CHAPTER 5

Appendix by Brian Conrad: The Shimura construction in weight 2

The purpose of this appendix is to explain the ideas of Eichler-Shimura for constructing the two-dimensional ℓ-adic representations attached to classical weight-2 Hecke eigenforms. We assume familiarity with the theory of schemes and the theory of newforms, but the essential arithmetic ideas are due to Eichler and Shimura. We warn the reader that a complete proof along the lines indicated below requires the verification of a number of compatibilities between algebraic geometry, algebraic topology, and the classical theory of modular forms. As the aim of this appendix is to explain the key arithmetic ideas of the proof, we must pass over in silence the verification of many such compatibilities. However, we at least make explicit what compatibilities we need. To prove them all here would require a serious digression from our expository goal; see [**18**, Ch. 3] for details. It is also worth noting that the form of the arguments we present is *exactly* the weight-2 version of Deligne's more general proof of related results in weight > 1, up to the canonical isomorphism

$$\mathbf{Q}_\ell \otimes_{\mathbf{Z}_\ell} \varprojlim \mathrm{Pic}^0_{X/k}[\ell^n](k) \cong H^1_{\acute{e}t}(X, \mathbf{Q}_\ell(1)) \cong H^1_{\acute{e}t,c}(Y, \mathbf{Q}_\ell(1))$$

for a proper smooth connected curve X over a separably closed field k of characteristic prime to ℓ, and Y a dense open in X. Using ℓ-adic Tate modules allows us to bypass the general theory of étale cohomology which arises in the case of higher weight.

5.1. Analytic preparations

Fix $i = \sqrt{-1} \in \mathbf{C}$ for all time. Fix an integer $N \geq 5$ and let $X_1(N)^{\mathrm{an}}$ denote the classical analytic modular curve, the "canonical" compactification of $Y_1(N)^{\mathrm{an}} = \Gamma_1(N)\backslash\mathfrak{h}$, where $\mathfrak{h} = \{z \in \mathbf{C} : \mathrm{Im}\, z > 0\}$ and $\Gamma_1(N) \subset \mathrm{SL}_2(\mathbf{Z})$ acts on the left via linear fractional transformations. The classical theory identifies the $\mathbf{C}$-vector space $H^0(X_1(N)^{\mathrm{an}}, \Omega^1_{X_1(N)^{\mathrm{an}}})$ with $S_2(\Gamma_1(N), \mathbf{C})$, the space of weight-2 cusp forms. Note that the classical Riemann surface $X_1(N)^{\mathrm{an}}$ has genus 0 if we consider $N < 5$, while $S_2(\Gamma_1(N), \mathbf{C}) = 0$ if $N < 5$. Thus, assuming $N \geq 5$ is harmless for what we will do.

The Hodge decomposition for the compact Riemann surface $X_1(N)^{\mathrm{an}}$ supplies us with an isomorphism of $\mathbf{C}$-vector spaces

$$\begin{aligned}
&S_2(\Gamma_1(N),\mathbf{C})\oplus\overline{S_2(\Gamma_1(N),\mathbf{C})}\\
&\qquad\qquad\cong H^0(X_1(N)^{\mathrm{an}},\Omega^1_{X_1(N)^{\mathrm{an}}})\oplus H^0(X_1(N)^{\mathrm{an}},\overline{\Omega}^1_{X_1(N)^{\mathrm{an}}})\\
&\qquad\qquad\xrightarrow{\sim} H^1(X_1(N)^{\mathrm{an}},\underline{\mathbf{C}})\\
&\qquad\qquad\cong H^1(X_1(N)^{\mathrm{an}},\underline{\mathbf{Z}})\otimes_{\mathbf{Z}}\mathbf{C}
\end{aligned}$$

(where $\underline{A}$ denotes the constant sheaf attached to an abelian group A). This will be called the (weight-2) *Shimura isomorphism*. We want to define "geometric" operations on $H^1(X_1(N)^{\mathrm{an}},\underline{\mathbf{Z}})$ which recover the classical Hecke operators on $S_2(\Gamma_1(N),\mathbf{C})$ via the above isomorphism.

The "geometric" (or rather, cohomological) operations we wish to define can be described in two ways. First, we can use explicit matrices and explicit "upper-half plane" models of modular curves. This has the advantage of being concrete, but it provides little conceptual insight and encourages messy matrix calculations. The other point of view is to identify the classical modular curves as the base of certain universal analytic families of (generalized) elliptic curves with level structure. A proper discussion of this latter point of view would take us too far afield, so we will have to settle for only some brief indications along these two lines (though this is how to best verify compatibility with the algebraic theory via schemes).

Choose a matrix $\gamma_n\in\mathrm{SL}_2(\mathbf{Z})$ with $\gamma_n\equiv\begin{pmatrix}n^{-1}&*\\0&n\end{pmatrix}\pmod N$, for $n\in(\mathbf{Z}/N\mathbf{Z})^*$. The action of γ_n on $\mathfrak{h}$ induces an action on $Y_1(N)^{\mathrm{an}}$ and even on $X_1(N)^{\mathrm{an}}$. Associating to each $z\in\mathfrak{h}$ the data of the elliptic curve $\mathbf{C}/[1,z]=\mathbf{C}/(\mathbf{Z}+\mathbf{Z}z)$ and the point $1/N$ of exact order N, we may identify $Y_1(N)^{\mathrm{an}}$ as a *set* with the set of isomorphism classes of pairs (E,P) consisting of an elliptic curve E over $\mathbf{C}$ and a point $P\in E$ of exact order N. The map $Y_1(N)^{\mathrm{an}}\to Y_1(N)^{\mathrm{an}}$ induced by γ_n can then described on the underlying set by $(E,P)\mapsto(E,nP)$, so it is "intrinsic", depending only on $n\in(\mathbf{Z}/N\mathbf{Z})^*$. We denote by $I_n:X_1(N)^{\mathrm{an}}\to X_1(N)^{\mathrm{an}}$ the induced map on $X_1(N)^{\mathrm{an}}$. Once this data (E,P) is formulated in a relative context over an analytic base, we could define the analytic map I_n conceptually, without using the matrix γ_n. We ignore this point here.

The map $z\mapsto\frac{-1}{Nz}$ on $\mathfrak{h}$ induces a map $Y_1(N)^{\mathrm{an}}\to Y_1(N)^{\mathrm{an}}$ which extends to $w_N:X_1(N)^{\mathrm{an}}\to X_1(N)^{\mathrm{an}}$. More conceptually and more generally, if $\zeta\in\mu_N(\mathbf{C})$ is a primitive Nth root of unity, consider the rule w_ζ that sends $(E,P)\in Y_1(N)^{\mathrm{an}}$ to $(E/P,P'\bmod P)$, where $P'\in E$ has exact order N and $\langle P,P'\rangle_N=\zeta$, with $\langle\,,\rangle_N$ the Weil pairing on N-torsion points (following the sign conventions of [**62, 77**]; opposite the convention of [**109**]). More specifically, on $\mathbf{C}/[1,z]$ we have $\langle\frac{1}{N},\frac{z}{N}\rangle_N=e^{2\pi i/N}$. The map w_ζ extends to an analytic map $X_1(N)^{\mathrm{an}}\to X_1(N)^{\mathrm{an}}$. When $\zeta=e^{2\pi i/N}$, we have $w_\zeta=w_N$ due to the above sign convention.

We have induced pullback maps

$$w_\zeta^*,I_n^*:H^1(X_1(N)^{\mathrm{an}},\underline{\mathbf{Z}})\to H^1(X_1(N)^{\mathrm{an}},\underline{\mathbf{Z}}).$$

We write $\langle n\rangle^*$ rather than I_n^*.

Finally, choose a prime p. Define $\Gamma_1(N,p)\subset\mathrm{SL}_2(\mathbf{Z})$ to be $\Gamma_1(N,p)=\Gamma_1(N)\cap\Gamma_0(p)$ when $p\nmid N$ and $\Gamma_1(N,p)=\Gamma_1(N)\cap\Gamma_0(p)^t$ when $p\mid N$, where the group $\Gamma_0(p)^t$ is the transpose of $\Gamma_0(p)$. Define $Y_1(N,p)^{\mathrm{an}}=\Gamma_1(N,p)\backslash\mathfrak{h}$ and let $X_1(N,p)^{\mathrm{an}}$ be its "canonical" compactification. Using the assignment

$$z\mapsto(\mathbf{C}/[1,z],\frac{1}{N},\langle\frac{1}{p}\rangle)$$

when $p \nmid N$ and

$$z \mapsto (\mathbf{C}/[1,z], \frac{1}{N}, \langle \frac{z}{p} \rangle)$$

when $p \mid N$, we may identify the *set* $Y_1(N,p)^{\mathrm{an}}$ with the set of isomorphism classes of triples (E,P,C) where $P \in E$ has exact order N and $C \subset E$ is a cyclic subgroup of order p, meeting $\langle P \rangle$ trivially (a constraint if $p \mid N$). Here and below, we denote by $\langle P \rangle$ the (cyclic) subgroup generated by P.

There are unique analytic maps

$$\pi_1^{(p)}, \pi_2^{(p)} : X_1(N,p)^{\mathrm{an}} \to X_1(N)^{\mathrm{an}}$$

determined on $Y_1(N,p)^{\mathrm{an}}$ by

$$\pi_1^{(p)}(E,P,C) = (E,P)$$

and

$$\pi_2^{(p)}(E,P,C) = (E/C, P \bmod C).$$

For example, $\pi_1^{(p)}$ is induced by $z \mapsto z$ on $\mathfrak{h}$, in terms of the above upper half plane uniformization of $Y_1(N)^{\mathrm{an}}$ and $Y_1(N,p)^{\mathrm{an}}$.

