Special Values

Nir Elber

Spring 2025

Contents

1 Special Values of Dirichlet L-Functions

This talk was given by Rui. Roughly speaking, the style of these sorts of special values results is that someone observes some equalities, then one works out examples, we make a general conjecture, and eventually it is proven.

1.1 Some Examples

Let's begin by discussing the simplest L-function: the Riemann ζ-function.

Definition 1. The *Riemann ζ-function* ζ is defined by the series

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

for $s \in \mathbb{C}$ such that $\operatorname{Re} s > 1$.

Example 2. Here is what is known about some small special values. Euler showed that $\zeta(s) = \frac{\pi^2}{6}$, and Apéry showed that $\zeta(3)$ is irrational.

Remark 3. In general, there is a conjecture that the values $\{\pi, \zeta(3), \zeta(5), \ldots\}$ forms an algebrically independent set. Roughly speaking, this is expected by the Grothendieck period conjecture.

Today, we will be happy working in only slightly larger generality, with Dirichlet L-functions.

Definition 4 (Dirichlet character)**.** Fix a positive integer N. Then a *Dirichlet character* $\pmod N$ is a character $\eta \colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$. The Dirichlet character η is *primitive* if and only if it does not factor through $(\mathbb{Z}/D\mathbb{Z})^\times$ for any divisor $D \mid N$. Further, we say that η is even (respectively, odd) if and only if $\eta(-1) = 1$ (respectively, $\eta(-1) = -1$).

Definition 5 (Dirichlet L-function)**.** Given a Dirichlet character $\eta \pmod N$, we define the *Dirichlet L-function* $L(\eta, s)$ by

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

where implicitly $\eta(n) = 0$ whenever $\gcd(n, N) > 1$.

Example 6. Let $\eta \colon (\mathbb{Z}/2\mathbb{Z})^\times \to \mathbb{C}^\times$ be the nontrivial character. Then $L(\eta, 1) = \frac{\pi}{4}$.

Example 7. Let $\eta \colon (\mathbb{Z}/8\mathbb{Z})^\times \to \mathbb{C}^\times$ be the character defined by $\eta(3) = \eta(5) = -1$. This can be proven via a trick. Consider the power series

$$f(x) \coloneqq x - \frac{1}{3}x - \frac{1}{5}x^5 + \frac{1}{7}x^7 + \cdots,$$

from which one finds $f'(x) = 1 - x^2 - x^4 + x^6 + \cdots = \frac{1-x^2-x^4+x^6}{1-x^8}$. Then one can integrate $f'(x)$ to get

$$f(x) = \frac{\sqrt{2}}{4} \log \left| \frac{x^2 + \sqrt{2}x + 1}{x^2 - \sqrt{x} + 1} \right|.$$

It follows that $L(\eta, 1) = \frac{\sqrt{2}}{2} \log\left(\sqrt{2} + 1\right)$.

The previous example is an example of the class number formula, and right now it looks like a miracle. To give a taste for what is remarkable here, we note that $1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times$ is a fundamental unit. As such, we expect some interesting arithmetic to be going on.

Here is a more general result.

Theorem 8. Suppose $\eta \pmod{N}$ is a primitive nontrivial Dirichlet character.

(a) If η is even, then for any positive integer m, we have

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

(b) If η is odd, then for any positive integer m, we have

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

The above is an instance of Deligne's conjecture.

For another general result, we note that an even primitive quadratic character $\eta\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \{\pm 1\}$ has kernel which is an index-2 subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times \cong \operatorname{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$, so it corresponds to a quadratic extension F of $\mathbb{Q}$. In fact, the fact that η is even tells us that complex conjugation fixes F, so F is totally real. It then turns out that

$$L(\eta, 1) \equiv \sqrt{\operatorname{disc}\mathcal{O}_F} \cdot \log|u_F| \pmod{\mathbb{Q}^\times},$$

where u_F is a fundamental unit of $\mathcal{O}_F$. This also comes from the class number formula, and it is an instance of Beilinson's conjecture.

1.2 Funtional Equations

As usual, to write down a suitable functional equation for our L-functions, we must add some archimedean factors.

Definition 9 (completed Dirichlet L-function)**.** Let $\eta\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a primitive Dirichlet character. Then we define $d \in \{0, 1\}$ by $\eta(-1) = (-1)^d$ and then

$$L_\infty(\eta, s) := \pi^{-\frac{s+\delta}{2}} \Gamma\left(\frac{s+\delta}{2}\right).$$

Then the *completed Dirichlet L-function* is $\Lambda(\eta, s) := L_\infty(\eta, s) L(\eta, s)$.

Remark 10. Recall that $\Gamma(s)$ is defined by

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

for s such that $\operatorname{Re} s > 0$. One also knows that $\Gamma(s)$ admits a meromorphic continuation with understood poles, and it has a functional equation $\Gamma(s+1) = s\Gamma(s)$.

And here is our functional equation.

Theorem 11. Let $\eta\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a primitive Dirichlet character. Then $L(\eta, s)$ admits a meromorphic continuation (with poles only at $s \in \{0, 1\}$ only when η is trivial) to all $\mathbb{C}$ and satisfies a functional equation

$$\Lambda(\eta, s) = \varepsilon(\eta, s) \Lambda\left(\eta^{-1}, 1 - s\right),$$

where $\varepsilon(\eta, s)$ is some appropriately normalized Gauss sum.

We will not prove this today (it is mildly technical). Instead, we will use it to show a partial version of Theorem 8. With that said, we will need to do something in the direction of a meromorphic continuation because we will try to understand negative integer values of $L(\eta, s)$.

By expanding out the series, we see that

$$\Gamma(s)L(\eta,s) = \int_0^\infty \sum_{\substack{n\geq 1\\ \gcd(n,N)=1}} \eta(n)e^{-nt}t^s\,\frac{dt}{t} = \int_0^\infty \frac{1}{1-e^{-Nt}}\sum_{n=0}^{N_1}\eta(n)e^{-nt}\,\frac{dt}{t}.$$

One now plugs into the general machine that produces analytic continuation and functional equations.

Lemma 12. Choose a smooth Schwarz function $f\colon \mathbb{R}_{\geq 0}\to\mathbb{R}$. Then

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

has an analytic continuation to all $\mathbb{C}$ and satisfies $L(f,-n) = (-1)^n f^{(n)}(0)$ for all $n\geq 0$.

Proof. To control singularities, we let $\varphi\colon \mathbb{R}_{\geq 0}\to\mathbb{R}$ be a smooth bump function satisfying $\varphi|_{[0,1]} = 1$ and $\varphi_{[2,\infty)} = 0$. Thus, if we expand $f = f_1 + f_2$ with $f_1 = \varphi f$ and $f_2 = (1-\varphi)f$, we see that

$$\int_0^\infty f_2(t)t^s\,\frac{dt}{t} = \int_1^\infty f_2(t)t^s\,\frac{dt}{t},$$

and the rapid decay of f grants this term an analytic continuation to all $\mathbb{C}$, and it even satisfies

$$L(f_2,-n) = \left(\frac{1}{\Gamma(-s)}\int_1^\infty f_2(t)t^s\,\frac{dt}{t}\right)\Bigg|_{s=-n} = 0.$$

Thus, we are allowed to ignore f_2 piece. For the f_1 part, we inductively integrate by parts. For example, our first integration by parts produces

$$L(f,s) = \underbrace{\frac{1}{\Gamma(s)}f_1(t)\frac{t^s}{s}\bigg|_0^\infty}_{0} - \frac{1}{s\Gamma(s)}\int_0^\infty f(t)t\cdot t^s\,\frac{dt}{t} = -L(f_1', s+1).$$

Thus, we have moved out s to $s+1$, and we can iteratively produce the needed continuation from the argument above. The result on the special value follows from a computation. ■

One can now use the lemma to see that

$$L(\eta,-n)\in\mathbb{Q}(\eta).$$

Then one can use the functional equation Theorem 11 to prove Theorem 8 after tracking everything through. I apologize, but I chose not to write down the details.

2 The Kummer Congruence and p-Adic Analysis on $\mathbb{Z}_p$

This talk was given by Mitch. We would like to motivate p-adic L-functions and prove the Kummer congruences, which are used in their construction.

2.1 The Kummer Congruence

Last time, we had an equality of the form

$$\int_{\mathbb{R}^+} \underbrace{\frac{1}{1-e^{-Nt}}\sum_{n=1}^{N-1}\eta(n)e^{-nt}}_{f_\eta(t):=}\cdot t^s\,\frac{dt}{t} = \Gamma(s)L(\eta,s),$$

where $\eta \pmod N$ is some primitive Dirichlet character. The moral of the story is that we see that we are taking a Mellin transform of some function $f_\eta(t)$, so it may be interesting to study these functions on their own terms.

