MATH 678: (MOTIVIC) L-FUNCTIONS

LECTURES BY PROF. KARTIK PRASANNA; NOTES BY ALEKSANDER HORAWA

These are notes from Math 678 taught by Professor Kartik Prasanna in Fall 2018, LaTeX'ed by Aleksander Horawa (who is the only person responsible for any mistakes that may be found in them).

This version is from January 15, 2019. Check for the latest version of these notes at

http://www-personal.umich.edu/~ahorawa/index.html

If you find any typos or mistakes, please let me know at ahorawa@umich.edu. Thanks to Peter Dillery for helping me catch up on anything I missed.

The class will involve 10 homeworks and a final project/talk. The homework, together with some supporting papers, will be posted on the shared course file.

Contents

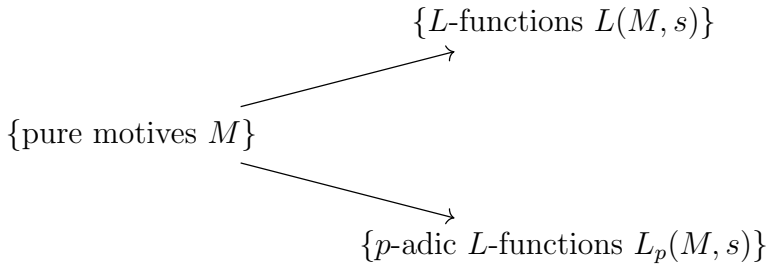
Date: January 15, 2019.

1. Overview

One can associate L-functions to varieties (or even pure motives) over number fields. The question is: how do L-functions capture arithmetic of algebraic varieties (motives)?

In this class, we will use the language of motives very loosely. The reader interested in the precise definitions and more details should consult the papers [Mil13, Kim10]

One can also associate p-adic L-functions to varieties (motives), which should conjecturally capture similar arithmetic information.



This class will focus on the following cases:

(1) Dirichlet characters,
(2) Hecke characters of imaginary quadratic extensions $k/\mathbb{Q}$
(3) elliptic curves over $\mathbb{Q}$.

General L-functions are unfortunately very hard to understand. In fact, the only cases where some of the conjectures are settled are those where one can associate an automorphic form to the geometric object. For example, it is known *any elliptic curve E over $\mathbb{Q}$ is modular*, i.e. $L(E,s) = L(f,s)$ for some modular form f. In this case, both the Hasse–Weil conjecture (about the analytic continuation and functional equation) and significant parts of the Birch–Swinnerton-Dyer conjecture (and the order of vanishing and special values of the L-function) are known.

In the above three cases, the associated automorphic forms are on the following groups:

(1) $\mathrm{GL}(1)_{\mathbb{Q}}$,
(2) $\mathrm{GL}(1)_k$,
(3) $\mathrm{GL}(2)_{\mathbb{Q}}$.

Time permitting, we might consider other reductive groups at the end of the class.

1.1. **First example: the ζ-function.** We start with the simplest example of an L-function, the ζ-function. It is defined for $\mathrm{Re}(s) > 1$ by the following Dirichlet series

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

It admits an Euler product

$$\zeta(s) = \prod_{p} \frac{1}{1-p^{-s}}.$$

In fact, it is the L-function of the *trivial motive*.

Analytic continuation. The function $\zeta(s)$ admits an analytic continuation to $\mathbb{C}$ with the exception of a pole of order one at $s = 1$.

Functional equation. Let $\xi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$. Then

$$\xi(s) = \xi(1-s).$$

The surprising factor $\pi^{-s/2}\Gamma(s/2)$ should be thought of as the *Euler factor at* ∞. It is actually, in some sense, the most important Euler factor. Some basic properties of the Γ function are recalled for the reader's convenience: We recall some useful properties of the Γ function:

(1) $\Gamma(z+1) = z\Gamma(z)$,
(2) $\Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin \pi z}$,
(3) $\Gamma(z)\Gamma(z+1/2) = 2^{1-2x}\sqrt{\pi}\Gamma(2z)$,
(4) $\Gamma(z)$ has poles at $0, -1, -2, \ldots$.

We are interested in the values of $\zeta(s)$ at integers. We know that $\zeta(2) = \frac{\pi^2}{6}$, $\zeta(4) = \frac{\pi^4}{90}$, and in general

$$\zeta(2k) \in \pi^{2k} \cdot \mathbb{Q}^\times \text{ for } k \geq 1.$$

Using the functional equation, we see that

$$\xi(1-2k) = \xi(2k),$$

so

$$\pi^{-\frac{1-2k}{2}} \underbrace{\Gamma\left(\frac{1-2k}{2}\right)}_{\in \sqrt{\pi}\mathbb{Q}^\times} \zeta(1-2k) = \pi^{-k} \underbrace{\Gamma(k)}_{\in \mathbb{Q}^\times} \zeta(2k).$$

This shows that

$$\zeta(1-2k) \in \pi^{-2k}\zeta(2k)\mathbb{Q}^\times = \mathbb{Q}^\times.$$

What about the odd positive numbers and even negative numbers?

Let us first think where are the zeros of ζ are. Note, first, that there are no zeros of $\zeta(s)$ for $\mathrm{Re}(s) > 1$, because of the Euler product expansion. By the functional equation and knowing the poles of Γ, we can hence conclude that $\zeta(s)$ does not have zeroes for $\mathrm{Re}(s) < 0$ but it does have zeroes at $-2, -4, \ldots$.

What about the values of $\zeta(s)$ at positive odd integers? Because of the poles of the Γ function and zeros of the zeta function, we see here that $\zeta(2k+1)$ is related by the functional equation to $\zeta'(-2k)$ for $k \geq 0$. This is the truly interesting case that is hard to tackle.

The remaining strip is the *critical strip* $0 \leq \mathrm{Re}(s) \leq 1$. The zeros there are conjectured to be only at $\mathrm{Re}(s) = \frac{1}{2}$ by the Riemann Hypothesis.

We finally summarize the situation in the following figure.

1.2. **Brief overview of general conjectures.** Recall that we can attach L-function to pure motives. Conjecturally, the category of pure motives sits in a bigger category of mixed motives. The zeros of the L-function of the pure motive are then related to Ext^1 in this larger category. In fact, the order r of vanishing of the L-function should be related to the rank of Ext^1. The arithmetic invariants of Ext are related to the values of $L^{(r)}(s)$.

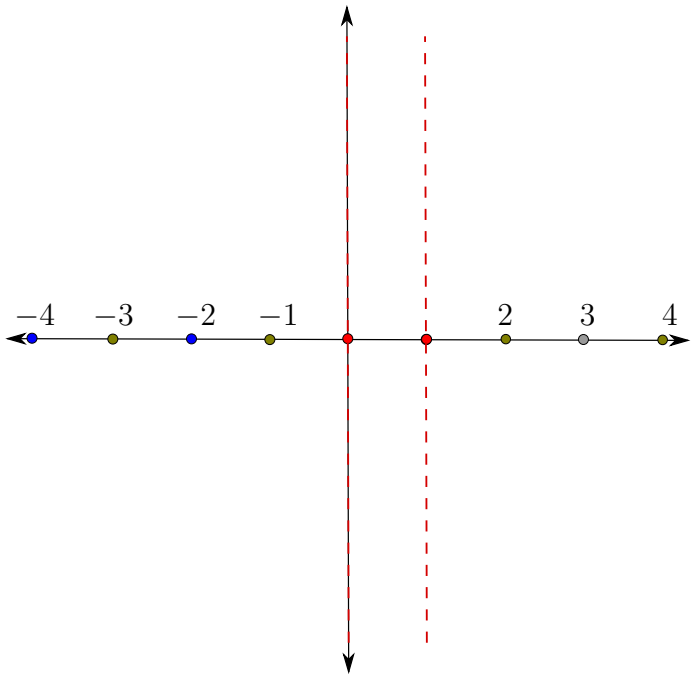


FIGURE 1. The green dots are the critical points, the red dots are values in the critical strip and were omitted from the discussion ($s = 1$ is a pole of ζ and $\zeta(0) \in \mathbb{Q}^\times$), the blue dots are zeros of the zeta function, the gray dots are the mysterious points where not much is known.

Definition 1.1 (Deligne, [Del79])**.** A *critical point* of a (motivic) L-function is an integer $s = n$ such that the Γ-factors on either side of the functional equation have no poles.

For example, the critical points for $\zeta(s)$ are the even positive numbers and the odd negative numbers. In these cases, the values of the ζ-function are known and can be written as a product of an explicit (transcendental) number and a rational number.

Sporadic results on special values.

Historically, people studied sums such as $\sum_{m+ni \in \mathbb{Z}+\mathbb{Z}i} \frac{1}{(m+ni)^4}$. These are related to period of CM elliptic curves and we will discuss them later in the course.

Later, Shimura [Shi76a] proved rationality of critical values of L-functions of modular forms. Then, Deligne [Del79] formulated the definition of critical points and stated a conjecture of rationality. For critical values n for M, he defined numbers $\Omega(M, n)$ and conjectured that

$$\frac{L(M, n)}{\Omega(M, n)} \in \mathbb{Q}^\times.$$

For example, for the ζ-function, $\Omega = (2\pi i)^{2k}$, as we have seen above.

The L-function of an elliptic curve is

$$L(E,s) = \prod_p \frac{1}{(1-\alpha_p p^{-s})(1-\beta_p p^{-s})} = \prod_p \frac{1}{(1-a_p p^{-s}+p^{1-2s}},$$

where $1 - a_p = \#E(\mathbb{F}_p)$.

The factor at infinity is $\Gamma(s)$ and the functional equation then also involves $\Gamma(2-s)$. Therefore, the only critical point is 1. This is the point relevant to the Birch–Swinnerton-Dyer conjecture.

No other points are critical for this L-function, but one could still study its values at non-critical integer points. The first person to do that was Bloch; for example, we studied $L(E,2)$ in the CM case. Later, Beilinson formulated a general conjecture for non-critical points.

Beilinson's conjectures.

Case 1. Let n be a point which is not the center of the center plus $\frac{1}{2}$. Then Beilinson defines $\mathrm{Reg}(M,n)$ and conjectures that

$$\frac{L(M,n)}{\Omega(M,n)\,\mathrm{Reg}(M,n)} \in \mathbb{Q}^\times.$$

Case 2. The point is center plus $\frac{1}{2}$. Beilinson states a similar conjecture in this case. Here, the point could be a pole and it is related to the Tate conjecture.

Case 3. The point is the center. Then the conjecture involves a height pairing. (See, for example, BSD.)

The order in which one would study these conjectures is:

(1) critical points away from the center,
(2) non-critical points when the order of vanishing is 1 and the center when the order of vanishing is 1,
(3) the case where the order of vanishing is ≥ 2 (very little is known here).

1.3. **p-adic L-functions.** Let us first go back to the ζ-function. Recall that $\zeta(1-n)$ for n even is rational. In fact, it is

$$\zeta(1-n) = -\frac{B_n}{n}$$

where B_n is the nth Bernoulli numbers, defined as

$$\frac{te^t}{e^t-1} = \sum_{n=1}^{\infty} B_n \frac{t^n}{n!}.$$

Kummer congruences. When $m \equiv n \not\equiv 0 \mod p-1$, then

$$\frac{B_m}{m} \equiv \frac{B_n}{n} \mod p$$

(both sides are p-adic integers). When $m \equiv n \not\equiv 0 \mod p^r(p-1)$, then

$$(1-p^{m-1})\frac{B_m}{m} \equiv (1-p^{n-1})\frac{B_n}{n} \mod p^n.$$

Kubota and Leopoldt constructed a p-adic analytic function $\zeta_p(s)$ whose values interpolate the values of ζ at negative integers.

In general, we already mentioned we can associate an L-function to a motive. We can also associate to it a p-adic L-function. In general, there can be more than one p-adic L-function and the theory seems richer than the archimedian theory.

2. L-functions of Dirichlet characters

We will start by talking about L-functions of Dirichlet characters. The goals are the following:

- analytic continuation,
- functional equation,
- formula for values at critical points,
- $\mathcal{L}(1, \chi)$ for $\chi \neq \mathbb{1}$.

2.1. **Dirichlet series.** Since the L-function is defined as a Dirichlet series, let us start by reviewing the general theory. A *Dirichlet series* is a series of the form

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

We want to determine a convergence criterion for this.

Lemma 2.1 (Partial summation)**.** *Consider two sequence (b_n), (c_n) and let $B_n = b_1 + b_2 + \cdots + b_n$ be the partial sum. Then*

$$\sum_{n=k}^{\ell} b_n c_n = B_\ell c_\ell + \sum_{n=k}^{\ell} B_n (c_n - c_{n+1}) - B_{k-1} c_k.$$

Proof. We have that

$$\begin{aligned} \sum_{n=k}^{\ell} b_n c_n &= \sum_{n=k}^{\ell-1} (B_n - B_{n-1}) c_n \\ &= B_\ell c_\ell + \sum_{n=k}^{\ell} B_n (c_n - c_{n+1}) - B_{k-1} c_k. \end{aligned}$$

This completes the proof. □

Proposition 2.2. *If $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ converges at s_0, then it converges for all s such that $\mathrm{Re}(s) > \mathrm{Re}(s_0)$. Moreover, it converges uniformly on compact subsets, and hence the limit is an analytic function in s for $\mathrm{Re}(s) > \mathrm{Re}(s_0)$.*

Proof. Write

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \sum_{n=1}^{\infty} \frac{a_n}{n^{s_0}} \cdot \frac{1}{n^{s-s_0}}$$

and let

$$P_\ell(s_0) = \sum_{n=1}^{\ell} \frac{a_n}{n^{s_0}}.$$

Using Partial summation 2.1, we have that

$$\begin{aligned}\sum_{n=k}^{\ell} \frac{a_n}{n^s} &= \sum_{n=k}^{\ell} \frac{a_n}{n^{s_0}} \frac{1}{n^{s-s_0}} \\ &= P_\ell(s_0)\frac{1}{\ell^{s-s_0}} + \sum_{n=k}^{\ell-1} P_n(s_0)\left(\frac{1}{n^{s-s_0}} - \frac{1}{n^{s-s_0-1}}\right) - P_{k-1}(s_0)\frac{1}{k^{s-s_0}}.\end{aligned}$$

Note that

$$\frac{1}{n^{s-s_0}} - \frac{1}{(n+1)^{s-s_0}} = (s-s_0)\int_n^{n+1} \frac{1}{x^{s-s_0+1}} dx.$$

If $\mathrm{Re}(s) \geq \mathrm{Re}(s_0) + \delta$, this shows that

$$\left|\frac{1}{n^{s-s_0}} - \frac{1}{(n+1)^{s-s_0}}\right| \leq \frac{|s-s_0|}{n^{\delta+1}}.$$

Applying this to the above sum, we have that

$$\left|\sum_{n=k}^{\ell} \frac{a_n}{n^s}\right| \leq \frac{|P_\ell(s_0)|}{\ell^\delta} + c|s-s_0| \cdot \sum_{n=k}^{\ell-1} \frac{1}{n^{\delta+1}} + \frac{|P_{k-1}(s_0)|}{\ell^s}.$$

Since the series $\sum_{n=1}^{\infty} \frac{1}{n^{\delta+1}}$ converges, this completes the proof. □

Proposition 2.3. *Consider* $\sum_{n=1}^{\infty} a_n n^{-s}$ *and let*

$$s_n = a_1 + \cdots + a_n.$$

Let $\sigma \geq 0$ *and suppose* $|A_n| \leq C \cdot n^\sigma$ *for some* C. *Then* $\sum_{n=1}^{\infty} a_n n^{-s}$ *converges for* $\mathrm{Re}(s) > \sigma$ *and defines an analytic function.*

Proof. The proof is similar to the proof above. Consider the partial sum

$$P_\ell(s) = \sum_{n=1}^{\ell} a_n n^{-s}.$$

Then

$$\begin{aligned}P_\ell(s) - P_{k-1}(s) &= \sum_{n=k}^{\ell} a_n \frac{1}{n^s} \\ &= \frac{A_\ell}{\ell^s} + \sum_{n=k}^{\ell-1} a_n \underbrace{\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right)}_{\leq \int_n^{n+1} \frac{1}{x^{s+1}} dx} - \frac{A_{k-1}}{k^s}.\end{aligned}$$

As in the previous proof, for $\mathrm{Re}(s) > \sigma$, we take $\delta > 0$ such that $\mathrm{Re}(s) \geq \sigma + \delta$ and complete the proof similarly. □

2.2. **Dirichlet characters.** A *Dirichlet character* is a homomorphism

$$\chi\colon \left(\frac{\mathbb{Z}}{f\mathbb{Z}}\right)^{\times} \to \mathbb{C}^{\times}.$$

The smallest f such that χ factors through $\left(\frac{\mathbb{Z}}{f\mathbb{Z}}\right)^{\times}$ is the *conductor* of χ.

We may then define

$$\chi(n) = \begin{cases} \chi([n]) & \text{if } (n, f) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

The L-function of χ is defined as

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

To consider its convergence, note that

$$\left|\sum_{n=1}^{\ell} \chi(n)\right| \leq \begin{cases} C \cdot \ell^0 & \text{if } \chi \text{ is non-trivial,} \\ C \cdot \ell^1 & \text{if } \chi \text{ is trivial.} \end{cases}$$

Then Proposition 2.3 yields the following result.

Proposition 2.4. *If $\chi \neq \mathbb{1}$, $L(s, \chi)$ converges to an analytic function for $\mathrm{Re}(s) > 0$. If $\chi = \mathbb{1}$, $L(s, \chi)$ converges to an analytic function for $\mathrm{Re}(s) > 1$.*

Exercise. Check that for $\mathrm{Re}(s) > 1$, we have that

$$\zeta(s) = \prod_{p} \frac{1}{1 - p^{-s}},$$

$$L(s, \chi) = \prod_{p} \frac{1}{1 - \chi(p)p^{-s}}.$$

2.3. **Analytic continuation.** Fix a Dirichlet character χ of conductor f. Define

$$F(z) = \sum_{a=1}^{f} \frac{\chi(a) \cdot z e^{az}}{e^{fz} - 1},$$

$$G(z) = \sum_{a=1}^{f} \frac{\chi(a) \cdot e^{-az}}{1 - e^{-fz}}.$$

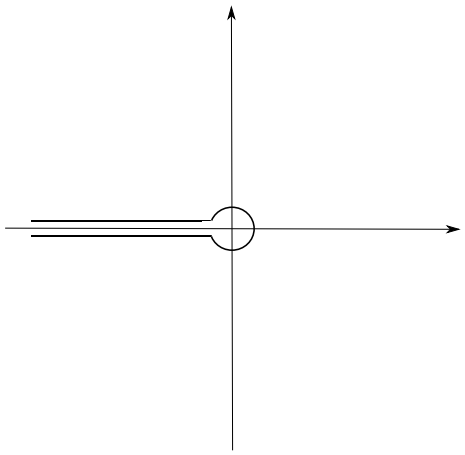
Note that $F(-z) = z \cdot G(z)$. The poles of F are at $2\pi i n/f$.

Note also that for $t \in \mathbb{R}_{\geq 0}$:

$$\begin{aligned} G(t) &= \sum_{a=1}^{f} \frac{\chi(a) \cdot e^{-az}}{1 - e^{-fz}} \\ &= \sum_{a=1}^{f} \chi(a) e^{-at}(1 + e^{-ft} + e^{-2ft} + \cdots) \\ &= \sum_{n} \chi(n) e^{-nt} \end{aligned}$$

which will provide a connection with the above L-function.

Let C be the contour consisting of the negative real numbers with a small circle C_ϵ around 0:



Define

$$H(s) = \int_C F(z) z^{s-1} \frac{dz}{z}$$

where $z^{s-1} = \exp((s-1)\log(z))$ and we take the principal branch of log.

The key observation is that for $s \in \mathbb{Z}$ we have that

$$H(s) = \int_{C_\epsilon} F(z) z^{s-1} \frac{dz}{z}.$$

Check that this integral converges absolutely and gives an analytic function of s.

Substituting $s \mapsto -s$, we see that

$$H(s) = \int_{-C} F(-z)(-z)^{s-1} \frac{dz}{z}$$

where $(-z)^s = \exp(s\log(-z)) = z^s e^{-\pi i s}$ because $\log(-z) = \log(z) - \pi i$. Then

$$\begin{aligned} H(s) &= -\int_{-C} F(-z) z^s e^{-\pi i s} z^{-1} \frac{dz}{z} \\ &= -e^{-\pi i s} \int_{-C} G(z) z^{s-1} dz \\ &= -e^{-\pi i s} \left(\int_{-C_\epsilon} G(z) z^{s-1} dz + (e^{2\pi i s} - 1) \int_\epsilon^\infty G(t) t^{s-1} dt \right). \end{aligned}$$

Now assume $\sigma = \mathrm{Re}(s) > 1$. Note that on C_ϵ, $|G(z)| < \frac{C_1}{\epsilon}$ on C_ϵ. Also, $|z^{s-1}| < C_2(s) \cdot \epsilon^{\sigma-1}$. Then we see that

$$\left| \int_{-C_\epsilon} G(z) z^{s-1} dz \right| \leq \frac{C_1}{\epsilon} C_2(s) \epsilon^{\sigma-1} \cdot 2\pi\epsilon \to 0 \text{ as } \epsilon \to 0.$$

Therefore, letting $\epsilon \to 0$, we see that

$$\begin{aligned} H(s) &= -e^{-\pi i s}(e^{2\pi i s} - 1) \int_0^\infty G(t) t^{s-1} dt \\ &= -(e^{\pi i s} - e^{-\pi i s}) \int_0^\infty \sum_{n=1}^\infty \chi(n) e^{-nt} t^{s-1} dt \\ &= -(e^{\pi i s} - e^{-\pi i s}) \cdot \sum_{n=1}^\infty \chi(n) \int_0^\infty e^{-nt} t^{s-1} dt \\ &= -(e^{\pi i s} - e^{-\pi i s}) \sum_{n=1}^\infty \chi(n) n^{-s} \int_0^\infty e^{-t} t^{s-1} dt. \end{aligned}$$

Altogether, we have shown that

$$H(s) = -(e^{\pi i s} - e^{-\pi i s}) \Gamma(s) L(s, \chi)$$

and we know that $H(s)$ is analytic. Finally,

$$-(e^{\pi i s} - e^{-\pi i s}) \Gamma(s) = -2i \sin(\pi s) \Gamma(s) = \frac{-2\pi i}{\Gamma(1-s)}.$$

This shows that

$$L(s, \chi) = -\frac{1}{2\pi i} \Gamma(1-s) H(s) \text{ for } \mathrm{Re}(s) > 1.$$

This will provide the analytic continuation. Indeed, the right hand side is defined for $\mathrm{Re}(s) \leq 1$, except for a possible pole at $s = 1$. To determine whether or not $L(s, \chi)$ has a pole at $s = 1$, we need to check if $H(s)$ has a zero at $s = 1$.

We have that

$$H(1) = \int_{C_\epsilon} F(z) \frac{dz}{z} = 2\pi i \, \mathrm{Res}_{z=0} \frac{F(z)}{z}.$$

Recall that

$$F(z) = \sum_{a=1}^f \frac{\chi(a) \cdot z e^{az}}{e^{fz} - 1}.$$

Taking the power series expansions, we see that

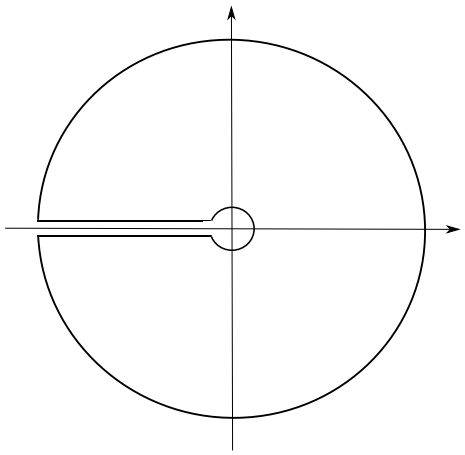
$$\operatorname{Res}_{z=0} \frac{F(z)}{z} = \sum_{a=1}^{f} \frac{\chi(a)}{f} = \begin{cases} 0 & \text{if } \chi \neq \mathbb{1}, \\ 1 & \text{otherwise.} \end{cases}$$

This completes the analytic continuation.

2.4. **Functional equation.** We will now establish the functional equation. Recall that

$$H(s) = \int_C F(z) z^{s-1} \frac{dz}{z}.$$

Let $\operatorname{Re}(s) < 0$. Consider the *keyhole contour* C'_R of radius R:



Then

$$H(s) = -\lim_{R \to \infty} \int_{C'_R} F(z) z^{s-1} \frac{dz}{z}.$$

(Check that this is actually true.) Considering the residues, we have that

$$H(s) = -2\pi i \sum_{\substack{n=-\infty, \\ n \neq 0}}^{\infty} \operatorname{Res}_{z=2\pi i n/f} (F(z) z^{s-2}).$$

We have that

$$\begin{aligned} R_n &:= \operatorname{Res}_{z=2\pi i n/f} F(z) z^{s-2} \\ &= \sum_{a=1}^{f} \frac{\chi(a) e^{2\pi i n a/f}}{f} e^{(s-1)(\log(2\pi n/f) + \pi/2)} \\ &= \frac{1}{f} \sum_{a=1}^{f} \chi(a) e^{2\pi i n a/f} \left(\frac{2\pi n}{f} \right)^{s-1} e^{(s-1)\frac{\pi}{2} i}. \end{aligned}$$

Recall that the *Gauss sum* is defined as

$$\mathfrak{g}_\chi = \sum_{a=1}^{f} \chi(a) e^{2\pi i a/f}.$$

Then

$$R_n = \frac{\overline{\chi}(n)}{f} \mathfrak{g}_\chi \left(\frac{2\pi n}{f}\right)^{s-1} e^{(s-1)\frac{\pi}{2}i}$$

for $n \geq 1$. Similarly,

$$R_{-n} = \frac{1}{f}\sum_{a=1}^{f} \chi(a) e^{-2\pi i a n/f} e^{(s-1)(\log(2\pi n/f) - \pi i/2} = \frac{\overline{\chi}(-n)}{f} \mathfrak{g}_\chi \left(\frac{2\pi n}{f}\right)^{s-1} e^{-(s-1)\frac{\pi}{2}i}.$$

Then

$$\begin{aligned}
H(s) &= -2\pi i \sum_{\substack{n=-\infty,\\ n\neq 0}}^{\infty} \mathrm{Res}_{z=2\pi i n/f}(F(z) z^{s-2}) \\
&= \sum_{n=1}^{\infty} \frac{-2\pi i}{f} \mathfrak{g}_\chi \left(\frac{2\pi n}{f}\right)^{s-1} \left(e^{(s-1)\frac{\pi}{2}i} + \chi(-1) e^{-(s-1)\frac{\pi}{2}i}\right) \overline{\chi}(n) \\
&= -i\mathfrak{g}_\chi \left(\frac{2\pi}{f}\right)^{s} \left(e^{(s-1)\frac{\pi}{2}i} + \chi(-1) e^{-(s-1)\frac{\pi}{2}i}\right) \underbrace{\sum_{n=1}^{\infty} \overline{\chi}(n) n^{s-1}}_{L(1-s,\overline{\chi})} \\
&= -\mathfrak{g}_\chi \left(\frac{2\pi}{f}\right)^{s} (e^{s\frac{\pi}{2}i} - \chi(-1) e^{-s\frac{\pi}{2}i}) L(1-s, \overline{\chi})
\end{aligned}$$

since $\mathrm{Re}(s) < 0$. Then

$$L(s,\chi) = \frac{1}{2\pi i}\Gamma(1-s) \left(\frac{2\pi}{f}\right)^{s} (e^{s\frac{\pi}{2}i} - \chi(-1) e^{s\frac{\pi}{2}i}) L(1-s, \overline{\chi}).$$

Using $\Gamma(1-s)\Gamma(s) = \frac{\pi}{\sin \pi s}$, we see that

$$L(s,\chi) = \frac{1}{2\pi i} \frac{\pi}{\sin(\pi s)\Gamma(s)} \left(\frac{2\pi}{f}\right)^{s} (e^{s\frac{\pi}{2}i} - \chi(-1) e^{s\frac{\pi}{2}i}) L(1-s, \overline{\chi}).$$

Finally, this shows that

$$L(s,\chi) = \frac{\mathfrak{g}_\chi \left(\frac{2\pi}{f}\right)^{s} L(1-s, \overline{\chi})}{(e^{\frac{\pi}{2}is} + \chi(-1) e^{-\frac{\pi}{2}is})\Gamma(s)},$$

which is the functional equation.

Finally, we have that

$$e^{\frac{\pi}{2}is} + \chi(-1) e^{-\frac{\pi}{2}is} = \begin{cases} 2\cos\frac{s\pi}{2} & \text{if } \chi \text{ is even} \\ 2i \sin\frac{s\pi}{2} & \text{if } \chi \text{ is odd.} \end{cases}$$

Letting δ be 0 or 1 according to whether χ is even or odd, we can write

$$e^{\frac{\pi}{2}is} + \chi(-1)e^{-\frac{\pi}{2}is} = 2i^\delta \cos\frac{\pi}{2}(s-\delta).$$

We can finally state a cleaned up version of the functional equation.

Theorem 2.5 (Functional equation)**.** *Suppose χ is a primitive character of conductor f. Let*

$$\Lambda(s,\chi) = \left(\frac{\pi}{f}\right)^{-\left(\frac{s+\delta}{2}\right)} \Gamma\left(\frac{s+\delta}{2}\right) L(s,\chi).$$

Then

$$\Lambda(s,\chi) = \left(\frac{g_\chi}{\sqrt{f}i^\delta}\right)\Lambda(1-s,\overline{\chi}).$$

It is an exercise to show that $|\mathfrak{g}_\chi| = \sqrt{f}$, which will show that the term $\left(\frac{g_\chi}{\sqrt{f}i^\delta}\right)$ has absolute value 1.

Proof. We have that

$$\begin{aligned}
\frac{\Lambda(s,\chi)}{\Lambda(1-s,\overline{\chi})} &= \frac{\left(\frac{\pi}{f}\right)^{-\left(\frac{s+\delta}{2}\right)}\Gamma\left(\frac{s+\delta}{2}\right)L(s,\chi)}{\left(\frac{\pi}{f}\right)^{-\left(\frac{1-s+\delta}{2}\right)}\Gamma\left(\frac{1-s+\delta}{2}\right)L(1-s,\overline{\chi})} \\
&= \left(\frac{\pi}{f}\right)^{\frac{1}{2}-s}\frac{\Gamma\left(\frac{s+\delta}{2}\right)}{\Gamma\left(\frac{1-s+\delta}{2}\right)}\frac{\mathfrak{g}_\chi\left(\frac{2\pi}{f}\right)^s}{\Gamma(s)2i^\delta\cos\frac{\pi}{2}(s-\delta)} \\
&= \left(\frac{\pi}{f}\right)^{\frac{1}{2}}\frac{\Gamma\left(\frac{s+\delta}{2}\right)}{\Gamma\left(\frac{1-s+\delta}{2}\right)}\frac{\mathfrak{g}_\chi\sqrt{\pi}2^{1-s}2^s}{\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s+1}{2}\right)2i^\delta\cos\frac{\pi}{2}(s-\delta)} \quad \text{by } \Gamma(z)\Gamma\left(z+\frac{1}{2}\right) = 2^{1-2z}\sqrt{\pi}\Gamma(2z) \\
&= \frac{\mathfrak{g}_\chi}{\sqrt{f}i^\delta}\frac{\pi}{\Gamma\left(\frac{1-s+\delta}{2}\right)\Gamma\left(\frac{s+1-\delta}{2}\right)}\frac{1}{\cos\frac{\pi}{2}(s-\delta)} \\
&= \frac{\mathfrak{g}_\chi}{\sqrt{f}i^\delta}\frac{\pi\sin\pi\left(\frac{s+1-\delta}{2}\right)}{\pi\cos\frac{\pi}{2}(s-\delta)} \qquad \text{by } \Gamma(1-s)\Gamma(s) = \frac{\pi}{\sin\pi s} \\
&= \frac{\mathfrak{g}_\chi}{\sqrt{f}i^\delta},
\end{aligned}$$

completing the proof. □

2.5. **Special values of $L(s,\chi)$.** Recall that we showed that

$$L(s,\chi) = -\frac{1}{2\pi i}\Gamma(1-s)H(s).$$

Therefore:

$$\begin{aligned} L(1-n,\chi) &= -\frac{1}{2\pi i}\Gamma(n)H(1-n) \\ &= -\frac{1}{2\pi i}\Gamma(n)\int_{C_\epsilon} F(z)z^{-n-1}dz \\ &= -\Gamma(n)\operatorname{Res}_{z=0}(F(z)z^{-n-1}). \end{aligned}$$

Let us take the equation

$$\sum_{a=1}^{f}\frac{\chi(a)te^{at}}{e^{ft-1}} = \sum_{n=0}^{\infty} B_{n,\chi}\frac{t^n}{n!}$$

as the definition of $B_{n,\chi}$, the *generalized Bernoulli numbers*. Note that $B_{n,\chi} \in \mathbb{Q}(\chi)$, the field of definition of χ. We then see that

$$L(1-n,\chi) = -\Gamma(n)\frac{B_{n,\chi}}{n!} = \frac{-B_{n,\chi}}{n}.$$

By the functional equation:

$$B_{n,\chi} = 0 \quad \text{if } n \not\equiv \delta \ (2)$$

except when $\chi = \mathbb{1}$, $n = 1$.

Looking at the power series expansion of the terms in the definition of F, we see that

$$\begin{aligned} F(t) &= \sum_{a=1}^{f}\frac{\chi(a)t(1+at+\frac{(at)^2}{2!}+\cdots)}{ft+\frac{(ft)^2}{2!}+\cdots} \\ &= \sum_{a=1}^{f}\frac{\chi(a)}{f}(1+at+\cdots)(1-\frac{ft}{2}+\cdots). \end{aligned}$$

Therefore,

$$B_{0,\chi} = \sum_{a=1}^{f}\frac{\chi(a)}{f} = \begin{cases} 0 & \text{if } \chi \neq \mathbb{1}, \\ 1 & \text{if } \chi = \mathbb{1}. \end{cases}$$

Similarly,

$$B_{1,\chi} = \sum_{a=1}^{f}\frac{\chi(a)a}{f} - \frac{1}{2}\sum_{a=1}^{f}\chi(a) = \begin{cases} \frac{1}{f}\sum\limits_{a=1}^{f}\chi(a)a & \text{if } \chi \neq \mathbb{1}, \\ \frac{1}{2} & \text{if } \chi = \mathbb{1}. \end{cases}$$

What about $L(1,\chi)$? We will prove the following theorem in the next section (Corollary 2.9).

Theorem 2.6 (Dirichlet)**.** *For $\chi \neq \mathbb{1}$, we have that*

$$L(1,\chi) \neq 0.$$

In particular, Dirichlet used this to show that there are infinitely many primes in arithmetic progressions. See, for example, [Ser73a].

2.6. **Zeta functions of number fields.** The reference for this is [Lan94].

Let K be any number field. Then we may define

$$\zeta_K(s) = \sum_{\mathfrak{a} \subseteq \mathcal{O}_K} \frac{1}{N\mathfrak{a}^s} = \prod_{\mathfrak{p} \text{ prime}} \frac{1}{1 - N\mathfrak{p}^{-s}}.$$

To show convergence, we note that we may write

$$\zeta_K(s) = \sum_n n^{-s} \cdot \#\{\mathfrak{a} \mid N\mathfrak{a} = n\},$$

which is a Dirichlet series. We have reduced the convergence problem to bounding

$$\#\{\mathfrak{a} \mid N\mathfrak{a} = n\}.$$

We define

$$\rho_K = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{w_K \sqrt{|d_K|}}$$

where r_1, r_2 are the numbers of real and complex embeddings of K, h_K is the class number, R_K is the regulator, w_K is the number of roots of unity, and $d_K = \mathrm{disc}_{K/\mathbb{Q}}$. Then one can show that

$$\#\{\mathfrak{a} \mid N\mathfrak{a} = n\} = \rho_K n + O(n^{1 - \frac{1}{[K:\mathbb{Q}]}}).$$

This implies that $\zeta_K(s)$ defines an analytic function for $\mathrm{Re}(s) > 1 - \frac{1}{[K:\mathbb{Q}]}$ with a simple pole at $s = 1$ of residue ρ_K. This is the analytic class number formula.

Similarly to the classical ζ-function, we have an analytic continuation and functional equation. Define

$$\Gamma_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma(s/2),$$
$$\Gamma_{\mathbb{C}}(s) = (2\pi)^{-s}\Gamma(s).$$

Then setting

$$\Lambda(s)\sqrt{|d_K|}^s \Gamma_{\mathbb{R}}(s)^{r_1}\Gamma_{\mathbb{C}}(s)^{r_2}\zeta_K(s),$$

we have that

$$\Gamma(s) = \Gamma(1 - s).$$

Example 2.7. Consider a primitive nth root of unity ζ_n and $K = \mathbb{Q}(\zeta_n)$. Then

$$\mathrm{Gal}(K/\mathbb{Q}) \xrightarrow{\cong} \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$$

canonically. Given a primitive nth root of unity ζ, we have that $\sigma\zeta = \zeta^{i(\sigma)}$ for some $i(\sigma)$ and the map is

$$\sigma \mapsto i(\sigma).$$

The injectivity of the map is clear. We prove surjectivity.

Suppose $(p, n) = 1$. We need to show that $\zeta \mapsto \zeta^p$ is an automorphism of $K/\mathbb{Q}$. Let $f(x)$ be the irreducible polynomial of ζ. Then $x^n - 1 = f(x)h(x)$. If ζ^p is not a root of f, then it is a root of $h(x)$, so ζ is a root of $h(x^p)$. Writing $h(x^p) = f(x)g(x)$ and reducing modulo p, we see that $\overline{h}(x)^p = \overline{f}(x)\overline{g}(x)$. This shows that $\overline{f}(x)$ has multiple roots. Since $(n, p) = 1$, $x^n - 1$ is separable modulo p, which is a contradiction. Thus $\zeta^p \in K$.

Therefore, we have that

$$(\zeta \mapsto \zeta^p) \mapsto [p] \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times.$$

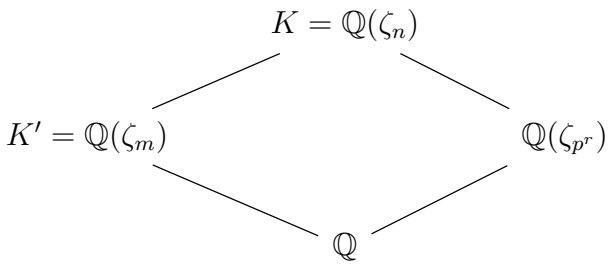
The element $\zeta \mapsto \zeta^p$ is the *Frobenius at* p, Frob_p.

Therefore, any character of conductor f dividing n is a character of the Galois group $\mathrm{Gal}(K/\mathbb{Q})$.

Theorem 2.8. *For $K = \mathbb{Q}(\zeta_n)$, we have that*

$$\zeta_K(s) = \prod_{\substack{\chi \text{ primitive} \\ \text{conductor dividing } n}} L(s, \chi).$$

Proof. Write $n = m \cdot p^r$ for $(p, m) = 1$. Then $K = \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_{p^r})$ and we have the following diagram



Then K' is the maximal extension of $\mathbb{Q}$ unramified at p. Letting $\mathbb{Q} \subseteq F \subseteq K'$ be the maximal extension in which p splits completely, we know that K' is the fixed field of inertia I_p and F is the fixed field of the decomposition group G_p. In particular, if p factors as

$$(p) = (\mathfrak{p}_1 \dots \mathfrak{p}_g)^e$$

in K, then the extensions have degrees

$$\begin{array}{c} K \\ \Big| e \\ K^{I_p} = K' \\ \Big| f \\ K^{G_p} = F \\ \Big| g \\ \mathbb{Q}. \end{array}$$

We consider the euler factor at p on both sides. On the left hand side, this is

$$\prod_{i=1}^{g} \left(1 - \frac{1}{N\mathfrak{p}_i^{-s}}\right) = \prod_{i=1}^{g} (1 - \frac{1}{p^{fs}}) = (1 - t^f)^g,$$

residue fields have size equal to f.

We now consider the right hand side. We first note that any Dirichlet character of conductor divisible by p will satisfy $\chi(p) = 0$, so we may only consider characters that factor through $(\mathbb{Z}/m\mathbb{Z})^\times = \mathrm{Gal}(K'/\mathbb{Q})$. Note that $[p]$ corresponds to Frob_p under this isomorphism, as mentioned above. In fact

$$\mathrm{Frob}_p \in \mathrm{Gal}(K'/F) \cong G_p/I_p$$

and $\#\,\mathrm{Gal}(K'/F) = f$. In particular, $\chi(\mathrm{Frob}_p)$ is an fth root of unity. Moreover, any choice of fth root of unity determines the character χ of $\mathrm{Gal}(K'/\mathbb{Q})$ and extends to exactly g characters of the whole Galois group $\mathrm{Gal}(K/\mathbb{Q})$.

This shows that

$$\prod_\chi (1 - \chi(p)t) = \prod_\chi (1 - \chi(\mathrm{Frob}_p)t) = \prod_{\mu^f=1} (1 - \mu t)^g = (1 - t^f)^g.$$

Since the Euler factors at p agree on both sides, this proves the theorem. □

Corollary 2.9. *For $\chi \neq \mathbb{1}$, we have that*

$$L(1, \chi) \neq 0.$$

Finally, we have the following generalization. Consider $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\zeta_n)$. Then

$$\zeta_K(s) = \prod_\chi L(s, \chi),$$

where the product is over characters of $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ which factor through $\mathrm{Gal}(K/\mathbb{Q})$.

2.7. **Evaluation of $L(1, \chi)$.** Suppose $\chi \neq \mathbb{1}$. For χ odd, we have that

$$L(1, \chi) = \frac{\mathfrak{g}_\chi \left(\frac{2\pi}{f}\right)^1}{2i} L(0, \overline{\chi}) = \frac{\mathfrak{g}_\chi \pi}{if}(-B_{1,\overline{\chi}}) = \frac{i\pi \mathfrak{g}_\chi}{f} \cdot \frac{1}{f} \sum_{a=1}^{f} \overline{\chi}(a) a.$$

Corollary 2.10. *If χ is an odd character,*

$$\sum_{a=1}^{f} \chi(a) a \neq 0.$$

While this fact is very elementary, it would be really hard to prove it directly.