We define

$$T_p^* = (\pi_1^{(p)})_* \circ (\pi_2^{(p)})^* : H^1(X_1(N)^{\mathrm{an}}, \underline{\mathbf{Z}}) \to H^1(X_1(N)^{\mathrm{an}}, \underline{\mathbf{Z}})$$

where $(\pi_1^{(p)})_* : H^1(X_1(N,p)^{\mathrm{an}}, \underline{\mathbf{Z}}) \to H^1(X_1(N)^{\mathrm{an}}, \underline{\mathbf{Z}})$ is the canonical trace map associated to the finite map $\pi_1^{(p)}$ of compact Riemann surfaces. More specifically, we have a canonical isomorphism

$$H^1(X_1(N,p)^{\mathrm{an}}, \underline{\mathbf{Z}}) \cong H^1(X_1(N)^{\mathrm{an}}, (\pi_1^{(p)})_* \underline{\mathbf{Z}})$$

since $(\pi_1^{(p)})_*$ is exact on abelian sheaves, and there is a unique trace map of sheaves $(\pi_1^{(p)})_* \underline{\mathbf{Z}} \to \underline{\mathbf{Z}}$ determined on stalks at $x \in X_1(N)^{\mathrm{an}}$ by

$$\begin{aligned} \prod_{\pi_1^{(p)}(y)=x} \mathbf{Z} &\to \mathbf{Z} \\ (a_y) &\mapsto \Sigma_y e_y a_y \end{aligned} \tag{5.1}$$

where e_y is the ramification degree of y over x via $\pi_1^{(p)}$.

A fundamental compatibility, whose proof we omit for reasons of space, is:

Theorem 5.1. *The weight-*2 *Shimura isomorphism*

$$\mathrm{Sh}_{\Gamma_1(N)} : S_2(\Gamma_1(N), \mathbf{C}) \oplus \overline{S_2(\Gamma_1(N), \mathbf{C})} \cong H^1(X_1(N)^{\mathrm{an}}, \underline{\mathbf{Z}}) \otimes_{\mathbf{Z}} \mathbf{C}$$

from (5.1) *identifies* $\langle n \rangle \oplus \overline{\langle n \rangle}$ *with* $\langle n \rangle^* \otimes 1$, $T_p \oplus \overline{T}_p$ *with* $T_p^* \otimes 1$, *and* $w_N \oplus \overline{w}_N$ *with* $w^*_{e^{2\pi i/N}} \otimes 1$.

Let $\mathbf{T}_1(N) \subset \mathrm{End}_{\mathbf{Z}}(H^1(X_1(N)^{\mathrm{an}}, \underline{\mathbf{Z}}))$ be the subring generated by the T_p^*'s and $\langle n \rangle^*$'s. By Theorem 5.1, this is identified via the Shimura isomorphism with the classical (weight-2) Hecke ring at level N. In particular, this ring is commutative (which can be seen directly via cohomological considerations as well). It is clearly a finite flat $\mathbf{Z}$-algebra.

The natural map

$$\mathbf{T}_1(N) \otimes_{\mathbf{Z}} \mathbf{C} \hookrightarrow \mathrm{End}_{\mathbf{C}}(H^1(X_1(N)^{\mathrm{an}}, \underline{\mathbf{Z}}) \otimes_{\mathbf{Z}} \mathbf{C}) \tag{5.2}$$

induces an *injection* $\mathbf{T}_1(N)\otimes\mathbf{C}\hookrightarrow \mathrm{End}_{\mathbf{C}}(S_2(\Gamma_1(N),\mathbf{C}))$, by Theorem 5.1. This is the classical realization of Hecke operators in weight 2.

Another compatibility we need is between the cup product on $H^1(X_1(N)^{\mathrm{an}},\underline{\mathbf{Z}})$ and the (non-normalized) Petersson product on $S_2(\Gamma_1(N),\mathbf{C})$. To be precise, we define an isomorphism $H^2(X_1(N)^{\mathrm{an}},\underline{\mathbf{Z}})\simeq\mathbf{Z}$ using the i-orientation of the complex manifold $X_1(N)^{\mathrm{an}}$ (i.e., the "$i\mathrm{d}z\wedge\mathrm{d}\overline{z}$" orientation), so we get via cup product a (perfect) pairing

$$(\,,\,)_{\Gamma_1(N)}:H^1(X_1(N)^{\mathrm{an}},\underline{\mathbf{Z}})\otimes_{\mathbf{Z}}H^1(X_1(N)^{\mathrm{an}},\underline{\mathbf{Z}})\to H^2(X_1(N)^{\mathrm{an}},\underline{\mathbf{Z}})\simeq\mathbf{Z}.$$

This induces an analogous pairing after applying $\otimes_{\mathbf{Z}}\mathbf{C}$. For $f,g\in S_2(\Gamma_1(N),\mathbf{C})$ we define

$$\langle f,g\rangle_{\Gamma_1(N)}=\int_{\Gamma_1(N)\backslash\mathfrak{h}} f(z)\overline{g}(z)\mathrm{d}x\mathrm{d}y$$

where this integral is absolutely convergent since f and g have exponential decay near the cusps. This is a perfect Hermitian pairing.

Theorem 5.2. *Under the weight-*2 *Shimura isomorphism* $\mathrm{Sh}_{\Gamma_1(N)}$,

$$\left(\mathrm{Sh}_{\Gamma_1(N)}(f_1+\overline{g}_1),\mathrm{Sh}_{\Gamma_1(N)}(f_2+\overline{g}_2)\right)_{\Gamma_1(N)}=4\pi\cdot(\langle f_1,g_2\rangle_{\Gamma_1(N)}-\langle f_2,g_1\rangle_{\Gamma_1(N)}).$$

Note that *both* sides are antilinear in g_1, g_2 and alternating with respect to interchanging the pair (f_1,g_1) and (f_2,g_2). The extra factor of 4π is harmless for our purposes since it does not affect formation of adjoints. What is important is that in the classical theory, conjugation by the involution w_N takes each $T\in\mathbf{T}_1(N)$ to its adjoint with respect to the Petersson product. The most subtle case of this is $T=T_p^*$ for $p\mid N$. For $p\nmid N$ the adjoint of T_p^* is $\langle p^{-1}\rangle^*T_p^*$ and the adjoint of $\langle n\rangle^*$ is $\langle n^{-1}\rangle^*$. These classical facts (especially for T_p^* with $p\mid N$) yield the following important corollary of Theorem 5.2.

Corollary 5.3. *With respect to the pairing* $[x,y]_{\Gamma_1(N)}=(x,w_\zeta^*y)_{\Gamma_1(N)}$ *with* $\zeta=e^{2\pi i/N}$, *the action of* $\mathbf{T}_1(N)$ *on* $H^1(X_1(N)^{\mathrm{an}},\underline{\mathbf{Z}})$ *is equivariant. That is,*

$$[x,Ty]_{\Gamma_1(N)}=[Tx,y]_{\Gamma_1(N)}$$

for all $T\in\mathbf{T}_1(N)$. *With respect to* $(\,,\,)_{\Gamma_1(N)}$, *the adjoint of* T_p^* *for* $p\nmid N$ *is* $\langle p^{-1}\rangle^*T_p^*$ *and the adjoint of* $\langle n\rangle^*$ *is* $\langle n^{-1}\rangle^*$ *for* $n\in(\mathbf{Z}/N\mathbf{Z})^*$.

Looking back at the "conceptual" definition of w_ζ^* for an arbitrary primitive Nth root of unity $\zeta\in\mu_N(\mathbf{C})$, which gives an analytic involution of $X_1(N)^{\mathrm{an}}$, one can check that $w_{\zeta^j}^*\circ w_\zeta^*=\langle j\rangle^*$ for $j\in(\mathbf{Z}/N\mathbf{Z})^*$. Since $\langle j\rangle^*$ is a unit in $\mathbf{T}_1(N)$ and $\mathbf{T}_1(N)$ is *commutative*, we conclude that Corollary 5.3 is true with $\zeta\in\mu_N(\mathbf{C})$ *any* primitive Nth root of unity (by reduction to the case $\zeta=e^{2\pi i/N}$).

Our final step on the analytic side is to reformulate everything above in terms of Jacobians. For any compact Riemann surface X, there is an isomorphism of complex Lie groups

$$\mathrm{Pic}_X^0\simeq H^1(X,\mathcal{O}_X)/H^1(X,\underline{\mathbf{Z}}) \tag{5.3}$$

via the exponential sequence

$$0\to\underline{\mathbf{Z}}\to\mathcal{O}_X\xrightarrow{e^{2\pi i(\cdot)}}\mathcal{O}_X^*\to 1$$

and the identification of the underlying group of Pic_X^0 with

$$H^1(X,\mathcal{O}_X^*)\simeq\check{H}^1(X,\mathcal{O}_X^*),$$

where the line bundle $\mathcal{L}$ with trivializations $\varphi_i : \mathcal{O}_{U_i} \cong \mathcal{L}|U_i$ corresponds to the class of the Čech 1-cocycle

$$\{\varphi_j^{-1} \circ \varphi_i : \mathcal{O}_{U_i \cap U_j} \cong \mathcal{O}_{U_i \cap U_j}\} \in \prod_{i<j} H^0(U_i \cap U_j, \mathcal{O}_X^*)$$

for an ordered open cover $\{U_i\}$. Beware that the tangent space isomorphism

$$T_0(\mathrm{Pic}_X^0) \cong H^1(X, \mathcal{O}_X)$$

coming from (5.3) is $-2\pi i$ times the "algebraic" isomorphism arising from

$$0 \to \mathcal{O}_X \to \mathcal{O}_{X[\varepsilon]}^* \to \mathcal{O}_X^* \to 1,$$

where $X[\varepsilon] = (X, \mathcal{O}_X[\varepsilon]/\varepsilon^2)$ is the non-reduced space of "dual numbers over X". This extra factor of $-2\pi i$ will not cause problems. We will use (5.3) to "compute" with Jacobians.

