 1} a_n x^n$$

with $a_n \in L$ tending to zero as $n \to \infty$; equivalently, it is a power series that converges on $\mathbf{Z}_p$. We write $\mathbf{A}(L) = \mathbf{A}(\mathbf{Z}_p, L)$ for the space of rigid analytic functions $\mathbf{Z}_p \to L$.

The space $\mathbf{A}(L)$ is a Banach space over L, where the norm of f is the supremum of $|f(x)|$ as x varies over the closed unit ball in $\mathbf{C}_p$ (upon which f converges by definition). We explore this in much more detail in §15.

Note that $\mathcal{V}_k(L)$ is contained in $\mathbf{A}(L)$ for all positive integers k; so this is the analytic version of the module V_k. Dually, we get the following analytic version of $\mathcal{V}_k^\vee$.

Definition 12.2. — A *rigid analytic distribution* is a continuous homomorphism

$$\mu : \mathbf{A}(L) \longrightarrow L.$$

We write $\mathbf{D}(L) = \mathbf{D}(\mathbf{Z}_p, L) = \mathrm{Hom}_{\mathrm{cts}}(\mathbf{A}(L), L)$.

Notation 12.3. — The coefficient field does not play a major role in the construction, and we sometimes drop it from the notation. Where we write $\mathbf{A}(L)$ or $\mathbf{D}(L)$ without specifying the domain, these are always functions or distributions on $\mathbf{Z}_p$.

Remarks 12.4. — (1) Note that any rigid analytic function on $\mathbf{Z}_p$ is continuous, and hence any measure $\mu \in \mathscr{M}(\mathbf{Z}_p, L)$ defines a rigid analytic distribution by restriction. Moreover, this restriction is injective, as $x^j \in \mathbf{A}(\mathbf{Z}_p, L)$ for all j, and we have seen that a measure is totally determined by its moments $\int x^j \cdot \mu$. Thus there is an inclusion

$$\mathscr{M}(\mathbf{Z}_p, L) \subset \mathbf{D}(\mathbf{Z}_p, L),$$

and the space of rigid analytic distributions is a huge space generalising the notion of measures.

(2) If $\mu \in \mathbf{D}(\mathbf{Z}_p, L)$, then since the binomial polynomials are rigid analytic, we may take the Amice transform

$$\mathscr{A}_\mu(T) = \int_{\mathbf{Z}_p} (1+T)^x \cdot \mu$$

analogously to [**RJW17**, §2]. From the definition, this is an element of $L[[T]]$. A distribution $\mu \in \mathbf{D}$ lives in the smaller space of measures if and only if $\mathscr{A}_\mu(T) \in L \otimes_{\mathcal{O}} \mathcal{O}[[T]]$.

(3) If $\mu \in \mathbf{D}(\mathbf{Z}_p, L)$, then $\mathscr{A}_\mu(T) \in L[[T]]$ converges on the open ball

$$B\left(0, p^{-\frac{1}{p-1}}\right) := \left\{x \in \mathbf{C}_p : v_p(x) > \tfrac{1}{p-1}\right\}.$$

(see [**Col10**, Thm. II.2.2], with $h = 0$).

The convergence in (3) above imposes a growth condition on the coefficients of $\mathscr{A}_\mu(T)$. It is more convenient, however, to characterise distributions using a different, and equivalent, set of data.

Definition 12.5. — Let $\mu \in \mathbf{D}(L)$. Define the *moments* of μ to be the sequence

$$\{\mu(x^n) : n \geq 0\}.$$

Lemma 12.6. — *Taking moments induces a bijection*

$$\mathbf{D}(\mathbf{Z}_p, L) \xrightarrow{\sim} \textit{(bounded sequences in } L\textit{)}.$$

Proof. — Let $\mu \in \mathbf{D}(\mathbf{Z}_p, L)$, and suppose that $\{\mu(x^j)\}$ is an unbounded sequence. Let (b_{j_m}) be a subsequence tending to ∞, $b_{j_m} = \mu(x^{j_m})$. Then

$$\psi(x) = \sum_{m \geq 0} \frac{x^{j_m}}{b_{j_m}} \in \mathbf{A}(\mathbf{Z}_p, L)$$

is rigid analytic. But $\mu(\psi)$ doesn't converge; so μ was not rigid analytic.

Conversely, for any bounded sequence (b_m), and any rigid analytic $\psi(x) = \sum a_m x^m$, the expression

$$\mu(f) := \sum a_m b_m$$

converges since $a_m \to 0$. This then defines a distribution μ. □

Corollary 12.7. — *Let*

$$\begin{aligned} \mathbf{D}(\mathcal{O}) &= \mathbf{D}(\mathbf{Z}_p, \mathcal{O}) \\ &:= \{\mu \in \mathbf{D}(L) : \mu(x^j) \in \mathcal{O} \forall j\}. \end{aligned}$$

Then

$$\mathbf{D}(\mathcal{O}) \otimes_{\mathcal{O}} L \cong \mathbf{D}(L).$$

Proof. — Let $\mu \in \mathbf{D}(L)$. Since the moments are bounded, there exists $c \in L$ such that $c\mu(x^n) \in \mathcal{O}$ for all n. Then

$$\begin{aligned} \mu = \mu \otimes 1 &= c\mu \otimes c^{-1} \\ &\in \mathbf{D}(\mathcal{O}) \otimes L. \end{aligned}$$ □

In particular, up to scaling by L, we may pass freely between integral and rational distributions.

12.2. Overconvergent modular symbols. — The top left corner of Figure 12.1 is given by modular symbols valued in $\mathbf{D}(L)$.

Definition 12.8. — Let

$$\Sigma_0(p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbf{Z}_p) : p|c, a \in \mathbf{Z}_p^\times, ad - bc \neq 0 \right\}.$$

When $p|N$, this monoid contains $\Gamma = \Gamma_0(N)$, as well as all the matrices required for a Hecke action.

Remark 12.9. — Note that $\Sigma_0(p)$ is generated by matrices of the form $\left(\begin{smallmatrix} 1 & 0 \\ c & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$, since

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ c/a & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ 0 & \Delta/a \end{pmatrix},$$

where $\Delta = ad - bc$.

Lemma 12.10. — *Let $k \geq 0$ be an integer. There is a well-defined left weight k action of $\Sigma_0(p)$ on $\mathbf{A}$, defined by*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \psi(x) = (a + cx)^k \psi\left(\frac{b + dx}{a + cx}\right).$$

Proof. — The only problem term is $(a + cx)^{-1}$. We compute that

$$\frac{1}{a + cx} = a^{-1} \frac{1}{1 + \frac{cx}{a}} = \sum_{n \geq 0} (-1)^n \left(\frac{cx}{a}\right)^n.$$

Since $p|c$ and a is a p-adic unit, this converges, giving a well-defined power series. It follows that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot \psi \in \mathbf{A}(L)$ using the algebra structure on power series. □

Remark 12.11. — Note that it is *crucial* that $p|c$ for this. In particular, it is not possible to define overconvergent modular symbols when p does not divide the level N. This does not cause a significant obstacle: given, for example, a newform of level M prime to p, we may always pass to an old eigenform of level Mp and consider overconvergent symbols at this level instead.

Notation 12.12. — We write $\mathbf{A}_k$ for the space $\mathbf{A}$ equipped with the weight k action. We write $\mathbf{D}_k$ for $\mathbf{D}$ with the induced dual action

$$\mu|\gamma(\psi) = \mu(\gamma \cdot \psi).$$

Definition 12.13. — The space of *overconvergent modular symbols of weight k and level* Γ is

$$\mathrm{Symb}_\Gamma(\mathbf{D}_k) = \mathrm{Hom}_\Gamma(\Delta_0, \mathbf{D}_k).$$

This space has a natural Hecke action defined in exactly the same manner as before; that is, if $T \in \mathbf{H}_N$ is defined on modular forms by

$$Tf = \sum_i f|_k\gamma_i,$$

then we define $T\Phi = \sum_i \Phi|\gamma_i$ for Φ an overconvergent modular symbol.

It is clear from the definitions that the injection $\mathcal{V}_k \hookrightarrow \mathbf{A}_k$ is equivariant for the $\Sigma_0(p)$ actions on both sides. Dualising this, we obtain a $\Sigma_0(p)$-equivariant surjection

$$\rho : \mathbf{D}_k \longrightarrow \mathcal{V}_k^\vee.$$

Corollary 12.14. — *There exists a Hecke equivariant specialisation map*

$$\rho : \mathrm{Symb}_\Gamma(\mathbf{D}_k) \longrightarrow \mathrm{Symb}_\Gamma(\mathcal{V}_k^\vee)$$

The Hecke equivariance follows immediately from $\Sigma_0(p)$-equivariance.

12.3. Stevens' control theorem. — Returning to our running diagram, we now have the situation of Figure 12.2; we are aiming to construct the top right part, and we have just filled in the top left part.

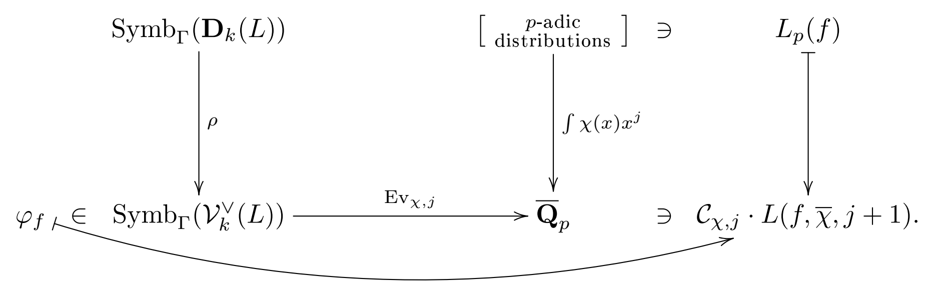

FIGURE 12.2.

We want to lift φ_f to an overconvergent modular symbol. The space $\mathrm{Symb}_\Gamma(\mathbf{D}_k(L))$ is enormous, however, whilst $\mathrm{Symb}_\Gamma(\mathcal{V}_k(L))$ is finite-dimensional; thus necessarily the kernel of ρ is massive.

Stevens' *control theorem* says that the kernel can be completely controlled by studying eigenspaces of the U_p-operator. In particular, if we restrict to certain U_p-eigenspaces, then ρ even becomes an isomorphism. The criterion we use is the *slope* of the U_p-operator.

12.3.1. *Slopes of modular forms.* —

Definition 12.15. — Let $f \in S_{k+2}(\Gamma)$ be an eigenform, with U_p-eigenvalue α_p. The *slope* of f at p is $v_p(\alpha) \in \mathbf{Q}$.

The form f has *finite slope* if $\alpha_p \neq 0$, and *infinite slope* otherwise. There are tight constrictions on the possible range of finite slopes.

Lemma 12.16. — *Suppose:*

(1) *f is new at p with $\alpha_p \neq 0$,*
(2) *or f is old at p, the p-stabilisation of a form g at level M prime to p.*

Then $0 \leq v_p(\alpha_p) \leq k+1$.

Proof. — Hecke eigenvalues are always algebraic integers. In particular, they are p-integral, so $v_p(\alpha_p) \geq 0$.

If f is new at p, then as $\alpha_p \neq 0$, we have $p||N$, corresponding to 'multiplicative reduction'; then it is classically known that $\alpha_p = \pm p^{k/2}$ for some choice of sign, in which case and $v_p(\alpha_p) = k/2 \leq k+1$.

Alternatively, suppose f is old at p, the p-stabilisation of a modular eigenform g of level prime M prime to p. Suppose

$$T_p g = a_p(g) g;$$

then the characteristic polynomial of U_p at level $N = Mp$ is $X^2 - a_p(g)X + p^{k+1}$. The eigenvalue α is a root of this polynomial. So $\alpha | p^{k+1}$ and hence $v_p(\alpha) \leq k+1$. □

12.3.2. *The control theorem.* —

***Theorem 12.17* (Stevens).** — *Let $\alpha \in L^\times$ with $v_p(\alpha) < k+1$. Then the restriction*

$$\rho_\alpha : \mathrm{Symb}_\Gamma(\mathbf{D}_k(L))^{U_p=\alpha} \xrightarrow{\sim} \mathrm{Symb}_\Gamma(\mathcal{V}_k^\vee(L))^{U_p=\alpha}$$

of ρ to the eigenspaces where U_p acts as α is an isomorphism.

An immediate corollary is the following.

Corollary 12.18. — *Let $f \in S_{k+2}(\Gamma)$ be an eigenform, $U_p f = \alpha_p f$. If $v_p(\alpha_p) < k+1$, then*

$$\mathrm{Symb}_\Gamma(\mathbf{D}_k(L))[f] \xrightarrow{\sim} \mathrm{Symb}_\Gamma(\mathcal{V}_k^\vee(L))[f].$$

In particular, there exists unique eigenlift $\Phi_f \in \mathrm{Symb}_\Gamma(\mathbf{D}_k)[f]$ of φ_f.

