

ARITHMETIC INVARIANT AND GEOMETRY

HARUZO HIDA

The first two to three lectures are an introductory discussion of problems concerning non-triviality of arithmetic invariant. For example, non-vanishing of L -values/values of modular forms modulo p , non-vanishing of \mathcal{L} -invariants in most cases of modular adjoint L -function, non-vanishing of Iwasawa power series of p -adic L -functions modulo p (vanishing of its μ -invariant) and high growth of Hecke fields over a p -adic analytic family.

Nonvanishing mod p results have seen powerful applications in divisibility problems of class numbers (see [W78], [FW79] and [ICF] Chapter 7) and in many proofs of the main conjectures in Iwasawa's theory. Recently, new methods of proving nonvanishing emerged in the work of Vatsal, Finis and myself (an overview of these works is in [V06]). In the first two to three lectures, we describe a geometric method, which was started by Sinnott in [Si84] and [Si87] and has been generalized in [H04], [H07], [H10a] and [H10b] via the theory of Shimura varieties.

We touch other invariants in later lectures.

Date: October 13, 2010.

Two first two lecture at Kyoto university 10/4 and 10/8/2010; the author is partially supported by the following NSF grants in the past 10 years up to today: DMS 9988043, DMS 0244401, DMS 0753991 and DMS 0854949 and by Clay Mathematics Institute as a Senior Scholar.

1. LECTURE 1: DIRICHLET L -VALUES MODULO p

1.1. **Statement of the theorem for Dirichlet L -values.** We consider the group scheme $\mathbb{G}_m = \text{Spec}(\mathbb{Z}[t, t^{-1}])$. We fix a Dirichlet character λ of $(\mathbb{Z}/N\mathbb{Z})^\times$ with $\lambda(-1) = -1$ and two embeddings $\mathbb{C} \xrightarrow{i_\infty} \overline{\mathbb{Q}} \xrightarrow{i_p} \overline{\mathbb{Q}}_p$. We regard λ as having values in any one of the three fields. Consider a rational function:

$$\Phi(t) = \Phi_\lambda(t) = \sum_{n=1}^{\infty} \lambda(n)t^n = \frac{\sum_{a=1}^N \lambda(a)t^a}{1-t^N} \in \mathbb{Z}[t, t^{-1}]_{(p, t-1)} = \mathcal{O}_{\mathbb{G}_m, 1}.$$

Since the numerator $\sum_{a=1}^N \lambda(a)t^a$ is divisible by $(t-1)$, the rational function Φ is finite at $t=1$.

Exercise 1.1. Why is the numerator $\sum_{a=1}^N \lambda(a)t^a$ divisible by $(t-1)$?

As Euler (essentially) discovered in 1735 (see [LFE] §2.3),

$$\Phi(1) = L(0, \lambda) \in \overline{\mathbb{Q}}.$$

Thus $L(0, \lambda)$ is a p -adic integer in the ring $\mathbb{Z}_p[\lambda]$ generated by the values of λ . Writing \mathfrak{P} for the maximal ideal of the p -adic valuation ring of $\overline{\mathbb{Q}}_p$, the theorem of Washington can be stated as follows:

Theorem 1.2. For almost all characters $\chi : \mathbb{Z}_\ell^\times \rightarrow \mu_{l^\infty}$, $L(0, \lambda\chi) \not\equiv 0 \pmod{\mathfrak{P}}$.

By Kummer's class number formula, we can relate this statement to the statement on the l -power cyclotomic class number.

The automorphic proof of this theorem has several steps.

(Step1) *Hecke operators:* Introduction of Hecke operators $U(l)$ acting on rational functions on $\mathbb{G}_m/\overline{\mathbb{F}}_p$ and functions on μ_{l^∞} .