For example, if $\eta = 1$ is the trivial character, then one finds that

$$tf_1(t) = \frac{t}{1-e^{-t}} = \sum_{m=0}^\infty B_m \frac{t^m}{m!},$$

where $\{B_m\}_{m\ge 0}$ are the Bernoulli numbers. (Indeed, this is a definition of the Bernoulli numbers.) More generally, one can expand

$$tf_\eta(t) = \sum_{m=0}^\infty B_{\eta,m} \frac{t^m}{m!}$$

to define "twisted" Bernoulli numbers.

For our special values result, we found an identity

$$L(f,-n) = (-1)^n f^{(n)}(0),$$

where $\Gamma(s)L(f,s)$ refers to the Mellin transform, which eventually implies a special values result

$$L(\eta,-n) = -\frac{(-1)^{n+1}B_{\eta,n+1}}{n+1}$$

after some rearrangement. Parity arguments actually allow us to more or less ignore the sign $(-1)^{n+1}$. Namely, when n is even, then $L(\eta,-n) = 0$ for even n (unless η is trivial); and when n is odd, then $L(\eta,-n) = 0$ for $n \ge 1$ odd.

We are now ready to state our Kummer congruences.

Theorem 13 (Kummer congruence)**.** Fix a nontrivial primitive Dirichlet character $\eta \pmod N$. Fix a prime p coprime to N. Choose nonnegative integers n_1, n_2, and k such that $n_1, n_2 \ge k$ and $n_1 \equiv n_2 \pmod{(p-1)p^{k-1}}$. Then

$$-\frac{B_{\eta,n_1+1}}{n_1+1} \equiv -\frac{B_{\eta,n_2+1}}{n_2+1} \pmod{p^k}.$$

If η is trivial, then we also need to require $p \nmid (n_1-1)(n_2-1)$.

The moral of the story is that the special values of $L(\eta,s)$ (at integers) admit some kind of continuity in $\mathbb{Z}_p$. This will motivate us to define a p-adic L-function which interpolates these values. This interpolation will turn out to be a profittable thing to do, essentially due to Euler systems.

Remark 14. Here is a historical remark. For reasons related to Fermat's last theorem, Kummer was interested in the notion of a "regular prime." Namely, an odd prime p is found to be regular if and only if $p \nmid \#\operatorname{Cl}(\mathbb{Q}(\zeta_p))$, which turns out to be equivalent to the prime p not dividing any of the numerators of $B_2, B_4, \ldots, B_{p-3}$.

2.2 Using the p-Adic L-Function

Let's begin to describe what a p-adic L-function should be. Fix a prime p and some (space of) characters $\eta^{(p)} \colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ where $\eta^{(p)} \pmod N$ is a Dirichlet character with $p \nmid N$. Additionally, we fix some $\eta_p \colon (\mathbb{Z}/p^r\mathbb{Z})^\times \to \mathbb{C}^\times$, and we would like to "interpolate" the values

$$L\left(\eta^{(p)}\eta_p, -n\right)$$

as $n \ge 0$ varies. More precisely, we will find that L should be thought of as a measure where η_p is an input.

For our construction, we choose some $f_{\eta_p,n} \colon \mathbb{Z}_p^\times \to \overline{\mathbb{Q}}_p^\times$ given by $f_{\eta_p,n}(a) := \eta_p(a)a^n$. Then we will be able to appropriately interpolate with this function.

Remark 15. Note that $f_{\eta_p,n}$ can be thought of as a Galois representation of $\operatorname{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$.

Now, we note

$$L^{\{p\}}\left(\eta^{(p)}\eta_p, s\right) := \prod_{\substack{q \text{ prime} \\ \gcd(q,Np)=1}} \frac{1}{1-\eta^{(p)}(q)q^{-s}} = \begin{cases} L\left(\eta^{(p)}\eta_p, s\right) & \text{if } \eta_p \neq 1, \\ L\left(\eta^{(p)}\eta_p, s\right)\left(1-\eta(p)p^{-s}\right) & \text{if } \eta_p = 1. \end{cases}$$

Morally, the $L^{\{p\}}$ product simply removes any problems at p, which are relevant while we are working p-adically. The interpolation now appeals to the following result.

Theorem 16. Fix a primitive Dirichlet character $\eta^{(p)} \pmod N$ with $p \nmid N$. Then there is a p-adic measure $d\mu_{\eta^{(p)}}$ such that for any Dirichlet character $\eta_p \pmod{p^k}$ admits

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

Remark 17. It is worth comparing this statement to Tate's thesis, where we represent some (completed) L-function of a Hecke character χ as the Mellin transform against a character. The bizarre measure $\mu_{\eta^{(p)}}$ can be seen as incorporating the bizarre prime-to-p parts of the character χ.

We have not bothered to define p-adic integration, but let's explain why this implies Theorem 13 first.

Proof that Theorem 16 implies Theorem 13. This proof is rather formal. Write η as $\eta^{(p)}\eta_p$, where $\eta^{(p)}$ as conductor prime to p, and η_p has conductor which is a power of p. Now, for n large (say, $n \geq k$), we see that

$$L^{\{p\}}\left(\eta^{(p)}\eta_p, -n\right) = \left(1-\eta(p)p^{-n}\right) L\left(\eta^{(p)}\eta_p, -n\right) \equiv L\left(\eta^{(p)}\eta_p, -n\right) \pmod{p^k}$$

if η_p is trivial, and the statement is still true when η_p is nontrivial. Thus, after plugging in our special values result as $-\frac{B_{\eta,n+1}}{n+1} = L(\eta, -n)$, and in light of Theorem 16, we would like to show

$$\int_{\mathbb{Z}_p^\times} \eta_p(x)x^{n_1} \, d\mu_{\eta^{(p)}}(x) \overset{?}{\equiv} \int_{\mathbb{Z}_p^\times} \eta_p(x)x^{n_2} \, d\mu_{\eta^{(p)}}(x) \pmod{p^k}$$

whenever $n_1 \equiv n_2 \pmod{(p-1)p^{k-1}}$. This last equivalence holds on the level of the integrands because we are looking $\pmod{p^k}$. ■

2.3 Integration

Let's say something about how $\mu_{\eta^{(p)}}$ functions.

Remark 18. Do note that we are not looking for the usual Haar measure: small cosets receive size $1/p^\bullet$, which is large p-adically. Additionally, this will have basically no hope of incorporating the prime-to-p information discussed in Remark 17.

So let's rebuild some functional analysis so that we can value our measures in $\mathbb{Q}_p$.

Definition 19 (Banach space)**.** Fix a complete valued p-adic field K. A *Banach space* over K is a complete normed vector space B over K whose norm $\|\cdot\|$ satisfies the triangle inequaltiy

$$\|v_1 + v_2\| \leq \|v_1\| + \|v_2\|.$$

Example 20. Fix a compact topological space X. Then the space $C^0(X, \mathbb{Q}_p)$ of continuous functions $X \to \mathbb{Q}_p$ is a Banach space over $\mathbb{Q}_p$. The norm is given by $\|\cdot\|_\infty$.

Definition 21 (orthonormal basis)**.** Fix a Banach space B overa complete valued field p-adic K. Then an *orthonormal basis* is a set $\{e_i\} \subseteq B$ such that $\|e_i\| = 1$ for all i, and any vector v admits a unique expansion

$$v = \sum_i x_i e_i,$$

which converges in the sense $x_i \to 0$ (namely, $\#\{i \in I : |x_i| \geq \varepsilon\}$ is finite for all $\varepsilon > 0$) where $\|v\| = \max_i |x_i|$.

Remark 22. We are not requiring that $\{e_i\}$ be countable. The condition that $x_i \to 0$ also includes a hypothesis that only finitely many of the $x_\bullet$s are nonzero.

Our key example will be $C^0(\mathbb{Z}_p, \mathbb{Q}_p)$. Here is a nice basis of this space.

Example 23. For nonnegative integers $n \geq 0$, define the function $\binom{x}{n} : \mathbb{Z}_p \to \mathbb{Q}_p$ as the polynomial

$$\binom{x}{n} = \frac{x(x-1)\cdots(x-(n-1))}{n!}.$$

This is continuous because polynomials are continuous. We also remark that $\left\|\binom{x}{n}\right\|_\infty = 1$, which can be seen by checking on the dense subset $\mathbb{Z} \subseteq \mathbb{Z}_p$.

Proposition 24. The functions $\left\{\binom{x}{n}\right\}_{n\geq 0}$ form an orthonormal basis of $C^0(\mathbb{Z}_p, \mathbb{Q}_p)$.

Proof. We proceed in steps.

1. We remark that these binomials provide a basis of the polynomial functions $\mathbb{Z} \to \mathbb{Z}$, which is why we may expect this to be true. Indeed, the idea is to consider finite differences, and binomials appear for reasons related to a finite-difference version of the binomial theorem. Explicitly, for $f \in C^0(\mathbb{Z}_p, \mathbb{Q}_p)$, we define the finite differences $f^{[n]} : \mathbb{Z}_p \to \mathbb{Q}_p$ recursively by

$$\begin{cases} f^{[0]}(x) := f(x), \\ f^{[n+1]}(x) := f^{[n]}(x+1) - f^{[n]}(x). \end{cases}$$

   One can show by induction that

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

   where the key point is to use Pascal's identity $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$ in the inductive step.