In the next section, we give a proof of this theorem.

12.4. Additional remarks. —

Remark 12.19. — We see that the slope at p 'detects' classical modular symbols in the space of overconvergent modular symbols. In particular, let Φ be an overconvergent eigensymbol, corresponding to an eigenpacket $\lambda : \mathbf{H}_N \to L$.

– If Φ has slope $< k+1$, then λ is the eigenpacket of a classical modular symbol, and hence a classical modular form by Eichler–Shimura.
– If Φ has slope $> k+1$, then λ is *never* classical, by Lemma 12.16;
– If the slope is exactly equal to $k+1$, then the situation is ambiguous. There are examples where ρ_α is an isomorphism, and examples where it is not. For more on this phenomenon, see [**PS12**] and [**Bel12**].

Remark 12.20. — This theorem has a close analogue in the theory of *overconvergent modular forms*, due to Coleman [**Col96**]. In particular, an overconvergent modular form of weight $k+2$ and slope $< k+1$ is classical. The parallels go further: it is a theorem of Stevens [**PS12**] that there is a bijection between systems of eigenvalues in overconvergent modular forms and overconvergent modular symbols (up to one exceptional system, denoted E_2^{crit} *op. cit.*, which occurs in modular symbols but not modular forms).

Remark 12.21. — In terms of p-adic L-functions, we're on the right track. Let

$$\mu_f = \Phi_f\{0 \to \infty\} \in \mathbf{D}.$$

For $0 \leq j \leq k$, we have $x^j \in \mathcal{V}_k \subset \mathbf{A}_k$, and hence the integral of x^j against μ_f factors through $\rho : \mathbf{D}_k \to \mathcal{V}_k^\vee$. Thus we have

$$\begin{aligned}\int_{\mathbf{Z}_p} x^j \cdot \mu_f &= \int_{\mathbf{Z}_p} x^j \cdot \rho(\mu_f)\\ &= \int_{\mathbf{Z}_p} x^j \cdot \varphi_f\{0 \to \infty\}\\ &= -\frac{j!}{(2\pi i)^{j+1}} \cdot L(f, j+1).\end{aligned}$$

In the context of Figure 12.2, we are completing the diagram with the top map being evluation at $\{0 \to \infty\}$.

We cannot yet call μ_f the p-adic L-function, however. The space $\mathbf{D}$ is *too* big, as $\mathbf{A}$ is too small; in particular, it does not contain any Dirichlet characters, which are not rigid analytic, but instead are only *locally* analytic. We also need to restrict to $\mathbf{Z}_p^\times$. We treat both of these issues in §14.

Remark 12.22. — In addition to the construction of p-adic L-functions of modular forms, as we will see in this course, Stevens' control theorem has a huge range of other applications, a some of which we briefly mention.

Stevens' original motivation was the study of p-adic families of modular forms, building on ideas of Serre, Katz and Coleman. Suppose f is an eigenform of weight k. Then one can deform k to infinitessimally p-adically close integer weights $k + p^n$. It turns out that for sufficiently large n, there are eigenforms f_n of weight $p + k^n$ whose eigenvalues converge, as $n \to \infty$, to the eigenvalues of f. One can see this from overconvergent modular symbols. In addition to being a beautiful in their own right, p-adic families of modular forms are a crucial tool in proving results such as the Iwasawa main conjecture.

In a different direction, Darmon has used the control theorem in his construction of *Stark–Heegner* or *Darmon* points, p-adic analogues of Heegner points on elliptic curves [**Dar01**]. In more recent work with Vonk [**DV17**], he has used it in a different context to give a conjectural approach to explicit class field theory over real quadratic fields.

13. Proof of Stevens' control theorem

We now give a proof of Stevens' control theorem. This was not Stevens' original proof: this proof is due to Greenberg, and first appeared in [**Gre07**].

Via the moments, the spaces of coefficients can be viewed as:

$$\begin{aligned}\mathbf{D}_k &= \text{data of } \mu(x^0), \mu(x^1), ..., \mu(x^k), \mu(x^{k+1}), ... && \in L^{\mathbf{N}}\\ \mathcal{V}_k^\vee &= \text{data of } \mu(x^0), \mu(x^1), ..., \mu(x^k) && \in L^{k+1}.\end{aligned}$$

The map from $\mathbf{D}_k$ to $\mathcal{V}_k^\vee$ is 'forget the moments $\mu(x^{k+1}),\ \mu(x^{k+2}),\ ...$'. Thus to lift, we need to reconstruct these higher moments from:

- the moments up to $\mu(x^k)$,
- and the property of being a U_p-eigensymbol.

Given this, there is only one sensible thing to do: we must iterate the U_p operator.

13.1. An example: improving with U_p. — The idea of Greenberg's proof is that each iteration of U_p 'improves' the information we have. Let us illustrate this with an example, indicating two key steps to make precise in the proof below.

Suppose for simplicity that $f \in S_2(\Gamma, \mathbf{Q})$ has weight 2 and rational coefficients. After scaling, this gives rise to a modular symbol $\varphi_f \in \mathrm{Symb}_\Gamma(\mathbf{Q}_p)$ with $U_p\varphi_f = \alpha\varphi_f$.

***Step 1* (Integral coefficients).** — Show that after possibly multiplying φ_f by a scalar in $\mathbf{Q}_p$, we may take

$$\varphi_f \in \mathrm{Symb}_\Gamma(\mathbf{Z}_p).$$

We may lift φ at a *set-theoretic* level to a function

$$\widetilde{\Phi} \in \mathrm{Maps}(\Delta_0, \mathbf{D}(\mathbf{Z}_p)),$$

imposing no homomorphism or Γ-invariance conditions. This involves so much choice that the result, at the moment, is essentially complete nonsense.

***Step 2* (An integral $\alpha^{-1}U_p$ operator).** — Make sense of the operator $\alpha^{-1}U_p$ with integral coefficients, so that

$$\alpha^{-1}U_p\widetilde{\Phi} \in \mathrm{Maps}(\Delta_0, \mathbf{D})$$

is well-defined. (*A priori* this operator takes values only in $\alpha^{-1}\mathbf{D}(\mathcal{O})$, which is strictly larger than $\mathbf{D}(\mathcal{O})$ if α is not a unit).

Where it is well-defined, $\alpha^{-1}U_p\widetilde{\Phi}$ is also a lift of φ_f, since $\alpha^{-1}U_p$ fixes φ_f:

$$\begin{array}{ccc} \widetilde{\Phi} & \longmapsto & \alpha^{-1}U_p\widetilde{\Phi} \\ \downarrow & & \downarrow \\ \varphi & \longmapsto & \varphi. \end{array}$$

For any $r, s \in \mathbf{P}^1(\mathbf{Q})$, we then compute the first moment to be

$$\begin{aligned} (\alpha^{-1}U_p\widetilde{\Phi})\{r \to s\}(x) &= \alpha^{-1}\sum_{a=0}^{p-1}\widetilde{\Phi}\left\{\frac{r+a}{p} \to \frac{s+a}{p}\right\}(a+px) \\ &\equiv \alpha^{-1}\sum\widetilde{\Phi}\left\{\frac{r+a}{p} \to \frac{s+a}{p}\right\}(a) \pmod{p} \\ &\equiv \alpha^{-1}\sum a\cdot\varphi\left\{\frac{r+a}{p} \to \frac{s+a}{p}\right\} \pmod{p}, \end{aligned}$$

which is well-defined and completely independent of our choice of lift $\widetilde{\Phi}$!

Thus: we seemingly started with no information about the first moment of values of $\widetilde{\Phi}$, which was simply an arbitrary set-theoretic lift to a $\mathbf{D}$-valued map. After a single application of U_p, we have a well-defined value for the first moment mod p: we have gained one digit of p-adic precision. The proof makes steps 1 and 2 precise and then extends this observation to higher moments and arbitrary precision.

13.2. Step 1: Passing to integral coefficients. —

Proposition 13.1. — $\Delta_0 = \mathrm{Div}^0(\mathbf{P}^1(\mathbf{Q}))$ *is a finitely generated* $\mathbf{Z}[\Gamma]$*-module.*

Proof. — We have two finiteness results:

- $\Gamma\backslash\mathbf{P}^1(\mathbf{Q}) = \mathrm{cusps}(\Gamma) = \{[c_1], ..., [c_m]\}$, for a choice of representatives $c_i \in \mathbf{Q}$,
- and $\Gamma = \langle\gamma_1, ..., \gamma_n\rangle$ is a finitely generated group.

Let $[r]-[s]\in\Delta_0$. Then we may write $r=g\cdot c_i$ and $s=g'\cdot c_j$, for $g,g'\in\Gamma$, as translates of our chosen cusp representatives. Then we compute that

$$\begin{aligned}[r]-[s] &= \Big([r]-[c_i]\Big)+\Big([c_i]-[c_j]\Big)+\Big([c_j]-[s]\Big)\\ &= (g-1)[c_i]+([c_i]-[c_j])+(1-g')[c_j].\end{aligned}$$

It follows that Δ_0 is generated as a $\mathbf{Z}[\Gamma]$-module by the (still infinite) set

$$\big\{(1-g)[c_j]:g\in\Gamma,1\leq j\leq m\big\}\ \cup\ \big\{([c_i]-[c_j])\big\}.$$

But for $g_1,g_2\in\Gamma$, we have relations

$$(1-g_1g_2)[c_i]=(1-g_1)[c_i]-g_1(1-g_2)[c_i],$$

so we may rewrite in terms of our generators of Γ, and Δ_0 is generated by the finite set

$$\big\{(1-\gamma_i)[c_j]:1\leq i\leq n,1\leq j\leq m\big\}\ \cup\ \big\{[c_i]-[c_j]:1\leq i<j\leq m\big\}.\qquad\square$$

Corollary 13.2. — *Let D be an $\mathcal{O}[\Gamma]$-module. Then*

$$\mathrm{Symb}_\Gamma(D\otimes_{\mathcal{O}}L)\cong\mathrm{Symb}_\Gamma(D)\otimes_{\mathcal{O}}L.$$

In particular,

$$\mathrm{Symb}_\Gamma(\mathbf{D}_k(L))\cong\mathrm{Symb}_\Gamma(\mathbf{D}_k(\mathcal{O}))\otimes_{\mathcal{O}}L,$$

and similarly for coefficients in $\mathcal{V}_k^\vee$.

Proof. — Let $d_1,...,d_n$ be a finite set of generators for Δ_0 as a $\mathbf{Z}[\Gamma]$-module. Let $\varphi\in\mathrm{Symb}_\Gamma(D\otimes_{\mathcal{O}}L)$. Then there exists a scalar $c\in L$ such that

$$c\varphi(d_i)\in D$$

for all i. Then $c\varphi\in\mathrm{Symb}_\Gamma(D)$. □

From Stevens' theorem with *integral* coefficients, therefore, we can deduce the stated form by tensoring with L.

13.3. Step 2: The integral $\alpha^{-1}U_p$-operator. — From now in, in this proof we will work with fixed k and only with integral coefficients. Thus for clarity of notation, for the rest of §13 we fix

$$\mathbf{D}=\mathbf{D}_k(\mathcal{O}),\qquad\mathcal{V}^\vee=\mathcal{V}_k^\vee(\mathcal{O}).$$

The condition that $\alpha^{-1}U_p$ is a well-defined operator on $\widetilde{\Phi}$ is equivalent to saying that $U_p\widetilde{\Phi}$ takes values in $\alpha\mathbf{D}$. To ensure this, we pass to a slightly smaller subspace.

Definition 13.3. — Let

$$\mathcal{V}^\alpha:=\Big\{\mu\in\mathcal{V}_k^\vee(\mathcal{O}):\mu(x^j)\in\alpha p^{-j}\mathcal{O}\Big\}\subset\mathcal{V}^\vee.$$

Let

$$\mathbf{D}^\alpha:=\Big\{\mu\in\mathbf{D}_k(\mathcal{O}):\rho(\mu)\in\mathcal{V}_k^\alpha\Big\}\subset\mathbf{D}.$$

Lemma 13.4. — *Let $\mu\in\mathbf{D}^\alpha$. Then*

$$\mu\Big|\begin{pmatrix}1&a\\0&p\end{pmatrix}\in\alpha\mathbf{D}.$$

Thus the operator $\alpha^{-1}U_p$ is well-defined on $\mathrm{Maps}(\Delta_0,\mathbf{D}^\alpha)$.

