Modular Forms and Galois Representations

Jeffrey Manning
Discussed with Professor Emerton

1 Introduction

Theorem 1.1 (Serre-Deligne)**.** *Let $f = \sum_{n=1}^{\infty} a_n(f)q^n \in \mathcal{S}_k(\Gamma_0(N))$ be a newform of level N and weight k. If $K = K_f = \mathbb{Q}(\{a_n(f)\}_{n=1}^{\infty})$ is the number field corresponding to f, and $\lambda \nmid N$ is a non-archimedean place of K_f, then there is a continuous representation $\rho_{f,\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_\lambda)$ which is unramified at all primes p with $(p, \lambda) = (p, N) = 1$, and such that $\rho_{f,\lambda}(\mathrm{Frob}_p) \in \mathrm{GL}_2(K_\lambda)$ has characteristic polynomial $x^2 - a_p(f) + p^{k-1} = 0$ for all such primes p.*

Our primary goal is to explain the construction of this representation in the case $k = 2$.

2 Modular Curves and Modular Forms

In this section we review the definitions and basic properties of modular curves and modular forms, our primary objects of study.

2.1 Modular Curves

Let $\mathbb{H} = \{z \in \mathbb{C} | \operatorname{Im} z > 0\}$ be the upper half plane, and let $\mathrm{SL}_2(\mathbb{Z})$ act on $\mathbb{H}$ via Möbius transformations (i.e. as $\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \dfrac{az+b}{cz+d}$). For any $N > 0$ let $\Gamma(N) = \ker(\mathrm{SL}_2(\mathbb{Z}) \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}))$ and say that a subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ is a *congruence subgroup* if $\Gamma \supseteq \Gamma(N)$ for some N. The most commonly occurring examples of congruence subgroups are the following:

$$\Gamma_0(N) := \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) \middle| \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod N \right\}, \quad \Gamma_1(N) := \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) \middle| \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod N \right\}.$$

For any congruence subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ let $Y(\Gamma) = \Gamma \backslash \mathbb{H}$ and let $X(\Gamma)$ be the standard compactification of $Y(\Gamma)$. Then $X(\Gamma)$ is a compact Riemann surface, and is thus a smooth projective

algebraic curve over $\mathbb{C}$. The curves $X(\Gamma)$ are known as *modular curves*. Also let $J(\Gamma) := \mathrm{Jac}(X(\Gamma))$ be the Jacobian of $X(\Gamma)$.

For convenience, we let $X_0(N) := X(\Gamma_0(N))$ and $X_1(N) := X(\Gamma_1(N))$, and define $Y_0(N)$, $Y_1(N)$, $J_0(N)$ and $J_1(N)$ similarly.

The curves $Y_0(N)$ and $Y_1(N)$ have the following interpretation as moduli spaces (justifying the term '*modular* curve')

Theorem 2.1. *For $N \geq 1$ let*

$$S_0(N) := \{(E, C) | E \text{ is an elliptic curve, } C \subseteq E \text{ is a cyclic subgroup of order } N\}/\cong$$
$$S_1(N) := \{(E, P) | E \text{ is an elliptic curve, } P \in E \text{ has order exactly } N\}/\cong$$

then there are natural isomorphisms $S_0(N) \cong Y_0(N)$ and $S_1(N) \cong Y_1(N)$.

The following alternate description of $S_0(pN)$ (and thus $Y_0(pN)$) for $p \nmid N$ prime will be used later:

Theorem 2.2. *If p is prime and $p \nmid N$, then*

$$S_0(pN) = \left\{ \left(E \xrightarrow{\psi} E', C \right) \middle| \begin{array}{l} E \text{ and } E' \text{ are elliptic curves, } (E, C) \in S_0(N), \\ \psi \text{ is an isogeny with } \deg \psi = p \end{array} \right\} /\cong$$

From now on, we will identify $Y_0(N)$ with $S_0(N)$.

2.2 Modular Forms

We now define the spaces $\mathcal{M}_k(\Gamma)$ and $\mathcal{S}_k(\Gamma)$, of modular forms and cusp forms, respectively, corresponding to a congruence subgroup Γ.

For any holomorphic function $f \in \mathcal{H}(\mathbb{H})$, any $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and any $k \in \mathbb{Z}$ define $f[\alpha]_k \in \mathcal{H}(\mathbb{H})$ by

$$(f[\alpha]_k)(z) = (cz + d)^{-k} f(\alpha(z)) = \frac{1}{(cz + d)^k} f\left(\frac{az + b}{cz + d}\right).$$

Now let $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup. We say that f is *weakly modular* of weight k with respect to Γ if $f[\alpha]_k = f$ for all $\alpha \in \Gamma$. Note that if f is weakly modular with respect to Γ, then $f[\alpha]_k$ is weakly modular with respect to $\alpha^{-1}\Gamma\alpha$.

Now if Γ is a congruence subgroup then $\gamma_h := \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \in \Gamma$ for some $h \geq 1$ (as $\Gamma(N) \subseteq \Gamma$ for some $N \geq 1$ and $\gamma_N \in \Gamma(N)$). Hence if f is weakly modular with respect to Γ, then

$$f(z) = (f[\gamma_h]_k)(z) = f(z + h)$$

and so f is periodic with period h. It then follows that f has a Fourier expansion:

$$f(z) = \sum_{n=-\infty}^{\infty} a_n q_h^n$$

with $q_h = e^{2\pi iz/h}$. We say that f is *holomorphic* at (resp. *vanishes* at) ∞ if $a_n = 0$ for all $n < 0$ (resp. for $n \leq 0$). Note that this definition is independent of the choice of h.

If f is weakly modular of weight k with respect to Γ, we say that f is *modular*, and write $f \in \mathcal{M}_k(\Gamma)$, if $f[\alpha]_k$ is holomorphic at ∞ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$. We say that f is a *cusp form*, and write $f \in \mathcal{S}_k(\Gamma)$ if $f[\alpha]_k$ vanishes at ∞ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$. We say that f has *level* N if it is modular with respect to $\Gamma_1(N)$ or $\Gamma_0(N)$.

Note that if $\Gamma = \Gamma_0(N)$ or $\Gamma_1(N)$ then $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma$, and so if $f \in \mathcal{M}_k(\Gamma)$, then $f(z+1) = f(z)$ by the above, and so f has a *q-expansion* $f = \sum_{n=0}^{\infty} a_n(f) q^n$, where $q = q_1 = e^{2\pi iz}$. If $f \in \mathcal{S}_k(\Gamma)$ then $a_0(f) = 0$ (but this condition is not sufficient to ensure $f \in \mathcal{S}_k(\Gamma)$).

The following consequence of the Riemann-Roch Theorem gives modular forms much of their power:

Proposition 2.3. *For any congruence subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ and any $k \in \mathbb{Z}$, $\mathcal{M}_k(\Gamma)$, and hence $\mathcal{S}_k(\Gamma)$, is finite dimensional.*

In fact, in most cases, one can give explicit formulas for $\mathcal{M}_k(\Gamma)$ and $\mathcal{S}_k(\Gamma)$ in terms of Γ and k. However, these formulas are often quite cumbersome, and so we will not state them. The special case below will be important later.

Note that if $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, then we have the identity $d\alpha(z) = (cz+d)^{-2} dz$. Thus if $f \in \mathcal{M}_2(\Gamma)$ then $f(z)dz$ is invariant under the action of Γ, and so defines a holomorphic differential form on $\Gamma\backslash\mathbb{H} = Y(\Gamma)$, and thus a meromorphic differential form on $X(\Gamma)$. In fact, we have

Proposition 2.4. *The map $f(z) \mapsto f(z)dz$ gives an isomorphism $\mathcal{S}_2(\Gamma) \cong \Omega^1_{\mathrm{hol}}(X(\Gamma))$. In particular, $\dim_{\mathbb{C}} \mathcal{S}_2(\Gamma) = \mathrm{genus}(X(\Gamma))$.*

In light of Proposition 2.4, we may now identify $\mathcal{S}_2(\Gamma)$ with $\Omega^1_{\mathrm{hol}}(X(\Gamma))$. This gives us the following useful description of the Jacobian $J(\Gamma)$ of $X(\Gamma)$:

Corollary 2.5. *For any congruence subgroup Γ, there is a lattice $\Lambda(\Gamma) \subseteq \mathcal{S}_2(\Gamma)^\vee$, and a natural isomorphism $J(\Gamma) \cong \mathcal{S}_2(\Gamma)^\vee / \Lambda(\Gamma)$.*

3 Hecke Operators

Much of the arithmetic significance of the modular curves $X_0(N)$ comes from the Hecke operators $\{T_n | n \in \mathbb{Z}_+\}$ acting on the modular Jacobians $J_0(N)$ and the space of cusp forms $\mathcal{S}_k(\Gamma_0(N))$.

In this section, we summarize the construction of these operators. We will initially define the Hecke operators T_p for p prime as correspondences $X_0(N) \rightsquigarrow X_0(N)$, and then deduce the other interpretations of T_p from this. Therefore we must first introduce the notion of correspondences.

3.1 Correspondences

If X and Y are smooth, projective curves, then a correspondence $X \rightsquigarrow Y$ is roughly a multivalued map from X to Y. Explicitly:

Definition 3.1. A *correspondence* $C : X \rightsquigarrow Y$ is a smooth, projective curve C together with surjective morphisms $\alpha : C \twoheadrightarrow X$ and $\beta : C \twoheadrightarrow Y$.