Let $f : X \to Y$ be a finite map between compact Riemann surfaces. Since f is finite flat, there is a natural trace map $f_*\mathcal{O}_X \to \mathcal{O}_Y$, and it is not difficult to check that this is compatible with the trace map $f_*\underline{\mathbf{Z}} \to \underline{\mathbf{Z}}$ as defined in (5.1). In particular, we have a trace map

$$f_* : H^1(X, \mathcal{O}_X) \cong H^1(Y, f_*\mathcal{O}_X) \to H^1(Y, \mathcal{O}_Y).$$

Likewise, we have compatible pullback maps $f^*\mathcal{O}_Y \cong \mathcal{O}_X$ and $f^*\underline{\mathbf{Z}} \cong \underline{\mathbf{Z}}$.

Thus, any such f gives rise to *commutative* diagrams

$$\begin{tikzcd}
H^1(Y, \mathcal{O}_Y) \arrow[r, "f^*"] & H^1(X, \mathcal{O}_X) & H^1(X, \mathcal{O}_X) \arrow[r, "f_*"] & H^1(Y, \mathcal{O}_Y) \\
H^1(Y, \underline{\mathbf{Z}}) \arrow[r, "f^*"] \arrow[u] & H^1(X, \underline{\mathbf{Z}}) \arrow[u] & H^1(X, \underline{\mathbf{Z}}) \arrow[r, "f_*"] \arrow[u] & H^1(Y, \underline{\mathbf{Z}}) \arrow[u],
\end{tikzcd}$$

where the columns are induced by the canonical maps $\underline{\mathbf{Z}} \to \mathcal{O}_Y$ and $\underline{\mathbf{Z}} \to \mathcal{O}_X$. Passing to quotients on the columns therefore gives rise to maps

$$f^* : \mathrm{Pic}_Y^0 \to \mathrm{Pic}_X^0, \qquad f_* : \mathrm{Pic}_X^0 \to \mathrm{Pic}_Y^0$$

of analytic Lie groups. These maps are "computed" by

Lemma 5.4. *In the above situation, $f^* = \mathrm{Pic}^0(f)$ is the map induced by Pic^0 functoriality and $f_* = \mathrm{Alb}(f)$ is the map induced by Albanese functoriality. These are dual with respect to the canonical autodualities of Pic_X^0, Pic_Y^0.*

The significance of the theory of Jacobians is that by (5.3) we have a canonical isomorphism

$$(5.4) \qquad \begin{aligned} T_\ell(\mathrm{Pic}^0_{X_1(N)^{\mathrm{an}}}) &\cong H^1(X_1(N)^{\mathrm{an}}, \underline{\mathbf{Z}}_\ell) \\ &\cong H^1(X_1(N)^{\mathrm{an}}, \underline{\mathbf{Z}}) \otimes_{\mathbf{Z}} \mathbf{Z}_\ell, \end{aligned}$$

connecting the ℓ-adic Tate module of $\mathrm{Pic}^0_{X_1(N)}$ with the $\mathbf{Z}$-module $H^1(X_1(N)^{\mathrm{an}}, \underline{\mathbf{Z}})$ that "encodes" $S_2(\Gamma_1(N), \mathbf{C})$ via the Shimura isomorphism. Note that this isomorphism is defined in terms of the analytic construction (5.3) which depends upon the choice of i. The intrinsic isomorphism (compatible with étale cohomology) has $\mathbf{Z}$ above replaced by $2\pi i\mathbf{Z} = -2\pi i\mathbf{Z}$.

Definition 5.5. We define endomorphisms of $\mathrm{Pic}^0_{X_1(N)^{\mathrm{an}}}$ via

$$T_p^* = \mathrm{Alb}(\pi_1^{(p)}) \circ \mathrm{Pic}^0(\pi_2^{(p)}), \quad \langle n \rangle^* = \mathrm{Pic}^0(I_n), \quad w_\zeta^* = \mathrm{Pic}^0(w_\zeta).$$

By Lemma 5.4, it follows that the above isomorphism (5.4) carries the operators on $T_\ell(\mathrm{Pic}^0_{X_1(N)^{\mathrm{an}}})$ over to the ones *previously defined* on $H^1(X_1(N)^{\mathrm{an}}, \underline{\mathbf{Z}})$ (which are, in turn, compatible with the classical operations via the Shimura isomorphism). By the faithfulness of the "Tate module" functor on complex tori, we conclude that $\mathbf{T}_1(N)$ *acts* on $\mathrm{Pic}^0_{X_1(N)^{\mathrm{an}}}$ in a unique manner compatible with the above definition, and (5.4) is an isomorphism of $\mathbf{T}_1(N) \otimes_{\mathbf{Z}} \mathbf{Z}_\ell$-modules. We call this the $(\,)^*$*-action* of $\mathbf{T}_1(N)$ on $\mathrm{Pic}^0_{X_1(N)^{\mathrm{an}}}$.

We must warn the reader that under the canonical isomorphism of $\mathbf{C}$-vector spaces

$$\begin{aligned} S_2(\Gamma_1(N), \mathbf{C}) &\cong H^0(X_1(N)^{\mathrm{an}}, \Omega^1_{X_1(N)^{\mathrm{an}}}) \\ &\cong H^0(\mathrm{Pic}^0_{X_1(N)^{\mathrm{an}}}, \Omega^1_{\mathrm{Pic}^0_{X_1(N)^{\mathrm{an}}}}) \\ &\cong \mathrm{Cot}_0(\mathrm{Pic}^0_{X_1(N)^{\mathrm{an}}}), \end{aligned}$$

the $(\,)^*$-action of $T \in \mathbf{T}_1(N)$ on $\mathrm{Pic}^0_{X_1(N)^{\mathrm{an}}}$ does *not* go over to the classical action of T on $S_2(\Gamma_1(N), \mathbf{C})$, but rather the adjoint of T with respect to the Petersson pairing. To clear up this matter, we make the following definition:

Definition 5.6.

$$(T_p)_* = \mathrm{Alb}(\pi_2^{(p)}) \circ \mathrm{Pic}^0(\pi_1^{(p)}), \quad \langle n \rangle_* = \mathrm{Alb}(I_n), \quad (w_\zeta)_* = \mathrm{Alb}(w_\zeta).$$

Since $I_n^{-1} = I_{n^{-1}}$ and $w_\zeta^{-1} = w_\zeta$ on $X_1(N)^{\mathrm{an}}$, we have $(w_\zeta)_* = w_\zeta^*$ and $\langle n \rangle_* = \langle n^{-1} \rangle^*$. We claim that the above $(\,)_*$ operators are the *dual* morphisms (with respect to the canonical principal polarization of $\mathrm{Pic}^0_{X_1(N)^{\mathrm{an}}}$) of the $(\,)^*$ operators and induce exactly the *classical* action of T_p and $\langle n \rangle$ on $S_2(\Gamma_1(N), \mathbf{C})$, so we also have a well-defined $(\,)_*$-action of $\mathbf{T}_1(N)$ on $\mathrm{Pic}^0_{X_1(N)^{\mathrm{an}}}$, dual to the $(\,)^*$-action. By Theorem 5.2, Corollary 5.3, and Lemma 5.4, this follows from the following general fact about compact Riemann surfaces. The proof is non-trivial.

Lemma 5.7. *Let X be a compact Riemann surface, and use the i-orientation to define $H^2(X, \underline{\mathbf{Z}}) \cong \mathbf{Z}$. Use $1 \mapsto e^{2\pi i/\ell^n}$ to define $\mathbf{Z}/\ell^n \cong \mu_{\ell^n}(\mathbf{C})$ for all n. The diagram*

$$\begin{tikzcd} H^1(X, \underline{\mathbf{Z}_\ell}) \otimes_{\mathbf{Z}_\ell} H^1(X, \underline{\mathbf{Z}_\ell}) \arrow[r, "\cup"] \arrow[d, "\cong"] & \mathbf{Z}_\ell \arrow[d, "\cong"] \\ T_\ell(\mathrm{Pic}^0_X) \otimes_{\mathbf{Z}_\ell} T_\ell(\mathrm{Pic}^0_X) \arrow[r] & \varprojlim \mu_{\ell^n}(\mathbf{C}) \end{tikzcd}$$

anticommutes (i.e., going around from upper left to lower right in the two possible ways gives results that are negatives of each other), where the bottom row is the ℓ-adic Weil pairing (with respect to the canonical principal polarization $\mathrm{Pic}^0_X \cong \widehat{\mathrm{Pic}^0_X}$ for the "second" Pic^0_X in the lower left.)

Note that the sign doesn't affect formation of adjoints. It ultimately comes from the sign on the bottom of [**77**, pg. 237] since our Weil pairing sign convention agrees with [**77**].

We now summarize our findings in terms of $V_\ell(N) = \mathbf{Q}_\ell \otimes_{\mathbf{Z}_\ell} T_\ell(\mathrm{Pic}^0_{X_1(N)^{\mathrm{an}}})$, which has a perfect alternating Weil pairing

$$(\,,\,)_\ell : V_\ell(N) \otimes V_\ell(N) \to \mathbf{Q}_\ell(1)$$

and has two $\mathbf{Q}_\ell \otimes \mathbf{T}_1(N)$-actions, via the $(\,)^*$-actions and the $(\,)_*$-actions. Since $(w_\zeta)_* = w_\zeta^*$, we simply write w_ζ for this operator on $V_\ell(N)$.

Theorem 5.8. *Let $\mathbf{T}_1(N)$ act on $V_\ell(N)$ with respect to the $(\,)^*$-action or with respect to the $(\,)_*$-action. With respect to $(\,,\,)_\ell$, the adjoint of T_p for $p \nmid N$ is $\langle p\rangle^{-1}T_p$ and the adjoint of $\langle n\rangle$ is $\langle n\rangle^{-1}$ for $n \in (\mathbf{Z}/N\mathbf{Z})^*$. With respect to*

$$[x,y]_\ell = (x, w_\zeta(y))_\ell$$

for $\zeta \in \mu_N(\mathbf{C})$ a primitive Nth root of unity, the action of $\mathbf{T}_1(N)$ on $V_\ell(N)$ is self-adjoint. In general, adjointness with respect to $(\,,\,)_\ell$ interchanges the $(\,)_*$-action and $(\,)^*$-action.

