Hecke Operators

Hao (Billy) Lee

November 2, 2015

Chapter 1

Preliminary

Everything in the preliminary section follows the notations and definitions from [3].

1.1 Modular Forms

Definition. For $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$, $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \tau = \frac{a\tau+b}{c\tau+d}$ for all $\tau \in \mathfrak{H}$ where $\mathfrak{H}$ is the complex half plane. We can extend action to the group $GL_2^+(\mathbb{Q})$ to act on $\mathbb{Q} \cup \{\infty\}$ by $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \left(\frac{m}{n}\right) = \frac{am+bn}{cm+dn}$.

Definition. For $N \in \mathbb{N}$, define the principal congruence subgroup of level N to be

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \mod N \right\}$$

and say a subgroup of Γ of $SL_2(\mathbb{Z})$ is a congruence subgroup if $\Gamma(N) \subseteq \Gamma$ for some $N \in \mathbb{N}$.

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \mod N \right\}$$

$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \mod N \right\}$$

Note that by taking $\Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^*$ by $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto d \mod N$ is a surjective homomorphism with kernel $\Gamma_1(N)$. This shows that $\Gamma_1(N)$ is normal in $\Gamma_0(N)$, and the quotient is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$.

Definition. For any $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2^+(\mathbb{Q})$, define the factor of automorphy $j(\gamma, \tau) \in \mathbb{C}$ for $\tau \in \mathfrak{H}$ to be $j(\gamma, \tau) = c\tau + d$. For such a γ, we can define the weight k operator $[\gamma]_k$ on functions $f : \mathfrak{H} \to \mathbb{C}$ by

$$\left(f\,[\gamma]_k\right)(\tau) = (\det \gamma)^{k-1} j(\gamma, \tau)^{-k} f\left(\gamma(\tau)\right)$$

for $\tau \in \mathfrak{H}$.

For a congruence subgroup Γ of $SL_2(\mathbb{Z})$, we say that a meromorphic function $f : \mathfrak{H} \to \mathbb{C}$ is weakly modular of weight k with respect to Γ, if $f\,[\gamma]_k = f$ for all $\gamma \in \Gamma$. That is, $f\left(\gamma(\tau)\right) = j\left(\gamma, \tau\right)^k f(\tau)$.

f is a modular form of weight k with respect to Γ, if it is holomorphic, weight-k invariant under Γ and $f[\alpha]_k$ is holomorphic at ∞ for all $\alpha \in SL_2(\mathbb{Z})$. If in addition, the first coefficient of the Fourier expansion of $f[\alpha]_k$ is zero for all $\alpha \in SL_2(\mathbb{Z})$, then f is a cusp form. We denote the set of modular forms of weight k with respect to Γ by $M_k(\Gamma)$, and cusp forms by $S_k(\Gamma)$.

1.2 Modular Curves

Definition. Let $\Gamma \subseteq SL_2(\mathbb{Z})$ be a congruence subgroup. Define the modular curve $Y(\Gamma) = \Gamma\backslash\mathfrak{H} = \{\Gamma\tau : \tau \in \mathfrak{H}\}$ to be the space of orbits of Γ acting on $\mathfrak{H}$.

In particular, denote $Y_0(N) = \Gamma_0(N)\backslash\mathfrak{H}$, $Y_1(N) = \Gamma_1(N)\backslash\mathfrak{H}$ and $Y(N) = \Gamma(N)\backslash\mathfrak{H}$.

We should note here that, technically, $Y(\Gamma)$ is a curve, which is the set of solutions of some given equation. what we are really defining here is $Y(\Gamma)(\mathbb{C})$.

Definition. The set of enhanced elliptic curve for $\Gamma_0(N)$, denoted $S_0(N)$, consists of ordered pairs (E, C) where E is an elliptic curve and C is a cyclic subgroup of E of order N. $(E, C) \sim (E', C')$ if there is an isomorphism of E and E' taking C to C'.

The set of enhanced elliptic curve for $\Gamma_1(N)$, denoted $S_1(N)$, consists of ordered pairs (E, Q) where E is an elliptic curve and Q is a point of order N. $(E, Q) \sim (E', Q')$ if there is an isomorphism of E and E' taking Q to Q'.

The set of enhanced elliptic curve for $\Gamma(N)$, denoted $S(N)$, consists of ordered pairs $(E, (P, Q))$ where E is an elliptic curve and (P, Q) are points in E that generates $E[N]$ with Weil pairing $e_N(P, Q) = e^{2\pi i/N}$. (Recall that $E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$). $(E, (P, Q)) \sim (E', (P', Q'))$ if there is an isomorphism of E and E' taking P to P' and Q to Q'.

Theorem. *[3, Thm 1.5.1] Modulo details, there are bijections $S_0(N) \cong Y_0(N)$, $S_1(N) \cong Y_1(N)$ and $S(N) \cong Y(N)$.*

Example. For $N = 1$, $Y_0(1) = Y_1(1) = Y(1) = SL_2(\mathbb{Z})\backslash\mathfrak{H}$. Recall that an elliptic curve can be determined by a lattice generated by 1 and some $\tau \in \mathfrak{H}$. Two lattices generated the same elliptic curve if $\tau' \in SL_2(\mathbb{Z})\tau$. This agrees with our theorem.