By basic algebraic geometry, a map $f : X \to Y$ of curves induces maps $f^* : \mathrm{Jac}(Y) \to \mathrm{Jac}(X)$ and $f_* : \mathrm{Jac}(X) \to \mathrm{Jac}(Y)$ on Jacobians, and maps $f^* : \Omega^1_{\mathrm{hol}}(Y) \to \Omega^1_{\mathrm{hol}}(X)$ and $\mathrm{tr}_f : \Omega^1_{\mathrm{hol}}(X) \to \Omega^1_{\mathrm{hol}}(Y)$ on differential forms. Moreover, the maps on differential forms are the pullbacks associated to the maps on Jacobians, under the identification $\Omega^1_{\mathrm{hol}}(\mathrm{Jac}(X)) = \Omega^1_{\mathrm{hol}}(X)$ (that is, $f^* = (f_*)^*$ and $\mathrm{tr}_f = (f^*)^*$). It follows that a correspondence $C : X \rightsquigarrow Y$ induces maps:

$$C : \mathrm{Jac}(X) \xrightarrow{\alpha^*} \mathrm{Jac}(C) \xrightarrow{\beta_*} \mathrm{Jac}(Y)$$
$$C : \Omega^1_{\mathrm{hol}}(Y) \xrightarrow{\beta^*} \Omega^1_{\mathrm{hol}}(C) \xrightarrow{\mathrm{tr}_\alpha} \Omega^1_{\mathrm{hol}}(Y)$$

and moreover, the map $C : \Omega^1_{\mathrm{hol}}(Y) \to \Omega^1_{\mathrm{hol}}(X)$ is the pullback of the map $C : \mathrm{Jac}(X) \to \mathrm{Jac}(Y)$.

Intuitively, one can think of this construction as starting with a multivalued function $C : X \rightsquigarrow Y$, then adding up outputs of the function to get a *single* valued function $C : X \to \mathrm{Jac}(Y)$, and then finally extending this to a map $C : \mathrm{Jac}(X) \to \mathrm{Jac}(Y)$ by additivity.

3.2 Hecke Operators

Now pick any $N \geq 1$. For each prime $p \nmid N$, we will define a correspondence $T_p : X_0(N) \rightsquigarrow X_0(N)$ as follows. Define maps $\alpha, \beta : Y_0(pN) \to Y_0(N)$ by

$$\alpha\left(E \xrightarrow{\psi} E', C\right) = (E, C), \qquad \beta\left(E \xrightarrow{\psi} E', C\right) = (E', \psi(C)),$$

where we use the characterization of $Y_0(pN)$ from Theorem 2.2. These maps can be shown to be algebraic morphisms. Hence α and β are rational maps $X_0(pN) \dashrightarrow X_0(N)$, and so (by the classification of smooth projective algebraic curves) extend uniquely to surjective morphisms $\alpha, \beta : X_0(pN) \to X_0(N)$. We define $T_p : X_0(N) \rightsquigarrow X_0(N)$ to be the correspondence $X_0(N) \xleftarrow{\alpha} X_0(pN) \xrightarrow{\beta} X_0(N)$.

One can similarly define correspondences $T_p : X_0(N) \rightsquigarrow X_0(N)$ for $p|N$ (here we must use a different modular curve, $X_0^0(N, p)$, in place of $X_0(pN)$), but for the sake of simplicity we omit the precise definition.

Thus we have a family of correspondences $T_p : X_0(N) \rightsquigarrow X_0(N)$, where p ranges over all primes. These induce operators $T_p : J_0(N) \to J_0(N)$ which in turn induce operators $T_p : \Omega^1_{\text{hol}}(X_0(N)) \to \Omega^1_{\text{hol}}(X_0(N))$. By Proposition 2.4, T_p in fact induces an operator $T_p : \mathcal{S}_2(\Gamma_0(N)) \to \mathcal{S}_2(\Gamma_0(N))$. By generalizing Proposition 2.4, one can show that T_p in fact induces operators $T_p : \mathcal{S}_k(\Gamma_0(N)) \to \mathcal{S}_k(\Gamma_0(N))$, for all $k \in \mathbb{Z}$.

Just as the action of T_p on $J_0(N)$ determines the action of T_p on $\mathcal{S}_2(\Gamma_0(N))$, the action of T_p on $\mathcal{S}_2(\Gamma_0(N))$ determines the action of T_p on $J_0(N)$. Explicitly,

Proposition 3.1. *For any N and any prime p, the action of T_p on $\mathcal{S}_2(\Gamma_0(N))$ induces a natural action on $\mathcal{S}_2(\Gamma_0(N))^\vee$. Under this action, we have $T_p\Lambda(\Gamma_0(N)) \subseteq \Lambda(\Gamma_0(N))$, and so T_p acts on $J_0(N) = \mathcal{S}_2(\Gamma_0(N))^\vee/\Lambda(\Gamma_0(N))$. This action coincides with the action defined above.*

The operators $T_p : J_0(N) \to J_0(N)$ have explicit descriptions in terms of moduli spaces:

Proposition 3.2. *For any prime p (including the case $p|N$) and any $(E, C) \in Y_0(N)$, we have*

$$T_p(E, C) = \sum_{\substack{C_p \subseteq E[p] \\ C_p \cong \mathbb{Z}/p\mathbb{Z} \\ C_p \cap C = 0}} (E/C_p, (C + C_p)/C_p)\,.$$

This extends by linearity and continuity to determine a unique morphism $T_p : J_0(N) \to J_0(N)$.

One can also describe the action of T_p on the space $\mathcal{S}_k(\Gamma_0(N))$ of cusp forms in terms of q-expansions.

Proposition 3.3. *Take $f = \sum_{n=1}^{\infty} a_n(f)q^n \in \mathcal{S}_k(\Gamma_0(N))$ and let $T_p f = \sum_{n=1}^{\infty} a_n(T_p f)q^n \in \mathcal{S}_k(\Gamma_0(N))$. Then we have*

$$a_n(T_p f) = a_{pn}(f) + p^{k-1}\mathbb{1}_N(p)a_{n/p}(f)$$

where

$$\mathbb{1}_N(p) := \begin{cases} 1 & p \nmid N \\ 0 & p|N \end{cases}$$

and we interpret $a_{n/p}(f) = 0$ if $p \nmid n$.

Using either Proposition 3.2 or 3.3 we get following useful corollary

Corollary 3.4. *For any primes p and q, we have that $T_pT_q = T_qT_p$. Hence $\{T_p | p \text{ prime}\}$ is a commuting family of linear operators on both $J_0(N)$ and $\mathcal{S}_k(\Gamma_0(N))$.*

As another immediate corollary of Proposition 3.3, we see that $a_1(T_p f) = a_p(f)$ for all primes p.

The formula in Proposition 3.3 now suggests the following definition:

Definition 3.2. We define the Hecke operators $\{T_n | n \in \mathbb{Z}_+\}$ inductively as follows: Let $T_1 = \mathrm{id}$. For any prime p, and any $r \geq 2$, define $T_{p^r} = T_p T_{p^{r-1}} - p^{k-1} \mathbb{1}_N(p) T_{p^{r-2}}$. Finally for any $m, n \in \mathbb{Z}_+$ with $\gcd(m, n) = 1$, define $T_{mn} = T_m T_n$,

One can easily verify that these definitions were chosen to ensure that $a_1(T_n f) = a_n(f)$ for all n and all $f \in \mathcal{S}_k(\Gamma_0(N))$.

3.3 The Hecke algebra

For many of the applications of Hecke operators it will be helpful to shift our focus away from the individual Hecke operators T_n, and towards the algebra generated by them. Explicitly, we make the following definitions:

Definition 3.3. Fix $N, k \geq 1$ and define

$$\mathbb{T}_{\mathbb{Z}} = \mathbb{Z}\left[\{T_n | n \in \mathbb{Z}_+\}\right] = \mathbb{Z}\left[\{T_p | p \text{ prime}\}\right] \subseteq \mathrm{End}_{\mathbb{C}}(\mathcal{S}_k(\Gamma_0(N)))$$
$$\mathbb{T}_{\mathbb{C}} = \mathbb{C}\left[\{T_n | n \in \mathbb{Z}_+\}\right] = \mathbb{C}\left[\{T_p | p \text{ prime}\}\right] \subseteq \mathrm{End}_{\mathbb{C}}(\mathcal{S}_k(\Gamma_0(N))).$$

While $\mathbb{T}_{\mathbb{Z}}$ and $\mathbb{T}_{\mathbb{C}}$ certainly depend on N and k, we typically omit these from our notation.

By definition, it now follows that $\mathcal{S}_k(\Gamma_0(N))$ is a $\mathbb{T}_{\mathbb{Z}}$ (and a $\mathbb{T}_{\mathbb{C}}$) module for all k. Also by Proposition 3.1, it follows that $\Lambda(\Gamma_0(N))$ is a $\mathbb{T}_{\mathbb{Z}}$-module, and so the quotient module $J_0(N) = \mathcal{S}_2(\Gamma_0(N))^\vee / \Lambda(\Gamma_0(N))$ is naturally a $\mathbb{T}_{\mathbb{Z}}$-module.

Note that Corollary 3.4 ensures that $\mathbb{T}_{\mathbb{Z}}$ and $\mathbb{T}_{\mathbb{C}}$ are commutative. The primary advantage to considering $\mathbb{T}_{\mathbb{Z}}$ and $\mathbb{T}_{\mathbb{C}}$ instead of the individual Hecke operators is the following simple result:

Proposition 3.5. *$\mathbb{T}_{\mathbb{Z}}$ is a finite-rank $\mathbb{Z}$-module. $\mathbb{T}_{\mathbb{C}}$ is a finite-dimensional $\mathbb{C}$-vector space.*

Proof. (sketch)

We have $\mathbb{T}_{\mathbb{C}} \subseteq \mathrm{End}_{\mathbb{C}}(\mathcal{S}_k(\Gamma_0(N))) \cong M_{\dim_{\mathbb{C}} \mathcal{S}_k(\Gamma_0(N))}(\mathbb{C})$ and so $\dim_{\mathbb{C}} \mathbb{T}_{\mathbb{C}} \leq (\dim_{\mathbb{C}} \mathcal{S}_k(\Gamma_0(N)))^2$.

For $\mathbb{T}_{\mathbb{Z}}$, we give the argument only for $k = 2$, as this has the strongest geometric interpretation. The action of $\mathbb{T}_{\mathbb{Z}}$ on $\mathcal{S}_2(\Gamma_0(N))$ induces a faithful action of $\mathbb{T}_{\mathbb{Z}}$ on $\mathcal{S}_2(\Gamma_0(N))^\vee$. As each T_n acts on $J_0(N)$, one can show using Corollary 2.5, that $T_n(\Lambda(\Gamma_0(N))) \subseteq \Lambda(\Gamma_0(N))$ for all n.

