Appendix A : a sketch of the construction of $\rho_{f,\lambda}$ when f has weight 2, following Eichler and Shimura.

The aim of this appendix is to give an idea of the original construction of the Galois representation $\rho_{f,\lambda}$ of Theorem ??, due to Eichler ($\varepsilon = 1$) and Shimura (any ε) when the weight k of f is 2, based on the *congruence relation*[1]. We insist that we shall not try to give below the cheapest proof (compare with the one in Shimura's book), notably regarding the input of algebraic geometry; on the other hand the ideas of the argument look reasonably clear this way.

Step 1: *Modular forms as differential forms on the modular curve* $X_1(N)(\mathbb{C})$. For $N \geq 4$, the group $\Gamma_1(N)$ acts freely on $\mathcal{H}$, hence it makes sense to consider (for any N) the complex Riemann surface

$$Y_1(N)(\mathbb{C}) := \Gamma_1(N)\backslash\mathcal{H}.$$

As is well known, this Riemann surface is non-compact, but has finitely many cusps, in natural bijection with $\Gamma_1(N)\backslash\mathbb{P}^1(\mathbb{Q})$. We denote by $X_1(N)(\mathbb{C})$ the compact Riemann surface obtained by adding these cusps. Remark that a holomorphic differential 1-form $f(\tau)d\tau$ on $\mathcal{H}$ is invariant by $\Gamma_1(N)$, *i.e.* descends to a holomorphic 1-form ω_f on $Y_1(N)(\mathbb{C})$ if $f \in M_2(N)$: this is obvious when $N \geq 4$ as $\Gamma_1(N)$ is torsion-free, and it is easily checked[2] to hold for any N. By an inspection of differentials at the cusps, one even checks that $f \mapsto \omega_f$ induces an isomorphism

$$S_2(N) \simeq H^0(X_1(N)(\mathbb{C}), \Omega^1)$$

(see e.g. Shimura's book). In particular, $\dim S_2(N)$ is the genus of $X_1(N)$. Using the Riemann-Hurwitz formula, one can show for instance that this genus if 0 for $1 \leq N \leq 12$ and $N \neq 11$, in which case $X_1(N)(\mathbb{C}) \simeq \mathbb{P}^1(\mathbb{C})$. It follows that, without loss of generality, we may assume that $N \geq 4$ anyway.

Recall the exact complex $0 \to \mathbb{C} \to \mathcal{O} \overset{f\mapsto df}{\to} \Omega^1 \to 0$ on any compact Riemann surface S. It is a classical fact that it leads to an exact sequence $0 \to H^0(S, \Omega^1) \to H^1(S, \mathbb{C}) \to H^1(S, \mathcal{O}) \to 0$, and that the last map has a natural section provided by the *anti-holomorphic* 1-*forms*, so we have $H^1(S, \mathbb{C}) = H^0(S, \Omega^1) \oplus \overline{H^0(S, \Omega^1)}$. In particular,

firstiso (0.1) $$S_2(N) \oplus \overline{S_2(N)} = H^1(X_1(N)(\mathbb{C}), \mathbb{C}).$$

Step 2: *Hecke correspondences.* If S and S' are two Riemann surfaces and $f : S' \to S$ is a finite (=non constant) morphism, we have a natural linear map $f^* : H^1(S, \mathbb{C}) \to H^1(S', \mathbb{C})$ given by the pull-back of differential 1-forms. In terms of the de Rham-Betti comparison theorem, f^* is the Poincaré dual to the direct image of 1-cycles on $H_1(S', \mathbb{C})$. Moreover, $f^*(H^0(S, \Omega^1)) \subset H^0(S', \Omega^1)$. There is also a trace map : $f_* : H^1(S', \mathbb{C}) \to H^1(S, \mathbb{C})$, which is dual to the inverse image

[1]There is an alternative proof due to Langlands and Kottwitz (that works for any $k \geq 2$) based on the comparison between the Selberg trace formula for $\mathrm{GL}_2/\mathbb{Q}$ applied to some specific functions and the formula giving the number of elliptic cuvres (plus some level structure) over a given finite field, gathered by isogeny classes (theory of Weil numbers of elliptic curves: Tate, Honda-Tate). This approach is actually much more demanding in mathematics, however it generalizes well to higher-dimensional Shimura varieties. See e.g. Clozel's Bourbaki talk on Kottwitz' results, Casselman's papers at the Corvallis conference, or the books of Laumon.)