(Step2) *Measure associated to $U(l)$ -eigenforms:* Choose a sequence of generators ζ_n in μ_{l^n} so that $\zeta_n^l = \zeta_{n-1}$ (for example, $\zeta_n = \exp(\frac{2\pi i}{l^n})$). Fix an isomorphism $\mathbb{Z}_l \cong \mathbb{Z}_l(1) = \varprojlim_n \mu_{l^n}$ given by $\mu_{l^n} \ni \zeta_n^a \mapsto a \in \mathbb{Z}/l^n\mathbb{Z}$. For an eigenform $\phi|U(l) = a\phi$ with unit eigenvalue $a \in \overline{\mathbb{F}}_p^\times$, construction of a measure $d\mu_\phi$ on \mathbb{Z}_l^\times with $\int_{a+l^n\mathbb{Z}_\ell} d\mu_\phi \doteq \phi(\zeta_n^a)$ for the image ζ_n^a of ζ^a in μ_{l^n} . Here a measure μ on \mathbb{Z}_l with values in $\overline{\mathbb{F}}_p$ is a $\overline{\mathbb{F}}_p$ -linear functional defined on a space $\mathcal{C}(\mathbb{Z}_l; \overline{\mathbb{F}}_p)$ of continuous functions: $\mathbb{Z}_l \rightarrow \overline{\mathbb{F}}_p$. Thus $\mu : \mathcal{C}(\mathbb{Z}_l; \overline{\mathbb{F}}_p) \rightarrow \overline{\mathbb{F}}_p$ is an $\overline{\mathbb{F}}_p$ -linear map.

(Step3) *Evaluation formula:* For a character $\chi : \Gamma = \mathbb{Z}_l^\times/\mu_{l-1} \rightarrow \overline{\mathbb{F}}_p^\times$:

$$L(0, \lambda\chi^{-1}) \doteq \int_{\mathbb{Z}_l^\times} \chi d\mu_\Phi = \int_\Gamma \chi d\mu_\Psi$$

for $\Psi(\zeta) = \sum_{\varepsilon \in \mu_{l-1}} \Phi(\zeta^\varepsilon)$ (not ζ^ε is defined only for $\zeta \in \mu_{l\infty}$).

(Step4) *Zariski density:* Regard Ψ as induced from the rational function $\tilde{\Psi}(t_\varepsilon) = \sum_{\varepsilon \in \mu_{l-1}/\{\pm 1\}} (\Phi(t_\varepsilon) + \Phi(t_\varepsilon^{-1}))$ on $G = \mathbb{G}_m^{\mu_{l-1}/\{\pm 1\}}$ by pull-back under the embedding $i : \mu_{l\infty} \hookrightarrow G$ given by $\zeta \mapsto (\zeta^\varepsilon)$. The Zariski density of $i(\mu_{l\infty})$ in a big subvariety in G defined by the relation of $\varepsilon \in \mu_{l-1}$ implies the constancy of $\tilde{\Psi}$ and hence of Φ (a contradiction) if $\int_{\mathbb{Z}_l^\times} \chi d\mu_\Phi = 0$ for infinitely many characters. For example, if $l = 7$, $\{1, \omega, \omega^2\} = \mu_3 \cong \mu_6/\{\pm 1\}$, and $1 + \omega + \omega^2 = 0$ gives $t_{\omega^2} t_\omega t_1 = 1$; so, the big subvariety is the one defined by $t_{\omega^2} t_\omega t_1 = 1$. The Zariski density is the idea of Sinnott [Si87].

We are going to describe each step.

1.2. Hecke operators. A little more generally, we start with $\mu_{l\infty}$ over an integral domain B whose quotient field is K . Take an algebraic closure \overline{K} of K . We suppose that l is invertible in B and all l -power roots of are in B . Fix a prime l prime to p . Define a Hecke operator $U(l)$ acting on functions ϕ on $\mu_{l\infty}$ by

$$\phi|U(l^h)(t) = \frac{1}{l^h} \sum_{\zeta \in \mu_{l^h}} \phi(\zeta t^{1/l^h}) = \frac{1}{l^h} \sum_{T^{l^h}=t} \phi(T).$$

Exercise 1.3. *Prove*

- (1) $U(l^h) = U(l)^h$ for $h = 1, 2, \dots$,
- (2) $a(n, \phi|U(l)) = a(nl, \phi)$ if $\phi(t) = \sum_{n \gg -\infty} a(n, \phi)t^n$ is a rational function on \mathbb{G}_m .