Thus $\mathbb{T}_{\mathbb{Z}}$ acts on $\Lambda(\Gamma_0(N))$ and so we have a homomorphism

$$\mathbb{T}_{\mathbb{Z}} \to \mathrm{End}_{\mathbb{Z}}(\Lambda(\Gamma_0(N))) \cong M_{2\dim_{\mathbb{C}} \mathcal{S}_2(\Gamma_0(N))}(\mathbb{Z}).$$

This homomorphism is injective, as $\Lambda(\Gamma_0(N))$ spans $\mathcal{S}_2(\Gamma_0(N))^\vee$, and so $\mathrm{rk}\, \mathbb{T}_{\mathbb{Z}} \leq 4(\dim_{\mathbb{C}} \mathcal{S}_2(\Gamma_0(N)))^2$. □

Proposition 3.5 allows us to consider a single 'finite' object, instead of an infinite collection of operators. As an immediate result of this corollary, we can see that there much be infinitely many 'nontrivial' relations among the operators $\{T_p | p \text{ prime}\}$ whereas up to this point, they had appeared to be entirely unrelated. These relations encode turn out to encode a huge amount of number theoretic information.

The following useful lemma gives more information about the structure of $\mathbb{T}_{\mathbb{C}}$

Lemma 3.6. *The map $\mathbb{T}_{\mathbb{C}} \times \mathcal{S}_2(\Gamma_0(N)) \to \mathbb{C}$ given by $(T, f) \mapsto a_1(Tf)$ is a nondegenerate pairing. This pairing then gives $\mathcal{S}_2(\Gamma_0(N))^\vee$ the structure of a free rank one $\mathbb{T}_{\mathbb{C}}$-module. This module structure is precisely the one induced by the usual action of $\mathbb{T}_{\mathbb{C}}$ on $\mathcal{S}_2(\Gamma_0(N))$.*

Proof. (sketch) Clearly the pairing $(T, f) \mapsto a_1(Tf)$ is bilinear. If, for some $f \in \mathcal{S}_2(\Gamma_0(N))$, $a_1(Tf) = 0$ for all T, then for all $n \geq 1$, $a_n(f) = a_1(T_n f) = 0$, giving $f = 0$, so the pairing is nondegenerate in the second component. Similarly if, for some $T \in \mathbb{T}_{\mathbb{C}}$, $a_1(Tf) = 0$ for all $f \in \mathcal{S}_2(\Gamma_0(N))$, then for all $T' \in \mathbb{T}_{\mathbb{C}}$ we have $a_1(T'(Tf)) = a_1(T(T'f)) = 0$ (as $\mathbb{T}_{\mathbb{C}}$ is commutative). By nondegeneracy in the second component, $Tf = 0$ for all $f \in \mathcal{S}_2(\Gamma_0(N))$, which implies that $T = 0$. So indeed the pairing is nondegenerate.

Most of the remaining statements follow easily from this. The final statement follows by noting that the isomorphism $\mathbb{T}_{\mathbb{C}} \cong \mathcal{S}_2(\Gamma_0(N))^\vee$ is actually a $\mathbb{T}_{\mathbb{Z}}$-module isomorphism, since $a_1((T'T)f) = a_1(T(T'f))$. □

Appealing to more advanced results, one can strengthen this argument to show

Lemma 3.7. *We have $\operatorname{rk} \mathbb{T}_{\mathbb{Z}} = \dim_{\mathbb{C}} \mathbb{T}_{\mathbb{C}} = \dim_{\mathbb{C}} \mathcal{S}_2(\Gamma_0(N))$. Hence the natural map $\mathbb{T}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{C} \to \mathbb{T}_{\mathbb{C}}$, induced by $\mathbb{T}_{\mathbb{Z}} \hookrightarrow \mathbb{T}_{\mathbb{C}}$, is an isomorphism.*

As the Hecke operators $\{T_n | \gcd(n, N) > 1\}$ behave somewhat differently from those in $\{T_n | \gcd(n, N) = 1\}$, it will sometimes be useful to exclude the former. Hence we define the following subalgebra of $\mathbb{T}_{\mathbb{Z}}$.

Definition 3.4. Fix $N, k \geq 1$ and define

$$\mathbb{T}^*_{\mathbb{Z}} = \mathbb{Z}\left[\{T_n | n \in \mathbb{Z}_+, \gcd(n, N) = 1\}\right] = \mathbb{Z}\left[\{T_p | p \text{ prime}, p \nmid N\}\right] \subseteq \mathbb{T}_{\mathbb{Z}}.$$

We will call $\mathbb{T}^*_{\mathbb{Z}}$ the *anemic Hecke algebra.*

4 Eigenforms and Newforms

In order to better understand the action of the Hecke operators on the vector space $\mathcal{S}_k(\Gamma_0(N))$, we would like to find a basis of simultaneous eigenvectors for the action of the operators $\{T_n | n \in \mathbb{Z}_+\}$ on $\mathcal{S}_k(\Gamma_0(N))$ (thus making the Hecke operators simultaneously diagonalizable). Unfortunately this is not possible in general. In this section we try to come as close as possible to giving $\mathcal{S}_k(\Gamma_0(N))$ a

basis of eigenvectors (called *eigenforms*). We shall construct a subspace $\mathcal{S}_k(\Gamma_0(N))^{\text{new}}$ of $\mathcal{S}_2(\Gamma_0(N))$, which will have a basis of eigenforms (which we will refer to as *newforms*). Finally, we will show how the Hecke algebra can be used to associate an abelian variety, A_f, to each newform f, and moreover, gives a decomposition of $J_0(N)$ into a product of these abelian varieties.

These abelian varieties, A_f, will be used in the next section to construct the Galois representations associated to newforms.

4.1 The Petersson Inner Product

Recall from linear algebra that a commuting family of *self-adjoint*, linear operators on a hermitian inner product space is simultaneously diagonalizable. It is thus natural to attempt to equip $\mathcal{S}_k(\Gamma)$ with a natural inner product.

Definition 4.1. If $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup and $k \geq 1$ then define $(\ ,\ )_\Gamma : \mathcal{S}_k(\Gamma) \times \mathcal{S}_k(\Gamma) \to \mathbb{C}$ by

$$(f,g)_\Gamma := \int_{X(\Gamma)} f(x+iy)\overline{g(x+iy)}y^k \frac{dxdy}{y^2}$$

(where $\int_{X(\Gamma)}$ denotes integration over a fundamental domain for the action of Γ on $\mathbb{H}$). $(\ ,\ )_\Gamma$ is referred to as the *Petersson inner product* on $\mathcal{S}_k(\Gamma)$.

Proposition 4.1. *The Petersson inner product is a well-defined hermitian inner product on* $\mathcal{S}_k(\Gamma)$.

When $\Gamma = \Gamma_0(N)$, we have the following result

Theorem 4.2. *For any* $f, g \in \mathcal{S}_k(\Gamma_0(N))$ *and any* n *with* $\gcd(n,N) = 1$, *we have* $(T_n f, g)_{\Gamma_0(N)} = (f, T_n g)_{\Gamma_0(N)}$, *and so* $T_n = T_n^*$. *Thus* $\mathcal{S}_k(\Gamma_0(N))$ *has an (orthogonal) basis of simultaneous eigenforms for the set* $\{T_n | \gcd(n,N) = 1\}$, *and thus for* $\mathbb{T}_\mathbb{Z}^*$.

Unfortunately, for $\gcd(n,N) > 1$, it is no longer necessarily true that $T_n = T_n^*$, and so the eigenforms guaranteed by Theorem 4.2 may not be eigenforms for T_n. In the next section, we partially remove this restriction.

4.2 Oldforms and Newforms

We first quote a standard result about transformations of modular forms

Lemma 4.3. *If* $f \in \mathcal{S}_k(\Gamma_0(M))$ *and* $g(z) = f(dz)$ *for some* $d \geq 1$, *then for any* $N \geq 1$ *with* $dM|N$, $g \in \mathcal{S}_k(\Gamma_0(N))$. *Moreover, for any* n *with* $\gcd(n, N/M) = 1$, $(T_n g)(z) = (T_n f)(dz)$.

This means that some of the modular forms in $\mathcal{S}_k(\Gamma_0(N))$, in some sense, 'belong' to $\mathcal{S}_k(\Gamma_0(M))$ for $M < N$. We would like to distinguish these forms from the ones which do come from any lower levels. Explicitly we make the following definitions:

Definition 4.2. For any $N, k \geq 1$, let

$$\mathcal{S}_k(\Gamma_0(N))^{\text{old}} = \langle f(dz) | f \in \mathcal{S}_k(\Gamma_0(M)), dM|N \rangle \leq \mathcal{S}_k(\Gamma_0(N))$$

and let $\mathcal{S}_k(\Gamma_0(N))^{\text{new}} = (\mathcal{S}_k(\Gamma_0(N))^{\text{old}})^{\perp}$ (where orthogonal complements are taken with respect to the Petersson inner product). $\mathcal{S}_k(\Gamma_0(N))^{\text{old}}$ and $\mathcal{S}_k(\Gamma_0(N))^{\text{new}}$ are referred to as the spaces of *oldforms* and *newforms*, respectively.

One should think of $\mathcal{S}_k(\Gamma_0(N))^{\text{new}}$ as the space of cusp forms which were 'created' at level N.

Theorem 4.2 and the last statement of Lemma 4.3 prove part of the following Lemma (although a different argument is required to to deal with T_p for $p|N$)

Proposition 4.4. *The spaces $\mathcal{S}_k(\Gamma_0(N))^{\text{old}}$ and $\mathcal{S}_k(\Gamma_0(N))^{\text{new}}$ are preserved by T_n for all $n \in \mathbb{Z}_+$ and so, are $\mathbb{T}_{\mathbb{Z}}$-modules. It follows (by Theorem 4.2) that $\mathcal{S}_k(\Gamma_0(N))^{\text{old}}$ and $\mathcal{S}_k(\Gamma_0(N))^{\text{new}}$ both have orthogonal bases of simultaneous eigenforms for $\mathbb{T}_{\mathbb{Z}}^*$.*

The following (difficult) result gives a useful criterion for recognizing oldforms:

Theorem 4.5. *Take $f \in \mathcal{S}_k(\Gamma_0(N))$. If $a_n(f) = 0$ for all n with $\gcd(n, N) = 1$, then $f \in \mathcal{S}_k(\Gamma_0(N))^{\text{old}}$.*

Note that the condition is certainly not necessary. For instance, if $f \in \mathcal{S}_k(\Gamma_0(M))$, then $f \in \mathcal{S}_k(\Gamma_0(N))^{\text{old}}$, for all $N > M$ with $M|N$, but it need not be the case that $a_n(f) = 0$ for *any* n.