Note that when χ is odd, 1 is a critical point of $L(s, \chi)$, so we get this simple formula.

Application. Suppose $K/\mathbb{Q}$ is imaginary quadratic. Then $K \subseteq \mathbb{Q}(\zeta_n)$ for some n by the Kronecker–Weber theorem. Therefore,

$$\zeta_K(s) = \zeta(s) L(s, \chi)$$

for some χ. What is χ? It is the unique non-trivial quadratic character of conductor equal to $|d_K|$. The residue at $s = 1$ gives

$$\frac{2\pi h_K}{w_K \sqrt{|d_K|}} = \frac{\pi i g_\chi}{|d_K|} \frac{1}{|d_K|} \left(\sum_{a=1}^{|d_K|} \chi(a) a \right).$$

Therefore, taking absolute values

$$h_K = \frac{w_K}{2}\frac{1}{|d_K|}\left|\sum_{a=1}^{|d_K|}\chi(a)a\right|.$$

This allows to compute the class number in some cases. For example, one can use this to compute $h_{\mathbb{Q}(\sqrt{-23})}$. This gives $h_K = 3$. More examples are given in the homework.

For real quadratic thing, we would obtain a factor corresponding to the regulator which could be harder to compute.

Assume now χ is even and non-trivial. In this case, 1 is not a critical point of $L(s,\chi)$. Nonetheless, we have that:

$$\begin{aligned} L(1,\chi) &= \sum_{n=1}^{\infty}\frac{\chi(n)}{n} \\ &= \sum_{n=1}^{\infty}\frac{1}{n}\frac{1}{\mathfrak{g}_{\overline{\chi}}}\sum_{a=1}^{f}\overline{\chi}(a)e^{2\pi ian/f} \\ &= \frac{1}{\mathfrak{g}_{\overline{\chi}}}\sum_{a=1}^{f}\overline{\chi}(a)\sum_{n=1}^{\infty}\frac{1}{n}e^{2\pi ian/f} \\ &= -\frac{1}{\mathfrak{g}_{\overline{\chi}}}\sum_{a=1}^{f-1}\overline{\chi}(a)\log(1-e^{2\pi ia/f}). \end{aligned}$$

This is valid when χ is odd as well, but we will simply recover the previous formula Corollary 2.10.

3. Kubota–Leopoldt p-adic L-function

We will use the formulas for $L(1-n,\chi)$ to p-adically interpolate these values. This will give the Kubota–Leopoldt p-adic L-function, which is our first example of a p-adic L-function. For most of this section, the reference is [Iwa72].

3.1. Power series over non-archimedean fields.

We fix notation as follows:

$$\begin{array}{c} \mathbb{C}_p = \text{ completion of } \overline{\mathbb{Q}_p} \\ \big| \\ \overline{\mathbb{Q}_p} = \text{ algebraic closure of } \mathbb{Q}_p \\ \big| \\ K = \text{ finite extension of } \mathbb{Q}_p \\ \big| \\ \mathbb{Q}_p \end{array}$$

We will assume that the absolute value on $\mathbb{Q}_p$ is normalized so that $|p| = \frac{1}{p}$.

Consider $K[\![x]\!]$, the ring of power series with coefficients in K. If $A(x) \in K[\![x]\!]$. Then for any $\xi \in K$, $A(\xi) = \sum a_n \xi^n$ converges if and only if $|a_n \xi^n| \to 0$.

Observe that if this power series converge for some ξ_0, then it converges for all ξ with $|\xi| \leq |\xi_0|$.

Lemma 3.1. *Let $A(x), B(x) \in K[\![x]\!]$, both convergent in some neighborhood of 0. Suppose there is a sequence $(\xi_n) \in \mathbb{C}_p$ of non-zero elements such that $\xi_n \to 0$ as $n \to \infty$, and $A(\xi_n) = B(\xi_n)$ for all n. Then $A = B$.*

Proof. By looking at $A - B$, we may assume that $A(\xi_n) = 0$ for all n and show that $A = 0$. Suppose

$$A(x) = a_m x^m + a_{m+1} x^{m+1} + \cdots \quad \text{and } a_m \neq 0.$$

Then we have that

$$\begin{aligned} 0 &= a_m \xi_k^m + a_{m+1} \xi_k^{m+1} + \cdots, \\ -a_m \xi_k^m &= a_{m+1} \xi_k^{m+1} + \cdots, \\ -a_m &= \xi_k (a_{m+1} + a_{m+2} \xi_k + \cdots). \end{aligned}$$

Since $A(x) = \sum a_n x^n$ converges in neighborhood of 0, there is an R such that $|a_i| R^i \to 0$, so $|a_i| \leq C \cdot R^{-i}$. For k large enough, $|\xi_k| < R^\ell$ where we choose ℓ such that

$$|a_{m+n} \xi_k^{n-1}| \leq C \cdot R^{-(m+n)} (R^\ell)^{n-1}.$$

By choosing ℓ appropriately, the sum $a_{m+1} + a_{m+2}\xi_k + \cdots$ is bounded as $k \to \infty$. Hence letting $k \to \infty$ in the expression above, $\xi_k \to 0$, so $-a_m = 0$, which is a contradiction. □

For $A = \sum a_n x^n$, we let $\|A\| = \sup_n |a_n|$. Let

$$P_K = \{A \in K[\![x]\!] \mid \|A\| < \infty\}.$$

Note that:

- $K[x] \subset P_K \subseteq K[\![x]\!]$,
- $\|A\| \geq 0$ and $\|A\| = 0$ if and only if $A = 0$,
- $\|A + B\| \leq \max\{\|A\|, \|B\|\}$,
- $\|cA\| = |c|\|A\|$, $\|AB\| \leq \|A\|\|B\|$.

To check that P_K is a Banach algebra, we just need to show it is complete.

Proposition 3.2. *The algebra P_K is complete for $\|-\|$.*

Proof. Suppose (A_k) is a Cauchy sequence in P_K. Write

$$A_k(x) = \sum_{n=1}^{\infty} a_{n,k} x^n.$$

For $\ell \geq k$, we have that

$$A_\ell(x) - A_k(x) = \sum_n (a_{n,\ell} - a_{n,k}) x^n.$$

Therefore, for each n, $(a_{n,k})$ is a Cauchy sequence. Let $a_n = \lim_{k\to\infty} a_{n,k}$ and

$$A(x) = \sum_{n=1}^{\infty} a_n x^n.$$

Then $|a_{n,k}| \leq \|A_k\|$. To see that $A(x) \in P_K$, note that $|a_n| = \lim_k |a_{n,k}|$ and so $|a_n| \leq \sup_k(\|A_k\|) < \infty$.

We now want to show that $\lim_{k\to\infty} A_k = A$. Given $\epsilon > 0$, there is an N such that for any $\ell \geq k \geq N$, $\|A_\ell - A_k\| < \epsilon$. Then

$$|a_{n,\ell} - a_{n,k}| < \epsilon \quad \text{for all } n \text{ and } \ell \geq k \geq N,$$

so

$$|a_n - a_{n,k}| \leq \epsilon \quad \text{for all } n \text{ and } k \geq N,$$

and hence

$$\|A - A_k\| \leq \epsilon \quad \text{for all } k \geq N.$$

This completes the proof. □

We want an estimate for $\left\|\binom{X}{n}\right\|$, where

$$\binom{X}{n} = \frac{X(X-1)\dots(X-n+1)}{n!}.$$

For that, we need to estimate the p-adic absolute value of $n!$.

Lemma 3.3. *We have that*

$$|p|^{\frac{n}{p-1}} \leq |p|^{\frac{n-1}{p-1}} \leq |n!| \leq np|p|^{\frac{n}{p-1}}.$$

Proof. Write $n = a_0 + a_1 p + \cdots + a_m p^m$ where $p^m \leq n < p^{m+1}$ and $0 \leq a_i \leq p-1$. Let $r = a_0 + a_1 + \cdots + a_m$. The power of p dividing $n!$ is

$$\begin{aligned}
\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots + \left[\frac{n}{p^m}\right] &= (a_1 + \cdots + a_m p^{m-1}) + (a_2 + a_3 p + \cdots) + \cdots + a_m \\
&= a_1 + a_2(p+1) + a_3(p^2+p+1) + \cdots + a_m(p^{m-1} + \cdots + 1) \\
&= \frac{1}{p-1}\left(a_1(p-1) + a_1(p^2-1) + \cdots + a_m(p^m-1)\right) \\
&= \frac{1}{p-1}\left(n - a_0 - a_1 - \cdots - a_m\right) \\
&= \frac{n-r}{p-1}.
\end{aligned}$$

Finally, we obtain that

$$|n!| = |p|^{\frac{n-r}{p-1}} \geq |p|^{\frac{n-1}{p-1}} \geq |p|^{\frac{n}{p-1}}.$$

For the other bound on $n!$, we have that $r \leq (m+1)(p-1)$, so

$$\frac{n-r}{p-1} \geq \frac{n}{p-1} - (m+1),$$

and hence

$$|n!| = |p|^{\frac{n-r}{p-1}} \leq |p|^{\frac{n}{p-1} - (m+1)} = p^{m+1}|p|^{\frac{n}{p-1}} \leq np|p|^{\frac{n}{p-1}},$$

proving the other inequality. □

The following theorem will be crucial in constructing p-adic L-functions by interpolation.

Theorem 3.4. *Let $(b_n)_{n\geq 0}$ be a sequence in K and $(c_n)_{n\geq 0}$ be defined by*

$$e^{-t}\sum_{n=0} b_n \frac{t^n}{n!} = \sum_{n=0}^{\infty} c_n \frac{t^n}{n!}.$$

Suppose there is a real number R, $0 < R < |p|^{\frac{1}{p-1}} < 1$ such that $|c_n| \leq C \cdot R^n$. Then there is a power series $A(x) \in P_K$ such that

1. *$A(x)$ coverges for all ξ such that $|\xi| < \frac{1}{R}|p|^{\frac{1}{p-1}}$,*
2. *$A(n) = b_n$.*

Proof. Let $A_k(x) = \sum_{i=0}^{k} c_i \binom{X}{i}$. Note that $\deg A_k \leq k$. We claim that $A_k(x)$ is a Cauchy sequence in P_K. We have that

$$\begin{aligned}\|A_\ell(x) - A_k(x)\| &= \left\| \sum_{i=k+1}^{\ell} c_i \binom{X}{i} \right\| \\ &\leq \max_{k+1\leq i\leq \ell} \left\| c_i \binom{X}{i} \right\| \\ &\leq \max_{k+1\leq i\leq \ell} CR^i \cdot p^{\frac{i}{p-1}}.\end{aligned}$$

Let $R_1 = Rp^{\frac{1}{p-1}}$. Note that $R_1 < 1$. Then by the above estimates

$$\|A_\ell(x) - A_k(x)\| \leq CR_1^{k+1},$$

showing that $A_k(x)$ is Cauchy.

By Proposition 3.2, there $A_k(x)$ converges, so let

$$A(x) = \lim_{k\to\infty} A_k(x) = \sum_{n=0}^{\infty} a_n x^n.$$

We may write

$$A_k(x) = \sum_{n=0}^{\infty} a_{n,k} x^n$$

where we note that $a_{n,k} = 0$ for $n \geq k$. Then $a_n = \lim_{k\to\infty} a_{n,k}$. Since $|a_n| = \lim_{k\to\infty} |a_{n,k}|$, the estimate

$$\begin{aligned}|a_{n,k}| &= |a_{n,k} - a_{n,n-1}| && \text{as } a_{n,n-1} = 0 \\ &\leq \|A_k - A_{n-1}\| \\ &\leq C \cdot R_1^n\end{aligned}$$

shows that $|a_n| \leq C \cdot R_1^n$.

Note that $A(x)$ converges for all ξ such that $|\xi| < \frac{1}{R_1}$ which shows (1). We now need to show that (2) $A(n) = b_n$.

We claim that $A(\xi) = \lim_{k\to\infty} A_k(\xi)$. We have that

$$A(\xi) - A_k(\xi) = \sum_{n=0}^{\infty}(a_n - a_{n,k})\xi^n.$$

For $n > k$, $a_{n,k} = 0$, so

$$|(a_n - a_{n,k})\xi^n| = |a_n\xi^n| \leq C \cdot R_1^n|\xi|^n \leq C \cdot (R_1|\xi|)^k.$$

For $n \leq k$,

$$|(a_n - a_{n,k})\xi^n| \leq \|A - A_k\||\xi|^n \leq CR_1^{k+1}|\xi|^n,$$

as $\|A - A_k\| \leq C \cdot R_1^{k+1}$. Finally, this shows that

$$|(a_n - a_{n,k})\xi^n| \leq \begin{cases} C \cdot R_1^{k+1} & \text{if } |\xi| < 1, \\ C \cdot R_1 \cdot (R_1|\xi|)^k & \text{if } |\xi| \geq 1. \end{cases}$$

As $k \to \infty$, these bounds show that $\lim_{k\to\infty}(A(\xi) - A_k(\xi)) = 0$. Finally, recall that $A_k(x) = \sum_{i=0}^{k} c_i\binom{X}{i}$, so

$$A_k(n) = \sum_{i=0}^{k} c_i\binom{n}{i} = b_n.$$

This shows existence and uniqueness follows from Lemma 3.1. □

This is the main tool that we will use to construct p-adic L-functions.

3.2. **Kubota–Leopoldt p-adic L-function.** Let p be an odd prime. The short exact sequence

$$1 \longrightarrow 1 + p\mathbb{Z}_p \longrightarrow \mathbb{Z}_p^\times \overset{\kappa}{\longrightarrow} \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times \longrightarrow 1$$

splits and the splitting is given by the map

$$\omega\colon \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times \to \{\text{roots of unity in } \mathbb{Z}_p^\times\}$$

defined by the relation $\omega(a) \equiv a\ (p)$. This is the *Teichmuller character*. We fix throughout embeddings $\overline{Q} \hookrightarrow \mathbb{C}$, $\overline{Q} \hookrightarrow \overline{\mathbb{Q}_p}$. Then ω defines a Dirichlet character via the first embedding.

The split short exact sequence shows that there is an isomorphism

$$\begin{aligned} \mathbb{Z}_p^\times &\to \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times \times (1 + p\mathbb{Z}_p) \\ a &\mapsto (\omega(a), \langle a\rangle). \end{aligned}$$

When $p = 2$, the situation is similar with p replaced by 4 where necessary:

$$1 \longrightarrow 1 + 4\mathbb{Z}_2 \longrightarrow \mathbb{Z}_2^\times \overset{\kappa}{\longrightarrow} \left(\tfrac{\mathbb{Z}}{4\mathbb{Z}}\right)^\times \longrightarrow 1.$$

We hence define

$$q = \begin{cases} p & \text{if } p \text{ odd} \\ 4 & \text{if } p = 2 \end{cases}$$

to deal with both cases simultaneously.

Theorem 3.5 (Kubota–Leopoldt)**.** *Let χ be a Dirichlet character and $K = \mathbb{Q}_p(\chi)$. Then there is a unique power series $A_\chi(x) \in P_K$ such that A_χ converges for $|\xi| < |q|^{-1}|p|^{\frac{1}{p-1}}$ and*

$$A_\chi(n) = (1 - \chi\omega^{-n}(p)p^{n-1})B_{n,\chi\omega^{-n}}.$$

Note that for primitive characters χ_1, χ_2, by $\chi_1\chi_2$ we mean the primitive character associated to the product.

We immediately note that the interpolation seems related to $L(1-n, \chi\omega^{-n})$ and investigate this further. First,

$$A_\chi(0) = (1 - \chi(p)p^{-1})B_{0,\chi} = \begin{cases} 0 & \text{if } \chi \neq \mathbb{1}, \\ (1 - p^{-1}) & \text{if } \chi = \mathbb{1}. \end{cases},$$

so we let

$$L_p(s, \chi) = \frac{1}{s-1}A_\chi(1-s).$$

Then

$$L_p(1-n, \chi) = \frac{1}{-n}(1 - \chi\omega^{-n}(p)p^{n-1})B_{n,\chi\omega^{-n}} = (1 - \chi\omega^{-n}(p)p^{n-1})L(1-n, \chi\omega^{-n}).$$

Therefore, this p-adic function interpolates the L-values of $L(s, \chi\omega^{-n})$.

The intuitive reason the factor $(1 - \chi\omega^{-n}(p)p^{n-1})$ comes up is that the sum $\sum \frac{1}{n^k}$ would behave badly p-adically if we allow p in the denominator. The reason for the Teichmuller character is a little harder to describe, but it is related to congruence between special values of L-functions.

We will next work towards proving this theorem. Recall that we define *Bernoulli numbers* via

$$\frac{te^t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}.$$

The *Bernoulli polynomials* are similarly defined by

$$e^{tx} \cdot \frac{te^t}{e^t - 1} = \sum_{n=0}^{\infty} B_n(x) \frac{t^n}{n!}.$$

Moreover, for a character χ, we defined the *generalized Bernoulli numbers* by

$$\sum_{a=1}^{f} \frac{\chi(a)te^{at}}{e^{ft} - 1} = \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!}.$$

Again, analogously, we define $B_{n,\chi}(x)$ the *generalized Bernoulli polynomials* by

$$e^{tx}\sum_{a=1}^{f}\frac{\chi(a)te^{at}}{e^{ft}-1}=\sum_{n=0}^{\infty}B_{n,\chi}(x)\frac{t^n}{n!}.$$

Proposition 3.6. *We have that*

(1) $B_{n,\mathbb{1}}(x)=B_n(x)$,
(2) $B_{n,\chi}(0)=B_{n,\chi}$,
(3) $B_{n,\chi}(x)=\sum_{i=0}^{n}\binom{n}{i}B_{i,\chi}x^{n-i}$,
(4) *if* $\chi\neq\mathbb{1}$, $B_{n,\chi}(-x)=(-1)^n\chi(-1)B_{n,\chi}(x)$ *and if* $\chi=1$, $B_{n,\mathbb{1}}(-x)=(-1)^nB_{n,\mathbb{1}}(x-1)$,
(5) $B_{n,\chi}=0$ *if* $\chi\neq\mathbb{1}$ *and* $n\equiv\delta$ (2),
(6) $B_{n,\chi}=f^{n-1}\sum_{a=0}^{f}\chi(a)B_n\left(\frac{a}{f}-1\right)$.

Proof. All of these properties are straightforward, so we just prove (6). We have that

$$\begin{aligned}\sum_{n=0}^{\infty}B_{n,\chi}(x)\frac{t^n}{n!}&=e^{tx}\sum_{a=1}^{f}\frac{te^{at}\chi(a)}{e^{ft}-1}\\&=\sum_{a=1}^{f}\frac{\chi(a)te^{t(a+x)}}{e^{ft}-1}\\&=\frac{1}{f}\sum_{a=1}^{f}\chi(a)\frac{(ft)e^{ft\frac{a+x}{f}}}{e^{ft}-1}\\&=\frac{1}{f}\sum_{a=1}^{f}\chi(a)\sum_{n=0}^{\infty}B_n\left(\frac{a+X}{f}-1\right)\frac{(ft)^n}{n!}.\end{aligned}$$

Then $B_{n,\chi}=B_{n,\chi}(0)=f^{n-1}\sum_{a=1}^{f}\chi(a)B_n\left(\frac{a}{f}-1\right)$. □

We may use Taylor expansions in the equality

$$\sum_{a=1}^{f}\chi(a)te^{at}=(e^{ft}-1)\sum_{n=0}B_{n,\chi}\frac{t^n}{n!}$$

to compute the Bernoulli numbers. In general, on the left side, we will get expressions of the form

$$S_{n,\chi}(k)=\sum_{a=1}^{k}\chi(a)a^n.$$

Lemma 3.7. *We have that*

(1) $S_{n,\chi}(kf)=\frac{1}{n+1}(B_{n+1,\chi}(kf)-B_{n+1,\chi}(0))$,
(2) $B_{n,\chi}=\lim_{h\to\infty}\frac{1}{p^hf}S_{n,\chi}(p^hf)$ *for any prime* p *(the limit is a* p*-adic limit).*

Proof. For (1), we let

$$F_\chi(t,x) = e^{tx}\sum_{a=1}^{f}\frac{\chi(a)te^{at}}{e^{ft}-1}.$$

Then

$$\begin{aligned}F_\chi(t,x)-F_\chi(t,x-f) &= e^{tx}\sum_{a=1}^{f}\frac{\chi(a)te^{at}}{e^{ft}-1} - e^{t(x-f)}\sum_{a=1}^{f}\frac{\chi(a)te^{at}}{e^{ft}-1}\\ &= \sum_{a=1}^{f}\frac{\chi(a)te^{at}}{e^{ft}-1}e^{tx}(1-e^{-ft})\\ &= \sum_{a=1}^{f}\chi(a)te^{t(x+a-f)}.\end{aligned}$$

Taking coefficients of t^n on both sides, we see that

$$\frac{B_{n,\chi}(x)-B_{n,\chi}(x-f)}{n!} = \sum_{a=1}^{f}\chi(a)\frac{(x+a-f)^{n-1}}{(n-1)!},$$

$$B_{n,\chi}(x)-B_{n,\chi}(x-f) = n\sum_{a=1}^{f}\chi(a)(x+a-f)^{n-1}.$$

Plugging in $x = f, 2f, \ldots, kf$, we see that

$$B_{n,\chi}(f)-B_{n,\chi}(0) = n\sum_{a=1}^{f}\chi(a)(a)^{n-1}$$

$$B_{n,\chi}(2f)-B_{n,\chi}(f) = n\sum_{a=1}^{f}\chi(a)(a+f)^{n-1}$$

$$\vdots$$

$$B_{n,\chi}(kf)-B_{n,\chi}((k+1)f) = n\sum_{a=1}^{f}\chi(a)(a+(k-1)f)^{n-1}$$

and summing these together, we get

$$B_{n,\chi}(kf)-B_{n,\chi}(0) = n\sum_{a=1}^{kf}\chi(a)a^{n-1}.$$

This shows (1).

We will use (1) to show (2). We have that

$$B_{n+1,\chi}(x) = \sum_{i=0}^{n+1}\binom{n+1}{i}B_{i,\chi}x^{n+1-i}.$$

Thus

$$B_{n+1,\chi}(kf)-B_{n+1,\chi}(0) = \sum_{i=0}^{n}\binom{n+1}{i}B_{i,\chi}(kf)^{n+1-i}.$$

Let $k = p^h$. Then

$$\frac{B_{n+1,\chi}(p^h f) - B_{n+1,\chi}(0)}{p^h f} = \sum_{i=0}^{n} \binom{n+1}{i} B_{i,\chi}(p^h f)^{n-i}.$$

Now, take the p-adic limit as $h \to \infty$:

$$\lim_{h\to\infty} \left(\frac{B_{n+1,\chi}(p^h f) - B_{n+1,\chi}(0)}{p^h f} \right) = (n+1) B_{n,\chi}.$$

By (1), we have that

$$\lim_{h\to\infty} \frac{S_{n,\chi}(p^h f)}{p^h f} = B_{n,\chi}.$$

This shows (2). □

We are finally ready to prove the existence of the p-adic L-function.

Proof of Theorem 3.5. We want to use Theorem 3.4. Let $\chi_n = \chi\omega^{-n}$ and

$$b_n = (1 - \chi_n(p)p^{n-1}) B_{n,\chi_n}.$$

Observe that $B_{n,\chi_n} = \lim_{h\to\infty} \frac{1}{p^h f} S_{h,\chi_n}(p^h f)$. This is true by Lemma 3.7 after noting that the conductor of χ_n is $f \cdot p^\epsilon$ where $\epsilon \in \{0, 1, -1\}$. Then

$$\begin{aligned}
b_n &= \lim_{h\to\infty} \frac{1}{p^h f} S_{n,\chi_n}(p^h f) - \chi_n(p)p^{n-1} \lim_{h\to\infty} \frac{1}{p^h f} S_{n,\chi_n}(p^h f) \\
&= \lim_{h\to\infty} \frac{1}{p^h f} S_{n,\chi_n}(p^h f) - \chi_n(p)p^{n-1} \lim_{h\to\infty} \frac{1}{p^{h-1} f} S_{n,\chi_n}(p^{h-1} f) \quad \text{letting } h \mapsto h-1 \text{ in second limit} \\
&= \lim_{h\to\infty} \frac{1}{p^h f} S_{n,\chi_n}(p^h f) - \chi_n(p)p^{n-1} \lim_{h\to\infty} \frac{1}{p^{h-1} f} \sum_{a=1}^{p^{h-1} f} \chi_n(a) a^n \\
&= \lim_{h\to\infty} \frac{1}{p^h f} \sum_{a=1}^{p^h f} \chi_n(a) a^n - \lim_{h\to\infty} \frac{1}{p^h f} \sum_{a=1}^{p^{h-1} f} \chi_n(ap)(ap)^n \\
&= \lim_{h\to\infty} \frac{1}{p^h f} \sum_{\substack{a=1 \\ (a,p)=1}}^{p^h f} \chi_n(a) a^n \\
&= \lim_{h\to\infty} \frac{1}{p^h f} \sum_{\substack{a=1 \\ (a,p)=1}}^{p^h f} \langle a \rangle^n \chi(a) \qquad \text{as } \chi_n(a) = \chi(a)\omega(a)^{-n} \\
&= \lim_{h\to\infty} \frac{1}{q^h f} \sum_{\substack{a=1 \\ (a,p)=1}}^{q^n f} \chi(a) \langle a \rangle^n.
\end{aligned}$$

Recall that in Theorem 3.4, we have that

$$c_n = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} b_i.$$

Then

$$c_n = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} \lim_{h\to\infty} \frac{1}{q^h f} \sum_{\substack{a=1 \\ (a,p)=1}}^{q^h f} \chi(a)\langle a\rangle^i = \lim_{h\to\infty} \frac{c_{n,h}}{q^h f}$$

for

$$c_{n,h} = \sum_{i=0}^{n} \sum_{\substack{a=1 \\ (a,p)=1}}^{q^h f} (-1)^{n-i} \binom{n}{i} \chi(a)\langle a\rangle^i.$$

Then

$$c_{n,h} = \sum_{a=1}^{q^h f} \chi(a) \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} \langle a\rangle^i = \sum_{\substack{a=1 \\ (a,p)=1}}^{q^h f} \chi(a)(\langle a\rangle - 1)^n.$$

We claim that

$$\frac{c_{n,h}}{q^h f} \equiv 0 \mod \frac{q^n}{q^2 f}$$

(for n large enough). In other words, $\frac{\frac{c_{n,h}}{q^h f}}{\frac{q^n}{q^2 f}}$ is a p-adic integer. To show this, we proceed by induction on h. For $h = 1$, we have that

$$\frac{c_{n,1}}{qf} = \frac{1}{qf} \sum_{\substack{a=1 \\ (a,p)=1}}^{qf} \chi(a)(\langle a\rangle - 1)^n$$

which is congruent to 0 modulo $\frac{q^n}{q^2 f}$, since $\langle a\rangle \equiv 1 \mod q$. For $h \geq 1$, recall that

$$\frac{c_{n,h+1}}{q^{h+1} f} = \frac{1}{q^{h+1} f} \sum_{\substack{a=1 \\ (a,p)=1}}^{q^h f} \chi(a)(\langle a\rangle - 1)^n.$$

For $1 \leq a \leq q^{n+1} f$, let $a = u + q^h f v$ for $1 \leq u \leq q^h f$, $0 \leq v < q$. Then $\omega(a) = \omega(u)$, so

$$\langle a\rangle = \omega(a)^{-1} a = \omega(u)^{-1}(u + q^h f v) = \langle u\rangle + \omega(u)^{-1} q^h f v.$$

Then

$$(\langle a\rangle - 1)^n = \sum_{i=0}^{n} \binom{n}{i} (\langle u\rangle - 1)^i (\omega(u)^{-1} q^h f v)^{n-i}.$$

We claim that:

$$(\langle a\rangle - 1)^n \equiv (\langle u\rangle - 1)^n \mod q^{n+h-1}.$$

This is because q^i divides $(\langle u\rangle - 1)^i$ and q^{n-i} divides the second term, and $i + h(n-i) = i + (n-i) + (h-1)(n-i) = n + (h-1)(n-i) \geq n + h - 1$ if $n - i \geq 1$. Thus, modulo

q^{n_h-1}, only the $i=n$ term survives. We have that

$$\begin{aligned} c_{n,h+1} &= \sum_{\substack{a=1\\(a,p)=1}}^{q^h f} \chi(a)(\langle a\rangle - 1)^n \\ &\equiv q \sum_{\substack{u=1\\(u,p)=1}}^{q^h f} \chi(u)(\langle u\rangle - 1)^n \\ &\equiv q c_{n,h} \mod q^{n+h-1} \end{aligned}$$

so

$$\frac{c_{n,h+1}}{q^{h+1}f} \equiv \frac{c_{n,k}}{q^h f} \mod \frac{q^{n+h-1}}{q^{n+1}f},$$

completing the proof. □

3.3. **p-adic logarithms, exponential functions, and power functions.** We will next work towards Leopoldt's theorem about the value $L_p(1,\chi)$. Note that 1 is outside of the normal interpolation range: $1-n$ for $n \geq 1$.

We first recall some facts and p-adic logarithms, exponential functions, and power functions.

Recall that the p-adic log is defined by the power series

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

which converges for $1+\xi$ where $\frac{|\xi|^n}{|n|} \to 0$ as $n \to \infty$, i.e. for $|\xi| < 1$. Then

$$\log_p \colon \underbrace{\{x \in \mathbb{C}_p \mid |x-1| < 1\}}_{U_1} \to \mathbb{C}_p$$

is a continuous homomorphism (checking that $\log_p(xy) = \log_p(x) + \log_p(y)$ is left as an exercise).

Theorem 3.8. *There is a unique extension of* $\log_p$ *to a homomorphism*

$$\log_p \colon \mathbb{C}_p^\times \to \mathbb{C}_p$$

such that $\log_p(p) = 0$. *Further,* $\log_p$ *is continuous and for all* $\sigma \in \mathrm{Aut}(\mathbb{C}_p/\mathbb{Q}_p) = \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$, $\log_p(\alpha)^\sigma = \log_p(\alpha^\sigma)$.

The choice of $\log_p(p) = 0$ is equivalent to choosing a branch of the logarithm. Note that the last identity is not true for complex analytic logs. This will make working with the p-adic logarithm much easier.

Proof. We have the following diagram

$$\begin{array}{ccc} \mathbb{C}_p^\times & & \\ | & & \\ \overline{\mathbb{Q}_p}^\times & \longrightarrow & \mathbb{Q} \\ | & & | \\ \mathbb{Q}_p^\times & \longrightarrow & \mathbb{Z} \end{array}$$

where the map is given by $\alpha \mapsto r$ if $|\alpha| = p^{-r}$.

Pick a section of this homomorphism, $r \mapsto P_r \in \overline{\mathbb{Q}_p}^\times$ such that $P_r \times P_s = P_{r+s}$ and if $r \in \mathbb{Z}$, then $P_r = p^r$. We may let $P_r = p^{m/n} = (p^m)^{1/n}$ for $r = m/n$, embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}$.

Let P be the image of this section. We have that $P \subseteq \overline{\mathbb{Q}_p}^\times \subseteq \mathbb{C}_p^\times$. We claim that

$$\mathbb{C}_p^\times = P \times W \times U_1$$

where W is the set of roots of unity in $\overline{\mathbb{Q}_p}$ of order prime to p and

$$U_1 = \{x \in \mathbb{C}_p \mid |x - 1| < 1\}.$$

For $\alpha \in \mathbb{C}_p^\times$, pick $\alpha_1 \in \overline{\mathbb{Q}_p}$ such that α_1 is close enough to α. Then $|\alpha| = |\alpha_1| = |P_r|$ for some $P_r \in P$. Therefore:

$$\left|\frac{\alpha}{P_r}\right| = 1$$

and setting $\beta = \frac{\alpha}{P_r}$, we can choose $\beta \in \mathbb{Q}_p^\times$ close enough to β such that

$$|\beta_1| = |\beta| = 1.$$

Consider $\mathbb{Q}_p \subseteq \mathbb{Q}_p(\beta_1)$. Then β_1 is a unit in $\mathcal{O}_K$ and if we consider the reduction map

$$\begin{array}{ccccc} & & \beta_1 & \longrightarrow & \overline{\beta_1} \\ \mathfrak{p} & & \mathcal{O}_K & \longrightarrow & \mathcal{O}_K/\mathfrak{p} = \mathbb{F}_{p^f} \\ | & & | & & | \\ (p) & & \mathbb{Z}_p & \longrightarrow & \mathbb{Z}_p/(p) = \mathbb{F}_p \end{array}$$

Since $\overline{\beta_1}^n = 1$ for some (n, p), by Hensel's Lemma, we can lift $\overline{\beta_1}$ to some nth root of unity $w \in \mathcal{O}_K^\times$ such that $\omega \equiv \beta_1 \mod \mathfrak{p}$. Then $|\omega - \beta_1| < 1$, and hence $|\beta_1/\omega - 1| < 1$, so $\beta_1/\omega \in U_1$.

We have hence written

$$\alpha = P_r \frac{\alpha}{P_r} = P_r \omega \frac{\beta}{\omega}.$$

Since β_1 is close to β, $\frac{\beta}{\omega} \in U_1$. We finally need to show that the product is direct. Suppose $P_r \cdot \omega \cdot u = 1$. Then $|P_r| = 1$, so $P_r = 1$, and hence $\omega \cdot u = 1$. Since $|\omega - 1| < 1$, $\omega = 1$, and hence also $u = 1$. We have hence shown that

$$\mathbb{C}_p^\times = P \times W \times U_1.$$

For $r = \frac{m}{n}$, $P_r^n = P_m = p^m$, so $n \log_p P_r = m \log_p p$. Setting $\log p = 0$, we get that

$$\log_p(P_r \omega u) = \log_p(u).$$

This defines the logarithm on $\mathbb{C}_p^\times$.

We finally have to show that $\log_p(\alpha^\sigma) = \log_p(\alpha)^\sigma$. Let $\alpha = P_r \omega u$. Then

$$\alpha^\sigma = P_r^\sigma \omega^\sigma u^\sigma.$$

For $r = \frac{m}{n}$, $P_r^n = p^m$, so $(P_r^\sigma) = p^m$. Hence $P_r^\sigma = P_r \cdot (n\text{th root of unity})$, showing that

$$n \log_p P_r^\sigma = m \log_p p = 0.$$

Finally, this shows that

$$\log_p(\alpha^\sigma) = \log(u^\sigma) = \log(u)^\sigma,$$

completing the proof. □

We define $\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$. To check convergence, recall that

$$|n!| \geq |p|^{\frac{n}{p-1}},$$

so

$$\left| \frac{\xi^n}{n!} \right| \leq \frac{|\xi|^n}{|p|^{\frac{n}{p-1}}},$$

showing that the above power series converges for

$$|\xi| < |p|^{\frac{1}{p-1}}.$$

Exercise. If $|x| < |p|^{\frac{1}{p-1}}$, then $\log_p(\exp(x)) = x$ and $\exp(\log_p(1+x)) = 1 + x$.

We want to define x^s for $s \in \mathbb{Z}_p$ as $\exp(s \log_p(x))$. For $x \in 1 + p\mathbb{Z}_p$, $\log_p(x) \in p\mathbb{Z}_p$, i.e. $|\log_p(x)| \leq |p| < |p|^{\frac{1}{p-1}}$ if $p \neq 2$. To deal with the case $p = 2$, we note that for $x \in 1 + q\mathbb{Z}_p$, we have that $\log_p(x) \in q\mathbb{Z}_p$, and we may define

$$x^s = \exp(s \log_p(x)).$$

However, we would still like to extend this to $1 + p\mathbb{Z}_p$ for all p.

Lemma 3.9. *For $x \in 1 + q\mathbb{Z}_p$ and $s \in \mathbb{Z}_p$,*

$$x^s = \sum_{n=0}^{\infty} \binom{s}{n} (x-1)^n.$$

Proof. We use the proof of Theorem 3.4. Here $c_n = (x-1)^n$ and we know that $|c_n| \leq |q|^n$. Then the right hand side converges for

$$|s| \leq \frac{1}{|q|} |p|^{\frac{1}{p-1}}.$$

In particular, it converges for $s \in \mathbb{Z}_p$. To check that the left hand side is equal to the right hand side, it suffices to check at all the integers (which are dense in $\mathbb{Z}_p$). We have that

$$\begin{aligned}\sum_{n=0}^{\infty} \binom{m}{n}(x-1)^n &= \sum_{n=0}^{m} \binom{m}{n}(x-1)^n \\ &= (x-1+1)^m \\ &= x^m,\end{aligned}$$

completing the proof. □

We may hence define x^s for $x \in 1+2\mathbb{Z}_p$ and $s \in \mathbb{Z}_2$ by the right hand side in the above lemma.

We now have defined x^s for $x \in 1+p\mathbb{Z}_p$ and $s \in \mathbb{Z}_p$. We want to analyze it as a function of the two variables. We define a function

$$\phi\colon \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$$

by

$$\phi(x,s) = \begin{cases} 0 & \text{if } x \notin \mathbb{Z}_p^\times, \\ \langle x \rangle^s & \text{if } p \neq 2,\ x \in \mathbb{Z}_p^\times, \\ x^s & \text{if } p = 2,\ x \in \mathbb{Z}_p^\times. \end{cases}$$

Consider a finite extension K of $\mathbb{Q}_p$. Then $C_K = \{f\colon \mathbb{Z}_p \to K \text{ continuous}\}$. Set

$$\|f\| = \sup_{x \in \mathbb{Z}_p} |f(x)| = \max_{x \in \mathbb{Z}_p} |f(x)|.$$

Note that

$$\|f+g\| \leq \max(\|f\|, \|g\|)$$

$$\|fg\| = \|f\|\|g\|,$$

$$\|af\| = |a|\|f\|,$$

and C_K is complete for $\|–\|$. Indeed, if f_n is a Cauchy sequence in C_k, for each s, $f_n(S)$ is a Cauchy sequence in K, so we may set $f(s) = \lim_n f_n(s)$ and this function is continuous.

Note that $K[x] \hookrightarrow C_K$, so, for example, the function $\binom{s}{n}$ is in C_K.

We define $\gamma_n \in C_K$ by

$$\gamma_n(s) = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} \phi(i,s).$$

Proposition 3.10. *We have that*

$$\phi(x,s) = \sum_{n=0}^{\infty} \gamma_n(s) \binom{x}{n}.$$

We first state a lemma.

Lemma 3.11. *We have that*

$$\sum_{i=0}^{n}(-1)^{n-i}\binom{n}{i}i^m$$

is divisible by $n!$.

We will prove this later.

Proof of Proposition 3.10. First, let us check this for $x = m$, Then the right hand side is

$$\begin{aligned}\sum_{n=0}^{m}\gamma_n(s)\binom{m}{n} &= \sum_{n=0}^{m}\binom{m}{n}\sum_{i=0}^{n}(-1)^{n-i}\binom{n}{i}\phi(i,s)\\ &= \sum_{i=0}^{m}\phi(i,s)\sum_{n=i}^{m}\binom{m}{n}\binom{n}{i}(-1)^{n-i}\end{aligned}$$

and we have that

$$\begin{aligned}\sum_{n=i}^{m}\binom{m}{n}\binom{n}{i}(-1)^{n-i} &= \sum_{n=i}^{m}\frac{m!}{n!(m-n)!}\frac{n!}{(n-i)!i!}(-1)^{n-i}\\ &= \frac{m!}{i!}\sum_{n=i}^{m}\frac{(-1^{n-i}}{(m-n)!(n-i)!}\\ &= \frac{m!}{i!}\sum_{t=0}^{m-i}\frac{(-1)^t}{(m-i-t)!t!} \qquad \text{where } n-i=t\\ &= \frac{m!}{i!}(1+(-1))^{m-i}\\ &= \delta_{mi}.\end{aligned}$$

Altogether, this shows that

$$\sum_{n=0}^{m}\gamma_n(s)\binom{m}{n} = \phi(m,s).$$

We claim that $\|\gamma_n\| \leq |n!|$. Pick a large integer m such that $p-1$ divides m and $|p^m| < |n!|$. Then we have that

$$\gamma_n(m) = \sum_{i=0}^{n}(-1)^{n-i}\binom{n}{i}\phi(i,m).$$

Now, for $i \in p\mathbb{Z}_p$, $\phi(i,m) = 0$ and otherwise $\phi(i,m) = \langle i\rangle^m = (i\omega(i)^{-1})^m = i^m$ since $p-1|m$. We then see that

$$\begin{aligned}\gamma_n(m) &= \sum_{i=0}^{n}(-1)^{n-i}\binom{n}{i}\phi(i,m)\\ &\equiv \sum_{i=0}^{n}(-1)^{n-i}\binom{n}{i}i^m \mod p^m.\end{aligned}$$

By Lemma 3.11, we see that $|\gamma_n(m)| \leq |n!|$. Since such m are dense in $\mathbb{Z}_p$, we have that $\|\gamma_n\| \leq |n!|$.

Now, we use Lemma 3.3 to conclude that

$$\|\gamma_n\| \leq |n!| \leq np|p|^{\frac{n}{p-1}}.$$

For $x \in \mathbb{Z}_p$, we have that $\left|\binom{x}{n}\right|$ is bounded and since $|\gamma_n(s)| \leq |n!| \to 0$ as $n \to \infty$, this shows convergence.

Hence the two functions are continuous functions $\mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$ which agree on a dense subset, and hence are equal. □

We now prove the lemma.

