TOPICS IN NUMBER THEORY: SPECIAL VALUES OF L-FUNCTIONS

FALL 2024

This is the lecture notes for a topic course in number theory, on the special values of L-functions, taught in Fall 2024. Each lecture is two hours long. We also include some exercises, with solutions at the end of the lecture notes.

Contents

1. Introduction and special values of Dirichlet L-functions

1.1. Dirichlet L-functions and their special values.

Definition 1.1.1. The *Riemann zeta function* is defined by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}} \qquad (\mathrm{Re}(s) > 1)$$

Fact 1.1.2. The following is known regarding the algebraicity of the special values of zeta-function.

- (Euler) $\zeta(2) = \frac{\pi^2}{6}$, $\zeta(4) = \frac{\pi^4}{90}$, $\dots$, $\zeta(2n) \in \mathbb{Q}^\times \cdot \pi^{2n}$ for any $n \in \mathbb{Z}_{\geq 1}$.
- (Apéry 1978) $\zeta(3)$ is irrational.[1]

Conjecture 1.1.3. *The numbers* $1, \pi, \zeta(3), \zeta(5), \zeta(7), \dots$ *are algebraically independent, i.e. if* $P(x, \underline{y}) \in \mathbb{Q}[x, y_3, y_5, y_7, \dots]$ *is a polynomial such that* $P(\pi, \zeta(3), \zeta(5), \zeta(7), \dots) = 0$, *then* $P \equiv 0$.

The irrationality and transcendence question of zeta values is a very important and difficult question in number theory. But we will not discuss this too much in this course.

Definition 1.1.4. Fix $N \in \mathbb{Z}_{>0}$, a character $\eta : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ is called a *Dirichlet character of order* N. It is called *primitive* if it does not factors through $(\mathbb{Z}/M\mathbb{Z})^\times$ for any $M|N$.

For an Dirichlet character $\eta : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$, define the *Dirichlet L-function* to be

$$L(\eta, s) = \sum_{(n,N)=1} \frac{\eta(n)}{n^s} = \prod_{\substack{p \text{ prime} \\ p \nmid N}} \frac{1}{1-\eta(p)p^{-s}}, \qquad (\mathrm{Re}(s) > 1).$$

Question 1.1.5. What are the special values of $L(\eta, s)$?

Example 1.1.6. Consider $\eta : (\mathbb{Z}/4\mathbb{Z})^\times \to \mathbb{C}^\times$ given by $\eta(-1) = -1$.

$$L(\eta, 1) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \cdots = \arctan 1 = \frac{\pi}{4}.$$

Example 1.1.7. Consider $\eta : (\mathbb{Z}/8\mathbb{Z})^\times \to \mathbb{C}^\times$ given by $\eta(3) = \eta(5) = -1$ and $\eta(-1) = \eta(3)\eta(5) = 1$. We want to compute

$$L(\eta, 1) = 1 - \frac{1}{3} - \frac{1}{5} + \frac{1}{7} + \frac{1}{9} - \frac{1}{11} - \frac{1}{13} + \frac{1}{15} + \cdots$$

The following approach is somewhat elementary. Consider the power series

$$f(x) = x - \frac{1}{3}x^3 - \frac{1}{5}x^5 + \frac{1}{7}x^7 + \frac{1}{9}x^9 - \frac{1}{11}x^{11} - \frac{1}{13}x^{13} + \frac{1}{15}x^{15} + \cdots$$

Then $f'(x) = 1 - x^2 - x^4 + x^6 + x^8 - \cdots = \dfrac{1 - x^2 - x^4 + x^6}{1 - x^8}$.

[1] Following the work of Apéry, there have been some further developments, such as Zudilin proved that at least one of $\zeta(3)$, $\zeta(5)$, $\zeta(7)$, and $\zeta(9)$ is irrational.

(Using some computer software), we can show that

$$f(x) = \int \frac{1 - x^2 - x^4 + x^6}{1 - x^8} dx = \frac{\sqrt{2}}{4}\Big(\ln\left|x^2 + \sqrt{2}x + 1\right| + \ln\left|x^2 - \sqrt{2}x + 1\right|\Big).$$

This alternating series converges at $x = 1$; so we may evaluate at $x = 1$ to see

$$L(\eta, 1) = f(1) = \frac{\sqrt{2}}{4} \ln\left(\frac{2 + \sqrt{2}}{2 - \sqrt{2}}\right) = \frac{\sqrt{2}}{2} \ln\left(\sqrt{2} + 1\right).$$

Remark 1.1.8. The number $\sqrt{2} + 1$ is the fundamental unit in $\mathbb{Z}[\sqrt{2}]$, and the factor $\sqrt{2}$ is related to $\sqrt{d_{\mathbb{Q}(\sqrt{2})}}$, for the discriminant of $\mathbb{Q}(\sqrt{2})$.

We have already seen that the two examples above give very distinct answers. The distinction is the value of $\eta(-1) \in \{\pm 1\}$.

Notation 1.1.9. We say a Dirichlet character $\eta : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ is

- *even* if $\eta(-1) = 1$;
- *odd* if $\eta(-1) = -1$.

The following known results provide a good understanding of the algebraicity of special values of Dirichlet L-functions.

Theorem 1.1.10. *We have the following.*

(1) *If η is even, for $m \in \mathbb{Z}_{\geq 1}$, we have*

$$L(\eta, 2m) \in \overline{\mathbb{Q}}^\times \cdot \pi^{2m}.$$

(2) *If η is odd, for $m \in \mathbb{Z}_{\geq 1}$, we have*

$$L(\eta, 2m - 1) \in \overline{\mathbb{Q}}^\times \cdot \pi^{2m-1}.$$

Theorem 1.1.11. *If $\eta : (\mathbb{Z}/N\mathbb{Z})^\times \to \{\pm 1\}$ is a primitive quadratic character such that $\eta(-1) = 1$, then $\tilde{\eta} : (\mathbb{Z}/N\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \xrightarrow{\eta} \{\pm 1\}$ corresponds to a* real *quadratic field F. We have*

$$L(\eta, 1) \in \mathbb{Q}^\times \cdot \sqrt{d_F} \cdot \ln|u_F|,$$

where d_F is the discriminant of F and $u_F \in \mathcal{O}_F^\times$ is a fundamental unit.

Remark 1.1.12. (1) The element -1 in $(\mathbb{Z}/N\mathbb{Z})^\times$ corresponds to the complex conjugation in $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$; so the subfield of $\mathbb{Q}(\zeta_N)$ defined by the kernel of $\eta : (\mathbb{Z}/N\mathbb{Z})^\times \to \{\pm 1\}$ is a *real* quadratic field.

(2) The theme of this course is to explain the philosophy behind the above two algebraicity results, and possible generalizations. These two theorems are of very different nature. Theorem 1.1.10 regarding powers of π is related to "periods" and will be discussed in the general framework of *Deligne's conjecture*. Theorem 1.1.11 relates the L-values with the regulator of a fundamental unit and will be discussed in the general framework of *Beilinson's conjecture*.

1.2. Functional equations of Dirichlet L-functions.

Definition 1.2.1. Let $\eta : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a primitive character of conductor N. We define the local L-factors as follows.

$$L_p(\eta, s) = \begin{cases} 1 & \text{if } p \mid N; \\ \frac{1}{1-\eta(p)p^{-s}} & \text{if } p \nmid N. \end{cases}$$

Then we have

$$L(\eta, s) = \prod_{p \text{ prime}} L_p(\eta, s).$$

For the purpose of functional equations, we put

$$L_\infty(\eta, s) := \begin{cases} \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2}) & \text{if } \eta(-1) = 1, \\ \pi^{-\frac{s+1}{2}}\Gamma(\frac{s+1}{2}) & \text{if } \eta(-1) = -1. \end{cases}$$

Here $\Gamma(s) = \displaystyle\int_0^\infty e^{-t}t^s \cdot \frac{dt}{t}$ is the usual Gamma function. (Note that $\frac{dt}{t}$ is a Haar measure of $\mathbb{R}^\times_{>0}$.)

We may then define the *complete Dirichlet L-function* to be

$$\Lambda(\eta, s) = L(\eta, s) \cdot L_\infty(\eta, s).$$

Notation 1.2.2. It is more convenient to put $\Gamma_{\mathbb{R}}(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})$.

$$\delta = \begin{cases} 0 & \text{if } \eta(-1) = 1 \\ 1 & \text{if } \eta(-1) = -1 \end{cases} \qquad \rightsquigarrow \qquad \eta(-1) = (-1)^\delta.$$

In the above definition, we have $L_\infty(\eta, s) = \Gamma_{\mathbb{R}}(s + \delta)$.

Theorem 1.2.3. *Every Dirichlet L-function $L(\eta, s)$ admits an* holomorphic *extension to $s \in \mathbb{C}$ (except when $\eta = \mathbf{1}$, $\zeta(s)$ has a simple pole at $s = 1$), and a functional equation*

$$\Lambda(\eta, s) = \varepsilon(\eta, s) \cdot \Lambda(\eta^{-1}, 1 - s).$$

where $\varepsilon(\eta, s) = G(\eta) \cdot N^{-s}/i^\delta$ with $G(\eta) = \sum_{a=1}^{N-1} \eta(a)e^{2\pi i \cdot a/N}$ being the Gauss sum.

The goal of this lecture is to prove the algebraicity Theorem 1.1.10 assuming the functional equation in Theorem 1.2.3.

1.3. Special values of Dirichlet L-functions at nonpositive integers.

Notation-Proposition 1.3.1. Recall that the Gamma function is defined to be

$$\Gamma(s) := \int_0^\infty e^{-t}t^s \cdot \frac{dt}{t} \qquad\qquad (\mathrm{Re}(s) > 1)$$

(1) For any s such that $\mathrm{Re}(s) > 1$, we have $\Gamma(s + 1) = s\Gamma(s)$. This gives rise to a meromorphic continuation of $\Gamma(s)$ with a simple pole at each of $s \in \mathbb{Z}_{\leq 0}$.
(2) For $n \in \mathbb{Z}_{\geq 1}$, we have $\Gamma(n) = (n - 1)!$.
(3) $\Gamma(\frac{1}{2}) = \sqrt{\pi}$. Applying (1), we have for $m \in \mathbb{Z}_{\geq 1}$

$$\begin{aligned} \Gamma(m + \tfrac{1}{2}) &= (m - \tfrac{1}{2})(m - \tfrac{3}{2}) \cdots \tfrac{1}{2} \cdot \sqrt{\pi} \in \mathbb{Q}^\times \cdot \sqrt{\pi}, \\ \Gamma(-m + \tfrac{1}{2}) &= (-m + \tfrac{1}{2})^{-1}(-m + \tfrac{3}{2})^{-1} \cdots (-\tfrac{1}{2})^{-1} \cdot \sqrt{\pi} \in \mathbb{Q}^\times \cdot \sqrt{\pi}. \end{aligned}$$

(4) The Gamma function $\Gamma(s)$ has no zeros.

1.3.2. *Apply this to Dirichlet L-functions.* We note that

$$\int_0^\infty e^{-nt}t^s \cdot \frac{dt}{t} = n^{-s} \cdot \Gamma(s).$$

Now, for a Dirichlet character $\eta : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$, we have (setting $\eta(n) = 0$ if $(n, N) \neq 1$)

$$\begin{aligned}\Gamma(s)L(\eta, s) &= \Gamma(s) \sum_{\substack{n\geq 1 \\ (n,N)=1}} \frac{\eta(n)}{n^s} = \int_0^\infty \sum_{\substack{n\geq 1 \\ (n,N)=1}} \eta(n)e^{-nt}t^s \cdot \frac{dt}{t} \\ &= \int_0^\infty \frac{\sum_{n=1}^N \eta(n)e^{-nt}}{1-e^{-Nt}} \cdot t^s \frac{dt}{t}.\end{aligned}$$

Thus, if we put[2]

$$f_\eta(t) := \frac{\sum_{n=1}^N \eta(n)e^{-nt}}{1-e^{-Nt}}, \tag{1.3.2.1}$$

then

$$L(\eta, s) = \frac{1}{\Gamma(s)} \int_0^\infty f_\eta(t)t^s \cdot \frac{dt}{t}.$$

Remark 1.3.3. Here the situation is a bit strange. For functional equations, one needs to multiply the L-function by the archimedean L-factor which is roughly $\Gamma(\frac{s}{2})$, but to reach the values at negative integers, one needs to multiply the L-function by $\Gamma(s)$.

The following is a key technical lemma, which we copied from Colmez's lectures at Tsinghua University [Col].

Lemma 1.3.4. *For a smooth function $f(t) \in C^\infty([0, \infty))$ (e.g. $t \cdot f_\eta$ above) that is* rapidly decreasing as $t \to +\infty$, *i.e.*

$$t^n \partial_t^m(f)(t) \to 0 \textit{ as } t \to +\infty \quad \textit{for any } m, n \in \mathbb{Z}_{\geq 0},$$

the function

$$L(f, s) := \frac{1}{\Gamma(s)} \int_0^\infty f(t)t^s \frac{dt}{t} \qquad (\mathrm{Re}(s) > 1)$$

has an analytic continuation to $s \in \mathbb{C}$, and

$$L(f, -n) = (-1)^n f^{(n)}(0) \qquad \textit{for any } n \in \mathbb{Z}_{\geq 0}.$$

Proof. We use integration by parts, viewing $f(t)t^{s-1}$ as $f(t) \cdot (\frac{t^s}{s})'$. So

$$L(f, s) = \frac{1}{\Gamma(s)} \left(f(t) \frac{t^s}{s} \right) \Bigg|_0^{+\infty} - \frac{1}{s\Gamma(s)} \int_0^{+\infty} f'(t)t^s \cdot dt.$$

[2]When $\eta = \mathbf{1}$, $f_{\mathbf{1}}(t) = \frac{e^{-t}}{1-e^{-t}}$.

Note that the first term tends to 0 as $t \to 0$ because $f(t)$ is continuous at $t = 0$, and it also gives zero when $t \to +\infty$ as $f(t)$ is rapidly decreasing. So we deduce that

$$L(f, s) = -\frac{1}{s\Gamma(s)} \int_0^{+\infty} f'(t)t^s \cdot dt = -\frac{1}{\Gamma(s+1)} \int_0^{+\infty} f'(t)t^{s+1} \cdot \frac{dt}{t} = -L(f', s+1).$$

By induction, this gives the analytic continuation of $L(f, s)$ to the entire $s \in \mathbb{C}$. $\square$

1.4. **Algebraicity of Dirichlet L-values.** For a primitive Dirichlet character η of conductor N, if we write

$$f_\eta(t) := \frac{\sum_{n=1}^{N} \eta(n)e^{-nt}}{1 - e^{-Nt}}$$

as in (1.3.2.1), and apply Lemma 1.3.4 to $t \cdot f_\eta$ we get[3]

$$L(\eta, -s) = \frac{1}{\Gamma(s)} \int_0^{\infty} f_\eta(t)t^s \frac{dt}{t} = \frac{1}{(s-1)\Gamma(s-1)} \int_0^{\infty} t f_\eta(t)t^{s-1} \frac{dt}{t} = \frac{L(tf_\eta, s-1)}{s-1}.$$

Proposition 1.4.1. *We have the following formula.*

$$L(\eta, -n) = \frac{L(tf_\eta, -n-1)}{-n-1} = -\frac{(-1)^{n+1}}{n+1}(tf_\eta)^{(n+1)}. \tag{1.4.1.1}$$

In particular, we have

$$L(\eta, -n) \in \mathbb{Q}(\eta) \qquad \textit{for } n \in \mathbb{Z}_{\geq 0}.$$

We may carefully study the function $f_\eta(t)$ to show that certain $L(\eta, -n)$ are zero depending on the parity of n.

Lemma 1.4.2. *We have the following.*

1. *When $\eta(-1) = 1$, f_η is an odd function, so $L(\eta, -n) = (-1)^{n+1}(tf_\eta)^{(n+1)} = 0$ when $n \geq 0$ is even (except when $\eta = \mathbf{1}$, $\zeta(0) = -\frac{1}{2}$).*
2. *When $\eta(-1) = -1$, f_η is an even function, so $L(\eta, -n) = (-1)^{n+1}(tf_\eta)^{(n+1)} = 0$ when $n \geq 1$ is odd.*

Proof. When $N \neq 1$, recall that we have assumed that $\eta(-1) = (-1)^\delta$ for $\delta \in \{0, 1\}$. Then we have

$$f_\eta(-t) = \frac{\sum_{n=1}^{N-1} \eta(n)e^{nt}}{1 - e^{Nt}} = \frac{e^{Nt} \cdot \sum_{n=1}^{N-1} \eta(n)e^{(n-N)t}}{e^{Nt} \cdot (e^{-Nt} - 1)}$$

$$\overset{m=N-n}{=} \frac{\eta(-1) \cdot \sum_{m=1}^{N-1} \eta(m)e^{-mt}}{-(1 - e^{-Nt})} = -\eta(-1)f_\eta(t).$$

This proves both (1) and (2).