Using Theorem 4.5, we finally obtain the promised result about eigenforms in $\mathcal{S}_k(\Gamma_0(N))^{\text{new}}$.

Theorem 4.6. *If $f \in \mathcal{S}_k(\Gamma_0(N))^{\text{new}}$ is an eigenform for all of $\{T_n | \gcd(n, N) = 1\}$, then it is an eigenform for all of $\{T_n | n \in \mathbb{Z}_+\}$. Hence $\mathcal{S}_k(\Gamma_0(N))^{\text{new}}$ has an orthogonal basis of eigenforms for $\{T_n | n \in \mathbb{Z}_+\}$, and thus for $\mathbb{T}_{\mathbb{Z}}$.*

Proof. We first show that if $g \in \mathcal{S}_k(\Gamma_0(N))^{\text{new}}$ is an eigenform[1] for all of $\{T_n | \gcd(n, N) = 1\}$, then $a_1(g) \neq 0$. Assume that $a_1(g) = 0$. Then for any $n \in \mathbb{Z}_+$ with $\gcd(n, N) = 1$, we have $T_n g = \xi_n g$ for some $\xi_n \in \mathbb{C}$, and so

$$a_n(g) = a_1(T_n g) = a_1(\xi_n g) = \xi_n a_1(g) = 0.$$

By Theorem 4.5, this implies that $g \in \mathcal{S}_k(\Gamma_0(N))^{\text{old}}$. But as $\mathcal{S}_k(\Gamma_0(N))^{\text{old}} \cap \mathcal{S}_k(\Gamma_0(N))^{\text{new}} = 0$, this implies that $g = 0$, a contradiction.

It thus follows that $a_1(f) \neq 0$, and so we can assume WLOG that $a_1(f) = 1$. Now say that $T_n f = \xi_n f$ for all n with $\gcd(n, N) = 1$. Then we have

$$a_n(f) = a_1(T_n f) = a_1(\xi_n f) = \xi_n a_1(f) = \xi_n.$$

[1] Here we do not consider 0 to be an eigenform.

Now for any $m \in \mathbb{Z}_+$, let $g_m = T_m f - a_m(f)f$, so that $a_1(g) = a_1(T_m f) - a_m(f) = 0$. By Proposition 4.4, $g_m \in \mathcal{S}_k(\Gamma_0(N))^{\text{new}}$. Now if $\gcd(n, N) = 1$

$$\begin{aligned} T_n g_m &= T_n(T_m f - a_m(f)f) = T_m(T_n f) - a_m(f)(T_n f) = T_m(a_n(f)f) - a_m(f)(a_n(f)f) \\ &= a_n(f)(T_m f - a_m(f)f) = a_n(f)g_m. \end{aligned}$$

By the above result, it follows that $g_m = 0$, and so $T_m f = a_m(f)f$ for all $m \in \mathbb{Z}_+$. The remaining claims are automatic. □

By the proof of Theorem 4.6, an eigenform, f, in $\mathcal{S}_k(\Gamma_0(N))^{\text{new}}$ can be normalized so that $a_1(f) = 1$.

Definition 4.3. A *newform* of level N is an eigenform $f \in \mathcal{S}_k(\Gamma_0(N))^{\text{new}}$ with $a_1(f) = 1$.

By Theorem 4.6, the newforms of level N form an orthogonal basis for $\mathcal{S}_k(\Gamma_0(N))^{\text{new}}$.

By the above, $\mathcal{S}_k(\Gamma_0(N))$ has a basis consisting of the the level N newforms, together with certain oldforms, i.e. eigenforms in $\mathcal{S}_k(\Gamma_0(N))^{\text{old}}$. It is natural to ask whether these oldforms are actually newforms of a lower level (and so each basis element was 'created' at some level, the newforms are just those that were created at level N). Indeed, we have the following

Theorem 4.7. *For any $N, k \geq 1$, the set*

$$\{f(dz) | f \text{ is a newform of level } M \text{ and } dM|N\}$$

is an orthogonal basis for $\mathcal{S}_k(\Gamma_0(N))$.

We are thus justified in only studying newforms.

4.3 The Action of $\mathbb{T}_{\mathbb{Z}}$ on a Newform

Let $f \in \mathcal{S}_k(\Gamma_0(N))$ be a newform (so that $a_1(f) = 1$). We shall consider the action of the Hecke algebra $\mathbb{T}_{\mathbb{Z}}$ on f, and thereby show that the Fourier coefficients, $a_n(f)$, are all algebraic integers, and all lie in some number field K_f. This observation provides one of the main links between the study of modular forms, and algebraic number theory.

If f is a newform, then it is an eigenform for each T_n, and so is an eigenform for $\mathbb{T}_{\mathbb{Z}}$. Hence there is a ring homomorphism $\xi : \mathbb{T}_{\mathbb{Z}} \to \mathbb{C}$, defined by $Tf = \xi(T)f$ for all $T \in \mathbb{T}_{\mathbb{Z}}$. By the argument in the proof of Theorem 4.6, $\xi(T_n) = a_n(f)$ for all n. As $\mathbb{T}_{\mathbb{Z}}$ has finite rank,

$$\xi(\mathbb{T}_{\mathbb{Z}}) = \xi(\mathbb{Z}[\{T_n | n \in \mathbb{Z}_+\}]) = \mathbb{Z}[\{\xi(T_n) | n \in \mathbb{Z}_+\}] = \mathbb{Z}[\{a_n(f) | n \in \mathbb{Z}_+\}] \subseteq \mathbb{C}$$

has finite rank as well. By basic algebraic number theory, we have thus proved the following:

Theorem 4.8. *If $f \in \mathcal{S}_k(\Gamma_0(N))$ is a newform, then $K_f := \mathbb{Q}[\{a_n(f) | n \in \mathbb{Z}_+\}]$ is a number field, and $a_n(f) \in \mathcal{O}_{K_f}$ for all n.*

Now that the Fourier coefficients of f lie in a number field, K_f, it is now natural to consider the Galois conjugates of f. Explicitly, if $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, then define $f^\sigma := \sum_{n=1}^{\infty} a_n(f)^\sigma q^n$. Unsurprisingly[2], we have the following

Proposition 4.9. *If f is a newform of level N, and $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, then f^σ is also a newform of level N.*

In light of this result, it is often customary to redefine a newform to be a Galois-conjugacy class $\{f^\sigma | \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\}$. We shall adopt this convention for the rest of this paper.

4.4 The Abelian Variety associated to a Newform

For the remainder of this section, let f be a newform of weight 2 and level N. We shall associate to f an abelian variety, A_f, of dimension $[K_f : \mathbb{Q}]$ (which will later be used to construct Galois representations).

For convenience, we will let $g = \dim J_0(N) = \dim \mathbb{T}_{\mathbb{C}}$ and $d = [K_f : \mathbb{Q}]$. Also to simplify notation, let $\mathcal{S}_2 = \mathcal{S}_2(\Gamma_0(N))$, $J_0 = J_0(N)$ and $\Lambda = \Lambda(\Gamma_0(N))$ (see Corollary 2.5).

We shall construct A_f as a quotient of the Jacobian J_0. Explicitly, let

$$I_f = \ker(\mathbb{T}_{\mathbb{Z}} \xrightarrow{\xi} \mathbb{C}) = \{T \in \mathbb{T}_{\mathbb{Z}} | Tf = 0\},$$

so that I_f is an ideal of $\mathbb{T}_{\mathbb{Z}}$ and $\mathrm{rk}\, I_f = \mathrm{rk}\, \mathbb{T}_{\mathbb{Z}} - \mathrm{rk}\, \xi(\mathbb{T}_{\mathbb{Z}}) = g - d$. Now define $A_f = J_0/I_f J_0$. We have the following

Theorem 4.10. *A_f is an abelian variety of dimension $[K_f : \mathbb{Q}]$. Moreover, A_f can be defined over $\mathbb{Q}$.*

Recall from Lemma 3.6 that we have a natural isomorphisms $\mathbb{T}_{\mathbb{C}} \cong \mathcal{S}_2^\vee$ and $J_0 \cong \mathbb{T}_{\mathbb{C}}/\Lambda$. Also as the action of $\mathbb{T}_{\mathbb{Z}}$ on $\mathbb{T}_{\mathbb{C}}$ by multiplication induces the action of $\mathbb{T}_{\mathbb{Z}}$ on J_0, we must have that $\mathbb{T}_{\mathbb{Z}}(\Lambda) \subseteq \Lambda$, and so $\Lambda(\Gamma_0(N))$ is a $\mathbb{T}_{\mathbb{Z}}$-module.

By Theorem 4.7, the newforms of level M (ranging over all $M|N$) essentially form a basis for $\mathcal{S}_2$, and so we have a decomposition $\mathcal{S}_2 = \bigoplus_{M|N} \bigoplus_{\substack{f \text{ level } M \\ \text{newform}}} [f]^{d(N/M)}$, where $d(N/M)$ is the number of divisors of N/M (recall that a 'newform' refers to a Galois conjugacy class of forms). It follows that

$$\mathbb{T}_{\mathbb{C}} = \mathcal{S}_2^\vee = \bigoplus_{M|N} \bigoplus_{\substack{f \text{ level M} \\ \text{newform}}} ([f]^\vee)^{d(N/M)}$$

It can be shown that passing to the quotient now gives:

[2]It should be noted that the proof of Proposition 4.9 is nontrivial. Indeed, the notion of modular forms (and by extension, newforms) is defined *analytically*, and so one cannot merely take the definition of a modular form and apply σ to it. Nevertheless, Proposition 4.9 is true, and can be proven (with a significant amount of work).