[2]Be sure to understand what has to be checked !

(or "correstriction") of 1-cycles on $H_1(S, \mathbb{C})$. As a consequence of all of this, if we have correspondence on S, i.e. a pair (p, q) of finite morphisms:

$$\begin{array}{ccc} & S' & \\ {}^{p}\swarrow & & \searrow^{q} \\ S & & S \end{array}$$

We have a natural linear map on $H^1(S, \mathbb{C})$ preserving $H^0(S, \Omega^1)$ defined by $\omega \mapsto p_* q^* \omega$. Of course, (q, p) defines a correspondence as well, called the dual or transpose of (p, q).

It turns out that by construction, the Hecke correspondences on $S_2(N)$ are of this form. Indeed, let ℓ be some prime such that $(\ell, N) = 1$, and set

$$Y_1(N, \ell)(\mathbb{C}) := \Gamma_1(N, \ell)\backslash\mathcal{H}, \quad \Gamma_1(N, \ell) := \Gamma_1(N) \cap \Gamma_0(\ell).$$

Again, this Riemann surface has a finite number of cusps in bijection with $\Gamma_1(N, \ell)\backslash\mathbb{P}^1(\mathbb{Q})$, and by adding these cusps we obtain a compact Rieman surface denoted by $X_1(N, \ell)(\mathbb{C})$.

Remark that if $x = \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q})^+$, then $\Gamma_1(N) \cap x^{-1}\Gamma_1(N)x = \Gamma_1(N, \ell)$. It follows that we can define two natural morphisms

$$p, q : X_1(N, \ell)(\mathbb{C}) \to X_1(N)(\mathbb{C})$$

as follows. First, p is the natural map induced by quotient from the inclusion $\Gamma_1(N, \ell) \subset \Gamma_1(N)$, and q is induced by the map $\tau \mapsto x\tau$ on $\mathcal{H}$. Concretely, if $\omega = \omega_f \in S_2(N)$ then $q^*\omega = (f|_2 x)(\tau)d\tau$ is invariant by $x^{-1}\Gamma_1(N)x$, hence by $\Gamma_1(N, \ell)$. If we choose a finite number of elements $y_i \in \Gamma_1(N)$ such that $\Gamma_1(N) = \coprod_i \Gamma_1(N, \ell)y_i$, then by definition $p_* q^* \omega == (\sum_{i=0}^{\ell} f|_2 x y_i)d\tau$. But we check easily that $\Gamma_1(N)x\Gamma_1(N) = \coprod_i \Gamma_1(N)xy_i$, so that

$$p_* q^* \omega = T_\ell(f)(\tau)d\tau$$

as claimed above.

Corollary 0.1. *If $f \in S_2(N, \varepsilon)$ is an eigenform, and $T_\ell(f) = a_\ell f$ for each prime ℓ prime to N, then a_ℓ is an algebraic integer and the coefficient field of f*

$$\mathbb{Q}(\{a_\ell, (\ell, N) = 1\}) \subset \mathbb{C}$$

is a finite extension of $\mathbb{Q}$.

Proof — Indeed, the Hecke correspondences beeing induced by correspondences on the Riemann surface $X_1(N)(\mathbb{C})$, they preserve the integral structure

$$H^1(X_1(N)(\mathbb{C}), \mathbb{Z}) \subset H^1(X_1(N)(\mathbb{C}), \mathbb{C})$$

defined by the Betti cohomology. The first statement follows then for instance from the Cayley-Hamilton theorem, and the second from the fact that the coefficient field of f arises then as a residue field of a commutative subalgebra of the endomorphisms of the finite dimensional $\mathbb{Q}$-vectorspace $H^1(X_1(N)(\mathbb{C}), \mathbb{Q})$. □

We refer to the exercises of Part I for the statements of the basic facts of Atkin-Lehner theory and newforms.

defVf PROPOSITION 0.2. *Assume that* $f = \sum_{n\geq 1} a_n q^n \in S_2(N, \varepsilon)$ *is a normalized newform and fix an embedding* $\iota_\infty : \overline{\mathbb{Q}} \to \mathbb{C}$. *The biggest subspace*

$$V_f \subset H^1(X_1(N)(\mathbb{C}), \mathbb{Q}) \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$$

over which each T_ℓ *for* $(\ell, N) = 1$ *acts by the scalar* $\iota_\infty^{-1}(a_\ell)$ *has* $\overline{\mathbb{Q}}$*-dimension* 2.

