Lecture 1: Overview

Brian Conrad
October 2, 2009
Notes by Sam Lichtenstein

1. Why Study Galois Representations?

Here we discuss the link between analytic L-functions and L-functions attached to varieties.

Let F be a number field and X a smooth projective variety over F.

Define the **partial Euler product**

$$\zeta_X^*(s) = \prod_{v \text{ good place of } F} \zeta(X \bmod v, q_v^{-s}), \qquad \operatorname{Re} s \gg_{\dim X} 0.$$

Here $X \bmod v$ denotes the smooth projective variety over $k(v) \simeq \mathbb{F}_{q_v}$ obtained by reduction of a smooth proper model of X over the valuation ring of F_v.

Example. Let X be an elliptic curve over F. Then

$$\zeta_E^*(s) = \prod_{E \text{ has good reduction at } v} \frac{1 - a_v q_v^{-s} + q_v^{1-2s}}{(1 - q_v^{-s})(1 - q_v^{1-s})} = \zeta^* F(s) \zeta_F^*(s-1) L^*(E,s)^{-1}, \qquad a_v = q_v + 1 - \#E(k(v)).$$

We would like to do the following.

(1) Fill in the "bad" factors to obtain an L-function with a good functional equation, analytic continuation, etc.

(2) Relate ζ_X^* to arithmetic properties of X. (E.g., Birch-Swinnerton-Dyer conjecture, etc.)

A clue for (1) comes from **Artin representations**:

$$G_F = \operatorname{Gal}(\overline{F}/F) \xrightarrow{\ \rho\ } \operatorname{GL}(W) = \text{f.d. v.s.}/\mathbb{C}$$

$$G_F \twoheadrightarrow \operatorname{Gal}(F'/F) = \text{Gal. gp. of finite Gal. extn.} \hookrightarrow \operatorname{GL}(W)$$

Note that F'/F is unramified at all but finitely many places. We define the **Artin L-function** of ρ to be

$$L(s,\rho) = \prod_v \det([1 - \rho(\mathrm{Frob}_v) q_v^{-s}]|_{W^{I_v}})^{-1}, \qquad W^{I_v} = \text{subspace of } W \text{ fixed by inertia at } v.$$

Grothendieck gave a related description of ζ_X^* using *continuous* p-adic representations

$$G_F \to \operatorname{GL}(\mathrm{H}^i_{\text{ét},c}(X_{\overline{F}}, \mathbb{Q}_p)) =: \operatorname{GL}(W^i).$$

These are unramified almost everywhere, including at all good places away from p. Here the ith cohomology group W^i above vanishes for $i > 2\dim X$. Grothendieck proved that if we remove the contribution of p-adic places to $\zeta_X^*(s)$ then

$$\zeta_X^*(s) = \prod_i L^*(s, W^i)^{(-1)^i},$$

where $L^*(s, W^i)$ is like the Artin L-function without the "bad" factors and the p-adic places:

$$L^*(s, W^i) = \prod_{\text{good } v \nmid p} \det([1 - \mathrm{Frob}_v\, q_v^{-s}]|_{W^i})^{-1}.$$

Note: The expression for $L^*(s, W^i)$ requires some care, since q_v^{-s} is a *complex number* acting on a *p-adic* vector space. What has to be proved is that the characteristic polynomial for the action of Frob_v on W^i has rational coefficients (and is independent of p), so evaluation using q_v^{-s} makes sense (and the Riemann Hypothesis ensures absolute convergence of the product in a suitable right half-plane depending only in $\dim X$).

We conclude from all this that it is a good idea to study L-functions of reasonable p-adic representations. Representation theory can often be used to fill in the bad factors later.

Eternal dangerous bend: The case of $v|p$ is tricky! The complication is that "unramifiedness" is not the right notion corresponding to "good reduction" for p-adic representations of Galois groups of p-adic fields.

2. Modular Galois representations and modularity lifting theorems

Definitions.

Definition. A **p-adic representation** of G_F is a continuous linear representation $\rho : G_F \to \mathrm{GL}(W)$, where W is a finite dimensional vector space over a p-adic field K (i.e. a finite extension $K/\mathbb{Q}_p$) and ρ is unramified at almost all places v of F.

Example. The repsentation $V_p(E) = T_p(E) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ arising from the Tate module of an elliptic curve E over F is historically the first really interesting example.

Example. Étale cohomology, with compact support: $W^i = \mathrm{H}^i_{\text{ét},c}(X_{\overline{F}}, \mathbb{Q}_p)$ for any separated F-scheme X of finite type. (Note that this is unramified at all but finitely many places, even if X is not smooth. The proof rests on properties of constructible ℓ-adic sheaves.)