2. We now take a moment to explain how these finite differences extract coefficients $a_n(f)$ so that $f = \sum_n a_n(f)\binom{\cdot}{n}$. Indeed, if we already had an expansion $f(x) = \sum_{n\geq 0} a_n(f)\binom{x}{n}$, then one finds (by induction) that

$$f^{[k]}(x) = \sum_{n\geq 0} a_n(f)\binom{x}{n-k},$$

   where again the point is to use Pascal's identity, so taking $x = 0$ finds $a_n(f) = f^{[n]}(0)$. We remark that this paragraph shows that the expansion of f into binomial coefficients is thus unique.

3. It remains to show that taking $a_n(f) := f^{[n]}(0)$ has $a_n(f) \to 0$ as $n \to \infty$ and $f(x) = \sum_{n \geq 0} a_n(f) \binom{x}{n}$. By scaling, we may assume that $\|f\|_\infty = 1$, and the explicit formula for $f^{[n]}(0)$ then verifies that $|a_n(f)| \leq 1$ for all n. In this step, we will check that $a_n(f) \to 0$.

   The main claim is that any continuous $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ has some ν such that $\operatorname{im} f^{[p^\nu]} \subseteq p\mathbb{Z}_p$. Indeed, because f is continuous, there is k such that the reduction $f \pmod p$ is constant on the cosets of $\mathbb{Z}_p/p^\nu\mathbb{Z}_p$, which implies that

$$f^{[p^\nu]}(x) = \sum_{k=0}^{p^\nu} (-1)^k \binom{p^\nu}{k} f\left(x + p^\nu - k\right) \equiv f\left(x + p^\nu\right) - f(x) \equiv 0 \pmod p,$$

   as required.

   Applying the claim inductively to the various finite differences of f, we see that there is a sequence of integers $\nu_0 \leq \nu_1 \leq \cdots$ such that $\operatorname{im} f^{[p^{\nu_\bullet}]} \subseteq p^\bullet\mathbb{Z}_p$ for each $\nu_\bullet$. Thus, for $n \geq \nu_\bullet$, we see that $a_n(f) \in p^\bullet\mathbb{Z}_p$, completing this step.

4. We now check that $f(x) = \sum_{n \geq 0} a_n(f) \binom{x}{n}$. We remark that these are both continuous functions $\mathbb{Z}_p \to \mathbb{Z}_p$ because we now know that $a_n(f) \to 0$ as $n \to \infty$. Thus, it is enough to check the equality on the dense subset $\mathbb{Z} \subseteq \mathbb{Z}_p$. One can then show equality on $\mathbb{Z}$ by induction: one needs to show that

$$f(n) = \sum_{k=0}^{n} a_n(f) \binom{n}{k}$$

   for each n, which can be done directly. ■

3 More on Measures

This talk was given by Rui Chen; I was not present for it. Today we set up some measure theory on $\mathbb{Z}_p$.

3.1 The Amice Transform

From the perspective of the Riesz representation theorem, a measure on $\mathbb{Z}_p$ is really just a distribution: it is some way to take controlled (say, compactly supported) functions and produce a number (which is the integral). Here is the corresponding definition over $\mathbb{Z}_p$.

Definition 25 (distribution)**.** The space of *distributions* on a profinite group G is the module

$$\mathcal{D}_0(G, \mathbb{Z}_p) := \operatorname{Hom}_{\text{cont}}\left(C^0(G, \mathbb{Z}_p), \mathbb{Z}_p\right).$$

Given some continuous $f\colon G \to \mathbb{Z}_p$, we may write $\int_G f\,d\mu$ or $\int_G f(x)\,d\mu(x)$ for $\mu(f)$.

Example 26 (Dirac distribution)**.** Fix some $g \in G$. Then there is a Dirac distribution $\delta_g \in \mathcal{D}_0(G, \mathbb{Z}_p)$ given by

$$\int_G f\,d\delta_g := f(g).$$

Remark 27. By continuity, a distribution $\mu \in \mathcal{D}_0(\mathbb{Z}_p, \mathbb{Z}_p)$ is uniquely determined by its values on the binomials $x \mapsto \binom{x}{n}$. Indeed, $\mu \mapsto \left(\mu\left(\binom{x}{n}\right)\right) \in \mathbb{Z}_p^{\mathbb{Z}_{\geq 0}}$, which we claim is an isomorphism. We will explain this again later, so let's be quick. It is certainly some $\mathbb{Z}_p$-linear map, and it is injective because we can expand out any $f \in C^0(\mathbb{Z}_p, \mathbb{Z}_p)$ as $f(x) = \sum_{n \geq 0} a_n(f)\binom{x}{n}$ with $a_n(f) \to 0$ as $n \to \infty$, thereby yielding

$$\mu(f) = \sum_{n \geq 0} a_n(f)\mu\left(\binom{x}{n}\right)$$

by continuity. Lastly, the above formula successfully defines a distribution no matter how we choose $\mu\left(\binom{x}{n}\right)$, which proves surjectivity of the constructed map.

The previous remark allows us to identify a measure by an infinite tuple of elements in $\mathbb{Z}_p$. It will turn out to be convenient to identify such infinite tuples with $\mathbb{Z}_p[[T]]$ for the following reason.

Definition 28 (Amice transform)**.** Given $\mu \in \mathcal{D}_0(\mathbb{Z}_p, \mathbb{Z}_p)$, we define the *Amice transform* $A_\mu(T) \in \mathbb{Z}_p[[T]]$ by

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

Remark 29. Intuitively, we are integrating the measure μ against the "character" $x \mapsto (1+T)^x$, so the Amice transform is a special case of a Fourier transform.

Let's quickly explain how to interpret $A_\mu(T)$ as an element of $\mathbb{Z}_p[[T]]$: the idea is to use the "binomial theorem" to expand $(1+T)^x$ as

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

Here, the interchange of the sum and integral $\overset{*}{=}$ should be understod as a formal operation because we have not previously defined what it means to integrate a formal power series in $\mathbb{Z}_p[[T]]$.

3.2 Distributions via the Iwasawa Algebra

The above construction is better understood in more generality. Let's begin by reinterpreting $\mathbb{Z}_p[[T]]$ in a more canonical way.

Definition 30 (Iwasawa algebra)**.** Fix a profinite group G. Then we define the *Iwasawa algebra* as

$$\mathbb{Z}_p[[G]] \coloneqq \varprojlim_{[H:G]<\infty} \mathbb{Z}_p[G/H].$$

Example 31. We compute $\mathbb{Z}_p[[\mathbb{Z}_p]]$. Indeed, for any $\nu \geq 0$, we note that there is a surjection $\mathbb{Z}_p[[T]] \twoheadrightarrow \mathbb{Z}_p[\mathbb{Z}_p/p^\nu\mathbb{Z}_p]$ given by $T \mapsto [1]-1$, and it becomes a bijection upon passing to the inverse limit. Thus, morally, we ought to view $T \in \mathbb{Z}_p[[T]]$ as providing an infinitesimal generator for functions centered at $1 \in \mathbb{Z}_p$.

Example 32. Fix a profinite group $G = \varprojlim G_\bullet$, we find

$$\mathcal{D}_0(G,\mathbb{Z}_p) = \operatorname{Hom}_{\text{cts}}\left(C^0(\varprojlim G_\bullet,\mathbb{Z}_p),\mathbb{Z}_p\right) = \varprojlim \operatorname{Hom}\left(C^0(G_\bullet,\mathbb{Z}_p),\mathbb{Z}_p\right).$$

Now, a distribution on the finite set $G_\bullet$ amounts to assigning a weight in $\mathbb{Z}_p$ to each element of $G_\bullet$, so it can be identified with $\mathbb{Z}_p[G_\bullet]$ (via the map $g \mapsto \delta_g$, where $\delta_g \in \mathcal{D}_0(G_\bullet,\mathbb{Z}_p)$ is the indiator of g). We conclude that we are looking at $\mathbb{Z}_p[[G]]$, and the isomorphism $\mathbb{Z}_p[[G]] \to \mathcal{D}_0(G,\mathbb{Z}_p)$ is given by extending $g \mapsto \delta_g$.

Thus, we see that the Iwasawa algebra provides a natural home for our distributions. For example, $\mathbb{Z}_p[[G]]$ has a natural multiplication structure, so we can look for this structure in distributions.

Definition 33 (convolution)**.** Fix a profinite group G, and choose two measures $\mu_1,\mu_2 \in \mathcal{D}_0(G,\mathbb{Z}_p)$. Then we define the *convolution* $(\mu_1 \star \mu_2) \in \mathcal{D}_0(\mathbb{Z}_p)$ by

$$\int_G f(g)\,d(\mu_1\star\mu_2)(g) \coloneqq \int_G\int_G f(gh)\,d\mu_1(g)\,d\mu_2(h).$$

Remark 34. Technically, we ought to check that the function

$$h \mapsto \int_G f(gh)\,d\mu_1(g)$$

is a continuous map $G \to \mathbb{Z}_p$. Let $\ell_\bullet\colon G \times C^0(G,\mathbb{Z}_p) \to C^0(G,\mathbb{Z}_p)$ denote right translation by h; then we would like to show that $h \mapsto \mu_1(\ell_h(f))$ is continuous. By composing appropriately, it is enough to check $\ell_\bullet$ is a continuous function, which holds as soon as we give $C^0(G,\mathbb{Z}_p)$ the correct topology. (For example, one can take a limit over the finite groups making up G.)