Proof — Indeed, as each T_ℓ preserves $H^1(X_1(N)(\mathbb{C}), \mathbb{Q})$, the eigenspace above is a $\overline{\mathbb{Q}}$-structure of the similar eigenspace in $H^1(X_1(N)(\mathbb{C}) = S_2(N) \oplus \overline{S_2(N)}$, which has dimension $1 + 1 = 2$ by Atkin-Lehner's theorem. □

Step 3. *The natural* $\mathbb{Q}$*-structure of modular curves and definition of* $\rho_{f,\lambda}$. The modular curves $X_1(N, \mathbb{C})$ and $X_1(N, \ell)(\mathbb{C})$ are compact Riemann surfaces. A theorem of Riemann asserts that any such surface is the complex point of a unique projective algebraic smooth curve over $\mathbb{C}$ (hence the $-(\mathbb{C})$ in their name). It turns out that both of them are defined over $\mathbb{Q}$, they even have a natural[3] $\mathbb{Q}$-structure. Indeed, it is enough to define a $\mathbb{Q}$-structure on their field of meromorphic functions[4], and a good definition turns out to be the following: a meromorphic function f on any of these curves is said $\mathbb{Q}$-rational if its q-expansion lies in $\mathbb{Q}((q))$. See Shimura for the proof that it is indeed a $\mathbb{Q}$-structure. An example of a non-constant such function is the usual j function, whose q-expansion

$$j(\tau) = q^{-1} + 744 + 196884q + \dots$$

even lies in $\mathbb{Z}((q))$. Denote for the moment by $X_1(N)$ and $X_1(N, \ell)$ the projective smooth algebraic curves over $\mathbb{Q}$ defined by these $\mathbb{Q}$-structures. A natural place to look for Galois representation of $G_{\mathbb{Q}}$ is the étale cohomology of these curves. (Recall that in the case of curves, a pocket substitute for the étale homology is provided by the Tate-module of the Pic^0 of the curve) Recall also the étale-Betti comparison theorem

$$H^1_{\mathrm{et}}(X_1(N)_{\overline{\mathbb{Q}}}, \mathbb{Q}_p) \xrightarrow{\sim} H^1_{\mathrm{et}}(X_1(N)_{\mathbb{C}}, \mathbb{Q}_p) \xrightarrow{\sim} H^1(X_1(N)(\mathbb{C}), \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{Q}_p.$$

If we fix an embedding $\iota_p : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_p$, it induces an isomorphism

$$H^1_{\mathrm{et}}(X_1(N)_{\overline{\mathbb{Q}}}, \overline{\mathbb{Q}}_p) := H^1_{\mathrm{et}}(X_1(N)_{\overline{\mathbb{Q}}}, \mathbb{Q}_p) \otimes_{\mathbb{Q}_p} \overline{\mathbb{Q}}_p \xrightarrow{\sim} H^1(X_1(N)(\mathbb{C}), \mathbb{Q}) \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_p.$$

These isomorphisms commute with correspondences on $X_1(N)$ defined over $\mathbb{Q}$. As we shall see below, the natural maps $X_1(N, \ell)(\mathbb{C}) \to X_1(N)(\mathbb{C})$ defined above are actually defined over $\mathbb{Q}$, hence so are the geometric Hecke-correspondences T_ℓ. It follows that if f is as in Prop. 0.2, and if $\iota_p \iota_\infty^{-1} : E \to \overline{\mathbb{Q}}_p$ induces the place λ of E, and if

$$V_{f,\lambda} \subset H^1_{\mathrm{et}}(X_1(N)_{\overline{\mathbb{Q}}}, \overline{\mathbb{Q}}_p)$$

[3]In general, if a complex algebraic curve is defined over $\mathbb{Q}$, there may well be non-isomorphic $\mathbb{Q}$-structure: for instance, the projective plane conics $x^2 + y^2 + z^2 = 0$ and $x^2 - y^2 + z^2 = 0$ are non isomorphic over $\mathbb{Q}$ (the first having no rational point) but they are over $\mathbb{C}$.