$Y(\Gamma)$ can be made into a Riemann surface (1 dimension complex manifold) by taking the quotient topology obtained from the quotient map $\pi : \mathfrak{H} \to \Gamma$ by $\tau \mapsto \Gamma\tau$. We can compactify $Y(\Gamma)$ to get $X(\Gamma) = SL_2(\mathbb{Z})\backslash(\mathfrak{H} \cup \mathbb{Q} \cup \{\infty\})$. The extra points are called the cusps. $X(\Gamma)$ is Hausdorf, connected and compact [3, Pro 2.4.2].

If f is weight k invariant with respect to Γ, then f is a degree k homogenous function on modular curves with respect to Γ. For details, see [3, Pg 41].

Chapter 2

Hecke Operators

We will motivate Hecke Operators following [3] by introducing double coset operators.

2.1 Double Coset

Definition. Let Γ_1 and Γ_2 be congruence subgroups and let $\alpha \in GL_2^+(\mathbb{Q})$, define

$$\Gamma_1 \alpha \Gamma_2 = \{\gamma_1 \alpha \gamma_2 : \gamma_1 \in \Gamma_1, \, \gamma_2 \in \Gamma_2\}$$

to be the double coset in $GL_2^+(\mathbb{Q})$.

The group Γ_1 acts on $\Gamma_1 \alpha \Gamma_2$ by left multiplication, partitioning it into orbits. It can be shown that the number of orbits is finite [3, pg 164]. Suppose $\Gamma_1 \alpha \Gamma_2 = \amalg_j \Gamma_1 \beta_j$ where $\{\beta_j\}$ are the orbit representatives

Definition. [3, Def 5.1.3] For congruence subgroups Γ_1 and Γ_2 of $SL_2(\mathbb{Z})$ and $\alpha \in GL_2^+(\mathbb{Q})$, the weight-$k$ $[\Gamma_1 \alpha \Gamma_2]_k$ operator takes functions $f \in M_k(\Gamma_1)$ to

$$f\,[\Gamma_1 \alpha \Gamma_2]_k = \sum_j f[\beta_j]_k$$

This is well-defined [3, Exercise 5.1.3]. In fact, we have the following theorem.

Theorem. $[\Gamma_1 \alpha \Gamma_2]_k : M_k(\Gamma_1) \to M_k(\Gamma_2)$ *and* $S_k(\Gamma_1) \to S_k(\Gamma_2)$.

Proof. The full proof can by found on page 165 of [3]. Here, we will only show invariance.

For all $\gamma \in \Gamma_2$, the map $\Gamma_1 \backslash \Gamma_1 \alpha \Gamma_2 \to \Gamma_1 \backslash \Gamma_1 \alpha \Gamma_2$ given by $\Gamma_1 \beta \mapsto \Gamma_1 \beta \gamma_2$ is well-defined and bijective. Therefore,

$$\left(f\,[\Gamma_1 \alpha \Gamma_2]_k\right)[\gamma]_k = \sum_j f\,[\beta_j \gamma]_k = f\,[\Gamma_1 \alpha \Gamma_2]_k\,.$$

□

Special cases [3]:

1. When $\Gamma_1 \supset \Gamma_2$, with $\alpha = I$ then $[\Gamma_1 \alpha \Gamma_2]_k$ is the natural inclusion of $M_k(\Gamma_1)$ into $M_k(\Gamma_2)$.

2. $\Gamma_1 \subset \Gamma_2$. Taking $\alpha = I$ again, and letting $\{\gamma_{2,j}\}$ be the set of coset representatives for $\Gamma_1 \backslash \Gamma_2$ makes the double coset operator $f\,[\Gamma_1 \alpha \Gamma_2]_k = \sum_j f\,[\gamma_{2,j}]_k$ the natural trace map that projects $M_k(\Gamma_1)$ onto $M_k(\Gamma_2)$ by symmetrizing over the quotient.

3. If $\alpha^{-1}\Gamma_1\alpha = \Gamma_2$ then $f\left[\Gamma_1\alpha\Gamma_2\right]_k = f\left[\alpha\right]_k$, the natural translation, is an isomorphism.

2.2 T_n and $\langle d\rangle$

Definition. Let $\Gamma_1 = \Gamma_2 = \Gamma_1(N)$ and let $\alpha \in \Gamma_0(N)$. Recall that $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^*$ by the map $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto d \mod N$. This shows that $\Gamma_1(N) \trianglelefteq \Gamma_0(N)$, and we have

$$f\left[\Gamma_1(N)\alpha\Gamma_1(N)\right]_k = f\left[\alpha\right]_k$$

for all $\alpha \in \Gamma_0(N)$ and $f \in M_k(\Gamma_1(N))$. This is case 3 from above.

Note that this induces an action of $\alpha \in \Gamma_0(N)$ on $M_k(\Gamma_1(N))$. Because $\Gamma_1(N)$ acts trivially on f, this really is an action of $(\mathbb{Z}/N\mathbb{Z})^*$ on $M_k\left(\Gamma_1(N)\right)$. For $d \in (\mathbb{Z}/N\mathbb{Z})^*$, we can define the Diamond Operator

$$\langle d\rangle : M_k\left(\Gamma_1(N)\right) \mapsto M_k\left(\Gamma_1(N)\right)$$

by $\langle d\rangle f = f\left[\alpha\right]_k$ for any $\alpha = \begin{bmatrix} a & b \\ c & \delta \end{bmatrix} \in \Gamma_0(N)$ with $\delta \equiv d \mod N$.