Remark 35. It is not hard to check that convolution makes $\mathcal{D}_0(G,\mathbb{Z}_p)$ into a ring without identity.

Proposition 36. Fix a profinite group G. The isomorphism $\mathbb{Z}[[G]] \to \mathcal{D}_0(G,\mathbb{Z}_p)$ given by $g \mapsto \delta_g$ is an isomorphism of rings.

Proof. By taking a limit, it is enough to check this at finite level, allowing us to assume that G is finite. Then any measure is a linear combination of Dirac distributions, so it is enough to check that $\delta_x \star \delta_y = \delta_{xy}$. Well, we compute

$$\begin{aligned}\int_G f\,d(\delta_x\star\delta_y) &= \int_G\int_G f(gh)\,d\delta_x(g)\,d\delta_y(h)\\ &= \int_G f(xh)\,d\delta_y(h)\\ &= f(xy),\end{aligned}$$

as required. ■

Anyway, we close this section by explaining the Amice transform.

Proposition 37. The Amice transform $A_\bullet \colon \mathcal{D}_0(\mathbb{Z}_p, \mathbb{Z}_p) \to \mathbb{Z}_p[[T]]$ is the composite of the isomorphisms

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

Proof. This is a direct computation. In short, it is enough to check this on finite level and then pass to the limit. Now, a measure μ on $\mathbb{Z}_p/p^\nu\mathbb{Z}_p$ becomes the polynomial

$$\sum_{a \in \mathbb{Z}_p/p^\nu\mathbb{Z}_p} \mu\left(a + p^\nu\mathbb{Z}_p\right)[a] \in \mathbb{Z}_p[\mathbb{Z}_p/p^\nu\mathbb{Z}_p],$$

which then goes to the polynomial

$$\sum_{a \in \mathbb{Z}_p/p^\nu\mathbb{Z}_p} \mu\left(a + p^\nu\mathbb{Z}_p\right)(1+T)^a,$$

which is $\int_{\mathbb{Z}_p} (1+T)^x \, d\mu(x)$. ■

4 The p-Adic Zeta Function

This talk was given by me. I did not have time to write up notes.

5 The Analytic Class Number Formula

This talk was given by Xin Wei.

5.1 Artin L-Functions

Our first topic today is about building L-functions attached to Galois representations. For our notation, F will be a number field, and we let $M_{F,f}$ denote the set of its finite places. Let's give some adjectives to our Galois representation.

Definition 38. Fix a Galois representation $\rho\colon \operatorname{Gal}(\overline{F}/F) \to \operatorname{GL}_n(\overline{\mathbb{Q}}_p)$.

(a) ρ is *unramified* at $v \in M_{F,f}$ if and only if ρ is trivial on the inertia subgroup I_v at v.

(b) ρ is *nice* if and only if it is unramified at all but finitely many places v satisfying the following conditions.

- For each $v \in M_{F,f}$ away from p, the characteristic polynomial of $\rho(\operatorname{Frob}_v)$ acting on V^{I_v} has algebraic coefficients.
- For each $v \in M_{F,f}$ above p, the local representation $\rho|_{\operatorname{Gal}(\overline{F}_v/F_v)}$ is de Rham, and the characteristic polynomial of $\rho(\operatorname{Frob}_v)$ acting on the module $\mathbb{D}_{\text{pst}}(\rho_v)^{I_v} = (\rho_v|_{L_w} \otimes B_{\text{st}})^{\operatorname{Gal}(L_w/F_v)}$ (coming from p-adic Hodge theory) has algebraic coefficients.

Remark 39. Intuitively, "de Rham" means potentially semistable.

Remark 40. When the image of ρ is finite, one can replace the submodule coming from p-adic Hodge theory with just V^{I_v}.

We are now ready to define our local L-factors.

Definition 41. Fix a nice Galois representation $\rho\colon \operatorname{Gal}(\overline{F}/F)\to\operatorname{GL}_n(\overline{\mathbb{Q}}_p)$. Then we define

$$L_v(\rho_v,s)\coloneqq\begin{cases}\det\left(1-\rho_v(\operatorname{Frob}_v)q_v^{-s};V^{I_v}\right)^{-1} & \text{if } v\mid p.\\ \det\left(1-\rho_v(\operatorname{Frob}_v)q_v^{-s};\mathbb{D}_{\text{st}}(\rho_v)^{I_v}\right)^{-1} & \text{if } \nmid p.\end{cases}$$

Then we define $L(\rho,s)\coloneqq\prod_{v<\infty}L_v(\rho_v,s)$ if it converges for $\operatorname{Re}s$ large enough.

Remark 42. It is not even known in general if $L(\rho,s)$ always converges if $\operatorname{Re}s$ is large enough, though this is true if ρ comes from geometry (such as if $\operatorname{im}\rho$ is finite). Similarly, little is known about meromorphic continuation or functional equation, where most results are known if one is able to associate ρ to an automorphic form.

Example 43 (Dirichlet character)**.** For a primitive Dirichlet character $\eta\pmod N$, there is a Galois representation $\widetilde{\eta}\colon\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\to\overline{\mathbb{Q}}^\times$ given by the following composite.

$$\begin{tikzcd}
\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \arrow[r, two heads] & \operatorname{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \arrow[r, phantom, "\simeq"] & (\mathbb{Z}/N\mathbb{Z})^\times \arrow[r] & \overline{\mathbb{Q}}^\times \\
\operatorname{Frob}_\ell \arrow[r, mapsto] & \operatorname{Frob}_\ell \arrow[r, mapsto] & \ell^{-1} \arrow[r, mapsto] & \eta(\ell)^{-1}
\end{tikzcd}$$

Here, one should take $\eta(p)=0$ for $p\mid N$, though this does not matter much. Because we have described explicitly what happens to the Frobenius elements above, we see that $L(\widetilde{\eta},s)=L\left(\eta^{-1},s\right)$.

Example 44 (Tate twist)**.** There is a cyclotomic character $\chi_{\text{cyc}}\colon\operatorname{Gal}(\overline{F}/F)\to\mathbb{Z}_p^\times$ given by restriction to $\operatorname{Gal}(F(\mu_{p^\infty})/F)\twoheadrightarrow\operatorname{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})=\mathbb{Z}_p^\times$. Expanding out this construction, we see that $\sigma(\zeta)=\zeta^{\chi_{\text{cyc}}(\sigma)}$ for any $\zeta\in\mu_{p^\infty}$. We may write this representation as the Tate twist $\mathbb{Z}_p(1)$ in the sequel; then $\mathbb{Z}_p(n)\coloneqq\mathbb{Z}_p(1)^{\otimes n}$ for $n\geq 0$ and $\mathbb{Z}_p(n)=\mathbb{Z}_p(-n)^\vee$ for $n<0$.

The up-shot of taking Tate twists is that we are able to shift L-functions. In particular, for a general Galois representation $\rho\colon\operatorname{Gal}(\overline{F}/F)\to\operatorname{GL}_{\overline{\mathbb{Q}}_p}(V)$ and $v\nmid p$, one can compute

$$L_v(V(n),s)=\det\left(1-\rho(n)(\operatorname{Frob}_v)q_v^{-s}\right)^{-1}=\det\left(1-\rho(n)(\operatorname{Frob}_v)q_v^{-s-n}\right)^{-1}=L_v(V,s+n),$$

and actually the same holds for $v\mid p$.

Example 45. Let's return to our p-adic measures μ_η briefly, where we recall that $\eta\colon(\mathbb{Z}/N\mathbb{Z})^\times\to\overline{\mathbb{Q}}_p^\times$ is some primitive Dirichlet character of conductor prime to p. Then for any primitive Dirichlet character $\chi\pmod{p^\nu}$, our measure μ_η satisfied

$$\int_{\mathbb{Z}_p^\times}\chi(x)x^n\,d\mu_\eta(x)=L^{(p)}(\eta,\chi,-n)=L^{(p)}(\widetilde{\eta}^{-1}\widetilde{\chi}^{-1}(-n),0),$$

allowing us to reinterpret the entire story in terms of Galois representations!

Remark 46. In general, one expects that a nice Galois representation ρ should admit a measure μ_ρ such that well-behaved χ have

$$\int_{\operatorname{Gal}(\overline{F}/F)_p^{\text{ab}}}\chi(x)\,d\mu_\rho(x)=L^{(p)}(\rho\otimes\chi,0),$$

where we are integrating over the pro-p part of the abelianization of the Galois group. We are now allowed to only work with 0 by shifting the value over by enough Tate twists.

Here are some basic properties.

Proposition 47. The following hold.