It should be noted that when making the translation to étale cohomology, the $(\,)^*$-action plays a more prominent role (since this is what makes (5.4) a $\mathbf{T}_1(N)$-equivariant map). However, when working directly with Tate modules and arithmetic Frobenius elements, it is the $(\,)_*$-action which gives the cleaner formulation of Shimura's results.

An important consequence of Theorem 5.8 is

Corollary 5.9. *The $\mathbf{Q}_\ell \otimes_{\mathbf{Z}} \mathbf{T}_1(N)$-module $V_\ell(N)$ is free of rank* 2 *for either action, and* $\mathrm{Hom}_{\mathbf{Q}}(\mathbf{Q}\otimes\mathbf{T}_1(N),\mathbf{Q})$ *is free of rank* 1 *over* $\mathbf{Q}\otimes\mathbf{T}_1(N)$ (*hence likewise with* $\mathbf{Q}$ *replaced by any field of characteristic* 0).

Remark 5.10. The assertion about $\mathrm{Hom}_{\mathbf{Q}}(\mathbf{Q}\otimes\mathbf{T}_1(N),\mathbf{Q})$ is equivalent to the intrinsic condition that $\mathbf{Q}\otimes\mathbf{T}_1(N)$ is *Gorenstein*. Also, this freeness clearly makes the two assertions about $V_\ell(N)$ for the $(\,)_*$- and $(\,)^*$-actions *e*quivalent. *For the proof,* the $(\,)^*$-action is what we use. But in what follows, it is the case of the $(\,)_*$-action that we need!

Proof. Using (5.4) and the choice of $(\,)^*$-action on $V_\ell(N)$, it suffices to prove

- $H^1(X_1(N)^{\mathrm{an}},\underline{\mathbf{Q}})$ is free of rank 2 over $\mathbf{Q}\otimes\mathbf{T}_1(N)$,
- $\mathrm{Hom}_{\mathbf{Q}}(\mathbf{Q}\otimes\mathbf{T}_1(N),\mathbf{Q})$ is free of rank 1 over $\mathbf{Q}\otimes\mathbf{T}_1(N)$.

Using $[\,,\,]_{\Gamma_1(N)}$, we have

$$H^1(X_1(N)^{\mathrm{an}},\underline{\mathbf{Q}}) \cong \mathrm{Hom}_{\mathbf{Q}}(H^1(X_1(N)^{\mathrm{an}},\underline{\mathbf{Q}}),\mathbf{Q}) \tag{5.5}$$

as $\mathbf{Q}\otimes\mathbf{T}_1(N)$-modules, so we may study this $\mathbf{Q}$-dual instead. Since $\mathbf{Q}\otimes\mathbf{T}_1(N)$ is semilocal, a finite module over this ring is locally free of constant rank if and only if it is *free* of that rank. But local freeness of constant rank can be checked after faithfully flat base change. Applying this with the base change $\mathbf{Q}\to\mathbf{C}$, and noting that $\mathbf{C}\otimes\mathbf{T}_1(N)$ is semilocal, it suffices to replace $\mathbf{Q}$ by $\mathbf{C}$ above.

Note that *if* the right hand side of (5.5) is free of rank 2, so is the left side, so choosing a basis of the left side and feeding it into the right hand side shows that $\mathrm{Hom}_{\mathbf{Q}}(\mathbf{Q}\otimes\mathbf{T}_1(N)^{\oplus 2},\mathbf{Q})$ is free of rank 2. In particular, the direct summand $\mathrm{Hom}_{\mathbf{Q}}(\mathbf{Q}\otimes\mathbf{T}_1(N),\mathbf{Q})$ is flat over $\mathbf{Q}\otimes\mathbf{T}_1(N)$ with full support over $\mathrm{Spec}(\mathbf{Q}\otimes\mathbf{T}_1(N))$, so it must be locally free with local rank at least 1 at all points of $\mathrm{Spec}(\mathbf{Q}\otimes\mathbf{T}_1(N))$. Consideration of $\mathbf{Q}$-dimensions then forces $\mathrm{Hom}_{\mathbf{Q}}(\mathbf{Q}\otimes\mathbf{T}_1(N),\mathbf{Q})$ to be locally free of rank 1, hence free of rank 1. In other words, it suffices to show that $\mathrm{Hom}_{\mathbf{Q}}(H^1(X_1(N)^{\mathrm{an}},\underline{\mathbf{Q}}),\mathbf{Q})$ is free of rank 2 over $\mathbf{T}_1(N)\otimes\mathbf{Q}$, or equivalently that $\mathrm{Hom}_{\mathbf{C}}(H^1(X_1(N)^{\mathrm{an}},\underline{\mathbf{C}}),\mathbf{C})$ is free of rank 2 over $\mathbf{T}_1(N)\otimes\mathbf{C}$.

Via the Shimura isomorphism (in weight 2), which is compatible with the Hecke actions, we are reduced to showing that $\mathrm{Hom}(S_2(\Gamma_1(N),\mathbf{C}),\mathbf{C})$ is free of rank 1 over $\mathbf{C}\otimes\mathbf{T}_1(N)$. For this purpose, we will study the $\mathbf{C}\otimes\mathbf{T}_1(N)$-equivariant $\mathbf{C}$-bilinear pairing

$$S_2(\Gamma_1(N),\mathbf{C})\otimes_{\mathbf{C}}(\mathbf{C}\otimes\mathbf{T}_1(N)) \to \mathbf{C}$$

$$(f,T)\mapsto a_1(Tf)$$

were $a_1(\cdot)$ is the "Fourier coefficient of q". This is $\mathbf{C}\otimes\mathbf{T}_1(N)$-equivariant, since $\mathbf{T}_1(N)$ is commutative. It suffices to check that there's no nonzero kernel on either side of this pairing. Since

$$\mathbf{C}\otimes\mathbf{T}_1(N)\to \mathrm{End}_{\mathbf{C}}(S_2(\Gamma_1(N),\mathbf{C}))$$

is *injective* (as noted in (5.2)) and $a_1(TT_nf)=a_n(Tf)$ for $T\in\mathbf{T}_1(N)$, the kernel on the right is trivial. Since $a_1(T_nf)=a_n(f)$, the kernel on the left is also trivial. □

5.2. Algebraic preliminaries

Let S be a scheme. An *elliptic curve* $E\to S$ is a proper smooth group scheme with geometrically connected fibers of dimension 1 (necessarily of genus 1). It follows from [**62**, Ch.2] that the group structure is commutative and uniquely determined by the identity section. Fix $N\geq 1$ and assume $N\in H^0(S,\mathcal{O}_S^*)$ (i.e., S is a $\mathbf{Z}[\frac{1}{N}]$-scheme). Thus, the map $N:E\to E$ is finite *étale* of degree N^2 as can be checked on geometric fibers. A *point of exact order N* on E is a section $P:S\to E$ which is killed by N (i.e., factors through the finite étale group scheme $E[N]$) and induces a point of exact order N on geometric fibers.

It follows from the stack-theoretic methods in [**25**] or the more explicit descent arguments in [**62**] that for $N\geq 5$ there is a proper smooth $\mathbf{Z}[\frac{1}{N}]$-scheme $X_1(N)$ equipped with a finite flat map to $\mathbf{P}^1_{\mathbf{Z}[\frac{1}{N}]}$, such that the open subscheme $Y_1(N)$ lying over $\mathbf{P}^1_{\mathbf{Z}[\frac{1}{N}]}-\{\infty\}=\mathbf{A}^1_{\mathbf{Z}[\frac{1}{N}]}$ is the base of a universal object $(E_1(N),P)\to Y_1(N)$ for elliptic curves with a point of exact order N over variable $\mathbf{Z}[\frac{1}{N}]$-schemes.

Moreover, the fibers of $X_1(N)\to\mathrm{Spec}\,\mathbf{Z}[\frac{1}{N}]$ are *geometrically connected*, as this can be checked on a single geometric fiber and by choosing the complex fiber we may appeal to the fact (whose proof requires some care) that there is an isomorphism $(X_1(N)\times_{\mathbf{Z}[\frac{1}{N}]}\mathbf{C})^{\mathrm{an}}\cong X_1(N)^{\mathrm{an}}$ identifying the "algebraic" data $(\mathbf{C}/[1,z],\frac{1}{N})$ in $Y_1(N)(\mathbf{C})\subset X_1(N)(\mathbf{C})$ with the class of $z\in\mathfrak{h}$ in $\Gamma_1(N)\backslash\mathfrak{h}=Y_1(N)^{\mathrm{an}}\subset X_1(N)^{\mathrm{an}}$ (and $X_1(N)^{\mathrm{an}}$ *is* connected, as $\mathfrak{h}$ is). These kinds of compatibilities are somewhat painful to check unless one develops a full-blown relative theory of elliptic curves in the analytic world (in which case the verifications become quite mechanical and natural).

Again fixing $N\geq 5$, but now also a prime p, we want an algebraic analogue of $X_1(N,p)^{\mathrm{an}}$ over $\mathbf{Z}[\frac{1}{Np}]$. Let $(E,P)\to S$ be an elliptic curve with a point of exact order N over a $\mathbf{Z}[\frac{1}{Np}]$-scheme S. We're interested in studying triples $(E,P,C)\to S$ where $C\subset E$ is an order-p finite locally free S-subgroup-scheme which is not contained in the subgroup generated by P on geometric fibers (if $p\mid N$). Methods in [**25**] and [**62**] ensure the existence of a universal such object $(E_1(N,p),P,C)\to Y_1(N,p)$ for a smooth affine $\mathbf{Z}[\frac{1}{Np}]$-scheme which naturally sits as the complement of a relative Cartier divisor in a proper smooth $\mathbf{Z}[\frac{1}{Np}]$-scheme $X_1(N,p)$ which is finite flat over $\mathbf{P}^1_{\mathbf{Z}[\frac{1}{Np}]}$ (with $Y_1(N,p)$ the preimage of $\mathbf{A}^1_{\mathbf{Z}[\frac{1}{Np}]}$). Base change to $\mathbf{C}$ and analytification recovers $X_1(N,p)^{\mathrm{an}}$ as before, so $X_1(N,p)\to\mathrm{Spec}\,\mathbf{Z}[\frac{1}{Np}]$ has geometrically connected fibers.