From this we conclude $\Phi|U(l) = \lambda(l)\Phi$. Hence Φ is a Hecke eigen function in

$$\mathcal{O}_{\mathbb{G}_m, 1} = \{\phi \in \overline{\mathbb{F}_p}(\mathbb{G}_m) | \phi \text{ is finite at } 1\} \quad (\text{the stalk of } \mathcal{O}_{\mathbb{G}_m} \text{ at } 1).$$

1.3. Measure associated to a $U(l)$ -eigen function. Since $\mathbb{Z}_\ell(1)$ is compact, any continuous function $f : \mathbb{Z}_\ell(1) \rightarrow \overline{\mathbb{F}_p}$ is a locally constant function. For a measure $\mu : \mathcal{C}(\mathbb{Z}_\ell(1); \overline{\mathbb{F}_p}) \rightarrow \overline{\mathbb{F}_p}$, we often write $\int_U f \chi_U d\mu$ for $\mu(f\chi_U)$ for the characteristic function χ_U of an open set $U \subset \mathbb{Z}_\ell(1)$.

Fix an identification $\mathbb{Z}_\ell(1) \cong \mathbb{Z}_\ell$, which is equivalent to choose a primitive l^n -th root ζ_{l^n} so that $\zeta_{l^{n+1}}^l = \zeta_{l^n}$. We have a coset decomposition

$$\mathbb{Z}_\ell(1) = \bigsqcup_{z \bmod \ell^n} \zeta_{l^n}^z \mathbb{Z}_\ell(1)^{l^n} = \bigsqcup_{z \bmod l^n} (z + l^n \mathbb{Z}_\ell)$$

for every n . The measure μ is determined by assigning the value $\Phi(\zeta_n^z) = \int_{\zeta_n^z \mathbb{Z}_\ell(1)^{l^n}} d\mu$ to $\zeta_n^z \mathbb{Z}_\ell(1)^{l^n}$. To be well defined, these values have to satisfy the following distribution relation for $n = 1, 2, \dots, \infty$:

$$\begin{aligned} \text{(Dist1)} \quad \Phi(\zeta_n^w) &= \int_{\zeta_n^w \mathbb{Z}_\ell(1)^{l^n}} d\mu = \sum_{z \equiv w \pmod{l^n}, z \in \mathbb{Z}/l^{n+1}\mathbb{Z}} \int_{\zeta_n^z \mathbb{Z}_\ell(1)^{l^{n+1}}} d\mu \\ &= \sum_{z \equiv w \pmod{l^{n+1}}} \Phi(\zeta_{n+1}^z) = \sum_{\zeta \in \mu_{l^{n+1}}, \zeta^l = \zeta_n^w} \Phi(\zeta) = l\Phi|U(l)(\zeta_n^w). \end{aligned}$$

In other words, if $\phi|U(l) = a\phi$ with $a \neq 0$, we can take $\Phi(\zeta_n^z) = l^{-n}a^{-n}\phi(\zeta_n^z)$, and get a measure μ_ϕ .