Definition. Again, let $\Gamma_1 = \Gamma_2 = \Gamma_1(N)$. Let $\alpha = \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix}$ for some prime p. Then define

$$T_P : M_k\left(\Gamma_1(N)\right) \to M_k\left(\Gamma_1(N)\right)$$

by $T_p f = f\left[\Gamma_1(N)\alpha\Gamma_1(N)\right]_k$.

Now, we will show that T_p and $\langle d\rangle$ commutes. For full detail, see page 169 of [3]. To do this, first observe that

$$\Gamma_1(N)\begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix}\Gamma_1(N) = \left\{\gamma \in M_2(\mathbb{Z}) : \gamma \equiv \begin{bmatrix} 1 & * \\ 0 & p \end{bmatrix} \mod N, \det\gamma = p\right\}.$$

In fact, for any $\gamma \in \Gamma_0(N)$, $\gamma\alpha\gamma^{-1} \equiv \begin{bmatrix} 1 & * \\ 0 & p \end{bmatrix} \mod N$. Suppose that $\Gamma_1(N)\alpha\Gamma_1(N) = \cup_j\Gamma_1(N)\beta_j$, and fix $\gamma \in \Gamma_0(N)$. Then

$$\begin{aligned} \Gamma_1(N)\alpha\Gamma_1(N) &= \Gamma_1(N)\gamma\alpha\gamma^{-1}\Gamma_1(N) \\ &= \gamma\Gamma_1(N)\alpha\Gamma_1(N)\gamma^{-1} \text{ by normality} \\ &= \gamma \cup_j \Gamma_1(N)\beta_j\gamma^{-1} \end{aligned}$$

Hence, we have $\cup_j\Gamma_1(N)\beta_j = \gamma \cup_j \Gamma_1(N)\beta_j\gamma^{-1}$ and thus $\cup_j\Gamma_1(N)\gamma\beta_j = \cup_j\Gamma_1(N)\beta_j\gamma^{-1}$. Note, it need not be the same for each term. We can now show commutativity with this identity.

Let $\gamma \in \Gamma_0(N)$ where the lower right corner entry is $\delta \equiv d \mod N$. Then

$$\langle d\rangle T_p f = \langle d\rangle \sum_j f\left[\beta_j\right]_k = \sum_j f\left[\beta_j\gamma\right]_k = \sum_j f\left[\gamma\beta_j\right]_k = T_p\langle d\rangle f$$

for all $f \in M_k\left(\Gamma_1(N)\right)$.

In fact, we can find that $\beta_j = \begin{bmatrix} 1 & j \\ 0 & p \end{bmatrix}$ for $0 \leq j < p$ and $\beta_\infty = \begin{bmatrix} m & n \\ N & p \end{bmatrix}\begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}$ if $p \nmid N$ where $mp-nN = 1$ [3, Page 170].

Proposition. *[3, Prop 5.2.1]*

$$T_p f = \begin{cases} \sum_{j=0}^{p-1} f\left[\begin{bmatrix} 1 & j \\ 0 & p \end{bmatrix}\right]_k & \text{if } p \mid N \\ \sum_{j=0}^{p-1} f\left[\begin{bmatrix} 1 & j \\ 0 & p \end{bmatrix}\right]_k + f\left[\begin{bmatrix} m & n \\ N & p \end{bmatrix}\begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}\right]_k & \text{if } p \nmid N \text{ where } mp-nN=1 \end{cases}$$

In other words,

$$T_p f(\tau) = \begin{cases} \frac{1}{p}\sum_{j=0}^{p-1} f\left(\frac{\tau+j}{p}\right) & \text{if } p \mid N \\ \frac{1}{p}\sum_{j=0}^{p-1} f\left(\frac{\tau+j}{p}\right) + p^{k-1} f(p\tau) & \text{if } p \nmid N \end{cases}$$

Note that in this last formula, it does not matter that $f \in M_k(\Gamma_1)$. In fact, with this algebraic formula, we can define Hecke operators on any congruence subgroup Γ.

Now, we try to extend $\langle d \rangle$ and T_P to all $n \in \mathbb{Z}^+$. For $n \in \mathbb{Z}^+$ with $\gcd(n, N) = 1$, define $\langle n \rangle$ to be $\langle n \mod N \rangle$. If $\gcd(n, N) > 1$, then define $\langle n \rangle = 0$. This definition makes $\langle \cdot \rangle$ multiplicative on $\mathbb{Z}^+$. For prime powers p^r, define $T_{p^r} = T_p T_{p^{r-1}} - p^{k-1}\langle p \rangle T_{p^{r-2}}$ for $r \geq 2$. Then for $n = \prod p_i^{e_i}$ as its prime factorization, define $T_n = \prod T_{p_i^{e_i}}$. By construction T_n and $\langle d \rangle$ still commute.