Proof. — We have

$$\mu\Big|\begin{pmatrix}1 & a\\ 0 & p\end{pmatrix}(x^m) = \mu((a+px)^m)$$
$$= \sum_{j=0}^{m}\binom{m}{j}a^{m-j}p^j\cdot\mu(x^j).$$

Recall by Lemma 12.16 that $v_p(\alpha)\leq k+1$. If $j>k$, then $v_p(p^j)\geq k+1\geq v_p(\alpha)$, and accordingly we have

$$\binom{m}{j}a^{m-j}p^j\cdot\mu(x^j)\in p^j\mathcal{O}\subset\alpha\mathcal{O},$$

as all the other terms are in $\mathcal{O}$. If $j\leq k$, then $\mu(x^j)=\rho(\mu)(x^j)\in\alpha p^{-j}\mathcal{O}$, and

$$\binom{m}{j}a^{m-j}p^j\cdot\mu(x^j)\in p^j\alpha p^{-j}\mathcal{O}=\alpha\mathcal{O}.$$

Thus every term in the sum defining the mth moment, and hence the mth moment itself, is in $\alpha\mathcal{O}$. But m was arbitrary, which proves that $\mu|\left(\begin{smallmatrix}1 & a\\ 0 & p\end{smallmatrix}\right)\in\alpha\mathbf{D}$, as required.

The last statement is an immediate corollary. □

Lemma 13.5. — *The modules $\mathcal{V}^\alpha\subset\mathcal{V}_k^\vee(\mathcal{O})$ and $\mathbf{D}^\alpha\subset\mathbf{D}_k(\mathcal{O})$ are stable under the action of $\Sigma_0(p)$.*

Proof. — Since ρ is $\Sigma_0(p)$-stable, it suffices to check this for $\mathcal{V}^\alpha$. This is an explicit check. By Remark 12.9, we may at least reduce this check to matrices of the form $\left(\begin{smallmatrix}1 & 0\\ c & 1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}a & b\\ 0 & d\end{smallmatrix}\right)$. We show this only for the first type, since the second is similar.

Compute that if $\mu\in\mathcal{V}^\alpha$, then

$$\mu\Big|\begin{pmatrix}1 & 0\\ c & 1\end{pmatrix}(x^j) = \mu\big[(1+cx)^{k-j}x^j\big]$$
$$= \sum_{n=j}^{k}\binom{k-j}{n-j}p^{n-j}\mu(x^n).$$

The binomial coefficients are p-integral, whilst $p^{n-j}\mu(x^n)\in p^{n-j}\alpha p^{-n}\mathcal{O}=\alpha p^{-j}\mathcal{O}$ by the assumption that $\mu\in\mathcal{V}^\alpha$. Thus $\mu|\left(\begin{smallmatrix}1 & 0\\ c & 1\end{smallmatrix}\right)(x^j)\in\alpha p^{-j}\mathcal{O}$, and $\mu|\left(\begin{smallmatrix}1 & 0\\ c & 1\end{smallmatrix}\right)\in\mathcal{V}^\alpha$, as required. □

In particular we may consider modular symbols with coefficients in $\mathcal{V}^\alpha$. Note that $\mathcal{V}_k^\alpha\otimes L\cong\mathcal{V}_k(L)$ and $\mathbf{D}^\alpha\otimes L\cong\mathbf{D}_k(L)$. Hence after possibly scaling further, we may take $\varphi_f\in\mathrm{Symb}_\Gamma(\mathcal{V}^\alpha)$, and it suffices to prove ρ induces an isomorphism

$$\rho:\mathrm{Symb}_\Gamma(\mathbf{D}^\alpha)^{U_p=\alpha}\xrightarrow{\sim}\mathrm{Symb}_\Gamma(\mathcal{V}^\alpha)^{U_p=\alpha},$$

which is the form of the theorem we show.

Remark 13.6. — Note that if $v_p(\alpha)=0$, that is if α is a p-adic unit, then $\mathcal{V}^\alpha=\mathcal{V}^\vee$ and $\mathbf{D}^\alpha=\mathbf{D}$. Thus in the case of *ordinary* modular forms we will prove a true integral control theorem.

13.4. Step 3: Improving with U_p.

— We now encode 'improving with U_p' via *filtrations.* In the example above, we started at what will be filtration step 0, and the U_p-operator moved us to step 1; we give a definition that formalises 'U_p moves from step n to $n+1$'.

Definition 13.7. — Let π be a uniformiser of $\mathcal{O}$. For $N\geq 0$, let

$$F^N(\mathbf{D})=\Big\{\mu\in\mathbf{D}:\mu(x^j)\in\pi^{N-j}\mathcal{O}\Big\}.$$

Recalling that $\mathbf{D} = \mathbf{D}_k(\mathcal{O})$, define the Nth filtration step to be

$$\begin{aligned}\mathrm{Fil}^N(\mathbf{D}^\alpha) &= F^N(\mathbf{D}) \ \cap\ \ker(\mathbf{D} \to \mathcal{V}_k^\vee) \ \cap\ \mathbf{D}^\alpha \qquad (13.1)\\ &= \Big\{\mu \in \mathbf{D}^\alpha : \mu(x^j) \in \pi^{N-j}\mathcal{O}\forall j, \quad \mu(x^j) = 0 \text{ for } 0 \le j \le k\Big\}.\end{aligned}$$

Definition 13.8. — Let $A^N(\mathbf{D}^\alpha) = \mathbf{D}^\alpha/\mathrm{Fil}^N(\mathbf{D}^\alpha)$.

We obtain an inverse system (A^N). If α is a p-adic unit, this can be described as

$$\begin{array}{rcl}\mathcal{V}_k^\alpha = & A^0 & := \mathcal{O}^{k+1}\\ & \uparrow & \\ & A^1 & := \mathcal{O}^{k+1} \times \frac{\mathcal{O}}{\pi}\\ & \uparrow & \\ & A^2 & := \mathcal{O}^{k+1} \times \frac{\mathcal{O}}{\pi^2} \times \frac{\mathcal{O}}{\pi}\\ & \uparrow & \\ & A^3 & := \mathcal{O}^{k+1} \times \frac{\mathcal{O}}{\pi^3} \times \frac{\mathcal{O}}{\pi^2} \times \frac{\mathcal{O}}{\pi}\\ & \uparrow & \\ & \vdots & \\ & \uparrow & \\ \mathbf{D}_k^\alpha \cong & \varprojlim A^i & = \mathcal{O}^{k+1} \times \mathcal{O} \times \mathcal{O} \times \mathcal{O} \times \cdots .\end{array}$$

More generally, we get the same picture, only $\mathcal{V}^\alpha$ is a finite-index subgroup of $\mathcal{O}^{k+1}$, which remains constant up the system (with all higher moments unchanged).

Lemma 13.9. — *The system (A^N) is stable under the weight k action of $\Sigma_0(p)$.*

Proof. — This is equivalent to proving that the filtration steps $\mathrm{Fil}^N(\mathbf{D}^\alpha)$ are stable under $\Sigma_0(p)$. It suffices to prove that each of the terms in the intersection 13.1 are stable.

- $\mathbf{D}^\alpha$ is $\Sigma_0(p)$-stable by Lemma 13.5;
- $\ker(\mathbf{D}^\alpha \to \mathcal{V}^\vee)$ is $\Sigma_0(p)$-stable, since the map is equivariant.

It remains to show that $F^N(\mathbf{D})$ is stable. This is similar to the proof of Lemma 13.5, and again we don't give all of the details, checking only for matrices of the form $\left(\begin{smallmatrix}1 & 0\\ c & 1\end{smallmatrix}\right)$. Note

$$\begin{aligned}\begin{pmatrix}1 & 0\\ c & 1\end{pmatrix} \cdot x^j &= x^j \cdot (1+cx)^{k-j}\\ &= \begin{cases} \sum_{m\ge 0} \binom{k-j}{m} c^m x^{m+j} & : j \le k\\ \sum_{m \ge 0} (-1)^m \binom{j-k+m-1}{m} c^m x^{m+j} & : j > k.\end{cases}\end{aligned}$$

In this calculation, we have $c^m \in p^m\mathbf{Z}_p$; and if $\mu \in F^N\mathbf{D}$, then $\mu(x^{m+j}) \in \pi^{N-m-j}\mathcal{O}$ by definition. Thus $\mu(c^m x^{m+j}) \in \pi^{N-j}\mathcal{O}$ and

$$\mu|\left(\begin{smallmatrix}1 & 0\\ c & 1\end{smallmatrix}\right)(x^j) \in \pi^{N-j}\mathcal{O},$$

as required. □

The next lemma encodes the key step that U_p moves us up the filtration, and marks the (first and only) point at which we must assume that $v_p(\alpha) < k+1$.

Lemma 13.10. — *Suppose $v_p(\alpha) < k+1$. Let $\mu \in \mathrm{Fil}^N\mathbf{D}^\alpha$. Then*

$$\mu\left|\begin{pmatrix}1 & a\\ 0 & p\end{pmatrix}\right. \in \alpha \cdot \mathrm{Fil}^{N+1}\mathbf{D}^\alpha.$$

Proof. — We have

$$\mu \Bigg| \begin{pmatrix} 1 & a \\ 0 & p \end{pmatrix} (x^m) = \sum_{j=0}^{m} \binom{m}{j} a^{m-j} p^j \mu(x^j).$$

As $\mu \in \ker(\mathbf{D}^\alpha \to \mathcal{V}^\vee)$, terms with $j \leq k$ vanish. Then

$$j \geq k+1 > v_p(\alpha),$$

by assumption. As p^j must be divisible by an integer power of π, we deduce that $p^j \in \alpha\pi\mathcal{O}$. As $\mu(x^j) \in \pi^{N-j}\mathcal{O}$, we have

$$p^j \mu(x^j) \in \alpha\pi^{N+1-j}\mathcal{O} \subset \alpha\pi^{N+1-m}\mathcal{O},$$

as $m \geq j$. Thus $\mu \Big| \begin{pmatrix} 1 & a \\ 0 & p \end{pmatrix} (x^m) \in \lambda\pi^{N+1-m}\mathcal{O}$, which immediately implies the result. □

13.5. Explicit lifting. — In the example of §13.1, we started with a symbol valued in A^0, applied U_p, and landed in A^1. We now show this holds in general.

Let $v_p(\alpha) < k+1$, and let $\varphi^N \in \mathrm{Symb}_\Gamma(A^N)^{U_p=\alpha}$ be an α-eigensymbol of U_p. Define $\varphi^{N+1} \in \mathrm{Hom}(\Delta_0, A^{N+1})$ as follows:

(1) Choose a lift of φ^N to $\Phi \in \mathrm{Hom}(\Delta_0, \mathbf{D}^\alpha)$.
(2) Apply $\alpha^{-1}U_p$.
(3) Reduce modulo Fil^{N+1}.

Remark 13.11. — Note that lifting to a *homorphism* is always possible. As Δ_0 is a countable torsion-free $\mathbf{Z}$-module, we may choose a $\mathbf{Z}$-basis, and then simply lift φ^N on each generator and extend linearly to a homomorphism. However, even this is not necessary. One may lift to an arbitrary set-theoretic map Φ; then [**Gre07**, Prop. 12] shows that φ^{N+1} is automatically a homomorphism.

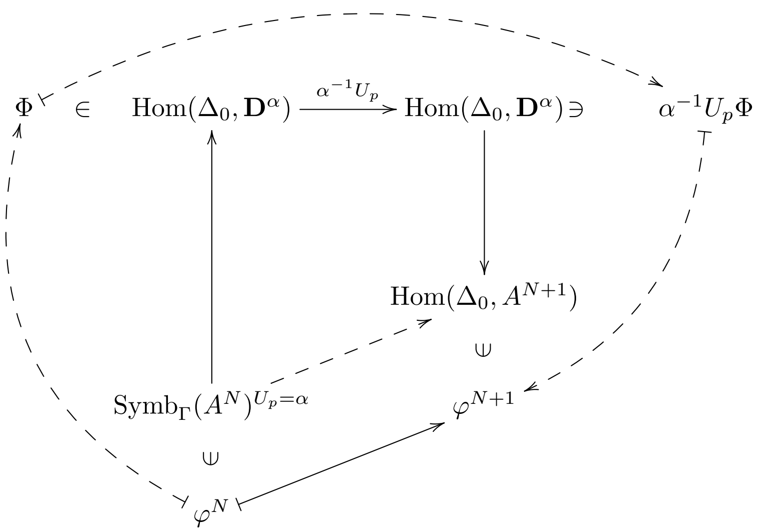

FIGURE 13.1. Definition of φ^{N+1}

Proposition 13.12. — *The homomorphism φ^{N+1}, as defined by the above process, is:*

– *independent of all choices,*
– *Γ-invariant,*
– *a U_p-eigensymbol with eigenvalue α.*

That is, we have

$$\varphi^{N+1} \in \mathrm{Symb}_\Gamma(A^{N+1}(\mathbf{D}^\alpha))^{U_p=\alpha}.$$

Proof. — (1) To show independence of lift, let Φ, Φ' be any two lifts to $\mathrm{Hom}(\Delta_0, \mathbf{D}^\alpha)$. As both have the same reduction module Fil^N, we have $\Phi - \Phi' \in \mathrm{Fil}^N$. Then by Lemma 13.10, we have

$$\alpha^{-1}U_p(\Phi - \Phi') \in \mathrm{Fil}^{N+1}.$$

Thus both $\alpha^{-1}U_p\Phi$ and $\alpha^{-1}U_p\Phi'$ have the same image in A^{N+1}.