[3] When $\eta \neq \mathbf{1}$, we may apply instead Lemma 1.3.4 to f_η directly because f_η is then a C^∞-function on $[0, +\infty)$ (note that the constant term of the sum $\sum_{n=1}^{N-1} \eta(n)e^{nt}$ is zero), but $f_{\mathbf{1}}(t)$ has a pole at $t = 0$; so we need to consider $tf_{\mathbf{1}}$ instead.

When $N = 1$ and $\eta = \mathbf{1}$, recall that $f_{\mathbf{1}}(t) = \dfrac{e^{-t}}{1-e^{-t}} = \dfrac{1}{e^t - 1}$ and we have

$$f_{\mathbf{1}}(-t) = \frac{1}{e^{-t}-1} = \frac{-e^t}{e^t-1} = -1 - f_{\mathbf{1}}(t).$$

This proves (1) when $n \geq 2$. When $n = 0$, we may compute directly that $f_{\mathbf{1}}(t) = \frac{1}{t} - \frac{1}{2} + \cdots$ and thus $\zeta(0) = -1/2$. □

1.4.3. *Compatibility of Lemma 1.4.2 with functional equations.* We explain Lemma 1.4.2 in terms of the functional equation of Dirichlet L-functions. We first write out the functional equation from Theorem 1.2.3 (recall $\eta(-1) = (-1)^\delta$):

$$\pi^{-\frac{s+\delta}{2}}\Gamma\Big(\frac{s+\delta}{2}\Big) \cdot L(\eta, s) = \epsilon(\eta, s) \cdot L(\eta^{-1}, 1-s) \cdot \pi^{-\frac{1-s+\delta}{2}}\Gamma\Big(\frac{1-s+\delta}{2}\Big).$$

Reorganizing terms, we have

$$\Gamma\Big(\frac{s+\delta}{2}\Big) \cdot L(\eta, s) = \frac{G(\eta)\cdot N^{-s}}{i^\delta} \cdot L(\eta^{-1}, 1-s) \cdot \pi^{s-\frac{1}{2}}\Gamma\Big(\frac{1-s+\delta}{2}\Big). \tag{1.4.3.1}$$

Take $s = -n$ with $n \in \mathbb{Z}_{\geq 0}$ in the above equation, we get

$$\underbrace{\Gamma\Big(\frac{-n+\delta}{2}\Big)}_{\text{pole if } n\equiv\delta \bmod 2} \cdot L(\eta, -n) = \frac{G(\eta)\cdot N^{n}}{i^\delta} \cdot \underbrace{L(\eta^{-1}, 1+n)}_{\neq 0,\text{ unless } \eta=\mathbf{1}, s=0} \cdot \underbrace{\pi^{-n-\frac{1}{2}}\Gamma\Big(\frac{1+n+\delta}{2}\Big)}_{\text{no poles or zeros}}.$$

By comparing both sides, we see that $L(\eta, -n)$ must be zero when $n \equiv \delta \bmod 2$ (except the case when $\eta = \mathbf{1}$ and $s = 0$, in which case, the pole of $\zeta(s)$ at $s = 1$ implies that $\zeta(0) \in \mathbb{Q}^\times$).

Lemma 1.4.4. *When $n \in \mathbb{Z}_{\geq 1}$ and $n \equiv \delta \bmod 2$ (except for the case $\eta = \mathbf{1}$ and $n = 1$), we have*

$$L(\eta, n) \in \mathbb{Q}_{\mathrm{cyc}}^\times \cdot \pi^n,$$

where $\mathbb{Q}_{\mathrm{cyc}}$ is the cyclotomic extension of $\mathbb{Q}$, i.e. $\mathbb{Q}(\zeta_n; n \in \mathbb{Z}_{\geq 1})$.

Proof. Apply $s = n$ with $n \in \mathbb{Z}_{\geq 1}$ and $n \equiv \delta \bmod 2$ to the equality (1.4.3.1), we get

$$\underbrace{\Gamma\Big(\frac{n+\delta}{2}\Big)}_{\text{in } \mathbb{Q}^\times} \cdot L(\eta, n) = \underbrace{\frac{G(\eta)\cdot N^{-n}}{i^\delta}}_{\text{belongs to } \mathbb{Q}_{\mathrm{cyc}}} \cdot \underbrace{L(\eta^{-1}, 1-n)}_{\text{in } \mathbb{Q}(\eta)} \cdot \pi^{n-\frac{1}{2}} \underbrace{\Gamma\Big(\frac{1-n+\delta}{2}\Big)}_{\text{in } \mathbb{Q}^\times\sqrt{\pi}}. \tag{1.4.4.1}$$

It then follows that $L(\eta, n) \in \mathbb{Q}_{\mathrm{cyc}} \cdot \pi^n$ (note that the Gauss sum $G(\eta)$ belongs to $\mathbb{Q}_{\mathrm{cyc}}$). Finally, as $L(\eta, n)$ admits a convergent product formula, $L(\eta, n) \neq 0$. □

Let $\mathbb{Q}^{\mathrm{alg}}$ denote the algebraic closure of $\mathbb{Q}$ inside $\mathbb{C}$. Then the Galois group $\mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/\mathbb{Q})$ acts on the set of Dirichlet characters $\eta : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{Q}^{\mathrm{alg},\times} \subseteq \mathbb{C}^\times$: for $\sigma \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/\mathbb{Q})$, it sends η to $\sigma \circ \eta$. It is then nature to compare $L(\eta, n)$ with $L(\sigma \circ \eta, n)$. We have the following.

Proposition 1.4.5. *Let $\eta : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{Q}^{\mathrm{alg},\times}$ be a primitive Dirichlet character of conductor $N > 1$.*

(1) *For $\sigma \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/\mathbb{Q})$,*

$$L(\sigma \circ \eta, -n) = \sigma(L(\eta, -n)) \quad \textit{when } n \in \mathbb{Z}_{\geq 0}.$$

(2) *When* $n \in \mathbb{Z}_{\geq 1}$ *and* $n \equiv \delta \bmod 2$*, if* $\sigma \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/\mathbb{Q}(\zeta_N))$*, we have*

$$\frac{L(\sigma \circ \eta, n)}{(2\pi i)^n} = \sigma\left(\frac{L(\eta, n)}{(2\pi i)^n}\right). \tag{1.4.5.1}$$

Proof. (1) is clear from Proposition 1.4.1.

For (2), we use the functional equation when $s = n$ with $n \equiv \delta \bmod 2$, or rather (1.4.4.1) to get

$$L(\eta, n) \in \frac{G(\eta)}{i^\delta} \cdot L(\eta^{-1}, 1-n) \cdot \pi^n \cdot \mathbb{Q}^\times.$$

Equivalently, we have (using $n \equiv \delta \bmod 2$)

$$\frac{L(\eta, n)}{(2\pi i)^n} \in G(\eta) \cdot L(\eta^{-1}, 1-n) \cdot \mathbb{Q}^\times.$$

Comparing with (1), we need only to prove that $\sigma(G(\eta)) = G(\sigma \circ \eta)$ for $\sigma \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/\mathbb{Q}(\zeta_N))$. But this is clear from the definition of Gauss sum. $\square$

Remark 1.4.6.
(1) In (2), it is "important" to divide the L-values by $(2\pi i)^n$ (as opposed to π^n), as it is the corresponding period. We will get to this point later in this course.
(2) For Proposition 1.4.5, it seems that the equality (1.4.5.1) does not hold for general $\sigma \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/\mathbb{Q})$, going back to the proof of Proposition 1.4.5, it is the Gauss sum $G(\eta)$ does not satisfy the relation $G(\sigma \circ \eta) = \sigma(G(\eta))$ for a general element $\sigma \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/\mathbb{Q})$. We cannot offer a better explanation at this stage.

1.5. **Exercises.**

Exercise 1.5.1 (Gauss sums)**.** Let $\eta : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a Dirichlet character of order $N \geq 2$, we define the Gauss sum of η as follows:

$$G(\eta) := \sum_{a=1}^{N-1} \eta(a) e^{2\pi i \cdot a/N} \in \mathbb{C}. \tag{1.5.1.1}$$

Prove the following properties of the Gauss sum.

(1) If η' is a Dirichlet character of order N' with $(N, N') = 1$, then $\eta\eta'$ may be viewed as a Dirichlet character of order NN'. Show that in this case $G(\eta\eta') = \eta(N')\eta'(N)G(\eta)G(\eta')$.
(2) If η is primitive, then $|G(\eta)| = \sqrt{N}$.
(3) When η and η' are both Dirichlet characters of same order N such that $\eta\eta'$ is a primitive Dirichlet character of order N, show that

$$G(\eta\eta') = \frac{G(\eta)G(\eta')}{J(\eta, \eta')}, \tag{1.5.1.2}$$

where $J(\eta, \eta')$ is the Jacobi sum

$$J(\eta, \eta') := \sum_{a \in \mathbb{Z}/N\mathbb{Z}} \eta(a)\eta'(1-a),$$

where we use the convention that $\eta(a) = 0$ if $(a, N) \neq 1$.

Remark 1.5.2. It would be interesting to compare Gauss sums with the Gamma functions. In some sense, the definition of (1.5.1.1) may be viewed as an integral of the product of an additive character $e^{2\pi i(\cdot)/N}$ of $\mathbb{Z}/N\mathbb{Z}$ and a multiplicative character η of $(\mathbb{Z}/N\mathbb{Z})^{\times}$. Similarly, the definition of Gamma function

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

can also be viewed as an integral of the product of the additive character e^{-t} and the multiplicative character t^s.

Analogous to the relation (1.5.1.2) between Gauss sum and the (finite) Jacobi sum, Gamma functions satisfy a similar property:

$$B(s, s') = \frac{\Gamma(s)\Gamma(s')}{\Gamma(s+s')},$$

where $B(s, s')$ is a beta function

$$B(s, s') = \int_0^1 t^{s-1}(1-t)^{s'-1} dt.$$

2.1. **Introduction to Kummer congruences.** In the previous lecture, we have determined the special values of Dirichlet L-functions, first up to $\overline{\mathbb{Q}}^\times$, and then up to $\mathbb{Q}^\times$ (by considering equivariant properties under $\mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/\mathbb{Q})$-action. In this lecture, we start to understand special values of Dirichlet L-functions in terms of congruences of the points of evaluation.

Notation 2.1.1. Recall that for a primitive Dirichlet character $\eta : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{Q}^{\mathrm{alg},\times}$ of conductor N, we introduced

$$tf_\eta(t) = \frac{t \cdot \sum_{n=1}^{N} \eta(n)e^{-nt}}{1 - e^{-Nt}} = \sum_{n \geq 0} B_{n,\eta} \frac{t^n}{n!},$$

where we have expanded the function into a Taylor expansion at $t = 0$. This polynomial is called the *η-Bernoulli polynomial*.

Notation 2.1.2. For the rest of this lecture series, we will fix an embedding $\iota_p : \mathbb{Q}^{\mathrm{alg}} \hookrightarrow \overline{\mathbb{Q}}_p$ (an algebraic closure of $\mathbb{Q}_p$). This amounts to fix a p-adic place of $\mathbb{Q}^{\mathrm{alg}}$, and all of our result will depend crucially on this choice.

In some literature, the authors are "lazy", and typically write "choose an isomorphism $\mathbb{C} \simeq \overline{\mathbb{Q}}_p$", but if one looks into the argument and construction, typically, the result only makes use of the embedding $\mathbb{Q}^{\mathrm{alg}} \hookrightarrow \overline{\mathbb{Q}}_p$ but not really the entire isomorphism $\mathbb{C} \simeq \overline{\mathbb{Q}}_p$.

The Kummer congruence is the following result. (In fact, Kummer only considered the case when $\eta = \mathbf{1}$.)

Theorem 2.1.3. *Let η be a primitive Dirichlet character of conductor N. Assume that $p \nmid N$. Let $k \in \mathbb{Z}_{\geq 1}$ and let integers $n_1, n_2 \geq k$ be such that $n_1 \equiv n_2 \bmod (p-1)p^{k-1}$ and that $p - 1 \nmid n_1$ when $\eta = \mathbf{1}$. Then we have*

$$L(\eta, -n_1) = -\frac{B_{n_1,\eta}}{n_1} \equiv -\frac{B_{n_2,\eta}}{n_2} = L(\eta, -n_2) \bmod p^k.$$

The purpose of this and the next lecture is to prove this theorem by constructing a p-adic L-function associated to the Dirichlet L-functions.

2.2. **Overview of the concept of p-adic L-functions.** Before giving any construction, we need to discuss the following

Question 2.2.1. What is a p-adic L-function?

2.2.2. *p-adic L-function, version I: p-adic interpolation.* It is natural to decompose a general Dirichlet character into the product $\eta\eta_p$ with

$$\eta : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{Q}^{\mathrm{alg},\times} \quad \text{and} \quad \eta_p : (\mathbb{Z}/p^r\mathbb{Z})^\times \to \mathbb{Q}^{\mathrm{alg},\times},$$

where $p \nmid N$ and we allow η_p to be trivial or nontrivial. We call η the *tame character* and η_p the p-part of the character.

We will fix the tame character η for the rest of the discussion.

Then a p-adic L-function may be viewed as a "function" that interpolates all

$$L(\eta \cdot \eta_p, -n)$$

for a **fixed** "tame" primitive Dirichlet character η and for **all** Dirichlet characters η_p at p and **all** $n \in \mathbb{Z}_{\geq 1}$, where we want n to vary p-adically.

2.2.3. *p-adic L-function, version II: interpretation via Galois representations.* The next step to give a more conceptual understanding of the Dirichlet character in terms of Galois representations. Given a Dirichlet character of conductor N, we have the following p-adic representation:

$$\tilde{\eta} : \mathrm{Gal}_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^{\times} \xrightarrow{\eta} \mathbb{Q}^{\mathrm{alg},\times} \xrightarrow{\iota_p} \overline{\mathbb{Q}}_p^{\times}. \tag{2.2.3.1}$$

We will learn in a few lectures about a general recipe to construct L-functions associated to a representation of the Galois group of $\mathbb{Q}$, and then the L-function associated to $\tilde{\eta}$ is precisely the Dirichlet L-function $L(\eta, s)$.

In terms of § 2.2.2, we may separate the tame part and the p-adic part:

$$\tilde{\eta} : \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^{\times} \xrightarrow{\eta} \overline{\mathbb{Q}}_p^{\times} \quad \text{and} \quad \tilde{\eta}_p : \mathrm{Gal}(\mathbb{Q}(\mu_{p^r})/\mathbb{Q}) \cong (\mathbb{Z}/p^r\mathbb{Z})^{\times} \to \overline{\mathbb{Q}}_p^{\times}.$$

The next big step towards understanding p-adic L-function is to explain how one can combine the p-adic variation of η_p and the p-adic variation of the integer n. This is an important theme in p-adic number theory.

Definition 2.2.4. Let $\eta_p : (\mathbb{Z}/p^r\mathbb{Z})^{\times} \to \mathbb{Q}_p^{\mathrm{alg},\times}$ be a primitive character of p-power conductor and let $n \in \mathbb{Z}_{\geq 0}$, we may combine the two information to obtain a p-adic continuous character

$$\begin{array}{rcccl} (\eta_p, n): \ \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) & \cong & \mathbb{Z}_p^{\times} & \longrightarrow & \overline{\mathbb{Q}}_p^{\times} \\ & & a & \longmapsto & \eta_p(a \bmod p^r) \cdot a^n, \end{array} \tag{2.2.4.1}$$

where $\mathbb{Q}(\mu_{p^\infty}) = \mathbb{Q}(\zeta_{p^r}; r \in \mathbb{Z}_{\geq 1})$ is the *p-cyclotomic extension* of $\mathbb{Q}$.

We may also view this as the function $\eta_p(x)x^n$ on $\mathbb{Z}_p^{\times}$.