(a) Summation: for nice Galois representations ρ_1 and ρ_2 of F, we have $L(\rho_1 \oplus \rho_2, s) = L(\rho_1, s)L(\rho_2, s)$.

(b) Induction: for an extension F'/F of number fields and nice Galois representation ρ of F', we have

$$L\left(\operatorname{Ind}_{\operatorname{Gal}(\overline{\mathbb{Q}}/F)}^{\operatorname{Gal}(\overline{\mathbb{Q}}/F')} \rho, s\right) = L(\rho, s).$$

Sketch. Summation is checked place-by-place. Induction is also checked place-by-place. Away from p, this merely relates to some careful tracking through of facts about prime-splitting; at p, one needs to work a little harder with the p-adic Hodge theory construction. ■

Example 48. One can view the Dedekind zeta function ζ_F as either coming from the trivial representation of F or the induction to F of the trivial representation 1 of $\mathbb{Q}$. This is easiest to check when the extension $F/\mathbb{Q}$ is Galois.

5.2 The Class Number Formula

We now state a special values result.

Theorem 49. Fix a number field F. Let $\zeta_F(s)$ be the Dedekind zeta function, and consider the following invariants.

- r_1 is the number of real embeddings $F \hookrightarrow \mathbb{R}$.
- r_2 is the number of complex embeddings $F \hookrightarrow \mathbb{C}$ counted up to conjugacy.
- h_F is the class number of $\mathcal{O}_F$.
- w_F is the number of roots of unity in $\mathcal{O}_F$.
- Reg_F is the covolume of the unit lattice sitting inside the trace-zero hyperplane of $\mathbb{R}^{r_1+r_2}$. Namely, one embeds $\mathcal{O}_F^\times \to \mathbb{R}^{r_1} \times \mathbb{R}^{r_2}$ by projecting along the various embeddings $F \hookrightarrow \mathbb{C}$ and taking logarithms appropriately.

Then

$$\lim_{s \to 1}(s-1)\zeta_F(s) = \frac{2^{r_1}(2\pi)^{r_2}\operatorname{Reg}_F h_F}{w_F\sqrt{|\operatorname{disc}\mathcal{O}_F|}}.$$

Sketch. Proving this requires one to know something analytic about $\zeta_F(s)$, so the best proofs come from Tate's thesis. In particular, Tate's thesis more or less implies that the residue of $\zeta_F(s)$ at $s = 1$ is given by the volume of the norm-1 idéle class group, which produes the given formula after some effort. ■

Remark 50. Using the functional equation for ζ_F, one can show that this is equivalent to

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

We will not say more about the proof, but we will give a few examples for flavor.

Example 51. For $F = \mathbb{Q}$, the right-hand side is

$$\frac{2^1(2\pi)^0 \cdot 1 \cdot 1}{2 \cdot 1} = 1.$$

So it remains to show that $(s-1)\zeta(s) \to 1$ as $s \to 1$. For this, we rouhgly speaking have to know something about a meromorphic continuation of $\zeta(s)$ to $s = 1$, so we follow the simplest such proof and write

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \int_1^{\infty} \frac{1}{x^s}\,dx + O(1) = \frac{1}{s-1} + O(1).$$

Proposition 52. We prove the analytic class number formula in the quadratic imaginary case.

Proof. In this case, $(r_1, r_2) = (0, 1)$, and the regulartor is 1, and $w_F \in \{2, 4, 6\}$. Thus, the hardest contribution will come from the ideal class group. The idea is to stratify the sum according to ideal classes. For motivation, we begin by working with principal ideals, where we see our sum is

$$\frac{1}{\#\mathcal{O}_F^\times} \sum_{\alpha \in \mathcal{O}_F \setminus \{0\}} \frac{1}{\operatorname{N}\alpha^s}.$$

Thus, we see that we are basically counting points in the lattice $\mathcal{O}_F \subseteq \mathbb{C}$ bounded by some circle. This is approximately the area of the corresponding ellipse, which can be computed by integrating along concentric circles. There are approximately $\frac{2}{\sqrt{|\operatorname{disc}\mathcal{O}_F|}}$ lattice points for each unit square (which can be seen by computing $\mathcal{O}_F$), so our sum looks like

$$\frac{1}{w_F} \int_1^{\infty} \frac{2}{\sqrt{|\operatorname{disc}\mathcal{O}_F|}} \cdot 2\pi R \cdot R^{-2s}\,dR$$

up to some constant which does not matter much. (To be rigorous, one would need to prove something a little technical about the Gauss circle problem.) This integral eventually collapses to

$$\frac{2\pi}{w_F\sqrt{|\operatorname{disc}\mathcal{O}_F|}}.$$

For the other ideal classes, one can multiply by an ideal in the inverse class so that we are still basically summing some sublattice of principal ideals, allowing us to appeal to the above argument (after passing to a sublattice of $\mathcal{O}_F$); the final answer does not change. Summing over ideal classes completes the proof. ■

Remark 53. One can do something similar for real quadratic fields by counting points bounded by hyperbolas.

6 Regulators

This talk was given by Qing.

6.1 Special Values for Even Dirichlet Characters

For today, we work with $F_n^+ := \mathbb{Q}(\zeta_n + \zeta_n^{-1})$. Then the class number formula yields the residue of the Dedekind zeta function $\zeta_{F_n^+}(s)$ at $s = 1$. On the other hand, decomposing the regular representation into characters shows that $\zeta_{F_n^+}(s)$ admits a factorization

$$\zeta_{F_n^+}(s) = \prod_{\eta} L(\eta, 1),$$

where the product is taken over characters η of the Galois group $\operatorname{Gal}(F_n^+/\mathbb{Q})$. Thus, we may compare the residue of $\zeta_{F_n^+}(s)$ with the values $L(\eta,1)$ when η is nontrivial (because trivial η yields a pole with controlled residue). Note that these values $L(\eta,1)$ must be nonzero for $\eta\neq 1$: they are certainly finite, and it must be nonzero because the class number formula forces the product to have a simple pole of order exactly 1.

In particular, we would like to know that the values $L(\eta,1)$ are finite and nonzero. Well, recall

$$L(\eta,1)=\sum_{n\geq 1}\frac{\eta(n)}{n}.$$

Now, $\eta(n)$ is some root of unity, so we may use the fact that

$$\sum_{n\geq 1}\frac{\zeta}{n}=-\log(1-\zeta)$$

for $|\zeta|=1$ not equal to 1. Explicitly, we may view η as lifted from a primitive Dirichlet character $\eta \pmod m$; note $\eta(-1)=1$ because we are requiring that η comes from F_n^+ instead of $\mathbb{Q}(\zeta_n)$. Now, via a Fourier transform, one may expand

$$\eta(n)=\sum_{i=0}^{m-1}a_i\zeta_m^{in}$$

for some coefficients a_i. Let's solve for these coefficients. Well, by suitalby averaging, we find that

$$a_i=\frac{1}{m}\sum_{j=0}^{m}\eta(j)\zeta_m^{-ij}.$$

For example, if $\gcd(i,m)=1$, then the sum rearranges to $\frac{1}{m\eta(i)}G(\eta)$, where $G(\eta)=\sum_j\eta(j)\zeta_m^j$ is the Gauss sum. On the other hand, if $\gcd(i,m)=d>1$, then we can see that the sum has a certain periodicity $\pmod d$ which is not shared by η (because η is primitive!), so the entire sum vanishes. In total, we find that

$$L(\eta,1)=\frac{G(\eta)}{m}\sum_{n\geq 1}\left(\sum_{\substack{1\leq i\leq m\\ \gcd(i,m)=1}}\frac{\zeta_m^{in}\eta(i)^{-1}}{n}\right).$$

Rearranging the sums, we see

$$L(\eta,1)=\frac{G(\eta)}{m}=-\frac{G(\eta)}{m}\sum_{i\in(\mathbb{Z}/m\mathbb{Z})^\times/\{\pm1\}}\eta(i)^{-1}\log\left|1-\zeta_m^i\right|^2,$$

where we have silently used the fact that $\eta(-1)=1$.

Remark 54. By using the functional equation, one can compute that

$$\lim_{s\to 0}s^{-1}L\left(\eta^{-1},s\right)=-\sum_{i\in(\mathbb{Z}/m\mathbb{Z})^\times/\{\pm1\}}\eta(i)^{-1}\log\left|1-\zeta_m^i\right|.$$

Amazingly, the Gauss sum term has vanished! This formula also holds if η fails to be primitive, basically by reducing to the primitive case.

6.2 p-Adic Special Values for Even Dirichlet Characters

Throughout, we fix a prime p. Given an even primitive Dirichlet character $\eta \pmod m$ of conductor prime to p, then we know that there is a measure $\mu_\eta^{\{p\}}$ such that

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

for and Dirichlet character η_p of p-power conductor. Thus, for our p-adic analogue, we will try to compute

$$L_p(\eta, 1) := \int_{\mathbb{Z}_p^\times} x^{-1} \, d\mu_\eta^{\{p\}}(x).$$

We are expecting to get a statement about some sum of logarithms of cyclotomic numbers; this logarithm should not be so surprising because we are integrating x^{-1}. For our computation, we pick up a few lemmas.