(2) To see φ^{N+1} is Γ-invariant: let $\gamma \in \Gamma$. Since the matrices $\left(\begin{smallmatrix}1 & a\\ 0 & p\end{smallmatrix}\right)$ are comprised of representatives of the double coset $[\Gamma \left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right) \Gamma]$, for each a we deduce the existence of $\gamma_a \in \Gamma$ such that

$$\alpha^{-1}\left(\Phi|U_p\right)|\gamma = \alpha^{-1}\sum_a \left(\Phi|\gamma_a\right)\left|\begin{pmatrix}1 & a\\ 0 & p\end{pmatrix}\right. .$$

As φ is Γ-invariant, $\Phi|\gamma_a$ is another lift of φ. By the same proof as (1) this is

$$= \alpha^{-1}\sum_a \Phi\left|\begin{pmatrix}1 & a\\ 0 & p\end{pmatrix}\right. \pmod{\mathrm{Fil}^{N+1}},$$

so φ^{N+1} is Γ-invariant.

(3) To see that φ^{N+1} is a U_p-eigensymbol, we show it is fixed by $\alpha^{-1}U_p$. By definition, we have

$$\begin{aligned}\alpha^{-1}U_p(\varphi^{N+1}) &= (\alpha^{-1}U_p)^2\Phi \pmod{\mathrm{Fil}^{N+1}}\\ &= \varphi^{N+1}.\end{aligned}$$

Here the last equality follows from (1), since $(\alpha^{-1}U_p)^2\Phi$ is also a lift of φ^N. □

Finally, we put all of this together to give Greenberg's proof of Stevens' control theorem.

Proof. — *(of Stevens' control theorem).* We are aiming to prove that ρ restricts to an isomorphism

$$\rho : \mathrm{Symb}_\Gamma(\mathbf{D}^\alpha)^{U_p=\alpha} \xrightarrow{\sim} \mathrm{Symb}_\Gamma(\mathcal{V}^\alpha)^{U_p=\alpha}.$$

To see that this map is surjective, let $\varphi = \varphi^0$ be in the target. Iterating Proposition 13.12 on φ gives elements φ^1, φ^2, and so on, until we get an element of the inverse limit

$$\begin{aligned}\Phi := \varprojlim \varphi^N &\in \varprojlim \mathrm{Symb}_\Gamma(A^N)^{U_p=\alpha}\\ &\cong \mathrm{Symb}_\Gamma(\mathbf{D}^\alpha)^{U_p=\alpha},\end{aligned}$$

where the last isomorphism is canonical and easily checked. By construction, Φ maps to $\varphi^0 = \varphi$ under ρ.

It remains to show that the map is injective. Let $\Phi \in \ker(\rho)$ be an α-eigensymbol. By definition of ρ, this implies that $\Phi \in \mathrm{Symb}_\Gamma(\mathrm{Fil}^0)^{U_p=\alpha}$. Using Lemma 13.10, we see that

$$\Phi = \alpha^{-1}U_p\Phi \in \mathrm{Symb}_\Gamma(\mathrm{Fil}^1)^{U_p=\alpha}.$$

Iterating, we deduce that $\Phi \in \mathrm{Symb}_\Gamma(\mathrm{Fil}^N)$ for all N. But it is easily checked that

$$\bigcap_N \mathrm{Fil}^N = 0;$$

indeed, any element μ of this intersection must have $\mu(x^j) \in \pi^{N-j}\mathcal{O}$ for all j and N, which can only happen if $\mu = 0$. It follows that $\Phi = 0$, and ρ is injective, completing the proof. □

14. The p-adic L-function of a modular form

In this section, we refine Stevens' control theorem to prove that the overconvergent lifts constructed land in a smaller space of *locally analytic* distributions, which allow us to evaluate their values at Dirichlet characters. We use this to construct the p-adic L-function attached to a modular form, and prove the interpolation property it satisfies.

14.1. Locally analytic distributions. — In Remark 12.21, we used Stevens' control theorem to construct a distribution $\mu_f \in \mathbf{D}(\mathbf{Z}_p, L)$ attached to f. To do this, we lifted the modular symbol φ_f to an overconvergent symbol $\Phi_f \in \mathrm{Symb}_\Gamma(\mathbf{D}_k(L))$, and then evaluated at $\{0 \to \infty\}$. We showed that the jth moment of μ_f computed $L(f, j+1)$ for $0 \le j \le k$. Unlike the Riemann zeta function, however, without twisting we only see finitely many L-values. It is thus necessary to consider twisted L-values as well.

Let, then, χ be a Dirichlet character of conductor p^n. As usual, we can lift this to a character χ on $\mathbf{Z}_p^\times$. But $\chi \notin \mathbf{A}$ is *not* a rigid analytic function on $\mathbf{Z}_p$, since it cannot be written as a single power series on all of $\mathbf{Z}_p$. It is, rather, a locally constant function.

As such, it is not clear that we may evaluate μ_f at χ at all, as our space $\mathbf{A}$ is too small to contain the functions $x \mapsto \chi(x)x^j$. As a result, the space $\mathbf{D}$ is too big. Fortunately, we may exhibit more control: we now prove the overconvergent symbol takes values in the (much smaller) space of locally analytic distributions.

Definition 14.1. — A function $\psi : \mathbf{Z}_p \to L$ is *locally analytic of order* r if for all $b \in \mathbf{Z}_p$, the restriction

$$\psi|_{b+p^r\mathbf{Z}_p}(x) = \sum_{n\ge 0} a_n(b)\cdot(x-b)^n$$

is analytic on $b + p^r\mathbf{Z}_p$ (that is, can be written as a single convergent power series). Note that for this to be well-defined, we must have $|a_n(b)|p^{-n} \to 0$ as $n \to \infty$. Write

$$\mathbf{A}[r](L) = \mathbf{A}[r](\mathbf{Z}_p, L) \subset \mathscr{C}(\mathbf{Z}_p, L)$$

for the subspace of such functions.

Definition 14.2. — A function $\psi : \mathbf{Z}_p \to L$ is *locally analytic* if for all $b \in \mathbf{Z}_p$, there is an open ball $\mathcal{U}$ around b such that the restriction $\psi|_{\mathcal{U}}$ is analytic (again, can be written as a single convergent power series). Write $\mathcal{A}(L)$ for the space of locally analytic functions.

Remarks 14.3. — (1) Since $\mathbf{Z}_p$ is compact, if ψ is locally analytic, there must exist some r such that ψ is locally analytic of order r. Thus

$$\mathcal{A}(L) = \bigcup_{r\ge 0} \mathbf{A}[r](L)$$

can be written as a union. Henceforth, we use this description.

(2) Note that $\mathbf{A}(L) = \mathbf{A}[0](L)$, and that for all r, we have $\mathbf{A}[r] \subset \mathbf{A}[r+1]$.

(3) Let χ be a Dirichlet character of conductor p^r, and lift as usual to a character of $\mathbf{Z}_p^\times$. Then since χ is locally constant on the cosets $a + p^r\mathbf{Z}_p$, we have $\chi \in \mathbf{A}[r] \subset \mathcal{A}$.

As before, we really want to consider the dual theory.

Definition 14.4. — Dually, let

$$\mathbf{D}[r](L) = \mathrm{Hom}_{\mathrm{cts}}(\mathbf{A}[r](L), L)$$

be the space of *locally analytic distributions on* $\mathbf{Z}_p$ *of order* r, and

$$\mathcal{D}(L) = \mathrm{Hom}_{\mathrm{cts}}(\mathcal{A}(L), L)$$

be the space of *locally analytic distributions on* $\mathbf{Z}_p$.

Remark 14.5. — – Note that any function ψ in $\mathbf{A}$ and $\mathcal{A}$ is continuous, and thus has a Mahler expansion

$$\psi(x) = \sum_{n\ge 0} a_n(\psi)\binom{x}{n}$$

as in [**RJW17**, Thm. 2.8]. In particular, any element of $\mathbf{D}$ or $\mathcal{D}$ is completely determined by its values on the binomial polynomials, and thus by its Amice transform

$$\mathscr{A}_\mu(T) = \sum_{n\ge 0}\left[\int_{\mathbf{Z}_p}\binom{x}{n}\cdot\mu(x)\right]T^n.$$

– Further, if $\psi \in \mathscr{C}(\mathbf{Z}_p, L)$, finer properties of ψ can be detected solely from how fast the Mahler coefficients of ψ decay. On the dual side, this translates into growth properties for the coefficients of the Amice transform. This is all explained in detail in [**Col10**, §2].

– The inclusions $\mathbf{A}[r] \hookrightarrow \mathbf{A}[r+1]$ give restriction maps

$$\mathbf{D}[r+1] \to \mathbf{D}[r].$$

Since the binomial polynomials are elements of $\mathbf{A}[0]$, the first part of this remark makes it clear that these restriction maps must be injective. We thus think of $\mathbf{D}[r+1]$ as a subset of $\mathbf{D}[r]$.

Proposition 14.6. — *We have*

$$\mathcal{D}(L) = \varprojlim_{r} \mathbf{D}[r] = \bigcap_{r \geq 0} \mathbf{D}[r].$$

Proof. — If μ is an element of the intersection, then it is defined on all $\mathbf{A}[r]$ and thus defined on $\mathcal{A}$, so we get a map $\cap \mathbf{D}[r] \to \mathcal{D}$. It is easy to check that this gives an inverse to the natural restriction map $\mathcal{D} \to \cap \mathbf{D}[r]$. □

These spaces all have natural $\Sigma_0(p)$-actions as before.

Definition 14.7. — The action of $\Sigma_0(p)$ on $\mathbf{A}[0]$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \psi(x) = (a+cx)^k \psi\left(\frac{b+dx}{a+cx}\right)$$

extends immediately to $\mathbf{A}[r]$ for all r. We get an action on the union $\mathcal{A}$, and dual actions on $\mathbf{D}[r]$ and $\mathcal{D}$. As before, when considering these spaces with the weight k action we decorate each space $\mathbf{A}_k[r]$, $\mathcal{A}_k$, $\mathbf{D}_k[r]$, $\mathcal{D}_k$ with a subscript k.

We thus have the following chain of p-adic analytic spaces:

$$\mathbf{A} = \mathbf{A}[0] \quad \subset \quad \mathbf{A}[1] \quad \subset \quad \mathbf{A}[2] \quad \subset \quad \cdots \quad \subset \quad \mathcal{A} \quad \subset \quad \mathscr{C}(\mathbf{Z}_p, L),$$

$$\mathbf{D} = \mathbf{D}[0] \quad \supset \quad \mathbf{D}[1] \quad \supset \quad \mathbf{D}[2] \quad \supset \quad \cdots \quad \supset \quad \mathcal{D} \quad \supset \quad \mathscr{M}(\mathbf{Z}_p, L),$$

and each of these has a weight k action of $\Sigma_0(p)$.

The following proposition says that U_p eigensymbols in $\mathrm{Symb}_\Gamma(\mathbf{D}_k)$ take values in the much smaller space of locally analytic distributions. The key observation is that U_p takes distributions that are locally analytic of order r to order $r+1$, and thus – for a second, completely independent time – iterating U_p allows us to move up a system.

Proposition 14.8. — *Let $\alpha \in L^\times$. There is an isomorphism*

$$\mathrm{Symb}_\Gamma(\mathbf{D}_k)^{U_p=\alpha} \cong \mathrm{Symb}_\Gamma(\mathcal{D}_k)^{U_p=\alpha}.$$

(Note the only condition we impose on α is that it is non-zero, that is we are in the case of finite slope).

Proof. — Since $\mathcal{D} \subset \mathbf{D}$, the inclusion from right to left is obvious.