2.2.5. *p-adic L-function, version III: p-adic L-function is a measure.* The "correct" mathematical object for a p-adic L-function is as a p-adic measure or a p-adic distribution (as opposed to a p-adic function). In view of Definition 2.2.4, the p-adic L-function will need to be able to "evaluate" on the continuous function $\eta_p(x)x^n$. This means that the correct definition of a p-adic L-function is a p-adic measure on $\mathbb{Z}_p^{\times}$, the dual of the space of continuous p-adic functions on $\mathbb{Z}_p^{\times}$.

Our target theorem is the following.

Theorem 2.2.6. *Let η be a primitive Dirichlet character of prime-to-p conductor N. Then there exists a "p-adic measure $d\mu_\eta$ on $\mathbb{Z}_p^{\times}$ such that, for any primitive character $\eta_p : (\mathbb{Z}/p^r\mathbb{Z})^{\times} \to \overline{\mathbb{Q}}_p^{\times}$ (allowing $\eta_p = \mathbf{1}$) and any $n \in \mathbb{Z}_{\geq 0}$, we have*

$$\int_{\mathbb{Z}_p^{\times}} \eta_p(x)x^n d\mu_\eta(x) = L^{\{p\}}(\eta \cdot \eta_p, -n), \tag{2.2.6.1}$$

where $\int_{\mathbb{Z}_p^{\times}}$ is a formal integration and its definition and the meaning of p-adic measures will be carefully explained later in this lecture. The "p-deprived" L-function $L^{\{p\}}(\eta \cdot \eta_p, s)$ is the *usual L-function but with the L-factor at p removed, namely,*

$$L^{\{p\}}(\eta\cdot\eta_p,s)=\prod_{\substack{q\text{ prime}\\(q,pN)=1}}\frac{1}{1-\eta(q)q^{-s}}=\begin{cases}L(\eta\cdot\eta_p,s) & \text{when } \eta_p \text{ is nontrivial}\\ L(\eta,s)\cdot(1-\eta(p)p^{-s}) & \text{when } \eta_p=\mathbf{1}.\end{cases}$$

In one sentence, a p-adic L-function is in fact a p-adic measure (or a p-adic distribution in some cases), whose evaluation at the continuous function formed by the finite character and the integer n gives the special values of the corresponding L-functions (with slight modification at p).

Remark 2.2.7. (1) We will prove a theorem when $\eta=\mathbf{1}$ too, but there is a slight technical issue, related to the fact that ζ-function admits a pole at $s=1$. Thus, accordingly, one expect the p-adic ζ-function to also have a pole at $s=1$; so it will not be a p-adic measure any more.

(2) In general, when defining the p-adic version of the L-functions, it is very natural to make modifications to the L-factor at p; the method of modification is not always removing the entire L-factor at p.

2.2.8. *Heuristic proof of Theorem 2.2.6 $\Rightarrow$ Theorem 2.1.3.* Even though we have not mathematically defined the p-adic measure yet, we feel it is helpful to explain why the existence of the p-adic L-function implies the Kummer's congruence relation.

Let k be a positive integer and let n_1 and n_2 are two integers greater than or equal to k. If the interpolation property (2.2.6.1) holds, then we have

$$\begin{array}{ccc}\displaystyle\int_{\mathbb{Z}_p^\times}\eta_p(x)x^{n_1}d\mu_\eta(x) & & \displaystyle\int_{\mathbb{Z}_p^\times}\eta_p(x)x^{n_2}d\mu_\eta(x)\\ \| & & \|\\ L^{\{p\}}(\eta,-n_1) & \overset{?}{\equiv} & L^{\{p\}}(\eta,-n_2)\end{array}$$

Since we assumed that $n_1\geq k$ and $n_2\geq k$, we must have for $i=1,2$,

$$L^{\{p\}}(\eta,-n_i)=L(\eta,-n_i)(1+\eta(p)p^{n_i})\equiv L(\eta,-n_i)\mod p^k.$$

(This is where the condition $n_1,n_2\geq k$ is used.)

If we want to prove Theorem 2.1.3: $L(\eta,-n_1)\equiv L(\eta,-n_2)\bmod p^k$, we would have to prove that

$$\int_{\mathbb{Z}_p^\times}\eta_p(x)x^{n_1}d\mu_\eta(x)\equiv\int_{\mathbb{Z}_p^\times}\eta_p(x)x^{n_2}d\mu_\eta(x)\mod p^k. \tag{2.2.8.1}$$

But note that condition for Kummer congruence is $n_1\equiv n_2\bmod (p-1)p^{k-1}$, which implies that $x^{n_1}\equiv x^{n_2}\bmod p^k$ for any $x\in\mathbb{Z}_p^\times$, that is to say the functions $\eta_p(x)x^{n_1}$ is congruent to $\eta_p(x)x^{n_2}$ modulo p^k, as functions on $\mathbb{Z}_p^\times$.

It is conceivable that the congruence $\eta_p(x)x^{n_1}\equiv\eta_p(x)x^{n_2}\bmod p^k$ implies the congruence of the integrals (2.2.8.1). From this, we deduce Theorem 2.1.3.

2.3. **Continuous p-adic functions on $\mathbb{Z}_p$.** As indicated in the previous subsection, we need to develop a theory for integration of p-adic valued continuous functions over a p-adic space.

Remark 2.3.1. We first point out that the naïve Haar measure and Riemann integral technique does not work. Suppose that we give $\mathbb{Z}_p$ volume 1, it is then conceivable to see that every $a+p^r\mathbb{Z}_p$ would have volume $\frac{1}{p^r}$. Then we would have an equality

$$\mathrm{vol}(\mathbb{Z}_p) = \sum_{a\in\mathbb{Z}/p^r\mathbb{Z}} \mathrm{vol}(a+p^r\mathbb{Z}_p).$$

Even though this is an equality, the partial sum converges seems to be quite bad because $\frac{1}{p^r}$ is p-adically very large.

We need some genuinely new setup. For this, we introduce some very basic concepts in p-adic functional analysis.

Definition 2.3.2. Let K be a completely valued field over $\mathbb{Q}_p$ (e.g. $K=\mathbb{Q}_p$) with valuation ring $\mathcal{O}_K$. Write $|\cdot|: K\to\mathbb{R}_{\geq 0}$ for the norm.

A (p-adic) *Banach space over* K is a K-vector space V complete with respect to a norm $\|\cdot\|: V\to\mathbb{R}_{\geq 0}$, such that

(1) $\|av\| = |a|\cdot\|v\|$ for every $a\in K$ and $v\in V$,
(2) $\|v+w\|\leq \max\{\|v\|,\|w\|\}$ for every $v,w\in V$,
(3) $\|v|\| = 0 \Leftrightarrow v=0$.

Example 2.3.3. The following is considered "the dual of L^∞ space":

$$\ell_\infty := \big\{(a_n)_{n\geq 0}\ \big|\ a_n\in K,\ \text{such that } a_n\to 0 \text{ when } n\to+\infty\big\},$$

with $\|(a_n)\| := \max_n\{|a_n|\}$. One can also write ℓ_∞ as

$$\ell_\infty \cong \Big(\widehat{\bigoplus_{n\geq 0}\mathcal{O}_K}\Big)\otimes_{\mathcal{O}_K} K.$$

Example 2.3.4. For X a compact topological space, define

$$\mathcal{C}^0(X,\mathcal{O}_K) := \{f: X\to\mathcal{O}_K \text{ continuous}\},\quad \mathcal{C}^0(X,K) := \mathcal{C}^0(X,\mathcal{O}_K)\otimes_{\mathcal{O}_K} K.$$

The norm is defined to be $\|f\|_{\sup} := \sup_{x\in X}|f(x)|$.

In p-adic functional analysis, there is a condition on Banach spaces which makes it a little like Hilbert spaces in real functional analysis.

Definition 2.3.5. For a Banach space V, an *orthonormal basis* is a family of elements $\{e_i\}_{i\in I}\subset V$ such that

(1) $\|e_i\| = 1$ for any $i\in I$,
(2) every $x\in V$ can be written *uniquely* as a sum $x=\sum_{i\in I} x_ie_i$ with each $x_i\in K$ and $x_i\to 0$ in the sense that, for any $\varepsilon>0$, $\#\{i \mid |x_i|>\varepsilon\}$ is finite, and
(3) $\|x\| = \max_{i\in I}\big\{|x_i|\big\}$.

We say such a Banach space V is *ONable* (short for *orthonormalizable*).

Notation 2.3.6. For the rest of this section, we mostly focus on one case

$$\mathcal{C}^0(\mathbb{Z}_p,\mathbb{Z}_p) := \big\{\text{continuous functions } f:\mathbb{Z}_p\to\mathbb{Z}_p\big\},\quad \|f\| := \sup_{x\in\mathbb{Z}_p}|f(x)|.$$

For a completely valued field K, we put

$$\mathcal{C}^0(\mathbb{Z}_p,\mathcal{O}_K) := \mathcal{C}^0(\mathbb{Z}_p,\mathbb{Z}_p)\,\widehat{\otimes}_{\mathbb{Z}_p}\mathcal{O}_K,\quad \mathcal{C}^0(\mathbb{Z}_p,K) := \mathcal{C}^0(\mathbb{Z}_p,\mathcal{O}_K)\otimes_{\mathcal{O}_K} K.$$

We start by producing some norm 1 elements in $\mathcal{C}^0(\mathbb{Z}_p, \mathbb{Z}_p)$.

Lemma 2.3.7. *For $n \in \mathbb{Z}_{\geq 0}$, we define*

$$\binom{x}{n} := \begin{cases} 1 & \text{when } n \geq 0 \\ \frac{x(x-1)\cdots(x-n+1)}{n!} & \text{when } n \geq 1. \end{cases}$$

Then the binomial function $\binom{x}{n} \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Z}_p)$ and $\left\|\binom{x}{n}\right\| \leq 1$.

Proof. It is clear that when $x \in \mathbb{Z}$, $\binom{x}{n} \in \mathbb{Z}$. By density of $\mathbb{Z}$ in $\mathbb{Z}_p$, we see that for $x \in \mathbb{Z}_p$, $\|\binom{x}{n}\| \leq 1$. Yet when $x = n$, $\binom{x}{n}|_{x=n} = \binom{n}{n} = 1$. So $\|\binom{x}{n}\| = 1$. $\square$

Theorem 2.3.8 (Mahler)**.** *Every $f \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$ admits a unique expansion, called* Mahler expansion*,*

$$f(x) = \sum_{n=0}^{\infty} a_n(f)\binom{x}{n} \quad \text{with } a_n(f) \to 0 \text{ as } n \to \infty. \tag{2.3.8.1}$$

Moreover, $\|f\| = \sup_n |a_n(f)|$. In other words, $\left\{\binom{x}{n}\right\}_{n\geq 0}$ is an orthonormal basis of $\mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$.

Alternatively speaking, the Mahler expansion gives an isomorphism

$$\begin{aligned} \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p) &\xrightarrow{\cong} \ell_\infty \\ f(x) &\longmapsto (a_n(f))_{n\geq 0}. \end{aligned}$$

Proof. We first assume the Mahler expansion and see how f determines the coefficients $a_n(f)$. Setting $x = 0$ gives $f(0) = a_0(f)$, and then setting $x = 1$ gives $f(1) = a_0(f) + a_1(f)$, ... One can see that it is possible to solve all $a_n(f)$ from this recursive process. We will do an elaborated version of this.

For $f \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$, inductively define

$$f^{[0]} := f, \quad \text{and} \quad f^{[k+1]}(x) := f^{[k]}(x+1) - f^{[k]}(x) \quad \text{for any } k \geq 0.$$

In particular, we have $(f^{[k]})^{[\ell]} = f^{[k+\ell]}$ for $k, \ell \in \mathbb{Z}_{\geq 0}$.

Now, suppose that we have known $f(x) = \sum_{n\geq 0} a_n(f)\binom{x}{n}$, then $f^{[1]}(x)$ would be equal to $\sum_{n\geq 0} a_n(f)\left(\binom{x+1}{n} - \binom{x}{n}\right) = \sum_{n\geq 0} a_n(f)\binom{x}{n-1}$. Inductively, we may show that for any $k \in \mathbb{Z}_{\geq 0}$, $f^{[k]}(x) = \sum_{n\geq 0} a_n(f)\binom{x}{n-k}$.

From this discussion, for $f \in \mathcal{C}^\circ(\mathbb{Z}_p, \mathbb{Q}_p)$, we put

$$a_k(f) := f^{[k]}(0).$$

We have the following explicit formulas that we will use later.

$$f^{[n]}(x) = \sum_{k=0}^{n} (-1)^k \binom{n}{k} f(x+n-k) \tag{2.3.8.2}$$

$$a_n(f) = f^{[n]}(0) = \sum_{k=0}^{n} (-1)^k \binom{n}{k} f(n-k) \tag{2.3.8.3}$$

From now on, we may assume that $\|f\| = 1$, in particular, $f \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Z}_p)$. Then we may determine the Mahler coefficients $a_n(f)$ using (2.3.8.3). We need to prove the following statements.

(1) $\sup_n |a_n(f)| = 1$.
(2) $a_n(f) \to 0$ as $n \to \infty$.
(3) $f(x) = \sum_{n \geq 0} a_n(f)\binom{x}{n}$.

For (1), since $f \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Z}_p)$, the explicit formula (2.3.8.3) implies that $|f(n)| \leq 1$ for every $n \geq 0$. Moreover, the condition $\|f\| = 1$ implies that there exists $m \in \mathbb{Z}_{\geq 0}$ such that $|f(m)| = 1$ (such m exists because $|f(-)|$ is locally constant.) We take the smallest such m, then by the explicit formula (2.3.8.3), we see that $|a_m(f)| = 1$.

For (2), we need a lemma.

Lemma For every $f \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Z}_p)$, there exists $k \in \mathbb{Z}_{\geq 1}$ such that $f^{[p^k]} \in p \cdot \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Z}_p)$.

Iteratively applying the Lemma, we see that there exists integers $N_1 < N_2 < \cdots$ such that $f^{N_i} \in p^i\mathcal{C}^0(\mathbb{Z}_p, \mathbb{Z}_p)$ for every i. This implies that $v_p(a_n(f)) \geq i$ whenever $n > N_i$. Thus $a_n(f) \to 0$ as $n \to \infty$.

Proof of Lemma: Consider the continuous function $\bar{f} : \mathbb{Z}_p \xrightarrow{f} \mathbb{Z}_p \xrightarrow{\bmod p} \mathbb{F}_p$. There exists $k \in \mathbb{Z}_{\geq 1}$ such that $\bar{f}$ is locally constant on each $a + p^k\mathbb{Z}_p$. Then

$$\begin{aligned} f^{[p^k]}(x) &= \sum_{j=0}^{p^k} (-1)^j \binom{p^k}{j} f(x + p^k - j) \\ &= f(x + p^k) - f(x) + p \cdot * \end{aligned}$$

belongs to $p \cdot \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Z}_p)$. The Lemma is proved, so is (2).

To prove (3), we simply note that (2) implies that the sum

$$\sum_{n \geq 0} a_n(f) \binom{x}{n} \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Z}_p)$$

defines a continuous function on $\mathbb{Z}_p$. In addition, by definition, we know that

$$f(x) - \sum_{n \geq 0} a_n(f) \binom{x}{n} \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Z}_p)$$

is zero at all $x \in \mathbb{Z}_{\geq 0}$. This implies that $f(x) = \sum_{n \geq 0} a_n(f)\binom{x}{n}$. $\square$

2.4. **Distribution on $\mathbb{Z}_p$.**

Definition 2.4.1. For a compact topological space, we define the space of *p-adic measures* on X to be

$$\mathcal{D}_0(X, \mathbb{Z}_p) := \mathrm{Hom}_{\mathrm{cont}}\big(\mathcal{C}^0(X, \mathbb{Z}_p), \mathbb{Z}_p\big).$$

For K a completely valued field, we define

$$\mathcal{D}_0(X, \mathcal{O}_K) := \mathcal{D}(X, \mathbb{Z}_p) \widehat{\otimes}_{\mathbb{Z}_p} \mathcal{O}_K \cong \mathrm{Hom}_{\mathrm{cont}}\big(\mathcal{C}^0(X, \mathcal{O}_K), \mathcal{O}_K\big)$$

$$\text{and} \quad \mathcal{D}_0(X, K) := \mathcal{D}_0(X, \mathcal{O}_K) \otimes_{\mathcal{O}_K} K.$$

Remark 2.4.2. Regarding the terminology measures versus distributions, we follow the convention that a measure is a bounded distribution. For the purpose of p-adic Dirichlet L-functions, we only need p-adic measures. It is likely that we will come back for more general p-adic distributions later in this semester.

