Math 726: L-functions and modular forms — Fall 2011

Lecture 18 : Eichler-Shimura Theory

Instructor: Henri Darmon — *Notes written by: Dylan Attwell-Duval*

Recall

We saw last time that the modular curves $Y_1(N)_{/\mathbb{Q}}$ are affine curves whose points are in correspondence with elliptic curves and level structure, up to $\overline{\mathbb{Q}}$-isomorphism ($\mathbb{Q}$-isomorphism when $N > 3$). See J.Milne's online notes for details.

Hecke Operators

In the last lecture we generalized the analytic notion of modular forms over $\mathbb{C}$ to an algebraic construction over an arbitrary ring S containing $\frac{1}{6}$. We now do the same for Hecke operators. Let $X_1(N)$ be the projective closure of $Y_1(N)_{/\mathbb{Q}}$.

Definition 1. A correspondence on $X_1(N)$ is a curve $T \subset X_1(N) \times X_1(N)$ whose projection maps are finite.

In the case of correspondences, the projection maps are both flat and proper so such a T induces a pair of maps on divisors of $X_1(N)$ (or equivalently finite linear combinations of points on $X_1(N)(\overline{\mathbb{Q}})$)

$$(\pi_2)_* \circ \pi_1^* : \mathrm{Div}(X_1(N)) \to \mathrm{Div}(X_1(N))$$
$$(\pi_2)_* \circ \pi_1^*([P]) = \sum_{P_i \in \pi_1^{-1}(P)} [\pi_2(P_i)]$$

and similarly

$$(\pi_1)_* \circ \pi_2^* : \mathrm{Div}(X_1(N)) \to \mathrm{Div}(X_1(N))$$

where of course the P_i need to be counted with the correct multiplicity corresponding to their scheme-theoretic preimage in T. See (Fulton, *Intersection Theory*, chapter 16) for a more general definition and discussion of correspondences.

We recall the definition of Hecke operators on modular forms of level N for all $(n, N) = 1$:

$$T_n(f)(\Lambda) = \sum_{\substack{\Lambda' \supset \Lambda \\ [\Lambda' : \Lambda] = n}} f(\Lambda')$$

Since the lattice Λ corresponds to elliptic curve $E = \mathbb{C}/\Lambda$, and $[\Lambda' : \Lambda] = n$ corresponds to the notion of an isogeny of degree n between the corresponding elliptic curves $E \twoheadrightarrow E'$, this motivates the algebraic generalization

$$T_n(f)(E, \alpha, \omega) = \sum_{\substack{\varphi: E \twoheadrightarrow E' \\ \deg \varphi = n}} f(E', \varphi \circ \alpha, (\varphi^*)^{-1}\omega).$$

Thus T_n induces an endomorphism of the graded vector space $\bigoplus_{k \geq 0} M_k(N, \mathbb{Q})$. Viewing modular forms on $X_1(N)$ as global sections of line bundles over $X_1(N)$ which have well defined divisors, T_n can be viewed as a map of divisors. In fact this map is a correspondence (See the link given at the end of the lecture for further details or chapter 5 of Milne's notes) the graph of which (ie. the curve in the definition of correspondences) is the set

$$\{((E, \alpha, \omega), (E', \alpha', \omega')) \mid \exists \text{ isogeny } \varphi \text{ of degree } n \text{ st. } \alpha' = \varphi \circ \alpha \text{ and } \omega' = (\varphi^*)^{-1}\omega\}.$$

Any correspondence preserves the subgroup of degree 0 divisors and the principal divisors, so induces an endomorphism of $\mathrm{Pic}^0(X_1(N)_{\overline{\mathbb{Q}}})$. It is a general fact of algebraic geometry that for smooth projective curves C of genus ≥ 1, there exists an abelian variety called the *Jacobian* of C (denoted $\mathrm{Jac}(C)$) whose groups structure is isomorphic to $\mathrm{Pic}^0(C)$. Proper maps between curves induce maps between their Jacobians. In our particular case, the Hecke correspondence T_n induces an endomorphism defined over $\mathbb{Q}$ of $J_1(N) := \mathrm{Jac}(X_1(N))$. For more details on Jacobians and abelian varieties see (Diamond and Shurman, chapter 6) or (Cornell and Silverman, *Arithmetic geometry*).