Remark. In the definition of a p-adic representation it is *equivalent* to take the coefficient field to be $\overline{\mathbb{Q}}_p$, because of the following fact: any compact subgroup of $\mathrm{GL}_n(\overline{\mathbb{Q}}_p)$ is contained in $\mathrm{GL}_n(K)$ for a finite extension $K/\mathbb{Q}_p$. The proof of this uses the Baire Category Theorem. [Warning! It is *false* if we consider $\mathbb{C}_p$ instead of $\overline{\mathbb{Q}}_p$!] So we *could* do everything over $\overline{\mathbb{Q}}_p$, but we will find it more convenient to take the coefficient field K to be locally compact.

Definition. A $\bmod p$ **representation** of G_F is a continuous representation $\overline{\rho} : G_F \to \mathrm{GL}(\overline{W})$, where $\overline{W}$ is a finite dimensional vector space over a finite extension $k/\mathbb{F}_p$. Note that $\mathrm{GL}(\overline{W})$ is thus a discrete topological group, so the continuity condition entails that $\overline{\rho}$ factors through a finite Galois group $\mathrm{Gal}(F'/F)$.

Example. The p-torsion of an elliptic curve: $E[p](\overline{F}) \otimes_{\mathbb{F}_p} \mathbb{F}_{p^r}$.

Example. Étale cohomology: $\mathrm{H}^i_{\text{ét},c}(X_{\overline{F}}, \mathbb{Z}/p\mathbb{Z})$.

Remark. It is "equivalent" to take the coefficient field to be $\overline{\mathbb{F}}_p$.

Reduction of Galois representations.

Proposition. Any p-adic representation $\rho : G_F \to \mathrm{GL}_K(W)$ has a G_F-stable $\mathcal{O}_K$-lattice $\Lambda \subset W$; i.e. ρ induces a map $\overline{\rho} : G_F \to \mathrm{GL}_{\mathcal{O}_K} \Lambda \approx \mathrm{GL}_n(\mathcal{O}_K) \twoheadrightarrow \mathrm{GL}_n(k)$ where $k = \mathcal{O}_K/\mathfrak{m}$. □

(Here by a **lattice** we mean a finitely generated $\mathcal{O}_K$-submodule of W such that $K \otimes_{\mathcal{O}_K} \Lambda = W$.) It is not hard to see that the characteristic polynomial of $\overline{\rho}$ is independent of the choice of lattice Λ.

Theorem (Cor. of Brauer-Nesbit Theorem)**.** *Let $\overline{\rho}^{ss} = \bigoplus\{$Jordan-Holder factors of $\overline{\rho}\}$. Then $\overline{\rho}^{ss}$ has the same characteristic polynomial as $\overline{\rho}$, and is determined up to isomorphism by its characteristic polynomial, and is therefore independent of the choice of Λ.*

In light of the theorem, we shall henceforce call $\overline{\rho}^{ss}$ "the" reduction of ρ. Here are a bunch of things to watch out for:

(1) $\overline{\rho}^{ss}$ is often denoted $\overline{\rho}$, even though it is certainly not just the "reduction mod p" of ρ in general.
(2) $\overline{\rho}^{ss}$ may be unramified at some places where ρ is ramifield. For example, if $\rho(I_v) \subset 1 + \mathfrak{m} \cdot \mathrm{Mat}_n \mathcal{O}_K$, then the inertia at v simply "disappears" mod v.
(3) If $\overline{\rho}^{ss}$ is irreducible, then in fact the only stable lattices in W were of the form $\pi^i \Lambda$, where π is a uniformizer for K and $i \in \mathbb{Z}$.
(4) Irreducibility is *not* the same as *absolute* irreducibility = irreducibility over $\overline{k}$.
(5) ρ might be absolutely irreducible over K, yet $\overline{\rho}^{ss}$ could be not only reducible, but even completely trivial! (Hence completely reducible...)

Exercise: If ρ is reducible then any Jordan-Holder filtration of ρ induces a similar filtration for $\overline{\rho}^{ss}$. So the last warning above is "one-directional".

Modular Galois representations. Let $f \in S_k(\Gamma_1(N), \chi)$ be a Hecke eigenform of weight $k \geq 1$. Let $K_f \subset \mathbb{C}$ be the field generated over $\mathbb{Q}$ by all the Fourier coefficients $a_\ell(f)$ of f for primes $\ell \nmid N$. Then K_f is a number field containing the values of the Nebentypus χ. Let λ be a place of K_f lying over p.