2.4.3. *Identification of $\mathcal{D}_0(\mathbb{Z}_p, \mathbb{Z}_p)$.* Since $\mathcal{C}^0(\mathbb{Z}_p, \mathbb{Z}_p)$ admits an orthonormal basis given by $\big\{\binom{x}{n} \,\big|\, n \in \mathbb{Z}_{\geq 0}\big\}$, its dual may be identified with $\prod\limits_{n\geq 0} \mathcal{O}_K$. More precisely, for $\underline{b} = (b_n)_{n\geq 0}$, the functional $\underline{b}$ defines is:

$$\Big\langle \sum_{n\geq 0} a_n \binom{x}{n},\ \underline{b} \Big\rangle := \sum_{n\geq 0} a_n b_n.$$

We may alternatively organize the sequence $\underline{b} = (b_n)_{n\geq 0}$ as a power series $\sum\limits_{n\geq 0} b_n T^n \in \mathbb{Z}_p[\![T]\!]$.

Notation-Proposition 2.4.4. For $\mu \in \mathcal{D}_0(\mathbb{Z}_p, \mathbb{Z}_p)$, the corresponding power series $A_\mu(T) \in \mathbb{Z}_p[\![T]\!]$ defined above admits an explicit formula, called the *Amice transform*:

$$A_\mu(T) = \int_{\mathbb{Z}_p} (1+T)^x d\mu(x).$$

This defines a topological isomorphism $\mathcal{D}_0(\mathbb{Z}_p, \mathbb{Z}_p) \cong \mathbb{Z}_p[\![T]\!]$.

Proof. We compute this formally:

$$\begin{aligned} \int_{\mathbb{Z}_p} (1+T)^x d\mu(x) &= \int_{\mathbb{Z}_p} \Big(\sum_{n\geq 0} \binom{x}{n} T^n \Big) d\mu(x) \\ &= \sum_{n\geq 0} \Big(\int_{\mathbb{Z}_p} \binom{x}{n} d\mu(x) \Big) T^n = \sum_{n\geq 0} b_n T^n = A_\mu(T). \end{aligned}$$

□

2.5. **Exercises.**

Exercise 2.5.1. (Modified Mahler basis) In this problem, we give a different orthonormal basis of $\mathcal{C}^0(\mathbb{Z}_p, \mathbb{Z}_p)$. Consider the function $f(z) = \frac{z^p - z}{p}$ on $\mathbb{Z}_p$.

(1) Show that $f \in \mathcal{C}^\circ(\mathbb{Z}_p, \mathbb{Z}_p)$.

Consider the following inductively defined functions:

$$f^{\{0\}}(z) = z, \quad f^{\{1\}}(z) = f(z) = \frac{z^p - z}{p}, \quad f^{\{2\}}(z) = f^{\{1\}}\Big(\frac{z^p - z}{p}\Big) = \frac{\big(\frac{z^p - z}{p}\big)^p - \frac{z^p - z}{p}}{p},$$

$$f^{\{k+1\}}(z) = f\big(f^{\{k\}}(z)\big), \qquad \text{for } k \geq 1.$$

For $n \geq 0$, write $n = n_0 + n_1 p + n_2 p^2 + \cdots$ for the p-adic expansion of n, i.e. each $a_i \in \{0, 1, \ldots, p-1\}$, put

$$e_n(z) = \big(f^{\{0\}}(z)\big)^{n_0} \big(f^{\{1\}}(z)\big)^{n_1} \big(f^{\{2\}}(z)\big)^{n_2} \cdots$$

We call $\{e_n(z)\}$ a *modified Mahler basis*.

(2) Prove that $e_p(z) + \binom{z}{p} \in \mathbb{Z}_p[z]$.

(3) Prove that each $e_n(z)$ may be written as a $\mathbb{Z}_p$-linear combination of binomial functions $\binom{z}{m}$'s, and show that the change of basis matrix from the Mahler basis to $e_n(z)$ is upper triangular with all entries in $\mathbb{Z}_p$ and diagonal entries in $\mathbb{Z}_p^\times$.
(4) Deduce that $\{e_n(z) \,|\, n \geq 0\}$ form an orthonormal basis of $\mathcal{C}^0(\mathbb{Z}_p, \mathbb{Z}_p)$.
(5) Assume that $p \geq 3$. Recall that $\mathbb{Z}_p^\times \cong \mu_{p-1} \times (1 + p\mathbb{Z}_p)^\times$, where μ_{p-1} is the subgroup of $(p-1)$th roots of unity in $\mathbb{Q}_p$. The group μ_{p-1} acts naturally on $\mathcal{C}^0(\mathbb{Z}_p, \mathbb{Z}_p)$ such that for $\zeta \in \mu_{p-1}$, it sends $h(z)$ to $h(\zeta z)$. Show that each of $e_n(z)$ is an eigenfunction for this action.

Remark 2.5.2. We call $e_n(z)$'s the *modified Mahler basis*. As (2) suggested, $e_n(z)$ is essentially the "leading terms" of $\binom{z}{n}$ up to a constant multiple.

The disadvantage of modified Mahler basis is that it is not compatible with the Amice transform. However, part (5) shows that the modified Mahler basis are formed by μ_{p-1}-eigenfunctions, which are useful in some applications.

Exercise 2.5.3. (Orthonormal basis of $\mathcal{C}^0(\mathbb{Z}_{p^r}, \mathbb{Z}_{p^r})$) Let $\mathbb{Q}_{p^r}$ be the unramified extension of $\mathbb{Q}_p$ of degree r, and $\mathbb{Z}_{p^r}$ be its ring of integers. In this problem, we will produce an orthonormal basis of $\mathcal{C}^0(\mathbb{Z}_{p^r}, \mathbb{Z}_{p^r})$ that is similar to the modified Mahler basis defined in the previous problem.

Let σ denote the (arithmetic) Frobenius on $\mathbb{Z}_{p^r}$, i.e. the automorphism of $\mathbb{Z}_{p^r}$ whose reduction modulo p sends $\bar{x}$ to $\bar{x}^p$. Write $z_0 : \mathbb{Z}_{p^r} \to \mathbb{Z}_{p^r}$ for the identify function, i.e. $z_0(a) = a$. We then inductively define

$$z_{j+1}(a) = \sigma(z_j(a)) \qquad \text{for } j \geq 0.$$

Clearly, $z_{j+r} = z_j$ for $j \geq 0$. It is also clear that $\mathbb{Q}_{p^r}[z_0, \dots, z_{r-1}]$ is a dense subring of $\mathcal{C}^0(\mathbb{Z}_{p^r}, \mathbb{Q}_{p^r})$ (but $\mathbb{Z}_p[z_0, \dots, z_{r-1}]$ is not dense in $\mathcal{C}^0(\mathbb{Z}_{p^r}, \mathbb{Z}_{p^r})$).

We define inductively

$$f_0 := 1, \quad f_1 := z_0, \quad f_p := \frac{z_0^p - z_1}{p}, \quad f_{p^{i+1}} = f_p \circ f_{p^r} = \frac{f_{p^i}^p - \sigma(f_{p^i})}{p}, \text{ with } i = 1, 2, \dots$$

For example, $f_{p^2} = \dfrac{\left(\frac{z_0^p - z_1}{p}\right)^p - \frac{z_1^p - z_2}{p}}{p}$.

If $m = s_0 + ps_1 + p^2 s_2 + \cdots$ is the p-adic expansion of a positive integer (with $s_i \in \{0, \dots, p-1\}$), we set

$$f_m := f_1^{s_0} f_p^{s_1} f_{p^2}^{s_2} \cdots$$

Finally, if $\mathbf{m} = (m_0, \dots, m_{r-1}) \in \mathbb{Z}_{\geq 0}^r$ is an r-tuple of index, we set

$$\mathbf{f_m} := f_{m_0} \cdot \varphi(f_{m_1}) \cdots \varphi^{r-1}(f_{m_{r-1}}). \tag{2.5.3.1}$$

(1) Show that each function $\mathbf{f_m}$ is a continuous function in $\mathcal{C}^0(\mathbb{Z}_{p^r}, \mathbb{Z}_{p^r})$, and compute its leading coefficients, as a polynomial in $z_0, \dots, z_{r-1}$.
(2) Show that $\mathbf{f_m}$'s form an orthonormal basis of $\mathcal{C}^0(\mathbb{Z}_{p^r}, \mathbb{Z}_{p^r})$.

(Hint: it might be helpful to compare this to a "known" (noncanonical) Mahler basis: choose a $\mathbb{Z}_p$-linear isomorphism

$$\begin{aligned} c : \mathbb{Z}_{p^r} &\xrightarrow{\ \cong\ } (\mathbb{Z}_p)^r \\ a &\longmapsto (\mathsf{c}_0^*(a), \dots, \mathsf{c}_{r-1}^*(a)). \end{aligned}$$

Here we may view each c_j^* as a function $\mathbb{Z}_{p^r}$ with values in $\mathbb{Z}_p$. Then the functions $\mathbf{u}_\mathbf{m} : a \mapsto \binom{\mathsf{c}_0^*(a)}{m_0} \cdots \binom{\mathsf{c}_{r-1}^*(a)}{m_{r-1}}$ for $\mathbf{m} \in \mathbb{Z}_{\geq 0}^r$ form an orthonormal basis of $\mathcal{C}^0(\mathbb{Z}_{p^r}, \mathbb{Z}_{p^r})$ with respect to the maximal norm $||\cdot||$. It is then a question to compare the two bases $\mathbf{f}_\mathbf{m}$ and $\mathbf{u}_\mathbf{m}$.)

3. p-adic Dirichlet L-functions

Recall that every continuous function $f \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Z}_p)$ admits a canonical Mahler expansion

$$f(x) = \sum_{n=0}^{\infty} a_n(f) \binom{x}{n}, \qquad \text{with } a_n(f) \in \mathbb{Z}_p.$$

The space of p-adic measures on $\mathbb{Z}_p$ admits the following nice description (called the Amice transform):

$$\begin{aligned} \mathcal{D}_0(\mathbb{Z}_p, \mathbb{Z}_p) &\xrightarrow{\quad\cong\quad} \mathbb{Z}_p[\![T]\!] \\ \mu &\longmapsto A_\mu(T) := \textstyle\int_{\mathbb{Z}_p} (1+T)^x d\mu(x). \end{aligned}$$

The goal of first part of this lecture is to give a more intrinsic definition of the Amice transform, in terms of "Iwasawa algebras".

3.1. **Iwasawa algebras.**

Definition 3.1.1. For a profinite group $G = \varprojlim_{H \lhd G \text{ finite}} G/H$, define the associated *Iwasawa algebra* for G to be

$$\mathbb{Z}_p[\![G]\!] = \varprojlim_{H \lhd G \text{ finite}} \mathbb{Z}_p[G/H].$$

Each $g \in G$ defines an element $[g] \in \mathbb{Z}_p[G]$; the ring $\mathbb{Z}_p[G]$ is dense inside $\mathbb{Z}_p[\![G]\!]$.

Remark 3.1.2. The construction of Iwasawa algebra is functorial in G, namely, if $\varphi : G \to H$ is a continuous group homomorphism of profinite group, then it induces a continuous ring homomorphism $\tilde{\varphi} : \mathbb{Z}_p[\![G]\!] \to \mathbb{Z}_p[\![H]\!]$.

Remark 3.1.3. We explain why the definition of $\mathbb{Z}_p[\![G]\!]$ in Definition 3.1.1 is natural. For G a discrete group, there is a natural equivalence of categories

$$\big\{\text{representations of } G \text{ on } \mathbb{Z}\text{-modules } M\big\} \xleftrightarrow{\quad\cong\quad} \big\{\mathbb{Z}[G]\text{-modules } M\big\}.$$

Similarly, there is a natural equivalence of categories

$$\big\{\text{continuous representations of } G \text{ on } \mathbb{Z}\text{-modules } M\big\} \xleftrightarrow{\quad\cong\quad} \big\{\text{continuous } \mathbb{Z}_p[\![G]\!]\text{-modules } M\big\}.$$

In particular, when G is a profinite abelian group that is topologically finitely generated, there is a one-to-one correspondence among the following (setting $\mathbb{C}_p$ to be the completion of $\overline{\mathbb{Q}}_p$):

1. continuous homomorphisms $\eta : G \to \mathbb{C}_p^\times$,
2. continuous ring homomorphism $\mathbb{Z}_p[\![G]\!] \to \mathbb{C}_p$,
3. $\mathbb{C}_p$-point of $(\operatorname{Spf} \mathbb{Z}_p[\![G]\!])^{\mathrm{rig}}$ (the rigid analytic space associated to $\mathbb{Z}_p[\![G]\!]$).

The key example in this lecture is the following.

Example 3.1.4. Consider $G = (\mathbb{Z}_p, +)$. Then we have

$$\begin{aligned}
\mathbb{Z}_p[\![\mathbb{Z}_p]\!] = \varprojlim_{m\to\infty} \mathbb{Z}_p[\mathbb{Z}/p^m\mathbb{Z}] &\cong \varprojlim_{m\to\infty} \mathbb{Z}_p[x]/(x^{p^m}-1) && 1 \leftrightarrow [0],\ x \leftrightarrow [1] \\
&\cong \varprojlim_{m\to\infty} \mathbb{Z}_p[T]/((1+T)^{p^m}-1) && T \leftrightarrow [1]-1 \\
&\cong \varprojlim_{m\to\infty} \mathbb{Z}_p[T]/(p,T)^m \cong \mathbb{Z}_p[\![T]\!].
\end{aligned}$$

If $\eta : \mathbb{Z}_p \to \mathbb{C}_p^\times$ is a continuous character, the $\mathbb{C}_p$-point it corresponds on $(\mathrm{Spf}\,\mathbb{Z}_p[\![T]\!])^{\mathrm{rig}}$ is

$$\begin{aligned}
\tilde{\eta} : \mathbb{Z}_p[\![T]\!] &\longrightarrow \mathbb{C}_p \\
f(T) &\longmapsto f(\eta(1)-1),
\end{aligned}$$

i.e. $\tilde{\eta}$ corresponds to the point $T = \eta(1) - 1$ on $(\mathrm{Spf}\,\mathbb{Z}_p[\![T]\!])^{\mathrm{rig}}$ (the rigid analytic open unit disc).

3.2. **Intrinsic definition of Amice transform.** We explain the relation between the space of p-adic measures and the Iwasawa algebra.

Notation-Lemma 3.2.1. If $X = \varprojlim_i X_i$ is a profinite set (and assume that in this inverse system, each X_i is finite and $X_j \to X_i$ is surjective whenever $j > i$). Then the space of *p-adic measures* on X defined by

$$\mathcal{D}_0(X, \mathbb{Z}_p) := \mathrm{Hom}_{\mathrm{cont}}\big(\mathcal{C}^0(X, \mathbb{Z}_p), \mathbb{Z}_p\big)$$

admits a natural formula:

$$\begin{aligned}
\mathcal{D}_0(X, \mathbb{Z}_p) &\cong \varprojlim_i \mathcal{D}_0(X_i, \mathbb{Z}_p) = \varprojlim_i \mathrm{Hom}_{\mathrm{cont}}\big(\mathcal{C}^0(X_i, \mathbb{Z}_p), \mathbb{Z}_p\big) \\
&= \varprojlim_i \mathbb{Z}_p[X_i] =: \mathbb{Z}_p[\![X]\!].
\end{aligned}$$

where $\mathbb{Z}_p[X_i] = \Big\{ \sum_{x\in X_i} c_x[x] \Big\}$ is the space of all possible weights in X_i.

In the special case when $X = G$ is a profinite group, we have a canonical isomorphism

$$\mathcal{D}_0(G, \mathbb{Z}_p) \cong \mathbb{Z}_p[\![G]\!]. \tag{3.2.1.1}$$

When G is a profinite group, the canonical isomorphism (3.2.1.1) preserves some additional structure.