Lemma 55. Choose $\mu \in D_0(\mathbb{Z}_p, \mathbb{Z}_p)$. Define $x\mu$ by $\int_{\mathbb{Z}_p} f(x) \, d(x\mu)(x) := \int_{\mathbb{Z}_p} x f(x) \, d\mu(x)$. Then the Amice transform satisfies

$$\mathcal{A}_{x\mu}(T) = (1+T)\frac{d}{dT}A_\mu(T).$$

Proof. Direct computation of the Amice transform. ■

Lemma 56. Choose $\mu \in D_0(\mathbb{Z}_p^\times, \mathbb{Z}_p)$. Define $x^{-1}\mu$ by $\int_{\mathbb{Z}_p^\times} f(x) \, d(x^{-1}\mu)(x) := \int_{\mathbb{Z}_p^\times} x^{-1} f(x) \, d\mu(x)$. Then the Amice transform satisfies

$$(1+T)\frac{d}{dT}A_{x^{-1}\mu}(T) = A_\mu(T)$$

and $\psi(A_{x^{-1}\mu}) = 0$. Here, ψ is the operation on $\mathbb{Z}_p[[T]]$ given by $\sum_i a_i(1+T)^i \mapsto \sum_i a_{ip}(1+T)^i$.

Proof. Use the previous lemma. ■

We now apply the above lemma to do our computation. By definition of μ_η, we have

$$A_{\mu_\eta}(T) = \frac{\sum_{a=1}^{m-1} \eta(a)(1+T)^a}{1-(1+T)^m},$$

which can be expanded into

$$A_{\mu_\eta}(T) = \sum_{a \geq 1} \eta(a)(1+T)^a.$$

Using a finite Fourier transform as before, we find

$$A_{\mu_\eta}(T) = \frac{1}{G\left(\eta^{-1}\right)} \sum_{i=1}^{m-1} \frac{\eta(i)^{-1}\zeta_m^i(1+T}{1-\zeta_m^i(1+T).}$$

Now, $A_{\mu_\eta^{\{p\}}}$ is the restriction $(1-\varphi\psi)A_{\mu_\eta}$ of A_{μ_η} to $\mathbb{Z}_p^\times$. One is able to write out this computation explicitly to find that the Amice transform

$$B(T) := -\frac{1}{G\left(\eta^{-1}\right)} \sum_{\substack{1 \leq i \leq m \\ \gcd(i,m)=1}} \eta(i)^{-1} \left(\log_p\left(1-\zeta_m^i(1+T)\right) - \frac{1}{p}\log_p\left(1-\zeta_m^p(1+T)^p\right) \right),$$

where $\log_p$ is the p-adic logarithm; for example, one can check by hand that $\psi(B(T)) = 0$, so this does in fact produce a measure on $\mathbb{Z}_p^\times$. Evaluating at $T=0$ to take the integral, we find that

$$L_p(\eta, 1) = -\frac{1}{G\left(\eta^{-1}\right)} \left(1-\eta(p)p^{-1}\right) \sum_{i=1}^{m-1} \eta(i)^{-1} \log_p\left(1-\zeta_m^i\right),$$

which is our desired result.

7 Cyclotomic Units

This talk was given by Qing.

7.1 Circular Units

For today, $F := \mathbb{Q}\left(\zeta_n + \zeta_n^{-1}\right)$ is the totally real subfield of $\mathbb{Q}(\zeta_n)$. Note $[F : \mathbb{Q}] = \frac{1}{2}\varphi(n)$, so $\mathcal{O}_F^\times$ has rank $\frac{1}{2}\varphi(n) - 1$. It would be nice to exhibit sufficiently many units.

Definition 57 (circular units)**.** Given an abelian number field $K \subseteq \mathbb{Q}(\zeta_n)$, we let the subgroup $\operatorname{Cyc}_K^\times$ of *circular units* be the subgroup

$$\mathcal{O}_K^\times \cap \langle -1, \zeta_n, \zeta_n^\bullet - 1 \rangle .$$

Remark 58. One can check that this subgroup does not depend on the choice of n. In short, this follows because the units $\zeta_n^\bullet - 1$ map to each other under norms.

Example 59. For $F = \mathbb{Q}(\zeta_{p^\nu})$, the only way to translate $\zeta_{p^\nu}^a - 1$ into a unit is to divide out by another generator of its principal ideal. It turns out that the principal ideal is the unique prime ideal above $(p) \subseteq \mathbb{Z}$, so one can vary a to produce lots of different generators. We conclude that the circular units in $\mathcal{O}_F^\times$ are generated by -1, ζ_n, and

$$\frac{\zeta_{p^\nu}^a - 1}{\zeta_{p^\nu} - 1}.$$

Example 60. For $F = \mathbb{Q}\left(\zeta_{p^\nu} + \zeta_{p^\nu}^{-1}\right)$, we see $\operatorname{Cyc}_F^\times$ is generated by -1 and the units

$$\frac{\zeta_{p^\nu}^{-a/2} - \zeta_{p^\nu}^{a/2}}{\zeta_{p^\nu}^{-1/2} + \zeta_{p^\nu}^{1/2}},$$

where $a < p^\nu/2$ is a positive integer coprime to p.

Let's check that we have produced enough units

Theorem 61. Fix $n \geq 1$. The elements

$$\left\{ \frac{\zeta_n^a - 1}{\zeta_n - 1} : a \in ((\mathbb{Z}/n\mathbb{Z})^\times \setminus \{\pm 1\})/\{\pm 1\} \right\}$$

forms a $\mathbb{Q}$-basis of $\mathbb{Z}[\zeta_n]^\times \otimes_\mathbb{Z} \mathbb{Q}$.

Proof. Set $e_a := \zeta_n^a - 1$ for brevity. Let $V_0 \subseteq \mathbb{Q}[\{e_a\}]$ be the subspace of elements which sum to 0. (Here, a in e_a varies over $(\mathbb{Z}/n\mathbb{Z})^\times/\{\pm 1\}$.) Then there is a map $V_0 \to \mathbb{Z}[\zeta_n]^\times \otimes_\mathbb{Z} \mathbb{Q}$, which we note is invariant under the ambient $(\mathbb{Z}/n\mathbb{Z})^\times$ actions on both sides: on one hand, $(\mathbb{Z}/n\mathbb{Z})^\times$ acts on V_0 by $b \cdot e_a \mapsto e_{ab}$, and on the other hand, $(\mathbb{Z}/n\mathbb{Z})^\times \cong \operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ acts on the units. Now, by some computation with Dirichlet's unit theorem, we would like to know if the elements $\{e_a - e_1\}$ provide a basis for V_0 (namely, are linearly independent), but by some character theory, we may as well tensor up with $\mathbb{Q}(\zeta_n)$ and instead ask for the elements

$$e_\eta := \sum_{b \in (\mathbb{Z}/n\mathbb{Z})^\times/\{\pm 1\}} \overline{\eta}(b) e_b$$

to be nontrivial for all characters η on $(\mathbb{Z}/n\mathbb{Z})^\times/\{\pm1\}$. (Namely, we have diagonalized V_0 according to the $(\mathbb{Z}/n\mathbb{Z})^\times$-action, so any kernel needs to now send one of these one-dimensional eigenspaces to zero.) However, we can take logs to compute that

$$\sum_{b\in(\mathbb{Z}/n\mathbb{Z})^\times/\{\pm1\}} \overline{\eta}(b)\log\left|1-\zeta_n^b\right|$$

was computed to be the residue of $L(\overline{\eta}, s)$ at $s=0$, which we know to be finite and nonzero! ■

8 (φ, Γ)-Modules and Galois Cohomology

I was not present for this talk.

8.1 (φ, Γ)-Modules

Let's start with a little p-adic Hodge theory. For today, E will be a field of positive characteristic p. Our goal is to understand Galois representations of E in positive characteristic. Importantly, we will not assume that E is perfect in order to allow $E = \mathbb{F}_p((t))$, which wil be a running example. For some notation, we define $\varphi\colon E^{\text{sep}} \to E^{\text{sep}}$ to be the arithmetic Frobenius given by $x \mapsto x^p$.

Definition 62 (φ-module)**.** A *φ-module* over E is a finite-dimensional E-vector space M together with an isomorphism $\Phi\colon M\otimes_{E,\varphi} E \to M$. Equivalently, we are asking for a sufficiently non-degenerate Frobenius-semilinear operator $\Phi\colon M \to M$, where the semilinearity means and $a\in E$ and $m \in M$ has

$$\Phi(am) = \varphi(a)\Phi(m).$$

The category of φ-modules over E is denoted $\operatorname{Mod}_E^\varphi$.

Theorem 63. Consider the following two functors between $\operatorname{Rep}_{\mathbb{F}_p}(\operatorname{Gal}_E)$ and $\operatorname{Mod}_E^\varphi$.