Let $B = \overline{\mathbb{F}}_p$ or $\overline{\mathbb{Q}}_p$. Let $\mathcal{O}_{\mathbb{G}_m, 1/B} = \{\phi \in B(\mathbb{G}_m) | \phi \text{ is finite at } t = 1\}$. Formally, adding the variable t , we may define a measure with variable

$$(la)^n \int f d\mu_\phi(t) = \sum_{x \in \mathbb{Z}/l^n\mathbb{Z}} f(x)\phi(\zeta_n^x t) \in \mathcal{O}_{\mathbb{G}_m, 1/B},$$

and then, $\int f d\mu_\phi$ is its evaluation at $t = 1$: $\int f d\mu_\phi(1)$. We then have for a primitive Dirichlet character $\chi : (\mathbb{Z}/l^n\mathbb{Z})^\times \rightarrow B^\times$

$$\begin{aligned} (la)^n \int \chi d\phi(t) &= \sum_x \sum_m \chi(x)a(m, \phi)(\zeta_n^x t)^m \\ &= \sum_m \left(\sum_{x \in \mathbb{Z}/l^n\mathbb{Z}} \chi(x)\zeta_n^{mx} \right) a(m, \phi)t^m = G(\chi) \sum_m \chi^{-1}(m)a(m, \phi)t^m, \end{aligned}$$

where $G(\chi)$ is the Gauss sum: $G(\chi) = \sum_{x \in \mathbb{Z}/l^n\mathbb{Z}} \chi(x)\zeta^x \neq 0$.

1.4. Evaluation formula. Applying the computation in the previous section to $\phi = \Phi_\lambda = \sum_{m=0}^{\infty} \lambda(m)t^m$ and evaluating the result at $t = 1$, we find

$$\int \chi d\mu_\Phi = (l\lambda(l))^{-n} G(\chi) \Phi_{\chi^{-1}\lambda}(1) = (l\lambda(l))^{-n} G(\chi) L(0, \chi^{-1}\lambda).$$

Since $\chi \neq 1$ is supported on \mathbb{Z}_ℓ^\times , we may restrict $d\mu_\Phi$ to \mathbb{Z}_ℓ^\times .

Since any character $\chi : \mathbb{Z}_\ell^\times \rightarrow \mu_{l^\infty}$ factors through $\Gamma = \mathbb{Z}_\ell^\times / \mu_{l-1}$, we want to have a measure φ supported on $\Gamma = \mathbb{Z}_\ell^\times / \mu_{l-1}$ so that we have

$$\int_\Gamma \chi d\varphi = \int_{\mathbb{Z}_\ell^\times} \chi d\mu_\Phi \quad \text{for all character } \chi \text{ of } \Gamma.$$

The measure φ is not associated to a rational function like Φ , but if we allow functions on μ_{l^∞} , φ is associated to a function Ψ close to Φ .

Noting that $\mu_{l-1} \subset \mathbb{Z}_\ell$ acts such functions by $\phi(\zeta) \mapsto \phi(\zeta^s)$ ($s \in \mathbb{Z}_\ell$), we find that $\varphi = d\mu_\Psi$ for Ψ given by

$$\Psi(\zeta) = \sum_{\varepsilon \in \mu_{l-1}} \Phi(\zeta^\varepsilon) = \sum_{\varepsilon \in \mu_{l-1}/\{\pm 1\}} (\Phi(\zeta^\varepsilon) + \Phi(\zeta^{-\varepsilon})) \quad \text{if } l \nmid N.$$

1.5. Zariski density. Assuming that $B = \overline{\mathbb{F}}_p$, we now state the following result in [Si87]:

Theorem 1.4 (Sinnott). *Let $\Xi \subset \mu_{l^\infty}(\overline{\mathbb{F}}_p)$ be an infinite set. Let \mathcal{F} be the $\overline{\mathbb{F}}_p$ -algebra of functions on Ξ with values in $\overline{\mathbb{F}}_p$. If $a_1, \dots, a_r \in \mathbb{Z}_\ell$ are linearly independent over \mathbb{Z} , the algebra homomorphism from the affine ring $R_0 = \overline{\mathbb{F}}_p[y_1, y_1^{-1}, \dots, y_r, y_r^{-1}]$ of \mathbb{G}_m^r sending y_j to a function on Ξ given by $\zeta \mapsto \zeta^{a_i}$ for $i = 1, 2, \dots, r$ is injective.*

We prove this theorem after stating a couple of exercises and a lemma.