Proof of Lemma 3.11. We have that

$$\begin{aligned}(e^x-1)^n &= \sum_{i=0}^{n}(-1)^{n-i}\binom{n}{i}(e^x)^i \\ &= \sum_{i=0}^{n}(-1)^{n-i}\binom{n}{i}\sum_{m=0}^{\infty}\frac{(xi)^m}{m!} \\ &= \sum_{m=0}^{\infty}\frac{x^m}{m!}\underbrace{\sum_{i=0}^{n}(-1)^{n-i}\binom{n}{i}i^m}_{d_{m,n}}\end{aligned}$$

We have that

$$d_{m,n} = \frac{d^m}{dx^m}(e^x-1)^n\Big|_{x=0}.$$

We have that

$$\frac{d^m}{dx^m}(e^x-1)^n = \frac{d^{m-1}}{dx^{m-1}}(x(e^x-1)^{n-1}e^x) = \frac{d^{m-1}}{dx^{m-1}}(x(e^x-1)^n + n(e^x-1)^{n-1}),$$

showing that

$$d_{m,n} = nd_{m-1,n} + nd_{m-1,n-1}.$$

By induction on m, we see that $n!|d_{m,n}$. □

Let $C_K = \{f\colon \mathbb{Z}_p \to K \| \text{ continuous}\}$ and

$$\mathcal{Q}_K = \{\text{formal power series } A = \sum_{n=0}^{\infty} x^n \mid a_n \in K,\ |a_n n!| \to \infty\}$$

with the sup norm $\|A\| = \sup_n |a_n n!|$. Then $K[x] \subseteq \mathcal{Q}_K$ is a dense subset.

Theorem 3.12. *There is a unique bounded linear map*

$$\Gamma\colon \mathcal{Q}_K \to C_K$$

such that $\Gamma(x^n) = \gamma_n(s)$. *It satisfies* $\Gamma((1+x)^n) = \phi(n,s)$.

Proof. Define a map $\Gamma\colon K[x] \to C_K$ by $\Gamma(x^n) = \gamma_n(s)$.

We have that $\|x^n\|_{\mathbb{Q}} = |n!|$, $\|\gamma_n\| \leq |n!|$, so $\|\Gamma(x^n)\| \leq \|x^n\|_{\mathbb{Q}}$. Hence

$$\|\Gamma(A)\| \leq \|A\|_{\mathbb{Q}} \text{ for all } A \in K[x].$$

Hence Γ is a continuous function $K[x] \to C_K$ and we may extend it uniquely to a bounded linear map $\mathbb{Q}_K \to C_K$. Then

$$\begin{aligned}\Gamma((1+n)^n) &= \Gamma\left(\sum_{i=0}^{n}\binom{n}{i}x^i\right)\\ &= \sum_{i=0}^{n}\binom{n}{i}\gamma(i,s)\\ &= \sum_{i=0}^{\infty}\binom{n}{i}\gamma(i,s)\\ &= \phi(n,s)\end{aligned}$$

by Proposition 3.10. □

Write $\Gamma(A) = \Gamma_A$. We write down a formula for $\Gamma_A(s)$.

Proposition 3.13. *Define $\delta_n(A)$ by*

$$A(e^t - 1) = \sum_{n=0}^{\infty}\delta_n(A)\frac{t^n}{n!}.$$

Then $\Gamma_A(s) = \lim_{n_i}\delta_{n_i}(A)$, where (n_i) is a sequence of integers such that $n_i \to \infty$ in $\mathbb{Z}$, $(p-1)|n_i$, and $n_i \to s$ in $\mathbb{Z}_p$.

Proof. Recall that

$$(e^t - 1)^n = \sum_{m=0}^{\infty}\frac{t^m}{m!}d_{m,n}$$

and we showed in Lemma 3.11 that $|d_{m,n}| \le |n!|$.

If $A = \sum_{n=0}^{\infty} a_n x^n$, then

$$A(e^t-1) = \sum_{n=0}^{\infty}a_n(e^t-1)^n = \sum_{n=0}^{\infty}a_n\sum_{m=0}^{\infty}\frac{t^m}{m!}d_{m,n} = \sum_{i=0}^{\infty}a_i\sum_{m=0}^{\infty}\frac{t^m}{m!}d_{m,i}.$$

What is $\delta_n(A)$? We have that

$$\delta_n(A) = \sum_{i=0}^{\infty}a_i d_{n,i}.$$

Since $|a_i d_{n,i}| \le |a_i i!|$, we have that

$$|\delta_n(A)| \le \sup_{0\le i\le n}|a_i i!| \le \|A\|_{\mathbb{Q}}.$$

To check the equality on polynomials $K[x]$, it is enough to check it for $A = (1+x)^m$. In that case, the left hand side is

$$\Gamma_A(s) = \phi(m,s)$$

and we need to check the right hand side is equal to this. We have that

$$A(e^t - 1) = \sum_{n=0}^{\infty} \frac{(mt)^n}{n!},$$

so $\delta_n(A) = m^n$. We need to evaluate $\lim_i m^{n_i}$. If $p|m$, $\phi(m,s) = 0$ and $\lim_i m^{n_i} = 0$ since $n_i \to \infty$ as integers.

In the case p not dividing m, we need to consider the two subcases $p = 2$ and p odd. We just deal with p odd, the other case is similar. Here, the left hand side is

$$\langle m \rangle^s$$

whereas the right hand side is

$$\lim_i m^{n_i} = \lim_i \langle m \rangle^{n_i} = \langle m \rangle^s$$

since $(p-1)|n_i$ and $n_i \to s$ p-adically. Therefore, the formula holds for all polynomials.

Finally, let $A \in \mathbb{Q}_K$. Fix $\epsilon > 0$. Then, there exists $B \in K[x]$ such that $\|A - B\|_{\mathbb{Q}} < \epsilon$. This implies that $\|\Gamma_A - \Gamma_B\| < \epsilon$. We then estimate

$$\begin{aligned} |\Gamma_A(s) - \delta_{n_i}(A)| &= |\Gamma_A(s) - \Gamma_B(s) + \Gamma_B(s) - \delta_{n_i}(B) + \delta_{n_i}(B) - \delta_{n_i}(A)| \\ &\leq \max\{\underbrace{|\Gamma_A(s) - \Gamma_B(s)|}_{<\epsilon}, \underbrace{|\Gamma_B(s) - \delta_{n_i}(B)|}_{<\epsilon \text{ for } i \gg 0}, \underbrace{|\delta_{n_i}(B) - \delta_{n_i}(A)|}_{\leq \|A-B\|_{\mathbb{Q}} < \epsilon}\} \\ &< \epsilon, \end{aligned}$$

completing the proof. □

Proposition 3.14. *Let* $A(x) = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{Q}_K$ *and*

$$\begin{aligned} A'(x) &= \sum_{n=0}^{\infty} n a_n x^{n-1} \in \mathbb{Q}_K, \\ (DA)(x) &= (1+x)\log(1+x)A'(x). \end{aligned}$$

Then $DA \in \mathbb{Q}_K$ *and* $\Gamma_{DA}(s) = s\Gamma_A(s)$.

Proof. We have that

$$\begin{aligned} (DA)(e^t - 1) &= te^t A'(e^t - 1) \\ &= \left(t\frac{d}{dt}\right) A(e^t - 1) \\ &= \left(t\frac{d}{dt}\right) \sum_{n=0}^{\infty} \delta_n(A) \frac{t^n}{n!} \\ &= \sum_{n=0}^{\infty} (n\delta_n(A)) \frac{t^n}{n!} \end{aligned}$$

By Proposition 3.13, we have that

$$\Gamma_{DA}(s) = \lim_i (n_i \delta_{n_i}(A)) = s \cdot \Gamma_A(s).$$

This completes the proof. □

Consider $A(x) = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{Q}_K$. Then $|a_n n!| \to 0$ and for $|\xi| \leq |p|^{\frac{1}{p-1}}$, since $|n!| \geq |p|^{\frac{n}{p-1}}$ by Lemma 3.3, so

$$|a_n \xi^n| \leq |a_n| \cdot |p|^{\frac{n}{p-1}} \leq |a_n n!| \to 0.$$

This shows that $A(\xi) = \sum_{n=0}^{\infty} a_n \xi^n$ converges.

For such ξ, $A(\xi)$ is defined and $|A(\xi)| \leq \|A\|_{\mathbb{Q}_K}$. In particular, this shows that $\xi \mapsto A(\xi)$ is continuous.

Proposition 3.15. *Let $A \in \mathbb{Q}_K$. Then*

$$\Gamma_A(0) = A(0) - \frac{1}{p} \sum_{\xi^p = 1} A(\xi - 1).$$

Proof. Since both sides are continuous in A, it is enough to check equality for polynomials $A \in K[x]$. Let $A(x) = (1+x)^m$. Then

$$\Gamma_A(s) = \phi(m, s).$$

If $p|m$, the left hand side is $\phi(m, s) = 0$ and the right hand side is

$$A(0) = 1 - \frac{1}{p} \sum_{\xi^p = 1} \xi^m = 0.$$

If p does not divide m, the left hand side is 1 and the right hand side is

$$1 - \frac{1}{p} \sum_{\xi^p = 1} \xi^m = 1.$$

This completes the proof. □

3.4. **Leopoldt's formula for $L_p(1, \chi)$.** The goal of this section is to prove a formula analogous to the one in section 2.7 about $L_p(1, \chi)$.

Suppose now that χ is a primitive character of conductor f. Let ζ be a fixed primitive fth root of unity. We may take $\zeta = e^{2\pi i/f}$. Let

$$h(z) = \sum_{a=1}^{f} \chi(a) z^{a-1},$$

$$H(z) = \frac{h(z)}{z^f - 1} = \sum_{a=1}^{f} \frac{\chi(a) z^{a-1}}{z^f - 1}.$$

Writing

$$\frac{1}{z^f - 1} = \sum_{a=1}^{f} \frac{1}{(z - \zeta^s)} \frac{\zeta^a}{f},$$

we have that

$$H(z) = \sum_{a=1}^{f} \frac{h(\zeta^a)}{z - \zeta^a} \frac{\zeta^a}{f}.$$

Now,

$$h(\zeta^a)\zeta^a = \sum_{b=1}^{f} \chi(b)(\zeta^a)^{b-1}\zeta^a = \sum_{b=1}^{f} \chi(b)(\zeta^a)^b = \overline{\chi}(a)\mathfrak{g}_\chi.$$

Finally,

$$H(z) = \frac{\mathfrak{g}_\chi}{f} \sum_{a=1}^{f} \frac{\overline{\chi}(a)}{z - \zeta^a}.$$

On the other hand,

$$H(e^t) = \sum_{a=1}^{f} \frac{\chi(a)e^{t(a-1)}}{e^{ft} - 1},$$

so we define

$$F(t) = te^t H(e^t) = \sum_{a=1}^{f} \frac{\chi(a)te^{at}}{e^{ft} - 1} = \sum_{n=0}^{\infty} B_{n,\chi}\frac{t^n}{n!}. \tag{1}$$

Pick an auxiliary integer N such that $(N, fp) = 1$. Let $\{\lambda\}$ be the set of all Nth roots of unity in $\overline{\mathbb{Q}_p}$.

Lemma 3.16. *We have that*

$$\frac{\mathfrak{g}_\chi}{f} \sum_{a=1}^{f} \sum_{\lambda} \frac{\overline{a}}{z - \lambda\zeta^a} = N\chi(N)z^{N-1}H(z^N).$$

In particular,

$$\frac{\mathfrak{g}_\chi}{f} \sum_{a=1}^{f} \sum_{\lambda \neq 1} \frac{\overline{\chi}(a)}{z - \lambda\zeta^a} = N\chi(N)z^{N-1}H(z^N) - H(z).$$

Proof. We have

$$\sum \frac{1}{z - \lambda\alpha} = \frac{Nz^{N-1}}{Z^N - \alpha^N}$$

so

$$\frac{\mathfrak{g}_\chi}{f} \sum_{a=1}^{f} \sum_{\lambda} \frac{\overline{a}}{z - \lambda\zeta^a} = \frac{\mathfrak{g}_\chi}{f} \sum_{a=1}^{f} \frac{\overline{\chi}(a)Nz^{N-1}}{z^N - \zeta^{aN}} = \frac{\mathfrak{g}_\chi\chi(N)}{f} \sum_{a=1}^{f} \frac{\overline{\chi}(aN)Nz^{N-1}}{z^N - \zeta^{aN}} = \mathfrak{g}_\chi N\chi(N)H(z^N),$$

which is what we claimed. The second assertion follows from the above description of $H(z)$. □

Theorem 3.17 (Leopoldt's theorem)**.** *We have that*

$$L_p(1, \chi) = -\frac{\mathfrak{g}_\chi}{f}\left(1 - \frac{\chi(p)}{p}\right) \sum_{a=1}^{f} \overline{\chi}(a) \log_p(1 - \zeta^a).$$

Comparing this to the standard equation for for $L(1,\chi)$, the only difference is the Euler factor at p which was taken out when we defined L_p, so we need to put it back in, and the use of p-adic logarithm instead of regular logarithm.

In the proof of the theorem, we will take $K/\mathbb{Q}_p$ containing $\{\lambda\}$, ζ, and the values of χ. We will then show that for

$$A(x) = \frac{\mathfrak{g}_\chi}{f}\sum_{a=1}^{f}\sum_{\lambda\neq 1}\overline{\chi}(a)\log\left(1+\frac{x}{1-\lambda\zeta^a}\right)$$

we have that

$$\Gamma_A(s) = (1-\chi(N)\langle N\rangle^s)L_p(1-s,\chi)$$

if p is odd (and similarly for $p=2$), and use Proposition 3.15 to get the result.

We first with proving the above formula for $\Gamma_A(s)$.

Theorem 3.18. *Let $K/\mathbb{Q}_p$ be a finite extension containing $\{\lambda\}$, ζ, and the values of χ. Let*

$$A(x) = \frac{\mathfrak{g}_\chi}{f}\sum_{a=1}^{f}\sum_{\lambda\neq 1}\overline{\chi}(a)\log\left(1+\frac{x}{1-\lambda\zeta^a}\right).$$

Then $A(x)\in\mathcal{Q}_K$ and

$$\Gamma_A(s) = \begin{cases}(1-\chi(N)\langle N\rangle^s)L_p(1-s,\chi) & \text{if } p \text{ is odd,}\\ (1-\chi(N)N^s)L_p(1-s,\chi) & \text{if } p=2.\end{cases}$$

Proof. Note that $(!-\lambda\zeta^a)$ is a unit, so $\log\left(1+\frac{x}{1-\lambda\zeta^a}\right)\in\mathcal{Q}_K$. This shows that $A(x)\in\mathcal{Q}_K$.

We suppose p is odd. The case $p=2$ is dealt with in the same way, omitting all the occurrences of $\langle-\rangle$. The idea is to use Proposition 3.13 to find $\Gamma_{DA}(s)$ and the apply Proposition 3.14. We have that

$$\begin{aligned}DA(x) &= \frac{\mathfrak{g}_\chi}{f}(1+x)\log(1+x)\sum_{a=1}^{f}\sum_{\lambda\neq 1}\overline{\chi}(a)\frac{1}{1+\frac{x}{1-\lambda\zeta^a}}\frac{1}{1-\lambda\zeta^a}\\ &= \frac{\mathfrak{g}_\chi}{f}(1+x)\log(1+x)\sum_{a=1}^{f}\sum_{\lambda\neq 1}\overline{\chi}(a)\frac{1}{x+(1-\lambda\zeta^a)}.\end{aligned}$$

Then

$$\begin{aligned}
DA(e^t-1) &= \frac{\mathfrak{g}_\chi}{f} te^t \sum_{a=1}^{f} \sum_{\lambda \neq 1} \overline{\chi}(a) \frac{1}{e^t - \lambda \zeta^a)} \\
&= te^t \left(N\chi(N)(e^t)^{N-1} H(e^{tN}) - H(e^t) \right) && \text{by Lemma 3.16} \\
&= \chi(N) Nte^{tN} H(e^{tN}) - te^t H(e^t) \\
&= \chi(N) F(Nt) - F(t) && \text{as } F(t) = te^t H(e^t) \text{ by definition} \\
&= \chi(N) \sum_{n=0}^{\infty} B_{n,\chi} \frac{(Nt)^n}{n!} - \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!} && \text{by equation (1)} \\
&= \sum_{n=0}^{\infty} \frac{t^n}{n!} (\chi(N) N^n - 1) B_{n,\chi}.
\end{aligned}$$

Letting $\delta_n(DA) = (\chi(N)N^n - 1)B_{n,\chi}$ and applying Proposition 3.13, we get that

$$\Gamma_{DA}(s) = \lim_{i \to \infty} \delta_{n_i}(DA)$$

where $n_i \to \infty$ as integers, $(p-1)|n_i$, and $n_i \to s$ p-adically. By definition of $L_p(1-n, \chi)$ (Theorem 3.5), we have that

$$L_p(1-n, \chi) = (1 - \chi\omega^{-n}(p)p^{n-1}) L(1-n, \chi\omega^{-n}).$$

Since $(p-1)|n_i$, $\omega^{-n_i}(p) = 1$, and we have that

$$L_p(1-n_i, \chi) = (1 - \chi(p)p^{n_i - 1}) L(1-n_i, \chi) = -(1 - \chi(p)p^{n_i-1}) \frac{B_{n_i,\chi}}{n_i}.$$

Taking the limit as $i \to \infty$, this shows that

$$\lim_{i \to \infty} B_{n_i,\chi} = L_p(1-s, \chi) \cdot s.$$

Since $(p-1)|n_i$, $N^{n_i} = \langle N \rangle^{n_i}$, and hence

$$\lim_{i \to \infty} N^{n_i} = \lim_{i \to \infty} \langle N \rangle^{n_i} = \langle N \rangle^s.$$

Finally, this shows that

$$\Gamma_{DA}(s) = \lim_{i \to \infty} \delta_{n_i}(DA) = (\chi(N)\langle N \rangle^s - 1) L_p(1-s, \chi).$$

Applying Proposition 3.14, we see that

$$\Gamma_A(s) = (1 - \chi(N), \langle N \rangle^s) L_p(1-s, \chi),$$

completing the proof. □

This allows to prove Leopoldt's formula 3.17 by applying Proposition 3.15.

Proof of Theorem 3.17. By Proposition 3.15, we have that

$$\Gamma_A(0) = A(0) - \frac{1}{p} \sum_{\xi^p = 1} A(\xi - 1).$$

For A from Theorem 3.18, we have that

$$\begin{aligned} A(0) &= 0, \\ A(\xi - 1) &= \frac{\mathfrak{g}_\chi}{f} \sum_{a=1}^{f} \sum_{\lambda \neq 1} \overline{\chi}(a) \log_p \left(\frac{\xi - \lambda \zeta^a}{1 - \lambda \zeta^a} \right). \end{aligned}$$

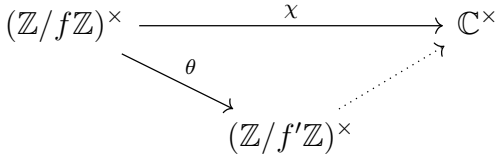
Therefore:

$$\begin{aligned} \Gamma_A(0) &= -\frac{\mathfrak{g}_\chi}{pf} \sum_{a=1}^{f} \overline{\chi}(a) \log_p \left(\prod_{\substack{\lambda \neq 1 \\ \xi^p = 1}} \frac{\xi - \lambda \zeta^a}{1 - \lambda \zeta^a} \right) \\ &= -\frac{\mathfrak{g}_\chi}{pf} \sum_{a=1}^{f} \overline{\chi}(a) \log_p \left(\prod_{\lambda \neq 1} \frac{1 - \lambda^p \zeta^{ap}}{(1 - \lambda \zeta^a)^p} \right) \\ &= -\frac{\mathfrak{g}_\chi}{pf} \sum_{a=1}^{f} \overline{\chi}(a) \log_p \left(\prod_{\lambda \neq 1} \frac{1 - \lambda \zeta^{ap}}{(1 - \lambda \zeta^a)^p} \right). \end{aligned}$$

We now split the sum as follows:

$$\sum_{a=1}^{f} \overline{\chi}(a) \log_p \left(\prod_{\lambda \neq 1} \frac{1 - \lambda \zeta^{ap}}{1 - \lambda \zeta^a} \right) = \underbrace{\sum_{a=1}^{f} \overline{\chi}(a) \log_p \left(\prod_{\lambda \neq 1} (1 - \lambda \zeta^{ap}) \right)}_{S_2} - p \cdot \underbrace{\sum_{a=1}^{f} \overline{\chi}(a) \log_p \left(\prod_{\lambda \neq 1} (1 - \lambda \zeta^a) \right)}_{S_1}.$$

We claim that $S_2 = \chi(p) S_1$. This is clear when $(p, f) = 1$ because ζ^a and ζ^p are both primitive roots of unity. When $p | f$, we may write $f = pf'$. Since χ has conductor f, it does not factor as follows:



and hence $\ker\chi \not\supseteq \ker\theta$, i.e. there is a b coprime to f such that $\chi(b) \neq 1$ but $b \equiv 1\ (f')$. In that case, $ab \equiv a\ (f')$, so $abp \equiv ap\ (f)$. Therefore:

$$\begin{aligned} S_2 &= \sum_{a=1}^{f} \overline{\chi}(a) \log_p \left(\prod_{\lambda \neq 1} (1 - \lambda \zeta^{ap}) \right) \\ &= \sum_{a=1}^{f} \overline{\chi}(ab) \log_p \left(\prod_{\lambda \neq 1} (1 - \lambda \zeta^{abp}) \right) \\ &= \overline{\chi}(b) \sum_{a=1}^{f} \overline{\chi}(a) \log_p \left(\prod_{\lambda \neq 1} (1 - \lambda \zeta^{ap}) \right) \\ &= \overline{\chi}(b) S_2. \end{aligned}$$

Since $\overline{\chi} \neq 0$, this shows that $S_2 = 0$.

In any case, we have shown that $S_2 = \chi(p) S_1$. Hence:

$$\begin{aligned} S_2 - pS_1 &= (\chi(p) - p) S_1 \\ &= (\chi(p) - p) \sum_{a=1}^{f} \overline{a} \log_p \frac{1 - \zeta^{aN}}{1 - \zeta^a} \\ &= (\chi(p) - p) \left(\sum_{a=1}^{f} \overline{\chi} \log_p (1 - \zeta^{aN}) - \sum_{a=1}^{f} \overline{\chi} \log_p (1 - \zeta^a) \right) \\ &= (\chi(p) - p)(\chi(N) - 1) \sum_{a=1}^{f} \overline{\chi}(a) \log_p (1 - \zeta^a). \end{aligned}$$

Altogether, we have shown that:

$$(1 - \chi(N)) L_p(1, \chi) = \Gamma_A(0) = -\frac{\mathfrak{g}_\chi}{fp} (\chi(p) - p)(\chi(N) - 1) \sum_{a=1}^{f} \overline{\chi}(a) \log_p (1 - \zeta^a).$$

We are free to choose N. As long as we choose N so that $\chi(N) \neq 1$, this shows that

$$L_p(1, \chi) = -\frac{\mathfrak{g}_\chi}{f} \left(1 - \frac{\chi(p)}{p} \right) \sum_{a=1}^{f} \overline{\chi}(a) \log_p (1 - \zeta^a),$$

i.e. Leopoldt's formula 3.17. □

3.5. **p-adic class number formula.** For the standard L-function, we proved that $L(1, \chi) \neq 0$ for $\chi \neq \mathbb{1}$ (Corollary 2.9) using the class number formula. We develop the analog of these notions in this section.

Recall that $L_p(1 - n, \chi) = (*) \cdot L(1 - n, \chi\omega^{-n})$. Suppose χ is odd. When n is even $\chi\omega^{-n}$ is even and $1 - n$ is even, so $L(1 - n, \chi\omega^{-n}) = 0$. Similarly, when n is even, $\omega\omega^{-n}$ is odd and $1 - n$ is odd, so $L(1 - n, \chi\omega^{-n}) = 0$. Therefore $L_p(s, \chi) \equiv 0$ for χ odd.

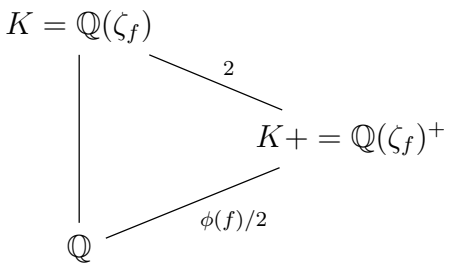
This is consistent with Leopoldt's formula 3.17: for χ odd

$$L_p(1,\chi) = \frac{1}{2}\left(\sum_{a=1}^{f} \overline{\chi}(a)\log_p(1-\zeta^a) - \sum_{a=1}^{f} \overline{\chi}(a)\log_p(1-\zeta^{-a})\right) = 0.$$

Therefore, we only consider even characters. In this case, the analog of Dirichlet's Theorem 2.9 holds.

Theorem 3.19. *If χ is even, then $L_p(1,\chi) \neq 0$.*

Recall that in the proof of Dirichlet's Theorem 2.9, we considered the zeta function of $K = \mathbb{Q}(\zeta_f)$. Because we only take even characters here, we need to consdier the totally real subfield $K^+ = \mathbb{Q}(\zeta_f)^+$ of K:



We previously showed that

$$\zeta_{K^+}(s) = \prod_{\substack{\chi \text{ character} \\ \text{of } G^+}} L(s,\chi)$$

and used the class number formula:

$$\frac{2^n h_{K^+} R_{K^+}}{2\sqrt{|d_{K^+}|}} = \prod_{\chi \neq 1} L(1,\chi).$$

How is the regulator defined? For K, by Dirichlet's unit theorem,

$$U_K/\text{torsion} \cong \mathbb{Z}^{r_1+r_2-1}$$

where r_1 is the number of real places and r_2 is the number of complex places. Then if

$$\sigma_1, \ldots, \sigma_{r_1}, \sigma_{r_1+1}, \overline{\sigma_{r_1+1}}, \ldots, \sigma_{r_1+r_2}, \overline{\sigma_{r_1+r_2}}$$

are all the embeddings of K into $\mathbb{C}$, then (dropping one of the embeddings)

$$R_K = \det(\log(\sigma_i(u_j))_{r\times r})$$

where $(u_1, \ldots, u_r)$ is a basis for $U_K/\text{torsion}$.

To get a p-adic analog for the class number formula, we want to define the p-adic regulator. Having fixed embeddings $\overline{\mathbb{Q}}$ into $\mathbb{C}$ and $\mathbb{C}_p$, embeddings $K \hookrightarrow \mathbb{C}$ are in bijection with embeddings $K \hookrightarrow \mathbb{C}_p$, but it is difficult to distinguish between the real and complex embeddings in $\mathbb{C}_p$. However, if K is a totally real field, there is no problem. If $\sigma_1, \ldots, \sigma_{r+1}$ are all the embeddings, then we define

$$R_{K,p} = \det(\log_p(\sigma_i(u_j))_{r\times r})$$

(dropping one of the embeddings.)

We know that for any K, $R_K \neq 0$. The analogous statement for the p-adic regulator is only conjectural.

Conjecture. For any totally real field K, $R_{K,p} \neq 0$.

It is known for K abelian.

Theorem 3.20. *If $K/\mathbb{Q}$ is an abelian totally realy field, then $R_{K,p} \neq 0$.*

We omit the proof of this here. This could be one of the final projects for this class. We instead focus on proving the following theorem.

Theorem 3.21 (p-adic class number formula)**.** *We have that*

$$\frac{2^n h_{K^+} R_{K^+,p}}{2\sqrt{|d_K|}} = \prod_{\chi \neq 1} \left(L_p(1,\chi) \left(1 - \frac{\chi(p)}{p}\right)^{-1} \right).$$

Combining these two theorem, we in particular get Theorem 3.19.

We only prove this theorem in the case $K = \mathbb{Q}(\zeta_{p^m})$. The general case is more complicated and we refer to [Was97] for that.

We need a way of producing units in $K^+ = \mathbb{Q}(\zeta_{p^m})^+$ in order to compute $R_{K^+,p}$. They will be indexed by the integers in the set

$$\{1 < a < p^m/2 \mid (a,p) = 1\}.$$

Note that there are $\frac{\phi(p^m)}{2} - 1 = n - 1$ of them. For each such a, we consider

$$\zeta_a = \zeta^{-(a-1)/2} \frac{\zeta^a - 1}{\zeta - 1},$$

where $\zeta = \zeta_{p^m}$.

Remark 3.22. If n is odd, $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{2n})$, so $\zeta^{\frac{1}{2}} \in K$. Thus $\zeta_a \in K$.

The map $\zeta \mapsto \zeta^{-1}$, generating $\mathrm{Gal}(K/K+)$, sends ζ_a to

$$\zeta^{(a-1)/2} \frac{\zeta^{-a} - 1}{\zeta^{-1} - 1} = \zeta^{-(a-1)/2} \frac{1 - \zeta^a}{1 - \zeta} = \zeta_a.$$

Hence $\zeta_a \in K^+$.

We finally check that ζ_a is a unit. It is clearly an integer, so we just need to check it has an inverse. Since $(a,p) = 1$, there exits a b such that $ab \equiv 1 \ (p^m)$. Then

$$\zeta_a = (\text{root of unity}) \cdot \frac{\zeta^a - 1}{\zeta^{ab} - 1},$$

which clearly shows it is a unit.

Define $C_{K^+} = \langle \zeta_a, -1 \rangle \subseteq U_{K^+}$. Then $C_{K^+}/(\text{torsion}) \subseteq U_{K^+}/(\text{torsion})$.

Theorem 3.23. *We have that C_{K^+} is finite index in U_{K^+} and $|U_{K^+}/C_{K^+}| = h_{K^+}$.*

Note that if $G = \mathrm{Gal}(K/\mathbb{Q})$, $G^+ = \mathrm{Gal}(K^+/\mathbb{Q})$, we have that

$$\begin{array}{ccc} G & \xrightarrow{\cong} & \{\sigma_b \mid 1 \le b < p^m,\ (b,p)=1\} \\ \downarrow & & \downarrow \\ G^+ & \xrightarrow{\cong} & \{\sigma_b \mid 1 \le b < p^m/2,\ (b,p)=1\}. \end{array}$$

We want to compute

$$\det\left(\log|\sigma_b(\zeta_a)|\right)_{1<a,b<p^m/2}.$$

We have that:

$$\begin{aligned} \log|\sigma_b(\zeta_a)| &= \log\left|\sigma_b\left(\frac{\zeta^{(a-1)/2}(\zeta^a-1)}{\zeta-1}\right)\right| \\ &= \log\left|\frac{\sigma_b(\zeta^a-1)}{\sigma_b(\zeta-1)}\right| \\ &= \log\left|\frac{\sigma_b(\sigma_a(\zeta-1))}{\sigma_b(\zeta-1)}\right| \\ &= \log|\sigma_b\sigma_a(\zeta-1)| - \log|\sigma_b(\zeta-1)|. \end{aligned}$$

Lemma 3.24. *Let G be a finite abelian group. Let $f\colon G \to k$ be any function, where k is an algebraically closed field of characteristic 0. Then*

(1) $\det[f(\sigma\tau^{-1})]_{\sigma,\tau\in G} = \displaystyle\prod_{\chi\colon G\to k^\times}\left(\sum_{\sigma\in G}\chi(\sigma)f(\sigma)\right)$,

(2) $\det[f(\sigma\tau^{-1})-f(\sigma)]_{\sigma,\tau\in G\setminus\{1\}} = \displaystyle\prod_{\substack{\chi\colon G\to k^\times \\ \chi\neq\mathbb{1}}}\left(\sum_{\sigma\in G}\chi(\sigma)f(\sigma)\right)$.

Proof. For (1), let $V = \{F\colon G \text{ tok}\}$. Then G acts on V by $(g\cdot F)(\sigma) = F(g\sigma)$. Consider

$$T = \sum_{\sigma\in G} f(\sigma)\sigma.$$

We compute the determinant of T. Let e_τ be the characteristic function of τ. Then

$$\begin{aligned} T(e_\tau)(\alpha) &= \left(\sum_\sigma f(\sigma)\sigma\right)(e_\tau)(\alpha) \\ &= \sum_\sigma f(\sigma)e_\tau(\sigma\alpha) \\ &= \sum_\sigma f(\sigma)e_{\tau\sigma^{-1}}(\alpha) \\ &= \sum_{\tau'} f(\tau(\tau')^{-1})e_{\tau'}(\alpha), \end{aligned}$$

and thus the matrix of T in this basis is $(f(\sigma\tau^{-1}))$.

Another basis for T is given by all the characters and

$$T(\chi)(\tau) = \sum_{\sigma} f(\sigma)\chi(\sigma\tau) = \left(\sum_{\sigma} f(\sigma)\chi(\sigma)\right)\chi(\tau).$$

This completes the proof of (1).

Finally, for (2), consider the subspace of V given by

$$V^0 = \left\{ F\colon G \to k \;\middle|\; \sum_{\sigma} f(\sigma) = 0 \right\}.$$

Then (2) follows in the same as above. □

This implies that

$$\det\left(\log|\sigma_b(\zeta_a)|\right)_{1<a,b<p^m/2} = \prod_{\substack{\chi\colon G\to k^\times \\ \chi\neq\mathbb{1}}} \sum_{\sigma\in G^+} \chi(\sigma)\log|\sigma(1-\zeta)|.$$

To complete the proof of the theorem, we recall that $\zeta = \zeta_{p^m}$, and we have that

$$\begin{aligned}
\sum_{\sigma\in G^+} \chi(\sigma)\log|\sigma(1-\zeta)| &= \sum_{1\le a<p^m/2} \chi(a)\log|1-\zeta_{p^m}^a| \\
&= \frac{1}{2}\sum_{1\le a<p^m} \chi(a)\log|1-\zeta_{p^m}^a| \\
&= \frac{1}{2}\sum_{\substack{b=1\\(b,p)=1}}^{p^k} \chi(b) \sum_{\substack{1\le a<p^m\\ a\equiv b \ (p^k)}} \log|1-\zeta_{p^m}^a| \qquad \text{where } \mathrm{cond}(\chi) = p^k | p^m \\
&= \frac{1}{2}\sum_{\substack{b=1\\(p,b)=1}}^{p^k} \chi(b)\log\left|\prod_{\substack{1\le a<p^m\\ a\equiv b \ (p^k)}} (1-\zeta_{p^m}^a)\right|.
\end{aligned}$$

Lemma 3.25. *We have that*

$$\prod_{\substack{1\le a<p^m\\ a\equiv b \ (p^k)}} (1-\zeta_{p^m}^a) = 1-\zeta_{p^k}^b.$$

Proof. Note that

$$1-x^{p^{m-k}} = \prod_{1\le j\le p^{m-k}} (1-\zeta_{p^{m-k}}^j X).$$

Setting $X = \zeta_{p^m}^b$, we get that

$$1-\zeta_{p^k}^b = \prod_{1\le j\le p^{m-k}} (1-\zeta_{p^{m-k}}^j \zeta_{p^m}^b) = \prod_{1\le j\le p^{m-k}} (1-\zeta_{p^m}^{jp^k+b}),$$

proving the lemma. □

This gives

$$\det\left(\log|\sigma_b(\zeta_a)|\right)_{1<a,b<p^m/2} = \prod_{\chi\neq\mathbb{1}}\left(\frac{1}{2}\sum_{\substack{b=1\\(b,p)=1}}^{f_\chi}\chi(b)\log|1-\zeta_{f_\chi}^b|\right).$$

Recall that

$$L(1,\chi) = \frac{-\mathfrak{g}_\chi}{f_\chi}\sum_{b=1}^{f_\chi}\overline{\chi}(b)\log|1-\zeta_{f_\chi}^b|.$$

Hence the determinant is equal to

$$\pm\frac{1}{2^{n-1}}\prod_{\chi}\frac{f_{\overline{\chi}}}{\mathfrak{g}_{\overline{\chi}}}L(1,\overline{\chi}) = \pm\frac{1}{2^{n-1}}\prod_{\chi}\overline{\mathfrak{g}_\chi}L(1,\chi).$$

Finally, the class number formula says that

$$\frac{2^n h_{K^+}R_{K^+}}{2\sqrt{|d_{K^+}|}} = \prod_{\chi\neq 1}L(1,\chi) = 2^{n-1}\frac{1}{\prod_\chi\overline{\mathfrak{g}_\chi}}\mathrm{Reg}(\zeta_a).$$

This implies that

$$h_{K^+}R_{K^+} = \mathrm{Reg}(\zeta_a)$$

and proves Theorem 3.23.

Let $N=\ell^m$ for some prime ℓ. We have $\mathbb{Q}\subseteq K^+\subseteq K=\mathbb{Q}(\zeta_N)$. By Theorem 3.23, we have that

$$R_{K^+,p} = \mathrm{Reg}_p(\zeta_a)/h_{K^+}.$$

Then the same proof as above shows that

$$R_{K^+,p} = \prod_{\chi\neq 1}\frac{1}{2}\sum_{a=1}^{N}\chi(a)\log_p(1-\zeta^a).$$

Leopoldt's formula 3.17 then shows that

$$L_p(1,\chi) = -\frac{g_\chi}{f_\chi}\left(\sum_{a=1}^{N}\overline{\chi}(a)\log_p(1-\zeta^a)\right)\cdot\left(1-\frac{\chi(p)}{p}\right).$$

Tracing through the same argument as above completes the proof of Theorem 3.21.

4. p-adic measures and power series

So far, we constructed p-adic L-functions as p-adic analytic functions. In this section, we provide a different construction using measures on a Galois group and power series. In the previous method, all the L-functions $L_p(1,\chi)$ for different χ were seemingly unrelated, but now we will see how we can work with all the characters simultaneously.

The Galois extensions in question are the following

$$\begin{array}{c} \mathbb{Q}(\zeta_{Np^\infty}) \\ \Big| {\scriptstyle (1+p\mathbb{Z}_p,\cdot)\cong(\mathbb{Z}_p,+)} \\ \mathbb{Q}(\zeta_{Np}) \\ \Big| {\scriptstyle \Delta} \\ \mathbb{Q} \end{array}$$

Hence the group we want to construct measures on is actually $\mathbb{Z}_p$.

Definition 4.1. Consider a finite extension K of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}$. An *$\mathcal{O}$-valued measure* on $\mathbb{Z}_p$ is a collection of maps

$$\mu_n \colon \mathbb{Z}/p^n\mathbb{Z} \to \mathcal{O}$$

such that

$$\mu_n(x) = \sum_{\substack{y \mapsto x \\ y \in \mathbb{Z}/p^{n+1}\mathbb{Z}}} \mu_{n+1}(y).$$

Theorem 4.2. *There is a canonical bijection*

$$\{\mathcal{O}\text{-valued measures on } \mathbb{Z}_p\} \leftrightarrow \mathcal{O}[\![x]\!].$$

Proof. Consider a measure given by $\mu_n \in \mathcal{O}[\mathbb{Z}/p^n\mathbb{Z}]$ and consider $\mu_{n+1} \in \mathcal{O}[\mathbb{Z}/p^{n+1}\mathbb{Z}]$ such that $\mu_n \mapsto \mu_{n+1}$. Then we have that

$$\mu \in \varprojlim \mathcal{O}[\mathbb{Z}/p^n\mathbb{Z}] \cong \varprojlim \frac{\mathcal{O}[T]}{T^{p^n}-1} \cong \varprojlim \frac{\mathcal{O}[x]}{(1+x)^{p^n}-1}.$$

The assertion now follows from Theorem 4.3. □

Theorem 4.3. *There is a canonical isomorphism*

$$\mathcal{O}[\![x]\!] = \varprojlim \frac{\mathcal{O}[x]}{(1+x)^{p^n}-1}.$$

In order to prove this theorem, we need some preparation about the power series ring.

4.1. **Power series.** We start with a division algorithm in $\mathcal{O}[\![x]\!]$.

Theorem 4.4 (Division algorithm)**.** *Consider $f(x) \in \mathcal{O}[\![x]\!]$ given by*

$$f(x) = a_0 + a_1 x + \cdots$$

with where the uniformizer π divides $a_0, \ldots, a_{d-1}$, but π does not divide a_d. Consider any $g(x) \in \mathcal{O}[\![x]\!]$. Then there exist unique $q(x) \in \mathcal{O}[\![x]\!]$ and $r(x) \in \mathcal{O}[x]$ such that $\deg r < d$ and

$$g(x) = q(x)f(X) + r(x).$$

Before we prove this, we will derive a corollary of this theorem.

Definition 4.5. A *distinguished polynomial* $p(x) \in \mathcal{O}[x]$ is a polynomial whose leading coefficient is a unit and all other coefficients are divisible by π.

Example 4.6. The polynomial $(1+x)^{p^n} - 1$ above is a distinguished polynomial.

Corollary 4.7 (Weierstrass Preparation Theorem)**.** *Given any $0 \neq f(x) \in \mathcal{O}[\![x]\!]$, we can factor it as*

$$f(x) = \pi^n \cdot h(x) \cdot u(x)$$

where $h(x)$ is a distinguished polynomial and $u(x)$ is a unit power series (i.e. the constant term is a unit). Moreover, this is "unique" (up to obvious ambiguity by $\mathcal{O}^\times$).