- There is a functor $\mathbb{D}\colon \operatorname{Rep}_{\mathbb{F}_p}(\operatorname{Gal}_E) \to \operatorname{Mod}_E^\varphi$ given by $\mathbb{D}(V) := (V\otimes_{\mathbb{F}_p} E^{\text{sep}})^{\operatorname{Gal}_E}$.
- There is a functor $\mathbb{V}\colon \operatorname{Mod}_E^\varphi \to \operatorname{Rep}_{\mathbb{F}_p}(\operatorname{Gal}_E)$ given by $\mathbb{V}(D) := (D\otimes_E E^{\text{sep}})^{\varphi=1}$.

Then these are inverse equivalences preserving dimensions.

Proof. We divide the proof into two similar checks.

- Choose $V \in \operatorname{Rep}_{\mathbb{F}_p}(\operatorname{Gal}_E)$ of dimension d. We claim that there a Galois-equivariant isomorphism $V\otimes_{\mathbb{F}_p} E^{\text{sep}} \to (E^{\text{sep}})^d$ of vector spaces. This comes down Hilbert's theorem 90. By choosing a basis for V, we see that each $g \in \operatorname{Gal}_E$ produces some matrix $a_g \in \operatorname{GL}_d(E)$, which we would like to be given by the standard Galois action after changing the basis suitably. Well, because V is a representation, we see that
$$a_{gh} = a_g \cdot g(a_h),$$
so $g \mapsto a_g$ defines a 1-cocycle in $Z^1(\operatorname{Gal}_E, \operatorname{GL}_d(E^{\text{sep}}))$. But all 1-cocycles and 1-coboundaries by Hilbert's theorem 90, so there is $b \in \operatorname{GL}_d(E^{\text{sep}})$ such that $a_g = b^{-1}\cdot g(b)$. Adjusting the basis by using b, we find that we may change the basis so that all the a_gs are the identity, and we are done.

  As an application of this, we note $\mathbb{D}(V) = \left(V\otimes_{\mathbb{F}_p} E^{\text{sep}}\right)^{\operatorname{Gal}_E} = V\otimes_{\mathbb{F}_p} E$ because there is an obvious map between them, and these vector spaces have the same dimension. Thus, $\dim \mathbb{D}(V) = \dim V$, and
$$\begin{aligned}\mathbb{V}(\mathbb{D}(V)) &= (\mathbb{D}(V)\otimes_E E^{\text{sep}})^{\varphi=1} \\ &= \left(V\otimes_{\mathbb{F}_p} E^{\text{sep}}\right)^{\varphi=1} \\ &= V.\end{aligned}$$

- Choose $D \in \operatorname{Mod}_E^\varphi$ of dimension d. Then we claim that $D \otimes_E E^{\text{sep}} \cong (E^{\text{sep}})^d$ as φ-modules. Well, upon choosing a basis of D as an E-vector space, we may write the matrix Φ as some matrix $F \in \operatorname{GL}_n(E)$.

  It is more illuminating to imagine we want to compute $(D \otimes_E E^{\text{sep}})^{\varphi=1}$, which amounts to solving the equation $\varphi(v) - P^{-1}v = 0$ for $v \in D$. This can be viewed as searching for the E^{sep}-points of the algebra
  $$\frac{E[v_1,\ldots,v_n]}{(\varphi(v)-P^{-1}v)}.$$
  The Jacobian criterion allows us to check that this is a finite étale algebra, so there are indeed p^d points over E^{sep}. Additionally, because étale morphisms need to factor through affine space, we see that $D \otimes_E E^{\text{sep}}$ is $(E^{\text{sep}})^d$ as φ-modules, as required.

  For the same sort of application, we note $D \otimes_E E^{\text{sep}} = \mathbb{V}(D) \otimes_{\mathbb{F}_p} E^{\text{sep}}$ because there is a map from the right to left, and these vector spaces have the same dimension.[1] We conclude $\dim \mathbb{V}(D) = \dim D$, and
  $$\begin{aligned}\mathbb{D}(\mathbb{V}(D)) &= (\mathbb{V}(D) \otimes_{\mathbb{F}_p} E^{\text{sep}})^{\operatorname{Gal}_E} \\ &= (D \otimes_E E^{\text{sep}})^{\operatorname{Gal}_E} \\ &= D.\end{aligned}$$

The above checks complete the proof. ■

Remark 64. It turns out that $\mathbb{D}$ and $\mathbb{V}$ are compatible with taking tensor products and duals, which we will not check.

We would like to upgrade Theorem 63 to keep track of integral structure. This will require replacing $\operatorname{Mod}_E^\varphi$ to a category which keeps track of some integrality.

Definition 65 (Cohen ring). Fix a field E of positive characteristic p. A *Cohen ring* C_E of E is a complete discrete valuation ring with residue field E such that p is a uniformizer.

Remark 66. If E fails to be perfect, then Cohen rings may not be unique. However, they always exist.

In the sequel, we will require our Cohen ring E to admit a Frobenius lift of $\varphi\colon E \to E$. We will also write C_E^{unr} to be a maximal unramified extension; note then that Henselian conditions imply that $C_E^{\text{unr}}/(p) = E^{\text{sep}}$.

Example 67. Consider $E = \mathbb{F}_p((t))$. Then we may take C_E as the ring $\mathbb{Z}_p((t))^\wedge$, where $(\cdot)^\wedge$ denotes a p-adic completion. The endomorphism $\varphi\colon C_E \to C_E$ defined by $\varphi(T) := (1+T)^p - 1$ is a suitable lift of the Frobenius.

And here is our analogue of Theorem 63.

Definition 68 (étale). Fix a field E of positive characteristic p, and choose a Cohen ring C_E of E. Then a φ-module M is *étale* if and only if the matrix representing $\Phi\colon M \to M$ has entries in C_E.

Theorem 69. Fix a field E of positive characteristic p. Fix a Cohen ring C_E of E admitting a Frobenius lift, and choose a maximal unramified extension C_E^{unr} of C_E. Then the following two functors are inverse equivalences of tensor categories.

- The functor $\mathbb{D}\colon \operatorname{Rep}_{\mathbb{Z}_p}(\operatorname{Gal}_E) \to \operatorname{Mod}_{C_E}^{\varphi,\text{ét}}$ given by $\mathbb{D}(V) := \left(V \otimes_{\mathbb{Z}_p} \widehat{C_E^{\text{unr}}}\right)^{\operatorname{Gal}_E}$.
- The functor $\mathbb{V}\colon \operatorname{MOd}_{C_E}^{\varphi,\text{ét}} \to \operatorname{Rep}_{\mathbb{Z}_p}(\operatorname{Gal}_E)$ given by $\mathbb{V}(D) := \left(D \otimes_{C_E} \widehat{C_E^{\text{unr}}}\right)^{\varphi=1}$.

[1] Actually, one can check that the natural map is an isomorphism after reducing to $\mathbb{F}_p$.

Let's now turn to positive characteristic. By the Kronecker–Weber theorem, we note that $\mathbb{Q}_p^{\mathrm{ab}} = \mathbb{Q}_p(\mu_\infty)$, which is $\mathbb{Q}_p(\mu_{p^\infty})$ because $\mathbb{Q}_p$ already has prime-to-p torsion. As for the nonabelian part, it turns out that

$$\operatorname{Gal}\left(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^{\mathrm{ab}}\right) \cong \operatorname{Gal}\left(E^{\mathrm{sep}}/E\right),$$

where $E := \mathbb{F}_p((t))$. It is now possible to prove a suitable version of Theorem 63.

Definition 70 ((φ,Γ)-module)**.** An *étale* (φ,Γ)*-module* is a finitely generated C_E-module M equipped with a semilinear Γ-action (namely, $\gamma(am) = \gamma(a)\gamma(m)$) and a Γ-equivariant Frobenius-semilinear isomorphism $\Phi\colon M \to M$ with integral matrix entries (and integral inverse). The category of (φ,Γ)-modules is denoted by $\operatorname{Mod}^{(\varphi,\Gamma)}$.

Theorem 71. Set $E := \mathbb{F}_p((t))$ and $C_E := \mathbb{Z}_p((t))^\wedge$, where C_E admits the Frobenius lift $\varphi\colon C_E \to C_E$ defined by $\varphi(t) := (1+t)^p - 1$. Then the following functors are inverse equivalences of tensor categories.

- The functor $\mathbb{D}\colon \operatorname{Rep}_{\mathbb{F}_p}^{\mathrm{free}}(\operatorname{Gal}_{\mathbb{Q}_p}) \to \operatorname{Mod}_E^{(\varphi,\Gamma),\text{ét},\mathrm{free}}$ given by $\mathbb{D}(V) := \left(V \otimes_{\mathbb{Z}_p} \widehat{C_E^{\mathrm{unr}}}\right)^{\operatorname{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^{\mathrm{ab}})}$.
- The functor $\mathbb{V}\colon \operatorname{Mod}_E^{(\varphi,\Gamma),\text{ét},\mathrm{free}} \to \operatorname{Rep}_{\mathbb{F}_p}^{\mathrm{free}}(\operatorname{Gal}_{\mathbb{Q}_p})$ given by $\mathbb{V}(D) := \left(D \otimes_{C_E} \widehat{C_E^{\mathrm{unr}}}\right)^{\varphi=1}$.