Claim: The action of $\left(\begin{smallmatrix} 1 & b \\ 0 & p \end{smallmatrix}\right)$ defines a map

$$\mathbf{A}[r+1] \longrightarrow \mathbf{A}[r].$$

Proof of claim: Suppose first $\psi \in \mathbf{A}[1]$, that is, it is analytic of form $\sum_n a_n(b)(x-b)^n$ on each subset $b + p\mathbf{Z}_p$. Let $x \in \mathbf{Z}_p$. We have

$$\begin{pmatrix} 1 & b \\ 0 & p \end{pmatrix} \cdot \psi(x) = \psi(b+px) = \sum_{n \geq 0} a_n(b)(b+px)^n,$$

which now converges on all of $\mathbf{Z}_p$. Thus $\left(\begin{smallmatrix} 1 & b \\ 0 & p \end{smallmatrix}\right) \cdot \psi \in \mathbf{A}[0]$.

The general case is proved identically. □

Dualising this map, the action of $\left(\begin{smallmatrix}1 & b\\ 0 & p\end{smallmatrix}\right)$ defines a map

$$\begin{pmatrix}1 & b\\ 0 & p\end{pmatrix} : \mathbf{D}[r] \longrightarrow \mathbf{D}[r+1] \subset \mathbf{D}[r].$$

Since

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

the U_p-operator thus defines a map

$$U_p : \mathrm{Symb}_\Gamma(\mathbf{D}[r]) \to \mathrm{Symb}_\Gamma(\mathbf{D}[r+1]).$$

Now let $\Phi \in \mathrm{Symb}_\Gamma(\mathbf{D}_k[0])$ be a U_p eigensymbol with non-zero eigenvalue α. Then

$$\Phi = (\alpha^{-r}U_p^r)\Phi \in \mathrm{Symb}_\Gamma(\mathbf{D}_k[r])$$

is valued in the smaller space $\mathbf{D}_k[r]$ for all r. So

$$\Phi \in \bigcap \mathrm{Symb}_\Gamma(\mathbf{D}_k[r]) = \mathrm{Symb}_\Gamma(\mathcal{D})$$

is valued in the space $\mathcal{D}$ of locally analytic distributions. □

Corollary 14.9. — *If $v_p(\alpha) < k+1$, the natural restriction map*

$$\rho : \mathrm{Symb}_\Gamma(\mathcal{D}_k)^{U_p=\alpha} \xrightarrow{\sim} \mathrm{Symb}_\Gamma(\mathcal{V}_k^\vee)^{U_p=\alpha}$$

is an isomorphism.

Remark 14.10. — In the proof of the claim, we saw that $\left(\begin{smallmatrix}1 & b\\ 0 & p\end{smallmatrix}\right) \cdot \psi(x)$ depends only on the restriction of ψ to $b + p\mathbf{Z}_p$. More generally, we see in the same way that $\left(\begin{smallmatrix}1 & b\\ 0 & p^n\end{smallmatrix}\right) \cdot \psi(x)$ depends only on the restriction of ψ to $b + p^n\mathbf{Z}_p$. In particular, this action defines a map

$$\begin{pmatrix}1 & b\\ 0 & p^n\end{pmatrix} : \mathcal{A}(b + p^n\mathbf{Z}_p, L) \to \mathcal{A}(\mathbf{Z}_p, L).$$

When we dualise, we see that the right action of this matrix then defines a map

$$\begin{pmatrix}1 & b\\ 0 & p^n\end{pmatrix} : \mathcal{D}(\mathbf{Z}_p, L) \longrightarrow \mathcal{D}(b + p^n\mathbf{Z}_p, L),$$

that is, if μ is supported on $\mathbf{Z}_p$, then $\mu|\left(\begin{smallmatrix}1 & b\\ 0 & p^n\end{smallmatrix}\right)$ is supported on $b + p^n\mathbf{Z}_p$. This is crucial in the next section when proving interpolation formulae at Dirichlet characters.

14.2. The p-adic L-function. — Let $f \in S_{k+2}(\Gamma)$ be an eigenform, and suppose $v_p(\alpha) < k+1$, where $U_pf = \alpha f$. Corollary 14.9 gives a unique overconvergent lift $\Phi_f \in \mathrm{Symb}_\Gamma(\mathcal{D}_k)^{U_p=\alpha}$ of the classical modular symbol φ_f.

Definition 14.11. — Let $L_p(f) := \Phi_f\{0 \to \infty\}|_{\mathbf{Z}_p^\times}$, the restriction of $\Phi_f\{0 \to \infty\}$ to $\mathbf{Z}_p^\times$. This is a locally analytic distribution on $\mathbf{Z}_p^\times$. We call $L_p(f)$ the *p-adic L-function* of f. If χ is a Dirichlet character of conductor p^n, and $j \in \mathbf{Z}$, then let

$$L_p(f, \overline{\chi}, j+1) := \int_{\mathbf{Z}_p^\times} \chi(x)x^j \cdot L_p(f).$$

We want this to satisfy an interpolation property. We now have the set-up of Figure 14.1; lifting ρ, evaluating at $\{0 \to \infty\}$, restricting to $\mathbf{Z}_p^\times$ and then integrating $\chi(x)x^j$ gives $L_p(f, \chi, j+1)$, whilst $\mathrm{Ev}_{\chi,j}$ computes $L(f, \overline{\chi}, j+1)$. We want to measure how far away this diagram is from being commutative at Φ_f, that is, to measure the failure of the equality of

$$\int_{\mathbf{Z}_p^\times} \chi(x)x^j \cdot \Phi_f\{0 \to \infty\} \ \sim\ \mathrm{Ev}_{\chi,j} \circ \rho(\Phi_f),$$

The following proposition shows that they differ only by a power of the eigenvalue α_p which depends on the conductor of χ.

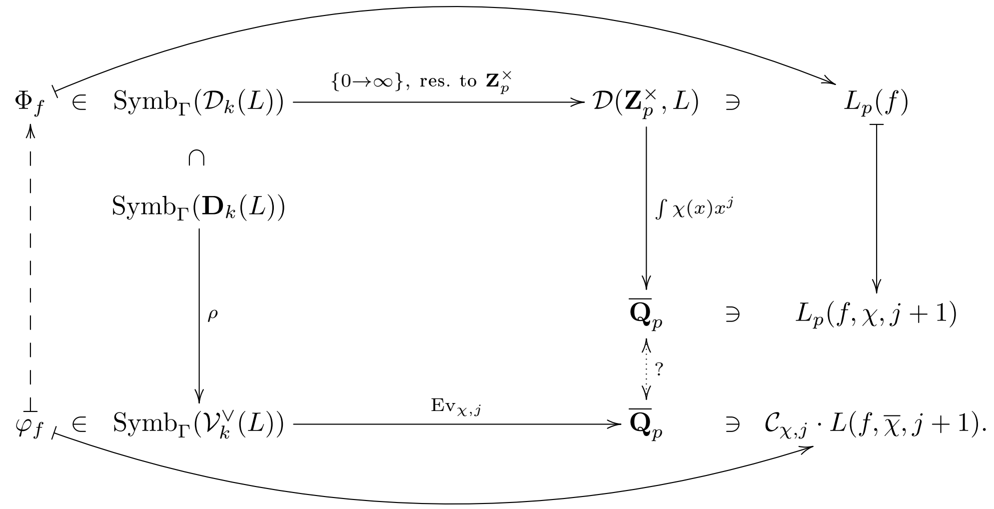

FIGURE 14.1. Construction of $L_p(f)$

Proposition 14.12. — *Let $\Phi \in \mathrm{Symb}_\Gamma(\mathcal{D}_k)$ be a U_p-eigensymbol with eigenvalue $\alpha \in L^\times$, and let χ be a Dirichlet character of conductor p^n with $n \geq 1$. Let $0 \leq j \leq k$. On Φ, the diagram*

$$\begin{array}{ccc}
\mathrm{Symb}_\Gamma(\mathcal{D}_k) & \xrightarrow{\ \Phi\mapsto\Phi\{0\to\infty\}|_{\mathbf{Z}_p^\times}\ } & \mathcal{D}(\mathbf{Z}_p^\times) \\
\downarrow{\scriptstyle \rho} & & \downarrow{\scriptstyle \mu\mapsto\int_{\mathbf{Z}_p^\times}\chi(x)x^j\cdot\mu} \\
\mathrm{Symb}_\Gamma(\mathcal{V}_k^\vee) & \xrightarrow{\ \alpha_p^{-n}\cdot\mathrm{Ev}_{\chi,j}\ } & \overline{\mathbf{Q}}_p
\end{array}$$

commutes.

Proof. — Since we assume $n \geq 1$, the function $\chi(x)x^j$ is already supported on $\mathbf{Z}_p^\times$, and we have

$$\int_{\mathbf{Z}_p^\times} \chi(x)x^j \cdot \Phi\{0\to\infty\} = \int_{\mathbf{Z}_p} \chi(x)x^k \cdot \Phi\{0\to\infty\}.$$

As Φ is a U_p-eigensymbol with non-zero eigenvalue, this is

$$\begin{aligned}
&= \alpha_p^{-n}\int_{\mathbf{Z}_p} \chi(x)x^k \cdot \Phi|U_p^n\{0\to\infty\} \\
&= \alpha_p^{-n}\sum_{a \pmod{p^n}} \chi(a)\int_{a+p^n\mathbf{Z}_p} x^k \cdot \Phi|U_p^n\{0\to\infty\}.
\end{aligned}$$

Now recall that

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

We study this term by term. Recall Remark 14.10, where we saw that $\Phi|\left(\begin{smallmatrix}1 & b\\ 0 & p^n\end{smallmatrix}\right)$ has support in $b + p^n\mathbf{Z}_p$. Explicitly, we have

$$\begin{aligned}\int_{a+p^n\mathbf{Z}_p} x^j \cdot \Phi\left|\begin{pmatrix}1 & b\\ 0 & p^n\end{pmatrix}\right.\{0\to\infty\} &= \Phi\left|\begin{pmatrix}1 & b\\ 0 & p^n\end{pmatrix}\right.\{0\to\infty\}\Big(x^j\cdot \mathbf{1}_{a+p^n\mathbf{Z}_p}(x)\Big)\\ &= \Phi\left\{\frac{b}{p^n}\to\infty\right\}\Big((b+p^nx)^j\mathbf{1}_{a+p^n\mathbf{Z}_p}(b+p^nx)\Big)\\ &= \begin{cases}\Phi|\left(\begin{smallmatrix}1 & a\\ 0 & p^n\end{smallmatrix}\right)\{0\to\infty\}(x^j) & : b=a\\ 0 & : b\neq a,\end{cases}\end{aligned}$$

recalling that $\mathbf{1}_X$ denotes the indicator function of X. The double sum over $a \pmod{p^n}$ and $b \pmod{p^n}$ thus collapses to give

$$\int_{\mathbf{Z}_p^\times}\chi(x)x^j\cdot\Phi\{0\to\infty\} = \alpha_p^{-n}\sum_{a \pmod{p^n}}\chi(a)\Phi\left|\begin{pmatrix}1 & a\\ 0 & p^n\end{pmatrix}\right.(x^j).$$

As we are working with $0\leq j\leq k$, we have $x^j\in\mathcal{V}_k(L)$. Thus evaluation at x^j factors through ρ, and we may replace Φ with $\rho(\Phi)$. But this gives

$$\begin{aligned}&= \alpha_p^{-n}\sum_{a \pmod{p^n}}\chi(a)\rho(\Phi)\left|\begin{pmatrix}1 & a\\ 0 & p^n\end{pmatrix}\right.(x^j)\\ &= \alpha_p^{-n}\mathrm{Ev}_{\chi,j}(\rho(\Phi)),\end{aligned}$$

as required. □

The case of $n=0$ – that is, the case of trivial character – is slightly different, since unlike above, the function x^j is not already supported on $\mathbf{Z}_p^\times$. We instead have the following.

Proposition 14.13. — *Let $\Phi\in\mathrm{Symb}_\Gamma(\mathcal{D}_k)$ be a U_p-eigensymbol with eigenvalue $\alpha\in L^\times$, and let $j\in\mathbf{Z}$ (an* arbitrary *integer). Then*

$$\int_{\mathbf{Z}_p^\times}x^j\cdot\Phi\{0\to\infty\} = \left(1-\frac{p^j}{\alpha}\right)\int_{\mathbf{Z}_p}x^j\cdot\Phi\{0\to\infty\}.$$

In particular, if $0\leq j\leq k$ and f is as in Definition 14.11, then

$$L_p(f,j+1) = -\left(1-\frac{p^j}{\alpha_p}\right)\cdot\frac{j!}{(2\pi i)^{j+1}}\cdot L(f,j+1).$$

Proof. — We exploit the decomposition

$$\begin{aligned}\mathbf{Z}_p &= p\mathbf{Z}_p\cup(1+p\mathbf{Z}_p)\cup\cdots\cup(p-1+p\mathbf{Z}_p)\\ &= p\mathbf{Z}_p\cup\mathbf{Z}_p^\times.\end{aligned}$$

From Remark 14.10, we know that if ψ is locally analytic on $\mathbf{Z}_p$, then $\left(\begin{smallmatrix}1 & a\\ 0 & p\end{smallmatrix}\right)$ is supported on $a+p\mathbf{Z}_p$.

