Math 726: L-functions and modular forms Fall 2011

Lecture 1: Overview of the course

Instructor: Henri Darmon *Notes written by: Luca Candelori*

Examples of L-functions

Roughly speaking, a L-function is a **generating series for arithmetic data**. Far from being a rigorous mathematical definition, that is nevertheless the guiding principle underlying the construction of every L-function, as the following examples show.

Example 1. The most elementary L-function is the **Riemann zeta function**. This is defined by the infinite series:

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

where $s \in \mathbb{C}$ must have $\Re[s] > 1$ to ensure convergence. This series has a product expansion, discovered by Euler:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1-p^{-s}}$$

which highlights its arithmetic properties. Such product expansion is a common feature of L-functions in general.

Example 2. The construction of Example 1 can be readily generalized to number fields. Let $K/\mathbb{Q}$ be a number field, and denote by $\mathcal{O}_K$ its ring of integers. The **Dedekind zeta function** of the number field K is defined by the infinite series:

$$\zeta_K(s) := \sum_{\mathfrak{a} \subset \mathcal{O}_K} \frac{1}{N_{K/\mathbb{Q}}(\mathfrak{a})^s} \qquad (\Re[s] > 1)$$

where the sum runs through all the non-zero integral ideals $\mathfrak{a}$ of K and $N_{K/\mathbb{Q}}$ is the ideal norm. Note that for $K = \mathbb{Q}$ we recover the Riemann zeta function, so this is a true generalization of Example 1. However, for a general number field K it no longer makes sense to form an infinite series by adding up *all* the integers, but rather just the integral ideals. A simple reason for this procedure is that convergence is no longer guaranteed whenever there are infinitely many units in $\mathcal{O}_K$. Moreover, unique factorization of ideals in a number field gives the product expansion:

$$\sum_{\mathfrak{a} \subset \mathcal{O}_K} \frac{1}{N_{K/\mathbb{Q}}(\mathfrak{a})^s} = \prod_{\mathfrak{p} \subset \mathcal{O}_K} \frac{1}{1-N_{K/\mathbb{Q}}(\mathfrak{p})^{-s}}$$

which would not be available if we included *every* integer in the series defining ζ_K.

From the product expansion, we deduce that Dedekind's ζ_K function is constructed entirely from **local** data, namely the size of the residue field of each prime ideal $\mathfrak{p}$ of K. The **class number formula**

$$\lim_{s\to 1^+}(s-1)\zeta_K(s) = \frac{h_K \cdot R_K}{w_K \cdot \sqrt{|D_K|}} \cdot 2^{r_1} \cdot (2\pi)^{r_2} \tag{1}$$

then asserts that this local data can be patched together to compute **global** invariants of K, namely:

h_K = Class number of K, $\qquad$ D_K = Discriminant of K,

R_K = Regulator of K, $\qquad$ w_K = number of roots of unity in K,

$[K:\mathbb{Q}] = n = r_1 + 2r_2$ where r_1 (resp. $2r_2$) is the number of real (resp. complex) embeddings of K.

From this point of view, L-functions can be seen as an attempt to patch local information together to yield global information about an arithmetic object.

Example 3. Emil Artin's **very influential idea** was to associate an L-function $L(\rho, s)$ to any continuous representation:

$$\rho : G_{\mathbb{Q}} \longrightarrow \mathbf{GL}_d(\mathbb{C}) \tag{2}$$

of the absolute Galois group $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. In many ways, number theory as a whole *is* the study of $G_{\mathbb{Q}}$, and the study of such complex Galois representations ρ is a natural starting point.

How can we attach a L-function to a complex Galois representation such as (2)? The key idea is to consider **Frobenius elements** attached to rational primes p. For each prime p, consider the p-adic completion $\mathbb{Q}_p$ of $\mathbb{Q}$, and pick an algebraic closure $\overline{\mathbb{Q}_p}$. The Galois group $G_{\mathbb{Q}_p}$ has a much simpler structure than $G_{\mathbb{Q}}$, and it provides the local data that we would like to patch together, in the following manner. The fields $\mathbb{Q}_p$, $\overline{\mathbb{Q}_p}$ have rings of integers $\mathbb{Z}_p$ and $\overline{\mathbb{Z}_p}$ respectively, on which $G_{\mathbb{Q}_p}$ acts. Reduction modulo p then relates $G_{\mathbb{Q}_p}$ to $G_{\mathbb{F}_p}$:

$$\begin{array}{ccccc}
\overline{\mathbb{Q}} & \hookrightarrow & \overline{\mathbb{Q}_p} \supseteq \overline{\mathbb{Z}_p} & \xrightarrow{\mathrm{red}_p} & \overline{\mathbb{F}_p} \\
\Big\downarrow{\scriptstyle G_{\mathbb{Q}}} & & \Big\downarrow{\scriptstyle G_{\mathbb{Q}_p}} & & \Big\downarrow{\scriptstyle G_{\mathbb{F}_p}} \\
\mathbb{Q} & \hookrightarrow & \mathbb{Q}_p \supseteq \mathbb{Z}_p & \xrightarrow{\mathrm{red}_p} & \mathbb{F}_p
\end{array}$$

Now $G_{\mathbb{Q}_p}$ sits inside $G_{\mathbb{Q}}$ as the **decomposition group** D_p of p (this is only defined up to conjugation in $G_{\mathbb{Q}}$). Inside D_p we have the **inertia group**

$$I_p := \{\sigma \in D_p : \overline{\sigma} = \mathrm{id}\}$$

where by $\overline{\sigma}$ we mean the element of $G_{\mathbb{F}_p}$ obtained by considering the action of σ on $\overline{\mathbb{F}_p}/\mathbb{F}_p$. We then have an isomorphism:

$$D_p/I_p \simeq G_{\mathbb{F}_p}$$

and

$$G_{\mathbb{F}_p} \simeq \varprojlim (\mathbb{Z}/n\mathbb{Z}) = \widehat{\mathbb{Z}}$$

is a profinite group generated by a single element $\sigma_p : x \mapsto x^p$ called the **Frobenius element** at p.

Going back to our representation $\rho : G_{\mathbb{Q}} \longrightarrow \mathbf{GL}(V)$, V a complex vector space of dimension d, we see that we have a canonical conjugacy class $\rho(\sigma_p)$ of linear maps acting on V^{I_p}, the subspace of V on which $\rho(I_p)$ acts as the identity. The **Artin L-function of** (V, ρ) is the L-function defined by the product:

$$L(\rho, s) := \prod_p \frac{1}{\det(1 - \rho(\sigma_p)|_{V^{I_p}} \cdot p^{-s})}.$$

Note that the characteristic polynomial of $\rho(\sigma_p)$ only depends on its conjugacy class, and therefore the product is well-defined.

Whenever $\rho(I_p) = \mathrm{id}$ we say that ρ is **unramified** at p. In this case, we can take $\rho(\sigma_p)$ to act on all of V. By topological considerations, we can moreover deduce that $\rho(\sigma_p)$ must be of finite order in $\mathbf{GL}(V) = \mathbf{GL}_d(\mathbb{C})$. The eigenvalues of $\rho(\sigma_p)$ are then roots of unity $\zeta_1^{(p)}, \ldots, \zeta_d^{(p)}$ and we obtain the following factorization:

$$L(\rho, s) := \prod_{p \text{ unramified}} \frac{1}{1 - \zeta_1^{(p)} p^{-s}} \cdot \ldots \cdot \frac{1}{1 - \zeta_d^{(p)} p^{-s}} \times \prod_{p \text{ ramified}} (\text{`Euler factors'}).$$

Note that the Euler factors come from lower-dimensional representations. For example, if $V^{I_p} = 0$ then the Euler factor at p is just 1.

Artin L-functions generalize the two previous L-functions of Examples 1 and 2. We just have to pick the right representation ρ:

- $\zeta(s) = L(\rho_{\mathrm{triv}}, s)$, where $\rho_{\mathrm{triv}} : G_{\mathbb{Q}} \to \mathrm{Aut}(\mathbb{C})$ is the trivial representation $\rho(\sigma) = 1$.
- $\zeta_K(s) = L(\mathrm{ind}_{G_K}^{G_{\mathbb{Q}}} \rho_{\mathrm{triv}}, s)$ where $\rho_{\mathrm{triv}} : G_K \to \mathrm{Aut}(\mathbb{C})$ is the trivial representation of $G_K \subset G_{\mathbb{Q}}$ (this will be given as an exercise in Homework 1).