Theorem (Deligne, Deligne-Serre, Ribet)**.** *There exists a unique continuous irreducible p-adic representaion*

$$\rho_{f,\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_{f,\lambda})$$

unramified at all $\ell \nmid Np$, such that for all such ℓ we have

$$\textit{sum of eigenvalues of } \mathrm{Frob}_\ell = \mathrm{Tr}(\rho_{f,\lambda}\,\mathrm{Frob}_\ell) = a_\ell(f) [= T(\ell)\textit{-eigenvalue of } f]$$

and

$$\det \circ \rho_{f,\lambda} = \chi \cdot \epsilon_p^{k-1}$$

where $\epsilon_p : G_{\mathbb{Q}} \to \mathbb{Z}_p^\times \subset \mathcal{O}_{K_{f,\lambda}}^\times$ is the p-adic cyclotomic character.

In particular, for $\ell \nmid Np$, the characteristic polynomial of $\rho_{f,\lambda}(\mathrm{Frob}_\ell)$ is

$$t^2 - a_\ell(f)t + \chi(\ell)\ell^{k-1} \in K_f[t] \subset K_{f,\lambda}[t],$$

a non-obvious integrality property. Note that this polynomial is independent of λ.

Remark. The independence of λ and the precise control on the unramified primes implies that the collection $\{\rho_{f,\lambda}\}_\lambda$ is a "compatible" family of of representations, with respect to K_f-characteristic polynomials, just like $\{V_pE\}_p$ is a "compatible" family of represention with respect to $\mathbb{Q}$-characteristic polynomials. Cf. Serre's book *Abelian ℓ-adic representations.*

Let us look at the partial Artin L-functions

$$L^*(s, \rho_{f,\lambda}) = \prod_{\ell \nmid Np} \det \left(1 - \rho_{f,\lambda}(\mathrm{Frob}_\ell) \cdot \ell^{-s}\right)^{-1} = \prod_{\ell \nmid Np} \frac{1}{1 - a_\ell(f)\ell^{-s} + \chi(\ell)\ell^{k-1-2s}} =: L^*(s, f).$$

Remark. Note that for a complex conjugation c, $\det \rho_{f,\lambda}(c) = \chi(-1)\epsilon_p^{k-1} = (-1)^k(-1)^{k-1} = -1$, so all the representations produced by the theorem above are *odd*!

Now consider the (semisimplified) reduction $\overline{\rho}_{f,\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}_2(k_{f,\lambda})$, which is continuous and semisimple, but might be reducible. In general, we say a mod-p representation $\overline{\rho}$ **is modular** if it is isomorphic over $\overline{\mathbb{F}}_p$ to some $\overline{\rho}_{f,\lambda}$.

Just *suppose* $\overline{\rho}_{f,\lambda}$ happens to be absolutely irreducible. By the last remark, it, too, is odd. Serre's conjecture is concerned with when mod-p representations with such properties are in fact modular.

Note that $\overline{\rho}_{f,\lambda}$ does not determine k or N. There could be congruences "$g \equiv f$" modulo λ for some eigenform $g \in S_{k'}(\Gamma_1(N'), \chi')$ (with the congruence taken in the sense of Fourier coefficients, say, relative to a p-adic place of $\overline{\mathbb{Q}}$ over λ on K_f and some chosen p-adic place of K_g). This would imply that $\overline{\rho}_{f,\lambda} = \overline{\rho}_{g,\lambda}$. This is actually abusive notation, since to obtain such a comparison, we might need to extend scalars on the residue fields of these reductions.

Wiles's insight. The prototype of a **modularity lifting theorem** is the following.

Theorem (Not really a theorem)**.** *Given any p-adic representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ such that $\overline{\rho}$ is irreducible and modular over $\overline{\mathbb{F}}_p$, and ρ is "nice" (at p, in the sense of p-adic Hodge theory!) then ρ is modular.*

In this seminar, we'll focus on those ρ such that

$$\rho|_{D_p} \approx \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}$$

where D_p is the decomposition group at p, ψ_2 is an unramified character, and ψ_1 is ϵ_p^{k-1} times an unramified character. These representations are "essentially like the ones that come from elliptic curves with good ordinary reduction at p".

3. Applications of the method

- Serre's conjecture.
- Sato-Tate.
- Gross-Zagier, Heegner points, Kolyvagin (need to provide a finite map $X_0(N_E) \to E$ over $\mathbb{Q}$, which is done via Faltings' theorem and the "modularity" of $V_\ell(E)$).
- FLT. (Modularity of the Galois rep. attached to the Frey curve.)