There are maps of $\mathbf{Z}[\frac{1}{Np}]$-schemes (respectively, $\mathbf{Z}[\frac{1}{N}]$-schemes)

$$\begin{tikzcd}
& Y_1(N,p) \arrow[dl, "\pi_1^{(p)}"'] \arrow[dr, "\pi_2^{(p)}"] & & Y_1(N) \arrow[r, "I_n"] & Y_1(N) \\
Y_1(N)[\frac{1}{p}] & & Y_1(N)[\frac{1}{p}] & &
\end{tikzcd}$$

determined by $(E,P,C) \xrightarrow{\pi_1^{(p)}} (E,P)$ and $(E,P,C) \xrightarrow{\pi_2^{(p)}} (E/C,P)$ (which makes sense in $Y_1(N)$ if $p \mid N$ by the "disjointness" condition on C and P) and $I_n(E,P) = (E,nP)$. Although $\pi_2^{(p)}$ is *not* a map over $\mathbf{A}^1_{\mathbf{Z}[\frac{1}{Np}]}$, it can be shown that these all uniquely extend to (necessarily finite *flat*) maps, again denoted $\pi_1^{(p)}$, $\pi_2^{(p)}$, I_n between $X_1(N,p)$, $X_1(N)[\frac{1}{p}]$, $X_1(N)$. A proof of this fact requires the theory of minimal regular proper models of curves over a Dedekind base; the analogous fact over $\mathbf{Q}$ is an immediate consequence of basic facts about proper smooth curves over a field, but in order to most easily do some later calculations in characteristic $p \nmid N$ it is convenient to know that we have the map I_p defined on $X_1(N)$ over $\mathbf{Z}[1/N]$ (though this could be bypassed by using liftings to characteristic 0 in a manner similar to our later calculations of T_p in characteristic p).

Likewise, over $\mathbf{Z}[\frac{1}{N},\zeta_N]$ we can define, for any primitive Nth root of unity $\zeta = \zeta_N^i$ ($i \in (\mathbf{Z}/N\mathbf{Z})^*$), an operator $w_\zeta : Y_1(N)_{/\mathbf{Z}[\frac{1}{N},\zeta_N]} \to Y_1(N)_{/\mathbf{Z}[\frac{1}{N},\zeta_N]}$ via $w_\zeta(E,P) = (E/\langle P\rangle, P')$ where $\langle P\rangle$ is the order-N étale subgroup-scheme generated by P and $P' \in (E[N]/\langle P\rangle)(S)$ is uniquely determined by the relative Weil pairing condition $\langle P,P'\rangle_N = \zeta$ (with $P' \in E[N](S)$ here). This really does extend to $X_1(N)_{/\mathbf{Z}[\frac{1}{N},\zeta_N]}$, and one checks that $w_{\zeta^j} w_\zeta = I_j$ for $j \in (\mathbf{Z}/N\mathbf{Z})^*$. In particular, $w_\zeta^2 = 1$.

Since $X_1(N) \to \operatorname{Spec}\mathbf{Z}[\frac{1}{N}]$ is a proper smooth scheme with geometrically connected fibers of dimension 1, $\mathrm{Pic}^0_{X_1(N)_{/\mathbf{Z}[\frac{1}{N}]}}$ is an abelian scheme over $\mathbf{Z}[\frac{1}{N}]$ and hence is the Néron model of its generic fiber. We have scheme-theoretic Albanese and Pic^0 functoriality for finite (flat) maps between proper smooth curves (with geometrically connected fibers) over any base at all, and analytification of such a situation over $\mathbf{C}$ recovers the classical theory of Pic^0 as used in Section 5.1.

For example, we have endomorphisms

$$\langle n\rangle^* = \mathrm{Pic}^0(I_n), \quad \langle n\rangle_* = \mathrm{Alb}(I_n)$$

on $\mathrm{Pic}^0_{X_1(N)_{/\mathbf{Z}[\frac{1}{N}]}}$,

$$w_\zeta^* = \mathrm{Pic}^0(w_\zeta) = \mathrm{Alb}(w_\zeta) = (w_\zeta)_*$$

on $\mathrm{Pic}^0_{X_1(N)_{/\mathbf{Z}[\frac{1}{N},\zeta_N]}}$, and

$$T_p^* = \mathrm{Alb}(\pi_1^{(p)}) \circ \mathrm{Pic}^0(\pi_2^{(p)})$$
$$(T_p)_* = \mathrm{Alb}(\pi_2^{(p)}) \circ \mathrm{Pic}^0(\pi_1^{(p)})$$

on $\mathrm{Pic}^0_{X_1(N)_{/\mathbf{Z}[\frac{1}{Np}]}}$. A key point is that by the *Néronian property*, T_p^* and $(T_p)_*$ uniquely extend to endomorphisms of $\mathrm{Pic}^0_{X_1(N)_{/\mathbf{Z}[\frac{1}{N}]}}$, even though the $\pi_i^{(p)}$ do *not* make sense over $\mathbf{Z}[\frac{1}{N}]$ from what has gone before. In particular, it makes sense to study T_p^* and $(T_p)_*$ on the abelian variety $\mathrm{Pic}^0_{X_1(N)_{/\mathbf{F}_p}}$ over $\mathbf{F}_p$ for $p \nmid N$. This will be rather crucial later, but note it requires the Néronian property in the definition.

Passing to the analytifications, the above constructions recover the operators defined on $\mathrm{Pic}^0_{X_1(N)^{\mathrm{an}}}$ in Section 5.1. The resulting subring of

$$\mathrm{End}(\mathrm{Pic}^0_{X_1(N)_{/\mathbf{Z}[\frac{1}{N}]}}) \subset \mathrm{End}(\mathrm{Pic}^0_{X_1(N)^{\mathrm{an}}})$$

generated by T_p^*, $\langle n\rangle^*$ (respectively, by $(T_p)_*$, $\langle n\rangle_*$) is identified with $\mathbf{T}_1(N)$ via its $()^*$-action (respectively, via its $()_*$-action) and using

$$\varprojlim \mathrm{Pic}^0_{X_1(N)_{/\mathbf{Z}[\frac{1}{N}]}}[\ell^n](\overline{\mathbf{Q}}) \cong T_\ell(\mathrm{Pic}^0_{X_1(N)^{\mathrm{an}}}) \tag{5.6}$$

(using $\overline{\mathbf{Q}} \subset \mathbf{C}$) endows our "analytic" $V_\ell(N)$ with a canonical *continuous* action of $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ unramified at all $p \nmid N\ell$ (via Néron-Ogg-Shafarevich) and *commuting* with the action of $\mathbf{T}_1(N)$ (via either the $()^*$-action or the $()_*$-action). We also have an endomorphism $w_\zeta = w_\zeta^* = (w_\zeta)_*$ on $\mathrm{Pic}^0_{X_1(N)_{/\mathbf{Z}[\frac{1}{N},\zeta_N]}}$ and it is easy to see that

$$(g^{-1})^* w_{g(\zeta)} g^* = w_\zeta$$

on $\overline{\mathbf{Q}}$-points, where $g \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ and g^* denotes the natural action of g on $\overline{\mathbf{Q}}$-points (corresponding to base change of degree 0 line bundles on $X_1(N)_{/\overline{\mathbf{Q}}}$). Since $w_\zeta = w_{\zeta^{-1}}$ (as $(E,P) \cong (E,-P)$ via -1), we see that w_ζ is defined over the real subfield $\mathbf{Q}(\zeta_N)^+$. By étale descent, the operator w_ζ is defined over $\mathbf{Z}[\frac{1}{N},\zeta_N]^+$.

In any case, w_ζ acts on $V_\ell(N)$, recovering the operator in Section 5.1, and so this conjugates the $()^*$-action to the $()_*$-action, taking each $T \in \mathbf{T}_1(N)$ (for either action on $V_\ell(N)$) to its Weil pairing adjoint, via the canonical principal polarization of the abelian scheme $\mathrm{Pic}^0_{X_1(N)_{/\mathbf{Z}[\frac{1}{N}]}}$. Using Corollary 5.3 and (5.6) we obtain

Lemma 5.11. *Let $\mathbf{T}_1(N)$ act on $V_\ell(N)$ through either the $()^*$-action or the $()_*$-action. Then $\rho_{N,\ell} : G_{\mathbf{Q}} \to \mathrm{Aut}(V_\ell(N)) \cong \mathrm{GL}(2, \mathbf{Q}_\ell \otimes \mathbf{T}_1(N))$ is a continuous representation, unramified at $p \nmid N\ell$.*

The main result we are after is

Theorem 5.12. *Let $\mathbf{T}_1(N)$ act on $\mathrm{Pic}^0_{X_1(N)_{/\mathbf{Z}[\frac{1}{N}]}}$ via the $()_*$-action. For any $p \nmid N\ell$, the characteristic polynomial of $\rho_{N,\ell}(\mathrm{Frob}_p)$ is*

$$X^2 - (T_p)_* X + p\langle p\rangle_*$$

relative to the $\mathbf{Q}_\ell \otimes \mathbf{T}_1(N)$-module structure on $V_\ell(N)$, where Frob_p denotes an arithmetic Frobenius element at p.