Lemma 3.2.2. *The multiplication for the ring structure on $\mathbb{Z}_p[\![G]\!]$ corresponds to the* convolution product *on $\mathcal{D}_0(G, \mathbb{Z}_p)$: for $\mu_1, \mu_2 \in \mathcal{D}_0(G, \mathbb{Z}_p)$,*

$$\int_G f(g) d(\mu_1 \star \mu_2)(g) := \int_G \int_G f(gh) d\mu_1(g) d\mu_2(h).$$

Proof. By taking limits, it is enough to prove this when G is finite. In this case, we may view μ_i as a (weight) function in $\mathbb{Z}_p[G]$. Write $\langle -, - \rangle$ for the pairing between the functions on G and the (weight) function on G, then for $f \in \mathcal{C}^0(G, \mathbb{Z}_p)$ and $\mu_1, \mu_2 \in \mathbb{Z}_p[G]$, we have

$$\begin{aligned}\big\langle f, \mu_1 \star \mu_2 \big\rangle = & \sum_{g \in G} f(g)(\mu_1 \star \mu_2)(g) = \sum_{g \in G} f(g) \sum_{h \in G} \mu_1(h)\mu_2(h^{-1}g) \\ \overset{h_1 = h^{-1}g}{=} & \sum_{h \in G} \sum_{h_1 \in G} \mu_1(h)\mu_2(h_1) \cdot f(hh_1). \end{aligned}$$

□

Now, we can give an intrinsic formulation of the Amice transform formula introduced in Notation-Proposition 2.4.4.

Theorem 3.2.3. *The Amice transform* $\mu \mapsto A_\mu(T) = \int_{\mathbb{Z}_p} (1+T)^x d\mu(x)$ *from* $\mathcal{D}_0(\mathbb{Z}_p, \mathbb{Z}_p)$ *to* $\mathbb{Z}_p[\![T]\!]$ *is exactly the composition of the following canonical isomorphisms*

$$\mathcal{D}_0(\mathbb{Z}_p, \mathbb{Z}_p) \overset{(3.2.1.1)}{\cong} \mathbb{Z}_p[\![\mathbb{Z}_p]\!] \cong \mathbb{Z}_p[\![T]\!].$$

Proof. We write out the sequence of isomorphisms explicit and compute the image of a p-adic measure $\mu \in \mathcal{D}_0(\mathbb{Z}_p, \mathbb{Z}_p)$ at each stage.

$$\begin{array}{ccc} \mathcal{D}_0(\mathbb{Z}_p, \mathbb{Z}_p) \cong \varprojlim\limits_{m \to \infty} \mathcal{D}_0(\mathbb{Z}/p^m, \mathbb{Z}_p) & & \mu \\ \downarrow \cong & & \downarrow \\ \varprojlim\limits_{m \to \infty} \mathbb{Z}_p[\mathbb{Z}/p^m\mathbb{Z}] & & \lim\limits_{m \to \infty} \Big(\sum\limits_{a \in \mathbb{Z}/p^m\mathbb{Z}} \mu(a + p^m\mathbb{Z}_p) \cdot [a] \Big) \\ \downarrow \cong & & \downarrow \\ \varprojlim\limits_{m \to \infty} \mathbb{Z}_p[T]/\big((1+T)^{p^m} - 1\big) & & \lim\limits_{m \to \infty} \Big(\sum\limits_{a \in \mathbb{Z}/p^m\mathbb{Z}} \mu(a + p^m\mathbb{Z}_p) \cdot (1+T)^a \Big). \end{array}$$

The last limit is clearly equal to $\displaystyle\int_{\mathbb{Z}_p} (1+T)^x d\mu(x) = A_\mu(T)$. □

3.3. **Further operations on measures over $\mathbb{Z}_p$.** We will first introduce a series of operators on the space of p-adic measures $\mathcal{D}_0(\mathbb{Z}_p, \mathbb{Z}_p)$ and the corresponding analogues on $\mathbb{Z}_p[\![T]\!]$. We quickly recall from Remark 3.1.2 that a continuous homomorphism $\phi : G \to H$ between two profinite groups induces a continuous ring homomorphism $\tilde{\phi} : \mathbb{Z}_p[\![G]\!] \to \mathbb{Z}_p[\![H]\!]$.

Notation-Lemma 3.3.1. The multiplication by p is a group homomorphism on $\mathbb{Z}_p$, it induces a ring homomorphism $\varphi : \mathbb{Z}[\![\mathbb{Z}_p]\!] \to \mathbb{Z}_p[\![\mathbb{Z}_p]\!]$ given by sending $[1] = 1 + T$ to $[p] = (1+T)^p$, i.e. $\varphi : \mathbb{Z}_p[\![T]\!] \to \mathbb{Z}_p[\![T]\!]$ is a ring homomorphism such that

$$\varphi(f(T)) = f\big((1+T)^p - 1\big).$$

The same multiplication-by-p map induces a pushforward map of p-adic measures on $\mathbb{Z}_p$, also denoted by φ. Explicitly, for $f \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Z}_p)$,

$$\int_{\mathbb{Z}_p} f(x) d\varphi(\mu)(x) := \int_{\mathbb{Z}_p} f(px) d\mu(x).$$

Then the following diagram is commutative:

$$\begin{tikzcd}
\mathcal{D}_0(\mathbb{Z}_p, \mathbb{Z}_p) \arrow[r, "\text{Amice transform}", "\cong"'] \arrow[d, "\varphi"] & \mathbb{Z}_p[\![T]\!] \arrow[d, "\varphi"] \\
\mathcal{D}_0(\mathbb{Z}_p, \mathbb{Z}_p) \arrow[r, "\text{Amice transform}", "\cong"'] & \mathbb{Z}_p[\![T]\!].
\end{tikzcd}$$

Proof. We verify the commutativity of the diagram, i.e. for $\mu \in \mathcal{D}_0(\mathbb{Z}_p, \mathbb{Z}_p)$, we have $\varphi(A_\mu(T)) = A_{\varphi(\mu)}(T)$. Indeed,

$$\begin{aligned}
A_{\varphi(\mu)}(T) &= \int_{\mathbb{Z}_p} (1+T)^x d\varphi(\mu)(x) = \int_{\mathbb{Z}_p} (1+T)^{px} d\mu(x) \\
&= \varphi\Big(\int_{\mathbb{Z}_p} (1+T)^x d\mu(x) \Big) = \varphi(A_\mu(T)).
\end{aligned}$$

□

Notation-Lemma 3.3.2. Write Γ for the group $\mathbb{Z}_p^\times$, and for $a \in \mathbb{Z}_p^\times$, write γ_a for the corresponding elements in Γ. For each $a \in \mathbb{Z}_p^\times$, multiplication by a induces a continuous group automorphism of $\mathbb{Z}_p$, which in turn induces an isomorphism γ_a of $\mathbb{Z}_p[\![T]\!]$ given by

$$\gamma_a(T) = (1+T)^a - 1.$$

The same multiplication-by-a map induces an isomorphism of p-adic measures $\mathcal{D}_0(\mathbb{Z}_p, \mathbb{Z}_p)$, denoted by γ_a. Explicitly, for $f \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Z}_p)$,

$$\int_{\mathbb{Z}_p} f(x) d\gamma_a(\mu)(x) := \int_{\mathbb{Z}_p} f(ax) d\mu(x).$$

We have the following commutative diagram.

$$\begin{tikzcd}
\mathcal{D}_0(\mathbb{Z}_p, \mathbb{Z}_p) \arrow[r, "\text{Amice transform}", "\cong"'] \arrow[d, "\gamma_a"] & \mathbb{Z}_p[\![T]\!] \arrow[d, "\gamma_a"] \\
\mathcal{D}_0(\mathbb{Z}_p, \mathbb{Z}_p) \arrow[r, "\text{Amice transform}", "\cong"'] & \mathbb{Z}_p[\![T]\!].
\end{tikzcd}$$

Notation-Lemma 3.3.3. For each $b \in \mathbb{Z}_p$, shift-by-b: $x \mapsto x + b$ is an homeomorphism of $\mathbb{Z}_p$, and induces an automorphism s_b of $\mathcal{D}_0(\mathbb{Z}_p, \mathbb{Z}_p)$, explicitly, for $\mu \in \mathcal{D}_0(\mathbb{Z}_p, \mathbb{Z}_p)$ and $f \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Z}_p)$,

$$\int_{\mathbb{Z}_p} f(x) ds_b(\mu)(x) := \int_{\mathbb{Z}_p} f(x+b) d\mu(x).$$

Identifying $\mathcal{D}_0(\mathbb{Z}_p, \mathbb{Z}_p)$ with $\mathbb{Z}_p[\![T]\!]$ via Amice transform, the operator s_b sends $A_\mu(T) \in \mathbb{Z}_p[\![T]\!]$ to

$$A_{s_b(\mu)}(T) = \int_{\mathbb{Z}_p} (1+T)^x ds_b(\mu)(x) = \int_{\mathbb{Z}_p} (1+T)^{x+b} d\mu(x) = (1+T)^b \cdot A_\mu(T).$$

In other words, s_b is the multiplication-by-$(1+T)^b$ map on $\mathbb{Z}_p[\![T]\!]$.

Notation-Lemma 3.3.4. Corresponding to the coset decomposition $\mathbb{Z}_p = \coprod_{i=0}^{p-1}(i+p\mathbb{Z}_p)$, the ring $\mathbb{Z}_p[\![T]\!]$ admits a direct sum decomposition as a free $\varphi(\mathbb{Z}_p[\![T]\!])$-module:

$$\begin{aligned} \mathbb{Z}_p[\![T]\!] &\xrightarrow{\cong} \bigoplus_{i=0}^{p-1}(1+T)^i\varphi\big(\mathbb{Z}_p[\![T]\!]\big). \\ h &\longmapsto \sum_{i=0}^{p-1}(1+T)^i\varphi(h_i), \end{aligned} \tag{3.3.4.1}$$

for unique elements $h_0, \dots, h_{p-1} \in \mathbb{Z}_p[\![T]\!]$.

We define an ψ-operator $\psi : \mathbb{Z}_p[\![T]\!] \to \mathbb{Z}_p[\![T]\!]$ given by $\psi(h) = h_0$ for the h_0 in the decomposition above.

Proof. We prove the decomposition (3.3.4.1). In fact, we show the inverse map is an isomorphism:

$$\begin{aligned} \Phi : \mathbb{Z}_p[\![T]\!]^{\oplus p} &\longrightarrow \mathbb{Z}_p[\![T]\!] \\ (h_0, \dots, h_{p-1}) &\longmapsto \sum_{i=0}^{p-1}(1+T)^i\varphi(h_i). \end{aligned}$$

First consider Φ modulo p; in this case, φ is nothing but the Frobenius, and we have

$$\begin{aligned} \bar{\Phi} : \mathbb{F}_p[\![T]\!]^{\oplus p} &\longrightarrow \mathbb{Z}_p[\![T]\!] \\ (h_0, \dots, h_{p-1}) &\longmapsto \sum_{i=0}^{p-1}(1+T)^i h_i(T^p) \end{aligned}$$

This $\bar{\Phi}$ is clearly an isomorphism. From this, and that both the source and the target of Φ is p-adically complete, we may easily deduce that Φ is an isomorphism. ☐

Remark 3.3.5.
(1) The ψ-operator satisfies $\psi \circ \varphi = \mathrm{id}$, but it is NOT LINEAR (in particular, we should avoid talking about matrix of ψ). It is somewhat ϕ^{-1}-linear in the sense that $\psi(\varphi(f)h) = f\psi(h)$ for $f, h \in \mathbb{Z}_p[\![T]\!]$.
(2) Another way to think of ψ-operator is that $\mathbb{Z}_p[\![T]\!]$ is a free module of rank p over $\varphi(\mathbb{Z}_p[\![T]\!])$, and ψ maybe viewed as the composition

$$\psi : \mathbb{Z}_p[\![T]\!] \xrightarrow{\frac{1}{p}\mathrm{Tr}_{\mathbb{Z}_p[\![T]\!]/\varphi(\mathbb{Z}_p[\![T]\!])}} \varphi(\mathbb{Z}_p[\![T]\!]) \xrightarrow[\cong]{\varphi^{-1}} \mathbb{Z}_p[\![T]\!].$$

In the following exercise, we will revisit this point of view.

Lemma 3.3.6. *Under the Amice transform $\mathcal{D}_0(\mathbb{Z}_p, \mathbb{Z}_p) \cong \mathbb{Z}_p[\![T]\!]$, the decomposition* (3.3.4.1) *corresponds to*

$$\begin{aligned} \mathcal{D}_0(\mathbb{Z}_p, \mathbb{Z}_p) &\xrightarrow{\cong} \bigoplus_{i=0}^{p-1}\mathcal{D}_0(i+p\mathbb{Z}_p, \mathbb{Z}_p) \xleftarrow[\cong]{\oplus s_i\circ\varphi} \bigoplus_{i=0}^{p-1}\mathcal{D}_0(\mathbb{Z}_p, \mathbb{Z}_p) \\ \mu &\longrightarrow \sum_{i=0}^{p-1}\mathrm{Res}_{i+p\mathbb{Z}_p}(\mu) \end{aligned}$$

where $\mathrm{Res}_{i+p\mathbb{Z}_p}(\mu)$ *is to restrict the measure to the given subset* $i+p\mathbb{Z}_p$*, or more explicitly, for* $f \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Z}_p)$, $\int_{\mathbb{Z}_p} f(x)\mathrm{Res}_{i+p\mathbb{Z}_p}(\mu)(x) := \int_{\mathbb{Z}_p} f(x)\mathbf{1}_{i+p\mathbb{Z}_p} d\mu(x)$.

Proof. As already proved in Notation-Lemma 3.3.3 and 3.3.1, sending h_i to $(1+T)^i\varphi(h_i)$ corresponds to $\mu_i \mapsto s_i \circ \varphi(\mu_i)$ for p-adic measures, which is supported on the coset $i+p\mathbb{Z}_p$. Therefore, decomposing $h \in \mathbb{Z}_p[\![T]\!]$ into the sum $\sum_{i=0}^{p-1}(1+T)^i\varphi(h_i)$ precisely decomposing μ into the sum $\sum_{i=0}^{p-1}\mathrm{Res}_{i+p\mathbb{Z}_p}(\mu)$, such that each $\mathrm{Res}_{i+p\mathbb{Z}_p}(\mu)$ takes the form of $s_i \circ \varphi(\mu_i)$ for some p-adic measure μ_i on $\mathbb{Z}_p$. □

Notation-Lemma 3.3.7. For $\mu \in \mathcal{D}_0(\mathbb{Z}_p, \mathbb{Z}_p)$, its restriction to $\mathbb{Z}_p^\times$ is precisely

$$\mathrm{Res}_{\mathbb{Z}_p^\times}(\mu) := (1-\varphi\psi)(\mu).$$

Under the Amice transform, if we write $A_\mu(T) = \sum_{i=0}^{p-1}(1+T)^i\varphi(h_i)$, then

$$A_{\mathrm{Res}_{\mathbb{Z}_p^\times}(\mu)}(T) = \sum_{i=1}^{p-1}(1+T)^i\varphi(h_i).$$

Proof. We compute this directly, setting $A_\mu(T) = \sum_{i=0}^{p-1}(1+T)^i\varphi(h_i)$, then

$$\begin{aligned} A_{\mathrm{Res}_{\mathbb{Z}_p^\times}(\mu)}(T) &= \sum_{i=1}^{p-1} A_{\mathrm{Res}_{i+p\mathbb{Z}_p}(\mu)}(T) = \sum_{i=1}^{p-1}(1+T)^i\varphi(h_i) \\ &= A_\mu(T) - \varphi(h_0) = (1-\varphi\psi)(A_\mu)(T). \end{aligned}$$ □

Corollary 3.3.8. *A* p*-adic measures* $\mu \in \mathcal{D}_0(\mathbb{Z}_p, \mathbb{Z}_p)$ *is supported on* $\mathbb{Z}_p^\times$ *if and only if* $\psi(\mu) = 0$*.*

Proof. We have μ is supported on $\mathbb{Z}_p^\times \Leftrightarrow \mu = \mathrm{Res}_{\mathbb{Z}_p^\times}(\mu) \Leftrightarrow \mu = (1-\varphi\psi)(\mu) \Leftrightarrow \varphi\psi(\mu) = 0 \Leftrightarrow \psi(\mu) = 0$. □

3.4. **p-adic Dirichlet L-functions.** The target of this subsection is the following.

Theorem 3.4.1. *Let* $\eta \neq \mathbf{1}$ *be a primitive Dirichlet character of prime-to-p conductor* N*. Then there exists a unique* p*-adic measure* $\mu_\eta^{\{p\}}$ *on* $\mathbb{Z}_p^\times$ *with values in the ring of integer* $\mathcal{O}$ *of* $\mathbb{Q}_p(\eta)$ *such that for any primitive finite character* $\eta_p : (\mathbb{Z}/p^r\mathbb{Z})^\times \to \mathbb{Q}^{\mathrm{alg},\times} \xrightarrow{\iota_p} \overline{\mathbb{Q}}_p^\times$ *and any* $n \in \mathbb{Z}_{\geq 0}$*, we have*

$$\int_{\mathbb{Z}_p^\times} \eta_p(x)x^n d\mu_\eta^{\{p\}}(x) = L^{\{p\}}(\eta\eta_p, -n). \tag{3.4.1.1}$$

Before proceeding, we explain a recipe that allows us to "compute" the p-adic Dirichlet L-function satisfying the needed interpolation condition (3.4.1.1). We focus on the case when $\eta_p = \mathbf{1}$.