Let $\mathbb{T}$ be the $\mathbb{Z}$-algebra generated by the "good" algebraic Hecke operators T_n (ie. $(n, N) = 1$) acting on $J_1(N)$.

Proposition 1. *The ring $\mathbb{T}$ is isomorphic to the Hecke algebra of "good" Hecke operators acting on $S_2(N, \mathbb{C})$.*

Proof. The map $\mathbb{T} \hookrightarrow \mathrm{End}(J_1(N)) \to \mathrm{End}(\Omega^1(J_1(N)_{/\mathbb{C}}))$ is injective. The sheaf $\Omega^1(J_1(N)_{/\mathbb{C}})$ is canonically identified with $\Omega^1(X_1(N)_{/\mathbb{C}})$ and the action of $\mathbb{T}$ on $\Omega^1(X_1(N)_{/\mathbb{C}})$ induced from this identification is the same as that induced from our original algebraic construction of the T_n, ie. as endomorphisms of $X_1(N)$. But then we get an action on the $\mathbb{C}$-vector space $\Gamma(\Omega^1(X_1(N)_{/\mathbb{C}}), X_0(N)) = S_2(N; \mathbb{C})$. Using this identification, it is relatively straightforward to check that the action of the algebraic T_n agrees with our analytic T_n on the cusp forms of weight 2.

Theorem 2. *(Eichler-Shimura, part 1) Let f be a (normalized) newform in $S_2(N, \epsilon)$. Then* *there exists a unique (up to isogeny) quotient A_f of $J_1(N)$, satisfying*

- (a) *The quotient map $\varphi_f : J_1(N) \to A_f$ is defined over $\mathbb{Q}$ and its kernel is stable under $\mathbb{T}$*
- (b) $\mathrm{End}_{\mathbb{Q}}(A_f) \otimes \mathbb{Q} \cong K_f$, *where K_f is the field generated by $a_n(f)$, $(n, N) = 1$*
- (c) *The Hecke operator T_n acts on A_f as multiplication by $a_n(f) \in K_f$.*
- (d) $\dim(A_f) = [K_f : \mathbb{Q}]$

We make some brief remarks about the proof of the theorem.

$\star$ The Eigenform f gives rise to a homomorphism $\zeta_f : \mathbb{T} \to K_f$ sending T_n to $a_n(f)$. Define

$$I_f := \mathrm{Ker}(\zeta_f) \qquad \text{and } A_f := J_1(N)/I_f \cdot J_1(N).$$

Clearly the action of $\mathbb{T}$ factors through the quotient because I_f is an ideal. Since I_f is an ideal of the $\mathbb{Q}$-endomorphisms of $J_1(N)$ by construction, the quotient of $J_1(N)$ is defined over $\mathbb{Q}$ so (a) follows.

$\star$ We have exact sequence

$$0 \to I_f \to \mathbb{T} \to \mathcal{O}_f \to 0$$

where $\mathcal{O}_f$ is an order of K_f generating K_f. In particular, $\mathrm{rank}_{\mathbb{Z}}(\mathcal{O}_f) = \dim_{\mathbb{Q}}(K_f) = [K_f : \mathbb{Q}]$. Now $\dim_{\mathbb{C}}(A_f) = \dim_{\mathbb{C}}(\Omega^1(J_1(N))/I_f\Omega^1(J_1(N)))$ and using the identification of $\Omega^1(J_1(N))$ with $\Omega^1(X_1(N)) \cong S_2(N, \mathbb{C})$, we can consider the action of $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{C}$ on $S_2(N, \mathbb{C})$. It turns out $S_2(N, \mathbb{C})$ is a free $\mathbb{T}_{\mathbb{C}}$-module of rank 1. Furthermore, because f is a newform $S_2(N, \mathbb{C})/I_f$ is a free $(\mathbb{T}/I_f)_{\mathbb{C}}$-module of rank 1. (d) then follows immediately. See (DDT, Fermat's Last Theorem, pg. 39 for details).