The proof of Theorem 5.12 will make essential use of the w_ζ operator. For the remainder of this section, we admit Theorem 5.12 and deduce its consequences. Let $f \in S_2(\Gamma_1(N), \mathbf{C})$ be a *newform* of level N. Let $K_f \subset \mathbf{C}$ be the number field generated by $a_p(f)$ for all $p \nmid N$, where $f = \sum a_n(f) q^n$, so by weak multiplicity one $a_n(f) \in K_f$ for all $n \geq 1$ and the Nebentypus character χ_f has values in K_f. Let $\mathfrak{p}_f \subset \mathbf{T}_1(N)$ be the minimal prime corresponding to f (i.e., the kernel of the map $\mathbf{T}_1(N) \to K_f$ sending each $T \in \mathbf{T}_1(N)$ to its eigenvalue on f).

We now require $\mathbf{T}_1(N)$ to act on $\mathrm{Pic}^0_{X_1(N)_{/\mathbf{Z}[\frac{1}{N}]}}$ via its $()_*$-action.

Definition 5.13. A_f is the quotient of $\mathrm{Pic}^0_{X_1(N)_{/\mathbf{Q}}}$ by $\mathfrak{p}_f \subset \mathbf{T}_1(N)$.

By construction, A_f has good reduction over $\mathbf{Z}[\frac{1}{N}]$ and the action of $\mathbf{T}_1(N)$ on $\mathrm{Pic}^0_{X_1(N)_{/\mathbf{Q}}}$ induces an action of $\mathbf{T}_1(N)/\mathfrak{p}$ on A_f, hence an action of $K_f \cong (\mathbf{T}_1(N)/\mathfrak{p}) \otimes_{\mathbf{Z}} \mathbf{Q}$ on A_f in the "up-to-isogeny" category.

Theorem 5.14 (Shimura)**.** *We have* $\dim A_f = [K_f : \mathbf{Q}]$ *and* $V_\ell(A_f)$ *is free of rank* 2 *over* $\mathbf{Q}_\ell \otimes_{\mathbf{Q}} K_f$, *with* Frob_p *having characteristic polynomial*

$$X^2 - (1 \otimes a_p(f))X + 1 \otimes p\chi_f(p)$$

for all $p \nmid N\ell$.

Proof. By Lemma 5.11 and Theorem 5.12, we just have to check that the $\mathbf{Q}_\ell \otimes \mathbf{T}_1(N)$-linear map

$$V_\ell(\mathrm{Pic}^0_{X_1(N)_{/\mathbf{Q}}}) \to V_\ell(A_f)$$

identifies the right hand side with the quotient of the left hand side by $\mathfrak{p}_f$. More generally, for any exact sequence

$$B' \to B \to A \to 0$$

of abelian varieties over a field of characteristic prime to ℓ, we claim

$$V_\ell(B') \to V_\ell(B) \to V_\ell(A) \to 0$$

is exact. We may assume the base field is algebraically closed, and then may appeal to Poincaré reducibility (see [**77**, pg. 173]). □

Choosing a place λ of K_f over ℓ and using the natural realization of $K_{f,\lambda}$ as a factor of $\mathbf{Q}_\ell \otimes K_f$, we deduce from Theorem 5.14:

Corollary 5.15. *Let* $f \in S_2(\Gamma_1(N), \mathbf{C})$ *be a newform and* λ *a place of* K_f *over* ℓ. *There exists a continuous representation*

$$\rho_{f,\lambda} : G_{\mathbf{Q}} \to GL(2, K_{f,\lambda})$$

unramified at all $p \nmid N\ell$, *with* Frob_p *having characteristic polynomial*

$$X^2 - a_p(f)X + p\chi_f(p) \in K_{f,\lambda}[X].$$

5.3. Proof of Theorem 5.12

Fix $p \nmid N$ and let

$$J_p = \mathrm{Pic}^0_{X_1(N)_{/\mathbf{F}_p}} \cong \mathrm{Pic}^0_{X_1(N)_{/\mathbf{Z}[\frac{1}{N}]}} \times_{\mathbf{Z}[\frac{1}{N}]} \mathbf{F}_p$$

with $\mathbf{T}_1(N)$ acting through the $()_*$-action. Fix a choice of Frob_p, or more specifically fix a choice of place in $\overline{\mathbf{Q}}$ over p. Note that this determines a preferred algebraic closure $\overline{\mathbf{F}}_p$ as a quotient of the ring of algebraic integers, and in particular a map $\mathbf{Z}[1/N, \zeta_N] \to \overline{\mathbf{F}}_p$. Thus, we may view w_ζ as inducing an endomorphism of the abelian variety $J_p \times_{\mathbf{F}_p} \overline{\mathbf{F}}_p$ over $\overline{\mathbf{F}}_p$ (whereas the elements in $\mathbf{T}_1(N)$ induce endomorphisms of J_p over $\mathbf{F}_p$). The canonical isomorphism

$$V_\ell(\mathrm{Pic}^0_{X_1(N)_{/\mathbf{Q}}}) \cong V_\ell(\mathrm{Pic}^0_{X_1(N)_{/\mathbf{Z}[\frac{1}{N}]}}) \cong V_\ell(J_p)$$

identifies the Frob_p-action on $\overline{\mathbf{Q}}$-points on the left hand side with the (arithmetic) Frobenius action on $\overline{\mathbf{F}}_p$-points on the right hand side. Obviously $V_\ell(J_p)$ is a module over the ring

$\mathbf{Q}_\ell \otimes \mathbf{T}_1(N)$ and is free of rank 2 as such. For *any* $\mathbf{F}_p$-schemes Z, Z' and any $\mathbf{F}_p$-map $f : Z \to Z'$ the diagram

(5.7)
$$\begin{tikzcd} Z \arrow[r, "f"] \arrow[d, "F_Z"'] & Z' \arrow[d, "F_{Z'}"] \\ Z \arrow[r, "f"] & Z' \end{tikzcd}$$

commutes, where columns are absolute Frobenius. Taking $Z = \operatorname{Spec} \overline{\mathbf{F}}_p$, $Z' = J_p$, we see that the Frob_p action of $V_\ell(J_p)$ through $\overline{\mathbf{F}}_p$-points is *identical* to the action induced by the intrinsic absolute Frobenius morphism $F : J_p \to J_p$ over $\mathbf{F}_p$. Here is the essential input, to be proven later.

Theorem 5.16 (Eichler-Shimura). *In* $\mathrm{End}_{\overline{\mathbf{F}}_p}(J_p)$,

$$(T_p)_* = F + \langle p \rangle_* F^\vee, \qquad w_\zeta^{-1} F w_\zeta = \langle p \rangle_*^{-1} F$$

where $F^\vee$ *denotes the dual morphism.*

The extra relation involving w_ζ is crucial. The interested reader should compare this with [**108**, Cor. 7.10].

Let us admit Theorem 5.16 and use it to prove Theorem 5.12. We will then prove Theorem 5.16. Using an $\mathbf{F}_p$-rational base point P (e.g., the cusp 0), we get a commutative diagram

$$\begin{tikzcd} X_1(N)_{/\mathbf{F}_p} \arrow[r, hook] \arrow[d, "F_{X_1(N)}"'] & J_p \arrow[d, "F"] \\ X_1(N)_{/\mathbf{F}_p} \arrow[r, hook] & J_p \end{tikzcd}$$

where $F_{X_1(N)}$ denotes the absolute Frobenius morphism of $X_1(N)_{/\mathbf{F}_p}$, so by Albanese functoriality $F = \mathrm{Alb}(F_{X_1(N)})$. Thus

$$\begin{aligned} FF^\vee &= \mathrm{Alb}(F_{X_1(N)}) \circ \mathrm{Pic}^0(F_{X_1(N)}) \\ &= \deg(F_{X_1(N)}) = p \end{aligned}$$

as $X_1(N)_{/\mathbf{F}_p}$ is a smooth *curve*. We conclude from $(T_p)_* = F + \langle p \rangle_* F^\vee$ that

$$F^2 - (T_p)_* F + p \langle p \rangle_* = 0$$

on J_p, hence in $V_\ell(J_p)$. Thus, $\rho_{N,\ell}(\mathrm{Frob}_p)$ satisfies the expected quadratic polynomial

$$X^2 - (T_p)_* X + p \langle p \rangle_* = 0.$$

Let $X^2 - aX + b$ be the *true* characteristic polynomial, which $\rho_{N,\ell}(\mathrm{Frob}_p)$ must also satisfy, by Cayley-Hamilton. We must *prove* that $a = (T_p)_*$, and then $b = p\langle p \rangle_*$ is forced. It is this matter which requires the second relation.

We want $\mathrm{tr}_{\mathbf{Q}_\ell \otimes \mathbf{T}_1(N)}(\rho_{N,\ell}(\mathrm{Frob}_p)) = (T_p)_*$ or equivalently

$$\mathrm{tr}_{\mathbf{Q}_\ell \otimes \mathbf{T}_1(N)}(V_\ell(F)) = (T_p)_*.$$

Using the modified Weil pairing

$$[x, y]_\ell = (x, w_\zeta y)_\ell$$

and using the fact that $V_\ell(J_p) \cong V_\ell(\mathrm{Pic}^0_{X_1(N)_{/\mathbf{Q}}})$ respects Weil pairings (by invoking the relativization of this concept, here over $\mathbf{Z}[\frac{1}{N}]$) we may identify (via Theorem 5.8 and a choice $\mathbf{Q}_\ell(1) \cong \mathbf{Q}_\ell$ as $\mathbf{Q}_\ell$-vector spaces)

$$V_\ell(J_p) \cong \mathrm{Hom}_{\mathbf{Q}_\ell}(V_\ell(J_p), \mathbf{Q}_\ell) := V_\ell(J_p)^*$$

as $\mathbf{Q}_\ell \otimes \mathbf{T}_1(N)$-modules, but taking the F-action over to the $\langle p\rangle_* F^\vee$-action, since adjoints with respect to Weil pairings are dual morphisms and $w_\zeta^{-1} F^\vee w_\zeta$ is dual to $w_\zeta^{-1} F w_\zeta = \langle p\rangle_*^{-1} F = F\langle p\rangle_*^{-1}$ (absolute Frobenius commutes with all morphisms of $\mathbf{F}_p$-schemes!)