2.3 Modular Curve Interpretation

Let Γ_1 and Γ_2 be congruence subgroups of $SL_2(\mathbb{Z})$. Suppose $\Gamma_1 \alpha \Gamma_2 = \amalg_j \Gamma_1 \beta_j$, where $\{\beta_j\}$ are coset representations. Let $X_1 = X(\Gamma_1)$ and $X_2 = X(\Gamma_2)$, then $[\Gamma_1 \alpha \Gamma_2]_k : Div(X_2) \to Div(X_1)$ by $\Gamma_2 \tau \mapsto \sum_j \Gamma_1 \beta_j(\tau)$ [3, Pg 166].

We will consider the case where the Hecke operators act on $\Gamma = \Gamma_1(N)$ (don't care about the weight). We will now give a geometric interpretation of this, following Remark 1.11 and section 1.3 of [4], and page 174 of [3]. Recall that the modular curve $Y_1(N)$ is in bijective correspondence with $S_1(N)$. $S_1(N)$ consists of pairs (E, Q) where E is an elliptic curve and Q is a point of E of order N. For $p \nmid N$, the moduli space interpretation is $T_P : Div(S_1(N)) \to Div(S_1(N))$ by $[E, Q] \mapsto \sum_C [E/C, Q + C]$ where the sum is taken over all subgroups C of E of order p such that $C \cap \langle Q \rangle = \{id_E\}$. This comes from the fact that we have the following correspondence,

$$\begin{array}{ccccccc} Div(Y_1(N)) & \overset{T_p}{\to} & Div(Y_1(N)) & \quad & \Gamma_1(N)\tau & \mapsto & \sum_j \Gamma_1(N)\beta_j(\tau) \\ \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow \\ Div(S_1(N)) & \overset{T_p}{\to} & Div(S_1(N)) & & \left[E_\tau, \frac{1}{N} + \Lambda_\tau\right] & \mapsto & \sum_C \left[E_\tau/C, \frac{1}{N} + C\right] \end{array}$$

For more details about why this is true, see page 174 of [3].

There is an isogeny from $\mathbb{C}/\Lambda$ to $\mathbb{C}/\Lambda'$ if and only if there exists some $m \in \mathbb{C}$ such that $m\Lambda \subseteq \Lambda'$. If $p \nmid N$, then there are exact $p+1$ distinct p-isogenies from $\left(\mathbb{C}/\langle \tau, 1 \rangle, \frac{1}{N}\right)$. Their images are: $\left(\mathbb{C}/\left\langle \frac{\tau+j}{p}, 1 \right\rangle, \frac{1}{N}\right)$ for $j = 0, ..., p-1$ and $\left(\mathbb{C}/\langle p\tau, 1 \rangle, \frac{p}{N}\right)$. If $p|N$, then we lose the last p-isogeny, because the point $\frac{p}{N}$ is of order less than N. Note, these $p+1$ isogenies are exactly $\phi_j(\tau) = \frac{\tau+j}{p}$ for $j = 0, ..., p-1$ and $\phi_\infty(\tau) = \langle p \rangle p\tau$. The map $f(\tau) \mapsto \omega_f = 2\pi i f(\tau) d\tau$ is an isomorphism between $S_2(\Gamma)$ and $\Omega^1(X_\Gamma)$ of holomorphic differentials on X_Γ [4, Lemma 1.12]. This also shows that $\dim S_2(\Gamma)$ is finite and equal to $g = genus(X(\Gamma))$. Notice that $\phi_j^*(\omega_f) = 2\pi i f\left(\frac{\tau+j}{p}\right) d\left(\frac{\tau+j}{p}\right) = \frac{2\pi i}{p} f\left(\frac{\tau+j}{p}\right) d\tau$

for all $j = 0, ..., p-1$. Combining this fact, with the algebraic definition of T_p, we see that for $p \nmid N$,

$$\omega_{T_p(f)} = \sum \phi_j^* (\omega_f).$$

2.4 Petersson Inner Product

Definition. Define the hyperbolic measure on the upper half plane $d\mu(\tau) = \frac{dxdy}{y^2}$ for all $\tau \in \mathfrak{H}$.

We can extend the measure to $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{Q} \cup \{\infty\}$ because $\mathbb{Q} \cup \{\infty\}$ has measure zero. This is invariant under under $GL_2^+(R)$, so in particular, it's $SL_2(\mathbb{Z})$-invariant. Recall that

$$D^* = \left\{\tau \in \mathfrak{H} : |Re(\tau)| \leq \frac{1}{2}, |\tau| \geq 1\right\} \cup \{\infty\}$$

is a fundamental domain of $\mathfrak{H}^*$ under the action of $SL_2(\mathbb{C})$. It can be shown that for any continuous and bounded functions $\phi : \mathfrak{H} \to \mathbb{C}$ and $\alpha \in SL_2(\mathbb{Z})$, $\int_{D^*} \phi(\alpha(\tau)) d\mu(\tau)$ converges. Let $\{\alpha_j\} \subseteq SL_2(\mathbb{Z})$ be a set of coset representatives, so that $SL_2(\mathbb{Z}) = \amalg_j \{\pm I\} \Gamma\alpha_j$.