We now use U_p. We have

$$\begin{aligned}\Phi\{0\to\infty\} &= \alpha^{-1}U_p\Phi\{0\to\infty\}\\ &= \alpha^{-1}\sum_{a=0}^{p-1}\Phi\left|\begin{pmatrix}1 & a\\ 0 & p\end{pmatrix}\right.\{0\to\infty\}\\ &= \alpha^{-1}\Phi\left|\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\right.\{0\to\infty\} + \alpha^{-1}\sum_{a=1}^{p-1}\Phi\left|\begin{pmatrix}1 & a\\ 0 & p\end{pmatrix}\right.\{0\to\infty\}.\end{aligned}$$

The first term is supported on $p\mathbf{Z}_p$, and the second on $\mathbf{Z}_p^\times$. We deduce that

$$\begin{aligned}\Phi\{0\to\infty\}|_{\mathbf{Z}_p^\times} &= \alpha^{-1}\sum_{a=1}^{p-1}\Phi\left|\begin{pmatrix}1 & a\\ 0 & p\end{pmatrix}\right.\{0\to\infty\}\\ &= \Phi\{0\to\infty\} - \alpha^{-1}\Phi\left|\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\right.\{0\to\infty\}.\end{aligned}$$

With this support condition in hand, we may now complete the calculation over $\mathbf{Z}_p$. At any function $\psi \in \mathcal{A}(\mathbf{Z}_p, L)$, we compute that

$$\begin{aligned}&\int_{\mathbf{Z}_p^\times}\psi(x)\cdot\Phi\{0\to\infty\}\\ &\quad= \int_{\mathbf{Z}_p}\psi(x)\cdot\left[\Phi\{0\to\infty\} - \alpha^{-1}\Phi\left|\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\right.\{0\to\infty\}\right]\\ &\quad= \int_{\mathbf{Z}_p}\left(\psi(x) - \frac{\psi(px)}{\alpha}\right)\cdot\Phi\{0\to\infty\},\end{aligned}$$

since $\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right)$ fixes $\{0\to\infty\}$ and sends $x\mapsto px$. At $\psi(x) = x^j$, this pulls out to be the required factor $(1 - p^j/\alpha)$.

The final statement follows immediately from combining this with Remark 12.21. □

We finally summarise everything in the following theorem/diagram.

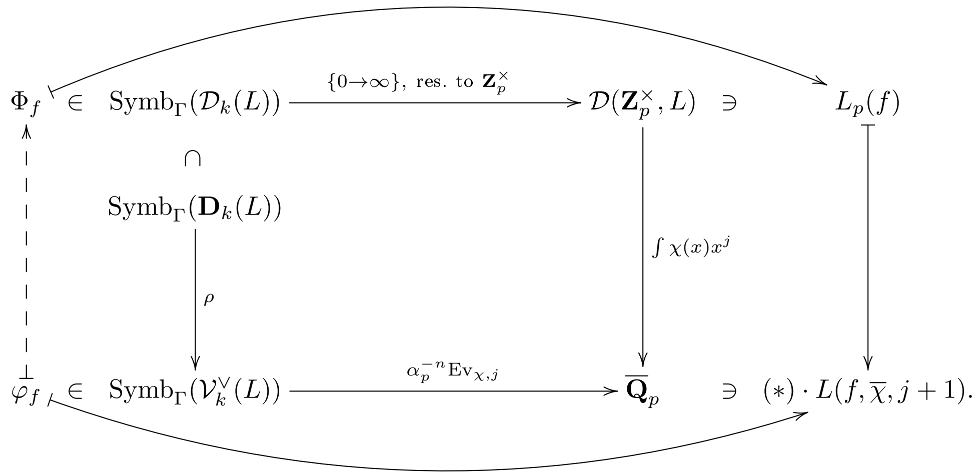

FIGURE 14.2. (Commutative) diagram describing Theorem 14.14

Theorem 14.14. — *Let $f\in S_{k+2}(\Gamma)$ be an eigenform, and suppose $v_p(\alpha) < k+1$, where $U_pf = \alpha f$. Let $L_p(f)$ be the p-adic L-function of f as constructed in Definition 14.11. Let χ be a Dirichlet character of conductor p^n, with $n\geq 0$, and let $0\leq j\leq k$. Then*

$$\int_{\mathbf{Z}_p^\times}\chi(x)x^j\cdot L_p(f) = -\alpha_p^{-n}\cdot\left(1-\chi(p)\frac{p^j}{\alpha_p}\right)\cdot\frac{G(\chi)\cdot j!\cdot p^{nj}}{(2\pi i)^{j+1}}\cdot\frac{L(f,\overline{\chi},j+1)}{\Omega_f^\pm}.$$

Proof. — First consider the case $n\geq 1$, in which case $\chi(p) = 0$ and $(1-\chi(p)p^j/\alpha_p) = 1$. Since Φ_f is a U_p-eigensymbol with non-zero eigenvalue, we may use Proposition 14.12 to compute directly that

$$\begin{aligned}\int_{\mathbf{Z}_p^\times}\chi(x)x^k\cdot L_p(f) &:= \Phi_f\{0\to\infty\}|_{\mathbf{Z}_p^\times}(\chi(x)x^j)\\ &= \alpha_p^{-n}\mathrm{Ev}_{\chi,j}(\rho(\Phi_f))\\ &= \alpha_p^{-n}\mathrm{Ev}_{\chi,j}(\varphi_f).\end{aligned}$$

But in Corollary 11.26 we already saw that

$$\mathrm{Ev}_{\chi,j}(\varphi_f) = -\frac{G(\chi)\cdot j!\cdot p^{nj}}{(2\pi i)^{j+1}}\cdot\frac{L(f,\overline{\chi},j+1)}{\Omega_f^{\pm}},$$

from which the result follows immediately.

In the case $n=0$, the character χ is trivial, and $(1-\chi(p)p^j/\alpha_p) = (1-p^j/alpha_p)$. We conclude from Proposition 14.13. □

Remark 14.15. — Our final interpolation formula differs slightly from that in [**PS11**]. We translate between the two:

– we have a -1 scalar out the front;
– we have $\tau(\chi)$ in the numerator, they have $\tau(\chi^{-1})$ in the denominator;
– they have an additional $(-1)^{j+1}$ in the denominator;
– they have an additional p^n in the numerator.

These are partially explained by the identity $\tau(\chi)\tau(\chi^{-1}) = \chi(-1)\mathrm{cond}(\chi) = \chi(-1)p^n$. After accounting for this, the two differ only by $\chi(-1)(-1)^j$, that is, by the Dirac distribution $[-1]$. Despite checking all the details, this author was unable to see where this difference arises – especially since they are ostensibly given by the same construction! – but it is at least consistent with what is possible.

In some other places in the literature, a formula is given which differs by only $(-1)^j$. This formulation, and the one presented here, cannot both be true. For example, if a measure takes the value $+1$ at all Dirichlet characters $x\mapsto\chi(x)$, it must also take the value $+1$ at all functions $x\mapsto\chi(x)x$, which would not be true of the difference between these two formulations. This is reflected in two contradictory general conjectures due to Coates–Perrin-Riou and Fukaya–Kato, which differ by precisely this issue; the version here matches Coates–Perrin-Riou. I want to make no authoritative statement on which is correct, as though the calculations above have been carefully checked and rechecked, it is inherently possible that there remains a sign error somewhere (tedious exercise: confirm or deny this). There is a careful, detailed account of this problem, and a proposed ruling in favour of Coates–Perrin-Riou, in [**Fï8**, §IV.3]. (Of course, for elliptic curves only $j=0$ arises, for which there is no problem).

15. Growth properties

Let $f\in S_{k+2}(\Gamma)$ be a cuspidal eigenform with $U_pf=\alpha_pf$ and $v_p(\alpha)<k+1$. Then we've constructed a p-adic distribution $L_p(f)$ interpolating the algebraic parts of certain special L-values of f (Theorem 14.14). In this section, we look at the question:

Question 15.1. — *Is $L_p(f)$ uniquely determined by this interpolation property?*

In our setting, we prove that the answer is *yes*. This requires a deeper investigation into p-adic analysis. So far, we've considered the systems

$$\begin{array}{ccccccccccc}\mathbf{A}=\mathbf{A}[0] & \subset & \mathbf{A}[1] & \subset & \mathbf{A}[2] & \subset & \cdots & \subset & \mathcal{A} & \subset & \cdots \quad \mathscr{C}(\mathbf{Z}_p,L),\\ \mathbf{D}=\mathbf{D}[0] & \supset & \mathbf{D}[1] & \supset & \mathbf{D}[2] & \supset & \cdots & \supset & \mathcal{D} & \supset & \cdots \quad \mathscr{M}(\mathbf{Z}_p,L)\end{array}$$

in p-adic analysis. There remains a huge difference between the space $\mathscr{C}(\mathbf{Z}_p,L)$ of arbitrary continuous functions on $\mathbf{Z}_p$, and the space $\mathcal{A}(\mathbf{Z}_p,L)$ of locally analytic functions, and correspondingly between the spaces $\mathscr{M}(\mathbf{Z}_p,L)$ of measures and $\mathcal{D}$ of locally analytic distributions. In particular, we've seen that a measure has Amice transform in $\sum_{n\geq 0}c_n(\mu)T^n\in\mathcal{O}[[T]]\otimes_{\mathcal{O}}L$, and thus has *bounded* coefficients, in the sense that $|c_n(\mu)|_p\leq C$ for some constant C.

Exercise 15.2. — Show that if $\mu \in \mathcal{D}$ is locally analytic, then $\mathscr{A}_\mu(T)$ converges on the open unit disc; that is,

$$\mathscr{A}_\mu(T) = \sum_{n\geq 0} c_n(\mu) z^n$$

converges for all $z \in \mathbf{C}_p$ with $v_p(z) > 0$.

Whilst obviously every power series with bounded coefficients converges on the open unit disc, the converse is far from true. For example, the power series $\sum_{n\geq 1} \frac{z^n}{n}$ has unbounded coefficients, but will converge on the open unit disc; and more generally, we could take coefficients c_n with $|c_n| \sim n^h$ for any $h \geq 0$, and the resulting power series will *still* converge on the open unit disc.

In this section, we will:

– For each $h \geq 0$, define a space $\mathcal{D}^h$ living between

$$\mathcal{D} \supset \mathcal{D}^\infty \supset \cdots \supset \mathcal{D}^h \supset \cdots \supset \mathcal{D}^0 = \mathscr{M}(\mathbf{Z}_p, L),$$

cut out by having "growth of order h".

– We give a criterion for detecting measures inside $\mathcal{D}$; namely, we will have

$$\begin{aligned} \text{measures} &= \text{distributions with growth of order 0} \\ &= \text{bounded distributions.} \end{aligned}$$

Remark 15.3. — In the context of the remarks above, the space $\mathcal{D}^h$ will be equal to the space of locally analytic distributions whose Amice transforms have coefficients that grow like $|c_n| = O(n^h)$. We will not prove this, however; see [**Col10**, Prop. II.3.1] for a proof (in the language of valuations). This gives another way of seeing that measures are distributions with growth of order 0.

15.1. Norms on distributions. — Recall that $\psi \in \mathbf{A}[r]$ if for all $b \in \mathbf{Z}_p$, we may write the restriction

$$\psi|_{b+p^r\mathbf{Z}_p}(x) = \sum_{n\geq 0} a_n(b)(x-b)^n$$

as a convergent power series for all $x \in b + p^r\mathbf{Z}_p$. Note that for this power series to converge is equivalent to $a_n(b)p^{rn} \to 0$ as $n \to \infty$; thus the following is well-defined.