Proof. Write $f(x) = \pi^n g(x)$ for $g(x) \in \mathcal{O}[\![x]\!]$ and at least one coefficient is a unit. Writing $g(x) = a_0 + a_1 x + \cdots$, we may assume that $\pi | a_0, \ldots, a_{d-1}$ and π does not divide a_d. By the division algorithm 4.4, we have that

$$x^d = q(x)g(x) + r(x)$$

for $r(x) < d$. Write $q(x) = b_0 + b_1 x + \cdots$ to see that

$$1 = b_0 a_d + b_1 a_{d-1} + \cdots$$

by looking at the coefficients of x^d. This implies that b_0 is a unit, so $q(x)$ is invertible. Looking at the coefficient of x^i for $i < d$, we see that the coefficients of $r(x)$ are divisible by π. Finally:

$$\begin{aligned} x^d - r(x) &= q(x)g(x) \\ g(x) &= \frac{1}{q(x)}(x^d - r(x)). \end{aligned}$$

Taking $u(x) = \frac{1}{q(x)}$ and $h(x) = x^d - r(x)$, we get the desired factorization. Uniqueness is easy to check. □

Corollary 4.8. *Any non-zero power series $f(x) \in \mathcal{O}[\![x]\!]$ has only finitely many zeros in the maximal ideal of $\mathcal{O}_{\mathbb{C}_p}$.*

Proof. Writing $f(x) = \pi^n h(x) u(x)$ as in the Weierstrass Preparation Theorem 4.7, we have that

$$f(\alpha) = \pi^n h(\alpha) u(\alpha),$$

so the roots of f are the roots of h and there are clearly finitely many of them. □

Lemma 4.9. *Suppose $h(x), g(x) \in \mathcal{O}[x]$ with $h(x)$ distinguished. If $h(x)$ divides $g(x)$ in $\mathcal{O}[\![x]\!]$, then $h(x)$ divides $g(x)$ in $\mathcal{O}[x]$.*

Proof. We have that $g(x) = h(x)f(x)$ in $\mathcal{O}[\![x]\!]$. Consider a finite extension $\widetilde{K}$ of K containing all the roots of $h(x)$. If $\widetilde{\mathcal{O}} \subseteq K$ is the ring of integers, then the roots of $h(x)$ lie in its maximal ideal because $h(x)$ is distinguished. Let α be such a root. Substituting α in $g(x) = h(x)f(x)$, we get that $g(\alpha) = 0$. Dividing both sides by $x - \alpha$, we get an equation

$$g_1(x) = h_1(x)f(x) \quad \text{in } \widetilde{\mathcal{O}}[\![x]\!].$$

Since $h_1(x)$ is still distinguished, we may continue this way to see that $f(x)$ is a polynomial in $\widetilde{K}[x]$, and hence also in $K[x]$. By Gauss' Lemma, $h(x) | g(x)$ in $\mathcal{O}[x]$. □

Proof of the division algorithm 4.4. This proof is due to Manin. Define two linear maps $\alpha, \tau \colon \mathcal{O}[\![x]\!] \to \mathcal{O}[\![x]\!]$:

$$\alpha(b_0 + b_1 x + \cdots) = b_0 + b_1 x + \cdots + b_{d-1} x^{d-1}$$
$$\tau(b_0 + b_1 x + \cdots) = b_d + b_{d+1} x + b_{d+2} x^2 + \cdots$$

Note that:

- $\alpha(F) = F$ if and only if F is a polynomial of degree less than d if and only if $\tau(F) = 0$,
- $\tau(x^d F) = F$.

The idea of the proof is to "*solve for* q". We want the equality:

$$g = qf + r.$$

This is equivalent to $\tau(g) = \tau(gf)$. We may write

$$f = \alpha(f) + x^d \tau(f)$$

and multiplying by q, we get that

$$qf = q\alpha(f) + x^d q\tau(f).$$

Now,

$$\tau(g) = \tau(qf) = \tau(q\alpha(f)) + q\tau(f).$$

Letting $z = q\tau(f)$, we get

$$\tau(g) = z + \tau\left(z \frac{\alpha(f)}{\tau(f)}\right).$$

Let H be multiplication by $\frac{\alpha(f)}{\tau(f)}$. Note that $\alpha(f)$ is divisible by π and $z(f)$ is a unit power series. Then we may write

$$\tau(g) = (I + \tau \circ H)(z).$$

The inverse of the operator $I + z \circ H$ is

$$(I + z \circ H)^{-1} = I - (z \circ H) + (z \circ H)^2 + \cdots.$$

Then

$$z = (I + z \circ H)^{-1} \tau(g).$$

Finally, we get

$$q = \frac{1}{z(f)} (I + \tau \circ H)^{-1} \tau(g)$$

and this also gives the r. Uniqueness follows immediately from this proof. □

We can finally go back to prove Theorem 4.3.

Proof of Theorem 4.3. Let $h_n(x) = (1+x)^{p^n} - 1$, so $h_{n+1}(x) = (1+x)^{p^{n+1}} - 1$. Then

$$\frac{h_{n+1}(x)}{h_n(x)} = \frac{(1+x)^{p^{n+1}} - 1}{(1+x)^{p^n} - 1} = \frac{t^p - 1}{t - 1} = 1 + t + t^2 + \cdots + t^{p-1},$$

where $t = (1+x)^{p^n} \in 1 + (p, x)$. Therefore:

$$\frac{h_{n+1}(x)}{h_n(x)} \in (p, x) \subseteq (\pi, x) \subseteq \mathcal{O}[x].$$

Starting with $f(x) \in \mathcal{O}[\![x]\!]$, we divide $f(x)$ by $h_n(x)$ to get

$$f(x) = q_n(x)h_n(x) + \gamma_n(x).$$

We then define

$$\begin{aligned} \mathcal{O}[\![x]\!] &\xrightarrow{\phi} \frac{\mathcal{O}[x]}{(1+x)^{p^n} - 1} \\ f(x) &\mapsto (\gamma_n(x)) \end{aligned}$$

To check that $(\gamma_n(x))$ is a compatible system, we note that

$$q_n(x)h(x) + \gamma_n(x) = f(x) = q_{n+1}h_{n+1} + \gamma_{n+1}(x)$$

so $h_n(x)$ divides $\gamma_{n+1} - \gamma_n(x)$ in $\mathcal{O}[\![x]\!]$, and hence $h_n(x)$ divides $\gamma_{n+1}(x) - \gamma_n(x)$ in $\mathcal{O}[x]$ as well by Lemma 4.9. Hence we have a well-defined homomorphism ϕ.

To show injectivity, suppose $\phi(x) = 0$. Then $f(x)$ is divisible by $h_n(x)$ for all n in $\mathcal{O}[x]$. But $h_n(x) \in (\pi, X)^n$, so $f(x) \in (\pi, x)^n \mathcal{O}[\![x]\!]$ for all n. By Krull's Theorem,

$$\bigcap_n (\pi, x)^n = 0,$$

so $f = 0$. Alternatively, one can note that $h_n(x) | f(x)$ for all n would imply that $f(x)$ has infinitely many zeros, contradicting Corollary 4.8.

To show surjectivity, let

$$(f_n(x)) \in \varprojlim \frac{\mathcal{O}[x]}{(h_n(x))}.$$

For $m \geq n$, $f_m - f_n \equiv 0 \ (h_n)$, so $f_m - f_n \in (\pi, x)^n = \mathfrak{m}^n$, so $\lim f_m$ exists and we can write $f = \lim f_m$. We use here that $R = \mathcal{O}[\![x]\!] \cong \varprojlim R/\mathfrak{m}^n$, because R is complete with respect to the $\mathfrak{m}$-adic topology.

We check that $\phi(f) = (f_n)$. Write

$$f_m - f_n = q_{m,n} \cdot h_n.$$

Then

$$q_{m,n} = \frac{f_m - f_n}{h_n} \to \frac{f - f_n}{h_n}.$$

Keeping n fixed and letting $m \to \infty$, we define $q_n = \lim_{m \to \infty} q_{m,n} \in \mathcal{O}[\![x]\!]$. Then $f = f_n + q_n h_n$,showing that $f \mapsto f_n$ under ϕ. □

This finally completes the proof of Theorem 4.2, establishing the bijection between measures and power series.

Example 4.10. Let $s \in \mathbb{Z}_p$ The *Dirac measure* supported on S is given by

$$\mu_n \colon \mathbb{Z}/p^n\mathbb{Z} \to \mathcal{O}$$

and

$$\mu_n(x) = \begin{cases} 1 & \text{if } x \equiv s \ (p^n), \\ 0 & \text{if } x \not\equiv s \ (p^n). \end{cases}$$

We will show that the power series associated to this measure is

$$(1+x)^s = \sum_{i=0}^{\infty} \binom{s}{i} x^i.$$

Pick $s_n \in \mathbb{Z}$ such that $s_n \equiv s\ (p^n\mathbb{Z})$. We have the isomorphisms

$$\begin{array}{rccc} \mathcal{O}[\mathbb{Z}/p^n\mathbb{Z}] & \xrightarrow{\cong} & \dfrac{\mathcal{O}[T]}{T^{p^n}-1} & \xrightarrow{\cong} \dfrac{\mathcal{O}[x]}{(1+x)^{p^n}-1}, \\ \text{characteristic function of } [s_n] & \mapsto & [T^{s_n}] & \mapsto [(1+x)^{s_n}]. \end{array}$$

This suggests that the power series is

$$(1+x)^s = \sum_{k=0}^{\infty} \binom{s}{k} x^k.$$

Indeed, the function

$$(1+x)^{s_n} = \sum_{k=0}^{s_n} \binom{s_n}{k} x^k = \sum_{k=0}^{\infty} \binom{s_n}{k} x^k$$

tends to $(1+x)^s$ as $s_n \mapsto s$. This shows the assertion by the proof of Theorem 4.3.

4.2. **Integration.** We now discuss integration of functions with respect to p-adic measures.

Let $C(\mathbb{Z}_p, \mathbb{C}_p) = \{f\colon \mathbb{Z}_p \to \mathbb{C} \mid \text{continuous}\}$ (a Banach space for the sup-norm) and let μ be an $\mathcal{O}$-valued p-adic measure on $\mathbb{Z}_p$. We want to define

$$\int f d\mu.$$

As in real analysis, we approximate f by *step functions*, i.e. functions that factor through $\mathbb{Z}/p^n\mathbb{Z}$ for large n. In other words, let $(f_n)_n$ be a sequence of functions $f_n\colon \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{C}_p$ be such that $f_n \to f$. Then define

$$\int f d\mu = \lim_n \int f_n d\mu_n,$$

where

$$\int f_n d\mu_n = \sum_{x \in \mathbb{Z}/p^n\mathbb{Z}} f_n(x)\mu_n(x).$$

It is easy to check this is well-defined. Also,

$$\left| \int f d\mu \right| \leq \|f\| \|\mu\|,$$

where $\|f\| = \sup_{x\in\mathbb{Z}_p} |f(x)|$ and $\|\mu\| = \sup\limits_{\substack{n\in\mathbb{N} \\ x\in\mathbb{Z}/p^n\mathbb{Z}}} |\mu_n(x)|$.

Then the map

$$\begin{aligned} C(\mathbb{Z}_p, \mathbb{C}_p) &\to \mathbb{C}_p \\ f &\mapsto \int f d\mu \end{aligned}$$

is a bounded linear functional on $C(\mathbb{Z}_p, \mathbb{C}_p)$.

Consider now continuous functions from $\mathbb{Z}_p$ to $\mathcal{O}$, $C(\mathbb{Z}_p, \mathcal{O})$. We have a functional

$$\begin{aligned} C(\mathbb{Z}_p, \mathcal{O}) &\xrightarrow{\lambda} \mathcal{O} \\ f &\mapsto \int f d\mu. \end{aligned}$$

Conversely, any linear functional of this sort comes from an $\mathcal{O}$-valued measure on $\mathbb{Z}_p$. Given λ, we can recover μ by setting $\mu_n(x) = \lambda(\mathbb{I}_{x+p^n\mathbb{Z}_p})$, where $\mathbb{I}_{x+p^n\mathbb{Z}_p}$ is the characteristic function of $x + p^n\mathbb{Z}_p$.

Remark 4.11. Given μ and a continuous function $\varphi\colon \mathbb{Z}_p \to \mathcal{O}$, we can construct a new measure $\varphi d\mu$ given by

$$\int f(\varphi d\mu) = \int f\varphi d\mu.$$

Theorem 4.12. *In the correspondence between power series and measures in Theorem 4.2, suppose $f(x) = c_0 + c_1 x + c_2 x^2 + \cdots$ corresponds to the measure μ_f. Then:*

$$c_k = \int_{\mathbb{Z}_p} \binom{x}{k} d\mu_f(x).$$

Proof. Considering $\mu_n\colon \mathbb{Z}/p^n\mathbb{Z} \to \mathcal{O}$, we have that

$$\begin{array}{ccccc} \mathcal{O}[\mathbb{Z}/p^n\mathbb{Z}] & \xrightarrow{\cong} & \dfrac{\mathcal{O}[T]}{T^{p^n}-1} & \xrightarrow{\cong} & \dfrac{\mathcal{O}[x]}{(1+x)^{p^n}-1}, \\ \displaystyle\sum_{r\in\mathbb{Z}/p^n\mathbb{Z}} \mu_n(r) r & \mapsto & \displaystyle\sum_{r=0}^{p^n-1} \mu_n(r) T^r & \mapsto & \displaystyle\sum_{r=0}^{p} \mu_n(r)(1+x)^r. \end{array}$$

We then compute that

$$\begin{aligned} \sum_{r=0}^{p} \mu_n(r)(1+x)^r &= \sum_{r=0}^{p^n-1} \sum_{k=0}^{r} \binom{r}{k} x^k \\ &= \sum_{r=0}^{p^n-1} \mu_n(r) \sum_{k=0}^{p^n-1} \binom{r}{k} x^k \\ &= \sum_{k=0}^{p^n-1} x^k \left(\sum_{r=0}^{p^n-1} \mu_n(r) \binom{r}{k} \right). \end{aligned}$$

Therefore,

$$c_k = \lim_{n\to\infty} \sum_{r=0}^{p^n-1} \mu_n(r) \binom{r}{k} = \int_{\mathbb{Z}_p} \binom{x}{k} d\mu,$$

as required. □

Corollary 4.13. *Suppose $\xi \in \mathfrak{m}$, where $\mathfrak{m}$ is the maximal ideal of $\mathcal{O}$. Then*

$$\int_{\mathbb{Z}_p} (1+\xi)^x d\mu_f(x) = f(\xi).$$

Proof. We have that:

$$\int_{\mathbb{Z}_p} \left(\sum_{k=0}^{\infty} \binom{x}{k} \xi^k \right) d\mu_f = \sum_{k=0}^{\infty} \xi^k \int_{\mathbb{Z}_p} \binom{x}{k} d\mu_f(x) = \sum_{k=0}^{\infty} \xi^k c_k = f(\xi)$$

by Theorem 4.12. □

Examples 4.14.

(1) We have that $\displaystyle\int_{\mathbb{Z}_p} d\mu_f(x) = f(0)$.

(2) Consider the measure $(1+\xi)^x d\mu_f(x)$. Suppose this measure corresponds to g. We will work out what g is by using Corollary 4.13. For $\xi' \in \mathfrak{m}$,

$$\begin{aligned} g(\xi') &= \int_{\mathbb{Z}_p} (1+\xi')^x d\mu_g(x) \\ &= \int_{\mathbb{Z}_p} (1+\xi')^x (1+\xi)^x d\mu_f(x) \\ &= ((1+\xi')(1+\xi))^x d\mu_f(x) \\ &= \int_{\mathbb{Z}_p} (1+\xi+\xi'+\xi\xi')^x d\mu_f(x) \\ &= f(\xi+\xi'+\xi\xi') \\ &= f((1+\xi)(1+\xi')-1). \end{aligned}$$

Therefore, $g(x) = f((1+\xi)(1+x)-1)$.

(3) If $\zeta \in \mathcal{O}$ is a p-power root of unity, then $\xi = \zeta - 1 \in \mathfrak{m}$. Then the above example shows that

$$\zeta^x d\mu_f(x) \longleftrightarrow f(\zeta(1+x)-1).$$

(4) Let φ be a step function on $\mathbb{Z}_p$, i.e. φ factors through $\mathbb{Z}/p^n\mathbb{Z}$ for some n. We assume that $\mathcal{O}$ contains all the p^nth roots of unity. Then

$$\varphi d\mu_f \longleftrightarrow \sum_{\zeta^{p^n}=1} \widehat{\varphi}(\zeta) f(\zeta(1+x)-1),$$

where for $G = \mathbb{Z}/p^n\mathbb{Z}$, the character group is $\overline{G} \cong \mu_{p^n}$, and we define

$$\widehat{\varphi}(\zeta) = \frac{1}{p^n} \sum_{x \in \mathbb{Z}/p^n\mathbb{Z}} \varphi(x)(\zeta^{-1})^x$$

to be the Fourier transform of φ. The Fourier inversion formula is

$$\varphi(x) = \sum_{\zeta \in \mu_{p^n}} \widehat{\varphi}(\zeta)\zeta^x.$$

Note that this holds for $x \in \mathbb{Z}/p^n\mathbb{Z}$, but may also be viewed as a formula for $x \in \mathbb{Z}_p$.

To show the above correspondence for $\varphi d\mu_f$, we now see that

$$\varphi d\mu_f = \sum_{\zeta \in \mu_n} \widehat{\varphi}(\zeta)\zeta^x d\mu_f,$$

and by Example (3) above, we see this corresponds to the power series

$$\sum_{\zeta \in \mu_{p^n}} \widehat{\varphi}(\zeta) f(\zeta(1+x)-1).$$

(5) Consider a power series $f(x)$ with the corresponding measure μ_f. We then have a measure $\mu_f|_{\mathbb{Z}_p^\times}$ by restricting to $\mathbb{Z}_p^\times$. Note that

$$\mu_f|_{\mathbb{Z}_p^\times} = \varphi \mu_f$$

where φ is the characteristic function of $\mathbb{Z}_p^\times$, a step function factoring through $\mathbb{Z}/p\mathbb{Z}$. We need to apply (4). Note that

$$\widehat{\varphi}(\zeta) = \frac{1}{p} \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \varphi(X)(\zeta^{-1})^x.$$

For $\zeta = 1$, we see that $\widehat{\varphi}(1) = \frac{p-1}{p}$. For $\zeta \neq 1$, we have that

$$\widehat{\varphi}(\zeta) = \frac{1}{p} \sum_{0 \neq x \in \mathbb{Z}/p\mathbb{Z}} (\zeta^{-1})^x = -\frac{1}{p}.$$

Therefore, the power series corresponding to $\mu_f|_{\mathbb{Z}_p^\times}$ is

$$\frac{p-1}{p} f(x) - \frac{1}{p} \sum_{\substack{\zeta \neq 1 \\ \zeta^p = 1}} f(\zeta(1+x)-1).$$

This is equal to

$$f(x) - \frac{1}{p} \sum_{\zeta^p = 1} f(\zeta(1+x)-1).$$

This is more or less the power series that came up in the proof of Leopoldt's formula 3.17.

Before we move onto the construction of a measure that gives $L_p(s, \chi)$, we discuss Γ-transforms and Mellin transforms.

Definition 4.15. Let μ be an $\mathcal{O}$-valued measure on $\mathbb{Z}_p$. The Γ-*transform* of μ is defined by

$$\Gamma_\mu(s) = \int_{\mathbb{Z}_p^\times} \langle x \rangle^s d\mu(x).$$

The *Mellin transform* is

$$M_\mu(s) = \Gamma_{x^{-1} d\mu(x)} = \int_{\mathbb{Z}_p^\times} \langle x \rangle^s x^{-1} d\mu(x).$$

Theorem 4.16. *The function $\Gamma_\mu(s)$ is a p-adic analytic function on $\mathbb{Z}_p$ (in fact, on a larger open disc).*

Proof. By breaking up $\mathbb{Z}_p^\times$ into costs, it suffices to prove this for a measure supported on $1+q\mathbb{Z}_p$. Then

$$\begin{aligned}\Gamma_\mu(s) &= \int\limits_{1+q\mathbb{Z}_p} x^s d\mu(x) \\ &= \int\limits_{1+q\mathbb{Z}_p} \sum_{k=0}^{\infty} \binom{s}{k} (x-1)^k d\mu(x) \\ &= \sum_{k=0}^{\infty} \binom{s}{k} \cdot \int\limits_{1+q\mathbb{Z}_p} (x-1)^k d\mu(x).\end{aligned}$$

We have that $|x-1| \leq |q|$ and $\left|\frac{1}{k!}\right| \leq |p|^{\frac{-k}{p-1}}$, and hence

$$\left|\frac{(x-1)^k}{k!}\right| \leq |q|^k |p|^{-\frac{k}{p-1}}.$$

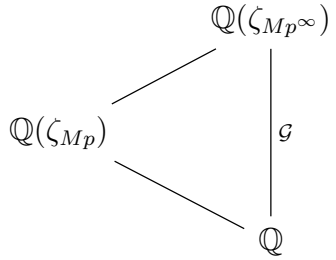
Thus the coefficients of s^n is bounded by

$$|q|^n |p|^{\frac{-n}{p-1}},$$

so the sum converges in the analytic disc $|s| < |q|^{-1}|p|^{1/p-1}$. □

4.3. **Alternative construction of $L_p(s,\chi)$.** We'll give an alternative construction of the p-adic L-function, as a measure.

Let χ be a character of conductor $N = M \cdot p^r$ where $(M,p) = 1$. We consider the following extensions:



where we note that

$$\begin{aligned}\mathcal{G} &\cong \varprojlim_r (\mathbb{Z}/Mp^r\mathbb{Z})^\times \\ &\cong (\mathbb{Z}/M\mathbb{Z})^\times \times \mathbb{Z}_p^\times \\ &\cong (\mathbb{Z}/Mq\mathbb{Z})^\times \times (1+qZ_{\mathfrak{p}}).\end{aligned}$$

We will construct a measure

$$dE_{1,c} \text{ on } \varprojlim \mathbb{Z}/Mp^r\mathbb{Z}$$

where $c \in \mathbb{Z}$, $(c, Mp) = 1$ and the 1 stands for the 1st Bernoulli polynomial.

Theorem 4.17. *Let χ be any finite order character of conductor Mp^r for $r \geq 0$. Then*

$$\int_{\mathcal{G}} \chi\omega^{-1}(x)\langle x\rangle^s dE_{1,c}(x) = -(1-\chi(c)\langle c\rangle^{s+1})L_p(-s,\chi).$$

Note that this gives a construction of all the p-adic L-functions of Dirichlet characters χ simultaneously, through one measure.

Example 4.18 ($M = 1$)**.** The above theorem gives the equality:

$$\int_{\mathbb{Z}_p^\times} \chi\omega^{-1}(x)\langle x\rangle^{s-1} dE_{1,c}(x) = -(1-\chi(c)\langle c\rangle^{s})L_p(1-s,\chi)$$

and the left hand side is simply

$$\int_{\mathbb{Z}_p^\times} \chi(x)\langle x\rangle^s x^{-1} dE_{1,c}(x) = M_{\chi dE_{1,c}}(s),$$

the Mellin transform of $\chi dE_{1,c}$. One should note the analogy of this to classical L-functions which also have integral representations as a Mellin transform.

Recall that we defined Bernoulli polynomials as

$$\frac{te^t}{e^t-1}e^{tx} = \sum_{k=0}^{\infty} B_k(x)\frac{t^k}{k!}.$$

We renormalize this slightly and define

$$\frac{t}{e^t-1}e^{tx} = \sum_{k=0}^{\infty} \widetilde{B_k}(x)\frac{t^k}{k!}$$

so that $B_k(x) = \widetilde{B}_k(x+1)$. In this notation, Proposition 3.6 becomes much nicer. If we define

$$\frac{t}{e^t-1} = \sum_{k=0}^{\infty} \widetilde{B_k}\frac{t^k}{k!}$$

then $\widetilde{B_1} = -\frac{1}{2}$ while previously we had $B_1 = +\frac{1}{2}$.

Proposition 4.19. *We have that*

(1) $\widetilde{B_k}(0) = \widetilde{B_k}$,

(2) $\widetilde{B_k}(x) = \sum_{i=0}^{k} \binom{k}{i} \widetilde{B_i} x^{k-i} = x^k - \frac{k}{2}x^{k-1} + (\text{lower order terms})$,

(3) *distribution relation:* $\widetilde{B_k}(x) = N^{k-1}\sum_{a=0}^{N-1} \widetilde{B}_k\left(\frac{x+a}{N}\right)$.

Proof. Since (1) and (2) are clear, we just prove (3). Note that

$$\frac{1}{k!}\sum_{a=0}^{N-1} \widetilde{B_k}\left(\frac{X+a}{N}\right) = \text{coefficient of } t^k \text{ in } \sum_{a=0}^{N-1} \frac{t}{e^t-1}e^{t\frac{X+a}{n}}.$$

Rearranging the power series, we get

$$\frac{t}{e^t-1}e^{tX/N}\sum_{a=0}^{N-1}e^{ta/N}=\frac{te^{tX/N}}{e^t-1}\frac{(e^{t/N})^N-1}{e^{t/N}-1}=N\frac{(t/N)e^{(t/N)x}}{e^{t/N}-1}=\frac{N\cdot N^{-k}}{k!}\widetilde{B_k}(x).$$

This shows (3). □

Definition 4.20. We define a function

$$E_k^{(N)}\colon \mathbb{Z}/N\mathbb{Z}\to\mathbb{Q}$$

by

$$E_k^{(N)}(x)=\frac{N^{k-1}}{k}\widetilde{B_k}\left(\left\{\frac{x}{N}\right\}\right),$$

where $\{\bullet\}$ denotes the fractional part.

This gives a *distribution* on $\hat{\mathbb{Z}}=\varprojlim\mathbb{Z}/n\mathbb{Z}$, i.e. if $N|M$, then

$$E_k^{(N)}(x)=\sum_{\substack{y\in\mathbb{Z}/M\mathbb{Z}\\ y\mapsto x}}E_k^{(M)}(y).$$

To check this relation, write $M=ND$. We may assume that $0\le x<N$. The left hand side is

$$E_k^{(N)}(x)=\frac{N^{k-1}}{k}\widetilde{B_k}\left(\frac{x}{N}\right)$$

and the right hand side is

$$\begin{aligned}\sum_{i=0}^{D}\frac{(ND)^{k-1}}{k}\widetilde{B_k}\left(\frac{x+iN}{ND}\right)&=\frac{N^{k-1}}{k}D^{k-1}\sum_{i=0}^{D-1}\widetilde{B_k}\left(\frac{x/N+i}{D}\right)\\&=\frac{N^{k-1}}{k}\widetilde{B_k}\left(\frac{x}{N}\right)\qquad\text{by Proposition 4.19 (3).}\end{aligned}$$

Finally, for $N=Mp^r$ and $c\in\mathbb{Z}$ such that $(c,Mp)=1$, define

$$E_{k,c}^{(N)}(x)=E_k^{(N)}(x)-c^kE_k^{(N)}(c^{-1}x).$$

Theorem 4.21. *We have that $E_{k,c}^{(N)}(x)\in\mathbb{Z}_p$.*

Proof of Theorem 4.21 for $k=1$. We first just show this for $k=1$. We have that

$$E_{1,c}^{(N)}(x)=E_1^{(N)}(x)-cE_1^{(N)}(c^{-1}x)=\widetilde{B_1}\left(\frac{x}{N}\right)-c\widetilde{B_1}\left(\left\{\frac{c^{-1}x}{N}\right\}\right).$$

Now, recall that $\widetilde{B_1}(x)=x-\frac{1}{2}$. Let $d\in\mathbb{Z}$ be such that $d=c^{-1}$ in $(\mathbb{Z}/N\mathbb{Z})^\times$, i.e. $cd\equiv 1\ (N)$. If $dx=qN+r$, $x\equiv cdx\equiv cr\ (N)$. Then by the above:

$$\begin{aligned}E_{1,c}^{(N)}(x)&=\widetilde{B_1}\left(\frac{x}{N}\right)-c\widetilde{B_1}\left(\frac{r}{n}\right)\\&=\frac{x}{N}-\frac{1}{2}-c\left(\frac{r}{n}-\frac{1}{2}\right)\\&=\frac{x-cr}{N}+\frac{c-1}{2}\in\mathbb{Z}_p.\end{aligned}$$

This completes the proof for $k = 1$. □

For $k > 1$, we need the following lemma.

Lemma 4.22. *Let $N = Mp^r$. Then*

$$E_{k,c}^{(N)}(x) \equiv x^{k-1} E_{1,c}^{(N)}(x) \mod \frac{N}{kD(k)}\mathbb{Z}_p,$$

where $D(k)$ is the least common multiple of the denominators of $\widetilde{B_k}(x)$.

Proof. Let $0 \le x < N$. First, if $dx = qN + r$ and $cr = x + Nt$, then it is easy to check that

$$E_{1,c}^{(N)}(x) = \frac{c-1}{2} - t.$$

Then

$$\begin{aligned}
E_{k,c}^{(N)}(x) &= \frac{N^{k-1}}{k}\left[\widetilde{B_k}\left(\frac{x}{N}\right) - c^k \widetilde{B_k}\left(\frac{r}{N}\right)\right] \\
&\equiv \frac{N^{k-1}}{k}\left[\left[\left(\frac{x}{N}\right)^k - \frac{k}{2}\left(\frac{x}{N}\right)^{k-1}\right] - c^k\left[\left(\frac{r}{N}\right)^k - \frac{k}{2}\left(\frac{r}{N}\right)^{k-1}\right]\right] \mod \frac{N}{kD(k)}\mathbb{Z}_p \\
&= \frac{1}{k}\left[\frac{x^k}{N} - \frac{k}{2}x^{k-1} - \frac{(x+Nt)^k}{N} + \frac{k}{2}c(x+Nt)^{k-1}\right] \\
&\equiv \frac{1}{k}\left[\frac{x^k}{N} - \frac{k}{2}x^{k-1} - \frac{x^k}{N} - \frac{kx^{k-1}Nt}{N} + \frac{kc}{2}x^{k-1}\right] \mod \frac{N}{kD(k)}\mathbb{Z}_p \\
&= x^{k-1}\left[-\frac{1}{2} - t + \frac{c}{2}\right] \\
&= x^{k-1} E_{1,c}^{(N)}(x).
\end{aligned}$$

This completes the proof. □

Proof of Theorem 4.21, general case. If $r \gg 0$, then the congruence in Lemma 4.22 shows that $E_{k,c}^{(N)}(x) \in \mathbb{Z}_p$. From the distribution relation, we get integrality for all N. □

We can finally prove Theorem 4.17. We only prove it in the case $M = 1$, where $\mathcal{G} = \mathbb{Z}_p^\times$. The general case will be given as an exercise.

We want to show that

$$\int_{\mathbb{Z}_p^\times} \chi\omega^{-1}(x)\langle x\rangle^{s-1} dE_{1,c}(x) = -(1 - \chi(c)\langle c\rangle^s) L_p(1-s, \chi).$$

We first note that Lemma 4.22 gives the following corollary.

Corollary 4.23. *We have that $dE_{k,c} = x^{k-1} dE_{1,c}$.*

Proof of Theorem 4.17 for $M = 1$. In this case $N = p^r$ is the conductor of χ. We have that

$$\begin{aligned}
\int_{\mathbb{Z}_p^\times} \chi\omega^{-1}(x)\langle x\rangle^{k-1} dE_{1,c}(x) &= \int_{\mathbb{Z}_p^\times} \underbrace{\chi\omega^{-k}}_{\chi'}(x)\cdot x^{k-1} dE_{1,c}(x) \\
&= \int_{\mathbb{Z}_p} \chi'(x)x^{k-1} dE_{1,c}(x) - \int_{p\mathbb{Z}_p} \chi'(x)x^{k-1} dE_{1,c}(x) \\
&= \int_{\mathbb{Z}_p} \chi'(x)x^{k-1} dE_{1,c}(x) - \int_{\mathbb{Z}_p} \chi'(py)y^{k-1}p^{k-1} dE_{1,c}(py) && \text{for } x = py \\
&= (1-\chi'(p)p^{k-1}) \int_{\mathbb{Z}_p} \chi'(x)x^{k-1} dE_{1,c}(x) \\
&= (1-\chi'(p)p^{k-1}) \int_{\mathbb{Z}_p} \chi'(x) dE_{k,c}(x) && \text{by Corollary 4.23.}
\end{aligned}$$

We now compute the last integral:

$$\begin{aligned}
\int_{\mathbb{Z}_p} \chi'(x) dE_{k,c}(x) &= \frac{N^{k-1}}{k}\left(\sum_{a=0}^{N-1} \widetilde{B_k}\left(\frac{a}{N}\right)\chi'(a) - c^k \sum_{a=0}^{N-1} \widetilde{B_k}\left(\frac{c^{-1}a}{N}\right)\chi'(a)\right) \\
&= \frac{N^{k-1}}{k}\left(\sum_{a=0}^{N-1} \widetilde{B_k}\left(\frac{a}{N}\right)\chi'(a)\right)(1-\chi'(c)c^k) \\
&= \frac{B_{k,\chi\omega^{-n}}}{k}(1-\chi\omega^{-k}(c)c^k) && \text{by Proposition 3.6.}
\end{aligned}$$

Then

$$\begin{aligned}
\int_{\mathbb{Z}_p^\times} \chi\omega^{-1}(x)\langle x\rangle^{k-1} dE_{1,c}(x) &= (1-\chi(p)p^{k-1})\frac{B_{k,\chi\omega^{-n}}}{k}(1-\chi(c)\omega(c)^{-k}c^k) \\
&= -L_p(1-k,\chi)(1-\chi(c)\langle c\rangle^k),
\end{aligned}$$

as claimed. □

As mentioned above, the proof of the general case of Theorem 4.17 is left as an exercise.

Remark 4.24. The same construction of $dE_{1,c}$ works if we take $c \in \mathbb{Z}_p^\times$ instead of $c \in \mathbb{Z}$ such that $(c,p) = 1$.

Recall that we showed

$$\int_{Z_p^\times} \chi(x)\langle x\rangle^s x^{-1} dE_{1,c}(x) = -(1-\chi(c)\langle c\rangle^s)L_p(1-s,\chi).$$

Recall that

$$\mathbb{Z}_p^\times \cong \underbrace{(\mathbb{Z}/q\mathbb{Z})^\times}_{\Delta} \times (1+q\mathbb{Z}_p).$$

An $\mathcal{O}$-*valued measure* on $\mathbb{Z}_p^\times$ is an element of

$$\mathcal{O}[\![\mathbb{Z}_p^\times]\!] \cong \mathcal{O}[\Delta][\![1+p\mathbb{Z}_p]\!].$$

Let θ be a character of Δ. Then θ gives a map $\mathcal{O}[\Delta] \to \mathcal{O}$ and for each θ we get a map

$$\mathcal{O}[\![1+q\mathbb{Z}_p]\!] \to \mathcal{O}[\![1+q\mathbb{Z}_p]\!] \cong \mathcal{O}[\![\mathbb{Z}_p]\!] \cong \mathcal{O}[\![x]\!],$$

where the isomorphism $\mathbb{Z}_p \cong 1+q\mathbb{Z}_p$ is given by sending 1 to a fixed topological generator γ of $1+q\mathbb{Z}_p$.

If $\mu = x^{-1}dE_{1,c}(x)$, let $d\mu^\theta$ be the associated measure on $1+q\mathbb{Z}_p$, $d\tilde{\mu}^\theta$ be the associate measure on $\mathbb{Z}_p$, and finally $\tilde{g}^\theta \in \mathbb{Z}_p[\![x]\!]$ be the corresponding power series.

Write $\chi = \theta \cdot \psi$, where

- θ is a character of the *first kind*, i.e. it factors through Δ,
- ψ is a character of the *second kind*, i.e. it factors through $1+q\mathbb{Z}_p$.

Therefore, we may rewrite the above integral as follows:

$$\begin{aligned}\int_{\mathbb{Z}_p^\times} \chi(x)\langle x\rangle^s x^{-1}dE_{1,c}(x) &= \int_{1+q\mathbb{Z}_p} \psi(x)x^s d\mu^\theta \\ &= \int_{\mathbb{Z}_p} \psi(\gamma^t)(\gamma^t)^s d\tilde{\mu}^\theta(t) \\ &= \int_{\mathbb{Z}_p} (\psi(\gamma)\gamma^s)^t d\tilde{\mu}^\theta(t) \\ &= \widetilde{g}^\theta(\psi(\gamma)\gamma^s - 1).\end{aligned}$$

We recall this integral was equal to $-(1-\chi(c)\langle c\rangle^s)L_p(1-s,\chi)$, so we get the equation:

$$\tilde{g}^\theta(\psi(\gamma)\gamma^s - 1) = -(1-\psi(\gamma)\gamma^s)L_p(1-s,\theta\psi) = (\psi(\gamma)\gamma^s - 1)L_p(1-s,\theta\psi).$$

Finally, define

$$g^\theta(x) = \frac{\tilde{g}^\theta(x)}{x}.$$

Then

$$g^\theta(\psi(\gamma)\gamma^s - 1) = L_p(1-s,\theta\psi).$$

If $\theta \neq \mathbb{1}$, then $g^\theta(x) \in \mathbb{Z}_p[\![x]\!]$. Taking $s=0$ and $\psi = \mathbb{1}$, the above equation gives:

$$\widetilde{g}^\theta(0) = 0$$

since $L_p(s,\theta)$ is analytic at $s=1$.

For the rest of this section, we assume that p is odd for simplicity.

If $\theta = \mathbb{1}$, then $\widetilde{g}^\theta(x)$ is a unit power series in $\mathbb{Z}_p[\![x]\!]$. Taking $\psi = \mathbb{1}$ and $s=1$, we see that

$$\widetilde{g}^{\mathbb{1}}(\gamma - 1) = -(1-\gamma)L_p(0,\mathbb{1}).$$

By the interpolation formula

$$L_p(1-n,\chi) = (1-\chi\omega^{-n}(p))L(1-n,\chi\omega^{-n}),$$

we see that

$$L_p(0,\mathbb{1}) = L(0,\omega^{-1}) = -\frac{B_{0,\omega^{-1}}}{1} = -\frac{1}{p}\sum_{a=1}^{p-1}\omega^{-1}(a)a \equiv -\frac{p-1}{p} \equiv \frac{1}{p} \mod \mathbb{Z}_p.$$

This shows that

$$\tilde{g}^{\mathbb{1}}(\gamma - 1) = -(1-\gamma)L_p(0,\mathbb{1}) \in \mathbb{Z}_p^\times,$$

so $\tilde{g}^{\mathbb{1}}$ is a unit power series.

Now, define

$$f^\theta(\chi) = g^\theta\left(\frac{\gamma}{1+x} - 1\right).$$

Then

$$f^\theta(\psi^{-1}(\gamma)\gamma^s - 1) = g^\theta\left(\frac{\gamma}{\psi^{-1}(\gamma)\gamma^s} - 1\right) = g^\theta(\psi(\gamma)\gamma^{1-s} - 1) = L_p(s,\theta\psi).$$

Note that

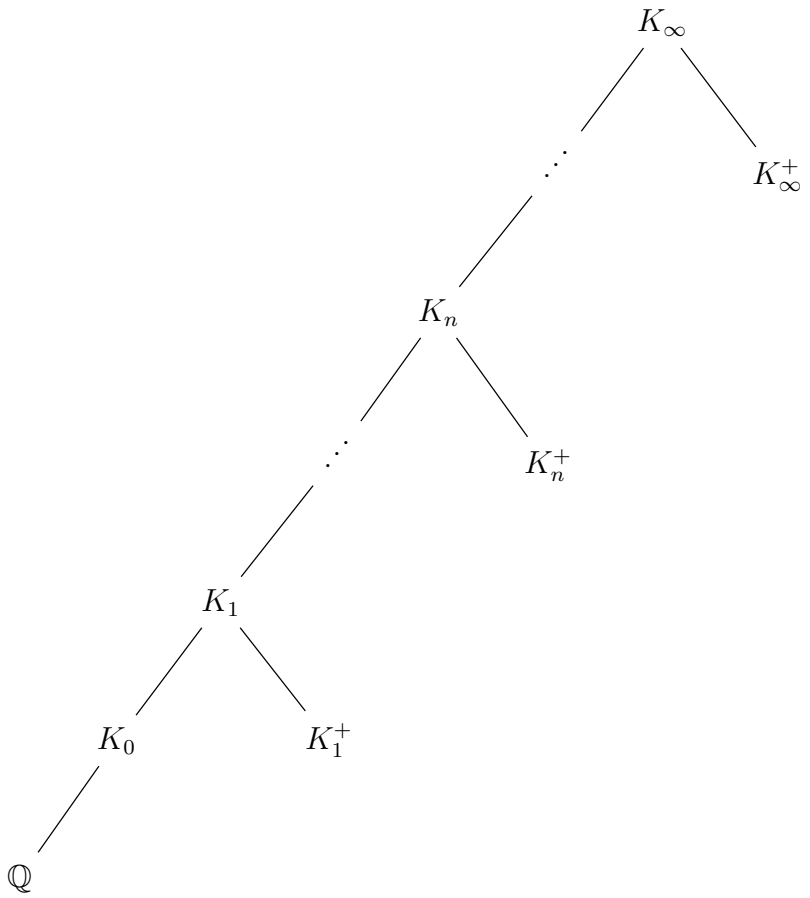
$$f^\theta(x) \in \mathbb{Z}_p[\![x]\!] \quad \text{if } \theta \neq \mathbb{1}$$

but for $\theta = \mathbb{1}$, we have only have that

$$f^{\mathbb{1}}(x) \in \frac{1}{\frac{\gamma}{1+x} - 1}\mathbb{Z}_p[\![x]\!].$$

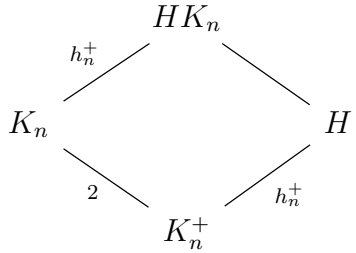
4.4. **Applications to class numbers in cyclotomic towers.** We keep the simplifying assumption that $p \neq 2$.

Let $K_n = \mathbb{Q}(\zeta_{p^{n+1}})$ and $K_\infty = \mathbb{Q}(\zeta_{p^\infty})$. Write K^+ for the totally real subfield of K. Then we have the following tower of extensions:



Iwasawa's idea was to try to understand how the class number behaves in this tower.

Let h_n be the class number of K_n and h_n^+ be the class number of K_n^+. We first note that h_n^+ divides h_n. Indeed, if H is the maximal unramified abelian extension of K_n^+ (at all places, including infinite ones), then we have:



Since HK_n is unramified and abelian over K_n, it is contained in the maximal unramified abelian extension of K_n. This shows that $h_n^+ | h_n$.