Now, consider $\phi : \mathfrak{H} \to \mathbb{C}$ in $M_k(\Gamma)$. Since ϕ and $d\mu$ are are Γ invariant, we have

$$\sum_j \int_{D^*} \phi(\alpha_j(\tau)) d\mu(\tau) = \int_{\cup\alpha_j D^*} \phi(\tau) d\mu(\tau). \tag{2.4.1}$$

Furthermore, $\cup\alpha_j D^*$ represents $X(\Gamma)$ up to some boundary identification, so we can define $\int_{X(\Gamma)} \phi(\tau) d\mu(\tau)$ to be equation (2.4.1).

Definition. For a congruence subgroup Γ, define the volume of Γ to be $V_\Gamma = \int_{X(\Gamma)} d\mu(\tau)$.

Fact. $V_\Gamma = [SL_2(\mathbb{Z}) : \{\pm\} \Gamma] V_{SL_2(\mathbb{Z})}$.

Definition. Let $\Gamma \subseteq SL_2(\mathbb{Z})$ be a congruence subgroup. Define the Petersson Inner product by

$$\langle \cdot, \cdot \rangle_\Gamma : S_k(\Gamma) \times S_k(\Gamma) \to \mathbb{C}$$

$$\langle f, g \rangle_\Gamma = \frac{1}{V_\Gamma} \int_{X(\Gamma)} f(\tau)\overline{g(\tau)} (Im(\tau))^k d\mu(\tau)$$

It can be shown that this is well-defined ($f(\tau)\overline{g(\tau)} (Im(\tau))^k$ is Γ invariant and the integral converges). Additionally, it is not hard to see that this is linear in the first variable, and conjugate linear in the second. Additionally, it's Hermitian-symmetric and positive definite. The reason for $\frac{1}{V_\Gamma}$ is so that if $\Gamma' \subseteq \Gamma$, then $\langle \cdot, \cdot \rangle_{\Gamma'} = \langle \cdot, \cdot \rangle_\Gamma$ on $S_k(\Gamma)$. This is only defined on cusp forms because because the inner product does not converge on all of $M_k(\Gamma)$.

For $\Gamma \subseteq SL_2(\mathbb{Z})$ a congruence subgroup and $\alpha \in GL_2^+(\mathbb{Q})$, define $\alpha' = \det(\alpha)\alpha^{-1}$. By computation, we have that $[\alpha]_k^* = [\alpha']_k$ and $[\Gamma\alpha\Gamma]_k^* = [\Gamma\alpha'\Gamma]_k$ are their adjoints under the Petersson Inner Product [3, Prop 5.5.2]. In particular, on $S_k(\Gamma_1(N))$, and for $p \nmid N$, we have adjoints: $\langle p \rangle^* = \langle p \rangle^{-1}$ and $T_p^* = \langle p \rangle^{-1} T_p$. For this, we can show that $\langle n \rangle$ and T_n for $\gcd(n, N) = 1$, are all normal. By the Spectral Theorem of linear algebra, since $S_k(\Gamma_1(N))$ is finite dimensional, and $\langle n \rangle$, T_n for $\gcd(n, N) = 1$ are a commuting family of normal operators, there exists an orthogonal basis of simultaneous eigenvectors for the operators.

Let $\mathbb{T}$ denote the $\mathbb{C}$-algebra generated by the all Hecke operators T_n and $\langle d \rangle$. A modular form is an eigenform if it is a simultaneous eigenvector for all $T \in \mathbb{T}$. Note that this does not form a basis, because $\mathbb{T}$ is not semi-simple. Let $\mathbb{T}^0$ denote the set of all T_n and $\langle n \rangle$ where $\gcd(n, N) = 1$. This algebra is semi-simple and so we have an orthogonal basis of simultaneous eigenforms.

2.5 Eigenforms

Definition. If $f \in S_k(\Gamma)$ is an eigenform if it is a simultaneous eigenvector for all $T \in \mathbb{T}$. If it has Fourier expansion $f(\tau) = \sum_{n=1}^{\infty} a_n(f) q^n$ where $a_1(f) = 1$ then we say f is normalized.

Let f be an eigenform, then it has an associated algebra homomorphism $\lambda_f : \mathbb{T} \to \mathbb{C}$ where $Tf = \lambda(T)f$ for all $T \in \mathbb{T}$. Additionally, we can define $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ by sending n to the eigenvalue of $\langle n \rangle$ corresponding to f, that is $\langle n \rangle f = \chi(n) f$. It can be shown that χ is a Dirichlet character.

Proposition. *[4, 1.17]Given a non-zero algebra homomorphism $\lambda : \mathbb{T} \to \mathbb{C}$, there is exactly one eigenform, up to scaling, such that $Tf = \lambda(T)f$ for all $T \in \mathbb{T}$.*

Proposition. *[3, Prop 5.8.5] Let $f \in M_k(N)$ with associated character χ. Then f is a normalized eigenform if and only if the coefficients of the Fourier series satisfies the following:*

1. $a_1(f) = 1$
2. $a_{p^r}(f) = a_p(f) a_{p^{r-1}}(f) - \chi(p) p^{k-1} a_{p^{r-2}}(f)$ *for all p prime and $r \geq 2$*
3. $a_{mn(f)} = a_m(f) a_n(f)$ *when* $\gcd(m, n) = 1$

To summarize, $a_n(f) = a_1(f)\lambda(T_n)$.