Lemma 3.4.2. *If $\mu \in \mathcal{D}_0(\mathbb{Z}_p, \mathbb{Z}_p)$ corresponds to $A_\mu(T) \in \mathbb{Z}_p[\![T]\!]$, we have*

$$\int_{\mathbb{Z}_p} x^n d\mu(x) = \Big((1+T)\frac{d}{dT}\Big)^n A_\mu(T)\Big|_{T=0}. \tag{3.4.2.1}$$

Proof. By Amice transform, we have

$$\int_{\mathbb{Z}_p} (1+T)^x d\mu(x) = A_\mu(T).$$

Applying the operator $(1+T)\frac{d}{dT}$ to this equation, we get

$$\int_{\mathbb{Z}_p} x \cdot (1+T)^x d\mu(x) = (1+T)\frac{d}{dT} A_\mu(T).$$

Iteratively apply the operator $(1+T)\frac{d}{dT}$ n times gives

$$\int_{\mathbb{Z}_p} x^n (1+T)^x d\mu(x) = \Big((1+T)\frac{d}{dT}\Big)^n A_\mu(T).$$

Setting $T=0$ gives the equality in the lemma. □

3.4.3. *Explicit construction of the p-adic measure.* Recall that for η a primitive Dirichlet character of conductor N (with $p \nmid N$), we defined

$$f_\eta(t) := \frac{\sum_{a=1}^{N-1} \eta(a) e^{-at}}{1-e^{-Nt}}, \qquad \text{then} \quad L(\eta, -n) = (-1)^n f_\eta^{(n)}(0) = \Big(-\frac{d}{dt}\Big)^n (f_\eta)\Big|_{t=0}.$$

But we need the special values $L^{\{p\}}(\eta, -n)$; so we need to modify above to put

$$f_\eta^{\{p\}}(t) := \frac{\sum_{\substack{a=1 \\ p\nmid a}}^{pN-1} \eta(a) e^{-at}}{1-e^{-pNt}} = \sum_{\substack{a \geq 1 \\ (a,pN)=1}} \eta(a) e^{-at}.$$

Then $L^{\{p\}}(\eta, s) = \dfrac{1}{\Gamma(s)} \displaystyle\int_0^\infty f_\eta^{\{p\}}(t) t^s \cdot \frac{dt}{t}$, and thus

$$L^{\{p\}}(\eta, -n) = \Big(-\frac{d}{dt}\Big)^n \big(f_\eta^{\{p\}}\big)\Big|_{t=0}. \tag{3.4.3.1}$$

Comparing this with the equality in Lemma 3.4.2, we note that $(1+T)\dfrac{d}{dT} = \dfrac{d}{d\log(1+T)}$. Thus, if we set $1+T = e^{-t}$, then $(1+T)\dfrac{d}{dT} = -\dfrac{d}{dt}$. Moreover, for this change of variables, we see that $t=0$ corresponds to $T=0$. Inspired by this, we put

$$A_\eta(T) := \frac{\sum_{a=1}^{N-1} \eta(a)(1+T)^a}{1-(1+T)^N}, \quad \text{and} \quad A_\eta^{\{p\}}(T) := \frac{\sum_{\substack{a=1 \\ (a,Np)=1}}^{pN-1} \eta(a)(1+T)^a}{1-(1+T)^{pN}}$$

Then clearly, we have $A_\eta(e^{-t}-1) = f_\eta(t)$ and $A_\eta^{\{p\}}(e^{-t}-1) = f_\eta^{\{p\}}(e^{-t}-1)$.

Proposition 3.4.4. *Keep the notation as above, let μ_η (resp. $\mu_\eta^{\{p\}}$) denote the measure corresponding to $A_\eta(T)$ (resp. $A_\eta^{\{p\}}(T)$) under the Amice transform. Then*

(1) *μ_η is a p-adic measure in $\mathcal{D}_0(\mathbb{Z}_p,\mathbb{Z}_p)$ and $\mu_\eta^{\{p\}} = (1-\varphi\psi)(\mu_\eta)$. In particular, $\mu_\eta^{\{p\}}$ is supported on $\mathbb{Z}_p^\times$.*

(2) *For any integer $n \in \mathbb{Z}_{\geq 0}$,*

$$\int_{\mathbb{Z}_p^\times} x^n d\mu_\eta^{\{p\}}(x) = L^{\{p\}}(\eta,-n).$$

Proof. (1) To prove this rigorously, we need to make the following observation: both $A_\eta(T)$ and $A_\eta^{\{p\}}(T)$ lies in the field $\mathbb{Q}_p(\eta)(T)$ (intersected with $\mathbb{Z}_p[\![T]\!]$). We may define the φ- and ψ-operator on this field using the same formula. This field carries a different completion, namely $\mathbb{Q}_p(\eta)((1+T))$ (which is not comparable to $\mathbb{Z}_p[\![T]\!]$. Thus, it is enough to verify the equality $A_\eta^{\{p\}} = (1-\varphi\psi)(A_\eta)$ in this other completion. Now, we may write

$$A_\eta(T) = \frac{\sum_{a=1}^{N-1}\eta(a)(1+T)^a}{1-(1+T)^N} = \sum_{\substack{a\geq 1\\(a,N)=1}} \eta(a)(1+T)^a.$$

So $$\big(1-\varphi\psi\big)\big(A_\mu(T)\big) = \sum_{\substack{a\geq 1\\(a,pN)=1}} \eta(a)(1+T)^a = \frac{\sum_{\substack{a=1\\(a,Np)=1}}^{pN-1}\eta(a)(1+T)^a}{1-(1+T)^{pN}} = A_\eta^{\{p\}}(T).$$

By Amice transform, we have $\mu_\eta^{\{p\}} = (1-\varphi\psi)(\mu_\eta)$.

(2) We combine our earlier discussions together to deduce that

$$\int_{\mathbb{Z}_p^\times} x^n d_\eta^{\{p\}}(x) \overset{(3.4.2.1)}{=} \Big((1+T)\frac{d}{dT}\Big)^n \big(A_\eta^{\{p\}}\big)\Big|_{T=0} = \Big(-\frac{d}{dt}\Big)^n \big(f_\eta^{\{p\}}\big)\Big|_{t=0} \overset{(3.4.3.1)}{=} L^{\{p\}}(\eta,-n).$$

□

We have proved above that the p-adic measure $\mu_\eta^{\{p\}}$ satisfies the interpolation property (3.4.1.1) when η_p is trivial. In fact, the *same* p-adic measure $\mu_\eta^{\{p\}}$ also satisfies the interpolation properties for all n and all η_p. This then completes the proof of Theorem 3.4.1.

Proposition 3.4.5. *Keep the notation as above, for any nontrivial primitive character $\eta_p : (\mathbb{Z}/p^r\mathbb{Z})^\times \to \mathbb{Q}^{\mathrm{alg},\times} \xrightarrow{\iota_p} \overline{\mathbb{Q}}_p^\times$ and any $n \in \mathbb{Z}_{\geq 0}$, we have*

$$\int_{\mathbb{Z}_p^\times} \eta_p(x)x^n d\mu_\eta^{\{p\}}(x) = L^{\{p\}}(\eta\eta_p,-n). \tag{3.4.5.1}$$

Proof. Consider the power series

$$f_{\eta\eta_p}(t) := \frac{\sum_{a=1}^{p^rN-1}\eta\eta_p(a)e^{-at}}{1-e^{-p^rNt}} = \sum_{\substack{a\geq 1\\(a,pN)=1}} \eta\eta_p(a)e^{-at}.$$

Since η_p is nontrivial, we have

$$L(\eta\eta_p, s) = L^{\{p\}}(\eta\eta_p, s) = \frac{1}{\Gamma(s)}\int_0^\infty f_{\eta\eta_p}(t)t^s\cdot\frac{dt}{t} \quad\text{and}\quad L(\eta\eta_p, -n) = \Big(-\frac{d}{dt}\Big)^n\big(f_{\eta\eta_p}\big)\Big|_{t=0}.$$

Similar to above, we put

$$A_{\eta\eta_p}(T) := \frac{\sum_{a=1}^{p^rN-1}\eta\eta_p(a)(1+T)^a}{1-(1+T)^{p^rN}} = \sum_{\substack{a\geq 1\\(a,pN)=1}}\eta\eta_p(a)(1+T)^a.$$

It is clear that $\psi(A_{\eta\eta_p}(T)) = 0$. Thus, we have an equality

$$L(\eta\eta_p, -n) = \Big((1+T)\frac{d}{dT}\Big)^n\big(A_{\eta\eta_p}\big)\Big|_{T=0} = \int_{\mathbb{Z}_p^\times} x^n d\mu_{\eta\eta_p}(x) \tag{3.4.5.2}$$

for $\mu_{\eta\eta_p}$ the distribution corresponding to $A_{\eta\eta_p}(T)$ under the Amice transform.

Now, comparing (3.4.5.2) to (3.4.5.1), it remains to prove that

$$\mu_{\eta\eta_p} = \sum_{\substack{a=1\\p\nmid a}}^{p^r-1}\eta_p(a)\cdot\mathrm{Res}_{a+p^r\mathbb{Z}_p}(\mu_\eta^{\{p\}}).$$

But this is clear, because the Amice transform of the right hand side has formal expansion in $(1+T)$ given by

$$\sum_{\substack{a=1\\p\nmid a}}^{p^r-1}\eta_p(a)\cdot\Bigg(\sum_{\substack{i\geq 1\\(i,N)=1\\i\equiv a \bmod p^r}}\eta(i)(1+T)^i\Bigg) = \sum_{\substack{a\geq 1\\(a,pN)=1}}\eta\eta_p(a)(1+T)^a = A_{\eta\eta_p}(T).$$

The proposition is proved. □

Remark 3.4.6. (1) In fact, the interpolation conditions in Proposition 3.4.4 already determines the p-adic measure $\mu_\eta^{\{p\}}$, and the additional interpolation properties given by Proposition 3.4.5 signifies certain strong congruence among special values of Dirichlet L-functions for characters that are differed by a power of p. We will prove this in the exercises. One should think of this as some sort of miraculous p-adic congruences.

(2) One should interpret $\mathbb{Z}_p^\times$ as the Galois group $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$, the Galois group of maximal p-abelian extension of $\mathbb{Q}$. We will come back to this interpretation in the next lecture.

3.5. **Exercises.**

Exercise 3.5.1 (An explicit formula for ψ-operator)**.** Let p be a prime number. Recall that on $\mathbb{Z}_p[\![T]\!]$, we have defined an operator φ such that $\varphi(T) = (1+T)^p - 1$. There is a left inverse to φ, given as follows: each $F \in \mathbb{Z}_p[\![T]\!]$ can be written uniquely as $F = \sum_{i=0}^{p-1}(1+T)^i\varphi(F_i)$; then $\psi(F) = F_0$.

(1) Let ζ_p denote a primitive p-th root of unity. Prove that ψ-operator admits the following characterization: for $F \in \mathbb{Z}_p[\![T]\!]$, $\psi(F)$ is the unique power series in $\mathbb{Z}_p[\![T]\!]$ such that

$$\psi(F)((1+T)^p - 1) = \frac{1}{p}\sum_{i=0}^{p-1} F((1+T)\zeta_p^i - 1). \tag{3.5.1.1}$$

(2) Show that φ and ψ can be naturally extended to the p-adic completion of $\mathbb{Z}_p((T))$, denoted by $\mathbb{A}_{\mathbb{Q}_p}$.

(3) Show that $\psi\Big(\dfrac{1}{T}\Big) = \dfrac{1}{T}$. (One might find (3.5.1.1) useful, but there is a "better" proof without using it.)

Remark 3.5.2. (1) Without going into details, let us simply remark that the actions of φ, ψ, and $\Gamma \cong \mathbb{Z}_p^\times$ on $\mathbb{Z}_p[\![T]\!]$ and their extensions to $\mathbb{A}_{\mathbb{Q}_p}$ defines the most important ground ring for (φ, Γ)-modules; this is a very useful tool in studying p-adic Hodge theory of local fields. We may encounter more of these constructions in the future (if we decide to introduce Coleman's power series).

(2) The right hand side of formula (3.5.1.1) may be viewed as taking the trace from $\mathbb{Z}_p[\![T]\!]$ to $\varphi(\mathbb{Z}_p[\![T]\!])$.

Exercise 3.5.3 ("Miraculous congruence" encoded in p-adic L-functions)**.** Assume $p \geq 3$ for simplicity. We have constructed p-adic Dirichlet L-functions as p-adic measures on $\mathbb{Z}_p^\times$ that interpolates special values of (p-modified) Dirichlet L-functions. It is natural to ask: is the p-adic Dirichlet L-function uniquely determined by these interpolation values? In fact, the answer is that these values "overdetermine" the p-adic L-functions. (We will discuss this in lectures at a later stage.) Assume that $p \geq 3$ is an odd prime number.

(1) Let G be a general profinite group and let $\chi : G \to R^\times$ be a continuous p-adic character with values in a p-adically complete ring R, then it induces a continuous ring homomorphism $\tilde{\chi} : \mathbb{Z}_p[\![G]\!] \to R$. Alternatively, χ can be viewed as a R-valued function on G, so one can integrate against a p-adic measure on G.

Prove that we have the following commutative diagram

$$\begin{tikzcd} \mathbb{Z}_p[\![G]\!] \arrow[rr, "\cong"] \arrow[dr, "\tilde{\eta}"'] & & \mathcal{D}_0(G, \mathbb{Z}_p) \arrow[dl, "\mu \mapsto \int_G \eta(g)d\mu(g)"] \\ & R & \end{tikzcd}$$

(2) Write $\Delta := \mathbb{F}_p^\times$, which may be viewed as a subgroup of $\mathbb{Z}_p^\times$ via Teichmüller character ω. Give an canonical isomorphism $\Phi : \mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!] \cong \mathbb{Z}_p[\Delta] \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\![X]\!]$, so that $X = [\exp(p)] - 1$, where $\exp(p) = 1 + p + \frac{p^2}{2!} + \cdots$ is the formal expansion.

(3) Let $\eta : (\mathbb{Z}/p^r\mathbb{Z})^\times \to \overline{\mathbb{Q}}_p^\times$ be a finite character and let $n \in \mathbb{Z}_{\geq 0}$; we may form the p-adic character

$$\begin{aligned} \chi_{\eta,n} : \mathbb{Z}_p^\times &\longrightarrow \overline{\mathbb{Q}}_p^\times \\ a &\longmapsto \eta(a)a^n. \end{aligned}$$

If we denote by $\bar{\chi}_{\eta,n}$ the restriction of $\chi_{\eta,n}$ to Δ, then for any $\mu \in \mathcal{D}_0(\mathbb{Z}_p^\times, \mathbb{Z}_p)$,

$$\int_{\mathbb{Z}_p^\times} \eta(x)x^n d\mu(x) = \Phi(\mu)|_{\Delta=\bar{\chi}_{\eta,n},\, T=\chi_{\eta,n}(\exp(p))-1}.$$

(4) Prove that two p-adic measures $\mu_1, \mu_2 \in \mathcal{D}_0(\mathbb{Z}_p^\times, \mathbb{Z}_p)$ are equal if for any $n \in \mathbb{Z}_{\geq 0}$,

$$\int_{\mathbb{Z}_p^\times} x^n d\mu_1(x) = \int_{\mathbb{Z}_p^\times} x^n d\mu_2(x).$$

(Hint: Show that the difference $\mu_1 - \mu_2$ is divisible by some infinite product.)

(5) Prove that two p-adic measures $\mu_1, \mu_2 \in \mathcal{D}_0(\mathbb{Z}_p^\times, \mathbb{Z}_p)$ are equal if for a *fixed* $n \in \mathbb{Z}_{\geq 0}$ but for all finite characters $\eta : (\mathbb{Z}/p^r\mathbb{Z})^\times \to \overline{\mathbb{Q}}_p^\times$ for all r, we have

$$\int_{\mathbb{Z}_p^\times} \eta(x)x^n d\mu_1(x) = \int_{\mathbb{Z}_p^\times} \eta(x)x^n d\mu_2(x).$$

Exercise 3.5.4. (Kubota–Leopoldt p-adic L-function) In the second and the third lectures, we have constructed the p-adic Dirichlet L-function when the (tame) Dirichlet character η is nontrivial. For the case when $\eta = \mathbf{1}$, we should also construct the corresponding p-adic zeta-function, traditionally called the Kubota–Leopoldt p-adic L-function. Unfortunately, this will not be a p-adic measure on $\mathbb{Z}_p^\times$, but only a "quasi-measure", which is philosophically related to that ζ-function has a pole at $s = 1$ (so should the p-adic zeta have). For this, we need some technical maneuver.