Note in particular that if $K/\mathbb{Q}$ is Galois, then ζ_K is the Artin L-function corresponding to the regular representation of $\mathrm{Gal}(K/\mathbb{Q})$.

EXAMPLE 4. In the same spirit as the the Artin L-functions, where we attach a L-function to a Galois representation with complex coefficients, we can define L-functions attached to **Galois representations with ℓ-adic coefficients**. These are continuous maps:

$$\rho : G_{\mathbb{Q}} \longrightarrow \mathbf{GL}_d(\mathbb{Q}_\ell) = \mathrm{Aut}(V) \tag{3}$$

where V is a d-dimensional $\mathbb{Q}_\ell$-vector space. Following the example of Artin L-functions, we are led to define:

$$L(\rho, s) := \prod_p \frac{1}{\det(1 - \rho(\sigma_p)|_{V^{I_p}} \cdot p^{-s})}. \tag{4}$$

There is an immediate problem with this definition: we are trying to evaluate the characteristic polynomial of $\rho(\sigma_p)|_{V^{I_p}}$, which has coefficients in $\mathbb{Q}_\ell$, at a complex number p^{-s}. This is not possible in general, hence we need to restrict our attention to specific classes of ℓ-adic representations, such as those where the characteristic polynomial of $\rho(\sigma_p)|_{V^{I_p}}$ has **rational coefficients**.

Now it turns out that all interesting ℓ-adic representations arise from geometry via ℓ-adic cohomology, and for those we can always defined a L-function as (4). In particular, let X be a smooth projective algebraic variety over $\mathbb{Q}$. The **ℓ-adic cohomology groups**:

$$V_{X,i}^{(\ell)} := H^i_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)$$

are $\mathbb{Q}_\ell$-vector spaces with a canonical action of $G_{\mathbb{Q}}$ arising from the action of $G_{\mathbb{Q}}$ on $X_{\overline{\mathbb{Q}}}$. We will not delve into the construction of these representations, but we will use the following properties that they enjoy:

- $V_{X,i}^{(\ell)}$ is unramified (i.e. $\rho(I_p) = \mathrm{id}$) at all $p \neq \ell$ at which X has good reduction (this means that if we take an integral model for X over $\mathbb{Z}$, its fiber over $\mathbb{F}_p$ is smooth).
- (Rationality property). For each $p \neq \ell$ of good reduction, $\rho(\sigma_p)$ has characteristic polynomial $P_p(t)$ in $\mathbb{Z}[t]$ which *does not depend* on ℓ.
- (Weight property). For $p \neq \ell$ of good reduction, factor $P_p(t)$ over $\mathbb{C}$ as:

$$P_p(t) = (t - \alpha_1^{(p)}) \cdot \ldots \cdot (t - \alpha_d^{(p)}).$$

Then

$$|\alpha_j^{(p)}| = p^{i/2}$$

Note in particular that by the weight property we deduce that $\rho(\sigma_p)$ **has infinite order** as soon as $i \neq 0$, otherwise the eigenvalues $\alpha_j^{(p)}$ would have absolute value equal to 1. This is in marked contrast with the complex setting, where $\rho(\sigma_p)$ is always of finite order.

EXAMPLE 5. The **Hasse-Weil L-function** of an elliptic curve $E/\mathbb{Q}$ is a special case of Example 4, and can be described explicitly. Suppose E is defined by:

$$E : y^2 = x^3 + ax + b, \qquad a, b \in \mathbb{Z}, \quad \Delta_E = -16(4a^3 + 27b^2) \neq 0.$$

Then the Hasse-Weil L-function is defined as:

$$L(E, s) := L(H^1_{\text{ét}}(E_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell), s).$$

The representation $H^1_{\text{ét}}(E_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)$ is 2-dimensional over $\mathbb{Q}_\ell$ and the characteristic polynomial of the Frobenius elements has integral coefficients and does not depend on the choice of ℓ (rationality property). Therefore the Hasse-Weil L-function is well-defined and it only depends on the elliptic curve E (and not on the choice of ℓ). Explicitly, we have:

$$L(E, s) = \prod_{p \nmid \Delta_E} \frac{1}{1 - a_p(E)p^{-s} + p^{1-2s}} \times \prod_{p | \Delta_E} (\text{Euler factors})$$

where

$$a_p(E) = p + 1 - \#E(\mathbb{F}_p)$$

can be readily computed by computing the number of points on the reduction of E modulo p (note that the fact that p is unramified implies that E has good reduction there, by the criterion of Neron-Ogg-Shafarevich).