Exercise 1.5. *Let K be a field and L/K be a finite field extension. Suppose that $K \supset \mu_l(\overline{K})$. For $\zeta \in \mu_{l^\infty}(L)$, prove that*

$$\mathrm{Tr}_{L/K}(\zeta) = \begin{cases} 0 & \text{if } \zeta \notin K, \\ [L : K]\zeta & \text{if } \zeta \in K. \end{cases}$$

Lemma 1.6. *If $b_1, \dots, b_s \in \mathbb{Z}_\ell$ be finitely many elements distinct in $\mathbb{Z}/l^N\mathbb{Z}$ for a given integer $N > 0$, then the zero set of the function $f : \mu_{l^\infty} \rightarrow \overline{\mathbb{F}}_p$ given by $f(\zeta) = \sum_{j=1}^r c_j \zeta^{b_j}$ with $c_1, \dots, c_s \in \overline{\mathbb{F}}_p$ is a finite set.*

Proof. Let k be the finite field generated by c_j ($j = 1, 2, \dots, r$) and $\mu_l(\overline{\mathbb{F}}_p)$ over \mathbb{F}_p . We write $l^{N_0} = |k \cap \mu_{l^\infty}(\overline{\mathbb{F}}_p)|$. By Exercise 1.5 applied to $K = k$, we have $\mathrm{Tr}_{k(\zeta)/k}(\zeta) = 0$ if $\zeta \in \mu_{l^\infty}(\overline{\mathbb{F}}_p) - k$. Thus if $f(\zeta) = 0$ for $\zeta \notin \mu_{l^M}(\overline{\mathbb{F}}_p)$ for $M = N_0 + N$, $0 = \mathrm{Tr}_{k(\zeta)/k}(\zeta^{-b_i} f(\zeta)) = [k(\zeta) : k]c_i$, because $\zeta^{b_j - b_i} \notin k$ ($i \neq j$). Since $[k(\zeta) : k]$ is an l -power, we find that the zero set is contained in $\mu_{l^M}(\overline{\mathbb{F}}_p)$. \square

Here is the proof of the theorem by Sinnott: Since a_1, \dots, a_r are linearly independent over \mathbb{Z} , for all monomials $y^k = y_1^{k_1} \dots y_r^{k_r}$ with $k = (k_1, \dots, k_r) \in \mathbb{Z}^r$ appearing in a nonzero Laurent polynomial $f(y_1, \dots, y_r)$ in R_0 , the l -adic numbers $k_1 a_1 + \dots + k_r a_r$ are distinct. Let us order these finitely many l -adic numbers $k_1 a_1 + \dots + k_r a_r$ as b_1, b_2, \dots, b_s . Since they are distinct in \mathbb{Z}_ℓ , there exists $0 < N \in \mathbb{Z}$ such that $b_j \pmod{l^N}$ are distinct. Thus the function $\zeta \mapsto f(\zeta^{a_1}, \dots, \zeta^{a_r})$ has only finitely many zeros in μ_{l^∞} ; so, $f \neq 0$ in \mathcal{F} . Thus the map $R_0 \rightarrow \mathcal{F}$ is injective. \square