Definition 15.4. — Define a norm $||\cdot||_r$ on $\mathbf{A}[r]$ by

$$||\psi||_r = \sup_{b\in\mathbf{Z}_p}\Big(\sup_n \big|a_n(b)\cdot p^{rn}\big|_p\Big).$$

An equivalent definition (see [**Bel12**, Prop. III.4.12]) is to pick any set $\mathcal{B} \subset \mathbf{Z}_p$ of representatives of $\mathbf{Z}_p/p^r\mathbf{Z}_p$, and take

$$||\psi||_r = \sup_{b\in\mathcal{B}}\Big(\sup_n \big|a_n(b)\cdot p^{rn}\big|_p\Big).$$

Remark 15.5 **(The sets $B_r(\mathbf{Z}_p)$ and alternative descriptions)**
This definition is well-suited to our purposes, but there is a much more conceptual definition which better explains why this does indeed define a norm. Define a subset

$$B_r(\mathbf{Z}_p) := \big\{x \in \mathbf{C}_p : \exists a \in \mathbf{Z}_p, |x-a| \leq p^{-r}\big\} \subset \mathbf{C}_p.$$

For $r = 0$, this is simply the closed unit ball in $\mathbf{C}_p$. For $r = 1$, this is the disjoint union of the p closed balls of radius $1/p$ around the points $0, 1, ..., p-1$ in $\mathbf{Z}_p$. Note that each of these p balls contains exactly one of the open sets $a + p\mathbf{Z}_p$ in $\mathbf{Z}_p$. If $\psi \in \mathbf{A}[1]$, the power series defining $\psi|_{a+p\mathbf{Z}_p}$ immediately extends to give a function on the entire corresponding closed ball in $\mathbf{C}_p$; and this gives an equality

$$\begin{aligned} \mathbf{A}[1](\mathbf{Z}_p, L) &= \mathbf{A}\big(B_1(\mathbf{Z}_p),\ L\big) \\ &:= \big\{\text{analytic functions on } B_1(\mathbf{Z}_p) \text{ defined over } L\big\}, \end{aligned}$$

since such analytic functions on $B_1(\mathbf{Z}_p)$ are given by a separate power series (with coefficients in L) on each of the disjoint components.

More generally, $B_r(\mathbf{Z}_p)$ is the union of p^r closed balls in $\mathbf{C}_p$, and there is an equality

$$\mathbf{A}[r](\mathbf{Z}_p, L) = \mathbf{A}\big(B_r(\mathbf{Z}_p),\ L\big).$$

One then can prove that $||\cdot||_r$ is a sup norm in the sense that

$$||\psi||_r = \sup_{x\in B_r(\mathbf{Z}_p)} |\psi(x)|_p.$$

This picture, which is the approach taken in [**PS11**], is described for $p = 3$ in Figure 15.1.

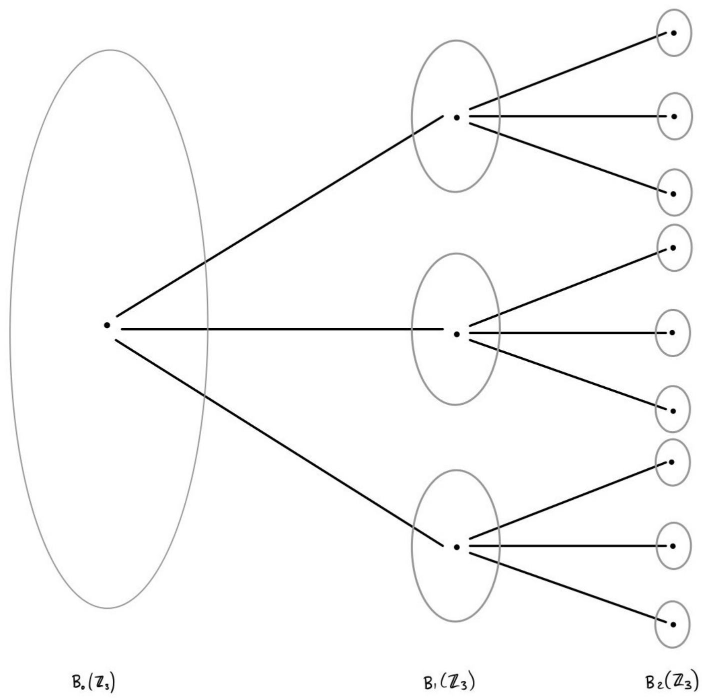

FIGURE 15.1. The sets $B_r(\mathbf{Z}_3)$ for small r

We get a corresponding dual norm on distributions.

Definition 15.6. — Define a norm

$$|\cdot|_r : \mathbf{D}[r](L) \longrightarrow L$$

by

$$|\mu|_r := \sup_{\psi\in\mathbf{A}[r]} \frac{|\mu(\psi)|_p}{||\psi||_r}.$$

Remark 15.7. — Both $\mathbf{A}[r]$ and $\mathbf{D}[r]$ are L-Banach spaces with respect to these norms, and the inclusion maps $\mathbf{D}[r+1] \subset \mathbf{D}$ are *compact* (or *completely continuous*). Here, as in the usual functional analysis sense, this means that the image of every bounded set is a relatively compact set (that is, a set with compact closure). See [**Col10**] for further details. When considering generalisations of overconvergent modular symbols, and of Stevens' control theorem, this property is extremely important (see, for example, [**AS08, Urb11, Han17**], which give very general formulations of this theorem; or [**BSW19**], where such a theorem is proved and used to construct p-adic L-functions in the more general setting of GL(2) over number fields).

Since $\mathcal{D}$ is contained in $\mathbf{D}[r]$ for all r, we obtain an induced family of norms on $\mathcal{D}$. Whilst $\mathcal{D} = \varprojlim \mathbf{D}[r]$ is no longer a Banach space, it is a projective limit of Banach spaces with compact transition maps. Such an object is called a *compact Fréchet space*.

Let $\mu \in \mathcal{D}$. Since

$$\mathbf{A}[r] \subset \mathbf{A}[r+1],$$

we have an inequality

$$\begin{aligned} |\mu|_r &= \sup_{\psi \in \mathbf{A}[r]} \frac{|\mu(\psi)|_p}{||\psi||_r} \\ &\leq \sup_{\psi \in \mathbf{A}[r+1]} \frac{|\mu(\psi)|_p}{||\psi||_{r+1}} = |\mu|_{r+1}. \end{aligned}$$

Here we have implicitly used that if $\psi \in \mathbf{A}[r]$, then

$$||\psi||_{r+1} = \sup_{x \in B_{r+1}(\mathbf{Z}_p)} |\psi(x)|_p \leq \sup_{x \in B_r(\mathbf{Z}_p)} |\psi(x)|_p = ||\psi||_r,$$

so that the denominator cannot grow.

The growth condition we will impose is a restriction on *how much* bigger this can be, via

$$\Big[\text{ growth order } h \Big] \longleftrightarrow \Big[\ p^h|\mu|_r \ \geq\ |\mu|_{r+1} \Big].$$

Definition 15.8. — Let $\mu \in \mathcal{D}$. We say that μ has *growth of order* h (or is h*-admissible*) if there exists a constant D such that

$$||\mu||_r \leq Dp^{rh}$$

as $r \to \infty$. We write

$$\mathcal{D}^h = \mathcal{D}^h(\mathbf{Z}_p, L) = \{\mu \in \mathcal{D}(\mathbf{Z}_p, L) : \mu \text{ has grwoth of order } h\} \subset \mathcal{D}.$$

The distributions that arise from overconvergent eigensymbols have growth equal to the slope at p.

Proposition 15.9. — *Suppose $\Phi \in \mathrm{Symb}_\Gamma(\mathcal{D}_k)$ is an eigensymbol with $U_p\Phi = \alpha_p\Phi$. Let $h = v_p(\alpha)$. Then for every $r, s \in \mathbf{P}^1(\mathbf{Q})$, we have*

$$\Phi\{r \to s\} \in \mathcal{D}^h$$

is a distribution with growth of order h.

Proof. — We give a very rough sketch of the proof here. Let $\mu = \Phi\{r \to s\}$ be a value of Φ. Recall that the action of the matrices in the U_p operator define maps

$$\begin{pmatrix} 1 & b \\ 0 & p \end{pmatrix} : \mathbf{A}[r+1] \longrightarrow \mathbf{A}[r].$$

So, we aim to perform a calculation akin to:

$$\begin{aligned} |\mu|_{r+1} &\sim \sup_{\psi \in \mathbf{A}[r+1]} |\mu(\psi)| \\ &\sim \sup_{\psi \in \mathbf{A}[r+1]} |\alpha_p^{-1} \cdot (\mu|U_p)(\psi)| \\ &\leq p^h \sup_{\psi \in \mathbf{A}[r]} |\mu(\psi)| \\ &\sim p^h |\mu|_r. \end{aligned}$$

(Of course, the above is entirely nonsense: we cannot simply apply U_p to the distribution μ without using Φ itself, and there are also denominators to consider. The work in the real proof is in making this strategy make sense on a rigorous level.) □

Since $L_p(f)$ is built from $\Phi_f\{0 \to \infty\}$, we thus see that it has growth of order $h = v_p(\alpha_p)$, and that we have pinned down the p-adic L-function to an even smaller space of distributions:

$$\begin{array}{ccccccccccccc} \mathbf{D} = \mathbf{D}[0] & \supset & \mathbf{D}[1] & \supset & \cdots & \supset & \mathcal{D} & \supset & \mathcal{D}^h & \supset & \cdots & \supset & \mathscr{M}(\mathbf{Z}_p, L) \\ & & & & & & & & \Cup & & & & \\ & & & & & & & & L_p(f). & & & & \end{array}$$

We conclude by giving the criterion for a distribution to be a measure.

Proposition 15.10. — *Let $\mu \in \mathcal{D}^0(\mathbf{Z}_p, L)$. Then μ is a measure.*

Proof. — Recall that a measure on $\mathbf{Z}_p$ is equivalent to a bounded additive function on open compact subsets of $\mathbf{Z}_p$ [**RJW17**, Rem. 2.2], via the association $\mu \mapsto \mu(\mathbf{1}_X) = \int_{\mathbf{Z}_p} \mathbf{1}_X \cdot \mu$.

Let $\mu \in \mathcal{D}(\mathbf{Z}_p, L)$, and suppose that is has growth of order 0. Then there exists a constant C such that

$$|\mu|_r = \sup_{\psi \in \mathbf{A}[r]} \frac{|\mu(\psi)|_p}{||\psi||_r} \leq C$$

independently of r. Let $X = a + p^r\mathbf{Z}_p$ be a basic open set in $\mathbf{Z}_p$; then its indicator function $\mathbf{1}_X \in \mathbf{A}[r]$, and clearly we have $||\mathbf{1}_X||_r = 1$. We deduce that

$$|\mu(\mathbf{1}_X)|_p \leq C \cdot ||\mathbf{1}_X||_r = C$$

Thus $\mu(\mathbf{1}_X)$ is bounded, so that μ is a measure. □

Corollary 15.11. — *Suppose f is an eigenform that is* ordinary *at p, that is, $v_p(\alpha_p) = 0$. Then*

$$L_p(f) \in \mathscr{M}(\mathbf{Z}_p, L) \cong \Lambda(\mathbf{Z}_p) \otimes_{\mathcal{O}} L$$

is a measure.

15.2. Uniqueness properties. — One of the major reasons to introduce the above growth conditions is the following uniqueness theorem, a distribution analogue of [**RJW17**, Lem. 3.8].

Theorem 15.12. — *Suppose $\mu \in \mathcal{D}$ has growth of order h. Then μ is uniquely determined by the values*

$$\int_{\mathbf{Z}_p} \chi(x)x^j \cdot \mu$$

for all χ of conductor p^s and for all $0 \leq j \leq h$.

Remark 15.13. — Via some basic representation theory, one can rewrite the functions $\{\mathbf{1}_{a+p^s\mathbf{Z}_p} : a \in (\mathbf{Z}/p^s\mathbf{Z})^\times\}$ as linear combinations of the characters $\{\chi : (\mathbf{Z}/p^s\mathbf{Z})^\times \to L^\times\}$ of conductor dviding p^s. In particular, knowing the integrals in the theorem is completely equivalent to knowing the values of the integrals

$$\int_{a+p^s\mathbf{Z}_p} x^j \cdot \mu$$

for $0 \leq j \leq h$, for all a, and for all $s \geq 0$. Thus to prove the theorem it suffices to prove that μ is uniquely determined by these values; which in turn, is equivalent to knowing the values

$$\int_{a+p^s\mathbf{Z}_p} P(x) \cdot \mu$$

for all polynomials P of degree $\leq h$, for all a, and for all s. This is the version of the theorem that we prove.

Proof. — Let $\mu \in \mathcal{D}$, and let $\psi \in \mathbf{A}[r]$. We want to exhibit a sequence (ψ_s) of locally polynomial functions of degree $\leq h$ such that

$$\mu(\psi_s) \longrightarrow \mu(\psi) \ \text{ as } s \longrightarrow \infty, \tag{15.1}$$

which would mean the value of μ at the (arbitrary) function ψ is completely determined by its values at the functions ψ_s.

To construct such a sequence, we define ψ_s by truncating the power series representations defining ψ as an element of $\mathbf{A}[s]$. We may consider

$$\begin{aligned}\psi &= \sum_{b \pmod{p^r}} \psi\big|_{b+p^r\mathbf{Z}_p} \\ &= \sum_{b \pmod{p^{r+1}}} \psi\big|_{b+p^{r+1}\mathbf{Z}_p} \\ &\ \ \vdots \\ &= \sum_{b \pmod{p^s}} \psi\big|_{b+p^s\mathbf{Z}_p},\end{aligned}$$

breaking ψ into pieces modulo p^r, p^{r+1}, and more generally modulo p^s for any $s \geq r$.