Since $V_\ell(J_p)$ is free of rank 2 over $\mathbf{Q}_\ell \otimes \mathbf{T}_1(N)$ and $\mathrm{Hom}_{\mathbf{Q}_\ell}(\mathbf{Q}_\ell \otimes \mathbf{T}_1(N), \mathbf{Q}_\ell)$ is free of rank 1 over $\mathbf{Q}_\ell \otimes \mathbf{T}_1(N)$, by Corollary 5.9, we conclude

$$\mathrm{tr}_{\mathbf{Q}_\ell \otimes \mathbf{T}_1(N)}(F|V_\ell(J_p)) = \mathrm{tr}_{\mathbf{Q}_\ell \otimes \mathbf{T}_1(N)}(\langle p\rangle_* F^\vee | V_\ell(J_p)^*).$$

We wish to invoke the following applied to the $\mathbf{Q}_\ell$-algebra $\mathbf{Q}_\ell \otimes \mathbf{T}_1(N)$ and the $\mathbf{Q}_\ell \otimes \mathbf{T}_1(N)$-module $V_\ell(J_p)$:

Lemma 5.17. *Let O be a commutative ring, A a finite locally free O-algebra with* $\mathrm{Hom}_O(A, O)$ *a locally free A-module* (*necessarily of rank* 1). *Let M be a finite locally free A-module, $M^* = \mathrm{Hom}_O(M, O)$, so M^* is finite and locally free over A with the same rank as M. For any A-linear map $f : M \to M$ with O-dual $f^* : M^* \to M^*$, automatically A-linear,*

$$\mathrm{char}(f) = \mathrm{char}(f^*)$$

in $A[T]$ (*these are the characteristic polynomials*).

Proof. Without loss of generality O is local, so A is semilocal. Making faithfully flat base change to the henselization of O (or the completion if O is noetherian or if we first reduce to the noetherian case), we may assume that A is a product of local rings. Without loss of generality, A is then local, so

$$M = \oplus A e_i$$

if free, and $\mathrm{Hom}_O(A, O)$ is free of rank 1 over A. Choose an isomorphism

$$h : A \cong \mathrm{Hom}_O(A, O)$$

as A-modules, so the projections

$$\pi_i : M \to Ae_i \cong A$$

satisfy $e_i^* = h(i) \circ \pi_i$ in M^*. These e_i^* are an A-basis of M^* and we compute matrices over A:

$$\mathrm{Mat}_{\{e_i\}}(f) = \mathrm{Mat}_{\{e_i^*\}}(f^*)^t.$$

□

We conclude that

$$\mathrm{tr}_{\mathbf{Q}_\ell \otimes \mathbf{T}_1(N)}(F|V_\ell(J_p)) = \mathrm{tr}_{\mathbf{Q}_\ell \otimes \mathbf{T}_1(N)}(\langle p\rangle_* f^\vee | V_\ell(J_p)).$$

By Theorem 5.16, we have

$$\begin{aligned} 2(T_p)_* &= \mathrm{tr}((T_p)_* | V_\ell(J_p)) \\ &= \mathrm{tr}(F + \langle p\rangle_* F^\vee | V_\ell(J_p)) \\ &= 2\,\mathrm{tr}(F|V_\ell(J_p)). \end{aligned}$$

This proves that $\mathrm{tr}(F|V_\ell(J_p)) = (T_p)_*$, so indeed $X^2 - (T_p)_* X + p\langle p\rangle_*$ *is* the characteristic polynomial. Finally, there remains

Proof of Theorem 5.16. It suffices to check the maps coincide on a Zariski dense subset of $J_p(\overline{\mathbf{F}}_p) = \mathrm{Pic}^0(X_1(N)_{/\overline{\mathbf{F}}_p})$. If g is the genus of $X_1(N)_{/\mathbf{Z}[\frac{1}{N}]}$ and we fix an $\overline{\mathbf{F}}_p$-rational base point, we get an induced surjective map

$$X_1(N)^g_{/\overline{\mathbf{F}}_p} \to J_{p/\overline{\mathbf{F}}_p},$$

so for any dense open $U \subset X_1(N)_{\overline{\mathbf{F}}_p}$, $U^g \to (J_p)_{/\overline{\mathbf{F}}_p}$ hits a Zariski dense subset of $\overline{\mathbf{F}}_p$-points. Taking U to be the ordinary locus of $Y_1(N)_{/\overline{\mathbf{F}}_p}$, it suffices to study what happens to a difference $(x)-(x')$ for $x, x' \in Y_1(N)(\overline{\mathbf{F}}_p)$ corresponding to (E,P), (E',P') over $\overline{\mathbf{F}}_p$ with E and E' *ordinary* elliptic curves.

By the commutative diagram (5.7), the map

$$J_p(\overline{\mathbf{F}}_p) \to J_p(\overline{\mathbf{F}}_p)$$

induced by F is the same as the map induced by the pth power map in $\overline{\mathbf{F}}_p$. By *definition* of Pic^0 functoriality, this corresponds to base change of an invertible sheaf on $X_1(N)_{/\overline{\mathbf{F}}_p}$ by the absolute Frobenius on $\overline{\mathbf{F}}_p$. By *definition* of $Y_1(N)_{/\overline{\mathbf{F}}_p}$ as a universal object, such base change induces on $Y_1(N)(\overline{\mathbf{F}}_p)$ *exactly* "base change by absolute Frobenius" on elliptic curves with a point of exact order N over $\overline{\mathbf{F}}_p$. We conclude

$$F((x)-(x')) = (E^{(p)}, P^{(p)}) - ((E')^{(p)}, P^{(p)})$$

where $(\,)^{(p)}$ denotes base change by absolute Frobenius on $\overline{\mathbf{F}}_p$.

Since $p = FF^\vee = F^\vee F$ and F is bijective on $\overline{\mathbf{F}}_p$-points, we have

$$\begin{aligned} F^\vee((x)-(x')) &= pF^{-1}((x)-(x')) \\ &= p((E^{(p^{-1})}, P^{(p^{-1})}) - ((E')^{(p^{-1})}, (P')^{(p^{-1})})). \end{aligned}$$

Thus,

$$\langle p\rangle_* F^\vee((x)-(x')) = p(E^{(p^{-1})}, pP^{(p^{-1})}) - p((E')^{(p^{-1})}, p(P')^{(p^{-1})})$$

so

$$\begin{aligned} (F+\langle p\rangle_* F^\vee)((x)-(x')) = {} & (E^{(p)}, P^{(p)}) + p(E^{(p^{-1})}, pP^{(p^{-1})}) \\ & - ((E')^{(p)}, (P')^{(p)}) + p((E')^{(p^{-1})}, p(P')^{(p^{-1})}). \end{aligned}$$

Computing $(T_p)_*$ on $J_p = \mathrm{Pic}^0_{X_1(N)_{/\mathbf{Z}[\frac{1}{N}]}} \times_{\mathbf{Z}[\frac{1}{N}]} \mathbf{F}_p$ is more subtle because $(T_p)_*$ was defined over $\mathbf{Z}[\frac{1}{Np}]$ (or over $\mathbf{Q}$) as $(\pi_2)_* \pi_1^*$ and was *extended* over $\mathbf{Z}[\frac{1}{N}]$ by the Néronian property. That is, we do *not* have a direct definition of $(T_p)_*$ in characteristic p, so we will need to lift to characteristic 0 to compute. It is *here* that the ordinariness assumption is crucial, for we shall see that, in some sense,

$$(T_p)_*((x)-(x')) = (F+\langle p\rangle_* F^\vee)((x)-(x'))$$

as *divisors* for ordinary points x, x'. This is, of course, much stronger than the mere linear equivalence that we need to prove.

Before we dive into the somewhat subtle calculation of $(T_p)_*((x)-(x'))$, let's quickly take care of the relation $w_\zeta^{-1} F w_\zeta = \langle p\rangle_*^{-1} F$, or equivalently,

$$Fw_\zeta = w_\zeta \langle p^{-1}\rangle_* F.$$

All maps here are induced by maps on $X_1(N)_{/\overline{\mathbf{F}}_p}$, with $F = \mathrm{Alb}(F_{X_1(N)})$, $w_\zeta = \mathrm{Alb}(w_{\zeta|_{X_1(N)}})$, $\langle p^{-1}\rangle_* = \mathrm{Alb}(I_{p^{-1}})$. Thus, it suffices to show

$$F_{X_1(N)} \circ w_\zeta = w_\zeta I_{p^{-1}} F_{X_1(N)}$$

on $X_1(N)_{/\overline{\mathbf{F}}_p}$, and we can check by studying $x = (E,P) \in Y_1(N)(\overline{\mathbf{F}}_p)$:

$$F_{X_1(N)} w_\zeta(x) = F_{X_1(N)}(E/P, P') = (E^{(p)}/P^{(p)}, (P')^{(p)})$$

where $\langle P, P'\rangle_N = \zeta$, so $\langle P^{(p)}, (P')^{(p)}\rangle_N = \zeta^p$ by compatibility of the (relative) Weil pairing with respect to base change. Meanwhile,

$$w_\zeta I_{p^{-1}} F_{X_1(N)}(x) = w_\zeta(E^{(p)}, p^{-1}P^{(p)}) = (E^{(p)}/(p^{-1}P^{(p)}), Q)$$

where $\langle p^{-1}P^{(p)}, Q\rangle_N = \zeta$, or equivalently $\langle P^{(p)}, Q\rangle = \zeta^p$. Since $Q = (P')^{(p)}$ is such a point, this second relation is established.