[4]If K is the field of meromorphic functions on $X_1(N)(\mathbb{C})$ say, a $\mathbb{Q}$-structure of K is a finitely generated subfield k such that $k \otimes_{\mathbb{Q}} \mathbb{C} = K$.

denotes the biggest subspace over which each T_ℓ with (ℓ, N) acts by multiplication by a_ℓ (or more precisely by $\iota_p\iota_\infty^{-1}(a_\ell)$), then the comparison theorem étale-Betti induces an isomorphism

$$V_{f,\lambda} \xrightarrow{\sim} V_f \otimes_{\overline{\mathbb{Q}}} \overline{\mathbb{Q}}_p,$$

and in particular, $V_{f,\lambda}$ has dimension 2 over $\overline{\mathbb{Q}}_p$. The Galois action of $G_\mathbb{Q}$ on $H^1_{\text{et}}(X_1(N)_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)$ commutes with all the Hecke correspondences defined over $\mathbb{Q}$, thus $V_{f,\lambda}$ is stable by $G_\mathbb{Q}$.

Definition 0.3. *Define $\rho_{f,\lambda}$ as the Galois representation of $G_\mathbb{Q}$ on $V_{f,\lambda}$.*

It remains to show that $\rho_{f,\lambda}$ has the required properties. We already know that, as any geometric Galois representation, it is unramified outside some finite set S. The statement asserts that S may be reduced to the set of divisors of $Np\infty$. It is enough to show that $X_1(N)$ has good reduction outside N, which is not obvious at all from the definition, but true (Igusa). This property will be included in the next (admitted) statement.

Step 4: *Arithmetic moduli of elliptic curves.* Recall that if E is a complex elliptic curve, then $E \simeq \mathbb{C}/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}$ which is unique up to multiplication by $\lambda \in \mathbb{C}^*$. For $\tau \in \mathcal{H}$, set $E_\tau = \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ and $P_\tau = \overline{1/N} \in E_\tau$ (it is a point of order N). The Riemann surface $Y_1(N)(\mathbb{C})$ parameterizes complex elliptic curves equipped with a point of order N:

lemmarep

Lemma 0.4. *The map $\tau \mapsto (E_\tau, P_\tau)$ induces a bijection between $Y_1(N)(\mathbb{C})$ and the set of isomorphism classes of pairs (E, P) with E a complex elliptic curve and $P \in E$ a point of order N.*

We leave this statement as an exercise to the reader. By definition, an (iso)morphism $(E, P) \to (E', P)$ is an (iso)morphism $E \to E'$ sending P to P'. Similarily, one can show that for $(\ell, N) = 1$, $Y_1(N, \ell)(\mathbb{C})$ parameterizes the isomorphism classes of triples (E, P, H) where E is an elliptic curve, $P \in E$ a point of order N, and $H \subset E$ a subgroup of order ℓ. From this point of view, the Hecke correspondence T_ℓ is the transpose of the map

$$Y_1(N)(\mathbb{C}) \to \mathrm{Div}(Y_1(N)(\mathbb{C})), \quad (E, P) \mapsto \sum_H [(E/H, (P + H)/H)],$$

where H runs over the $\ell + 1$ sugroups of E of order ℓ.

It is an important fact that whenever $N \geq 4$, the moduli properties above of complex modular curves extend to their $\mathbb{Q}$-structures defined above, which actually gives another way to see this $\mathbb{Q}$-structure. This actually extends beautifully over $\mathbb{Z}$. For all of this we refer to the book of Katz-Mazur “Arithmetic moduli of elliptic curves" (other useful references : Deligne-Rapoport paper in “Modular functions in 1-variables II", Hida "Geometric modular forms and elliptic curve"). We give below a brief survey of what we shall need from this book.

If S is a scheme, an elliptic curve over S (understand : “a family of elliptic curves parameterized by S") is a proper smooth morphism $E \to S$ equipped with a section $O \in E(S)$ such that for any point $s \in S$, the fiber E_s is an elliptic curve over the residue field $k(s)$ with neutral element $O \times_S s$. If E is such an elliptic curve, it may be given a structure a commutative S-group scheme over E with neutral element 0 in a natural way, which coincides over the fibers of S with the group law of elliptic curves encountered before. For any $N \geq 1$ its N-torsion $E[N]$ is a finite flat group scheme over S of degree N^2, which is étale if and only if $N \in \mathcal{O}(S)^\times$. We refer to Fargues' lectures for the basics about finite flat commutative group schemes.