Construction of λ-adic representations associated to A_f

Fix a prime l. The $\mathbb{Z}_l$ module

$$\varprojlim_n A_f[l^n](\overline{\mathbb{Q}})$$

is isomorphic to $\mathbb{Z}_l^{2d}$, where $d = [K_f : \mathbb{Q}] = \dim A_f$. Define

$$V_{f,l} := \left(\varprojlim_n A_f[l^n](\overline{\mathbb{Q}}) \right) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \cong \mathbb{Q}_l^{2d}.$$

Then $V_{f,l}$ has the obvious $G_{\mathbb{Q}}$ action defined by its action on the coordinates of A_f. Moreover, $V_{f,l}$ can be viewed as a rank two $K_f \otimes_{\mathbb{Q}} \mathbb{Q}_l$-module by part 1 of Eichler-Shimura above. This action commutes with the Galois action of $G_{\mathbb{Q}}$, so we get a representation

$$\rho_l : G_{\mathbb{Q}} \to GL_2(K_f \otimes \mathbb{Q}_l).$$

Next observe that the $\mathbb{Q}_l$-algebra $K_f \otimes \mathbb{Q}_l$ decomposes into the direct sum of fields

$$K_f \otimes \mathbb{Q}_l = \bigoplus_{\lambda | l} K_{f,\lambda}$$

where $K_{f,\lambda}$ denotes the completion of K_f at the prime ideal λ, as λ runs over all primes dividing l in K_f. The representation $\{V_{f,l}, \rho_l\}$ therefore decomposes into a direct sum of representations $\{V_{f,\lambda}, \rho_{f,\lambda}\}$, where $\rho_{f,\lambda}$ is the composition of maps

$$\rho_{f,\lambda} = \pi_{K_{f,\lambda}} \circ \rho_l : G_{\mathbb{Q}} \to GL_2(K_f \otimes \mathbb{Q}_l) \to GL_2(K_{f,\lambda}).$$

THEOREM 3. *(Eichler-Shimura, part 2) The collection of representations $\{\rho_{f,\lambda}\}_{\lambda \in P(K_f)}$ is a compatible system of λ-adic representations of $G_{\mathbb{Q}}$. Furthermore, $L(\{V_{f,\lambda}\}, s) = L(f, s)$. Namely, $\forall p \nmid N \cdot l$,*

$$\det(1 - x \operatorname{Frob}_p) \circlearrowleft V_{f,\lambda} = 1 - a_p(f)x + \epsilon(p)px^2.$$

The key issue with the proof of this theorem is that we need to relate the Galois-theoretic object Frob_p with the action of Hecke operator T_p. We will do this next time, but lay some of the groundwork now.

DEFINITION 4. Given a curve C over $\overline{\mathbb{F}}_p$, the *Frobenius morphism* is a map

$$\Phi_p : C \to C^{(p)}$$

sending the coordinates of a point in C to their p^{th} powers, where $C^{(p)}$ is the curve obtained from C by raising all coefficients in the defining equations to their p^{th} powers. The Frobenius map always exists (as an algebraic map) and is natural.

EXAMPLE 5. $C : y^2 = x^3 + ax + b$, an elliptic curve defined over $\overline{\mathbb{F}_p}$. Then

$$C^{(p)} : y^2 = x^3 + a^p x + b^p \quad \text{and} \quad \Phi_p(\alpha, \beta) = (\alpha^p, \beta^p).$$

REMARK 1. The extension of fields induced from $\Phi_p : C \to C^{(p)}$ is purely inseparable and of degree p.

Recall that for an elliptic curve defined over a field of characteristic p, the "multiplication by p" map $[p] : E \to E$ is of degree p^2 and the induced field extension is either purely inseparable, or has separability degree p.

Link to discussion on algebraic Hecke operators and correspondences:
http://modular.math.washington.edu/edu/Fall2003/252/lectures/10-31-03/10-31-03.pdf