Now we turn to the problem of computing

$$(T_p)_*((x) - (x'))$$

for "ordinary points" $x = (E,P)$, $x' = (E',P')$ as above. Let $R = \mathbf{Z}_p^{\mathrm{un}}$, $W(\overline{\mathbf{F}}_p)$, or more generally any henselian (e.g., complete) discrete valuation ring with residue field $\overline{\mathbf{F}}_p$ and fraction field K of characteristic 0. Since $p \nmid N$, R is a $\mathbf{Z}[\frac{1}{N}]$-algebra. Since $Y_1(N)$ is *smooth* over $\mathbf{Z}[\frac{1}{N}]$, we conclude from the (strict) henselian property that $Y_1(N)(R) \to Y_1(N)(\overline{\mathbf{F}}_p)$ is surjective. Of course, this can be seen "by hand": if (E,P) is given over $\overline{\mathbf{F}}_p$, choose a Weierstrass model $\mathcal{E} \hookrightarrow \mathbf{P}^2_R$ lifting E (this is canonically an elliptic curve, by [**62**, Ch 2]). The finite *étale* group scheme $\mathcal{E}[N]$ is *constant* since R is strictly henselian. Thus there exists a unique closed immersion of group schemes $\mathbf{Z}/N\mathbf{Z} \hookrightarrow \mathcal{E}[N]$ lifting $P : \mathbf{Z}/N\mathbf{Z} \hookrightarrow E[N]$.

Let $(\mathcal{E},\mathcal{P})$, $(\mathcal{E}',\mathcal{P}')$ over R lift x, x' respectively. We view these sections to $X_1(N)_{/R} \to \mathrm{Spec}\, R$ as relative effective Cartier divisors of degree 1. Using the reduction map

$$\mathrm{Pic}^0_{X_1(N)_{/\mathbf{Z}[\frac{1}{N}]}}(R) \to J_p(\overline{\mathbf{F}}_p)$$

and the *definition* of $(T_p)_*$, we see that $(T_p)_*((x) - (x'))$ is the image of $(T_p)_*((\mathcal{E},\mathcal{P}) - (\mathcal{E}',\mathcal{P}'))$. Now R is *NOT* a $\mathbf{Z}[\frac{1}{Np}]$-algebra but K *is*, and we have an injection (even bijection)

$$\mathrm{Pic}^0_{X_1(N)_{/\mathbf{Z}[\frac{1}{N}]}}(R) \hookrightarrow \mathrm{Pic}^0_{X_1(N)_{/\mathbf{Z}[\frac{1}{N}]}}(K),$$

as $\mathrm{Pic}^0_{X_1(N)_{/\mathbf{Z}[\frac{1}{N}]}} \to \mathrm{Spec}\,\mathbf{Z}[\frac{1}{N}]$ is separated (even proper).

Thus, we will first compute $(T_p)_*((x) - (x'))$ by working with $\overline{K}$-points, where $\overline{K}$ is an algebraic closure of K. Since $p \nmid N$, we have

$$(\pi_2)_*\pi_1^*((\mathcal{E},\mathcal{P})_{/\overline{K}}) = \sum_C (\mathcal{E}_{\overline{K}}/C, \mathcal{P}_{\overline{K}} \bmod C)$$

where C runs through all $p+1$ order-p subgroups of $\mathcal{E}_{/\overline{K}}$. Since $\mathcal{E} \to \mathrm{Spec}\, R$ has *ordinary* reduction, and R is strictly henselian, the connected-étale sequence of $\mathcal{E}[p]$ is the short exact sequence of finite flat R-group schemes

$$0 \to \mu_p \to \mathcal{E}[p] \to \underline{\mathbf{Z}/p\mathbf{Z}} \to 0.$$

Enlarging R to a finite extension does not change the residue field $\overline{\mathbf{F}}_p$, so we may assume that

$$\mathcal{E}[p]_{/K} \cong \underline{\mathbf{Z}/p\mathbf{Z}} \times \underline{\mathbf{Z}/p\mathbf{Z}}.$$

Taking the scheme-theoretic closure in $\mathcal{E}[p]$ of the $p+1$ distinct subgroups of $\mathcal{E}[p]_{/K}$ gives $p+1$ *distinct* finite flat subgroup schemes $\mathcal{C} \subset \mathcal{E}$ realizing the $p+1$ distinct C's over $\overline{K}$.

Exactly one of these $\mathcal{C}$'s is killed by $\mathcal{E}[p] \to \underline{\mathbf{Z}/p\mathbf{Z}}$ over R, as this can be checked on the generic fiber, so it must be $\mu_p \hookrightarrow \mathcal{E}[p]$. For the remaining $\mathcal{C}$'s, the map $\mathcal{C} \to \underline{\mathbf{Z}/p\mathbf{Z}}$ is an isomorphism on the generic fiber. We claim these maps

$$\mathcal{C} \to \underline{\mathbf{Z}/p\mathbf{Z}}$$

over R are isomorphisms. Indeed, if $\mathcal{C}$ is *étale* this is clear, yet $\mathcal{C} \hookrightarrow \mathcal{E}[p]$ is a finite flat closed subgroup-scheme of order p, so a consideration of the closed fiber shows that if $\mathcal{C}$ is *not* étale then it is multiplicative. But $\mathcal{E}[p]$ has a *unique* multiplicative subgroup-scheme since

$$\mathcal{E}[p]^{\vee} \cong \mathcal{E}[p]$$

by Cartier-Nishi duality and $\mathcal{E}[p]$ has a *unique* order-*p* *étale* quotient (as any such quotient must kill the μ_p we have inside $\mathcal{E}[p]$.)

Thus,

$$\begin{aligned}(\pi_2)_*\pi_1^*((\mathcal{E},\mathcal{P})_{/\overline{K}}) &= \sum_{\mathcal{C}}(\mathcal{E}/\mathcal{C},\mathcal{P} \bmod \mathcal{C}) - \sum_{\mathcal{C}'}(\mathcal{E}'/\mathcal{C}',\mathcal{P}' \bmod \mathcal{C}') \\ &\in \mathrm{Pic}^0_{X_1(N)_{/\mathbf{Z}[\frac{1}{N}]}}(R)\end{aligned}$$

coincides with $(T_p)_*((\mathcal{E},\mathcal{P})-(\mathcal{E}',\mathcal{P}'))$ as both induce the same $\overline{K}$-point. Passing to closed fibers,

$$\begin{aligned}(T_p)_*((x)-(x')) = {} & (E/\mu_p, P \bmod \mu_p) + p(E/\underline{\mathbf{Z}/p\mathbf{Z}'}, P \bmod \mathbf{Z}/p\mathbf{Z}) \\ & - (E'/\mu_p, P' \bmod \mu_p) + p(E'/\underline{\mathbf{Z}/p\mathbf{Z}}, P' \bmod \mathbf{Z}/p\mathbf{Z})\end{aligned}$$

where $E[p] \cong \mu_p \times \underline{\mathbf{Z}/p\mathbf{Z}}$ and $E'[p] \cong \mu_p \times \underline{\mathbf{Z}/p\mathbf{Z}}$ are the *canonical* splittings of the connected-étale sequence over the perfect field $\overline{\mathbf{F}}_p$.

Now consider the relative Frobenius morphism

$$F_{E/\overline{\mathbf{F}}_p} : E \to E^{(p)},$$

which sends O to O (and P to $P^{(p)}$) and so is a map of *elliptic curves* over $\overline{\mathbf{F}}_p$. Recall that in characteristic p, for any map of schemes $X \to S$ we define the relative Frobenius map $F_{X/S} : X \to X^{(p)}$ to be the unique S-map fitting into the diagram

$$\begin{tikzcd}
X \arrow[r, "F_{X/S}"'] \arrow[rr, bend left, "F_X"] \arrow[dr] & X^{(p)} \arrow[r] \arrow[d] & X \arrow[d] \\
& S \arrow[r, "F_S"'] & S
\end{tikzcd}$$

where F_S, F_X are the absolute Frobenius maps. Since $E \to \mathrm{Spec}\,\overline{\mathbf{F}}_p$ is smooth of pure relative dimension 1, $F_{E/\overline{\mathbf{F}}_p}$ is finite flat of degree $p^1 = p$. It is bijective on points, so $\ker(F_{E/\overline{\mathbf{F}}_p})$ must be connected of order p.

The *only* such subgroup-scheme of E is $\mu_p \hookrightarrow E[p]$ by the *ordinariness*. Thus

$$E/\mu_p \cong E^{(p)}$$

is easily seen to take P mod μ_p to $P^{(p)}$.

Similarly, we have

$$\begin{tikzcd} E \arrow[r, "F_{E/\overline{\mathbf{F}}_p}"'] \arrow[rr, bend left, "p"] & E^{(p)} \arrow[r, "F^{\vee}_{E/\mathbf{F}_p}"'] & E \end{tikzcd}$$

so $F^{\vee}_{E/\mathbf{F}_p}$ is étale of degree p and base extension by $\mathrm{Frob}^{-1} : \overline{\mathbf{F}}_p \to \overline{\mathbf{F}}_p$ gives

$$\begin{tikzcd} E^{(p^{-1})} \arrow[r] \arrow[rr, bend left, "p"] & E \arrow[r] & E^{(p^{-1})} \\ P^{(p^{-1})} \arrow[r, mapsto] & P \arrow[r, mapsto] & p \cdot P^{(p^{-1})}. \end{tikzcd}$$

As the second map in this composite is étale of degree p, we conclude

$$(E_{/\underline{\mathbf{Z}/p\mathbf{Z}}}, P \mod \mathbf{Z}/p\mathbf{Z}) \cong (E^{(p^{-1})}, pP^{(p^{-1})}).$$

Thus, in $\mathrm{Pic}^0_{X_1(N)}(\overline{\mathbf{F}}_p)$,

$$\begin{aligned}(T_p)_*((x)-(x')) = {} & (E^{(p)}, P^{(p)}) + p \cdot (E^{(p^{-1})}, p \cdot P^{(p^{-1})}) \\ & - ((E')^{(p)}, (P')^{(p)}) - p \cdot ((E')^{(p^{-1})}, p \cdot (P')^{(p^{-1})})\end{aligned}$$

which we have seen is equal to $(F + \langle p \rangle_* F^{\vee})((x)-(x'))$.

□