To conclude the assertion of (Step4), we need to make the following variable change: Let A be the additive subgroup of \mathbb{Z}_ℓ generated by μ_{l-1} and take a \mathbb{Z} -basis $I = \{a_1, \dots, a_r\}$ of A . Take a complete set of representatives $\varepsilon_1, \dots, \varepsilon_n$ for $\mu_{l-1}/\{\pm 1\}$ and write $\varepsilon_j = \sum_i c_{ij} a_i$ ($c_{ij} \in \mathbb{Z}$). Write $T = \mathbb{G}_m^{\mu_{l-1}/\{\pm 1\}} = \text{Spec}(R)$ (resp. $Y = \text{Spec}(R_0) = \mathbb{G}_m^I$) for $R = \overline{\mathbb{F}}_p[t_1, t_1^{-1}, \dots, t_n, t_n^{-1}]$ (resp. $R_0 = \overline{\mathbb{F}}_p[y_1, y_1^{-1}, \dots, y_r, y_r^{-1}]$). Here t_j corresponds to the component indexed by ε_j . Consider the ring homomorphism $\pi^* : R \hookrightarrow R_0$ sending t_j to $\prod_i y_i^{c_{ij}}$. This algebra homomorphism is the pull-back of a group homomorphism $\pi : Y \rightarrow T$ given as follows: Note that $Y = \mathbb{G}_m \otimes_{\mathbb{Z}} \mathbb{Z}^r$ ($A = \mathbb{Z}^r$ via the basis $\{a_i\}$) and $T := \text{Spec}(R) = \mathbb{G}_m \otimes_{\mathbb{Z}} \mathbb{Z}^n$. Regard \mathbb{Z}^r and \mathbb{Z}^n as row vector modules. For the $r \times n$ matrix $C = (c_{ij})$, $C : \mathbb{Z}^r \rightarrow \mathbb{Z}^n$ given by $x \mapsto xC$ induces $\pi : Y = \text{Spec}(R_0) \cong \mathbb{G}_m \otimes_{\mathbb{Z}} \mathbb{Z}^r \xrightarrow{\text{id} \otimes C} \mathbb{G}_m \otimes_{\mathbb{Z}} \mathbb{Z}^n \cong \text{Spec}(R) = T$; so, π is a morphism of algebraic groups. Since a_1, \dots, a_r is a basis of A and $\varepsilon_1, \dots, \varepsilon_n$ generate A , the matrix C has rank r ; so, $C : \mathbb{Z}^r \rightarrow \mathbb{Z}^n$ is injective. This shows that $\text{Ker}(\pi)$ is finite.

Exercise 1.7. *Why is $\text{Ker}(\pi)$ finite?*

Lemma 1.8. *For an infinite subset $\Xi \subset \mu_{l^\infty}$, $\tilde{\Xi} = \{(\zeta^{\varepsilon_1}, \dots, \zeta^{\varepsilon_n}) \in T(\overline{\mathbb{F}}_p) \mid \zeta \in \Xi\}$ is the image of $\Xi_Y := \{(\zeta^{a_1}, \dots, \zeta^{a_r}) \in Y(\overline{\mathbb{F}}_p) \mid \zeta \in \Xi\}$ under π and is Zariski dense in $\pi(Y)$.*

Proof. Note

$$\zeta^{\varepsilon_j} = \zeta^{\sum_i a_i c_{ij}} \Leftrightarrow t_j|_{t_j=\zeta^{\varepsilon_j}} = \prod_i y_i^{c_{ij}}|_{y_i=\zeta^{a_i}} = \pi(t_j)|_{y_i=\zeta^{a_i}}.$$

Thus we find $\tilde{\Xi} = \pi(\{\zeta^{a_1}, \dots, \zeta^{a_r}\} \in Y \mid \zeta \in \Xi)$. Take $f \in R$. We need to show that if $f(\pi(\zeta^{\varepsilon_1}, \dots, \zeta^{\varepsilon_n})) = 0$ for all $\zeta \in \Xi$, we have $f|_{\pi(Y)} = 0$. The vanishing $f|_{\tilde{\Xi}} = 0$ implies $f|_{\Xi} = 0$ in \mathcal{F} . Then by Theorem 1.4, $f|_{\pi(Y)} = 0$; so, $\tilde{\Xi}$ is dense in $\pi(Y)$. \square

In the following section, we conclude the assertion of (Step4) from

Lemma 1.9. *Let the notation be as above. Then a relation of the form:*

$$(*) \quad (P_1(t_1) + \dots + P_n(t_n))|_{\pi(Y)} = 0$$

for $P_j(z) \in \overline{\mathbb{F}}_p[z, z^{-1}]$ can only occur if $P_j(z) \in \overline{\mathbb{F}}_p$ for all j .