Denote by F the contravariant functor from schemes over $\mathbb{Z}[1/N]$ to sets, where $F(S)$ is the set of isomorphism classes of pairs (E, P) where E is an elliptic curve over S and $P : \mu_N \to E[N]$ an embedding of S-group schemes. We also denote by F_ℓ the similar functor parameterizing isomorphism classes of triples (E, P, H) where H is furthermore a finite flat S-subgroup of $E[\ell]$ of order ℓ.

Theorem 0.5. *(Shimura, Igusa, Deligne-Rapoport, Katz-Mazur, Drinfeld). Assume $N \geq 5$. The functor F is representable by a smooth affine curve $Y_1(N)$ over $\mathbb{Z}[1/N]$ whose complex points are isomorphic to the Riemann surface $Y_1(N)(\mathbb{C})$ introduced above in a compatible way with lemma* lemmarep *0.4. This scheme $Y_1(N)$ is an open subscheme of a natural proper smooth curve $X_1(N)$ over $\mathbb{Z}[1/N]$ ("theory of the Tate curve"), and whose complex points are isomorphic to the Riemann surface $X_1(N)(\mathbb{C})$ introduced above.*

Similarily, if $(\ell, N) = 1$, then F_ℓ is representable by a flat affine curve $Y_1(N, \ell)$ over $\mathbb{Z}[1/N]$, whose complex points are isomorphic to the Riemann surface $Y_1(N, \ell)(\mathbb{C})$ introduced above (again in a compatible way with the identification above for the $\mathbb{C}$-points). This scheme $Y_1(N, \ell)$ is an open subscheme of a natural proper flat curve $X_1(N, \ell)$ over $\mathbb{Z}[1/N]$ (idem), which is smooth over $\mathbb{Z}[1/N\ell]$, and whose complex points are isomorphic to the Riemann surface $X_1(N, \ell)(\mathbb{C})$ introduced above.

The morphisms $F_\ell \to F$, defined by $(E, P, H) \mapsto (E, P)$ and $(E, P, H) \mapsto (E/H, (P + H)/H)$, extend to finite flat morphisms $X_1(N, \ell) \to X_1(N)$. In particular the geometric Hecke correspondence T_ℓ extends to a finite flat correspondence on $X_1(N)$ over $\mathbb{Z}[1/N]$.

We take all of this as a (rather heavy) black-box. It is understood that the modular curves over $\mathbb{Z}[1/N]$ defined by this theorem coincide with our previous $X_1(N)$ and $X_1(N, \ell)$ when pulled-back to $\mathbb{Q}$. Let us stress that the most difficult part of this statement is to prove the representability of F and F_ℓ. It is then comparatively easy to check for instance that $X_1(N)$ is a smooth curve over $\mathbb{Z}[1/N]$ (so that $X_1(N)_\mathbb{Q}$ has good reduction outside the primes dividing N).

Till now, we have defined $\rho_{f,\lambda}$ and explained why it is unramified outside $Np\infty$. Indeed, by property (i) and (iii) and Example (iii) of the paragraph on étale cohomology there are natural isomorphisms for $(\ell, Np) = 1$:

$$H^1_{\text{et}}(X_1(N)_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)_{|G_{\mathbb{F}_\ell}} \xrightarrow{\sim} H^1_{\text{et}}(X_1(N)_{\overline{\mathbb{F}_\ell}}, \mathbb{Q}_p) \xrightarrow{\sim} \operatorname{Hom}_{\mathbb{Z}_p}(T_p(X_1(N)_{\mathbb{F}_\ell}), \mathbb{Q}_p)$$

and these isomorphisms commute with the geometric T_ℓ correspondences (this uses that T_ℓ is finite flat over $\mathbb{Z}[1/N]$ for the commutation with the Grothendieck's base change theorems). In particular,

almostfini
$$(V^\vee_{f,\lambda})_{|G_{\mathbb{F}_\ell}} = (T_p(X_1(N)) \otimes_{\mathbb{Z}_p} \overline{\mathbb{Q}}_p)[f] \qquad (0.2)$$

where the $[f]$ on the right means "the biggest subspace over which all each T_ℓ's act by multiplication by $\iota_p \iota_\infty^{-1} a_\ell$". It makes now sense to talk about $\det(1 - T\rho_{E,\lambda}(\mathrm{Frob}_\ell))$ for ℓ prime to Np.