Let us write $h_n = h_n^+ h_n^-$. We will try to understand how the p-part of h_n^- grows with n. Let $K^+ = K_n^+$ and $K = K_n$. Then we have that

$$\frac{(2\pi)^d h_k R_K}{w_k \sqrt{|d_K|}} = \prod_{\chi \neq \mathbb{1}} L(1,\chi) \qquad \text{characters } \chi \text{ of } \mathrm{Gal}(K/\mathbb{Q}),$$

$$\frac{2^d h_{K^+} R_{K^+}}{2\sqrt{|d_{K^+}|}} = \prod_{\chi \neq \mathbb{1}} L(1,\chi) \qquad \text{characters } \chi \text{ of } \mathrm{Gal}(K^+/\mathbb{Q}).$$

Dividing on equation by the other, we get that

$$\pi^d h_K^- \frac{R_K}{R_{K^+}} = \frac{w_k}{2} \prod_{\chi \text{ odd}} L(1,\chi) \frac{\sqrt{|d_K|}}{\sqrt{|d_{K^+}|}}.$$

Therefore:

$$h_K^- \frac{R_K}{R_{K^+}} = \frac{w_K}{2} i^d \prod_{\chi} \frac{\mathfrak{g}_\chi}{f_\chi} B_{1,\chi} \frac{\sqrt{|d_K|}}{\sqrt{|d_{K^+}|}}$$

using

$$L(1,\chi) = \frac{\pi i \mathfrak{g}_\chi}{f_\chi} B_{1,\overline{\chi}}.$$

One can also show that

$$\prod_{\chi} \frac{\mathfrak{g}_\chi}{f_\chi} \frac{\sqrt{|d_K|}}{\sqrt{|d_{K^+}|}} = i^d$$

and

$$\frac{R_K}{R_{K^+}} = 2^{d-1}.$$

Altogether, we see that:

$$h_K^- = w_k \prod_{\chi \text{ odd}} \left(-\frac{1}{2} B_{1,\chi} \right).$$

Recall that we had $K = K_n$, so we may write for any n:

$$h_n^- = w_n \prod_{\substack{\chi \text{ odd} \\ \mathrm{Gal}(K_n/\mathbb{Q})}} \left(-\frac{1}{2} B_{1,\chi} \right)$$

$$h_0^- = w_0 \prod_{\substack{\chi \text{ odd} \\ \mathrm{Gal}(K_0/\mathbb{Q})}} \left(-\frac{1}{2} B_{1,\chi} \right)$$

Note that $w_n = w_0 p^n$, so this shows that

$$h_n^- = h_0^- \cdot p^n \cdot \prod_{\chi} \left(-\frac{1}{2} B_{1,\chi} \right),$$

where the product is now over all odd characters χ of $\mathrm{Gal}(K_n/\mathbb{Q})$ that do not factor through $\mathrm{Gal}(K_0/\mathbb{Q})$.

We may write $\chi\omega = \theta\psi$ for θ even and note that

$$L_p(0, \chi\omega) = (1 - \chi(p))L(0, \chi) = L(0, \chi) = -B_{1,\chi}.$$

Finally, we see that:

$$h_n^- \sim h_0^- \cdot p^n \cdot \prod_{\substack{\theta \text{ even}, \\ \psi \neq \mathbb{1}}} L_p(0, \chi\omega),$$

where $\sim$ means *up to p-adic units* (as elements of $\mathbb{Z}_p$). Recall that we're assuming $p \neq 2$, so 2 is a p-adic unit.

We will now use the power series that gives the p-adic L-function. Recall that $\chi\omega = \theta\psi$. Then

$$\begin{aligned} h_0^- \cdot p^n \cdot \prod_{\substack{\theta \text{ even}, \\ \psi \neq \mathbb{1}}} L_p(0, \chi\omega) &= h_0^- \cdot p^n \cdot \prod_{\substack{\theta \text{ even}, \\ \psi \neq \mathbb{1}}} f^\theta(\psi^{-1}(\gamma) - 1) \\ &= p^n \cdot h_0^- \cdot \prod_{\theta \text{ even}} \prod_{\substack{\zeta^{p^n} \\ \zeta \neq 1}} f^\theta(\zeta - 1) \\ &= p^n \cdot h_0^- \cdot \left(\prod_{\substack{\zeta^{p^n} \\ \zeta \neq 1}} f^{\mathbb{1}}(\zeta - 1) \right) \cdot \prod_{\substack{\zeta^{p^n} \\ \zeta \neq 1}} A(\zeta - 1) \end{aligned}$$

where we define

$$A(x) = \prod_{\theta \neq \mathbb{1}} f^\theta(x).$$

Recall that

$$f^{\mathbb{1}}(x) = \frac{\tilde{g}^{\mathbb{1}}\left(\frac{\gamma}{1+x} - 1\right)}{\frac{\gamma}{1+x} - 1}.$$

Setting $\zeta - 1$, we see that

$$f^{\mathbb{1}}(\zeta - 1) = \frac{\tilde{g}^{\mathbb{1}}\left(\gamma\zeta^{-1} - 1\right)}{\gamma\zeta^{-1} - 1},$$

so

$$|f^{\mathbb{1}}(\zeta - 1)| = \frac{1}{|\gamma\zeta^{-1} - 1|} = \frac{1}{|\zeta^{-1} - 1|}.$$

Finally,

$$\prod_{\substack{\zeta^{p^n} \\ \zeta \neq 1}} |f^{\mathbb{1}}(\zeta - 1)| = \frac{1}{|p^n|}.$$

Therefore:

$$|h_n^-| = |h_0^-| \left| \prod_{\substack{\zeta^{p^n} \\ \zeta \neq 1}} A(\zeta - 1) \right|.$$

By Weierstrass preparation theorem 4.7, we may write

$$A(x) = p^\mu P(x) U(x),$$

where $P(x)$ is a distinguished polynomial and $U(x)$ is a unit power series. Then:

$$|h_n^-| = |h_0^-||p^\mu|^{p^n-1}\prod_{\substack{\zeta^{p^n}\\ \zeta\neq 1}}|P(\zeta-1)|.$$

Recall that

$$P(X) = X^\lambda + a_{\lambda-1}X^{\lambda-1} + \cdots.$$

with $a_{\lambda-1},\ldots$ is divisible by p. For $n \gg 0$, we hence have that

$$|P(\zeta-1)| = |(\zeta-1)^\lambda|.$$

Finally, this shows that

$$|h_n^-| = |h_0^-||p^\mu|^{p^n-1}|p^n|^\lambda$$

for $n \gg 0$. In particular, for $n \gg 0$,

$$v_p(h_n^-) = v_p(h_0^-) + \mu(p^n-1) + n\lambda = \mu p^n + \lambda n + C.$$

Therefore, the existence of the power series shows something very non-trivial about how h_n^- behave in the tower of extensions.

Remark 4.25. Iwasawa proved that $\mu = 0$ in this case. In particular, $v_p(h_n^-)$ grows linearly with n. The proof can be found in [Was97] and could be a potential project in this class.

4.5. **Main conjecture of Iwasawa theory.** We recall that we had an infinite tower of extensions

$$\mathbb{Q} \subseteq K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq \cdots K_\infty.$$

Let C_i be the p-part of the class group of K_i.

Let $C = \varprojlim_i C_i$, which is a $\mathbb{Z}_p[\![\mathcal{G}]\!]$-module, where $\mathcal{G} = \Delta \times (1+p\mathbb{Z}_p)$. Let ϵ be a character of Δ and write

$$e_\epsilon = \frac{1}{|\Delta|}\sum_{a\in\Delta}\epsilon^{-1}(a)a.$$

Let $\Lambda = \mathbb{Z}_p[\![x]\!] \cong \mathbb{Z}_p[\![\Gamma]\!]$. Then $C^\epsilon = e_\epsilon C$ is a Λ-module. Here, $\Gamma = 1+p\mathbb{Z}_p \cong \mathbb{Z}_p$.

Theorem 4.26. *We have that C^ϵ is a finitely-generated Λ-module.*

We say that M and N are *pseudoisomorphic*— and write $M \sim N$ if there is a morphism $\varphi M \to N$ of Λ-modules with finite kernel and cokernel.

Theorem 4.27. *Any finitely-generated Λ-module is pseudoisomorphic to*

$$\bigoplus_{i=1}^n \Lambda/(f_i).$$

In that case, let $\mathrm{char}(M)$ be the ideal generated by the product $\prod_{i=1}^n f_i$. We call this the *characteristic ideal of M*.

Theorem 4.28 (Iwasawa's Main Conjecture)**.** *Suppose ϵ is odd and $\epsilon \neq \omega$. Then*

$$\mathrm{char}(C^\epsilon) = (f^{\epsilon^{-1}\omega}(x)).$$

Remark 4.29. We give a brief overview of the history of this conjecture. First, Herbrand showed that if p divides a particular Bernoulli number, then a particular part of the class group does not vanish. In 1976, Ribet [Rib76a] succeeded in proving the converse by a striking use of modular forms to construct unramified p-extensions of $\mathbb{Q}(\zeta_p)$.

This inspired the work of Mazur and Wiles [MW84] who proved Iwasawa's Main Conjecture (for all real abelian extensions of $\mathbb{Q}$ and p odd).

Later, a more elementary proof was found by Rubin using Kolyvagin's Euler systems. This is the proof that can be found in [Was97] and Lang [Lan90, Appendix by Rubin].

5. Serre's construction of the p-adic L-function

The goal of this section is to discuss an alternative construction of the p-adic L-function due to Serre [Ser73b] which uses congruences between modular forms and develops the first approach to p-adic modular forms.

5.1. Classical modular forms.

We start with a review of some of the necessary notions from the theory of modular forms. Some standard references for this topic are [Shi94] and [Miy06] and we refer to these two for a complete treatment of the topic. In particular, the proofs of the unproven results of this section can be found there.

Let $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. A *modular form* of weight k for Γ is a holomorphic function $f\colon \mathfrak{h} \to \mathbb{C}$ such that

(1) $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$ where $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$,

(2) holomorphic at cusps, i.e. since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma$, $f(z+1) = f(z)$, so we may write $f(z) = \sum_{n\in\mathbb{Z}} a_n e^{2\pi i n z}$, and we require that requires $a_n = 0$ for $n < 0$.

We write $q = e^{2\pi i z}$ so that the Fourier expansion is

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

We let $M_k(\Gamma)$ be the set of forms of weight k for Γ, $S_k(\Gamma) \subseteq M_k(\Gamma)$ be the subset of cusp forms (i.e. forms with $a_0 = 0$).

We know $M_k(\Gamma)$ and $S_k(\Gamma)$ are finite-dimensional. In fact, they can be expressed as global sections of a line bundle, so we may compute their dimensions using the Riemann–Roch Theorem.

Proposition 5.1.

(1) *If k is odd, then $M_k(\Gamma) = 0$.*

(2) *For $k \geq 2$ even,*

$$\dim S_k(\Gamma) = \begin{cases} 0 & \text{if } k = 2, \\ \lfloor \frac{k}{2} \rfloor & \text{if } k \equiv 2 \ (12), \\ \lfloor \frac{k}{12} \rfloor & \text{if } k \not\equiv 2 \ (12), \end{cases}$$

and

$$\dim M_k(\Gamma) = \begin{cases} \lfloor \frac{k}{12} \rfloor & \text{if } k \equiv 2 \ (12), \\ \lfloor \frac{k}{12} \rfloor + 1 & \text{if } k \not\equiv 2 \ (12). \end{cases}$$

How does one construct examples of modular forms? We may define the *Eisenstein series* as

$$\widetilde{E}_k(z) = \sum_{(m,n) \in \mathbb{Z}^2 \setminus \{(0,0)\}} \frac{1}{(mz+n)^k}.$$

We write $\widetilde{E}_k$, because we want to reserve E_k for a different normalization.

Proposition 5.2. *For $k \geq 4$ even, this series converges absolutely and uniformly on compact subsets, so it defines a holomorphic function on $\mathfrak{h}$. Moreover, $\widetilde{E}_k \in M_k(\Gamma)$ and its Fourier expansion is*

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

Proof. For convergence, see [Shi94] or [Miy06]. For the last assertion, let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then

$$\begin{aligned} \widetilde{E_k}(\gamma z) &= \sum_{(m,n)} \frac{1}{\left(m\frac{az+b}{cz+d} + n\right)^k} \\ &= (cz+d)^k \sum_{(m,n)} \frac{1}{((ma+nc)z + (mb+nd))^k} \\ &= (cz+d)^k \widetilde{E_k}(z) \qquad \qquad \begin{pmatrix} m \\ n \end{pmatrix} \mapsto \begin{pmatrix} a & c \\ b & d \end{pmatrix}^{-1} \begin{pmatrix} m \\ n \end{pmatrix} \end{aligned}$$

To show that it is holomorphic at the cusps, we compute the Fourier expansion at ∞. Recall that

$$\pi \cot(\pi z) = \frac{1}{z} + \sum_{n=1}^{\infty} \left(\frac{1}{z+n} + \frac{1}{z-n} \right).$$

Also

$$\begin{aligned}\pi\cot(\pi z) &= (i\pi)\frac{e^{\pi iz}+e^{-\pi iz}}{e^{\pi iz}-e^{-\pi iz}}\\ &= i\pi\frac{e^{2\pi iz}+1}{e^{2\pi iz}-1}\\ &= i\pi\left(1+\frac{2}{e^{2\pi iz}-1}\right)\\ &= i\pi\left(1-2\sum_{n=0}^{\infty}e^{2\pi inz}\right).\end{aligned}$$

Differentiating this $k-1$ times, we get that:

$$-2\pi i(2\pi i)^{k-1}\sum_{n=0}^{\infty}n^{k-1}e^{2\pi inz} = (-1)^{k-1}(k-1)!\left(\frac{1}{z^k}+\sum_{n=1}^{\infty}\left(\frac{1}{(z+n)^k}+\frac{1}{(z-n)^k}\right)\right).$$

Finally,

$$\begin{aligned}\widetilde{E_k}(z) &= \sum_{(m,n)}\frac{1}{(mz+n)^k}\\ &= \sum_{n\neq 0}\frac{1}{n^k}+\sum_{m\neq 0}\frac{1}{(mz+n)^k}\\ &= 2\zeta(k)+2\sum_{m=0}^{\infty}\frac{(-1)^k(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty}n^{k-1}e^{2\pi inmz}\\ &= 2\zeta(k)+2\frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty}\underbrace{\left(\sum_{d|n}d^{k-1}\right)}_{\sigma_{k-1}(n)}e^{2\pi inz}\\ &= 2\zeta(k)\left(1+\frac{-2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n\right).\end{aligned}$$

In particular, this shows that $\widetilde{E_k}\in M_k(\Gamma)$. □

We define

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

This is the normalized Eisenstein series. Note that it has rational Fourier coefficients.

Note that $B_4 = -\frac{1}{30}$ and $B_6 = \frac{1}{42}$. Therefore,

$$E_4 = 1+240\sum_{n=1}^{\infty}\sigma_3(n)q^n,$$

$$E_6 = 1-504\sum_{n=1}^{\infty}\sigma_5(n)q^n.$$

Ramanujan studied these functions, denoting E_4 by Q and E_6 by R.

Theorem 5.3. *There is an isomorphism of graded algebras*

$$\bigoplus_{k\geq 0} M_k(\Gamma) = \mathbb{C}[E_4, E_6],$$

where E_4 has degree 4 and E_6 has degree 6. In particular, for any $f \in M_k(\Gamma)$, we can write $f = F(E_4, E_6)$ where F is isobaric *of weight k.*

The proof of this is standard and can be find in textbooks such as Shimura, Miyake.

Example 5.4. The smallest k where there exists a cusp form is $k = 12$. We let

$$\Delta = 12^{-3}\left[E_4^3 - E_6^2\right].$$

Then

- $\Delta(q) = q\prod_{n=1}^{\infty}(1-q^n)^{24}$,
- Δ has no zeros on $\mathfrak{h}$,
- if $J(z) = \dfrac{E_4^3}{\Delta}$, then $J(\tau) = j(\mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z}))$ is the *j-invariant* of the elliptic curve.

Corollary 5.5. *Let $M_k(\Gamma, \mathbb{Q})$ be the subspace of $M_k(\Gamma)$, consisting of forms with rational Fourier coefficients in $\mathbb{Q}$. Then*

$$M(\Gamma, \mathbb{Q}) = \bigoplus_k M_k(\Gamma, \mathbb{Q}) = \mathbb{Q}[E_4, E_6].$$

5.2. **Reduction modulo p.** Fix a prime p and write

$$M_k = \left\{ f = \sum a_n q^n \in M_k(\Gamma) \mid a_n \in \mathbb{Q},\ v_p(a_n) \geq 0 \text{ for all } n \right\}.$$

(We omit the p from the notation.) We then have a map

$$\begin{aligned} M_k &\to \widetilde{M_k} \subseteq \mathbb{F}_p[\![q]\!] \\ f &\mapsto \widetilde{f} = \sum \overline{a_n} q^n \in \mathbb{F}_p[\![q]\!]. \end{aligned}$$

Similarly, for $M = \bigoplus_{k\geq 0} M_k$, we consider the quotient map

$$M \twoheadrightarrow \widetilde{M}.$$

Assume $p \geq 5$.

Exercise. Show that $M = \mathbb{Z}_{(p)}[E_4, E_6]$. (Hint: use induction on the weight using Δ.)

Consider

$$\begin{aligned} \mathbb{Z}_{(p)}[x, y] &\xrightarrow{\cong} M, \\ x &\mapsto E_4, \\ y &\mapsto E_6. \end{aligned}$$

We want to study the map φ given by

$$\begin{array}{ccc} \mathbb{Z}_{(p)}[x,y] & \xrightarrow{\cong} & M \\ \downarrow & & \twoheadrightarrow \\ \mathbb{F}_p[x,y] & \xrightarrow{\varphi} & \widetilde{M} \end{array}$$

The main goal of this section is to prove the following theorem.

Theorem 5.6. *Write $E_{p-1} = A(Q,R)$, $A \in \mathbb{Z}_{(p)}[x,y]$. Then*

$$\ker(\varphi) = (\widetilde{A}(x,y) - 1).$$

Recall that $Q = E_4$, $R = E_6$.

Before we prove this, we need to discuss some preliminaries. We introduce

$$P = E_2 = 1 - 24\sum_{n=1}^{\infty} \sigma_1(n) q^n$$

by analogy with the definition of E_2. The $-\frac{1}{24}$ comes from a Bernoulli number. This would like to be a modular forms of weight 2, but it cannot be, because there is no weight 2 modular forms.

We know that $\mathrm{SL}_2(\mathbb{Z})$ is generated by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Since E_2 is given by a q-series, it is immediately invariant under the first matrix, but it will fail to be invariant under the second. The precise formula is given in Lemma 5.9.

Define the differential operator

$$\theta = q\frac{d}{dq}$$

on q-expansions. In terms of z, we have that

$$\theta = \frac{1}{2\pi i}\frac{d}{dz}.$$

Theorem 5.7. *Let $f \in M_k(\Gamma)$. Then $\theta f - \frac{k}{12} P f \in M_{k+2}(\Gamma)$.*

Definition 5.8. We define $\partial = 12\theta - kP \colon M_k(\Gamma) \to M_{k+2}(\Gamma)$.

Lemma 5.9. *We have that*

$$E_2\left(-\frac{1}{z}\right) = z^2 E_2(z) + \frac{12z}{2\pi i}.$$

We will prove this lemma later. For now, we show how it implies Theorem 5.7.

Proof of Theorem 5.7. We have that $f\left(-\frac{1}{z}\right) = z^k f(z)$ because $f \in M_k(\Gamma)$. Differentiating this, we get:

$$f'\left(-\frac{1}{z}\right)\frac{1}{z^2} = z^k f'(z) + k z^{k-1} f(z).$$

Let

$$g(z) = \frac{1}{2\pi i}\frac{d}{dz} f - \frac{k}{12} P f.$$

Then

$$\begin{aligned} g\left(-\frac{1}{z}\right) &= \frac{1}{2\pi i} z^2 [z^k f'(z) + k z^{k-1} f(z)] - \frac{k}{12} P\left(-\frac{1}{z}\right) f\left(-\frac{1}{z}\right) \\ &= \frac{1}{2\pi i} [z^{2+k} f'(z) + k z^{1+k} f(z)] - \frac{k}{12} z^k f(z) [z^k P(z) + \frac{12z}{2\pi i}] \\ &= \frac{1}{2\pi i} z^{2+k} f'(z) - \frac{k}{12} z^{2+k} f(z) P(z) \\ &= z^{k+2} g(z). \end{aligned}$$

This shows that $\theta f - \frac{k}{12} P f \in M_{k+2}(\Gamma)$. □

Remark 5.10. The map ∂ is a derivation on $\bigoplus M_k(\Gamma)$, i.e.

$$\partial(\alpha\beta) = \alpha\partial(\beta) + \beta\partial(\alpha).$$

Indeed, for modular forms f and g of weights k and ℓ, we see that

$$\partial(fg) = 12\theta(fg) - (k+\ell) P f g = 12(f\theta(g) + g\theta(f)) - (k+\ell) P f g = f\partial g + g\partial f.$$

Example 5.11. We compute ∂ applied in a few examples. We know that ∂Q is a multiple of R. We figure out what multiple, we just consider the constant term in the q-expansions. We had

$$Q = 1 + 240 \sum \sigma_3(n) q^n, \qquad R = 1 - 504 \sum \sigma_5(n) q^n.$$

Then

$$\begin{aligned} 120Q - 4PQ &= 12[240 \sum n\sigma_3(n) q^n] - 4[1 - 24 \sum \sigma_1(n) q^n][1 + 240 \sum \sigma_3(n) q^n] \\ &= -4R. \end{aligned}$$

Therefore:

$$\partial(Q) = -4R.$$

One could similarly compute that $\partial(R) = -6Q^2$, but we omit this here.

We still have to prove Lemma 5.9. We will do this using Dirichlet series, so we first prove a general result.

Theorem 5.12. *Suppose* $f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}$, $g(z) = \sum_{n=0}^{\infty} b_n e^{2\pi i n z}$ *satisfy* $a_n, b_n = O(n^c)$. *Consider*

$$\phi(s) = \sum_{n=1}^{\infty} a_n n^{-s}, \qquad \Phi(s) = (2\pi)^{-s} \Gamma(s) \phi(s),$$

$$\psi(s) = \sum_{n=1}^{\infty} b_n n^{-s}, \qquad \Psi(s) = (2\pi)^{-s} \Gamma(s) \psi(s).$$

Let $k > 0$ be a positive integer. Then the following are equivalent:

(1) $\Phi(s) + \frac{a_0}{s} + \frac{b_0}{k-s}$ *admits an analytic continuation to all $s \in \mathbb{C}$, which is bounded in vertical strips, and*

$$\Phi(k-s) = \Psi(s),$$

(2) $f\left(\frac{-1}{z}\right) = \left(\frac{z}{i}\right)^k g(z)$.

Proof. We have that

$$\begin{aligned}\Phi(s) &= (2\pi)^{-s}\Gamma(s)\sum_{n=1}^{\infty} a_n n^{-s} \\ &= \sum_{n=1}^{\infty} a_n (2\pi n)^{-s} \int_0^{\infty} t^s e^{-t}\frac{dt}{t} \\ &= \int_0^{\infty}\left(\sum_{n=1}^{\infty} a_n e^{-2\pi n t}\right) t^s \frac{dt}{t} \\ &= \int_0^{\infty} (f(it) - a_0) t^s \frac{dt}{t} \\ &= \int_0^{1} (f(it) - a_0) t^s \frac{dt}{t} + \int_1^{\infty} (f(it) - a_0) t^s \frac{dt}{t}.\end{aligned}$$

The second integral $\displaystyle\int_1^{\infty} (f(it) - a_0) t^s \frac{dt}{t}$ converges uniformly on vertical strips, and hence defines an analytic function bounded in vertical strips. The key will be to deal with the first integral.

Let us prove that (2) implies (1). In the first variable, we make the change of variables $t \mapsto \frac{1}{t}$ to get

$$\begin{aligned}\int_0^{1} (f(it) - a_0) t^s \frac{dt}{t} &= \int_{\infty}^{1} (f(i/t) - a_0) t^{-s} \frac{-1/t^2}{1/t} dt \\ &= \int_1^{\infty} (f(i/t) - a_0) t^{-s} \frac{dt}{t} \\ &= -a_0 \int_1^{\infty} t^{-1-s} dt + \int_1^{\infty} t^k g(it) t^{-s} t^{-s} \frac{dt}{t} \qquad \text{by (2)} \\ &= \frac{-a_0}{s} + \int_1^{\infty} t^{k-s}(g(it) - b_0)\frac{dt}{t} + \int_1^{\infty} t^{k-s} b_0 \frac{dt}{t} \\ &= -\frac{a_0}{s} - \frac{b_0}{k-s} + \int_1^{\infty} t^{k-s}(g(it) - b_0)\frac{dt}{t}.\end{aligned}$$

Therefore,

$$\Phi(s) + \frac{a_0}{s} + \frac{b_0}{k-s} = \int_1^{\infty} t^{k-s}(g(it) - b_0)\frac{dt}{t} + \int_1^{\infty} (f(it) - a_0) t^s \frac{dt}{t},$$

which gives an analytic continuation to the complex plane, bounded in vertical strips (EBV). Replacing g by f in the above argument and noting that $g\left(-\frac{1}{z}\right) = \left(\frac{z}{i}\right)^k f(z)$, we get that

$$\Psi(s) + \frac{b_0}{s} + \frac{a_0}{k-s} = \int_1^\infty t^{k-s}(f(it) - a_0)\frac{dt}{t} + \int_1^\infty (g(it) - b_0)t^s \frac{dt}{t}.$$

Therefore, $\Phi(k-s) = \Psi(s)$.

We now show that (1) implies (2). We have that

$$\Phi(s) = \int_0^\infty (f(it) - a_0)t^s \frac{dt}{t},$$

is the Mellin transform of $f(it) - a_0$. The inverse Mellin transform shows that

$$f(it) - a_0 = \frac{1}{2\pi i} \int_{\mathrm{Re}(s)=\sigma \gg 0} t^{-s}\Phi(s)ds.$$

Considering a large rectangular contour, we obtain

$$\begin{aligned}
f(it) - a_0 &= \frac{1}{2\pi i} \int_{\mathrm{Re}(s)=\sigma \gg 0} t^{-s}\Phi(s)ds \\
&= -a_0 + b_0 t^{-k} + \frac{1}{2\pi i} \int_{\mathrm{Re}(s)=\sigma \ll 0} t^{-s}\Phi(s)ds \\
&= -a_0 + b_0 t^{-k} + \frac{1}{2\pi i} \int_{\mathrm{Re}(s)=\sigma \ll 0} t^{-(k-s)}\Phi(k-s)ds && \text{letting } s \mapsto k-s \\
&= -a_0 + b_0 t^{-k} + \frac{1}{2\pi i} \int_{\mathrm{Re}(s)=\sigma \ll 0} t^{-(k-s)}\Psi(s)ds && \text{using } \Psi(k-s) = \Phi(s) \\
&= -a_0 + b_0 t^{-k} + t^{-k}\left(g\left(\frac{i}{t}\right) - b_0\right) && \text{same argument for } g
\end{aligned}$$

This shows that

$$f(it) = t^{-k} g(i/t),$$

and hence

$$f(z) = \left(\frac{z}{i}\right)^{-k} g\left(-\frac{1}{z}\right).$$

This completes the proof. □

Recall that we defined

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

for $k \geq 2$ even. We renormalize it as follows:

$$G_k = -\frac{B_k}{2k} + \sum_{n=1}^\infty \sigma_{k-1}(n)q^n.$$

If $\phi_k(s)$ is the associated Dirichlet series, then

$$\begin{aligned}\phi_k(s) &= \sum_{n=1}^{\infty} \sigma_{k-1}(n) n^{-s} \\ &= \sum_{n=1}^{\infty} \left(\sum_{d|n} d^{k-1} \right) n^{-s} \\ &= \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} m^{k-1} (mn)^{-s} \\ &= \left(\sum_{n} n^{-s} \right) \left(\sum_{m} m^{k-1-s} \right) \\ &= \zeta(s)\zeta(s+1-k).\end{aligned}$$

Let

$$\Phi_k(s) = (2\pi)^{-s}\Gamma(s)\zeta(s)\zeta(s+1-k).$$

Note that

$$\begin{aligned}(2\pi)^{-s}\Gamma(s)\zeta(s) &= \frac{2^{-s}\pi^{-s/2}\pi^{-s/2}\Gamma(s/2)\Gamma((s+1)/2)}{2^{1-s}\sqrt{\pi}} \\ &= \frac{1}{\sqrt{\pi}}\pi^{-s/2}\Gamma((s+1)/2)\pi^{-(1-s)/2}\Gamma((1-s)/2)\zeta(1-s) \quad \text{functional equation for } \zeta \\ &= \frac{1}{2\pi}\Gamma((s+1)/2)\Gamma((1-s)/2)\zeta(1-s) \\ &= \frac{1}{2}\frac{\zeta(1-s)}{\sin\left(\pi\left(\frac{s+1}{2}\right)\right)} \\ &= \frac{\zeta(1-s)}{2\cos\frac{\pi s}{2}}.\end{aligned}$$

This gives

$$\begin{aligned}\Phi_k(s) &= (2\pi)^{-s}\Gamma(s)\zeta(s)\zeta(s+1-k) \\ &= \frac{\zeta(1-s)\zeta(s+1-k)}{2\cos\frac{\pi s}{2}} \\ &= (-1)^{k/2}\Phi(k-s),\end{aligned}$$

which is the functional equation.

In the notation of Theorem 5.12, we have that

$$a_0 = -\frac{B_k}{2k}, \quad b_0 = (-1)^{k/2+1}\frac{B_k}{2k}.$$

If we can show that

$$(2\pi)^{-s}\Gamma(s)\zeta(s)\zeta(s+1-k) + \frac{a_0}{s} + \frac{b_0}{k-s}$$

is analytic, then we can prove the modularity of $G_k(z)$.

We make a table of potential poles and zeros of each of the factors

	$\Gamma(s)$	$\zeta(s)$	$\zeta(s+1)-k$
negative even integers	pole, order 1	zero	holomorphic
negative odd integers	pole, order 1	holomorphic	zero
0	pole, order 1	holomorphic	holomorphic
1	holmorphic	pole, order 1	$\zeta(2-k)$
k	$\Gamma(k)$	$\zeta(k)$	pole, order 1

We check the residue at $s=0$ to make sure that the pole is cancelled:

$$1\frac{-1}{2}\left(-\frac{B_k}{k}\right)+a_0=0.$$

We do the same at $s=k$:

$$(2\pi)^{-k}\Gamma(k)\zeta(k)-(-1)^{k/2+1}\frac{B_k}{k}=0.$$

When $k\neq 2$, we have that $\zeta(2-k)=0$, so the pole of order 1 of $\zeta(s)$ cancels, and hence this function is holomorphic. Overall, this shows that

$$G_k\left(-\frac{1}{z}\right)=\left(\frac{z}{i}\right)^k(-1)^{k/2}G_k(z)=z^kG_k(z),$$

as we already knew by Proposition 5.2

When $k=2$, $\zeta(2-k)=\zeta(0)$ does not have a zero, so this method does not apply. We consider this case separately. We have to trace through the proof of Theorem 5.12 and see what happens in this case. We have that

$$\Phi_2(s)=-\Phi_2(2-s)$$

where

$$\Phi_2(s)=(2\pi)^{-s}\Gamma(s)\zeta(s)\zeta(s-1).$$

Then

$$\begin{aligned}
G_2(it)-a_0&=\frac{1}{2\pi i}\int\limits_{\mathrm{Re}(s)=\sigma\gg 0}t^{-s}\Phi_2(s)ds\\
&=\sum_{i=0}^{2}\mathrm{Res}_{s=i}+\frac{1}{2\pi i}\int\limits_{\mathrm{Re}(s)=\sigma\ll 0}t^{-s}\Phi_2(s)ds\\
&=\sum_{i=0}^{2}\mathrm{Res}_{s=i}-\frac{1}{2\pi i}\int\limits_{\mathrm{Re}(s)=\sigma\gg 0}t^{-(2-s)}\Phi_2(s)ds \qquad 2\mapsto 2-s\\
&=\sum_{i=0}^{2}\mathrm{Res}_{s=i}-t^{-2}\frac{1}{2\pi i}\int\limits_{\mathrm{Re}(s)=\sigma\gg 0}t^{s}\Phi_2(s)ds\\
&=\sum_{i=0}^{2}\mathrm{Res}_{s=i}-(G_2(i/2)-a_0),
\end{aligned}$$

where the residues are of the function

$$\Phi_2(s)t^{-s}=(2\pi)^{-s}\Gamma(s)\zeta(s)\zeta(s-1)t^{-s}.$$

Finally, we do the residue calculation

$$\begin{aligned}\mathrm{Res}_{s=0} &= \left(-\frac{1}{2}\right)\left(-\frac{1}{12}\right) = \frac{1}{24},\\ \mathrm{Res}_{s=1} &= (2\pi)^{-1}\left(-\frac{1}{2}\right)t^{-1} = -\frac{1}{4\pi t},\\ \mathrm{Res}_{s=2} &= (2\pi)^{-2}\frac{\pi^2}{6}t^{-2} = \frac{1}{24}t^{-2}.\end{aligned}$$

Therefore:

$$G_2(it) + \frac{1}{24} = \frac{1}{24} - \frac{1}{4\pi t} + \frac{1}{24}t^{-2} - t^{-2}\left(G_2(i/t) + \frac{1}{24}\right).$$

This gives

$$G_2\left(-\frac{1}{z}\right) = -\frac{z}{4\pi i} + z^2 G_2(z).$$

Coming back to the other normalization of the Eisenstein series, we get that

$$E_2\left(-\frac{1}{z}\right) = \frac{12z}{2\pi i} + z^2 E_2(z),$$

completing the proof of Lemma 5.9.

We now prove an analog of Theorem 5.7 for $P = E_2$.

Proposition 5.13. *We have that $(12\theta - P)P$ is a modular forms of weight 4. Specifically:*

$$(12\theta - P)P = -Q.$$

Proof. Differentiating the equation from Lemma 5.9, we see that

$$P'\left(-\frac{1}{z}\right)\frac{1}{z^2} = z^2 P'(z) + 2zP(z) + \frac{12}{2\pi i},$$

so

$$P'\left(-\frac{1}{z}\right) = z^4 P'(z) + 2z^3 P(z) + \frac{12}{2\pi i}z^2.$$

Therefore:

$$\begin{aligned}(12\theta - P)P\left(-\frac{1}{z}\right) &= \frac{12}{2\pi i}\left[z^4 P'(z) + 2z^3 P(z) + \frac{12}{2\pi i}z^2\right] - \left[z^2 P(z) + \frac{12}{2\pi i}z\right]^2\\ &= \frac{12}{2\pi i}z^4 P'(z) - z^4 P(z)^2\\ &= z^4(12\theta P - P^2)(z).\end{aligned}$$

This shows that $12\theta - P$ is a modular form of weight 4. To check it is $-Q$, compare q-expansions. □

Recall that $M = \mathbb{Z}_{(p)}[E_4, E_6]$. Consider

$$\begin{aligned}\mathbb{Z}_{(p)}[x, y] &\xrightarrow{\cong} M,\\ x &\mapsto E_4,\\ y &\mapsto E_6.\end{aligned}$$

We want to study the kernel of the map φ given by

$$\begin{array}{ccc} \mathbb{Z}_{(p)}[x,y] & \xrightarrow{\cong} & M \\ \downarrow & & \downarrow \\ \mathbb{F}_p[x,y] & \xrightarrow{\varphi} & \widetilde{M} \end{array}$$

Write $E_{p-1} = A(Q,R)$, $A \in \mathbb{Z}_{(p)}[x,y]$. Then Theorem 5.6 states that

$$\ker(\varphi) = (\widetilde{A}(x,y) - 1).$$

We will finally want to prove this.

Recall that $\partial y = -6x^2$ and $\partial x = -4y$. The derivation ∂ makes sense as a derivation on M but also on $\mathbb{F}_p[x,y]$.

Theorem 5.14 (Kummer congruences)**.** *If $m \equiv n\ (p-1)$ but $m \not\equiv 0\ (p-1)$. Then*

$$\frac{\widetilde{B_m}}{m} \equiv \frac{\widetilde{B_n}}{n} \mod p.$$

Instead of presenting the classical proof, we will use the slightly roundabout way that uses p-adic L-functions. We do this in the interest of time.

Proof. Let c be a primitive root modulo p, i.e. a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$. Then, by a homework problem,

$$(1-c^m)\frac{\widetilde{B_m}}{m} = \int_{\mathbb{Z}_p} x^{m-1} dE_{1,c}$$
$$(1-c^n)\frac{\widetilde{B_n}}{n} = \int_{\mathbb{Z}_p} x^{n-1} dE_{1,c}$$

Since $c^m - 1$ and $c^n - 1$ are p-units and $c^m \equiv c^n\ (p)$, we have that

$$(1-c^m)\left(\frac{\widetilde{B_m}}{m} - \frac{\widetilde{B_n}}{n}\right) - \underbrace{(c^m - c^n)\frac{\widetilde{B_n}}{n}}_{\in p\mathbb{Z}_p} = \underbrace{\int_{\mathbb{Z}_p} (x^{m-1} - x^{n-1}) dE_{1,c}}_{\in p\mathbb{Z}_p}.$$

This completes the proof. □

Theorem 5.15 (Van Staudt)**.** *If $k \equiv 0\ (p-1)$, then*

$$B_k \equiv -\frac{1}{p} \mod \mathbb{Z}_p.$$

Proof. Assume $p \neq 2$. Take $c = 1 + p$. We have that

$$(1-c^k)\frac{\widetilde{B_k}}{k} = \int_{\mathbb{Z}_p} x^{k-1} dE_{1,c}.$$

We claim that $c^k \equiv 1 + pk \ (p^k k\mathbb{Z}_p)$. We prove this by induction on $v_p(k)$. For $v_p(k) = 0$, we have that $(1+p)^k = 1 + pk \ (p^2\mathbb{Z}_p)$, so the assertion follows. Now, assuming the claim for k, we prove it for pk. We have that

$$c^{pk} \equiv (1+pk)^p = 1 + p^2 k + \binom{p}{2}(pk)^2 + \cdots \equiv 1 + p(pk) \mod (p^3 k\mathbb{Z}_p).$$

This proves that $c^k \equiv 1 + pk \ (p^k k\mathbb{Z}_p)$. Then

$$\begin{aligned}
\frac{1}{1-c^k} &= \frac{1}{1-(1+pk+p^k t)} \\
&= \frac{1}{-pk(1+pt)} \\
&= -\frac{1}{pk}(1+ps) && \text{for } s \in \mathbb{Z}_p.
\end{aligned}$$

Therefore,

$$\begin{aligned}
B_k &= -\frac{1}{p}(1+ps)\int_{\mathbb{Z}_p} x^{k-1} dE_{1,c} \\
&\equiv -\frac{1}{p}(1+ps)\sum_{i=0}^{p-1} i^{k-1}\int_{i+p\mathbb{Z}_p} dE_{1,c}(x) && \mod (\mathbb{Z}_p) \\
&= -\frac{1}{p}(1+ps)\sum_{i=0}^{p-1} i^{k-1}\left(\left\{\frac{i}{p}\right\} - c\left\{\frac{c^{-1}i}{p}\right\} + \frac{c-1}{2}\right) \\
&= -\frac{1}{p}(1+ps)\sum_{i=0}^{p-1} i^{k-1}\left(\frac{i}{p} - (1+p)\frac{i}{p} + \frac{p}{2}\right) \\
&= -\frac{1}{p}(1+ps)\sum_{i=0}^{p-1}(-i^k + \frac{p}{2} i^{k-1}) \\
&\equiv -\frac{1}{p}(1+ps)\sum_{i=0}^{p-1}(-i^k) && \mod (\mathbb{Z}_p) \\
&\equiv \frac{(p-1)}{p}(1+ps) && \mod (\mathbb{Z}_p) \\
&\equiv -\frac{1}{p} && \mod (\mathbb{Z}_p)
\end{aligned}$$

This completes the proof when $p \neq 2$. We omit the case $p = 2$, since we assume $p \geq 5$ later on anyway. □

Now recall that

$$E_{p+1} = 1 - \frac{2(p+1)}{B_{p+1}}\sum_{n=1}^{\infty}\sigma_p(n)q^n$$

$$E_{p-1} = 1 - \frac{2(p-1)}{B_{p-1}}\sum_{n=1}^{\infty}\sigma_{p-2}(n)q^n.$$

Since $B_{p-1} \equiv -\frac{1}{p}$ $(\mathbb{Z}_p)$, we have that

$$\frac{2(p-1)}{-\frac{1}{p}+t} = \frac{2p(p-1)}{(-1+pt)} \equiv 0 \mod p.$$

Therefore, $E_{p-1} \equiv 1$ (p). This shows that $\widetilde{E_{p-1}} = 1$.

Moreover,

$$\frac{B_{p+1}}{p+1} \equiv \frac{B_2}{2} \equiv \frac{1}{12} \mod p,$$

so

$$\frac{B_{p+1}}{p+1} \in \mathbb{Z}_p^\times,$$

as $p \geq 5$. Moreover,

$$1 - \frac{2(p+1)}{B_{p+1}} \sum_{n=1}^{\infty} \sigma_p(n) q^n \equiv 1 - 24 \sum_{n=1}^{\infty} \sigma_1(n) q^n = E_2 \mod p,$$

because

$$\sigma_p(n) = \sum_{d|n} d^p \equiv \sigma_1(n) \mod p.$$

Note that $E_{p-1} = A(Q,R)$, $E_{p+1} = B(Q,R)$, where A, B are isobaric polynomials of weight $p-1$ and $p+1$, respectively. We may think of $A(x,y), B(x,y) \in \mathbb{Z}_{(p)}[x,y]$ and $\widetilde{A}(x,y), \widetilde{B}(x,y) \in \mathbb{F}_p[x,y]$.

Lemma 5.16. *We have that*

(1) $\widetilde{A}(\widetilde{Q},\widetilde{R}) = 1$, $\widetilde{B}(\widetilde{Q},\widetilde{R}) = \widetilde{P}$,
(2) $\partial\widetilde{A}(x,y) = \widetilde{B}(x,y)$, $\partial\widetilde{B}(x,y) = -x\widetilde{A}(x,y)$.