Proof. Since a_j is a basis of A , the equation $\varepsilon_j = \sum_i c_{ij} a_i$ determines integers $(c_{ij})_i$ uniquely. Since $t_j = \prod_i y_i^{c_{ij}}$ on $\pi(Y)$, $P_i(t_i)|_{\pi(Y)}$ and $P_j(t_j)|_{\pi(Y)}$ for $i \neq j$ do not contain common monomials of y_i as an element of R_0 . Since monomials of $\{y_i\}_i$ are linearly independent over $\overline{\mathbb{F}}_p$, we find that the relation $(*)$ implies $P_i(z) \in \overline{\mathbb{F}}_p$ for all i . \square

1.6. Proof of Theorem 1.2 via Zariski density. We first assume that $\int_{\Gamma} \chi d\varphi = 0$ (that is, $L(0, \chi^{-1}\lambda) \equiv 0 \pmod{\mathfrak{P}}$) for all $\chi : \Gamma \rightarrow \mu_{l^\infty}$. Then by orthogonality relation of characters, we find $\tilde{\Psi}(\zeta) = 0$ for all $\zeta \in \mu_{l^\infty}$. Since the image of μ_{l^∞} in $\mathbb{G}_m^{\mu_{l-1}/\{\pm 1\}}$ by $\zeta \mapsto (\zeta^\varepsilon)_\varepsilon$ is Zariski dense in $\pi(Y)$ (over $\overline{\mathbb{F}}_p$), we find that $\Phi(t_\varepsilon) + \Phi(t_\varepsilon^{-1})$ is constant by Lemma 1.9, which is impossible by the t -expansion of Φ . As we show now, from a slightly weaker Zariski density in $Y = \mathbb{G}_m^I$ proven by Sinnott (Theorem 1.4), we can still conclude that a nonconstant linear combination of translations of $\Phi(t^\varepsilon)$ (under the multiplication on \mathbb{G}_m) is a constant in $\overline{\mathbb{F}}_p$. By this contradiction, we get the generic nonvanishing of the L -values.

Proof of Theorem 1.2. Our way of proof is via contradiction. Thus we assume that we have an infinite sequence of characters $\{\chi_j\}_j$ of order l^{n_j} with $\int_{\Gamma} \chi_j d\varphi = 0$, which implies by variable change:

$$\int_{\Gamma} \chi_j(x) d\varphi(ax) \stackrel{x \mapsto a^{-1}x}{=} \chi_j(a)^{-1} \int_{\Gamma} \chi_j d\varphi = 0.$$

Exercise 1.10. For any field k of characteristic different from l , prove the following formula for a primitive l^n -th root of unity ζ_{l^n} with $n \geq 2$ not in k :

$$\mathrm{Tr}_{k[\zeta_{l^n}]/k}(\zeta_{l^n}^x) \neq 0 \Leftrightarrow \zeta_{l^n}^x \in k \text{ for } x \in \mathbb{Z}_\ell.$$

Hint: This follows from Exercise 1.5 and the minimal polynomial of ζ_{l^n} : $X^{l^{n-1}(l-1)} + X^{l^{n-1}(l-2)} + \dots + 1 = 0$ over \mathbb{Z} .