Step 5. *Eichler-Shimura's congruence relation.* Fix an ℓ prime to Np. The curve $X_1(N)$ has a natural action of $(\mathbb{Z}/N\mathbb{Z})^\times$, usually denoted by $d \mapsto \langle d \rangle$, given on the moduli problem F by raising the μ_N-point P to the power d. On the $\mathbb{C}$-points, it is simply induced by the left action of $\Gamma_0(N)/\Gamma_1(N)$ on $X_1(N)$.

THEOREM 0.6. *(Eichler-Shimura) On* $\mathrm{Pic}(X_1(N)_{\mathbb{F}_\ell})$ *we have*

$$T_\ell = \mathrm{frob}_\ell + \ell\langle\ell\rangle\mathrm{frob}_\ell^{-1}.$$

Let C be a projective smooth algebraic curve over $\mathbb{F}_\ell$. Recall that there is a geometric Frobenius endomorphism $\mathrm{Fr}_\ell : C \to C$ which is finite, purely inseparable, of degree ℓ (it is just raising to the ℓ-th power on functions). The action induced by Fr_ℓ on $C(\overline{F})$ coincides with the natural one of frob_ℓ, so the correspondence $(\mathrm{id}, \mathrm{Fr}_\ell) : C \to C$ is the natural endomorphism frob_ℓ on $\mathrm{Div}(C)$ and $\mathrm{Pic}^0(C)$. Its dual correspondence $\mathrm{Fr}_\ell^\vee = (\mathrm{Fr}_\ell, \mathrm{id})$ acts then via $\ell\ \mathrm{Fr}_\ell^{-1}$ on these spaces.

Assume now that $C = X_1(N)_{\mathbb{F}_\ell}$. By the main theorem of Step 4, $Y_1(N)(\overline{\mathbb{F}}_\ell)$ is in natural bijection with pairs (E, P) where E is an elliptic curve over $\overline{\mathbb{F}}_\ell$ and $P : \mu_N(\overline{\mathbb{F}}_\ell) \to E(\overline{\mathbb{F}}_\ell)[N]$ a $\mathbb{Z}[G_{\mathbb{F}_\ell}]$-equivariant embedding. Moreover, the correspondence T_ℓ acts on $\mathrm{Div}(Y_1(N)_{\mathbb{F}_\ell})$ by the formula

$$(E, P) \mapsto \sum_H (E/H, (P + H)/H)$$

where H runs over the $\ell + 1$ subgroup schemes of $E[\ell]$. By $(P + H)/H$ we simply mean the composite of P with the natural isomorphism $E(\overline{\mathbb{F}}_\ell)[N] \to (E/H)(\overline{\mathbb{F}}_\ell)[N]$.

Let $D^{\mathrm{ord}} \subset \mathrm{Div}(C)$ be the subgroup generated by the points in $C(\overline{\mathbb{F}}_\ell)$ which are in $Y_1(N)$, so of the form (E, P), and such that furthermore E is an ordinary elliptic curve. We refer to Silverman's book for the basics about ordinary elliptic curves. Recall that all but finitely many points of $C(\overline{\mathbb{F}}_\ell)$ (omitting cusps as well) have this form. As any divisor on a curve is always linearly equivalent to a divisor omitting any given finite set of points, it follows that the natural map

$$D^{\mathrm{ord}} \to \mathrm{Pic}(C)$$

is surjective. It is thus enough to check Eichler-Shimura's relation on the free abelian group D^{ord}.