Theorem 4.11. *There is a* $\mathbb{Q}$*-isogeny*[3]

$$J_0(N) \xrightarrow{\sim} \bigoplus_{M|N} \bigoplus_{\substack{f \text{ level } M \\ \text{newform}}} A_f^{d(N/M)}$$

Thus, at least up to isogeny, the abelian varieties A_f completely determine $J_0(N)$.

[3] a surjective $\mathbb{Q}$-morphism of abelian varieties with finite kernel

5 Tate Modules and Galois Representations

Let A be an abelian variety over a perfect field k. In this section, we construct the *Tate module*, $\mathrm{Ta}_\ell(A)$ of A (where $\ell \neq \operatorname{char} k$ is prime) and give its basic properties. This module will be a free $\mathbb{Z}_\ell$-module of rank $2(\dim A)$, and moreover, the absolute Galois group $G_k := \mathrm{Gal}(\overline{k}/k)$ of k will act on $\mathrm{Ta}_\ell(A)$. Thus the Tate module of A will define a representation $\rho_{A,\ell} : G_k \to \mathrm{GL}_{2\dim A}(\mathbb{Z}_\ell)$.

Now for the remainder of this paper, f will represent a newform of weight 2 and level N. In Theorem 4.10 we constructed an abelian variety $A_f/\mathbb{Q}$ of dimension $[K_f : \mathbb{Q}]$ corresponding to f. Constructing the Tate module of A_f will now give a Galois representation $\rho_{f,\ell} = \rho_{A_f,\ell} : G_\mathbb{Q} \to \mathrm{GL}_{2[K_f:\mathbb{Q}]}(\mathbb{Z}_\ell)$. This is *almost* the representation promised in Theorem **??**, except that this is a $2[K_f : \mathbb{Q}]$-dimensional representation, instead of the promised 2-dimensional representation. We shall get around this difficulty by considering the action of $\mathbb{T}_\mathbb{Z}/I_f$ on A_f, and showing that this allows us to decompose $\rho_{f,\ell}$ into a product $\prod_{\lambda|\ell} \rho_{f,\lambda}$ of two dimensional representations (where λ ranges over all primes in $\mathcal{O}_{K_f}$ lying over ℓ).

5.1 The Tate Module of an Abelian Variety

Fix a perfect field k (e.g. a field of characteristic zero or a finite field) and let A/k be an abelian variety of dimension $d \geq 1$. Recall the following standard result

Proposition 5.1. *For any integer $n \geq 1$, if either $\operatorname{char} k = 0$ or $\gcd(n, \operatorname{char} k) = 1$, then $A[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2d}$.*

As the addition map $+ : A \times A \to A$ is defined over k, for any $\sigma \in G_k$ the map $\sigma : A(\overline{k}) \to A(\overline{k})$ is a group homomorphism. Now for any n, the multiplication by n map, $[n] : A(\overline{k}) \to A(\overline{k})$ is defined over k, and moreover $A[n] = \ker[n] \subseteq A(\overline{k})$. It follows that $\sigma[n] = [n]\sigma$ for all $\sigma \in G_k$, and so G_k acts on $\ker[n] = A[n]$. Thus $A[n]$ defines is a G_k-module, and so defines a (continuous) map $G_k \to \mathrm{Aut}(A[n])$.

Now pick a prime $\ell \neq \operatorname{char} k$. For any $r \geq 1$, we have $A[\ell^r] \cong (\mathbb{Z}/\ell^r\mathbb{Z})^{2d}$ by Proposition 5.1, and so for each $r \geq 1$, we have a continuous map $G_k \to \mathrm{GL}_{2d}(\mathbb{Z}/\ell^r\mathbb{Z})$. Now for any $r \geq 1$, the multiplication by ℓ map $[\ell] : A[\ell^{r+1}] \twoheadrightarrow A[\ell^r]$ is a group homomorphism which is defined over k, and so is a homomorphism of G_k-modules. This thus defines an inverse system of G_k-modules:

$$\cdots \twoheadrightarrow A[\ell^3] \twoheadrightarrow A[\ell^2] \twoheadrightarrow A[\ell].$$

By taking the inverse limit of this sequence, we the Tate module

Definition 5.1. For a prime $\ell \neq \operatorname{char} k$, $\mathrm{Ta}_\ell(A) := \varprojlim A[\ell^r]$ with the induced action of G_k.

Since $A[\ell^r] \cong (\mathbb{Z}/\ell^r\mathbb{Z})^{2d}$, it follows that $\mathrm{Ta}_\ell(A) \cong \mathbb{Z}_\ell^{2d}$ as a group, and so the action of G_k defines a continuous homomorphism $\rho_{A,\ell} : G_k \to \mathrm{GL}_{2d}(\mathbb{Z}_\ell)$.

It will often be convenient to define $V_\ell(A) := \mathrm{Ta}_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, so that $V_\ell(A) \cong \mathbb{Q}_\ell^{2d}$ defines a continuous homomorphism $\rho_{A,\ell} : G_k \to \mathrm{GL}_{2d}(\mathbb{Q}_\ell)$ (this has the advantage of allowing us to work over vector spaces instead of $\mathbb{Z}_\ell$-modules).

As might be expected, the construction $A \to \mathrm{Ta}_\ell(A)$ is functorial. Explicitly, let A and A' be abelian varieties over k, and let $f : A \to A'$ be a morphism of abelian varieties over k. By definition, $f : A(\overline{k}) \to A'(\overline{k})$ is a group homomorphism, and so it restricts to a homomorphism $f : A[\ell^r] \to A'[\ell^r]$ for all r. As f is defined over k, this is in fact a map of G_k-modules. It follows that f induces a map $f_{\mathrm{Ta}} : \mathrm{Ta}_\ell(A) \to \mathrm{Ta}_\ell(A')$ of G_k-modules. In particular, it follows that the endomorphism ring $\mathrm{End}_k(A)$ of A acts on the $\mathrm{Ta}_\ell(A)$, and this action commutes with the action of G_k.

It is often useful to consider abelian varieties only up to isogeny (and so to not care explicitly about the isomorphism class of an abelian variety). Thus we would like $\mathrm{Ta}_\ell(A)$ not to depend to heavily on the isomorphism class of A. Indeed we have the following

Proposition 5.2. *If $f : A \to A'$ is a k-isogeny of abelian varieties, then $f_{\mathrm{Ta}} : V_\ell(A) \to V_\ell(A')$ is an isomorphism of G_k-modules.*

Proof. We shall first show that $f_{\mathrm{Ta}} : \mathrm{Ta}_\ell(A) \to \mathrm{Ta}_\ell(A')$ is injective. Assume that $f_{\mathrm{Ta}}(x) = 0$ for some $x \in \mathrm{Ta}_\ell(A)$. As $x \in \mathrm{Ta}_\ell(A) = \varprojlim A[\ell^r]$, we can write $x = (x_1, x_2, \ldots)$ where $x_r \in A[\ell^r]$ and $x_r = [\ell]x_{r+1}$ for all $r \geq 1$.

Now by definition, $f_{\mathrm{Ta}}(x) = (f(x_1), f(x_2), \ldots)$, so if $f_{\mathrm{Ta}}(x) = 0$, then $f(x_r) = 0$ for all r, and so $x_r \in \ker f$ for all r. But also, $x_r \in A[\ell^r] \subseteq A[\ell^\infty] := \bigcup_{s=1}^\infty A[\ell^s]$ for all r, and so $x_r \in (\ker f) \cap A[\ell^\infty]$. But now $\ker f$ is finite (by the definition of isogeny) and so $(\ker f) \cap A[\ell^\infty]$ is also finite. But now as $(\ker f) \cap A[\ell^\infty] \subseteq A[\ell^\infty] = \bigcup_{s=1}^\infty A[\ell^s]$, we have $(\ker f) \cap A[\ell^\infty] \subseteq A[\ell^{r_0}]$ for some r_0. Hence $x_r \in A[\ell^{r_0}]$ for all r.

But this implies that $x_r = [\ell^{r_0}]x_{r+r_0} \in [\ell^{r_0}]A[\ell^{r_0}] = 0$ for all r, and so $x = 0$. Thus $f : \mathrm{Ta}_\ell(A) \to \mathrm{Ta}_\ell(A')$ is injective.

It now follows that $f_{\mathrm{Ta}} : V_\ell(A) \to V_\ell(A')$ is also injective. Indeed, say that $f_{\mathrm{Ta}}(x) = 0$ for some $x \in V_\ell(A)$. By the definition of $V_\ell(A) = \mathrm{Ta}_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, we have $mx \in \mathrm{Ta}_\ell(A)$ for some $m > 0$. Thus $f_{\mathrm{Ta}}(mx) = mf_{\mathrm{Ta}}(x) = 0$, and so $mx = 0$, giving $x = 0$ (recall that $\mathrm{char}\, \mathbb{Q}_\ell = 0$).

But now as $V_\ell(A)$ and $V_\ell(A')$ are vector spaces of the same dimension (as A and A' are isogenous, they have the same dimension), it follows that f_{Ta} is also surjective. Thus it is a bijection, and thus a G_k-module isomorphism. □

Note that this does *not* imply that $f_{\mathrm{Ta}} : \mathrm{Ta}_\ell(A) \to \mathrm{Ta}_\ell(A')$ is an isomorphism. In particular, recalling the isogeny from Theorem 4.11, we have

Corollary 5.3. *For any N and ℓ,*

$$V_\ell(J_0(N)) \cong \bigoplus_{M|N} \bigoplus_{\substack{f \text{ level } M \\ \text{newform}}} V_\ell(A_f)^{d(N/M)}.$$

The component representations, $V_\ell(A_f)$ will play a big role in later.

From now on, assume that $k \subseteq \mathbb{C}$ (in particular, $\operatorname{char} k = 0$). In this case, we can give an alternate description of $\mathrm{Ta}_\ell(A)$ which is often easier to work with.