Definition. For a modular form $f \in M_k(N)$ where χ is a Dirichlet character, define its L-function to be $L(s, f) = \sum_{n=1}^{\infty} a_n n^{-s}$ where $f(\tau) = \sum_{n=0}^{\infty} a_n e^{2\pi i n \tau}$ is its Fourier series expansion.

With some work, the previous proposition shows that f is a normalized eigenform, if and only if its L function has an Euler product expansion [4, Thm 1.26] [3, Thm 5.9.2]

$$L(s, f) = \prod_p \left(1 - a_p p^{-s} + \chi(p) p^{k-1-2s}\right)^{-1}.$$

Here, we take $\chi(p) = 0$ for $p | N$.

Chapter 3

Galois Representation

The definitions and constructions in this chapter come from various sections of [4].

3.1 Jacobian

Recall that the map $f(\tau) \mapsto w_f = 2\pi i f(\tau)d\tau$ is an isomorphism between $S_2(\Gamma)$ and $\Omega^1(X_\Gamma)$ of holomorphic differentials on X_Γ [4, Lemma 1.12]. This shows that $\dim S_2(\Gamma)$ is equal to $g = genus\,(X(\Gamma))$.

Let $V = S_2(\Gamma)^v = Hom\,(S_2(\Gamma), \mathbb{C})$ be the dual space of $S_2(\Gamma)$, the weight 2 cusp forms of some congruence subgroup Γ of $SL_2(\mathbb{Z})$. This is a complex vector space of dimension $g = genus\,(X(\Gamma))$. The integral homology $\Lambda = H_1(X(\Gamma), \mathbb{Z})$ maps naturally to V by sending a homology cycle c to the functional ϕ_c where $\phi_c(f) = \int_c w_f$. The image of Λ is a discrete $\mathbb{Z}$-module of rank $2g$, so it can be viewed as a lattice in V. We call the complex torus V/Λ, the Jacobian variety of $X(\Gamma)$ over $\mathbb{C}$. If $\Gamma = \Gamma_0(N)$ or $\Gamma_1(N)$, we will write $J_0(N)$ and $J_1(N)$ respectively.

Fix $\tau_0 \in \mathfrak{H}$. Define the Abel-Jacobi map $\Phi_{AJ} : X(\Gamma)(\mathbb{C}) \to J_\Gamma$ by $\Phi_{AJ}(P)(f) = \int_{\tau_0}^{p} w_f$. This is well-defined and does not depend on the choice of path. By linearity, we can extend this to a map on $Div\,(X(\Gamma))$. Then we can restrict it down to the degree 0 divisors $Div^0\,(X(\Gamma))$. Here, the Abel-Jacobi map no longer depends on the base point τ_0.

Theorem. *[4, Thm 1.15] (Abel-Jacobi Theorem). The map $\Phi_{AJ} : Div^0\,(X(\Gamma)) \to J_\Gamma$ has kernel consisting of precisely $P\,(X(\Gamma))$ which is the set of princial divisors. Therefore, the map induces an isomorphism between J_Γ and the Picard group, $Pic^0\,(X(\Gamma)) = Div^0\,(X(\Gamma))\,/P\,(X(\Gamma))$.*

Hecke operators act on $V = (S_2(\Gamma))^v$ via duality and they hold Λ stable. Hence, Hecke operators give rise to endomorphisms of J_Γ.

Definition. A correspondence on a curve X is a divisor C on $X \times X$ taken modulo $\{P\} \times X$ and $X \times \{Q\}$.

Let π_1 and π_2 denote the projection of $X \times X$ onto each of the factors. Then C induces a map on $Div(X)$ by $C(D) = \pi_2\left(\pi_1^{-1}(D) \cdot C\right)$, where $D_1 \cdot D_2$ denotes intersection of the two divisors. C preserves the divisors of degree 0 and sends principal divisors to principal divisors. Hence C gives an algebraic endomorphism of $Jac(X)$. We can in fact define composition of correspondences to get that the set of correspondences form a ring. See [6] for more details.

Now, back to $X(\Gamma)$. See page 32 of [4] for more details. We define the Hecke correspondence T_n to be the closure in $X_\Gamma \times X_\Gamma$ of the locus of points (A, B) in $Y_\Gamma \times Y_\Gamma$, where there is a degree n isogeny of elliptic curves with Γ structure from A to B. Let's examine a concrete example, with $\Gamma = \Gamma_1(N)$ and let $p \nmid N$. Consider the graph of T_p in $(X_1(N) \times X_1(N))$. This is a correspondence. Consider what the induced map of T_p is on divisors. By definition,

$$T_p\left((E,P)\right) = \pi_2\left(\pi_1^{-1}\left((E,P)\right)\cdot T_p\right) = \sum (E/C,\, P \mod C)$$

where the sum runs over the subgroups C of E with order p. If (A,B) belongs to T_p then the isogeny dual to $A \to B$ gives a p-isogeny from B to pA so that $T_p^v = \langle p\rangle^{-1} T_p$.