Remark 72. There is a suitable analogue replacing $\mathbb{F}_p$-coefficients of our Galois coefficeints with coefficients of $\mathbb{Z}_p$ which consists of replacing our φ-modules over E with φ-modules over C_E.

9 Iwasawa Cohomology

This talk was given by Yashi.

9.1 Some Kummer Theory

Let's begin by reviewing some Kummer theory. Let F be a field of characteristic not p, and let G_F be the absolute Galois group. Then there is a short exact sequence

$$1 \to \mu_{p^n} \to F^\times \overset{p^n}{\to} F^\times \to 1$$

which upon taking Galois cohomology yields the short exact sequence

$$1 \to \mathrm{H}^0(G_F, \mu_{p^n}) \to \mathrm{H}^0(G_F, F^{\mathrm{sep}^\times}) \to \mathrm{H}^0(G_F, F^{\mathrm{sep}\times}) \to \mathrm{H}^1(G_F, \mu_{p^n}) \to 1,$$

where the last term vanishes by Hilbert's theorem 90. We conclude that the connecting morphism defines an isomorphism

$$\frac{F^\times}{F^{\times p^n}} \to \mathrm{H}^1(G_F, \mu_{p^n}).$$

This map has good functoriality properties. For example, if $F \subseteq E$ is a field extension, then one can check that the norm map on H^0 is simply corestriction, so the diagram

$$\begin{tikzcd}
E^\times/E^{\times p^n} \arrow[r] \arrow[d, "\mathrm{N}_{E/F}"'] & \mathrm{H}^1(G_E, \mu_{p^n}) \arrow[d, "\mathrm{cores}"] \\
F^\times/F^{\times p^n} \arrow[r] & \mathrm{H}^1(G_F, \mu_{p^n})
\end{tikzcd}$$

commutes. As another nice functoriality property, we note that we can take an ivnerse limit over p^n, which produces an isomorphism $F^\times \widehat{\otimes} \mathbb{Z}_p \to \mathrm{H}^1(G_F, \mathbb{Z}_p(1))$.

Let's give a "global" variant. If S is a finite set of places of a global field F, we let F^S denote the maximal extension of F which is unramified outside S, and we let $G_{F,S}$ be its Galois group. In our application, we now fix S to be the places above p and ∞, in which case we find that the short exact sequence

$$1 \to \mu_{p^n} \to \mathcal{O}_{F^S}\left[p^{-1}\right]^\times \to \mathcal{O}_{F^S}\left[p^{-1}\right] \to 1,$$

so the same sort of connecting morphism argument prduces an injection

$$\mathcal{O}_F\left[p^{-1}\right]\widehat{\otimes}\mathbb{Z}_p \hookrightarrow \mathrm{H}^1(G_{F,S},\mathbb{Z}_p(1)).$$

9.2 Iwasawa Cohomology

We are now allowed to define Iwasawa cohomology. We consider the following lattice of fields.

$$\begin{tikzcd}
F(\mu_{p^\infty}) & F^S(\mu_{p^r}) \\
F(\mu_{p^r}) \arrow[u, dash] \arrow[ur, dash] & F^S \arrow[u, equal] \\
F \arrow[u, dash] \arrow[ur, dash] &
\end{tikzcd}$$

Now, for a representation V of $G_{F,S}$, we define

$$\mathrm{H}^1_{\mathrm{IW}}(G_{F,S},V) := \varprojlim_r \mathrm{H}^1(G_{F(\mu_{p^r}),S},V),$$

where this Galois group acts on V by $G_{F(\mu_{p^r}),S} = \mathrm{Gal}(F^S/F(\mu_{p^r}))$.

Here is our application of Kummer theory: the commutative diagram

$$\begin{tikzcd}
\mathbb{Z}[\mu_{p^r}]\left[p^{-1}\right]^\times \widehat{\otimes}\mathbb{Z}_p \arrow[r, hook] \arrow[d] & \mathrm{H}^1(G_{\mathbb{Q}(\mu_{p^r}),S},\mathbb{Z}_p(1)) \arrow[d] \\
\mathbb{Q}_p(\mu_{p^r})^\times\widehat{\otimes}\mathbb{Z}_p \arrow[r, hook, two heads] & \mathrm{H}^1(G_{\mathbb{Q}_p(\mu_{p^r})},\mathbb{Z}_p(1))
\end{tikzcd}$$

with horizontal arrows given by Kummer theory produces a commutative diagram

$$\begin{tikzcd}
\varprojlim \mathbb{Z}[\mu_{p^\bullet}]\left[p^{-1}\right]^\times \widehat{\otimes}\mathbb{Z}_p \arrow[r, hook] \arrow[d] & \mathrm{H}^1_{\mathrm{IW}}(G_{\mathbb{Q},S},\mathbb{Z}_p(1)) \arrow[d] \\
\varprojlim \mathbb{Q}_p[\mu_{p^\bullet}]^\times\widehat{\otimes}\mathbb{Z}_p \arrow[r, hook, two heads] & \mathrm{H}^1_{\mathrm{IW}}(G_{\mathbb{Q}_p,S},\mathbb{Z}_p(1))
\end{tikzcd}$$

where the limits are taken with respect to norms.

Proposition 73. One has

$$\mathrm{H}^1_{\mathrm{IW}}(G_{\mathbb{Q}_p},V) \cong \mathbb{D}(V)^\psi,$$

where ψ is a certain quasi-inverse of the Frobenius.

Proof. Let's set up some notation. Let $\gamma \in \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p)$ be a topological generator, namely the Frobenius, and we let γ_{1+p^r} be the corresponding topoloical generator of $\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty}),\mathbb{Q}_p(\mu_{p^r}))$. Now, there are restriction and corestriction maps between $\mathrm{H}^i(G_{\mathbb{Q}_p},V)$ and $\mathrm{H}^i(G_{\mu_p(\mu_{p^r})},V)$, which should be seen on the level of the Herr complex by the folowing diagram.

$$\begin{tikzcd}
\mathbb{D}V \arrow[r, "{(\psi-1,\gamma-1)}"] \arrow[d, shift left, "\mathrm{id}"] & \mathbb{D}V\oplus\mathbb{D}V \arrow[r, "{(\gamma-1),1-\psi)}"] \arrow[d, shift left, "\mathrm{id}"] & \mathbb{D}V \arrow[d, shift left, "\sum_i \gamma^i"] \\
\mathbb{D}V \arrow[r, "{(\psi-1,\gamma_{1+p^r}-1)}"'] \arrow[u, shift left, "\mathrm{id}"] & \mathbb{D}V\oplus\mathbb{D}V \arrow[r, "{(\gamma_{1+p^r}-1,1-\psi)}"'] \arrow[u, shift left, "\sum_i \gamma^i"] & \mathbb{D}V \arrow[u, shift left, "\mathrm{id}"]
\end{tikzcd}$$

(The middle morphisms are slightly wrong. I have described the maps on the left $\mathbb{D}V$, but the maps on the right $\mathbb{D}V$ are reversed.) The rows can be viewed as the total complex for a filtration, so the Grothendieck spectral sequence yields a short exact sequence

$$0 \to \frac{\mathbb{D}V^{\psi=1}}{\gamma_{1+p^r} - 1} \to \mathrm{H}^1_{\psi,\gamma_{1+p^r}}(\mathbb{D}V) \to \left(\frac{\mathbb{D}V}{\psi - 1}\right)^{\gamma_{1+p^r}=1} \to 0.$$

We now note that this short exact sequence fits into a morphism

$$\begin{tikzcd}
0 \arrow[r] & \frac{\mathbb{D}V^{\psi=1}}{\gamma_{1+p^{r+1}}-1} \arrow[r] \arrow[d, two heads] & \mathrm{H}^1_{\psi,\gamma_{1+p^{r+1}}}(\mathbb{D}V) \arrow[r] \arrow[d, "\text{cores}"] & \left(\frac{\mathbb{D}V}{\psi-1}\right)^{\gamma_{1+p^{r+1}}=1} \arrow[r] \arrow[d, "\sum_i \gamma^i"] & 0 \\
0 \arrow[r] & \frac{\mathbb{D}V^{\psi=1}}{\gamma_{1+p^r}-1} \arrow[r] & \mathrm{H}^1_{\psi,\gamma_{1+p^r}}(\mathbb{D}V) \arrow[r] & \left(\frac{\mathbb{D}V}{\psi-1}\right)^{\gamma_{1+p^{r+1}}=1} &
\end{tikzcd}$$

given by compatibility of corestriction. The result now follows upon taking the inverse limit because the right-hand term of the short exact sequence vanishes. ■

Remark 74. Technically, all of these constructions have integrality built in, so we must work with V defined over $\mathbb{Z}_p$. Notably, the last sentence needs V to be over $\mathbb{Z}_p$.