Note that $A(\mathbb{C})$ is an abelian variety over $\mathbb{C}$, and so is a complex torus. We can thus write $A(\mathbb{C}) = \mathbb{C}^d/\Lambda$ for some lattice $\Lambda \in \mathbb{C}^d$. Now for any n, we have the natural identification

$$A[n] = (\mathbb{C}^d/\Lambda)[n] = \left(\frac{1}{n}\Lambda\right)/\Lambda \cong \Lambda/n\Lambda.$$

Moreover, under this identification, the map $[\ell] : A[\ell^{r+1}] \to A[\ell^r]$ corresponds to the quotient map $\Lambda/\ell^{r+1}\Lambda \twoheadrightarrow \Lambda/\ell^r\Lambda$. Thus we can identify

$$\mathrm{Ta}_\ell(A) = \varprojlim A[\ell^r] = \varprojlim \Lambda/\ell^r\Lambda = \varprojlim(\Lambda \otimes_{\mathbb{Z}} \mathbb{Z}/\ell^r\mathbb{Z}) = \Lambda \otimes_{\mathbb{Z}} \varprojlim \mathbb{Z}/\ell^r\mathbb{Z} = \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_\ell,$$

and similarly, $V_\ell(A) = \mathrm{Ta}_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell = \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell = \Lambda \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$.

Now let $f : A \to A'$ be a k-morphism of abelian varieties. Let $A(\mathbb{C}) = \mathbb{C}^d/\Lambda$ and $A'(\mathbb{C}) = \mathbb{C}^{d'}/\Lambda'$. As $f : A(\mathbb{C}) \to A'(\mathbb{C})$ is a morphism of complex tori, f is induced by some $\mathbb{C}$-linear map $f_{\mathbb{C}} : \mathbb{C}^d \to \mathbb{C}^{d'}$ with $f(\Lambda) \to \Lambda'$. In particular, f induces a $\mathbb{Z}$-linear map $f_{\mathbb{Z}} : \Lambda \to \Lambda'$ (and f is determined by $f_{\mathbb{Z}}$). Extending scalars to $\mathbb{Z}_\ell$, $f_{\mathbb{Z}}$ induces a map $f_{\mathbb{Z}_\ell} : \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to \Lambda' \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$, and it can easily be seen that, under the above identifications, $f_{\mathbb{Z}_\ell} = f_{\mathrm{Ta}}$. In particular, the action of $\mathrm{End}_k(A)$ on A induces an action of $\mathrm{End}_k(A)$ on Λ, and so makes Λ into a $\mathrm{End}_k(A)$-module. We now have $\mathrm{Ta}_\ell(A) \cong \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ as $\mathrm{End}_k(A)$-modules.

Therefore, the functor $A \mapsto \mathrm{Ta}_\ell(A)$ (sending abelian varieties to $\mathbb{Z}_\ell$-modules) can be completely described in terms of the lattice Λ (this in particular, allows for easy passage from $\mathrm{Ta}_\ell(A)$ to $\mathrm{Ta}_{\ell'}(A)$ for $\ell \neq \ell'$).

This picture however, does adequately describe the action of G_k on $\mathrm{Ta}_\ell(A)$. Indeed, there is no natural action of G_k on Λ, and so the action of G_k must be defined at the level of $\Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. The main reason for this is that, by treating A as a complex torus, the above construction completely ignores the algebraic structure of A/k, where as the action of G_k is defined entirely in terms of this algebraic structure. For instance, we know by our general theory that G_k must act on $\Lambda/\ell^r\Lambda$ for all r (as this space is identified with $A[\ell^r]$), but actually determining this action is generally quite difficult.

As a result of considerations like this, it is in general quite difficult to relate the $\mathrm{End}_k(A)$-module structure of $\mathrm{Ta}_\ell(A)$ to its G_k-module structure. Much of the significance of the Eichler-Shimura relations (discussed later) is that they do provide a nontrivial relationship between the actions of $\mathrm{End}_{\mathbb{Q}}(J_0(N))$ (or rather, the action of $\mathbb{T}_{\mathbb{Z}} \subseteq \mathrm{End}_{\mathbb{Q}}(J_0(N))$) and $G_{\mathbb{Q}}$ on $\mathrm{Ta}_\ell(J_0(N))$.

To conclude this section, we discuss one more result which will be useful later when we consider reductions of modular curves. Let $k = \mathbb{Q}$, and let $A/\mathbb{Q}$ be an abelian variety of dimension d. Pick some prime p, such that A has good reduction at p (that is, that $A_{\mathbb{F}_p}$ is still a smooth abelian variety over $\mathbb{F}_p$). The reduction of A at p gives a surjective group homomorphism $\pi : A(\overline{\mathbb{Q}}) \twoheadrightarrow A_{\mathbb{F}_p}(\overline{\mathbb{F}_p})$.

Now by Theorem 5.1, $A[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2d} \cong A_{\mathbb{F}_p}[n]$ provided that $p \nmid n$. It follows that, for all primes $\ell \neq p$, π induces an isomorphism $\mathrm{Ta}_\ell(A) \xrightarrow{\sim} \mathrm{Ta}_\ell(A_{\mathbb{F}_p})$ of $\mathbb{Z}_\ell$-modules. Moreover, the actions of $G_{\mathbb{Q}}$ and $G_{\mathbb{F}_p}$ on $\mathrm{Ta}_\ell(A)$ and $\mathrm{Ta}_\ell(A_{\mathbb{F}_p})$, respectively, are 'compatible' under this isomorphism in the manner described below

Theorem 5.4. *If $A/\mathbb{Q}$ is an abelian variety with good reduction at p, then the map $\pi : A(\overline{\mathbb{Q}}) \twoheadrightarrow A(\overline{\mathbb{F}}_p)$ induces an isomorphism $\pi_{\mathrm{Ta}} : \mathrm{Ta}_\ell(A) \xrightarrow{\cong} \mathrm{Ta}_\ell(A_{\mathbb{F}_p})$. Moreover, if $\varphi_p \in G_{\mathbb{F}_p}$ is the Frobenius automorphism $\varphi_p(x) = x^p$, and $\mathrm{Frob}_p \in G_{\mathbb{Q}}$ is any lift of φ_p, then $\pi_{\mathrm{Ta}} \circ \mathrm{Frob}_p = \varphi_p \circ \pi_{\mathrm{Ta}}$.*

5.2 The Galois Representation associated to a Newform

Now again let f be a weight 2 newform of level N. Also let $K = K_f$ and let $d = [K : \mathbb{Q}]$. By Theorem 4.10, f determines an abelian variety, A_f, of dimension d which is defined over $\mathbb{Q}$. By the previous section, $\mathrm{Ta}_\ell(A_f)$ defines a continuous Galois representation $\rho_{f,\ell} := \rho_{A_f,\ell} : G_{\mathbb{Q}} \to \mathrm{GL}_{2d}(\mathbb{Q}_\ell)$. If $d = 1$ (so that $K = \mathbb{Q}$), then this is the two-dimensional Galois representation promised in Theorem **??**. However, in the general case, this will be a $2d$-dimensional representation, not a two dimensional representation. To produce 2-dimensional representation, we must consider the action of $\mathbb{T}_{\mathbb{Z}}$ on $\mathrm{Ta}_\ell(A_f)$.

As $\mathbb{T}_{\mathbb{Z}}$ acts on $J_0 := J_0(N)$, it acts on $A_f = J_0/I_f J_0$. Moreover, I_f clearly acts trivially on A_f, and so we in fact have a (faithful) action of $\mathbb{T}_{\mathbb{Z}}/I_f$ on A_f. Now using the homomorphism $\xi : \mathbb{T}_{\mathbb{Z}} \to \mathbb{C}$, we may identify $\mathbb{T}_{\mathbb{Z}}/I_f$ with $\xi(\mathbb{T}_{\mathbb{Z}}) = \mathbb{Z}[\{a_n(f) | n \in \mathbb{Z}_+\}] \subseteq \mathbb{C}$, and so we have an action of $\xi(\mathbb{T}_{\mathbb{Z}})$ on A_f. By passing to the Tate module, this gives us an action of $\xi(\mathbb{T}_{\mathbb{Z}})$ on $\mathrm{Ta}_\ell(A_f)$. Moreover, as the action of $\mathbb{T}_{\mathbb{Z}}$ on J_0, and the quotient map $J_0 \twoheadrightarrow A_f$ are both defined over $\mathbb{Q}$, the action of $\xi(\mathbb{T}_{\mathbb{Z}})$ on A_f is defined over $\mathbb{Q}$. It follows that the action of $\xi(\mathbb{T}_{\mathbb{Z}})$ on $\mathrm{Ta}_\ell(A_f)$ commutes with the action of $G_{\mathbb{Q}}$.

Now for convenience we pass from Ta_ℓ to V_ℓ. Recall that $V_\ell(A) = \mathrm{Ta}_\ell(A_f) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is a $\mathbb{Q}_\ell$-vector space, and the $\mathbb{Q}_\ell$-action commutes with both the $\xi(\mathbb{T}_{\mathbb{Z}})$ action and the $G_{\mathbb{Q}}$ action. Since the $\xi(\mathbb{T}_{\mathbb{Z}})$ and $\mathbb{Q}_\ell$ actions commute, we in fact have an action of $\xi(\mathbb{T}_{\mathbb{Z}}) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$. Now by basic algebraic number theory, we have a natural isomorphism

$$\xi(\mathbb{T}_{\mathbb{Z}}) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \cong (\xi(\mathbb{T}_{\mathbb{Z}}) \otimes_{\mathbb{Z}} \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong \mathbb{Q}[\{a_n(f) | n \in \mathbb{Z}_+\}] \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong \prod_{\lambda | \ell} K_\lambda,$$

where the final product is taken over primes in $\mathcal{O}_K$ lying over ℓ. It follows that $V_\ell(A_f)$ decomposes as a product $V_\ell(A_f) \cong \prod_{\lambda|\ell} V_\lambda(A_f)$, where for each λ, $V_\lambda(A_f) := e_\lambda V_\ell(A_f)$ with $e_\lambda = (0, \ldots, 0, 1, 0, \ldots, 0) \in \prod_{\lambda|\ell} K_\lambda$. As the action of $\prod_{\lambda|\ell} K_\lambda$ commutes with the action of $G_{\mathbb{Q}}$, each $V_\lambda(A_f)$ is a $G_{\mathbb{Q}}$-module.