Proof. The above discussion already shows (1). For (2), we compute

$$\begin{aligned}(\widetilde{\partial A - B})(Q,R) &= (12\theta - (\widetilde{p-1)P})A(Q,R) - \widetilde{B(Q,R)} \\ &= \widetilde{P} - \widetilde{B}(\widetilde{Q},\widetilde{R}) \\ &= 0.\end{aligned}$$

Thus $(\partial A - B)(x,y)$ is p times a polynomial in (x,y), so $\partial\widetilde{A} = \widetilde{B}$. The second equality is proved similarly:

$$(\widetilde{\partial B + xA})(Q,R) = (12\theta - (\widetilde{p+1)P})B(Q,R) + Q\widetilde{A(Q,R)} = (12\theta - \widetilde{P})\widetilde{P} + \widetilde{Q} = 0,$$

as required. □

Lemma 5.17. *We have that $\widetilde{A}(x,y)$ has no repeated factors and is prime to $\widetilde{B}(x,y)$.*

Proof. Write $\widetilde{A}(x,y) = x^a y^b \cdot p(x,y)$, where $p(x,y)$ is an isobaric polynomial with not all terms involving both x and y. Over $\overline{\mathbb{F}_p}$, it factors as

$$\widetilde{A}(x,y) = x^a y^b \prod_i (x^3 - c_i y^2)^{n_i}.$$

Suppose $\widetilde{A}(x,y)$ is divisible exactly by $(x^3-cy^2)^n$ with $n \geq 2$. Note that x^3-y^2 does not divide $\widetilde{A}(X,Y)$ (which we see by plugging in $x=\widetilde{Q}$, $y=\widetilde{R}$). Now,

$$\partial(x^3-cy^2) = 3x^2(-4y) - c(2y)(-6x^2) = 12(c-1)x^2y,$$

which is coprime to x^3-cy^2. Also note that $n<p$. Then

$$\widetilde{A}(x,y) = (x^3-cy^2)n \cdot (\text{coprime to it})$$

and

$$\widetilde{B}(x,y) = \partial\widetilde{A}(x,y) = n(x^3-cy^2)^{n-1} \cdot (\text{coprime to } (x^3-cy^2))$$

is divisible exactly by $(x^3-cy^2)^{n-1}$. Since $n \geq 2$, we can repeat the same argument to see that $-x\widetilde{A} = \partial\widetilde{B}$ is divisible exactly by $(x^3-cy^2)^{n-2}$. This is a contradiction. One can use the same trick to show that $a,b \leq 1$.

The fact that $\widetilde{A}$ is prime to $\widetilde{B}$ follows by a similar argument. □

Proof of Theorem 5.6. We want to compute the kernel of the map

$$\mathbb{F}_p[x,y] \twoheadrightarrow \widetilde{M}.$$

Let I be the kernel. Since $\widetilde{M}$ is a domain which is not a field, I is prime, but it is not maximal. Moreover, $(\widetilde{A}(x,y)-1) \subseteq I$ by Lemma 5.16 (1). Then

$$(\widetilde{A}(x,y)-1) \subseteq I \subsetneq \mathfrak{m}$$

and $\mathbb{F}_p[x,y]$ has dimension 2, so it suffices to show that

$$\widetilde{A}(x,y)-1$$

is irreducible.

Suppose to the contrary that and irreducible factor $\phi(x,y)$ divides it and

$$\widetilde{A}(x,y)-1 = \underbrace{(\phi_n(x,y)+\phi_{n-1}(x,y)+\cdots+1)}_{\phi(x,y)} \cdot (*)$$

with $\phi_n(x,y)$ isobaric of degree n. Let $c \in \mathbb{F}_p^\times$ whcih is a primitive $(p-1)$st root of unity. Then

$$\widetilde{A}(c^4x, c^6y) = c^{p-1}\widetilde{A}(x,y) = \widetilde{A}(x,y).$$

Therefore, $\phi(c^4x,c^6y)$ also divides A and is not equal to $\phi(x,y)$ since $n<p-1$, so it is coprime to it. Therefore, we must have

$$\widetilde{A}(x,y)-1 = (\phi_n(x,y)+\phi_{n-1}(x,y)+\cdots+1)\cdot\big(\phi_n(c^4x,c^6y)+\cdots+1\big)\cdot(*).$$

Looking at the leading degree terms, we see that $\phi_n(x,y)\cdot\phi_n(c^4x,c^6y)$ divides $\widetilde{A}(x,y)$, and hence $\phi_n(x,y)^2$ divides $\widetilde{A}(x,y)$ (because $\phi_n(x,y)$ was isobaric of degree n). This is a contradiction with Lemma 5.17. □

Examples 5.18. For $p=11$, $E_{10}=QR$ and

$$\widetilde{M} \cong \frac{\mathbb{F}_{11}[Q,R]}{(QR-1)}.$$

For $p = 13$, $E_{12} = \dfrac{441Q^3 + 250R^2}{691}$, so

$$\widetilde{M} \cong \frac{\mathbb{F}_{13}[Q,R]}{(Q^3 + 3R^2 + 11)}.$$

Recall that we had the following picture

$$\begin{array}{ccccc}
\mathbb{Z}_{(p)}[x,y] & \xrightarrow{\cong} & M = \mathbb{Z}_{(p)}[Q,R] & \hookrightarrow & \mathbb{Z}_{(p)}[\![q]\!] \\
\downarrow & & \downarrow & & \downarrow \\
\frac{\mathbb{F}_p[x,y]}{(\widetilde{A}(x,y)-1)} & \xrightarrow{\cong} & \widetilde{M} & \hookrightarrow & \mathbb{F}_p[\![q]\!]
\end{array}$$

where $E_{p-1} = A(Q,R)$.

As a corollary to Theorem 5.6, we get the diagram

$$\begin{array}{ccc}
M_k & \xrightarrow{\cdot E_{p-1}} & M_{k+(p-1)} \\
\downarrow & & \downarrow \\
\widetilde{M_k} & \hookrightarrow & \widetilde{M_{k+(p-1)}}
\end{array}$$

For $\alpha \in \mathbb{Z}/(p-1)\mathbb{Z}$, we define

$$\widetilde{M}^{(\alpha)} = \varinjlim_{k \equiv \alpha \ (p-1)} \widetilde{M_k} = \bigcup_{k \equiv \alpha \ (p-1)} \widetilde{M_k}.$$

Remark 5.19. If α is not even, then $\widetilde{M}^{(\alpha)} = 0$. Also,

$$\widetilde{M} = \sum \widetilde{M}^{(\alpha)}.$$

Corollary 5.20. *We have that*

$$\widetilde{M} = \bigoplus_{\alpha \in \mathbb{Z}/(p-1)\mathbb{Z}} \widetilde{M}^{(\alpha)}$$

and

$$\widetilde{M}^{(\alpha)} \cdot \widetilde{M}^{(\beta)} \subseteq \widetilde{M}^{(\alpha+\beta)}.$$

In other words, $\widetilde{M}$ is graded with respect to $\mathbb{Z}/(p-1)\mathbb{Z}$.

Proof. One can check this using the fact that $\widetilde{A}(\widetilde{Q}, \widetilde{R}) = 1$ is the only relation. □

Corollary 5.21. *If $f \in M_k$ and $g \in M_{k'}$ satisfy $f \equiv g \not\equiv 0 \ (p)$, then $k \equiv k' \ (p-1)$.*

Proof. Since $\widetilde{f} = \widetilde{g} \neq 0$, they belong to the same graded piece, so $k \equiv k' \ (p-1)$ using Corollary 5.20. □

The next goal will be to prove a generalization of this, replacing p with a power of p. We will work towards this by studying the above diagram in more detail.

Proposition 5.22. *The operator θ preserves $\widetilde{M}$. In fact, if $\widetilde{f} \in \widetilde{M}_k$, then $\theta\widetilde{f} \in \widetilde{M}_{k+p+1}$.*

Proof. Lift $\widetilde{f}$ to some $f \in M_k$ and write $f = \phi(Q, R)$. Then

$$\partial f = (12\theta - kP)f,$$

so

$$12\theta f = \partial f + kPf = \partial\phi(Q, R) + kPf.$$

Reducing this modulo p, we get that

$$\begin{aligned} 12\theta\widetilde{f} &= \partial\widetilde{\phi}(\widetilde{Q}, \widetilde{R}) + k\widetilde{P}\widetilde{f} \\ &= \widetilde{A}(\widetilde{Q}, \widetilde{R})\partial\widetilde{\phi}(\widetilde{Q}, \widetilde{R}) + k\widetilde{B}(\widetilde{Q}, \widetilde{R})\widetilde{f} \\ &= (\widetilde{E_{p-1}\partial\phi + kE_{p+1}f}) \end{aligned}$$

Therefore, $\partial\widetilde{f}$ is a reduction of a modular form of weight $k + p + 1$. □

Note, however, that $\theta\widetilde{f}$ could live in $\widetilde{M_\ell}$ for $\ell < k + p + 1$. This motivates the following definition.

Definition 5.23 (Weight filtration)**.** Let $\widetilde{f}$ be a graded element in $\widetilde{M}$, i.e. it lives in $\widetilde{M}^{(\alpha)}$ for some α. Then $w(\widetilde{f})$ is the smallest integer $k \equiv \alpha\ (p-1)$ such that $\widetilde{f} \in \widetilde{M}_k$.

Remark 5.24. For $f \in M_k$, $f = \Phi(Q, R)$ where Φ is isobaric of degree k. Then $\widetilde{f} = \widetilde{\Phi}(\widetilde{Q}, \widetilde{R}) \in \widetilde{M}_k$. Then $w(\widetilde{f}) \le k$ and $w(\widetilde{f}) < k$ if and only if $\widetilde{A}$ divides $\widetilde{\Phi}$.

Proposition 5.25. *Let $\widetilde{f} \in \widetilde{M}$ be a graded element. Then:*

1. $w(\theta\widetilde{f}) \le w(\widetilde{f}) + p + 1$,
2. $w(\theta\widetilde{f}) = w(\widetilde{f}) + p + 1$ *if and only if* $w(\widetilde{f}) \not\equiv 0\ (p)$.

Proof. Part (1) is clear. For (2), let $k = w(\widetilde{f})$. Then $\widetilde{f}$ lifts to $f \in M_k$. We use the equality

$$12\theta\widetilde{f} = \widetilde{A}(\widetilde{Q}, \widetilde{R})\partial\widetilde{\phi}(\widetilde{Q}, \widetilde{R}) + k\widetilde{B}(\widetilde{Q}, \widetilde{R})\widetilde{f}$$

from the proof of Proposition 5.22.

If $p|k$, then $\theta\widetilde{f} = \widetilde{\partial\phi}$, so $w(\theta\widetilde{f}) \le k + 2 < k + (p+1)$.

If $k \not\equiv 0\ (p)$, then $\widetilde{A}$ does not divide $\widetilde{A}\partial\widetilde{\phi} + k\widetilde{B}\widetilde{\phi}$, so $w(\widetilde{\theta f}) = k + (p+1)$. □

Theorem 5.26. *Suppose $f \in M_k$, $f' \in M_{k'}$ such that $f \equiv f\ (p^m)$ but $f, f' \not\equiv 0\ (p)$. Then*

$$k \equiv k'\ (p^{m-1}(p-1)).$$

Proof. For $m = 1$, this is simply Corollary 5.21. We may hence assume $m \ge 2$.

Let $h = k' - k$. We have that

$$E_{p^n(p-1)} = 1 - \frac{2p^n(p-1)}{B_{p^n(p-1)}} \cdot \sum_k \sigma_{p^n(p-1)-1}(k)q^k \equiv 1\ (p^{n+1})$$

by the van Staudt congruence 5.15.

Multiplying f' by $E_{p^n(p-1)}$ for $n \gg 0$, we may assume that $h \geq 4$. Since $(p-1)|h$, we have that

$$E_h \equiv 1 \mod p.$$

We want to show that $v_p(h) \geq m-1$, i.e. $v_p(h)+1 \geq m$. Write $r = v_p(h)+1$ and suppose $r < m$. Then look at

$$fE_h - f' = \underbrace{(f-f')}_{\equiv 0 \ (p^m)} + \underbrace{f(E_h-1)}_{\equiv 0 \ (p^r)}.$$

Then

$$fE_h - f' \equiv 0 \ (p^r).$$

Now, we have that

$$p^{-r}\underbrace{(fE_h - f')}_{\in M_{k'}} \equiv p^{-r} f(E_h - 1) \ (p).$$

Now,

$$p^{-r}(E_h - 1) = \lambda \sum_{n=1}^{\infty} \sigma_{h-1}(n) q^n$$

where λ is a unit. Let

$$\phi = \sum_{n=1}^{\infty} \sigma_{h-1}(n) q^n.$$

Then

$$f\phi \equiv g \ (p)$$

where

$$g = \lambda^{-1} p^{-r}(fE_h - f') \in M_{k'}.$$

Reducing this equations modulo p, we get that $\widetilde{f}\widetilde{\phi} = \widetilde{g}$ and $\widetilde{f} \neq 0$, so

$$\widetilde{\phi} = \frac{\widetilde{g}}{\widetilde{f}} \in \text{fraction field of } \widetilde{M}.$$

Since $k' \equiv k \ (p-1)$,

$$\widetilde{\phi} \in \text{fraction field of } \widetilde{M}^{(0)}.$$

Now, we recall that

$$\phi = \sum_{n=1}^{\infty} \sigma_{h-1}(n) q^n.$$

Since $h \equiv 0 \ (p-1)$, $h-1 \equiv p-2 \ (p-2)$, and hence

$$\phi \equiv \sum_{n=1}^{\infty} \sigma_{p-2}(n) q^n \ (p).$$

Therefore,

$$\phi^p \equiv \sum_{n=1}^{\infty} \sigma_{h-1}(pn) q^{np}$$

and $\sigma_{h-1}(np) = \sigma_{h-1}(n)$, so

$$\widetilde{\phi} - \widetilde{\phi}^p = \widetilde{\psi}$$

where

$$\psi = \sum_{\substack{n=1 \\ (p,n)=1}}^{\infty} \sigma_{p-2}(n) q^n.$$

We claim that

$$\psi \equiv \theta^{p-2} \left(\sum_{n=1}^{\infty} \sigma_1(n) q^n \right).$$

This is clear since

$$\sigma_{p-2}(n) = \sum_{d|n} d^{p-2} \equiv \sum_{d|n} d^{-1}$$

$$n^{p-2}\sigma_1(n) = n^{p-2} \left(\sum_{d|n} d \right) \equiv n^{-1} \sum_{d|n} d$$

when p does not divide n.

Now,

$$\psi \equiv \theta^{p-2} \left(\sum_{n=1}^{\infty} \sigma_1(n) q^n \right) = -\frac{1}{24} \theta^{p-2}(\widetilde{P}) = -\frac{1}{24} \theta^{p-2}(\widetilde{E_{p+1}}).$$

Hence

$$\widetilde{\psi} \in \widetilde{M}^{(0)}$$

since $\widetilde{\psi} \in \widetilde{M}_{(p+1)+(p-2)(p+1)} = \widetilde{M}_{(p+1)(p-1)}$.

Fact. The space $\widetilde{M}^{(0)}$ is integrally closed. This will be Theorem 6.7.

We assume this fact for now and prove it later. Then the above argument shows that

$$\widetilde{\phi} \in \widetilde{M}^{(0)}.$$

Let $\ell = w(\widetilde{\phi})$. We may then write

$$\widetilde{\phi} = \Phi(\widetilde{Q}, \widetilde{R})$$

where Φ is isobaric of degree ℓ and $\widetilde{A}$ does not divide Φ. Then

$$\widetilde{\phi}^p = \Phi^p(\widetilde{Q}, \widetilde{R})$$

and $\widetilde{A}$ does not divide Φ^p. Therefore, $w(\widetilde{\phi}^p) = \ell p$, which shows that

$$w(\widetilde{\psi}) = w(\widetilde{\phi} - \widetilde{\phi}^p) = \ell p.$$

Now, note that $w(\widetilde{E_{p+1}}) = p + 1$ (because P is not modular). By Proposition 5.25, we get that

$$w(\theta^{p-2}(\widetilde{E_{p+1}})) = p + 1 + (p-2)(p+1) = (p+1)(p-1).$$

This cannot be equal to ℓp, which is a contradiction. □

We still need to prove the fact that $\widetilde{M}^{(0)}$ is integrally closed. This is quite difficult, so we delay the proof of this further (Theorem 6.7).

5.3. **Serre's p-adic modular forms.** The goal of this section is to prove the existence of the p-adic L-functions using congruences between modular forms. The references are [SD73] and [Ser73b]. This is the most classical approach to p-adic modular forms.

We will later present a different, more geometric approach to p-adic modular forms due to Katz [Kat73].

Recall that M is the set of forms with $\mathbb{Z}_{(p)}$-coefficients. Then $M \otimes \mathbb{Q}$ are the forms with $\mathbb{Q}$-coefficients. Let

$$A = \{f \in \mathbb{Q}_p[\![q]\!] \mid v_p(f) = \inf_n v_p(a_n(f)) > -\infty\} = \mathbb{Z}_p[\![q]\!] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \subseteq \mathbb{Q}_p[\![q]\!].$$

Then we have maps

$$M \hookrightarrow M \otimes \mathbb{Q} \overset{q\text{-expansion}}{\longrightarrow} A \subseteq \mathbb{Q}_p[\![q]\!].$$

Definition 5.27. If f_n and f are elements of $\mathbb{Q}_p[\![q]\!]$, we say that $f_n \to f$ if the coefficients of f_n tend to the coefficients of f uniformly.

Definition 5.28. A *p-adic modular form* (in the sense of Serre) is a formal power series

$$f = \sum_{n=0}^{\infty} a_n q^n \in \mathbb{Q}_p[\![q]\!]$$

such that there is a sequence of $f_i \in M \otimes \mathbb{Q}$ such that $f_i \to f$.

Remark 5.29. Note that a p-adic modular form f is an element of A.

What is the *weight* of a p-adic modular form? Let

$$X_m = \mathbb{Z}/p^{m-1}(p-1)\mathbb{Z} \cong \mathbb{Z}/p^{m-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}$$

and

$$X = \varprojlim X_m = \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}.$$

Note that there is a natural diagonal embedding $\Delta\colon \mathbb{Z} \hookrightarrow X$.

Theorem 5.30. *Let f be a p-adic modular form. Then f has a well-defined weight $\kappa \in X$ defined by $\kappa = \lim_i k_i$ where $f_i \to f$ and f_i has weight k_i.*

Proof. By multiplying f by a power of p, we may assume that $v_p(f) = 0$. Taking $f_i \to f$, eventually $v_p(f_i) = v_p(f) = 0$, so $f_i \in M$ and $f_i \not\equiv 0\ (p)$.

Given m, for any $i, j \gg 0$, we have that $v_p(f_i - f_j) \geq m$. By Theorem 5.26,

$$k_i \equiv k_j\ (p^{m-1}(p-1)).$$

Therefore, $\lim_i k_i$ is well-defined in X. It is also easy to see this is independent of the choice of f_i. □

Lemma 5.31. *If f, f' are two p-adic modular forms of the same weight, then $f + f'$ is also a p-adic modular form of that weight.*

Proof. Choose convergent sequences $f_i \to f$ of weights k_i and $f_i' \to f$ of weights k_i'. By assumption $\lim_i k_i = \lim_i k_i'$. Then multiply the terms of the sequences by appropriate Eisenstein series $E_{(p-1)p^m}$ to get new sequences $\hat{f}_i \to f$, $\hat{f}_i' \to f'$ of the same weights $k_i'' \to \kappa$. Then $\hat{f}_i + \hat{f}_i''$ is a sequence of modular forms of weights k_i'' converging to $f + f'$. □

We remark that Theorem 5.26 has the following generalization.

Corollary 5.32. *If $v_p(f - f') \geq v_p(f) + m$, then $k \equiv k'$ $(p^{m-1}(p-1))$.*

Proof. If $v_p(f) = r$, then $v_p(p^{-r}f) = 0$, so $v_p(p^{-r}f' - p^{-r}f) \geq m$. Then $k' \equiv k$ $(p^{m-1}(p-1))$ by Theorem 5.26. □

This has the following generalization for p-adic modular forms.

Theorem 5.33. *Suppose f' and f are p-adic modular forms of weight $\kappa, \kappa' \in X$, and suppose that $v_p(f' - f) \geq v_p(f) + m$. Then $\kappa' = \kappa$ in X_m.*

Proof. Write $f = \lim_i f_i$, $f' = \lim_i f_i'$. Then $v_p(f) = v_p(f_i)$, $v_p(f') = v_p(f_i')$ for $i \gg 0$. Similarly,

$$v_p(f_i) + m \leq v_p(f - f') = v_p(f_i - f_i') \quad \text{for } i \gg 0.$$

Hence $k_i' \equiv k_i$ $(p^{m-1}(p-1))$ for $i \gg 0$ by Corollary 5.32. Then $\kappa' = \kappa$ in X_m. □

Corollary 5.34. *Let $f = a_0 + a_1 q + \cdots$ be a p-adic modular form of weight κ. Suppose $\kappa \neq 0$ in X_{m+1}. Then $v_p(a_0) + m \geq \inf_i v_p(a_i)$.*

Proof. This is equivalent to saying that if $a_i \in \mathbb{Z}_p$ for all $i \geq 1$ and at least one is a unit, then $v_p(a_0) \geq -m$. We may assume that $a_0 \neq 0$. Suppose $v_p(a_0) = -r$. We want to show that $r \leq m$. Suppose contrary that $r > m$. We have that

$$p^{m+1}f = p^{m+1}a_0 + \sum_{i=1}^{\infty}(p^{m+1}a_i)q^i.$$

Then

$$v(p^{m+1}f) = v(p^{m+1}a_0) \leq 0.$$

Let $f' = p^{m+1}a_0$. Note, moreover, that

$$v_p(p^{m+1}f - f') \geq m + 1 \geq m + 1 + v_p(f').$$

By Theorem 5.33, this shows that $\kappa = 0$ in X_{m+1}, which is a contradiction. Therefore, $r \leq m$. □

Theorem 5.35. *Let $f^{(i)} = \sum_{n=0}^{\infty} a_n^{(i)} q^n$ be a sequence of p-adic modular forms of weights $\kappa^{(i)}$ such that*

(a) *$a_n^{(i)} \to a_n \in \mathbb{Q}_p$ uniformly for $n \geq 1$,*
(b) *$\kappa^{(i)} \to \kappa \neq 0$ in X.*

Then $a_0^{(i)}$ also converges to some $a_0 \in \mathbb{Q}_p$ and

$$f = a_0 + a_1 q + a_2 q^2 + \cdots$$

is a p-adic modular form of weight κ.

Proof. By (b), there exists m such that $\kappa^{(i)} \neq 0$ in X_m for $i \gg 0$. Also, there exists $t \in \mathbb{Z}$ such that $v_p(a_n^{(i)}) \geq t$ for all $n \geq 1$ and all $i \gg 0$. By Corollary 5.34,

$$v_p(a_0^{(i)}) + m \geq t \quad \text{for } i \gg 0.$$

Therefore, $a_0^{(i)}$ for $i \gg 0$ belong to a closed ball, and hence there exists a convergent subsequence $a_0^{(i_j)} \to a_0$. Then

$$f^{(i_j)} \to f = a_0 + a_1 q + \cdots .$$

Since each $f^{(i_j)}$ are all p-adic modular forms, f is also a p-adic modular form of weight κ.

Suppose $a_0^{(i'_j)} \to a'_0$ was a different convergent subsequence, we would get that

$$f^{(i_j)} \to f' = a'_0 + a_1 q + \cdots$$

which is also a p-adic modular form of weight κ. Then $f - f' = a_0 - a'_0$ is a p-adic modular form of weight κ by Lemma 5.31. But it is a constant $a_0 - a'_0$ so it is a p-adic modular form of weight 0. Since $\kappa \neq 0$, this is a contradiction. □

Take $\kappa \in X = \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$ and let $\kappa = (s, u)$. Let

$$\sigma^*_{\kappa-1}(n) = \sum_{\substack{d|n \\ (p,d)=1}} d^{\kappa-1}$$

where

$$d^\kappa = \langle d \rangle^s \omega(d)^u.$$

Observe that if $k_i \to \kappa$ in X and $k_i \to \infty$ as integers, then

$$\sigma^*_{\kappa-1}(n) = \lim_i \sigma_{k_i-1}(n),$$

because

$$\lim_i \sigma_{k_i-1}(n) = \lim_i \sum_{\substack{d|n \\ (p,d)=1}} d^{k_i-1} = \sigma^*_{\kappa-1}(n)$$

uniformly.

Recall that

$$G_{k_i} = -\frac{B_{k_i}}{2k_i} + \sum_{n=1}^{\infty} \sigma_{k_i-1}(n) q^n.$$

Since

$$\sum_{n=1}^{\infty} \sigma_{k_i-1}(n) q^n \to \sum_{n=1}^{\infty} \sigma_{\kappa-1}(n) q^n$$

Theorem 5.35 shows that

$$\lim_i \frac{-B_{k_i}}{k_i}$$

exists and we define it to be

$$\zeta^*(1-\kappa).$$

If $1-\kappa=(s,u)$, we define

$$\zeta^*(s,u) := \lim_{\substack{k_i\to\kappa \\ k_i\to\infty}} \zeta(1-k_i),$$

which is defined except when $s=1$ and $u=1$. For fixed u, this is a continuous function in s.

Definition 5.36 (p-adic Eisenstein series)**.** For a weight $\kappa\in X$, $\kappa\neq 0$, we set

$$G_\kappa^* = \frac{1}{2}\zeta^*(1-\kappa) + \sum_{n=1}^{\infty}\sigma_{\kappa-1}^*(n)q^n.$$

Theorem 5.37. *We have that $\zeta^*(s,u)=L_p(s,\omega^{1-u})$.*

Since this is a continuous function on $\mathbb{Z}_p$, we just need to evaluate $\zeta^*(s,u)$ for $s=1-k$. This is not easy to do. On the other hand, knowing that the p-adic L-function exists, it is not so hard to check that the two definitions agree. We will prove that this is true without assuming the existence of the p-adic L-function. In other words, we will show directly that

$$\zeta^*(1-k) = -\frac{B_k}{k}(1-p^{k-1})$$

for $k\in\mathbb{Z}$, $k\geq 2$.

5.4. **Hecke operators.** Let $f=\sum_{n\geq 0}a_nq^n$. We define operators U, V, and T_ℓ for $\ell\neq p$:

$$f|U = \sum_{n=0}^{\infty} a_{np}q^n$$

$$f|V = \sum_{n=0}^{\infty} a_n q^{pn}$$

$$f|_\kappa T_\ell = \sum_{n=0}^{\infty} a_{\ell n}q^n + \ell^{\kappa-1}\sum_{n=0}^{\infty}a_n q^{\ell n} \qquad \text{for } \kappa\in X$$

Theorem 5.38. *If f is a p-adic modular form of weight κ, then so are $f|U$, $f|V$, and $f|_\kappa T_\ell$.*

Proof. Consider modulars forms f_i of weight k_i such that $f_i\to f$. Note that $k_i\to\kappa$ in X. Replacing f_i by $f_i\cdot E_{p^i(p-1)}$, we may assume that $k_i\to\infty$.

Fact. The Hecke operator $|_kT_\ell$ preserves the space of usual modular forms of weight k.

Now,

$$f_i|_{k_i}T_\ell = \sum_{n=0}^{\infty}a_{\ell n,i}q^n + \ell^{k_i-1}\sum_{n=0}^{\infty}a_{n,i}q^{\ell n}.$$

Suppose $\ell\neq p$. Then the above expression tends to

$$\sum_{n=0}^{\infty}a_{\ell n}q^n + \ell^{\kappa-1}\sum_{n=0}^{\infty}a_nq^{\ell n} = f|_\kappa T_\ell.$$

Hence, $f|_\kappa T_\ell$ is a p-adic modular form, since it is the limit of regular modular forms $f_i|_{k_i}T_\ell$.

Now, suppose $\ell = p$. Then the above expression tends to

$$\sum_{n=0}^{\infty} a_{pn} q^n = f|U.$$

Hence $f|U$ is a p-adic modular form of weight κ.

Applying this to the modular form f_i, we see that $f_i|U$ is a p-adic modular form of weight k_i. Moreover,

$$f_i|_{k_i} T_p = \underbrace{\sum_{n=0}^{\infty} a_{np,i} q^n}_{f_i|U} + \underbrace{\ell^{k_i-1} \sum_{n=0}^{\infty} a_{n,i} q^{np}}_{f_i|V}.$$

Hence $f_i|V$ is a p-adic modular form of weight k_i by Lemma 5.31.

Finally, $f|V = \lim_i f_i|V$ is also a p-adic modular form. □

Suppose $k \geq 4$ in an integer. Then

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

We claim that G_k is an eigenfunction of all the T_ℓ with

$$G_k|_k T_\ell = (1 + \ell^{k-1}) G_k.$$

To see this, we just compute:

$$\begin{aligned} G_k|_k T_\ell &= \frac{1}{2}\zeta(1-k) + \sum_{n=1}^{\infty} \sigma_{k-1}(n\ell) q^n + \ell^{k-1} \left[\sum_{n=1}^{\infty} \sigma_{k-1}(n) q^{\ell n} + \frac{1}{2}\zeta(1-k) \right] \\ &= \frac{1}{2}\zeta(1-k)(1+\ell^{k-1}) + \sum_{n=1}^{\infty} q^n (\sigma_{k-1}(n\ell) + \ell^{k-1}\sigma_{k-1}(n/\ell)). \end{aligned}$$

We need to check that

$$\sigma_{k-1}(n\ell) + \ell^{k-1}\sigma_{k-1}(n/\ell) = (1+\ell^{k-1})\sigma_{k-1}(n),$$

i.e.

$$\sigma_{k-1}(n\ell) - \sigma_{k-1}(n) = \ell^{k-1}(\sigma_{k-1}(n) - \sigma_{k-1}(n/\ell)).$$

When ℓ does not divide n, this is clear. Otherwise, write $n = \ell^r m$ for $(\ell, m) = 1$. Then the expression above is:

$$\sigma_{k-1}(\ell^{r+1})\sigma_{k-1}(m) - \sigma_{k-1}(\ell^r)\sigma_{k-1}(m) = \ell^{k-1}(\sigma_{k-1}(\ell^r) - \sigma_{k-1}(\ell^{r-1}))\sigma_{k-1}(m).$$

Finally, this expression simplifies to

$$(\ell^{r+1})^{k-1} = \ell^{k-1}(\ell^r)^{k-1},$$

which is clearly true.

Recall that

$$G_\kappa^* = \lim_{\substack{k_i \to \kappa \\ k_i \to \infty}} G_{k_i}.$$

Proposition 5.39. *If $k \geq 4$, then*

$$G_k^* = G_k - p^{k-1}G_k|V.$$

Proof. We have that

$$\begin{aligned} G_k - p^{k-1}G_k|V &= -\frac{B_k}{2k} + \sum_{n\geq 1}\sigma_{k-1}(n)q^n - p^{k-1}\left[-\frac{B_k}{2k} + \sum_{n\geq 1}\sigma_{k-1}(n)q^{np}\right] \\ &= -(1-p^{k-1})\frac{B_k}{2k} + \sum_{n=1}^{\infty}(\sigma_{k-1}(n) - p^{k-1}\sigma_{k-1}(n/p))q^n \end{aligned}$$

We claim that

$$\sigma_{k-1}(n) - p^{k-1}\sigma(n/p) = \sigma_{k-1}^*(n).$$

If p does not divide n, this is clear. If $p|n$,

$$\sigma_{k-1}^*(n) = \sum_{d|n} d^{k-1} - \sum_{\substack{d|n \\ p|d}} d^{k-1} = \sigma_{k-1}(n) - p^{k-1}\sigma(n/p).$$

Therefore,

$$G_k - p^{k-1}G_k|V = -(1-p^{k-1})\frac{B_k}{2k} + \sum_{n=1}^{\infty}\sigma_{k-1}^*(n)q^n.$$

Since $G_k - p^{k-1}G_k|V$ and G_k^* are both p-adic modular forms of the same weight and all their terms agree except possibly the constant term. By Theorem 5.35, this implies that $G_k - p^{k-1}G_k|V = G_k^*$. □

Remark 5.40. This finishes the proof of Theorem 5.37.

Assume for now that this proposition holds also for $k = 2$.

Corollary 5.41. *The Eisenstein series G_2 is a p-adic modular form.*

Proof. We have that $G_k^* = G_k|(1 - p^{k-1}V)$. Therefore,

$$G_k = G_k^*|(1 + p^{k-1}V + ()p^{k-1}V)^2 + \cdots)$$

is a limit of p-adic modular forms, and hence a p-adic modular form. □

However, to prove the above proposition for $k = 2$, we need to check that

$$\zeta(-1)(1-p) = \lim_{k_i \to 2}\zeta(1-k_i).$$

Recall that the Kummer congruences 5.14 say that

$$m \equiv n \not\equiv 0\ (p-1) \text{ implies that } \frac{B_m}{m} \equiv \frac{B_n}{n} \mod (p).$$

Exercise. If $m \equiv n\ (p^{r-1}(p-1))$, $m \not\equiv 0\ (p-1)$, then

$$(1-p^{m-1})\frac{B_m}{m} \equiv (1-p^{n-1})\frac{B_n}{n} \mod (p^r).$$

Therefore, modulo large powers of p,

$$(1-p^{k_i-1})\frac{B_{k_i}}{k_i} \equiv (1-p)\frac{B_2}{2}.$$

Since $k_i \to \infty$, this shows that

$$\zeta(-1)(1-p) = \lim_{k_i \to 2} \zeta(1-k_i).$$

We have hence just proven the following proposition.

Proposition 5.42. *The Eisenstein series P is a p-adic modular form of weight 2.*

Theorem 5.43. *Let $f = \sum_{n\geq 0} a_n q^n$ be a p-adic modular form of weight κ. Then*

$$\theta f = \sum_{n\geq 0} n a_n q^n$$

is a p-adic modular form of weight $\kappa + 2$.

Proof. Take classical modular forms f_i of weight k_i such that $f_i \to f$. Recall that we introduce the operator ∂ such that

$$\partial f_i = (12\theta - k_i P) f_i$$

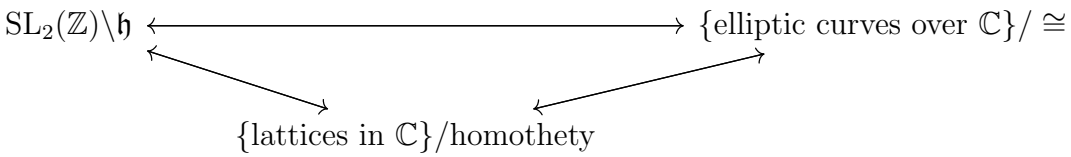
is a modular form of weight $k_i + 2$. Hence θf_i is a p-adic modular form of weight $k_i + 2$ by Proposition 5.42. Hence $\theta f = \lim_i \theta f_i$ is a p-adic modular form of weight $\kappa + 2$. □

6. Moduli-theoretic interpretation of modular forms

Note that the results of Section 5 assume the fact that $M^{(0)}$ in integrally closed. The proof of this relies on a geometric reinterpretation of modular forms due to Katz [Kat73].

6.1. Modular forms over $\mathbb{C}$.

Recall that, over $\mathbb{C}$, we have the following diagram:



For an element $\tau \in \mathfrak{h}$, the corresponding lattice is $\mathbb{Z}\tau + \mathbb{Z}$. Changing the lattice $\mathbb{Z}\tau + \mathbb{Z}$ by a homothety corresponds to changing τ by an element of $\mathrm{SL}_2(\mathbb{Z})$. Give a lattice L, the corresponding elliptic curve is $\mathbb{C}/L$. Indeed, the elliptic curve is given by the equation

$$E : y^2 = 4x^3 - g_2(L)x - g_3(L)$$

where

$$g_2(L) = 60 \sum_{\ell \in L\setminus\{0\}} \frac{1}{\ell^4},$$

$$g_3(L) = 140 \sum_{\ell \in L\setminus\{0\}} \frac{1}{\ell^6}.$$

Then the isomorphism is defined using the Weierstrass $\wp$ function

$$\begin{aligned}\mathbb{C}/L &\xrightarrow{\cong} E \\ z &\mapsto (\wp(z;L), \wp'(z;L)).\end{aligned}$$

Note also that the canonical differential $\frac{dx}{y}$ on E pulls back to dz on $\mathbb{C}/L$.

A modular form of weight k satisfies

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z).$$

Therefore, we can think of it as a function on lattices

$$F(L) = f(\omega_1/\omega_2)\omega_2^{-k} \quad \text{where } L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2,\ \omega_1/\omega_2 \in \mathfrak{h}.$$

Then, note that $F(\lambda L) = \lambda^{-k}F(L)$.

Finally, we may consider it as a function on pairs (E,ω) where E is an elliptic curve and ω is a differential on E. Then

$$f(E,\lambda\omega) = \lambda^{-k}F(E,\omega).$$

Now, consider the change of variables $q = e^{2\pi i\tau}$. First note that

$$F(\mathbb{C}/(\mathbb{Z}\tau+\mathbb{Z}), dz) = F(\mathbb{C}/(2\pi i(\mathbb{Z}\tau+\mathbb{Z})), 2\pi i dz).$$

Moreover, applying the exponential map

$$\exp\colon \mathbb{C}/(2\pi i(\mathbb{Z}\tau+\mathbb{Z})) \to \mathbb{C}^*/q^{\mathbb{Z}},$$

we get that

$$F(\mathbb{C}/(\mathbb{Z}\tau+\mathbb{Z}), dz) = F\left(\mathbb{C}^*/q^{\mathbb{Z}}, \frac{dt}{t}\right),$$

where the variable on $\mathbb{C}^*/q^{\mathbb{Z}}$ is denoted by t.

Finally, we may write

$$y^2 = 4x^3 - \frac{E_4}{12}x + \frac{E_6}{216}$$

with the differential $\frac{dx}{y}$. Then

$$F\left(y^2 = 4x^3 - \frac{E_4}{12}x + \frac{E_6}{216}, \frac{dx}{y}\right) \in \mathbb{C}(\!(q)\!),$$

considering the q-expansions of the Eisenstein series. The modular form is holomorphic at infinity if this belongs to $\mathbb{C}[\![q]\!]$.

Consider the change of variables $X = x + \frac{1}{12}$ and $Y = x + 2y$. Then the elliptic curve is

$$Y^2 + XY = X^3 + B(q)X + C(Q)$$

where

$$B(q) = -5\left(\frac{E_4 - 1}{240}\right),$$
$$C(q) = \frac{-5\left(\frac{E_4-1}{240}\right) - 7\left(\frac{E_6-1}{-504}\right)}{12}.$$

One can check that this is an elliptic curve over $\mathbb{Z}(\!(q)\!)$. It is called the *Tate curve*. The differential on it is given by

$$\frac{dX}{2Y + X}.$$

We denote it by $\mathrm{Tate}(q)$.

6.2. **Modular forms over an arbitrary ring.**

Definition 6.1. A *modular form* of weight k defined over a ring R is a function on pairs $(E/R', \omega)$ where $p\colon E \to \mathrm{Spec}(R')$ is an elliptic curve where R' is an R-algebra and ω is a nowhere vanishing differential form, i.e. a generator of $\underline{\omega}_{E/R} = p_*(\Omega^1_{E/R})$, satisfying the following properties:

(1) $f(E/R', \omega) \in R'$ only depends on the isomorphism class of $(E/R', \omega)$,
(2) $f(E/R', \lambda\omega) = \lambda^{-k} f(E/r', \omega)$ for $\lambda \in (R')^\times$,
(3) given a pullback of $E' \to \operatorname{Spec} R'$ along $\varphi\colon R' \to R''$:

$$\begin{array}{ccc} E'' & \longrightarrow & E' \\ \downarrow & & \downarrow \\ \mathrm{Spec}(R'') & \longrightarrow & \mathrm{Spec}(R') \end{array}$$

and if ω' pulls back to ω'', then

$$f(E''/R'', \omega'') = \varphi(f(E'/R', \omega')).$$

Recall that we defined an elliptic curve $\mathrm{Tate}(q)$ over $\mathbb{Z}(\!(q)\!)$. Base changing it to $\mathbb{Z}(\!(q)\!) \otimes R$ gives an elliptic curve over $\mathbb{Z}(\!(q)\!) \otimes R$ with a canonical differential. We may then evaluate

$$f(\mathrm{Tate}_R, \omega_{\mathrm{can}}) \in \mathbb{Z}(\!(q)\!) \otimes R.$$

This is the *q-expansion* of f. We will denote it by $\mathrm{qexp}(f)$. We say that f is *holomorphic* if

$$f(\mathrm{Tate}_R, \omega_{\mathrm{can}}) \in \mathbb{Z}[\![q]\!] \otimes R.$$

Let $\mathrm{Mod}_k(R)$ be the R-modular of holomorphic modular forms of weight k, defined over R.

For $R \to R'$, we have the diagram

$$\begin{array}{ccc} \mathrm{Mod}_k(R) & \longrightarrow & \mathrm{Mod}_k(R') \\ \downarrow{\scriptstyle \mathrm{qexp}} & & \downarrow{\scriptstyle \mathrm{qexp}} \\ \mathbb{Z}[\![q]\!] \otimes R & \longrightarrow & \mathbb{Z}[\![q]\!] \otimes R' \end{array}$$

Theorem 6.2 (Deligne–Rapoport/Katz, q-expansion principle)**.**

(1) *If* $f \in \mathrm{Mod}_k(R)$ *and* $\mathrm{qexp}(f) = 0$*, then* $f = 0$.
(2) *If* $R \hookrightarrow R'$ *and if* $f \in \mathrm{Mod}_k(R')$ *is such that* $\mathrm{qexp}(f) \in \mathbb{Z}[\![q]\!] \otimes R$*, then* $f \in \mathrm{Mod}_k(R)$.

Exercise. If $f \in M_k(\mathrm{SL}_2(\mathbb{Z}), \mathbb{C})$, then f is a modular form defined over $\mathbb{C}$, i.e.

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

Fix a prime $p \geq 5$. Recall that

$M_k = \{\text{fourier expansions of holomorphic modular forms with coefficients in } \mathbb{Z}_{(p)}\} \subseteq \mathbb{Z}_{(p)}[\![q]\!]$.