For simplicity, we assume that λ has values in \mathbb{F}_p^\times . Then applying the Frobenius automorphism $F(x) = x^p$, we find for $\chi = \chi_j$

$$\begin{aligned} 0 &= \left(\int_{\Gamma} \chi(x) d\varphi(ax) \right)^{p^n} = \left(\sum_u \chi(u) \Psi(\zeta_{l^n}^{au}) \right)^{p^n} \\ &= \sum_u \chi^{p^n}(u) \Psi(\zeta_{l^n}^{aup^n}) = \chi^{p^n}(p^n)^{-1} \int_{\Gamma} \chi^{p^n} d\varphi(ax) \end{aligned}$$

for all n . Thus taking the trace from the field $\mathbb{F}_p[\chi_j]$ generated by the values of χ_j to $\mathbb{F}_p[\mu_l]$, we find that

$$\sum_{u \in \chi_j^{-1}(\mathbb{F}_p[\mu_l]) \subset \Gamma/\Gamma^{l^{n_j}}} \chi_j(u) \Psi(\zeta_{l^{n_j}}^{au}) = 0$$

for all $a \in \Gamma$. The above sum only involves $u \in \Gamma^{l^{n_j-m}}/\Gamma^{l^{n_j}}$. Writing the order of the l -primary part of $(\mathbb{F}_p[\mu_l])^\times$ as l^m and taking n_j so that $n_j \geq 2m$, we can identify the multiplicative group $\Gamma^{l^{n_j-m}}/\Gamma^{l^{n_j}}$ with the

additive one $\mathbb{Z}/l^m\mathbb{Z}$ by $\mathbb{Z}/l^m\mathbb{Z} \ni v \mapsto 1 + l^{n_j-m}v = u$. We can then write $\chi_j(u) = \zeta_{l^m}^{b_j v}$ for $b_j \in (\mathbb{Z}/l^m\mathbb{Z})^\times$ and $\zeta_{l^m}^{au} = \zeta_{l^n}^a \zeta_{l^m}^v$. Since $\{\chi_j\}$ is infinite, we may assume that b_j is a constant b . Then we have for any $a \in \mathbb{Z}_l^\times$

$$\sum_{v \pmod{l^m}} \zeta_{l^m}^{bv} \Psi(\zeta_{l^{n_j}}^a \zeta_{l^m}^v) = \sum_{v \pmod{l^m}} \zeta_{l^m}^{bv} \Psi|_{\zeta_{l^m}^v}(\zeta_{l^{n_j}}^a) = 0,$$

where for $f \in \overline{\mathbb{F}}_p(\mathbb{G}_m)$, $f|x \in \overline{\mathbb{F}}_p(\mathbb{G}_m)$ is defined by $f|x(t) = f(tx)$ for $x \in \mathbb{G}_m(\overline{\mathbb{F}}_p)$. Since $\pi(\Xi)$ for $\Xi = \bigcup_j \mu_{l^{n_j}}^\times$ is still dense in Y , applying Lemma 1.9 to $P_j(z) = \Phi'_j(z) + \Phi'_j(z^{-1})$ for

$$\Phi'_j(z) = \sum_{v \pmod{l^m}} \zeta_{l^m}^{bv} \Phi|_{\zeta_{l^m}^v}(z)$$

on $\mathbb{G}_m = \text{Spec}(\overline{\mathbb{F}}_p[z, z^{-1}])$, we conclude $P_j(z) \in \overline{\mathbb{F}}_p$. Let us compute the Taylor expansion at $z = 1$ of $P_j(z)$. We have

$$\begin{aligned} \Phi'_j(z) &= \sum_{v \pmod{l^m}} \zeta_{l^m}^{bv} \Phi|_{\zeta_{l^m}^v}(z) \\ &= \sum_v \zeta_{l^m}^{bv} \sum_{n=1}^{\infty} \lambda(n) (\zeta_{l^m} t)^n \\ &= \sum_{n \geq 1} \lambda(n) t^n \sum_v \zeta_{l^m}^{(b+n)v} \\ &= l^m \sum_{n > 0, n \equiv -b \pmod{l^m}} \lambda(n) t^n, \end{aligned}$$

which is nonconstant, and P_j is also nonconstant. This finishes the proof of Theorem 1.2.