Moreover, for each λ, $K_\lambda \subseteq \prod_{\lambda|\ell} K_\lambda$ acts naturally (and nontrivially) on $V_\lambda(A_f)$, and this action commutes with the action of $G_{\mathbb{Q}}$. Hence $V_\lambda(A_f)$ is a K_λ-vector space, and $G_{\mathbb{Q}}$ acts on $V_\lambda(A_f)$ by K_λ-linear maps. It thus remains to show the following

Proposition 5.5. *For any $\lambda|\ell$, $\dim_{K_\lambda} V_\lambda(A_f) = 2$.*

Proof. Let $A_f(\mathbb{C}) = \mathbb{C}^d/\Lambda$ for some lattice $\Lambda \subseteq \mathbb{C}^d$. We have that $\mathrm{End}_{\mathbb{Q}}(A_f)$ acts on Λ by the discussion in the previous section, and so (as $\xi(\mathbb{T}_{\mathbb{Z}}) \subseteq \mathrm{End}_{\mathbb{Q}}(A_f)$), Λ is a $\xi(\mathbb{T}_{\mathbb{Z}})$-module. Let $\Lambda_{\mathbb{Q}} = \Lambda \otimes \mathbb{Z}$, so that $\Lambda_{\mathbb{Q}}$ is a $\xi(\mathbb{T}_{\mathbb{Z}}) \otimes_{\mathbb{Z}} \mathbb{Q} = K$-vector space. Note that $V_\ell(A_f) = \Lambda_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$, and so

$$V_\lambda(A_f) = V_\ell(A_f) \otimes_{\prod_{\lambda'|\ell} K_{\lambda'}} K_\lambda = (\Lambda_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{Q}_\ell) \otimes_{K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell} K_\lambda = \Lambda_{\mathbb{Q}} \otimes_K K_\lambda.$$

It follows that

$$\dim_{K_\lambda} V_\lambda(A_f) = \dim_{K_\lambda}(\Lambda_{\mathbb{Q}} \otimes_K K_\lambda) = \dim_K \Lambda_{\mathbb{Q}} = \frac{\dim_{\mathbb{Q}} \Lambda_{\mathbb{Q}}}{\dim_{\mathbb{Q}} K} = \frac{\mathrm{rk}\,\Lambda}{[K:\mathbb{Q}]} = \frac{2(\dim A_f)}{[K:\mathbb{Q}]} = \frac{2[K:\mathbb{Q}]}{[K:\mathbb{Q}]} = 2.$$

□

So indeed, for any ℓ and any $\lambda|\ell$ (and thus any prime λ in $\mathcal{O}_K$), we have an action of $G_{\mathbb{Q}}$ on a 2-dimensional K_λ-vector space $V_\lambda(A_f)$, which gives a continuous homomorphism $\rho_{f,\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_\lambda)$, as promised in Theorem **??**.

6 The Eichler-Shimura Relations

We have now constructed a family of Galois representations $\rho_{f,\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_\lambda)$ for a weight 2 newform f of level N, with $K_f = K$. Thus far, however, these Galois representations have no clear relation to f, besides the fact that f was used in their construction. As promised in Theorem **??**, for almost all primes, p, (namely $p \nmid \ell N$), the characteristic polynomial of $\rho_{f,\lambda}(\mathrm{Frob}_p)$ is determined by the original Fourier coefficients $\{a_n(f)\}$ of f. Specifically, it is $x^2 - a_p(f)x + p$ (recall that we are only considering the case $k = 2$).

This condition essentially characterizes $\rho_{f,\lambda}$ as the set $\{\mathrm{Frob}_p \,|p \nmid \ell N\}$ is dense in $G_{\mathbb{Q}}$ by Chebotarev density[4]. This often allows us to treat the construction of $\rho_{f,\lambda}$ as a 'black box.' Namely, once we know that $\rho_{f,\lambda}$ exists (by the above construction) we can often forget the precise details of the construction, and simply study the characteristic polynomials of Frob_p. This simplification is even more useful in the $k \neq 2$ case, when the construction of $\rho_{f,\lambda}$ is significantly more complicated.

Our main goal in this section is to sketch the proof of this fact. The bulk of the argument lies in establishing the Eichler-Shimura relations, which give a description of the Hecke operator $T_p : J_0(N) \to J_0(N)$ modulo p (for $p \nmid N$). From now on, fix some $N \geq 1$, and let p be a prime with $p \nmid N$. First we need the following result:

Theorem 6.1. *The modular curve $X_0(N)$ and the modular Jacobian $J_0(N)$ both have good reduction at p.*

[4]Technically some care is necessary here, as Frob_p is not defined in $G_{\mathbb{Q}}$, *even up to conjugation*, since every prime is ramified in $\overline{\mathbb{Q}}/\mathbb{Q}$. Thus the above statement must be refined slightly. However, we do not concern ourselves with this.

This means that $X_0(N)$ defines a smooth curve, denoted $\widetilde{X}_0(N)$, over $\mathbb{F}_p$ whose Jacobian, $\widetilde{J}_0(N)$, is the reduction of $J_0(N)$ at p. It turns out that the moduli space interpretation of $X_0(N)$ given in Theorem 2.1, also applies to $\widetilde{X}_0(N)$ (where our elliptic curves are taken over $\overline{\mathbb{F}_p}$, instead of $\mathbb{C}$). In fact this even applies (in some sense) when $p|N$. We shall use these facts freely without proof (and without a precise statement).

As $\widetilde{X}_0(N)$ is defined in characteristic p, there is a natural morphism $\varphi_p : \widetilde{X}_0(N) \to \widetilde{X}_0(N)$ given by $x \mapsto x^p$. This induces pushforward and pullback maps $\varphi_{p,*}, \varphi_p^* : \widetilde{J}_0(N) \to \widetilde{J}_0(N)$. The Eichler-Shimura relations state the following:

Theorem 6.2 (Eichler-Shimura)**.** *If p is a prime and $p \nmid N$, then the Hecke operator $T_p : J_0(N) \to J_0(N)$ reduces to a morphism $\widetilde{T}_p : \widetilde{J}_0(N) \to \widetilde{J}_0(N)$, and we have $\widetilde{T}_p = \varphi_{p,*} + \varphi_p^*$ in $\mathrm{End}_{\mathbb{F}_p}(\widetilde{J}_0(N))$.*

Proof. (sketch) Recall the definition of T_p as a correspondence $T_p : X_0(N) \rightsquigarrow X_0(N)$ given in Section 3.2. We would like to reduce the maps $\alpha, \beta : X_0(pN) \to X_0(N)$ to maps $\widetilde{\alpha}, \widetilde{\beta} : \widetilde{X}_0(pN) \to \widetilde{X}_0(N)$, and use these maps to define a correspondence $\widetilde{T}_p : \widetilde{X}_0(N) \rightsquigarrow \widetilde{X}_0(N)$. Unfortunately this is somewhat problematic, as the curve $X_0(pN)$ has bad reduction at p, and so we cannot construct $\widetilde{X}_0(pN)$ as a smooth curve over $\mathbb{F}_p$.

Luckily, the reduction of $\widetilde{X}_0(pN)$ at p is still 'good enough' to allow us to describe it nicely. We shall need the following lemma

Lemma 6.3. *If E and E' are elliptic curves over $\mathbb{F}_p$, and $\psi : E \to E'$ is an isogeny with $\deg \psi = p$, then up to isomorphism, either $\psi = \varphi_p : E \to E^{\varphi_p}$ or $\psi = \widehat{\varphi_p} : E^{\varphi_p} \to E$.*

Here E^{φ_p} is the elliptic curve over $\mathbb{F}_p$ obtained by applying φ_p to the polynomials defining E. Also, for any isogeny $\psi : E \to E'$, $\widehat{\psi} : E' \to E$ is the dual isogeny (which can be thought of as the pullback map associated to ψ, by identifying $\mathrm{Jac}(E) = E$ and $\mathrm{Jac}(E') = E'$). It can be shown that $\psi \circ \widehat{\psi} = \widehat{\psi} \circ \psi = [\deg \psi]$ and $\deg \psi = \deg \widehat{\psi}$.

Proof. (Lemma 6.3) Since $\deg \psi = p$, we have that $\widehat{\psi} \circ \psi = [p] : E \to E$. Now in characteristic p, the map $[p] : E \to E$ is not separable, and so $\deg_{\mathrm{ins}}([p]) > 1$. Hence

$$(\deg_{\mathrm{ins}} \psi)(\deg_{\mathrm{ins}} \widehat{\psi}) = \deg_{\mathrm{ins}}(\psi \circ \widehat{\psi}) = \deg_{\mathrm{ins}}([p]) > 1.$$

Thus either $\deg_{\mathrm{ins}} \psi > 1$ or $\deg_{\mathrm{ins}} \widehat{\psi} > 1$.

If $\deg_{\mathrm{ins}} \psi > 1$, then as $\deg_{\mathrm{ins}} \psi | \deg \psi = p$, it follows that $\deg_{\mathrm{ins}} \psi = p$, and so $\deg_{\mathrm{sep}} \psi = 1$, and so ψ is purely inseparable. But, up to isomorphism, the only purely inseparable morphisms in characteristic p are powers of φ_p. As $\deg \psi = p = \deg \varphi_p$, it follows that $\psi = \varphi_p$, up to isomorphism. On the other hand, if $\deg_{\mathrm{ins}} \widehat{\psi} > 1$, then by the same argument $\widehat{\psi} = \varphi_p$, and so $\psi = \widehat{\varphi_p}$. □

It is worth noting that the two cases in Lemma 6.3 are not mutually exclusive - it is possible that $\psi = \varphi_p = \widehat{\varphi_p}$. By the argument above we can see that this happens iff $\deg_{\mathrm{ins}}[p] = p^2$ or equivalently,

$\deg_{\text{sep}}[p] = 1$. Since $\#E[p] = \deg_{\text{sep}}[p]$, this happens iff $E[p] = 0$, which (by definition) happens iff E is a *supersingular* elliptic curve.