Fix a compatible system of representatives of $\mathbf{Z}/p^s$ as s varies; there is an obvious choice, namely the integers $\{0, 1, ..., p^s - 1\}$. Then on each of the local pieces mod p^s, we have a (necessarily unique) power series representation

$$\psi\big|_{b+p^s\mathbf{Z}_p}(x) = \sum_{n\geq 0} a_n(b)\cdot(x-b)^n.$$

We truncate each term in this sum. Fix $N = \lfloor h \rfloor$ the largest integer less than or equal to the growth of μ, and define

$$\psi_s^N\big|_{b+p^s\mathbf{Z}_p}(x) = \sum_{n=0}^{N} a_n(b)(x-b)^n.$$

The term at s of our sequence will then be the sum of these approximations:

$$\psi_s^N = \sum_{b \pmod{p^s}} \psi_s^N\big|_{b+p^s\mathbf{Z}_p}.$$

Thus we have defined a sequence

$$\psi_r^N, \psi_{r+1}^N, ...$$

of functions that are all locally polynomial degree $\leq N$. (Note that after truncating, the function ψ_s^N will in general only be locally analytic of order s, *not* of order r). We prove that this sequence satisfies the property (15.1).

Claim. — *We have*

$$\big|\big|\psi - \psi_s^N\big|\big|_s \leq \left(\frac{p^r}{p^s}\right)^{N+1} ||\psi||_r.$$

Proof. — Computing directly, we have

$$\begin{aligned}\big|\big|\psi - \psi_S^N\big|\big|_s &= \sup{}_{b=0}^{p^s-1} \left|\left|(\psi - \psi_S^N)\big|_{b+p^s\mathbf{Z}_p}\right|\right|_s \\ &= \sup{}_{b=0}^{p^s-1} \left|\left|\sum_{n\geq N+1} a_n(b)(x-b)^n\right|\right|_s.\end{aligned}$$

For each b, we have

$$\left|\left|\sum_{n\geq N+1} a_n(b)(x-b)^n\right|\right|_s = \sup_{n\geq N+1}\Big(|a_n(b)|\cdot p^{-ns}\Big)$$
$$= \sup_{n\geq N+1}\left[\left(\frac{p^r}{p^s}\right)^n |a_n(b)|\cdot p^{-nr}\right]$$
$$\leq \left(\frac{p^r}{p^s}\right)^{N+1} \sup_{n\geq N+1}\Big(|a_n(b)|\cdot p^{-nr}\Big),$$

since $N+1\leq n$. By definition of $||\cdot||_r$, this is

$$\leq \left(\frac{p^r}{p^s}\right)^{N+1} ||\psi||_r,$$

completing the proof of the claim. □

The claim implies that if we allow our norm function to change, any ψ can be arbitrarily approximated by polynomial functions of degree $\leq N$. The growth condition on μ turns out to be exactly enough to force the sequence $\mu(\psi_s^N)$ to converge to $\mu(\psi)$. In particular, by definition we have

$$|\mu|_s = \sup_{g\in\mathbf{A}[s]} \frac{|\mu(g)|}{||g||_s},$$

and in particular this must be

$$\geq \frac{|\mu(\psi-\psi_s^N)|}{||\psi-\psi_s^N||_s}.$$

Rearranging, we have

$$|\mu(\psi-\psi_s^N)| \leq |\mu|_s\cdot||\psi-\psi_s^N||_s$$
$$\leq |\mu|_s\cdot\left(\frac{p^r}{p^s}\right)^{N+1}\cdot||\psi||_r \qquad \text{(by the claim)}$$
$$\leq Dp^{sh}\cdot\left(\frac{p^r}{p^s}\right)^{N+1}\cdot||\psi||_r$$

for some constant D, since μ has growth of order h,

$$= D'\cdot(p^s)^{h-N-1} \qquad \text{(for some constant } D'\text{)}$$
$$\longrightarrow 0 \quad \text{as } s\to\infty,$$

since $h < N+1 = \lfloor h\rfloor + 1$. Thus $\mu(\psi_s^N)\to\mu(\psi)$, as required. □

Remark 15.14. — In [**Col10**], an alternative, but equivalent, approach is given. Colmez defines the notion of being 'continuous of order h' as an intrinisic notion on continuous functions. We may denote the space of such functions $C^h(\mathbf{Z}_p, L)$. Then $\mathcal{D}^h$ is the dual of this space. This theorem is then equivalent to the statement that locally polynomial functions of degree $\leq h$ are dense in the space C^h. Note this also gives a converse to Proposition 15.10, since the values of any measure are bounded, and hence any measure extends to a locally analytic distribution with growth of order 0.

Remark 15.15. — This change of language makes leads to a natural converse of the theorem. Let μ be an additive function on locally polynomial functions of degree $\leq h$, satisfying the growth condition that

$$\left|\int_{b+p^r\mathbf{Z}_p}\left(\frac{x-b}{p^r}\right)^k\cdot\mu\right| \leq Cp^{rh},$$

for some constant C. Then μ extends to a unique distribution μ with growth of order h. See [**Bel12**, Thm. III.4.31] for a direct proof of this converse without introducing the spaces $C^h(\mathbf{Z}_p, L)$.

Finally, we arrive at the corollary we set out to prove.

Corollary 15.16. — *If $U_p f = \alpha_p f$ with $v_p(\alpha_p) < k+1$, then the p-adic L-function $L_p(f)$ is uniquely determined by the interpolation property of Theorem 14.14.*

Proof. — We know from Proposition 15.9 that $L_p(f)$ has growth order $h = v_p(\alpha_p)$. Thus by Theorem 15.12 it is determined uniquely by the values

$$\int_{\mathbf{Z}_p^\times} \chi(x)x^j \cdot L_p(f)$$

for $j \leq h$. But $h < k+1$, and the interpolation formula gives these values for $0 \leq j \leq k$, from which we conclude. □

References

[AS86] Avner Ash and Glenn Stevens. Modular forms in characteristic ℓ and special values of their L-functions. *Duke Math.*, 53, no. 3:849 – 868, 1986.

[AS08] A. Ash and G. Stevens. p-adic deformations of arithmetic cohomology. 2008. Preprint.

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14:843–939, 2001.

[Bel] Joël Bellaïche. Eigenvarieties, families of galois representations, p-adic L-functions. Incomplete notes from a course at Brandeis university, Fall 2010.

[Bel12] Joël Bellaïche. Critical p-adic L-functions. *Invent. Math.*, 189:1 – 60, 2012.

[BSW19] Daniel Barrera Salazar and Chris Williams. p-adic L-functions for GL_2. *Canad. J. Math.*, 71(5):1019–1059, 2019.

[Coa89] John Coates. On p-adic L-functions attached to motives over $\mathbf{Q}$. II. *Bol. Soc. Brasil. Mat. (N.S.)*, 20(1):101–112, 1989.

[Col96] Robert F. Coleman. Classical and overconvergent modular forms. *Invent. Math.*, 124 (1):215 – 241, 1996.

[Col10] Pierre Colmez. Fonctions d'une variable p-adique. *Asterisque*, 330:13–59, 2010.

[CPR89] John Coates and Bernadette Perrin-Riou. On p-adic L-functions attached to motives over $\mathbf{Q}$. In *Algebraic number theory*, volume 17 of *Adv. Stud. Pure Math.*, pages 23–54. Academic Press, Boston, MA, 1989.

[CRJ18] Antonio Cauchi and Joaquín Rodrigues Jacinto. Norm-compatible systems of Galois cohomology classes for GSp_6. 2018. Preprint.

[Dar01] Henri Darmon. Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications. *Ann. of Math.*, 154:589–639, 2001.

[Del79] Pierre Deligne. Valeurs de fonctions L et périodes d'intégrales. *Proc. Symp. Pure Math.*, 33:313–346, 1979.

[DS05] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[DV17] Henri Darmon and Jan Vonk. Singular moduli for real quadratic fields. Preprint, 2017.

[FÏ8] Michael Fütterer. *Motivic p-adic L-functions for families of modular forms.* PhD thesis, Universität Heidelberg, 2018. URL: `https://www.mathi.uni-heidelberg.de/~mfuetterer/texts/diss_fuetterer.pdf`.

[Gre89] Ralph Greenberg. Iwasawa theory for p-adic representations. In *Algebraic number theory*, volume 17 of *Adv. Stud. Pure Math.*, pages 97–137. Academic Press, Boston, MA, 1989.

[Gre07] Matthew Greenberg. Lifting modular symbols of non-critical slope. *Israel J. Math.*, 161:141–155, 2007.

[Han17] David Hansen. Universal eigenvarieties, trianguline Galois representations and p-adic Langlands functoriality. *J. Reine. Angew. Math.*, 730:1–64, 2017.

[Hid88] Haruzo Hida. On p-adic Hecke algebras for GL_2 over totally real fields. *Ann. of Math.*, 128:295–384, 1988.

[Hid94] Haruzo Hida. On the critical values of L-functions of GL(2) and GL(2)$\times$GL(2). *Duke Math.*, 74:432–528, 1994.

[JSW17] Dimitar Jetchev, Christopher Skinner, and Xin Wan. The Birch and Swinnerton-Dyer formula for elliptic curves of analytic rank one. *Cambridge J. Math.*, 5(3):369–434, 2017.

[Kat04] Kazuya Kato. p-adic Hodge theory and values of zeta functions of modular forms. *Astérisque*, 295:117–290, 2004.

[KLZ17] Guido Kings, David Loeffler, and Sarah Zerbes. Rankin–Eisenstein classes and explicit reciprocity laws. *Cambridge J. Math.*, 5(1), 2017.

[LLZ14] Antonio Lei, David Loeffler, and Sarah Zerbes. Euler systems for Rankin-Selberg convolutions of modular forms. *Ann. of Math.*, 180 no. 2:653–771, 2014.

[LLZ15] Antonio Lei, David Loeffler, and Sarah Livia Zerbes. Euler systems for modular forms over imaginary quadratic fields. *Compos. Math.*, 151(9):1585–1625, 2015.

[LLZ18] Antonio Lei, David Loeffler, and Sarah Livia Zerbes. Euler systems for Hilbert modular surfaces. *Forum Math. Sigma*, 6:e23, 67, 2018.

[LSZ17] David Loeffler, Christopher Skinner, and Sarah Livia Zerbes. Euler systems for GSp_4. *J. Euro. Math. Soc.*, 2017. To appear.

[LZ18] David Loeffler and Sarah Livia Zerbes. Euler systems. Lecture notes from the 2018 Arizona Winter School, http://swc.math.arizona.edu/aws/2018/, 2018.

[Pol11] Robert Pollack. Overconvergent modular symbols. Lecture Notes from the Arizona Winter School, 2011.

[PS11] Robert Pollack and Glenn Stevens. Overconvergent modular symbols and p-adic L-functions. *Annales Scientifique de l'Ecole Normale Superieure*, 2011.

[PS12] Robert Pollack and Glenn Stevens. Critical slope p-adic L-functions. *J. Lond. Math. Soc.*, 2012.

[RJW17] Joaquín Rodrigues Jacinto and Chris Williams. An introduction to p-adic L-functions. Lecture notes, 2017.

[Roh91] David Rohrlich. Nonvanishing of L-functions and structure of Mordell-Weil groups. *J. Reine Angew. Math.*, 417:1 – 26, 1991.

[RS17] Ken Ribet and William Stein. Lectures on modular forms and Hecke operators. Lecture notes, 2017.

[Rub00] Karl Rubin. *Euler Systems*. Annals of Mathematics Studies. Princeton University Press, 2000.

[Ski18] Christopher Skinner. Lectures on the Iwasawa theory of elliptic curves. Lecture notes from the 2018 Arizona Winter School, http://swc.math.arizona.edu/aws/2018/, 2018.

[Ste94] Glenn Stevens. Rigid analytic modular symbols. Preprint, 1994.

[SU14] Christopher Skinner and Eric Urban. The Iwasawa Main Conjectures for GL(2). *Invent. Math.*, 195 (1):1–277, 2014.

[TW95] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[Urb11] Eric Urban. Eigenvarieties for reductive groups. *Ann. of Math.*, 174:1695 – 1784, 2011.

[Wei71] André Weil. *Dirichlet Series and Automorphic Forms*, volume 189 of *Lecture Notes in Math.* Springer, 1971.

[Wil95] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math.*, 142 (3):443 – 551, 1995.

Chris Williams, University of Warwick • *E-mail :* christopher.d.williams@warwick.ac.uk