EXAMPLE 6. Let E_1, E_2 be elliptic curves over $\mathbb{Q}$. Consider the 4-dimensional representation

$$V := H^1_{\text{ét}}(E_{1/\overline{\mathbb{Q}}}, \mathbb{Q}_\ell) \otimes_{\mathbb{Q}_\ell} H^1_{\text{ét}}(E_{2/\overline{\mathbb{Q}}}, \mathbb{Q}_\ell).$$

This representation also has an L-function, since 'it comes from geometry'. To see it, note that by the Künneth Formula for étale cohomology:

$$H^2_{\text{ét}}(E_1 \times E_{2/\overline{\mathbb{Q}}}, \mathbb{Q}_\ell) = \oplus_{i=0}^{i=2} H^i(E_1) \otimes H^{2-i}(E_2)$$

the representation V shows up as the piece $i = 1$ of the above decomposition, hence it has a well-defined L-function. These types of L-functions arise when one wishes to consider correspondences between elliptic curves. The étale cycle class map in fact maps divisors on $E_1 \times E_2$ (i.e. correspondences) into $H^2(E_1 \times E_2)$.

All the examples of L-functions described so far lead to the notion of **motivic L-functions**, i.e. L-functions attached to pieces of motivic cohomology of a variety defined over $\mathbb{Q}$. These motivic L-functions satisfy an amazing collection of conjectural properties:

Analytic continuation and functional equation: The functions $L(V,s)$ converge for $\Re[s] > i/2+1$ by the weight property. In fact, we have:

CONJECTURE. *L(V,s) has a meromorphic continuation to all of* $\mathbb{C}$.

This conjecture is known to be true only in handful of cases:

- Riemann ζ function (due to Riemann himself).
- 1-dimensional representations of $G_{\mathbb{Q}}$ (e.g. Dirichlet L-functions, class field theory).
- Some 2-dimensional representations (e.g. Hecke L-functions attached to modular forms, Hasse-Weil L functions via Wiles' Theorem).
- $L(H^1(E_1) \otimes H^1(E_2), s)$ is also known to have analytic continuation, via Rankin's method.

Special values of L-functions: Evaluating L-functions at 'special values' often yields global information about the arithmetic object to which they are attached. The prototypical example of this phenomenon is the class number formula (1). Similarly, Euler proved that for the Riemann ζ function:

$$\begin{aligned} \zeta(2k) &\in \mathbb{Q} \cdot \pi^{2k}, \quad k \in \mathbb{Z}_{\geq 1} \\ \zeta(1-2k) &\in \mathbb{Q} \end{aligned}$$

and these values have been related to important arithmetic invariants. More generally, **Deligne's conjecture** on 'critical points' gives precise expectations on which **algebraic numbers** we are supposed to obtain when we evaluate L-functions at prescribed special values.

p-adic interpolation: Once the special values of an L-function are known and are algebraic, we can interpolate them p-adically. The prototypical example of this construction is the **Kubota-Leopoldt** p-adic L-function. Let

$$\zeta_p(1-2k) := (1-p^{2k-1})\zeta(1-2k), \quad (k \geq 1).$$

Then by the Kummer-Clausen-von Staudt congruences we know that $\zeta_p : \mathbb{Z} \to \mathbb{Q}$ extends to a continuous function:

$$\mathbb{Z}/(p-1) \times \mathbb{Z}_p \longrightarrow \mathbb{Q}_p.$$

Other examples of p-adic L-functions which interpolate special values of L-functions are:

- **Mazur-Swinnerton-Dyer** p-adic L-function attached to an elliptic curve.

- **p-adic Rankin** L-functions attached to $H^1(E_1) \otimes H^1(E_2)$.

Once such p-adic L-functions are available, one can talk about **special values** of p-adic L-functions, and a whole new host of conjectures concerning them (p-adic Birch and Swinnerton-Dyer conjecture, p-adic Bloch-Beilinson conjecture,...).