Now treat $\widetilde{X}_0(pN)$ as (the compactification of) the moduli space $S_0(pN)$ from Theorem 2.2. By Lemma 6.3, we can divide $S_0(pN)$ into two sets, those $\left(E \xrightarrow{\psi} E', C\right)$ with $\psi = \varphi_p$ and those with $\psi = \widehat{\varphi_p}$. Thus we would expect $\widetilde{X}_0(pN)$ to be a union of two smooth curves over $\mathbb{F}_p$, glued together at a finite collection of points. Indeed we have the following

Proposition 6.4. *Define the maps $i, j : \widetilde{X}_0(N) \to \widetilde{X}_0(pN)$ (at the level of moduli spaces) by*

$$i(E, C) = \left(E \xrightarrow{\varphi_p} E^{\varphi_p}, C\right), \qquad j(E, C) = \left(E^{\varphi_p} \xrightarrow{\widehat{\varphi_p}} E, C^{\varphi_p}\right).$$

Then we have $\widetilde{X}_0(pN) = i(\widetilde{X}_0(N)) \cup j(\widetilde{X}_0(N)) \cong \widetilde{X}_0(N) \cup_\Sigma \widetilde{X}_0(N)$, where $\Sigma = i(\widetilde{X}_0(N)) \cap j(\widetilde{X}_0(N)) \hookrightarrow \widetilde{X}_0(N)$ is the set of points in $\widetilde{X}_0(N)$ corresponding to supersingular elliptic curves.

We are now ready to finish the proof of Theorem 6.2. Define $\widetilde{\alpha}, \widetilde{\beta} : \widetilde{X}_0(pN) \to \widetilde{X}_0(N)$, as in Section 3.2, by

$$\widetilde{\alpha}\left(E \xrightarrow{\psi} E', C\right) = (E, C), \qquad \widetilde{\beta}\left(E \xrightarrow{\psi} E', C\right) = (E', \psi(C)).$$

Notice that we have

$$\begin{aligned}
\widetilde{\alpha}(i(E, C)) &= \widetilde{\alpha}\left(E \xrightarrow{\varphi_p} E^{\varphi_p}, C\right) = (E, C) \\
\widetilde{\alpha}(j(E, C)) &= \widetilde{\alpha}\left(E^{\varphi_p} \xrightarrow{\widehat{\varphi_p}} E, C^{\varphi_p}\right) = (E^{\varphi_p}, C^{\varphi_p}) \\
\widetilde{\beta}(i(E, C)) &= \widetilde{\alpha}\left(E \xrightarrow{\varphi_p} E^{\varphi_p}, C\right) = (E^{\varphi_p}, C^{\varphi_p}) \\
\widetilde{\beta}(j(E, C)) &= \widetilde{\alpha}\left(E^{\varphi_p} \xrightarrow{\widehat{\varphi_p}} E, C^{\varphi_p}\right) = (E, C)
\end{aligned}$$

and so $\widetilde{\alpha} \circ i = \widetilde{\beta} \circ j = \text{id}$ and $\widetilde{\alpha} \circ j = \widetilde{\beta} \circ i = \varphi_p$, as maps $\widetilde{X}_0(N) \to \widetilde{X}_0(N)$ (and thus are all bijections).

Now up to birational equivalence, $\widetilde{X}_0(pN)$ looks like two disjoint copies of $\widetilde{X}_0(N)$. The definitions of pushforward and pullback of maps $\widetilde{X}_0(pN) \to \widetilde{X}_0(N)$ are thus defined for all but finitely many points of $\widetilde{X}_0(N)$ and $\widetilde{X}_0(pN)$ (specifically for points not in Σ). Thus for any $(E, C) \in \widetilde{X}_0(N) \smallsetminus \Sigma$, we have the following computation:

$$\begin{aligned}
\widetilde{T}_p(E, C) &= \widetilde{\beta}_*(\widetilde{\alpha}^*(E, C)) = \widetilde{\beta}_*\left(i(\widetilde{\alpha} \circ i)^*(E, C) + j(\widetilde{\alpha} \circ j)^*(E, C)\right) = \widetilde{\beta}_*\left(i(E, C) + j\varphi_p^*(E, C)\right) \\
&= \widetilde{\beta}_*\left(i(E, C) + pj(E^{\varphi_p^{-1}}, C^{\varphi_p^{-1}})\right) = \widetilde{\beta}(i(E, C)) + p\widetilde{\beta}(j(E^{\varphi_p^{-1}}, C^{\varphi_p^{-1}})) \\
&= (E^{\varphi_p}, C^{\varphi_p}) + p(E^{\varphi_p^{-1}}, C^{\varphi_p^{-1}}) = \varphi_{p,*}(E, C) + \varphi_p^*(E, C).
\end{aligned}$$

Thus $\widetilde{T_p} = \varphi_{p,*} + \varphi_p^*$ on a Zariski-open subset of $\widetilde{J_0}(N)$. As these are both morphisms of $\widetilde{J_0}(N)$, we get that $\widetilde{T_p} = \varphi_{p,*} + \varphi_p^*$ on all of $\widetilde{J_0}(N)$ by continuity. $\square$

Now we also have $\varphi_{p,*} \circ \varphi_p^* = \varphi_p^* \circ \varphi_{p,*} = [\deg \varphi_p] = [p]$ by standard facts about Jacobians. Thus in $\mathrm{End}_{\mathbb{F}_p}(\widetilde{J_0}(N))$, $\varphi_{p,*}$ and φ_p^* satisfy the polynomial

$$(x - \varphi_{p,*})(x - \varphi_p^*) = x^2 - (\varphi_{p,*} + \varphi_p^*)x + \varphi_{p,*} \circ \varphi_p^* = x^2 - \widetilde{T_p}x + [p]$$

Now pick a prime $\ell \neq p$ and consider the Tate module $\mathrm{Ta}_\ell(\widetilde{J_0}(N))$. Writing $\varphi_{p,\mathrm{Ta}} := (\varphi_{p,*})_{\mathrm{Ta}}$ we have that

$$\varphi_{p,\mathrm{Ta}}^2 - \widetilde{T}_{p,\mathrm{Ta}}\varphi_{p,\mathrm{Ta}} + p = 0$$

in $\mathrm{End}(\mathrm{Ta}_\ell(\widetilde{J_0}(N)))$.

Now by Theorem 5.4, we have an isomorphism $\pi_{\mathrm{Ta}} : \mathrm{Ta}_\ell(J_0(N)) \xrightarrow{\sim} \mathrm{Ta}_\ell(\widetilde{J_0}(N))$. Moreover, we have $\pi_{\mathrm{Ta}} \circ \mathrm{Frob}_p = \varphi_p \circ \pi_{\mathrm{Ta}}$ and $\pi_{\mathrm{Ta}} \circ T_p = \widetilde{T}_{p,\mathrm{Ta}} \circ \pi_{\mathrm{Ta}}$ (since $\widetilde{T_p}$ is the reduction of T_p modulo p), we have that

$$\mathrm{Frob}_p^2 - T_p \,\mathrm{Frob}_p + p = 0$$

in $\mathrm{End}(\mathrm{Ta}_\ell(J_0(N)))$ (where $\mathrm{Frob}_p \in \mathrm{End}(\mathrm{Ta}_\ell(J_0(N)))$ comes from the action of $G_{\mathbb{Q}}$ on $\mathrm{Ta}_\ell(J_0(N))$).

Extending coefficients to $\mathbb{Q}_\ell$, we see that this relation holds in $V_\ell(J_0(N))$. Now by Corollary 5.3 and the work of Section 5.2, we see that (for any f and $\lambda|\ell$), $V_\lambda(A_f)$ is a direct summand of $V_\ell(J_0(N))$. Thus in $V_\lambda(A_f)$ we still have

$$\rho_{f,\lambda}(\mathrm{Frob}_p)^2 - T_p\rho_{f,\lambda}(\mathrm{Frob}_p) + p = 0.$$

But now, recalling the definition of the action of K_λ on $V_\lambda(A_f)$, we see that T_p acts on $V_\lambda(A_f)$ as $a_p(f) \in K \subseteq K_\Lambda$, and so $\rho_{f,\lambda}(\mathrm{Frob}_p) \in \mathrm{GL}(V_\lambda(A_f))$ satisfies

$$\rho_{f,\lambda}(\mathrm{Frob}_p)^2 - a_p(f)\rho_{f,\lambda}(\mathrm{Frob}_p) + p = 0.$$

This implies that the minimal polynomial of $\rho_{f,\lambda}(\mathrm{Frob}_p)$ over K_λ divides $x^2 - a_p(f)x + p$. Now *provided that* $\rho_{f,\lambda}(\mathrm{Frob}_p)$ *is not a scalar*, the minimal polynomial of $\rho_{f,\lambda}(\mathrm{Frob}_p)$ has degree 2, and so its minimal polynomial, and thus its characteristic polynomial, is just $x^2 - a_p(f)x + p$.

In the unlikely event that $\rho_{f,\lambda}(\mathrm{Frob}_p)$ is a scalar (so that its minimal polynomial has degree 1), some more care must be taken. It is possible (through and argument which we will not give) to show that $\det \rho_{f,\lambda}(\mathrm{Frob}_p) = p$ independently of the above argument. This, combined with the above work, is enough to ensure that $x^2 - a_p(f)x + p$ is the minimal polynomial of $\rho_{f,\lambda}(\mathrm{Frob}_p)$. (Explicitly, if $\rho_{f,\lambda}(\mathrm{Frob}_p)$ is a scalar with determinant p, then $\rho_{f,\lambda}(\mathrm{Frob}_p) = \pm\sqrt{p}$. Since $\rho_{f,\lambda}(\mathrm{Frob}_p)$ satisfies $x^2 - a_p(f)x + p$, one of the roots of this polynomial must be $\pm\sqrt{p}$. Hence the other root is also $\frac{p}{\pm\sqrt{p}} = \pm\sqrt{p}$, and so $x^2 - a_p(f)x + p = (x \mp \sqrt{p})^2$, the characteristic polynomial of $\rho_{f,\lambda}(\mathrm{Frob}_p) = \pm\sqrt{p}$.)