Pick $a \in \mathbb{Z}_{>1}$ prime to p. Consider

$$\zeta_a(s) := (1 - a^{1-s}) \cdot \zeta(s) = \sum_{\substack{n\geq 1\\ (n,a)=1}} \frac{1}{n^s} - a \cdot \sum_{\substack{n\geq 1\\ a|n}} \frac{1}{n^s}$$

$$A_a(T) = (1 - a\gamma_a)\Big(\frac{1+T}{1-(1+T)}\Big) = \frac{1+T}{1-(1+T)} - a \cdot \frac{(1+T)^a}{1-(1+T)^a},$$

where $\gamma_a \in \Gamma = \mathbb{Z}_p^\times$ is the element corresponds to $a \in \mathbb{Z}_p^\times$, which acts on $\mathbb{Z}_p[\![T]\!]$ by sending T to $(1+T)^a - 1$.

(1) Show that $A_a(T) \in \mathbb{Z}_p[\![T]\!]$ defines a p-adic measure; so is $A_a^{\{p\}}(T) := (1-\varphi\psi)(A_a(T))$.

Define $\mu_a^{\{p\}}$ to be the p-adic measure associated to $A_a^{\{p\}}(T)$ via Amice transform. For any primitive character $\eta : (\mathbb{Z}/p^r\mathbb{Z})^\times \to \mathbb{Q}^{\mathrm{alg},\times}$, define

$$L^{\{p\}}(\eta, s) = (1 - \eta(p)p^{-s}) \cdot L(\eta, s).$$

$$L_a^{\{p\}}(\eta, s) = (1 - a^{1-s}) \cdot L^{\{p\}}(\eta, s) = \sum_{\substack{n\geq 1\\ (n,ap)=1}} \frac{1}{n^s} - a \cdot \sum_{\substack{n\geq 1\\ (n,p)=1}} \frac{1}{(an)^s}$$

(2) Show that for any character η and any $n \in \mathbb{Z}_{\geq 0}$, we have

$$\int_{\mathbb{Z}_p^\times} \eta(x)x^n d\mu_a^{\{p\}}(x) = L^{\{p\}}(\eta, -n).$$

(3) Recall the identification $\mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!] \cong \mathbb{Z}_p[\Delta] \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\![X]\!]$. We may define the *Kubota–Leopoldt p-adic L-function* to be the element

$$\mu_{\mathrm{KL}} := \frac{\mu_a^{\{p\}}}{(1 - a[\gamma_a])} \in \mathbb{Z}_p[\Delta] \otimes \frac{1}{X}\mathbb{Z}_p[\![X]\!].$$

Sometimes, this is called a *pseudo-measure*; show that μ_{KL} is independent of the choice of $a \in \mathbb{Z}_p^\times$. (Hint: We need only to prove that $(1-b\gamma_b)(\mu_a^{\{p\}}) = (1-a\gamma_a)(\mu_b^{\{p\}})$ for two different $a, b \in \mathbb{Z}_{>1}$ relatively prime to p. One can make use of Exercise 3.5.3(4)(5).)

Remark 3.5.5. Our definition of pseudo-measure slightly differs from that of Jacinto–Williams' note, who shifted the p-adic Kubota–Leopolds L-function so that the pole is at $s = 0$.

Exercise 3.5.6 (A more classical version of p-adic L-function)**.** Historically, there is also an old version of p-adic L-function which is really just p-adic functions. In this exercise, we recover the classical p-adic L-function from the p-adic measures, and we will see that the p-adic measures contains stronger congruence relations than classical p-adic L-functions.

(To avoid talking about pseudo-measures, we again work with p-adic Dirichlet L-functions.) Let η be a primitive Dirichlet character of conductor N (with $p \nmid N$). We have constructed a p-adic measure $\mu_\eta^{\{p\}}$ such that

$$\int_{\mathbb{Z}_p^\times} x^n d\mu_\eta^{\{p\}}(x) = L^{\{p\}}(\eta, -n).$$

(This measure also interpolates Dirichlet L-functions for varying the character at p; we will not use it here.)

We are interested in understanding the p-adic function $\zeta_{p,i}$ on $\mathbb{Z}_p$ for $i = 0, 1, \ldots, p-2$, defined by for $s \in \mathbb{Z}$ such that $s \equiv i \bmod p-1$,

$$\zeta_{p,i}(s) := \int_{\mathbb{Z}_p^\times} x^s d\mu_\eta^{\{p\}}(x) = L^{\{p\}}(\eta, -s).$$

(1) Show that $\zeta_{p,i}(s)$ extends naturally to a continuous function on $s \in \mathbb{Z}_p$. (So far, this is weaker than a function on $s \in \mathcal{O}_{\mathbb{C}_p}$.)

Now we study these functions $\zeta_{p,i}$ more carefully. Abstractly by Exercise 3.5.3, we may view $\mu_\eta^{\{p\}}$ as an element in $\mathbb{Z}_p[\Delta] \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\![X]\!]$, where $X = [\exp(p)] - 1$. (Here we view $\Delta = \mathbb{F}_p^\times$ as a subgroup of $\mathbb{Z}_p^\times$ via the Teichmüller character ω.) For $i = 0, \ldots, p-2$, write $\mu_{\eta,i}(X) \in \mathcal{O}[\![X]\!]$ for the image of $\mu_\eta^{\{p\}}$ under the map $\Delta \to \mathbb{Z}_p^\times$ sending x to $\omega(x)^i$.

(2) Show that (formally)

$$\zeta_{p,i}(s) = \mu_{\eta,i}(\exp(ps)). \tag{3.5.6.1}$$

(3) From (2), deduce that $\zeta_{p,i}(s)$ extends to a p-adic analytic function for $s \in p^{-\frac{p-2}{p-1}}\mathfrak{m}_{\mathbb{C}_p}$.

Remark 3.5.7. One sees from this exercise that the classical p-adic L-function only captures part of the information provided. Even knowing the convergence of $\zeta_{p,i}(s)$ for $s \in p^{-\frac{p-2}{p-1}}\mathfrak{m}_{\mathbb{C}_p}$, it is far from enough to deduce the integrality of $\mu_\eta^{\{p\}}$. For more discussion in this direction, see the post `https://mathoverflow.net/questions/435265/why-p-adic-measures`.

4.1. L-functions associated to Galois representations.

Notation 4.1.1. Let F be a number field. Denote

$$\mathsf{M}_F = \{\text{all places of } F\} \supseteq \mathsf{M}_{F,f} = \{\text{finite places of } F\}.$$

For each $v \in \mathsf{M}_{F,f}$, write $\mathcal{O}_v$ for the ring of integers of F_v, and ϖ_v a uniformizer. Put $k_v := \mathcal{O}_v/(\varpi_v)$ for the residue field and $\mathsf{q}_v := \# k_v$. Write I_v for the inertia subgroup of Gal_{F_v} and $\mathrm{Gal}_{F_v}/\mathrm{I}_v \cong \mathrm{Gal}_{k_v}$. Write ϕ_v for a geometric Frobenius, i.e. an element in Gal_{F_v} whose image in Gal_{k_v} acts on $\overline{k}_v$ by sending $x \mapsto x^{1/\mathsf{q}_v}$.

If $S \subseteq \mathsf{M}_F$ is a finite set of places, we write F^S for the maximal extension of F that is unramified outside S, and $\mathrm{Gal}_{F,S} := \mathrm{Gal}(F^S/F)$ for the Galois group.

Write $\mathbb{Q}^{\mathrm{alg}} \subseteq \mathbb{C}$ for the algebraic closure of $\mathbb{Q}$. Fix a prime p and an embedding $\mathbb{Q}^{\mathrm{alg}} \hookrightarrow \overline{\mathbb{Q}}_p$.

Notation 4.1.2. A continuous representation $\rho : \mathrm{Gal}_F \to \mathrm{GL}_n(\overline{\mathbb{Q}}_p) = \mathrm{GL}(V)$ is called "nice" if the following condition holds.

(1) ρ is unramified outside of a finite subset $S \subseteq \mathsf{M}_F$ of places. (Without loss of generality, S contains all archimedean places and p-adic places.) We may write the representation as $\rho : \mathrm{Gal}_{F,S} \to \mathrm{GL}_n(\overline{\mathbb{Q}}_p)$ instead.

(2) For every place $v \in \mathsf{M}_{F,f}$ that is not p-adic, the characteristic polynomial of the geometric Frobenius $\rho(\phi_v)$ acting on V^{I_v} belongs to $\mathbb{Q}^{\mathrm{alg}}[x]$.

(3) For a p-adic place v of F, $\rho_v := \rho|_{\mathrm{Gal}_{F_v}}$ is De Rham and the action of $\rho(\phi_v)$ on $\mathbb{D}_{\mathrm{pst}}(\rho_v)^{\mathrm{I}_v}$ has characteristic polynomial in $\mathbb{Q}^{\mathrm{alg}}[x]$. (Here $\mathbb{D}_{\mathrm{pst}}(-)$ is a p-adic Hodge theory

Remark 4.1.3. We will not discuss now in details of the question where to find "nice" Galois representations; they appear naturally in the étale cohomology of varieties over number fields. We will come back to this in future lectures.

Definition 4.1.4. Let $\rho : \mathrm{Gal}_F \to \mathrm{GL}_n(\overline{\mathbb{Q}}_p)$ be a "nice" continuous representation. For each $v \in \mathsf{M}_{F,f}$, define the local L-factor

$$L_v(\rho_v, s) = \begin{cases} \dfrac{1}{\det\big(\mathbf{1} - \rho_v(\phi_v)\mathsf{q}_v^{-s};\ V^{\mathrm{I}_v}\big)} & \text{if } v \text{ is not } p\text{-adic,} \\ \dfrac{1}{\det\big(\mathbf{1} - \phi_v\mathsf{q}_v^{-s};\ \mathbb{D}_{\mathrm{pst}}(\rho_v)^{\mathrm{I}_v}\big)} & \text{if } v \text{ is } p\text{-adic.} \end{cases}$$

We put

$$L(\rho, s) = \prod_{v \in \mathsf{M}_{F,f}} L_v(\rho_v, s),$$

if the product converges (when $\mathrm{Re}(s) \gg 0$).

Remark 4.1.5. (1) One expects a meromorphic continuation of $L(\rho, s)$; and functional equations relating $L(\rho, s)$ with $L(\rho^\vee, 1-s)$. But this is a very difficult question. The solution to this question is to first associate an automorphic representation Π_ρ to ρ, and use the analytic properties of Π_ρ to deduce the properties of $L(\rho, s)$.

(2) When ρ has finite image, we call ρ an *Artin representation*. In this case, we may ignore the p-adic Hodge theory construction of $\mathbb{D}_{\mathrm{pst}}(-)$ and simply use $\rho_v^{\mathrm{I}_v}$ in Notation 4.1.2(3).

(3) When ρ has finite image, the meromorphic continuation of $L(\rho, s)$ can be proved using the meromorphic continuations of finite Hecke characters and Brauer induction theorem.

We now list a few properties of the construction of general L-functions.

Lemma 4.1.6 (Comparison with Dirichlet L-function)**.** *Let η be a primitive Dirichlet character of conductor N. Then we may associate a Galois representation*

$$\tilde{\eta} : \mathrm{Gal}_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\eta} \mathbb{C}^\times.$$

We have $L(\tilde{\eta}, s) = L(\eta^{-1}, s)$.

Proof. To compare the two L-functions, we make explicit the map $\tilde{\eta}$:

$$\begin{array}{rcccc} \tilde{\eta} : \mathrm{Gal}_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) & \cong & (\mathbb{Z}/N\mathbb{Z})^\times & \xrightarrow{\quad\eta\quad} & \mathbb{C}^\times \\ \text{geometric Frobenius } \phi_p & \longmapsto & p^{-1} & \longmapsto & \eta(p)^{-1}. \end{array}$$

Then we can make computation:

$$L(\tilde{\eta}, s) = \prod_{p \nmid N} \frac{1}{1 - \tilde{\eta}(\phi_p) p^{-s}} = \prod_{p \nmid N} \frac{1}{1 - \eta(p)^{-1} p^{-s}} = L(\eta^{-1}, s).$$

$\square$

Remark 4.1.7. Note that conversely, we can associate a primitive Dirichlet character to a finite Galois character $\tilde{\eta}$. Somehow, for $\tilde{\eta}$, the primitive condition is not needed, and we may read off the conductor from the "ramification data" of $\tilde{\eta}$.

Notation 4.1.8. Write μ_{p^∞} for the group of all p-power roots of unity. We denote the p-adic cyclotomic character

$$\chi_{\mathrm{cyc}} : \mathrm{Gal}_F \twoheadrightarrow \mathrm{Gal}\big(F(\mu_{p^\infty})/F\big) \hookrightarrow \mathbb{Z}_p^\times,$$

characterized by the properties that, for any p-power roots of unity ζ and any $\sigma \in \mathrm{Gal}(F(\mu_{p^\infty})/F)$, we have

$$\sigma(\zeta) = \zeta^{\chi_{\mathrm{cyc}}(\sigma)}.$$

In particular, for a place $v \nmid p$, $\chi_{\mathrm{cyc}}(\phi_v) = \mathsf{q}_v^{-1}$.

Sometimes, we abbreviate χ_{cyc} into $\mathbb{Z}_p(1)$ or $\mathbb{Q}_p(1)$. Put $\mathbb{Z}_p(n) := \mathbb{Z}_p(1)^{\otimes n}$ for $n \geq 0$ and $\mathbb{Z}_p(-n) = \mathrm{Hom}(\mathbb{Z}_p(n), \mathbb{Z}_p)$.

For a representation V of Gal_F as above, define $V(n) := V \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(n)$.

Lemma 4.1.9. *The L-functions for V and for $V(n)$ are related as follows:*

$$L(V(n), s) = L(V, n + s).$$

Proof. We compute each finite L-factor: for a finite place $v \nmid p$

$$L_v(V(n), s) = \frac{1}{\det\big(\mathbf{1} - \phi_v \mathsf{q}_v^{-s};\ V(n)\big)} = \frac{1}{\det\big(\mathbf{1} - \phi_v \mathsf{q}_v^{-n} \mathsf{q}_v^{-s};\ V\big)} = L_v(V, n + s).$$

Taking product, we get $L(V(n), s) = L(V, s + n)$. $\square$

4.1.10. *Reinterpretation of p-adic Dirichlet L-functions.* In view of L-functions associated to Galois representations, we give the following reinterpretation of the p-adic Dirichlet L-functions.

Recall that for a primitive Dirichlet character $\eta : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{Q}^{\mathrm{alg},\times}$ with $p \nmid N$ and $N \neq 1$, we may associate a Galois representation $\tilde{\eta} : \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\eta} \mathbb{Q}^{\mathrm{alg},\times}$.

Theorem 3.4.1 says that there exists a p-adic measure $\mu_\eta^{\{p\}} \in \mathcal{D}_0(\mathbb{Z}_p^\times, \mathcal{O})$ such that, for any finite character $\eta_p : (\mathbb{Z}/p^r\mathbb{Z})^\times \to \mathbb{Q}^{\mathrm{alg},\times} \subset \overline{\mathbb{Q}}_p^\times$ and any $n \in \mathbb{Z}_{\geq 0}$, we have

$$\int_{\mathbb{Z}_p^\times} \eta_p(x) x^n d\mu_\eta^{\{p\}}(x) = L^{\{p\}}(\eta\eta_p, -n).$$

On the other hand, for each η_p and n we may form a p-adic representation

$$\chi_{\eta_p,n} := \tilde{\eta}_p \chi_{\mathrm{cyc}}^n : \mathrm{Gal}(\mathbb{Q}(\zeta_N)(\mu_{p^\infty})/\mathbb{Q}) \to \overline{\mathbb{Q}}_p^\times,$$

where $\tilde{\eta}_p$ is the Galois representation of $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$ associated to η_p.