Via the q-expansion, using the q-expansion principle,

$$\mathrm{Mod}_k(\mathbb{Z}_{(p)}) \cong M_k.$$

We then have

$$\begin{array}{ccccc} \mathrm{Mod}_k(\mathbb{Z}_{(p)}) & \xrightarrow{\cong} & M_k & \hookrightarrow & \mathbb{Z}_{(p)}[\![q]\!] \\ \downarrow & & \downarrow & & \\ \mathrm{Mod}_k(\mathbb{F}_p) & \xrightarrow{\cong} & \widetilde{M_k} & \hookrightarrow & \mathbb{F}_p[\![q]\!] \end{array}$$

Consider $E_{p-1} \in \mathrm{Mod}_k(\mathbb{Z}_{(p)})$ and recall that its q-expansion is congruent to 1 modulo p. Therefore, we get an element

$$\overline{E_{p-1}} \in \mathrm{Mod}_{p-1}(\mathbb{F}_p)$$

whose q-expansion is 1.

We will construct explicitly an element of $\mathrm{Mod}_{p-1}(\mathbb{F}_p)$, called the *Hasse invariant* $\widehat{A}$ and check that $\overline{E_{p-1}} = \overline{A}$.

Definition 6.3. Let R be an $\mathbb{F}_p$-algebra and E/R be an elliptic curve. The absolute Frobenius

$$F_{\mathrm{abs}} \colon E \to E$$

defines a pullback

$$F_{\mathrm{abs}}^* \colon H^1(E, \mathcal{O}_E) \to H^1(E, \mathcal{O}_E)$$

which is not R-linear, but rather p-linear:

$$F_{\mathrm{abs}}^*(\alpha x) = \alpha^p F_{\mathrm{abs}}^*(x)$$

for $\alpha \in R$. Picking a differential ω on E/R, we get η which is a *dual basis* of $H^1(E, \mathcal{O}_E)$. Then we define the *Hasse invariant* $\overline{A}$ to be:

$$F_{\mathrm{abs}}^*(\eta) = \overline{A}(E, \omega) \cdot \eta.$$

Note that taking $\omega \mapsto \lambda\omega$ gives $\eta \mapsto \lambda^{-1}\eta$, then

$$F_{\mathrm{abs}}^*(\lambda^{-1}\eta) = \lambda^{-p} F_{\mathrm{abs}}^*(\eta) = \lambda^{-p}\overline{A}(E, \omega)\eta = \lambda^{-(p-1)}\overline{A}(E, \omega)(\lambda^{-1}\eta).$$

This shows that

$$\overline{A}(E, \lambda\omega) = \lambda^{-(p-1)}\overline{A}(E, \omega),$$

so $\overline{A}$ is a modular form of weight $p - 1$.

Theorem 6.4. *We have that* $\overline{A} = \overline{E_{p-1}}$.

We defer the proof of this theorem until later. For now, we discuss its applications.

Definition 6.5. Let K be a field of characteristic p. We say that an elliptic curve E/K is *supersingular* if

$$F_{\text{abs}}\colon H^1(E, \mathcal{O}_E) \to H^1(E, \mathcal{O}_E)$$

is the zero map.

Therefore, an elliptic curve is supersingular if and only if its Hasse invariant vanishes.

Theorem 6.6. *There are only finitely many supersingular j-invariants; in fact all of them lie in $\mathbb{F}_{p^2}$.*

Exercise. Pick your favorite modular form f and an elliptic curve with a differential (E, ω). Compute $f(E, \omega)$. You can use Magma or Sage for this. If you pick a modular form with rational coefficient and a rational elliptic curve, your answer will be a rational number.

Theorem 6.7. *Recall that*

$$\widetilde{M}^{(0)} = \varinjlim_{k \equiv 0 \ (p-1)} \widetilde{M}_k.$$

Then

$$\widetilde{M}^{(0)} \cong \mathcal{O}(\mathbb{P}^1_{\mathbb{F}_p} \setminus \{\textit{supersingular points}\}),$$

so it is integrally closed.

Sketch of proof. Take $f \in \widetilde{M}^{(0)}$. Then consider

$$f \in \widetilde{M}_{h(p-1)} = \text{Mod}_{k(p-1)}(\mathbb{F}_p).$$

Note that also

$$\overline{E_{p-1}}^h \in \text{Mod}_{h(p-1)}(\mathbb{F}_p).$$

Then

$$f \Big/ \overline{E_{p-1}}^h$$

is a function on non-supersingular elliptic curves over $\mathbb{F}_p$. Check that this is a rational function on $\mathbb{P}^1_{\mathbb{F}_p}$ with poles only at supersingular points.

Exercise. The map

$$\widetilde{M}^{(0)} \to \mathcal{O}(\mathbb{P}^1_{\mathbb{F}_p} \setminus \{\text{supersingular points}\})$$

is injective and surjective. □

We still need to prove Theorem 6.4:

$$\overline{A} = \overline{E_{p-1}}.$$

The original proof due to Deligne is to compute the q-expansion of $\overline{A}$. We will instead present a proof due to Kaneko–Zagier [KZ98]. We will only show the equality up to a non-zero scalar, but one can trace through the details of the proof to get the actual equality.

We need to check

$$\overline{A}(E, \omega) = \overline{E_{p-1}}(E, \omega)$$

for every (E, ω) over $\overline{\mathbb{F}_p}$.

Let us think how to evaluate the modular form $\overline{E_{p-1}}$ at an elliptic curve $E/\mathbb{F}_p$. First, we lift the elliptic curve to $\widetilde{E}/\mathbb{Z}_{(p)}$, then evaluate E_{p-1} at this lift of the elliptic curve, and reduce the answer modulo p.

Remark 6.8. An elliptic curve E over $\overline{\mathbb{F}_p}$ is supersingular if and only if $E[p](\overline{\mathbb{F}_p}) = 0$.

Suppose E is given by the equation $y^2 = f(x)$ where $f(x)$ is a cubic polynomial.

Proposition 6.9. *Let $E/\mathbb{F}_q$ be defined by the equation $y^2 = f(x)$. Let a_p be the coefficient of x^{p-1} in $f(x)^{\frac{p-1}{2}}$. Then*

$$|E(\mathbb{F}_q)| = 1 - N_{\mathbb{F}_q/\mathbb{F}_p}(a_p) \quad \text{in } \mathbb{F}_p.$$

Proof. We count the number of solutions to $y^2 = f(x)$ for fixed x:

- if $f(x) \notin \mathbb{F}_p^2$, then there are 0 solutions,
- if $f(x) = 0$, then there is 1 solution,
- if $f(x) \in (\mathbb{F}_p^\times)^2$, then there are 2 solutions.

This may be written concisely as

$$(1 + f(x))^{\frac{q-1}{2}} \quad \text{in } \mathbb{F}_q.$$

Therefore,

$$|E(\mathbb{F}_q)| = 1 + \sum_{x \in \mathbb{F}_q} (1 + f(x)^{\frac{q-1}{2}}) \quad \text{in } \mathbb{F}_q.$$

Hence

$$|E(\mathbb{F}_q)| = 1 + \sum_{x \in \mathbb{F}_q} f(x)^{\frac{q-1}{2}} \quad \text{in } \mathbb{F}_q.$$

The degrees of the monomials appearing in this expression are between 0 and $\frac{3(q-1)}{2}$. Note that

$$\sum_{x \in \mathbb{F}_q} = \begin{cases} 0 & \text{if } j \neq q-1, \\ -1 & \text{if } j = 1. \end{cases}$$

Therefore:

$$|E(\mathbb{F}_q)| = 1 - \left(\text{coefficient of } x^{q-1} \text{ in } f(x)^{\frac{q-1}{2}}\right) \quad \text{in } \mathbb{F}_q.$$

Finally,

$$\begin{aligned} f(x)^{\frac{q-1}{2}} &= f(x)^{\frac{p^r-1}{2}} \\ &= f(x)^{\frac{p-1}{2}(1+p+\cdots+p^{r-1})} \\ &= f(x)^{\frac{p-1}{2}} f^{(p)}(x^p)^{\frac{p-1}{2}} \cdots f^{(p^{r-1})}(x^{p^{r-1}})^{\frac{p-1}{2}}. \end{aligned}$$

Write

$$x^{q-1} = x^{a_0} x^{pa_1} \cdots x^{p^{r-1}a_{r-1}}$$

according to the above decomposition. Then

$$q - 1 = a_0 + pa_1 + \cdots + p^{r-1}a_{r-1} = (p-1) + p(p-1) + \cdots + p^{r-1}(p-1)$$

we see that

$$0 \leq a_i \leq 3\frac{(p-1)}{2}.$$

In particular,

$$|a_i - (p-1)| \leq p-1.$$

Then induction on i gives $a_i = p-1$. Hence the coefficient of x^{q-1} in $f(x)^{\frac{q-1}{2}}$ is

$$a_p a_p^p \cdots a_p^{p^r-1} = N_{\mathbb{F}_q/\mathbb{F}_p}(a_p).$$

This completes the proof. □

Corollary 6.10. *An elliptic curve is supersingular if and only if $a_p = 0$.*

Proof. Suppose $a_p \neq 0$. Then there is an n such that $N_{\mathbb{F}_q/\mathbb{F}_p}(a_p)^n = 1$. Then

$$\#E(\mathbb{F}_{q^n}) = 1 - N_{\mathbb{F}_{q^n}/\mathbb{F}_p}(a_p) = 1 - N_{\mathbb{F}_q/\mathbb{F}_p}(a_p)^n = 0 \quad \text{in } \mathbb{F}_p$$

by Proposition 6.9. This shows that $E(\mathbb{F}_q)[p] \neq \emptyset$, so the curve is not supersingular. □

Let $E_\lambda : y^2 = x(x-1)(x-\lambda)$ be an elliptic curve in Legandre form. When is E_λ supersingular?

The coefficient of x^{p-1} in $(x(x-1)(x-\lambda))^{\frac{p-1}{2}}$ is the coefficient of $x^{\frac{p-1}{2}}$ in $((x-1)(x-\lambda))^{\frac{p-1}{2}}$ which is

$$\sum_{i=0}^{r=(p-1)/2} (-1)^{r-i}\binom{r}{r-i}(-\lambda)^i\binom{r}{i} = (-1)^r \sum_{i=0}^{r}\binom{r}{i}^2\lambda^i.$$

We call this polynomial $H(\lambda)$. Then the corollary says that E_λ is supersingular if and only if $H(\lambda) = 0$.

Observation. Since $\lambda \mapsto j(E_\lambda)$ is a rational function of degree 6 is roughly 6-to-1. Therefore, there are roughly $\frac{p-1}{12}$ supersingular j-invariants (up to a constant).

In fact, one can prove a precise result of this form by analyzing when two j-invariants can be equal. The details of this are in Silverman's book [Sil09].

Proposition 6.11 (Ihara)**.** *The polynomial $H(\lambda)$ has no multiple roots.*

Proof. Consider the differential operator

$$D = 4\lambda(1-\lambda)\frac{d^2}{d\lambda^2} + 4(1-2\lambda)\frac{d}{d\lambda} - 1.$$

We claim that $DH(\lambda) = 0$.

$$\begin{aligned}
(-1)^r DH(\lambda) &= 4\lambda(1-\lambda)\sum_{i=0}^{r}\binom{r}{i}^2 i(i-1)\lambda^{i-2} + 4(1-2\lambda)\sum_{i=0}^{r}\binom{r}{i}^2 i\lambda^{i-1} - \sum_{i=0}^{r}\binom{r}{i}^2\lambda^i \\
&= \sum_{i=0}^{r}\binom{r}{i}^2\left[4(i)(i-1)\lambda(1-\lambda)\lambda^{i-2} + 4(1-2\lambda)i\lambda^{i-1} - \lambda^i\right] \\
&= \sum_{i=0}^{r}\binom{r}{i}^2\left[\lambda^i(-4i(i-1) - 8i - 1) + \lambda^{i-1}(4i(i-1)+4i)\right] \\
&= \sum_{i=0}^{r}\binom{r}{i}^2\left[\lambda^i(-4i^2 - 4i - 1) + \lambda^{i-1}(4i^2)\right] \\
&= \sum_{i=0}^{r}\lambda^i\left[\binom{r}{i}^2(-4i^2-4i-1) + \binom{r}{i+1}^2 4(i+1)^2\right] \\
&= \sum_{i=0}^{r}\lambda^i\binom{r}{i}^2\left[(-4i^2-4i-1) + (r-i)^2\cdot 4\right] \\
&= \sum_{i=0}^{r}\lambda^i\binom{r}{i}^2[-4i^2-4i-1+4r^2-8ri+4i^2-4i-1+(p-1)^2-4(p-1)i] \\
&= 0
\end{aligned}$$

in $\mathbb{F}_p$. For $\lambda \neq 0, 1$, this shows that the polynomial $H(\lambda)$ has no multiple roots. For $\lambda = 0, 1$, one can check this by hand. □

Since the roots of $H(\lambda)$ are at λ corresponding to supersingular elliptic curves E_λ, we immediately get the following corollary.

Corollary 6.12. *The numerator*[1] *of the rational function* $\overline{A}\left(E_\lambda, \frac{dx}{y}\right)$ *in* λ *is divisible by* $H(\lambda)$.

We now reach the idea of Kaneko and Zagier. They consider

$$\begin{aligned}
E_k &= \text{usual Eisenstein series} \\
\widetilde{G_k} &= \text{coefficient of } x^k \text{ in } (1 - 3E_4(\tau)x^4 + 2E_6(\tau)x^6)^{-\frac{1}{2}} \\
H_k &= \text{coefficient of } x^k \text{ in } (1 - 3E_4(\tau)x^4 + 2E_6(\tau)x^6)^{\frac{k}{2}},
\end{aligned}$$

which are all modular forms of weight k.

Proposition 6.13. *We have that*

$$\widetilde{G_{p-1}} \equiv H_{p-1} \equiv \pm E_{p-1} \mod p.$$

[1]Note that $\overline{A}\left(E_\lambda, \frac{dx}{y}\right)$ is a rational function in λ with only possibly λ or $\lambda - 1$ in the denominator.

Proof. It is easy to see that $\widetilde{G_{p-1}} \equiv H_{p-1} \mod p$. Note that

$$\widetilde{G_k} = \mathrm{Res}_{x=0} \frac{dx}{x^{k+1}\sqrt{1-3E_4x^4+2E_6x^6}}.$$

The elliptic curve given by the equation

$$y^2 = x^3 - 3E_4(\tau)x + 2E_6(\tau)$$

is isomorphic to $E_\tau = \mathbb{C}/(\mathbb{Z}\tau+\mathbb{Z})$ defined before. In fact, it is parameterized by

$$x = \wp(z),\ y = -\frac{1}{2}\wp'(z)$$

where we recall that

$$\wp(z) = \frac{1}{z^2} + \sum_{\ell \in (\mathbb{Z}\tau+\mathbb{Z})'} \left(\frac{1}{(z-\ell)^2} - \frac{1}{\ell^2} \right).$$

Writing

$$\frac{1}{(z-\ell)^2} - \frac{1}{\ell^2} = \frac{1}{\ell^2}\left[\frac{2z}{\ell} + \frac{3z^2}{\ell^2} + \cdots \right],$$

we get that

$$\wp(z) = \frac{1}{z^2} - \sum_{\substack{n \geq 4 \\ \text{even}}} \frac{12^{n/2}B_n}{(n-2)!n} E_n(\tau) z^{n-2}.$$

Consider the substitution $X = \wp(z)^{-\frac{1}{2}}$. Then

$$1 - 3E_4X^4 + 2E_6X^6 = 1 - 3E_4\wp(z)^{-2} + 2E_6\wp(z)^{-3}.$$

The residue expression for $\widetilde{G_k}$ above becomes

$$\begin{aligned}
\widetilde{G_k} &= \mathrm{Res}_{z=0} \frac{-\frac{1}{2}\wp(z)^{-\frac{3}{2}}\wp'(z)dz}{\wp(z)^{-\left(\frac{k+1}{2}\right)}\sqrt{1-3E_4\wp(z)^{-2}+2E_6\wp(z)^{-3}}} \\
&= -\frac{1}{2}\,\mathrm{Res}_{z=0} \frac{\wp'(z)dz}{\sqrt{\wp(z)^3 - 3E_4\wp(z) + 2E_6}} \wp(z)^{\frac{k+1}{2}} \\
&= \mathrm{Res}_{z=0}\, \wp(z)^{\frac{k+1}{2}} dz \\
&= \text{coefficient of } z^k \text{ in } \left(1 - \sum_{\substack{n \geq 4 \\ \text{even}}} \frac{12^{n/2}B_n}{(n-2)!n} E_n(\tau) z^n \right)^{\frac{k+1}{2}}.
\end{aligned}$$

For $k = p-1$, we get that

$$\widetilde{G_{p-1}} = \text{coefficient of } z^k \text{ in } \left(1 - \sum_{\substack{n \geq 4 \\ \text{even}}} \frac{12^{n/2}B_n}{(n-2)!n} E_n(\tau) z^n \right)^{\frac{p}{2}}.$$

Note that for $4 \leq n < p-1$,

$$\frac{B_n}{(n-2)!n} E_n(\tau)$$

is p-integral. Note that

$$\begin{aligned}\left(1-\frac{12^{\frac{p-1}{2}}B_{p-1}}{(p-3)!(p-1)}E_{p-1}(z)z^{p-1}\right)^{\frac{p}{2}} &\approx -\frac{p}{2}\frac{12^{\frac{p-1}{2}}B_{p-1}}{(p-3)!(p-1)}E_{p-1}(\tau)\\ &\equiv 12^{\frac{p-1}{2}}E_{p-1}(\tau) && \text{as } \frac{pB_{p-1}}{(p-1)!}\equiv 1\ (p)\\ &\equiv \pm E_{p-1}(\tau) && \bmod p.\end{aligned}$$

This completes the proof. □

We therefore see that

$$\begin{aligned}\pm\overline{E_{p-1}}\left(E_\lambda,\frac{dx}{y}\right) &= \overline{H_{p-1}}\left(E_\lambda,\frac{dx}{y}\right)\\ &= (\text{constant})\cdot H(\lambda)\end{aligned}$$

where the last inequality is given by noticing that H_{p-1} is the coefficient of x^{p-1} in

$$(x^3-3Qx+2R)^{\frac{p-1}{2}},$$

evaluating it at the Legendre family. and checking it agree with the definition of $H(\lambda)$ after converting from Legandre form to Weiestrass form. This can be found in Hartshorne [Har77].

Combining this with Corollary 6.12, we have shown that

$$\pm\frac{\overline{E_{p-1}}}{\overline{A}}\left(E_\lambda,\frac{dx}{y}\right)=\lambda^\alpha(\lambda-1)^\beta$$

for some α,β. We just need to show that $\alpha=\beta=0$. Since the ratio

$$\frac{\overline{E_{p-1}}}{\overline{A}}$$

is a function of elliptic curves (invariant scaling the differential forms), it must be a rational function in j. Moreover,

$$j(E_\lambda)=256\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$$

and one can verify by an elementary calculation that the maps

$$\lambda\mapsto 1-\lambda \tag{2}$$

$$\lambda\mapsto\frac{1}{\lambda} \tag{3}$$

preserve this expression. Then (2) shows that $\alpha=\beta$ and (3) shows that $\alpha=\beta=0$. We have hence finally proved Theorem 6.4.

7. p-adic L-functions associated to Hecke characters

We will be interested in p-adically interpolating special values of L-functions of Hecke characters of imaginary quadratic fields, We will first have to establish algebraicity results.

Let K be an imaginary quadratic field. Assume that it has class number 1 for simplicity. *Unramified (algebraic) Hecke character* are multiplicative functions

$$\chi\colon I \to \mathbb{C}^\times$$

where I is the set of ideal of K such that

$$\chi((\alpha)) = \alpha^k \overline{\alpha}^j = \alpha^{k-j}(\alpha\overline{\alpha})^j$$

where k and j are integers and the number of roots of unity divides $k-j$ (so that this is well-defined). We then say that χ has *infinity type* (k,j).

For definition of L-functions, let us assume χ has infinity type $(k,-j)$. The L-function such a character χ is

$$L(\chi,s) = \sum_{\mathfrak{a}\subseteq\mathcal{O}_K} \chi(\mathfrak{a}) N\mathfrak{a}^{-s} = \prod_{\mathfrak{p}} (1-\chi(\mathfrak{p})N\mathfrak{p}^{-s})^{-1}.$$

Note that replacing s by $s+1$ scales the Dirichlet L-funtion by $N\mathfrak{a}$. For $\mathfrak{a}=(\alpha)$, $N\mathfrak{a}=(\alpha\overline{\alpha})$. Therefore, it is enough to compute the L-function at 0 and the other values at integers will be obtained by changing the character by the norm. We have

$$\begin{aligned} L(\chi^{-1},0) &= \frac{1}{w_K}\sum_{\alpha\in\mathcal{O}_K} \frac{\overline{\alpha}^j}{\alpha^k} \\ &= \frac{1}{w_K}\sum_{\alpha\in\mathcal{O}_K} \frac{(\alpha\overline{\alpha})^j}{\alpha^{j+k}} \\ &= \frac{1}{w_K}\sum_{\alpha\in\mathcal{O}_K} \frac{1}{\alpha^{j+k}|\alpha|^{-2j}} \\ &= \frac{1}{w_K}\sum_{\substack{(m,n)\in\mathbb{Z}^2\\ \neq(0,0)}} \frac{1}{(m\tau_0+n)^{j+k}|m\tau_0+n|^{-2j}} \qquad \text{where } \mathcal{O}_K = \mathbb{Z}+\mathbb{Z}\tau_0 \text{ for } \tau_0\in\mathfrak{h}. \end{aligned}$$

7.1. **Real analytic Eisenstein series.** The above calculation motivates the definition of real analytic Eisenstein series.

Definition 7.1. The *real analytic Eisenstein series* is defined as

$$\widetilde{E_k}(z,s) = \sum_{(m,n)} \frac{1}{(mz+n)^k|mz+n|^{2s}}.$$

This is absolutely convergent when $k+2s>2$, but we will ignore this issue for now.

Note that $\widetilde{E_k}(z,0) = \widetilde{E_k}(z)$. Also,

$$\widetilde{E_k}(z,-r)\cdot \mathrm{Im}(z)^{-r}$$

is a modular form of weight k, but it is not holomorphic (merely analytic).

Strategy. To relate $\widetilde{E_k}(z,-r)$ to the usual holomorphic Eisenstein series via differential operators.

Definition 7.2. The *Shimura–Maass* operator is defined as

$$\delta_k = \frac{1}{2\pi i}\left(\frac{\partial}{\partial z} + \frac{k}{2iy}\right) = \left(\theta - \frac{k}{4\pi y}\right).$$

Note that

$$\delta_k = \frac{1}{2\pi i} y^{-k} \frac{\partial}{\partial z}(y^k \cdot f).$$

Remark 7.3. This is a *level raising operator* on the Lie algebra of GL_2 written out explicitly.

Proposition 7.4. *If f is modular of weight k, then $\delta_k f$ is modular of weight $k+2$.*

Proof. Recall that $\partial = \theta - \frac{k}{12}P$ takes modular forms of weight k to modular forms of weight $k+2$ by Theorem 5.7. It is hence enough to check that

$$\frac{P}{12} - \frac{1}{4\pi y} = \frac{E_2(z)}{12} - \frac{2i}{4\pi(z-\overline{z})}$$

is a real analytic modular form of weight 2. We just need to check invariance under $z \mapsto -\frac{1}{z}$ Recall that by Lemma 5.9, we have that

$$E_2\left(-\frac{1}{z}\right) = z^2 E_2(z) + \frac{12z}{2\pi i}.$$

Then the expression above after letting $z \mapsto -\frac{1}{z}$ is

$$\frac{z^2 E_2(z)}{12} + \frac{z}{2\pi i} + \frac{z\overline{z}}{2\pi i(z-\overline{z})} = z^2\left(\frac{E_2(z)}{12} + \frac{1}{(2\pi i)(z-\overline{z})}\right).$$

This completes the proof. □

Definition 7.5 (Shimura)**.** A *nearly holomorphic* modular form of weight k is

$$f(z) = \sum_{j=0}^{p} f_j(z) y^{-j}$$

where f_j are holomorphic modular forms, f transforms like a modular form of weight k, and the finiteness condition at the cusp is satisfies. The space of such forms is denoted by $N_k^p(\Gamma)$, where p is the maximal power of y^{-1} allowed.

In this notation, Proposition 7.4 implies that the map δ_k on $N_k^p(\Gamma)$ is

$$\delta_k \colon N_k^p(\Gamma) \to N_{k+2}^{p+1}(\Gamma).$$

Definition 7.6. We let $\delta_k^r = \delta_{k+2r-2} \circ \cdots \circ \delta_{k+2} \circ \delta_k$. If k is known, we simply write δ^r.

Lemma 7.7. *We have that*

$$\delta_k^r \widetilde{E_k}(z,s) = \frac{1}{(2\pi i)^r}(z-\overline{z})^{-r}\widetilde{E_{k+2r}}(z, s-r) \cdot \frac{\Gamma(k+r)}{\Gamma(k)} + s \cdot (\textit{holomorphic function in } s).$$

Letting $s = 0$, we obtain the following corollary.

Corollary 7.8. *Setting $s = 0$,*

$$\delta_k^r \widetilde{E_k}(z) = \left(-\frac{1}{4\pi y}\right)^r \frac{\Gamma(k+r)}{\Gamma(k)} \widetilde{E_{k+2r}}(z, -r).$$

Proof of Lemma 7.7. We proceed by induction on r. We have that

$$\begin{aligned}(2\pi i\delta_k)^{r+1}\widetilde{E_k}(z,s) &= \frac{\Gamma(k+r)}{\Gamma(k)}(z-\overline{z})^{-(k+2r)}\frac{\partial}{\partial z}\left[(z-\overline{z})^{k+r}\cdot\sum_{(m,n)}\frac{1}{(mz+n)^{k+2r}|mz+n|^{2(s-r)}}\right]\\ &= \frac{\Gamma(k+r)}{\Gamma(k)}\cdot(z-\overline{z})^{-(k+2r)}\Bigg[\sum(k+r)(z-\overline{z})^{k+r-1}(mz+n)^{-(k+2r)}|mz+n|^{-2s+2r}\\ &\quad-(z-\overline{z})^{k+r}(k+2r)(mz+n)^{-(k+2r+1)}|mz+n|^{-2(s-r)}m\\ &\quad+(z-\overline{z})^{k+r}(mz+n)^{-(k+2r)}(|mz+n|^2)^{r-s-1}(m\overline{z}+n)m(r-s)\Bigg]\\ &= (z-\overline{z})^{-(r+1)}\Bigg[\sum(k+r)(mz+n)^{-(k+zr)}|mz+n|^{-2s+2r}\\ &\quad-(k+2r)(mz+n)^{-(k+2r+1)}|mz+n|^{-2s+2r}((mz+n)-(m\overline{z}+n))\\ &\quad+(mz+n)^{-(k+2r)}|mz+n|^{2r-2s-2}(m\overline{z}+n)[(mz+n)-(m\overline{z}+n)](r-s)\Bigg]\end{aligned}$$

where we note that $(z-\overline{z})m=(mz+n)-(m\overline{z}+n)$. Multiplying this out, we get a sum of 5 terms:

$$\begin{aligned}&(1){:}+(k+r)(mz+n)^{-(k+2r)}|mz+n|^{-2s+2r}\\ &(2){:}-(k+2r)(mz+n)^{-(k+2r)}|mz+n|^{-2s+2r}\\ &(3){:}+(k+2r)(mz+n)^{-(k+2r+2)}|mz+n|^{-2s+2r+2}\\ &(4){:}+(r-s)(mz+n)^{-(k+2r)}|mz+n|^{-2s+2r}\\ &(5){:}-(r+s)(mz+n)^{-(k+2r+2)}|mz+n|^{2r-2s+2}\end{aligned}$$

Combining (1), (2), and (4), we get something which only involves something which is s times a holomorphic function in s, so we may ignore that. Combining (3) and (5), we finally get that the part not equal to s times a holomorphic function in s is equal to:

$$(z-\overline{z})^{-(r+1)}\frac{\Gamma(k+r)}{\Gamma(k)}(k+r)\widetilde{E_{k+2r+2}}(z,s-r-1).$$

This completes the proof by induction on r. □

Take $\Gamma\subseteq\Gamma(N)\subseteq\mathrm{SL}_2(\mathbb{Z})$.

Definition 7.9 (Shimura)**.** Let $k\geq 0$. Define

$$\mathcal{A}_k(\overline{\mathbb{Q}})=\{\text{meromorphic functions } F/G \mid F\in M_{k+r}(\Gamma,\overline{\mathbb{Q}}),\ G\in M_r(\Gamma,\overline{\mathbb{Q}})\}$$

Theorem 7.10 (Shimura)**.** *Let $f\in\mathcal{A}_k(\overline{\mathbb{Q}})$, $k\geq 0$. Then $\delta^r f$ behaves like an element of $\mathcal{A}_{k+2r}(\overline{\mathbb{Q}})$ at all CM points. More precisely, if $\tau\in\mathfrak{h}$ belongs to an imaginary quadratic field, then*

$$\frac{\delta^r f(\tau)}{g(\tau)}\in\overline{\mathbb{Q}}$$

for all $g\in\mathcal{A}_{k+2r}(\overline{\mathbb{Q}})$ such that $g(\tau)\neq 0$.

Proof. For $\tau \in K$ and any $\alpha \in K^\times$, we note that

$$\alpha \begin{bmatrix} \tau \\ 1 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \tau \\ 1 \end{bmatrix}$$

for some

$$\gamma_\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Q})^+.$$

This defines a map

$$K \to M_2(\mathbb{Q})$$

such that $\gamma_\alpha(\tau) = \tau$. As always, we define

$$(f|_k\gamma_\alpha)(z) = f(\gamma_\alpha(z))j(\gamma_\alpha, z)^{-k}.$$

Exercise. If $f \in M_k(\Gamma, \overline{\mathbb{Q}})$, then

$$(f|_k\gamma_\alpha) \in M_k(\Gamma', \overline{\mathbb{Q}})$$

for some $\Gamma' \subseteq \Gamma$.

This shows that

$$\frac{f|_k\gamma_\alpha}{f} = h \in \mathcal{A}_0(\overline{\mathbb{Q}}).$$

Explicitly:

$$h = j(\gamma_\alpha, \tau)^{-k}.$$

Then

$$\delta_k(f|_k\gamma_\alpha) = \delta_k(fh) = \delta_k f h + f\delta_0 h.$$

Exercise. Check that

$$\delta_k(f|_k\gamma) = (\delta_k f)|_{k+2}\gamma$$

(in general).

Therefore:

$$(\delta_k f)(\gamma_\alpha(\tau))j(\gamma_\alpha, \tau)^{-(k+2)} = (\delta_k f)(\tau)h(\tau) + (f\delta_0(h))(\tau).$$

By definition of γ_α:

$$(\delta_k f)(\tau) \cdot \alpha^{-(k+2)} = (\delta_k f)(\tau)\alpha^{-k} + (f \cdot \delta_0(h))(\tau).$$

Dividing by $g(z)$, we get that

$$\frac{\delta_k(f)(\tau) \cdot \alpha^{-k}(\alpha^{-2} - 1)}{g(z)} = \frac{(f \cdot \delta_0(h))(\tau)}{g(\tau)} \in \overline{\mathbb{Q}},$$

since

$$f \cdot \delta_0(h) \in \mathcal{A}_{k+2}(\overline{\mathbb{Q}}).$$

This settles the case $r = 1$. The general case follows by induction:

$$\delta^r(f|_k\gamma_\alpha) = \delta^r(fh) = \delta^r(f)h + \sum \delta^a(f)\delta^b(h) \cdot (\text{coefficient}) + \delta^r(h)$$

and

$$\delta^r(h) = \delta^{r-1}(\underbrace{\delta_0 h}_{\in \mathcal{A}_2(\overline{\mathbb{Q}})}).$$

Filling in the details of this step is left as an exercise. □

7.2. **Algebraicity of L-values.** We renormalize the infinity type of the character χ as follows:

$$\chi((\alpha)) = \alpha^{k+j}\overline{\alpha}^{-j} = \alpha^{k+2j}(\alpha\overline{\alpha})^j.$$

Then

$$\begin{aligned}
L(\chi^{-1},0) &= \sum_{(\alpha)} \frac{(\alpha\overline{\alpha})}{\alpha^{k+2j}} \\
&= w_K^{-1} \cdot \sum_{\alpha\in\mathcal{O}_K\setminus\{0\}} \frac{(\alpha\overline{\alpha})^j}{\alpha^{k+2j}} \\
&= w_K^{-1} \cdot \sum \frac{1}{(m+n\tau_0)^{k+2j}|m+n\tau_0|^{-2j}} \\
&\sim_{\overline{\mathbb{Q}}^\times} \widetilde{E_{k+2j}}(\tau_0,-j) \\
&\sim_{\overline{\mathbb{Q}}^\times} \delta^j\widetilde{E_k}(\tau_0)\pi^j && \text{by Corollary 7.8} \\
&\sim_{\overline{\mathbb{Q}}^\times} \pi^{j+k}E_k && \text{as } \widetilde{E_k}\sim\pi^k E_k \\
&\sim_{\overline{\mathbb{Q}}^\times} \pi^{j+k}g(\tau_0),
\end{aligned}$$

where g is any holomorphic modular form of weight $k+2j$ with algebraic coefficients that is non-zero at τ_0; it exists by Shimura's Theorem 7.10.

The elliptic curve $\mathbb{C}/\mathbb{Z}\tau_0+\mathbb{Z}$ has CM by K and is defined over $\overline{\mathbb{Q}}$. Pick any elliptic curve E over $\overline{\mathbb{Q}}$ with CM by K. Then the period lattice of E is

$$\Omega\cdot(\mathbb{Z}\tau'+\mathbb{Z})$$

for $\tau'\in K$, where for a non-vanishing differential $\omega\in H^0(E,\Omega^1)$ and a K-basis γ of $H_1(E,\mathbb{Q})\cong K$,

$$\Omega = \int_\gamma \omega \in \mathbb{C}^\times/\overline{\mathbb{Q}}^\times.$$

One can then easily show that

$$g(\tau_0) \sim_{\overline{\mathbb{Q}}^\times} \left(\frac{\Omega}{\pi}\right)^{k+2j}.$$

Finally, we have shown that

$$L(\chi^{-1},0) \sim \pi^{j+k}\left(\frac{\Omega}{\pi}\right)^{k+2j} \sim \pi^{-j}\Omega^{k+2j}.$$

Example 7.11. Let $K=\mathbb{Q}(i)$. For $j=0$, $k=4\ell$, one can pick the elliptic curve $y^2=1-x^4$ to obtain that

$$\sum_{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(mi+n)^{4\ell}} \sim_{\overline{\mathbb{Q}}^\times} \Omega^{4\ell}$$

for

$$\Omega = \int_0^1 \frac{dx}{\sqrt{1-x^4}}.$$

One can get a more precise rationality result, but one has to pick the elliptic curve more carefully.

Remark 7.12. So far, we need to assume that $k \geq 4$ to use the Eisenstein series $\widetilde{E_k}$. But, in fact, the result also holds for $k = 2$.

(1) We may defined $\widetilde{E_2}(z)$ by analytically continuing
$$\sum \frac{1}{(mz+n)^2|mz+n|^{2s}}$$
in s. In fact, if we let
$$E_2^\flat(z) = \frac{E_2(z)}{12} - \frac{1}{4\pi y},$$
which is a modular form of weight 2, which appeared in the proof of Proposition 7.4, then
$$\widetilde{E_2}(z) \sim \pi^2 E_2^\flat.$$
(2) At this point we cannot use $\delta^j E_2^\flat(z)$, because $E_2^\flat(z)$ is not holomorphic. We may, however, rewrite it as
$$E_2^\flat(z) = \frac{\delta(\Delta)}{\Delta}.$$

The details of this can be found in [Kat76].

7.3. ***p*-adic interpolation.** Recall that if $\chi((\alpha)) = \alpha^{k+j}\overline{\alpha}^{-j}$, then we have shown that
$$L(\chi^{-1}, 0) = (-4\pi y_0)^j \frac{\Gamma(k)}{\Gamma(k+j)} \delta^j \widetilde{E_k}(\tau_0)$$
where $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\tau$ for $\tau_0 \in \mathfrak{h}$ and $y_0 = \mathrm{Im}(\tau_0)$. Recall that
$$\widetilde{E_k} = 2\zeta(k)E_k = \frac{2(2\pi i)^k}{(k-1)!} G_k.$$
Supposing that K has odd discriminant $-D$, we have that
$$\tau_0 = \frac{1+\sqrt{-D}}{2}.$$
Then
$$L(\chi^{-1}, 0) = 2(2\pi i)^j \sqrt{D}^j \frac{\Gamma(k)}{\Gamma(k+j)} \frac{(2\pi i)^k}{\Gamma(k)} \delta^j G_k(\tau_0).$$
Recall that we fixed an isomorphism $(E, \omega) \cong (\mathbb{C}/\mathcal{O}_K, \Omega dz)$. Then
$$\left(\frac{2\pi i}{\Omega}\right)^{k+2j} \delta^j G_k(\tau_0) = \delta^j G_k(E, \omega) \in \overline{\mathbb{Q}}.$$

The value we will interpolate is hence
$$\frac{1}{2} \frac{(2\pi i)^j \Gamma(k+j) \sqrt{D}^{-j} L(\chi^{-1}, 0)}{\Omega^{k+2j}} = \delta^j G_k(E, \omega).$$
We will eventually get a 2-variable p-adic L-functions (after taking out an Euler factor at p), where we allow both j and k to vary. However, we will first let $j = 0$ and just let k vary.

When $j = 0$, the character is $\chi_k((\alpha)) = \alpha^k$. We assume that k is divisible by the number of roots of unity, as before. The weight space is $W = \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$.

Suppose $p = \mathfrak{p}\overline{\mathfrak{p}}$ is split in K. Recall that we have fixed embeddings

$$\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}, \quad \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}.$$

We normalize so that $\mathfrak{p}$ is the prime corresponding to this fixed embedding.

Theorem 7.13. *There is a continuous function*

$$\mathcal{L}_p \colon W \setminus \{0\} \to \mathbb{C}_p$$

such that

$$\mathcal{L}_p(k) = G_k(E, \omega) \cdot \left(1 - \frac{\chi_k(\mathfrak{p})}{p}\right)$$

for $k \geq 2$.

We only prove this for $k \geq 4$.

Remark 7.14. There is a more general statement for ramified characters, but we restrict to this simpler case.

The idea is to construct the function as follows

$$\begin{array}{ccc} W \setminus \{0\} & \longrightarrow & p\text{-adic modular forms} \\ & \searrow^{\mathcal{L}_p} & \downarrow \text{evaluate at } (E,\omega) \\ & & \mathbb{C}_p \end{array}$$

We first discuss evaluating p-adic modular forms. Fix some model for (E, ω) defined over the ring of integers of a number field with good reduction at p. View (E, ω) as defined over $R = \mathcal{O}_{\overline{\mathbb{Q}_p}}$.

The key point is that E has ordinary reduction at primes above p. This is because (by the theory of complex multiplication)

$$a_p = \xi + \overline{\xi}$$

where ξ is a generator of $\mathfrak{p}$. Therefore, p does not divide a_p.

If (E, ω) is defined over R and has ordinary reduction, we may define $f(E, \omega)$ for any p-adic modular form f. We write $f = \lim_i f_i$ for f_i of weight k_i such that $k_i \to \infty$. Then

$$f(E, \omega) = \lim_i f_i(E, \omega).$$

To check convergence, taking f_i and f_j, we know that $f_i \equiv f_j \ (p^m)$, so $k_i = k_j + rp^{m-1}(p-1)$, and hence

$$f_i E_{p-1}^{p^{m-1}r} \equiv f_j$$

as modular forms. This shows convergence.

If f is a usually modular form, want $f(E, \omega)$ to be the same as before. If we take

$$f \cdot E_{p-1}^{p^m} \to f$$

and then we easily check that the limit of the evaluations is the evaluation.

Finally, the other map is simple to define

$$W \setminus \{0\} \to p\text{-adic modular forms}$$
$$\kappa \mapsto G_\kappa^* = \frac{1}{2}\zeta^*(1-\kappa) + \sum_{n\geq 1} \sigma_{\kappa-1}^*(n)q^n.$$

In particular, we define

$$\mathcal{L}_p(\kappa) = G_\kappa^*(E,\omega).$$

Proof of Theorem 7.13. We just need to show that for $k \geq 4$,

$$G_k^*(E,\omega) = G_k(E,\omega)\cdot\left(1 - \frac{\chi_k(\mathfrak{p})}{p}\right).$$

Recall that

$$G_k^* = G_k - p^{k-1}G_k|V,$$

and $T_p = U + p^{k-1}V$. We hence need a modular interpretation of T_p, U, V. Recall that $E[p] \cong (\mathbb{Z}/p\mathbb{Z})^2$, and hence it has $(p+1)$ subgroup schemes of order p, $C_0, \dots, C_p$. If we define

$$\phi_i \colon E \to E_i = E/C_i$$

then for a modular form f of weight k:

$$(f|T_p)(E,\omega) = p^{k-1}\sum_i f(E_i, \phi_i^*(\omega)).$$

When (E,ω) is define over R and has ordinary reduction, there is a *canonical subgroup*, C_0. It is the kernel of the reduction modulo p map from $E[p]$.

Then the modular interpretation of V is

$$(f|V)(E,\omega) = f(E_0, \phi_0^*\omega).$$

One can check these identities using q-expansions.