Fix E an ordinary elliptic curve over $\overline{\mathbb{F}}_\ell$. Recall that $[\ell] : E \to E$ has degree ℓ^2, and inseparable degree ℓ in this case. The group scheme $E[\ell]$ has exactly one connected subgroup of order ℓ (isomorphic to μ_ℓ), namely $H := E[\ell]^0 =$ the kernel of the Frobenius map

$$\mathrm{Fr}_\ell : E \longrightarrow E^{(\ell)} := E \times_{\overline{\mathbb{F}}_\ell} \overline{\mathbb{F}}_\ell$$

the latter scalar extension being given by $\mathrm{frob}_{\mathbb{F}_\ell}$ (it just amounts to raising the coefficients of a Weierstrass equation of E to the power ℓ to get $E^{(\ell)}$). In particular, Fr_ℓ induces an isomorphism $E/H \xrightarrow{\sim} E^{(\ell)}$, sending any μ_N-point P on the point $P^{(\ell)} := P \times_{\overline{\mathbb{F}}_\ell} \overline{\mathbb{F}}_\ell \to E^{(\ell)}$. In other words

$$[(E/H, (P + H)/H)] = \mathrm{frob}_\ell[(E, P)] \quad \text{if} \ \ H = E[p]^0.$$

The ordinary elliptic curve E has exactly ℓ subgroups of order ℓ different from $E[\ell]^0$, which are all étale subgroups. For each such subgroup, say H, consider the associated factorization of the multiplication by ℓ :

$$[\ell] : E \stackrel{\mathrm{can}}{\to} E/H \stackrel{j}{\to} E.$$

Then j is finite and purely inseparable of degree ℓ, so it necessarily factors as

$$E/H \stackrel{\mathrm{Fr}_\ell}{\to} (E/H)^{(\ell)} \stackrel{j'}{\to} E,$$

as so does any inseparable morphism of degree ℓ between two projective smooth curves over $\overline{\mathbb{F}}_\ell$ (see e.g. Hartschorne's book), and j' is an isomorphism. If P is a μ_N-point of E, then j' sends the point $\mathrm{Fr}_\ell \,\mathrm{o}\, \mathrm{can}(P) = ((P+H)/H)^{(\ell)}$ to $[\ell]P$. It follows that

$$\mathrm{frob}_\ell[(E/H, (P+H)/H)] = \langle \ell \rangle [(E,P)]$$

whenever H is étale of order ℓ, which concludes the proof as there are ℓ such subgroups, and $\langle \ell \rangle$ is defined over $\mathbb{F}_\ell$ hence commutes with frob_ℓ^{-1}. □

Remark. Let E be an elliptic curve over $\overline{\mathbb{Q}}_\ell$ with good ordinary reduction $\overline{E}$ over $\overline{\mathbb{F}}_\ell$. If $H \subset E(\overline{\mathbb{Q}}_\ell)[\ell]$ is a subgroup of order ℓ, the analysis above may be reformulated (say forgetting the μ_N-points) as a congruence in $\overline{\mathbb{F}}_\ell$:

$$j(E/H) \equiv j(E)^\ell \text{ or } j(E/H) \equiv j(E)^{\ell^{-1}}$$

the first case occuring iff H reduces to $\overline{E}[\ell]^0$. (This makes sense as if E has good reduction over $\overline{\mathbb{Q}}_\ell$ then $j(E) \in \overline{\mathbb{Z}}_\ell$ and this property is preserved under isogenies) For this reason, the Eichler-Shimura's theorem is often called the *congruence relation*.

Step 6. *End of the proof.* By property (MF1) of modular forms, the operators $\langle d \rangle$ act by multiplication by $\varepsilon(\ell)$ on V_f. A complement to the main theorem of Step 4 is that these isomorphisms of $Y_1(N)$ actually extend to isomorphisms of $X_1(N)$ over $\mathbb{Z}[1/N]$. It follows that they commute with all the various kind of comparison theorems used above, hence that $\langle \ell \rangle$ acts by multiplication by $\varepsilon(\ell)$ on $V_{f,\lambda}$ for $(\ell, N) = 1$ (we omit the $\iota_p \iota_\infty^{-1}$). As T_ℓ acts on $V_{f,\lambda}$ by multiplication by a_ℓ, the Eichler-Shimura theorem reads on $V_{f,\lambda}$:

$$\mathrm{frob}_\ell^2 - a_\ell \mathrm{frob}_\ell + \ell\varepsilon(\ell) = 0, \;\; (\ell, Np) = 1.$$

It only remains to explain why the traces of $\mathrm{Fr}_\ell = \mathrm{frob}_\ell$ and of $\varepsilon(\ell)\mathrm{Fr}_\ell^\vee = \ell\varepsilon(\ell)\mathrm{frob}_\ell^{-1}$ coincide on $V_{f,\lambda}$. (to be continued)