Let $\Gamma = \Gamma_1(N)$. Let $\phi_{X_1(N)}$ be the Frobenius morphism on $X_1(N)_{/\mathbb{F}_p}$ which is a degree p isogeny that raises coordinates to the p-th power. Here, $X_1(N)_{/\mathbb{F}_p}$ is the reduction of the curve to characteristic p. For more detail on how this is done, see page 36 of [4]. Consider the graph of $\phi_{X_1(N)}$ in $(X_1(N) \times X_1(N))_{/\mathbb{F}_p}$. It is a correspondence of degree p, which will now be called F. Fix a point $(E,P) \in X_1(N)_{/\mathbb{F}_p}$. Our goal is to compute $T_p\left((E,P)\right)$ using the Frobenius map. Let $(E_\infty, P_\infty) = \phi_{X_1(N)}\left((E,P)\right)$. To find the other elliptic curves p-isogenous to E, we can consider the ellitpic curves E, such that when we apply the Frobenius to it, we get E. To do so, we consider the transpose correspondence F' (interchange the two factors of $X_1(N) \times X_1(N)$). The corresponding endomorphism on J_Γ induced by F' is the dual endomorphism of ϕ_{J_Γ}. Consider the divisor

$$F'\left((E,P)\right) = (E_1,P_1) + ... + (E_p,P_p)$$

Since ϕ_{E_i}, the Frobenius endomorphism on E_i, is an isogeny of degree p from (E_i,P_i) to (E,P), we also have the dual isogeny from (E,P) to (E_i,pP_i). If E is ordinary at p then (E_∞,P_∞), (E_1,pP_1),..., (E_p,pP_p) are a complete list of distinct curves with Γ-structure which are p-isogenous to (E,P). Hence, we have the following equality on divisors,

$$T_p\left((E,P)\right) = (E_\infty,P_\infty) + (E_1,pP_1) + ... + (E_p,pP_p) = \left(F + \langle p\rangle F'\right)\left((E,P)\right).$$

Since ordinary points are dense in $X_1(N)_{/\mathbb{F}_p}$, $T_p = \left(F + \langle p\rangle F'\right)$ as endomorphisms of $J_1(N)_{/\mathbb{F}_p}$.

Theorem. *[4, Thm 1.29] For $p \nmid N$, the endomorphism of T_p of $J_{\Gamma/\mathbb{F}_q}$ satisfies $T_p = F + \langle p\rangle F'$. This is called the Eichler-Shimura congruence relation.*

3.2 Shimura's Construction

Definition. Let $S_2(\Gamma,\mathbb{Z})$ to be the space of modular forms with integral Fourier coefficients in $S_2(\Gamma)$. Given a ring A, define $S_2(\Gamma,A) = S_2(\Gamma,\mathbb{Z}) \otimes A$. Note, $S_2(T,\mathbb{C}) = S_2(\Gamma)$. Let $\mathbb{T}_\mathbb{Z}$ be the ring generated over $\mathbb{Z}$ by the Hecke operators T_n and $\langle d\rangle$ acting on $S_2(\Gamma,\mathbb{Z})$. Given a ring A, define $\mathbb{T}_A = \mathbb{T}_\mathbb{Z} \otimes A$. $\mathbb{T}_A$ acts on $S_2(\Gamma,A)$ in a canonical way.

Let $f = \sum_{n=1}^{\infty} a_n(f)q^n$ be an eigenform. Let K_f be a number field generated by all the $a_n(f)$'s. Let $\lambda_f : \mathbb{T}_\mathbb{Q} \to K_f$ be associated algebra homomorphism. $I_f = \ker \lambda_f \cap \mathbb{T}_\mathbb{Z}$. The image of $I_f(J_\Gamma)$ is a subabelian variety of J_Γ which is stable under the actions of $\mathbb{T}_\mathbb{Z}$ and is defined over $\mathbb{Q}$.

Definition. Define $A_f = J_\Gamma / I_f(J_\Gamma)$. It is an abelian variety defined over $\mathbb{Q}$ and depends only on $[f]$ the orbit of f under $G_\mathbb{Q}$. Its endomorphism ring contains $\mathbb{T}_\mathbb{Z}/I_f$ which is isomorphic to an order in K_f. In fact, from the actions of $\mathbb{T}$, we get an embedding $K_f \hookrightarrow End_\mathbb{Q}(A_f) \otimes \mathbb{Q}$ [4, Prop 1.49] .

A_f is a complex tori [4, Lemma 1.46]. Let V_f of $V = S_2(\Gamma)^v$ on which $\mathbb{T}$ acts on via λ_f $(\{f : Tf = \lambda(T)f \,\forall T \in \mathbb{T}\}$. V_f has dimension 1 as a complex vector space[4, Thm 1.22, Lemma 1.34]. Let π_f be the orthogonal projection of V onto V_f relative to the Petersson inner product.

Let $[f]$ be all the eigenforms whose Fourier coefficients are Galois conjugates to those of f. The number of forms is $[K_f : \mathbb{Q}]$. Let $V_{[f]} = \oplus_{g\in[f]} V_g$ and $\pi_{[f]} = \sum_{g\in[f]} \pi_g$ which is simply the orthogonal projection of V onto $V_{[f]}$. It should be noted that $\pi_f \in \mathbb{T}_{K_f}$ and $\pi_{[f]} \in \mathbb{T}_{\mathbb{Q}}$.