Altogether, we see that

$$G_k^*(E,\omega) = G_k(E,\omega) - p^{k-1}(G_K|V)(E,\omega).$$

The map

$$E \to E/C_0$$

corresponds to

$$\mathbb{C}/\mathcal{O}_K \to \mathbb{C}/\mathfrak{p}^{-1}\mathcal{O}_K.$$

The dual isogeny is multiplication by p, so the differential dz pulls back to pdz. Altogether, if

$$(E,\omega) \cong (\mathbb{C}/\mathcal{O}_K, \Omega dz),$$

then

$$(E_0, \phi_0^*\omega) \cong (\mathbb{C}/\mathfrak{p}^{-1}\mathcal{O}_K, \Omega p dz).$$

Multiplication by ξ, where $\mathfrak{p} = (\xi)$, gives a further isomorphism

$$(\mathbb{C}/\mathfrak{p}^{-1}\mathcal{O}_K, \Omega p dz) \cong \left(\mathbb{C}/\mathcal{O}_K, \frac{\Omega p}{\xi}dz\right).$$

Altogether, this shows that

$$G_k^*(E,\omega) = G_k(E,\omega)(1-p^{k-1}\overline{\xi}^{-k}).$$

Finally,

$$\left(1-\frac{\chi_k(\mathfrak{p})}{p}\right) = 1-\xi^k p^{-1} = 1-p^{k-1}(\overline{\xi})^{-k}.$$

This completes the proof. □

We would like to define the two variable p-adic L-function as

$$\theta^j G_k^*(E,\omega).$$

However, when we differentiate the q-expansion of G_k^*, we get

$$\sum_{n=1}^{\infty} n\sigma_{k-1}^*(n)q^{n-1}$$

so the n do not interpolate p-adically well when $p|n$. Therefore, we will get rid of q^n for $p|n$. Recall that

$$\sum a_n q^n \overset{U}{\mapsto} \sum a_{np}q^n,$$

$$\sum a_n q^n \overset{V}{\mapsto} \sum a_n q^{np}.$$

Then

$$f|VU = f,$$
$$f|UV = \sum a_{np}q^{np}.$$

Then

$$f|_k(VU-UV) = f|_k(I-(T_p-p^{k-1}V)V) = f|_k(I-T_pV+p^{k-1}V^2)$$

is the *p-deprived* version of f. Define

$$G_k^{**} = G_k|_k(I-T_pV+p^{k-1}V^2) = G_k|(I-(1+p^{k-1})V+p^{k-1}V^2) = \sum_{(p,n)=1}\sigma_{k-1}(n)q^n.$$

Then we define a function as above

$$\begin{array}{ccc} W\times W & \longrightarrow & p\text{-adic modular forms} \\ & \searrow & \downarrow \\ & & \mathbb{C}_p \end{array}$$

with the vertical map sending (k,j) to

$$\theta^j G_k^{**} = \sum_{\substack{n\geq 1\\(p,n)=1}} n^j\sigma_{k-1}^*(n)q^n.$$

We have that:

$$\begin{aligned}
\theta^j G_k^{**}(E,\omega) &= \theta^j(G_k|(I-(1+p^{k-1})V+p^{k-1}V^2))(E,\omega)\\
&= (\theta^j G_k)|(I-(1+p^{k-1})p^jV+p^{k-1+2j}V^2)(E,\omega)\\
&= \theta^j G_k(E,\omega)\left(1-\frac{(1+p^{k-1})p^j}{\overline{\xi}^{k+2j}}+p^{k-1+2j}\frac{1}{\overline{\xi}^{2k+4j}}\right) && \text{by the proof of Theorem 7.13}\\
&= \theta^j G_k(E,\omega)\left(1-\frac{p^{k-1}p^j}{\overline{\xi}^{k+2j}}\right)\left(1-\frac{p^j}{\overline{\xi}^{k+2j}}\right)\\
&= \theta^j G_k(E,\omega)(1-\xi^{k+j-1}\overline{\xi}^{-j-1})(1-\xi^j\overline{\xi}^{-k-j}) && \text{as } p=\xi\overline{\xi}\\
&= \theta^j G_k(E,\omega)\left(1-\frac{\chi(\mathfrak{p})}{p}\right)\left(1-\chi^{-1}(\overline{\mathfrak{p}})\right) && \chi_k(\mathfrak{p})=\xi^{k+j}\overline{\xi}^j
\end{aligned}$$

Remark 7.15. Note that the factor

$$\left(1-\frac{\chi(\mathfrak{p})}{p}\right)$$

is not an Euler factor. However,

$$(1-\chi^{-1}(\overline{\mathfrak{p}}))$$

is the Euler factor of $L(\chi^{-1},0)$ at $\overline{\mathfrak{p}}$.

Theorem 7.16 (Katz)**.** *We have that*

$$\delta^j G_k(E,\omega)=\theta^j G_k(E,\omega).$$

More generally, if $f\in M_k$ and (E,ω) is an ordinary CM point, then

$$\delta^j f(E,\omega)=\theta^j f(E,\omega)$$

Sketch of proof. Suppose $j=1$. Recall that

$$\begin{aligned}
\delta &= \theta-\frac{k}{4\pi y},\\
\partial &= 12\theta-kP,\\
\theta &= \frac{1}{12}\partial+\frac{kP}{12},\\
\delta &= \frac{1}{12}\partial+\frac{kP}{12}-\frac{k}{4\pi y}.
\end{aligned}$$

We therefore just need to show that the p-adic modular form P of weight 2 is equal to the C^∞ modular form $S=P-\frac{3}{\pi y}$ of weight 2 at ordinary CM points.

Then for $j=1$, proving the theorem reduces to checking that $P(E,\omega)=S(E,\omega)$ for ordinary CM points.

Suppose E/L has good reduction at primes above $\mathfrak{p}$, where L/K is a finite extension. We have the short exact sequence

$$0 \longrightarrow H^0(E, \Omega^1_E) \longrightarrow H^1_{\mathrm{dR}}(E) \longrightarrow H^1(E, \mathcal{O}_E) \longrightarrow 0$$

Then

$$H^1_{\mathrm{dR}}(E/L) = L \cdot \omega + L \cdot \eta$$

where ω is a basis of $H^0(E, \Omega^1_E)$ and η is the dual basis of $H^1(E, \mathcal{O}_E)$. Note that (ω, η) is a symplectic basis for H^1_{dR}, i.e. $\langle \omega, \eta \rangle_{\mathrm{dR}} = 1$.

If E is given by the equation $y^2 = x^3 + ax + b$, then we can write

$$\omega = \frac{dx}{y}, \quad \eta = \frac{xdx}{y}.$$

Note that we have a Hodge decomposition:

$$H^1_{\mathrm{dR}}(E/\mathbb{C}) = H^{1,0} \oplus H^{0,1}.$$

Here ω generates $H^{1,0}$ and $\overline{\omega}$ generates $H^{0,1}$. We may hence write

$$\overline{\omega} = a\omega + b\eta, \qquad \text{with } b \neq 0.$$

We then define the *slope* to be $\frac{a}{b}$.

Exercise. $S(E, \omega) = \frac{a}{b}$.

For the p-adic side, note that we have a Frobenius action on

$$H^1_{\mathrm{dR}}(E/L) \otimes L_{\mathfrak{P}},$$

where the prime $\mathfrak{P}$ is induced by the fixed embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$.

Since E is ordinary, one eigenvalue of the Froebnius is a p-adic unit and the other is not. Let u be the eigenvector with unit eigenvalue. Then

$$u = a'\omega + b'\eta$$

and the slope is

$$\frac{a'}{b'}.$$

Fact. $P(E, \omega) = \frac{a'}{b'}$. This requires some computations with the Tate curves.

Now, for an ordinary elliptic curve with complex multiplciation $i \colon K \to \mathrm{End}_L(E)$, we have that

$$H^1_{\mathrm{dR}} = L\omega + L\omega'$$

with $i(\alpha)\omega = \alpha\omega$ and $i(\alpha)\omega' = \overline{\alpha}\omega'$.

Fact. Then

$$\overline{\omega} \in \mathbb{C}\omega',$$
$$u \in L_{\mathfrak{P}}\omega'.$$

The details of the proof can be found in [Kat76]. □

We have hence constructed the 2-variable p-adic L-function for χ with infinity type $(k+j, -j)$ and $k \geq 2$ and $j \geq 0$. Working with higher level modular forms, one can get $k \geq 1$. Altogether, this gives the following theorem.

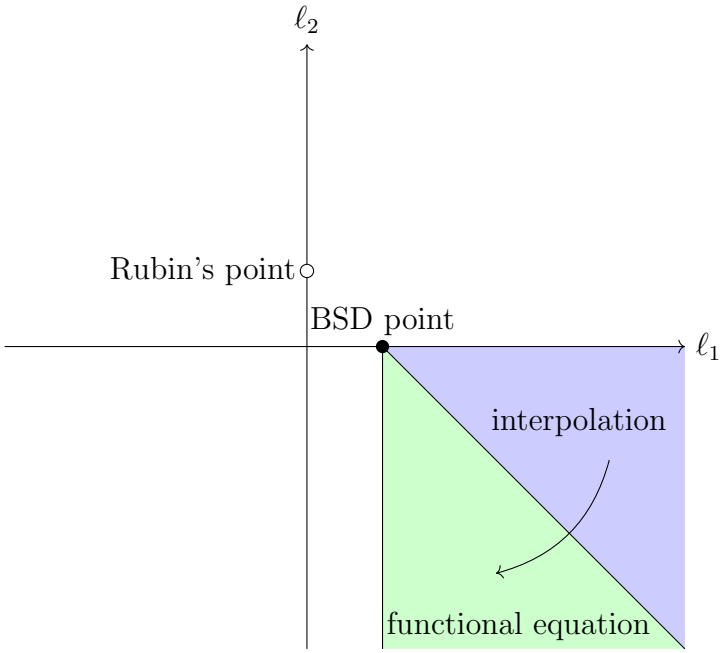
Theorem 7.17. *Fix some conductor $\mathfrak{f}$ (ideal in $\mathcal{O}_K$). Consider the extension $K(\mathfrak{f}\mathfrak{p}^\infty)$ of K and write $\mathcal{G}$ for the Galois group. Then there exists a measure $d\mu$ on $\mathcal{G}$ such that for $k \geq 1$ and $j \geq 0$:*

$$\frac{1}{\Omega_p^{k+2j}} \int \chi d\mu = \frac{\left(1 - \frac{\chi(\mathfrak{p})}{p}\right) L_{\mathfrak{f}\overline{\mathfrak{p}}}(\chi^{-1}, 0)}{\Omega^{k+2j}} \left(\frac{2\pi}{\sqrt{d}}\right)^j \mathfrak{g}_\chi,$$

where Ω_p is some p-adic period.

Let us write $(\ell_1, \ell_2) = (k+j, -j)$. We do not want to restrict to the case $k \geq 2$, because the point $(\ell_1, \ell_2) = (1, 0)$ is relevant to the Birch–Swinnerton-Dyer conjecture.

Since $k \geq 1$ and $j \geq 0$, $\ell_1 \geq 1$, $\ell_2 \leq 0$, and $\ell_1 + \ell_2 \geq 1$. Then the functional equation gives a similar interpolation property for points with $\ell_1 + \ell_2 \leq 1$.



The blue region is the interpolation region. The green region is the region where the functional equation gives the interpolation. Rubin's point refers to Theorem 7.19 below.

Example 7.18 (A grossencharacter of type $(1,0)$)**.** Consider $K = \mathbb{Q}(\sqrt{-7})$ and note that $j(\mathcal{O}_K) \in \mathbb{Q}$. We have that

$$(\mathcal{O}_K/(\sqrt{-7}))^\times \cong (\mathbb{Z}/7\mathbb{Z})^\times \xrightarrow{\epsilon} \{\pm 1\}$$

with $\epsilon(-1) = -1$. One can the define a Hecke character ψ by

$$\psi((\alpha)) = \alpha \cdot \epsilon(\alpha), \quad \text{for } \alpha \text{ prime to } 7.$$

The corresponding elliptic curve E has conductor 49. Moreover,

$$L(E, s) = L(\psi, s) = L(\overline{\psi}, s)$$

by the theory of complex multiplication. Then

$$\mathcal{L}_p(\psi) = L(E, 1)(*).$$

Therefore, to study $L(E,1)$ (which is the goal of the Birch–Swinnerton-Dyer conjecture), the p-adic L-function is useful.

Theorem 7.19 (Rubin [Rub92])**.** *Let $E/\mathbb{Q}$ be an elliptic curve with CM by K and let $\psi\colon \mathbb{A}_K^\times \to \mathbb{C}^\times$ be the associated Hecke character. Suppose the sign of $L(E,s)$ is equal to -1 and suppose $L(E,s)$ vanishes to order one at $s=1$. (In that case, the theorem of Gross–Zagier and Kolyvagin implies that $E(\mathbb{Q})$ has rank one.) Suppose $E(\mathbb{Q})\otimes\mathbb{Q} = \mathbb{Q}\cdot P$ (so Q is a Heegner point). Then*

$$\mathcal{L}_p(\psi^*) \doteq \log_p(P)^2,$$

where ψ^* is ψ composed with complex conjugation,

$$\log_p\colon E(\mathbb{Q}_p) \to \mathbb{Q}_p$$

is the formal group logarithm, and $\doteq$ means 'up to explicit constants'.

Remark 7.20. Note that $\mathcal{L}_p(\psi) \doteq L(E,1) = 0$. This is why we look at ψ^* instead of ψ. However, ψ^* has infinity type $(0,1)$ which is outside of the range of interpolation.

This should, therefore, be though of as an analog of Leopoldt's formula 3.17 which evaluates the Kubota–Leopoldt p-adic L-function outside of the range of interpolation.

An alternative proof of this theorem without the assumption that K is CM was given in [BDP12], [BDP13]. We will discuss this next.

8. p-adic L-function for Rankin–Selberg L-function

Let f, g be two modular forms on $\mathrm{SL}_2(\mathbb{Z})$ with weights k, ℓ, respectively.

Assume f, g are cusp forms and eigenfunctions for all the Hecke operators T_p. Write

$$f = \sum a_n q^n, \quad g = \sum b_n q^n$$

and normalize them so that $a_1 = 1$, $b_1 = 1$. Then

$$L(s,f) = \sum \frac{a_n}{n^s} = \prod_p \frac{1}{(1 - a_p p^{-s} + p^{k-1-2s})} = \prod_p \frac{1}{(1-\alpha_p p^{-s})(1-\alpha_p' p^{-s})}.$$

Here, α_p and α_p' are two roots of Frob_p acting on the Galois representation $\rho_{f,\ell}$ associated to f. For g, we have a similar equation with β_p and β_p'.

It is well known that $L(s,f)$, $L(s,g)$ admit analytic continuation and functional equation.

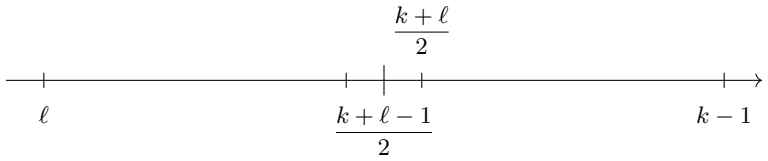
We will be interested in the Rankin–Selberg L-functions associated to f and g:

$$L(s, f\times g) = \prod_p \frac{1}{(1-\alpha_p\beta_p p^{-s})(1-\alpha_p\beta_p' p^{-s})(1-\alpha_p'\beta_p p^{-s})(1-\alpha_p'\beta_p')}.$$

Note that

$$L(s, f\times g) = L(s, \rho_f \otimes \rho_g).$$

We assume that $k > \ell$ and $k \equiv 2$ (2). The center of the functional equation is $s = \frac{k+\ell-1}{2}$. The critical points are:



We will be interested in the critical points to the right of the center.

Consider the Dirichlet series:

$$D(s,f,g)=\sum\frac{a_nb_n}{n^s}.$$

Proposition 8.1. *We have that*

$$D(s,f,g)=\frac{L(s,f\times g)}{\zeta(2s+2-k-\ell)}.$$

Proof. We have that

$$\begin{aligned}D(s,f,g)&=\sum a_nb_nn^{-s}\\&=\prod_p\sum_n a_{p^n}b_{p^n}(p^n)^{-s}\end{aligned}$$

Note that

$$\begin{aligned}a_{p^n}&=\frac{\alpha_p^{n+1}-(\alpha_p')^{n+1}}{\alpha_p-\alpha_p'},\\b_{p^n}&=\frac{\beta_p^{n+1}-(\beta_p')^{n+1}}{\beta_p-\beta_p'}.\end{aligned}$$

Therefore, the Euler factor at p is:

$$\begin{aligned}&\sum_n\frac{\alpha_p^{n+1}-(\alpha_p')^{n+1}}{\alpha_p-\alpha_p'}\frac{\beta_p^{n+1}-(\beta_p')^{n+1}}{\beta_p-\beta_p'}(p^{-s})^n\\&=\frac{\sum_n(\alpha_p\beta_p)(\alpha_p\beta_pp^{-s})^n-(\alpha'\beta_p)(\alpha_p'\beta_pp^{-s})^n-(\alpha_p\beta_p')(\alpha_p\beta_p'p^{-s})^n+(\alpha_p'\beta_p'p^{-s})^n(\alpha_p'\beta_p')}{(\alpha_p-\alpha_p')(\beta_p-\beta_p')}\\&=\frac{1}{(\alpha_p-\alpha_p')(\beta_p-\beta_p')}\left[\frac{\alpha_p\beta_p}{1-\alpha_p\beta_p}-\frac{\alpha_p'\beta_p}{1-\alpha_p'\beta_pp^{-s}}-\frac{\alpha_p\beta_p'}{1-\alpha_p\beta_p'p^{-s}}+\frac{\alpha_p'\beta_p'}{1-\alpha_p'\beta_p'p^{-s}}\right]\\&=\frac{1-\alpha_p\alpha_p'\beta_p\beta_p'p^{-2s}}{(1-\alpha_p\beta_p)\dots(1-\alpha_p'\beta_p')}\end{aligned}$$

Therefore, the Euler factors at p agree for all p. □

8.1. **Algebraicity of critical values.** We follow [Shi76b] to prove algebraicity of critical values of the Rankin–Selberg convolution of two cusp forms f and g.

Definition 8.2. Let $f_\rho(z)=\overline{f(-\overline{z})}=\sum_{n=0}^{\infty}\overline{a_n}e^{2\pi inz}$.

Note that

$$\int_0^1 \overline{f_\rho(z)} g(z) dx = \int_0^1 \left(\sum_{n=1}^\infty a_n e^{-2\pi n y} e^{-2\pi i n x} \right) \left(\sum_{n=1}^\infty b_n e^{2\pi n y} e^{2\pi i n x} \right) dx$$
$$= \sum_{n=1}^\infty a_n b_n e^{-4\pi n y}.$$

Therefore,

$$\int_0^\infty y^{s-1} \int_0^1 \overline{f_\rho(z)} g(z) dx dy = \int_0^\infty y^{s-1} \sum_{n=1}^\infty a_n b_n e^{-4\pi n y} dy = (4\pi)^{-s} \Gamma(s) D(s, f, g)$$

for $\mathrm{Re}(s) \gg 0$. The left hand side is equal to

$$\int_S \overline{f_\rho(z)} g(z) y^{s+1} \frac{dx dy}{y^2}$$

where $S = \{z = x + iy \mid 0 \leq 0 \leq 1,\ y > 0\}$. For each

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}).$$

Note that

$$\overline{f_\rho(z)} g(z) y^{s+1} \circ \gamma = (cz + d)^k (cz + d)^\ell |cz + d|^{-2s-2}$$
$$= (cz + d)^{\ell - k} |cz + d|^{2k - 2s - 2}.$$

To make the integrand invariant under Γ, we need to multiply by something. Note that the integrand is already invariant under $x \mapsto x + 1$. Let R be a set of representatives for $\Gamma_\infty \backslash \mathrm{SL}_2(\mathbb{Z})$, where

$$\Gamma_\infty = \left\{ \pm \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \;\middle|\; m \in \mathbb{Z} \right\}.$$

Then let

$$E_\lambda(z, s) = \sum_{r \in R} \frac{1}{(cz + d)^\lambda |cz + d|^{2s}}.$$

Note that

$$\Gamma_\infty \backslash \mathrm{SL}_2(\mathbb{Z}) \cong \{(c, d) \in \mathbb{Z}^2 \mid (c, d) = 1\} / \pm 1.$$

Exercise. Check that

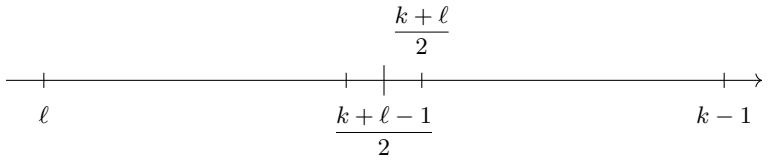
$$\widetilde{E_\lambda}(z, s) = 2\zeta(2s + \lambda) E_\lambda(z, s),$$

where the left hand side is the real analytic Eisenstein series from Section 7.1.

Altogether, we have that

$$(4\pi)^{-s} \Gamma(s) D(s, f, g) = \int_{\mathrm{SL}_2(\mathbb{Z}) \backslash \mathfrak{h}} \overline{f_\rho(z)} g(z) y^{s+1} E_{k-\ell}(z, s + 1 - k) \frac{dx dy}{y^2}.$$

Recall that the critical points were given by the following picture



and we were interested in studying the points to the right of the center, i.e.

$$D(k-1-r,f,g) \quad \text{for } 0 \leq r \leq \frac{k-\ell}{2}-1.$$

According to the above formula:

$$(4\pi)^{-(k-1-r)}\Gamma(k-1-r)D(k-1-r,f,g) = \int\limits_{\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{h}} \overline{f_\rho} g E_{k-\ell}(z,-r) y^{s-1} dxdy.$$

Now, similarly as for $\widetilde{E}$, we have that

$$\delta^r E_\lambda(z) = \left(-\frac{1}{4\pi y}\right)^r \frac{\Gamma(\lambda+r)}{\Gamma(\lambda)} E_{\lambda+2r}(z,-r).$$

Here, we want to take $\lambda = k-\ell-2r$, to get

$$D(k-1-r,f,g) = (4\pi)^{k-1}\frac{\Gamma(k-\ell-2r)\cdot(-1)^r}{\Gamma(k-\ell-r)\Gamma(k-1-r)} \int\limits_{\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{h}} \overline{f_\rho} g \delta^r E_{k-\ell-2r}(z) y^k \frac{dxdy}{y^2}$$

Definition 8.3. If $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ and ϕ, ψ are modular forms of weight k for Γ, then the *Petersson inner product* is defined as

$$\langle \phi, \psi \rangle = \frac{1}{\mathrm{vol}(\Gamma\backslash\mathfrak{h})} \int_{\Gamma\backslash\mathfrak{h}} \overline{\phi} \cdot \psi \cdot y^k \frac{dxdy}{y^2}.$$

Write

$$C = \frac{4^{k-1}}{3}\frac{\Gamma(k-\ell-2r)}{\Gamma(k-\ell-r)\Gamma(k-1-r)}(-1)^r.$$

Altogether, we conclude that:

$$D(k-1-r,f,g) = C \cdot \pi^k \cdot \langle f_\rho, g \cdot \delta^r E_{k-\ell-2r} \rangle.$$

Remark 8.4. Note that the $s = k$ i.e. the rightmost point ($r = k$), is the easiest point to study. Indeed, in the case we just have a holomorphic Eisenstein series.

We first deal with the case $r = 0$. We have that

$$D(k-1,f,g) = C \cdot \pi^k \langle f_\rho, g E_{k-\ell} \rangle.$$

Here, $G = g \cdot E_{k-\ell}$ is a holomotphic modular form of weight k, defined over $\overline{\mathbb{Q}}$.

Theorem 8.5 (Shimura)**.** *For* $0 \leq r \leq \frac{k-\ell}{2} - 1$,

$$\frac{\pi^{-k} D(k-1-r, f, g)}{\langle f, f \rangle}$$

is algebraic.

Proof of Theorem 8.5, $r = 0$. Take an orthonormal basis for $S_k(\Gamma)$ where the first vector is f_ρ and all other elements in this basis are defined over $\overline{\mathbb{Q}}$. Then

$$G = \alpha \cdot f_\rho + H$$

where H is orthogonal to f_ρ. Then

$$\langle f_\rho, G \rangle = \alpha \langle f_\rho, f_\rho \rangle = \alpha \langle f, f \rangle.$$

However, $\alpha \in \overline{\mathbb{Q}}$, because both f and G are defined over $\overline{\mathbb{Q}}$. □

To prove the general case, we need the following theorem. Recall that $N_k^r(\Gamma)$ is the space of nearly holomorphic modular forms of weight k such that the polynomial in $\frac{1}{y}$ is degree at most r.

Theorem 8.6. *Let $h \in N_k^t(\Gamma)$ and suppose $k > 2r$. Then*

$$h = \sum_{\nu=0}^{r} \delta^\nu h_\nu, \quad h_\nu \in M_{k-2\nu}.$$

Moreover, this decomposition is unique.

Note that the condition $k > 2r$ is necessary: indeed, the form E_2 has $k = 2$, $r = 1$, but there are no modular forms of lower level.

Proof. Write

$$h = g_0 + y^{-1} g_1 + \cdots + y^{-r} g_r.$$

Note that

$$y^{-1}(\gamma(z)) = \frac{|cz+d|^2}{y} = \frac{(cz+d)(c\overline{z}+d)}{y} = \frac{(cz+d)(cz+d+c(\overline{z}-z))}{y} = \frac{(cz+d)^2}{y} - 2ic(cz+d).$$

Therefore:

$$\begin{aligned} h(z) &= h(\gamma(z))(cz+d)^{-k} \\ &= (cz+d)^{-k} \left[g_0(\gamma(z)) + y_1^{-1} g_1(\gamma(z)) + \cdots + y^{-1}(\gamma(z))^r g_r(\gamma(z)) \right] \end{aligned}$$

so the coefficient of y^{-r} in this expression is

$$g_r(\gamma(z))(cz+d)^{2r-k}.$$

Since the expression above is unique, this shows that

$$g_r(\gamma(z))(cz+d)^{2r-k} = g_r(z),$$

so g_r is a modular form of weight $k - 2r$. As long as $k > 2r$, there is a constant C such that

$$h - C \cdot \delta^r g_r \in N_k^{r-1}(\Gamma),$$

because

$$\delta = \frac{1}{2\pi i}\left[\frac{d}{dz} + \frac{\text{weight}}{2iy}\right].$$

This completes the proof by induction. **Exercise.** Check uniqueness. □

Recall that we showed that

$$(4\pi)^{-s}\Gamma(s)D(s,f,g) = \int_{\Gamma\backslash\mathfrak{h}} \overline{f_\rho(z)}g(z)y^{s+1}E_{k-\ell}(z,s+1-k)\frac{dxdy}{y^2}$$

for $k > \ell$. In fact, this still holds for $k = \ell$, where $E_0(z,s)$ is defined by analytic continuation.

Fact 8.7. *The Eisenstein series $E_0(z,s)$ is holomorphic in s for $\mathrm{Re}(s) > 1$ and has a simple pole at $s = 1$ with residue $\frac{3}{\pi y}$.*

Therefore:

$$(4\pi)^{-k}\Gamma(k)\,\mathrm{Res}_{s=k}\,D(s,f,g) = \int_{\Gamma\backslash\mathfrak{h}} \overline{f_\rho(z)}g(z)\frac{3}{\pi y}y^{k-1}dxdy = \langle f_\rho, g\rangle.$$

Note that this is just $0 = 0$ when f_ρ is in a different isotypic component than g. The interesting case is hence $g = f_\rho$. Rewriting this in that case, we get

$$\begin{aligned}\langle f, f\rangle &= (4\pi)^{-k}\Gamma(k)\,\mathrm{Res}_{s=k}\,D(s,f,f_\rho)\\ &= \frac{(4\pi)^{-k}\Gamma(k)}{\zeta(2)}\,\mathrm{Res}_{s=k}\,L(s,f\times f_\rho).\end{aligned}$$

If f had Hecke eigenvalues α and β, then f_ρ has Hecke eigenvalues $\overline{\alpha}$, $\overline{\beta}$. If f has Nebentypus ϵ, then

$$\begin{aligned}\alpha\cdot\overline{\alpha} &= p^{k-1},\\ \alpha\cdot\beta &= \epsilon(p)p^{k-1},\\ \overline{\alpha} &= \beta\cdot\overline{\epsilon(p)},\\ \overline{\beta} &= \alpha\cdot\overline{\epsilon(p)}.\end{aligned}$$

Computing the pairwise products, we get:

$$(\alpha^2\overline{\epsilon(p)}, \alpha\beta\overline{\epsilon(p)}, \alpha\beta\overline{\epsilon(p)}, \beta^2\overline{\epsilon(p)}).$$

By the above, $\alpha\beta\overline{\epsilon(p)} = p^{k-1}$. Now, note that

$$\prod\left(1 - \frac{p^{k-1}}{p^s}\right)^{-1} = \zeta(s-k+1).$$

Using the formula

$$L(s,f\times f_\rho) = D(s,f,g)\zeta(2s-2k+2).$$

Now, we also get a factorization

$$L(s,f\times f_\rho) = L(s,\mathrm{adj}^0 f)\zeta(s-k+1)\zeta(2s-2k+2).$$

This finally shows that

$$(4)\qquad (4\pi)^k\Gamma(k)^{-1}\langle f,f\rangle = \mathrm{Res}_{s=k}\,L(s,f\times f_\rho) = L(\text{twist on } \mathrm{sym}^2 f, k) = L(\mathrm{adj}^0 f, 1),$$

because the ζ factor has no pole at $s = k$.

This is the representation comes up in Wiles' paper proving modularity.

Proposition 8.8. *If $f \in S_k$, $g \in S_\ell$, $k = \ell + 2r$, then*

$$\langle f, \delta^r g \rangle = 0.$$

Proof. If $g(z) = \sum_{n=0}^{\infty} b_n e^{2\pi i n z}$, then

$$\begin{aligned}\delta^r g &= (2\pi i)^{-r} \sum_{\nu=0}^{r} c_\nu (2iy)^{\nu-r} \left(\frac{d}{dz}\right)^\nu g \\ &= \sum_{\nu=0}^{r} (-4\pi y)^{\nu-r} c_\nu \sum_{n=0}^{\infty} b_n n^\nu e^{2\pi i n z}.\end{aligned}$$

As in section 8.1, we can easily show that:

$$\int_0^\infty y^{s-1} \int_0^1 \overline{f_\rho} \delta^r g \, dx dy = (4\pi)^{-s} D(s-r, f, g) \sum_{\nu=0}^{r} (-1)^{\nu-r} c_\nu \Gamma(s+\nu-r).$$

Moreover, the left hand side is

$$\int_{\Gamma \backslash \mathfrak{h}} \overline{f_\rho} \delta^r g E_0(z, s+1-k) y^{s-1} dx dy.$$

The residue of this as $s = k$ is

$$\langle \overline{f_\rho}, \delta^r g \rangle.$$

The residue of the right hand side above is 0, which completes the proof. □

Exercise. Use Theorem 8.6 together with Proposition 8.8 to complete the proof of Theorem 8.5.

8.2. ***p*-adic interpolation.** Let f be a modular form of weight k, K be an imaginary quadratic field, and χ be a Hecke character of K of infinity type $(\ell, 0)$.

Consider the L-function $L(s, f_K \times \chi)$. For example, if f corresponds to an elliptic curve E, then base change E to K and twist the Galois representation by χ. We may it as the Rankin–Selberg L-function as

$$L(s, f \times \theta_\chi)$$

where

$$\theta_\chi = \sum_{\mathfrak{a}} \chi(\mathfrak{a}) e^{2\pi i (N\mathfrak{a}) z} \in S_{\ell+1}.$$

Recall that the period that makes this algebraic depends on which weight is dominant. Therefore, we have the following dichotomy.

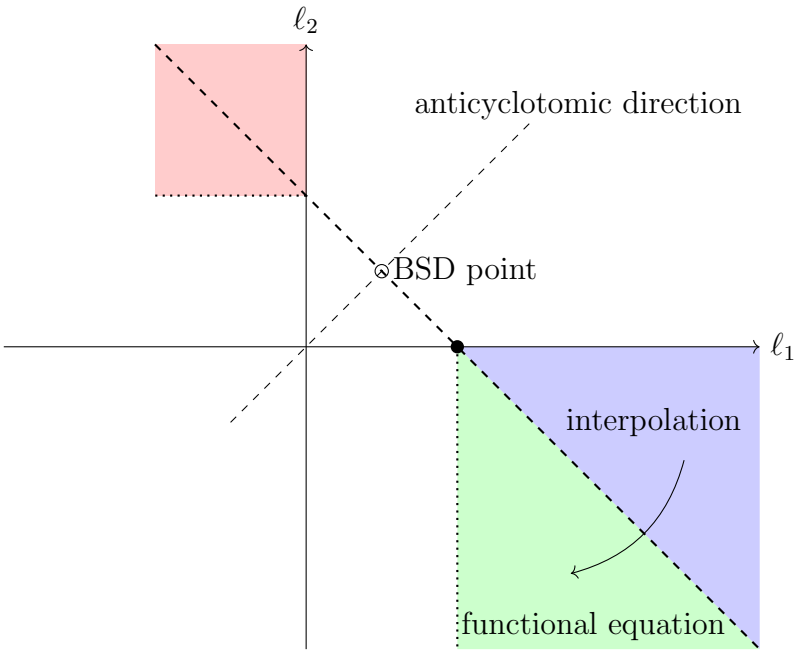
- When $k > \ell$, the period is $\pi^{(*)} \langle f, f \rangle$.

- When $k \leq \ell$, the period is $\pi\langle\theta_\chi, \theta_\chi\rangle$. Taking the residue at $s = \ell + 1$, we get that

$$\begin{aligned}\langle\theta_\chi, \theta_\chi\rangle &\sim \pi^{(*)} \operatorname{Res}_{s=\ell+1} \frac{L(\chi, \overline{\chi^\rho}, s)\zeta_K(s-\ell)}{\zeta_{\mathbb{Q}}(2s-2\ell)} && \text{by equation (4)} \\ &= \pi^{(*)} \frac{1}{\zeta(2)} L(\epsilon_K, 1) L(\chi\overline{\chi^\rho}, \ell+1) && \text{as } \zeta_K(s) = \zeta_{\mathbb{Q}}(s)L(s, \epsilon_K) \\ &\sim \pi^{(*')}\Omega^{(*)},\end{aligned}$$

  where Ω is the CM period.

Suppose f corresponds to an elliptic curve E. We have the following diagram for the p-adic L-function interpolating $L(f, \chi^{-1}, 0)$, according to the weight for χ:



The dashed line $\ell_2 = 2 - \ell_1$ is the line of symmetry, which is also the *cyclotomic direction*. The other dashed line $\ell_2 = \ell_1$ is the *anticyclotomic direction*.
The blue region is the interpolation region. The green region is the region where the functional equation gives the interpolation. The BSD point is the point relevant to the three formulas below. The red region is where evaluating the p-adic L-function should give interesting arithmetic information, but we currently do not know anything about.

We have three formulas:

(1) Gross–Zagier [GZ86]: $L'(E, 1) \doteq \langle P_K, P_K\rangle$,
(2) Perrin-Riou [PR87]: $\mathcal{L}_p^1(N) \doteq L(E, 1) = 0$; then $(\mathcal{L}_p^1)' = \langle P_K, P_K\rangle_{p\text{-adic height}}$, where the p-adic L-function is in the *cyclotomic direction*,
(3) Bertolini–Darmon–Prasanna [BDP13]: $(\mathcal{L}_p^2)'(\mathbb{N}) \doteq \log_p^2(P_K)$, where p-adic L-function is in the *anticyclotomic direction*.

Appendix A. Project topics

(1) Herbrand–Ribet Theorem. The goal of this project is to work through the proofs of Herbrand's theorem (see, for example, [Was97]) and Ribet's converse to Herbrand theorem [Rib76b].
(2) Gross's paper [Gro80] on factorization of p-adic L-functions of imaginary quadratic fields.
(3) Deligne–Ribet's paper [DR80] on p-adic L-functions of totally real number fields.
(4) Gekeler's paper [Gek88] on Drinfeld modular forms (i.e. the function field case).

References

[BDP12] Massimo Bertolini, Henri Darmon, and Kartik Prasanna, *p-adic Rankin L-series and rational points on CM elliptic curves*, Pacific J. Math. **260** (2012), no. 2, 261–303, doi:10.2140/pjm.2012.260.261, https://doi.org/10.2140/pjm.2012.260.261. MR 3001796

[BDP13] ———, *Generalized Heegner cycles and p-adic Rankin L-series*, Duke Math. J. **162** (2013), no. 6, 1033–1148, With an appendix by Brian Conrad, doi:10.1215/00127094-2142056, https://doi.org/10.1215/00127094-2142056. MR 3053566

[Del79] P. Deligne, *Valeurs de fonctions L et périodes d'intégrales*, Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 1979, With an appendix by N. Koblitz and A. Ogus, pp. 313–346. MR 546622

[DR80] Pierre Deligne and Kenneth A. Ribet, *Values of abelian L-functions at negative integers over totally real fields*, Invent. Math. **59** (1980), no. 3, 227–286, doi:10.1007/BF01453237, https://doi.org/10.1007/BF01453237. MR 579702

[Gek88] Ernst-Ulrich Gekeler, *On the coefficients of Drinfeld modular forms*, Invent. Math. **93** (1988), no. 3, 667–700, doi:10.1007/BF01410204, https://doi.org/10.1007/BF01410204. MR 952287

[Gro80] Benedict H. Gross, *On the factorization of p-adic L-series*, Invent. Math. **57** (1980), no. 1, 83–95, doi:10.1007/BF01389819, https://doi.org/10.1007/BF01389819. MR 564185

[GZ86] Benedict H. Gross and Don B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320, doi:10.1007/BF01388809, https://doi-org.proxy.lib.umich.edu/10.1007/BF01388809. MR 833192

[Har77] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York-Heidelberg, 1977, Graduate Texts in Mathematics, No. 52. MR 0463157

[Iwa72] Kenkichi Iwasawa, *Lectures on p-adic L-functions*, Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1972, Annals of Mathematics Studies, No. 74. MR 0360526

[Kat73] Nicholas M. Katz, *p-adic properties of modular schemes and modular forms*, 69–190. Lecture Notes in Mathematics, Vol. 350. MR 0447119

[Kat76] ———, *p-adic interpolation of real analytic Eisenstein series*, Ann. of Math. (2) **104** (1976), no. 3, 459–571, doi:10.2307/1970966, https://doi.org/10.2307/1970966. MR 0506271

[Kim10] Minhyong Kim, *An introduction to motives i: classical motives and motivic l-functions*, http://people.maths.ox.ac.uk/kimm/papers/ihes3.pdf.

[KZ98] M. Kaneko and D. Zagier, *Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials*, Computational perspectives on number theory (Chicago, IL, 1995), AMS/IP Stud. Adv. Math., vol. 7, Amer. Math. Soc., Providence, RI, 1998, pp. 97–126. MR 1486833

[Lan90] Serge Lang, *Cyclotomic fields I and II*, second ed., Graduate Texts in Mathematics, vol. 121, Springer-Verlag, New York, 1990, With an appendix by Karl Rubin, doi:10.1007/978-1-4612-0987-4, https://doi.org/10.1007/978-1-4612-0987-4. MR 1029028

[Lan94] ———, *Algebraic number theory*, second ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994, doi:10.1007/978-1-4612-0853-2, https://doi.org/10.1007/978-1-4612-0853-2. MR 1282723

[Mil13] James S. Milne, *Motives—Grothendieck's dream*, Open problems and surveys of contemporary mathematics, Surv. Mod. Math., vol. 6, Int. Press, Somerville, MA, 2013, pp. 325–342. MR 3204952

[Miy06] Toshitsune Miyake, *Modular forms*, english ed., Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2006, Translated from the 1976 Japanese original by Yoshitaka Maeda. MR 2194815

[MW84] B. Mazur and A. Wiles, *Class fields of abelian extensions of* **Q**, Invent. Math. **76** (1984), no. 2, 179–330, doi:10.1007/BF01388599, https://doi.org/10.1007/BF01388599. MR 742853

[PR87] Bernadette Perrin-Riou, *Points de Heegner et dérivées de fonctions L p-adiques*, Invent. Math. **89** (1987), no. 3, 455–510, doi:10.1007/BF01388982, https://doi-org.proxy.lib.umich.edu/10.1007/BF01388982. MR 903381

[Rib76a] Kenneth A. Ribet, *A modular construction of unramified p-extensions ofQ*(μ_p), Invent. Math. **34** (1976), no. 3, 151–162, doi:10.1007/BF01403065, https://doi.org/10.1007/BF01403065. MR 0419403

[Rib76b] ———, *A modular construction of unramified p-extensions ofQ*(μ_p), Invent. Math. **34** (1976), no. 3, 151–162, doi:10.1007/BF01403065, https://doi.org/10.1007/BF01403065. MR 0419403

[Rub92] Karl Rubin, *p-adic L-functions and rational points on elliptic curves with complex multiplication*, Invent. Math. **107** (1992), no. 2, 323–350, doi:10.1007/BF01231893, https://doi.org/10.1007/BF01231893. MR 1144427

[SD73] H. P. F. Swinnerton-Dyer, *On l-adic representations and congruences for coefficients of modular forms*, 1–55. Lecture Notes in Math., Vol. 350. MR 0406931

[Ser73a] J.-P. Serre, *A course in arithmetic*, Springer-Verlag, New York-Heidelberg, 1973, Translated from the French, Graduate Texts in Mathematics, No. 7. MR 0344216

[Ser73b] Jean-Pierre Serre, *Formes modulaires et fonctions zêta p-adiques*, 191–268. Lecture Notes in Math., Vol. 350. MR 0404145

[Shi76a] Goro Shimura, *The special values of the zeta functions associated with cusp forms*, Comm. Pure Appl. Math. **29** (1976), no. 6, 783–804, doi:10.1002/cpa.3160290618, https://doi-org.proxy.lib.umich.edu/10.1002/cpa.3160290618. MR 0434962

[Shi76b] ———, *The special values of the zeta functions associated with cusp forms*, Comm. Pure Appl. Math. **29** (1976), no. 6, 783–804, doi:10.1002/cpa.3160290618, https://doi.org/10.1002/cpa.3160290618. MR 0434962

[Shi94] ———, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, Princeton, NJ, 1994, Reprint of the 1971 original, Kanô Memorial Lectures, 1. MR 1291394

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009, doi:10.1007/978-0-387-09494-6, https://doi-org.proxy.lib.umich.edu/10.1007/978-0-387-09494-6. MR 2514094

[Was97] Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997, doi:10.1007/978-1-4612-1934-7, https://doi.org/10.1007/978-1-4612-1934-7. MR 1421575