In view of Lemma 4.1.6, we have

$$L^{\{p\}}(\eta\eta_p, -n) = L^{\{p\}}(\tilde{\eta}^{-1}\tilde{\eta}_p^{-1}, -n) = L^{\{p\}}(\tilde{\eta}^{-1}\tilde{\eta}_p^{-1}\chi_{\mathrm{cyc}}^{-n}, 0) = L^{\{p\}}(\tilde{\eta}^{-1}\chi_{\eta_p,n}^{-1}, 0).$$

So maybe the correct formulation of p-adic Dirichlet L-function is: for a nontrivial Galois representation $\tilde{\eta} : \mathrm{Gal}_{\mathbb{Q}} \to \mathbb{Q}^{\mathrm{alg},\times}$ unramified at p (associated to a primitive Dirichlet character η of prime-to-p conductor), the p-adic L-function associated to $\tilde{\eta}$ is

$$\mu_{\tilde{\eta}} := \iota^*\big(\mu_{\eta^{-1}}^{\{p\}}\big) \in \mathcal{D}_0(\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}), \mathcal{O}),$$

where $\iota : \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$ is $x \mapsto x^{-1}$. The interpolation property can be written as: for a p-adic character $\chi : \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \to \overline{\mathbb{Q}}_p^\times$ of the form $\tilde{\eta}_p\chi_{\mathrm{cyc}}^{-n}$ with $\tilde{\eta}_p$ a finite character and $n \geq 0$,

$$\int_{\mathbb{Z}_p^\times} \chi(x) d\mu_{\tilde{\eta}}(x) = L(\tilde{\eta}\chi, 0).$$

Properties 4.1.11. The L-functions associated to Galois representations enjoy the following two additional properties:

(1) If $\rho = \rho_1 \oplus \rho_2$, then $L(\rho, s) = L(\rho_1, s) \cdot L(\rho_2, s)$.

(2) If $\rho : \mathrm{Gal}_F \to \mathrm{GL}_n(\overline{\mathbb{Q}}_p)$ is a "nice" representation, then $\mathrm{Ind}_{\mathrm{Gal}_F}^{\mathrm{Gal}_{\mathbb{Q}}} \rho$ is a "nice" representation of $\mathrm{Gal}_{\mathbb{Q}}$, then

$$L(\rho, s) = L\big(\mathrm{Ind}_{\mathrm{Gal}_F}^{\mathrm{Gal}_{\mathbb{Q}}} \rho, s\big).$$

Notation 4.1.12. For an ideal $\mathfrak{a} \subseteq \mathcal{O}_F$, write $||\mathfrak{a}|| := \#(\mathcal{O}_F/\mathfrak{a})$.

Example 4.1.13. Consider the trivial representation $\mathbf{1}_F : \mathrm{Gal}_F \to \mathbb{Q}_p^\times$, the associated L-function is called the *Dedekind zeta function*:

$$\zeta_F(s) = L(\mathbf{1}_F, s) = \prod_{\mathfrak{p} \text{ prime ideal}} \frac{1}{1 - ||\mathfrak{p}||^{-s}} = \sum_{\mathfrak{a} \neq 0 \text{ ideal}} \frac{1}{||\mathfrak{a}||^s} \qquad (\mathrm{Re}(s) > 1).$$

A special case is when $F = \mathbb{Q}(\zeta_N)$. In this case,

$$\mathrm{Ind}_{\mathrm{Gal}_F}^{\mathrm{Gal}_{\mathbb{Q}}} \mathbf{1}_F \cong \bigoplus_{\eta : \mathrm{Gal}(F/\mathbb{Q}) \to \mathbb{C}^\times} \eta,$$

(where the right hand side is the same as the direct sum over all primitive Dirichlet characters of conductor M dividing N.) We have

$$\zeta_F(s) = \prod_{\eta:(\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times} L(\eta, s).$$

4.2. **Analytic class number formula.**

4.2.1. *Functional equation for Dedekind ζ-function $\zeta_F(s)$.* Assume that F has r_1 real embeddings $\tau_1, \dots, \tau_{r_1}$ and r_2 pairs of complex embeddings $\tau_{r_1+1}, \bar{\tau}_{r_1+1}, \dots, \tau_{r_1+r_2}, \bar{\tau}_{r_1+r_2}$. Recall that $\Gamma_\mathbb{R}(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})$ and $\Gamma_\mathbb{C}(s) = 2(2\pi)^{-s}\Gamma(s)$. Define the complete Dedekind zeta-function to be

$$\Lambda_F(s) := \Gamma_\mathbb{R}(s)^{r_1}\Gamma_\mathbb{C}(s)^{r_2} \cdot \zeta_F(s).$$

Then $\Lambda_F(s)$ admits a meromorphic continuation satisfying a functional equation

$$\Lambda_F(s) = |\Delta_F|^{\frac{1}{2}-s}\Lambda_F(1-s),$$

where Δ_F is the discriminant of $F/\mathbb{Q}$.

Theorem 4.2.2 (Analytic class number formula)**.** *If F is a number field, then the Dedekind zeta function $\zeta_F(s)$ has a simple pole at $s = 1$ and satisfies*

$$\lim_{s\to 1}(s-1)\zeta_F(s) = \frac{2^{r_1}(2\pi)^{r}_{2} \cdot \mathrm{Reg}_F \cdot h_F}{w_F \cdot |\Delta_F|^{\frac{1}{2}}},$$

where $h_F = \#\mathrm{Cl}(\mathcal{O}_F)$ is the class number of F, $w_F = \#\mu(F)$ with $\mu(F)$ being the set of roots of unity in F, Reg_F is the regulator of F (with precise definition below).

We will give the proof of this theorem in the case when F is a quadratic extension of $\mathbb{Q}$, and leave the general proof as an exercise.

Definition 4.2.3. Let F be a number field as above. The Dirichlet unit theorem says that $\mathcal{O}_F^\times \simeq \mu(F) \times \mathbb{Z}^{r_1+r_2-1}$. The *regulator map* is given by

$$\begin{aligned} \mathrm{reg}_F : \mathcal{O}_F^\times &\longrightarrow (\mathbb{R}^{r_1+r_2})^{\mathrm{sum}=0} \\ u &\longmapsto \big(c_i \log|\tau_i(u)|\big)_{i=1,\dots,r_1+r_2} \end{aligned} \qquad \text{where } c_i = \begin{cases} 1 & \text{if } \tau_i \text{ is real} \\ 2 & \text{if } \tau_i \text{ is complex.} \end{cases}$$

If $u_1, \dots, u_{r_1+r_2-1}$ is a set of generators of $\mathcal{O}_F^\times/\mu(F)$, then

$$\mathrm{Reg}_F = \Big| \det\big(c_i \log\big|\tau_i(u_j)\big|\big)_{i,j=1,\dots,r_1+r_2-1} \Big|$$

(This is equivalent to, in an imprecise way, the volume of $(\mathbb{R}^{r_1+r_2})^{\mathrm{sum}=0}/\mathrm{reg}_F(\mathcal{O}_F^\times)$.

We think maybe a better formulation of the analytic class number formula is the following.

Proposition 4.2.4 (Analytic class number formula at $s = 0$)**.** *We have*

$$\lim_{s\to 0} s^{r_1+r_2-1}\zeta_F(s) = -\frac{\mathrm{Reg}_F \cdot h_F}{w_F}.$$

This follows from Theorem 4.2.2 and the functional equation for Dedekind zeta function. We leave the details to Exercise 4.4.1(1).

4.3. **Proof of analytic class number formula in the quadratic case.** A more advanced proof makes use of Tate's thesis, but we present here a simpler proof.

4.3.1. *Case of $\zeta_{\mathbb{Q}}(s)$.* Consider $s \to 1^+$, up to a bounded number, we may replace the infinite sum by integration:

$$\zeta_{\mathbb{Q}}(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \int_1^{\infty} \frac{1}{x^s} dx + O(1) = \frac{x^{1-s}}{1-s}\Big|_{x=1}^{x=\infty} + O(1) = \frac{1}{1-s} + O(1).$$

4.3.2. *Setup.* We will only treat the case when F is quadratic (separating the real quadratic case and the imaginary quadratic case), and the general case may be viewed as a generalization of the two cases.

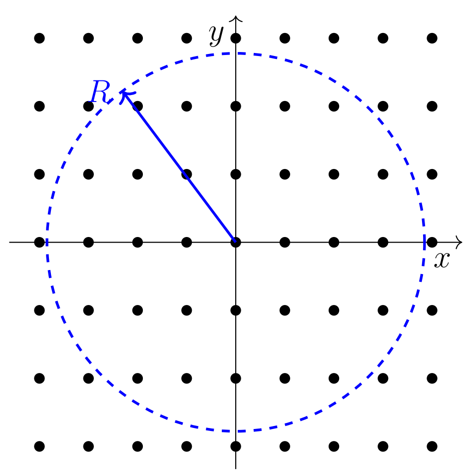
We write $[\mathfrak{c}]$ to denote a class in $\mathrm{Cl}(\mathcal{O}_F)$. Then we have

$$\zeta_F(s) = \sum_{\mathfrak{a} \neq 0 \text{ ideal}} \frac{1}{||\mathfrak{a}||^s} = \sum_{[\mathfrak{c}] \in \mathrm{Cl}(\mathcal{O}_F)} \sum_{\mathfrak{a} \in [\mathfrak{c}]} \frac{1}{||\mathfrak{a}||^s}. \tag{4.3.2.1}$$

4.3.3. *Proof of class number formula when F is imaginary quadratic.* We first compute the case when $[\mathfrak{c}]$ is the set of principal ideals, which corresponds to $\big(\mathcal{O}_F \backslash \{0\}\big)/\mathcal{O}_F^{\times}$. (In this case $\mathcal{O}_F^{\times} = \mu(F)$.)

$$\sum_{\mathfrak{a} \text{ principal ideal}} \frac{1}{||\mathfrak{a}||^s} = \frac{1}{w_F} \sum_{a \in \mathcal{O}_F \backslash \{0\}} \frac{1}{|\mathrm{Nm}(a)|^s}.$$

We view $\mathcal{O}_F$ as a lattice in $\mathbb{C}$, then the number of lattice of points with norm between R^2 and $(R+\delta_R)^2$ is $\frac{2}{|\Delta_F|^{1/2}} \cdot 2\pi R \cdot \delta_R$. (It is easy to test this in the case when $\mathbb{Z}[\sqrt{-D}]$ which has discriminant $-4D$ and density of lattice points $\sqrt{D}$.)



So we have

$$\frac{1}{w_F}\sum_{a\in\mathcal{O}_F\backslash\{0\}}\frac{1}{|\mathrm{Nm}(a)|^s}=\frac{1}{w_F}\int_{R=1}^{\infty}\frac{2}{|\Delta_F|^{1/2}}\big(2\pi R+O(1)\big)\cdot\frac{1}{R^{2s}}dR$$
$$=\frac{2}{w_F|\Delta_F|^{1/2}}\cdot\int_{R=1}^{\infty}\Big(\frac{2\pi}{R^{2s-1}}+\frac{O(1)}{R^{2s}}\Big)dR$$
$$=\frac{2}{w_F|\Delta_F|^{1/2}}\cdot\Big(\frac{2\pi}{2-2s}R^{2-2s}\Big|_{R=1}^{\infty}+\frac{1}{1-2s}R^{1-2s}\Big|_{R=1}^{\infty}\Big)$$
$$=\frac{2}{w_F|\Delta_F|^{1/2}}\cdot\frac{\pi}{s-1}+O(1).$$

Now for a general ideal class $[\mathfrak{c}]$, fix an ideal $I_\mathfrak{c}\in[\mathfrak{c}]$. Then every genuine ideal in $[\mathfrak{c}]$ takes the form of $I_c\cdot(\alpha)$ for $\alpha\in I_\mathfrak{c}^{-1}\backslash\{0\}$. So by the same argument as above, we have

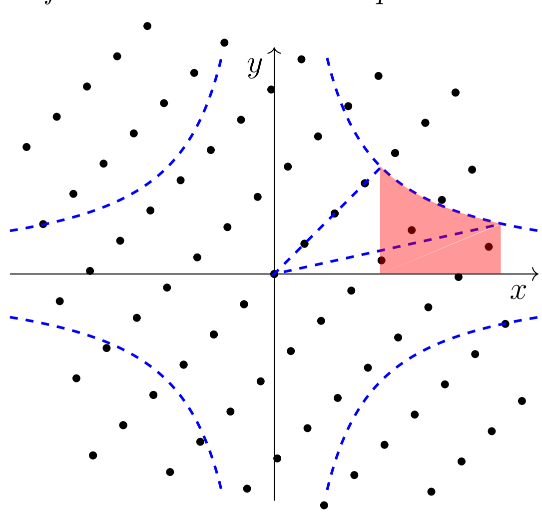
$$\sum_{\mathfrak{a}\in[\mathfrak{c}]}\frac{1}{||\mathfrak{a}||^s}=\sum_{\alpha\in I_\mathfrak{c}^{-1}\backslash\{0\}}\frac{1}{||I_\mathfrak{c}||^s\cdot(N\alpha)^s}$$
$$=\frac{1}{||I_\mathfrak{c}||}\cdot\frac{2}{w_F|\Delta_F|^{1/2}}\cdot\frac{\pi}{s-1}\cdot||I_\mathfrak{c}||+O(1)$$
$$=\frac{2}{w_F|\Delta_F|^{1/2}}\cdot\frac{\pi}{s-1}+O(1).$$

Combining all above, we see that

$$\zeta_F(s)=\sum_{[\mathfrak{c}]\in\mathrm{Cl}(\mathcal{O}_F)}\sum_{\mathfrak{a}\in[\mathfrak{c}]}\frac{1}{||\mathfrak{a}||^s}=h_F\cdot\frac{2\pi}{w_F|\Delta_F|^{1/2}}\cdot\frac{1}{s-1}+O(1).$$

This proves Theorem 4.2.2 when F is an imaginary quadratic field.

4.3.4. *Proof of class number formula when F is real quadratic.*



4.4. **Exercises.**

Exercise 4.4.1 (Volume of ideles class group versus residue of Dedekind zeta values)**.** Let F be a number field with r_1 real embeddings and r_2 pairs of complex embeddings. Let $\mathbb{A}_F^\times$

be the group of ideles and $\mathbb{A}_F^{\times,1} := \{x \in \mathbb{A}_F^\times \mid |x| = 1\}$ be the subgroup of norm one elements. We have stated (and proved in the quadratic case) of the analytic class number formula, for the Dedekind zeta function $\zeta_F(s)$ at $s = 1$:

$$\lim_{s\to 1}(s-1)\zeta_F(s) = \frac{2^{r_1}(2\pi)^{r_2}\cdot h_F \mathrm{Reg}_F}{w_F\sqrt{|\Delta_F|}}, \tag{4.4.1.1}$$

where h_F is the class number, Reg_F is the regulator for units of F, w_F is the number of roots of unity contained in F, and Δ_F is the discriminant of F.

(1) Using the functional equation of Dedekind zeta function to deduce from (4.4.1.1) the following analytic class number formula at $s = 0$:

$$\lim_{s\to 0} s^{-r_1-r_2+1}\zeta_F(s) = -\frac{h_F\cdot \mathrm{Reg}_F}{w_F}.$$

(2) Show that the right hand side of (4.4.1.1) can be interpreted as $\mathrm{Vol}(\mathbb{A}_F^{\times,1}/F^\times)$, if we provide the Haar measure on $\mathbb{A}_F^{\times,1}$ so that under the product decomposition $\mathbb{A}_F^\times = \mathbb{A}_F^{\times,1}\times\mathbb{R}^\times$ (where $\mathbb{R}^\times$ is provided with the measure $\frac{dx}{x}$) admits the following Haar measure:
- at a real place v of F, the Haar measure on $F_v^\times$ is $\frac{dx}{|x|}$,
- at a complex place v of F, the Haar measure on $F_v^\times \simeq \mathbb{C}^\times$ is $\frac{2dx\wedge dy}{|x^2+y^2|} = \frac{2drd\theta}{r}$,
- at a p-adic place v of F with different ideal $\mathfrak{d}_v \subseteq F_v$, the Haar measure on $F_v^\times$ is so that volume of $\mathcal{O}_{F_v}^\times$ is $||\mathfrak{d}_v||^{-\frac{1}{2}}$, where $||\mathfrak{d}_v|| = \#(\mathcal{O}_{F_v}/\mathfrak{d}_v)$.

5. Iwasawa main conjecture

Exercise I

References

[Col] P. Colmez, Fontaine's rings and p-adic L-functions, *notes at Tsinghua University*.

Solution to exercises