Lemma. *[4, Lemma 1.46] The abelian variety is isomorphic over $\mathbb{C}$ to the complex torus $V_{[f]}/\pi_{[f]}(\Lambda)$ with the map $\pi_{[f]} : V/\Lambda \to V_{[f]}/\pi_{[f]}(\Lambda)$ corresponding to the natural projection from J_Γ to A_f.*

This also shows that A_f is of dimension $[K_f : \mathbb{Q}]$.

Proposition. *[4, Proposition 1.53] The following are equivalent:*

- *The curve E is isogenous over $\mathbb{Q}$ to A_f for some newform f on some congruence gorup Γ*
- *There is a non-constant morphism defined over $\mathbb{Q}$ from $X_0(N)$ to E*

We won't discuss what newforms are, but basically we can decompose $S_k(\Gamma_1(N))$ into newforms and oldforms. For more information, see section 5.6 of [3].

In particular, if E is an elliptic curve that satisfy the above property, then we say it is a modular elliptic curve.

Conjecture. Shimura-Taniyama Conjecture [4, Conj 1.54]. All elliptic curves defined over $\mathbb{Q}$ are modular.

Of course, we now know this is true for semi-stable elliptic curves (Andrew Wiles).

Define the Tate module of A_f by $T_\ell(A_f) = \lim_{\leftarrow}(A_f[\ell^n])$. $T_\ell(A_f) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is free $K_f \otimes \mathbb{Q}_\ell$ module of rank 2 [4, Lemma 1.48].

Theorem. *[4, Thm 1.41] For $p \nmid N\ell$, the characteristic polynomial of the Frobenius endomorphism F on $\mathbb{T}_{\mathbb{Q}_\ell}$-module $T_\ell(A_f) \otimes \mathbb{Q}_\ell$ is $X^2 - T_pX + \langle p\rangle p = 0$.*

Proof. By Eichler-Shimura relation. □

3.3 Main Theorems

For this section, we will let $f = \sum_{n=1}^{\infty} a_n(f)q^n$ be an eigenform of weight 2 and level N. Let $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to C^*$ be its associated character, such that$\langle d\rangle f = \chi(d)f$. Let K_f be a number field generated by all the $a_n(f)$'s and values of χ.

The action of the Hecke algebra on $J_1(N)$ provides an embedding $K_f \hookrightarrow End_{\mathbb{Q}}(A_f)\otimes\mathbb{Q}$. Recall that $T_\ell(A_f)\otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is a free $K_f \otimes \mathbb{Q}_\ell$ module of rank 2. The action of the Galois group commutes with that of K_f, so by choosing a basis for the Tate module, we get an interpretation $G_{\mathbb{Q}} \to GL_2(K_f \otimes \mathbb{Q}_\ell)$. Because $K_f \otimes \mathbb{Q}_\ell$ can be identified with the product of completions of K_f at the primes over ℓ, we just induced an ℓ-adic representation of $G_{\mathbb{Q}}$ from f.

Theorem. *[5, Thm 4.4.1]*

1. *Suppose $k \geq 2$. Then for all primes $\mathfrak{p}$ of K_f, there exists an odd irreducible Galois representation*

$$\rho_{f,\mathfrak{p}} : G_{\mathbb{Q}} \to GL_2\left((K_f)_{\mathfrak{p}}\right)$$

such that for all ℓ prime to N and to $\mathfrak{p}$, $\rho_{f,\mathfrak{p}}$ is unramified at ℓ, and the characteristic polynomial of $\rho_{f,\mathfrak{p}}(Frob_\ell)$ is $x^2 - a_\ell(f)x + \chi(\ell)\ell^{k-1}$.

2. *Suppose $k = 1$. Then there exists an odd irreducible Galois representation*

$$\rho_f : G_{\mathbb{Q}} \to GL_2(\mathbb{C})$$

such that for all ℓ prime to N, ρ_f is unramified at ℓ, and the characteristic polynomial of $\rho_f(Frob_\ell)$ is $x^2 - a_\ell(f)x + \chi(\ell)$.

Full proofs of these statements can be found in [1] and [2] for statements 1 and 2 respectively. The reason why the weight 1 case is stated in a separate statement is because it comes from Artin representations, and statement 1 comes from ℓ-adic representations.

For $k = 2$, $J_1(N)$ has good reduction at all primes $p \nmid N$. This shows that the action of the Galois group on $T_\ell(A_f) \otimes \mathbb{Q}_\ell$ is unramified and is described by the Frobenius endormorphism ϕ on the Tate module of the reduciton. The characteristic polynomial of ϕ is $X^2 - T_pX + \langle p \rangle p = 0$ by the Eichler-Simura relation.

Bibliography

[1] P. Deligne. Formes modulaires et représentations l-adiques. *Séminaire Bourbaki*, 11:139–172, 1968-1969.

[2] P. Deligne and J.-P. Serre. Formes modulaires de poids 1. *Annales scientifiques de l'École Normale Supérieure*, 7(4):507–530, 1974.

[3] F. Diamond and J. Shurman. A First Course in Modular Form. *Information Security and Privacy*, 2005.

[4] H. Darmon and F. Diamond and R. Taylor. Fermat's Last Theorem. *Current Developments in Mathematics*, 1:1–157, 1995.

[5] J. Weinstein. Reciprocity laws and Galois representations: Recent Breakthrough. 2015.

[6] A. Weil. Variétés abéliennes et courbes algébriques. 1948.