Galois Representations attached to Modular Curves

In this note, I'll discuss attaching a Galois representation to a modular curve, forming a sort of precursor to the definition of the Galois representation attached to a modular form. We do this by associating some abelian variety to our curve, then taking its Tate module. The right variety to consider is the *Picard group* of the modular curve, and we obtain the associated homomorphism

$$\rho_{X_0(N),\ell} : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(\mathrm{Ta}_\ell \mathrm{Pic}^0(X_0(N)) \cong \mathrm{GL}_{2g}(\mathbb{Z}_\ell).$$

Having defined the Picard group, we then look at its reduction modulo a prime p, obtaining the *Eichler-Shimura relation*, a description of the T_p operator mod p in terms of the Frobenius map induced by $x \mapsto x^p$. This then lets us describe the image under $\rho_{X_0(N),\ell}$ of general Frobenius elements $\mathrm{Frob}_{\mathfrak{p}}$, where $\mathfrak{p}$ is a prime of $\overline{\mathbb{Z}}$ lying above p.

1. Modular Curves 101

Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup. Define the *compactified modular curve for* Γ to be

$$X(\Gamma) := \Gamma\backslash\mathcal{H}^*,$$

where $\mathcal{H}^*$ is the extended upper half-plane $\mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$.

Facts: (i) The modular curve $X(\Gamma)$ is a compact, Hausdorff Riemann surface. (see [DS05], Chapter 2).

(ii) The genus of $X(\Gamma)$ is equal to $\dim_{\mathbb{C}} S_2(\Gamma)$. (see [DS05], Chapter 3).

(iii) $X(\Gamma)$ has a model as an algebraic curve over $\mathbb{Q}$. (see [DS05], Chapter 7). (In fact, it has a model as a scheme over $\mathbb{Z}[1/N]$; see [Loe14]).

Hecke operators have a geometric interpretation using $X(\Gamma)$: if we define $\gamma_p := \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$, and

$$\Gamma' := \Gamma \cap \gamma_p \Gamma \gamma_p^{-1}, \quad \Gamma'' := \gamma_p^{-1}\Gamma\gamma_p \cap \Gamma,$$

then we have the following diagram of congruence subgroups, where the top map is an isomorphism and the vertical maps are inclusions:

$$\begin{tikzcd} \Gamma' \arrow[r, "x \mapsto \gamma_p^{-1} x \gamma_p"] \arrow[d] & \Gamma'' \arrow[d] \\ \Gamma & \Gamma \end{tikzcd}.$$

This then leads the the following diagram of modular curves, where α is the isomorphism induced by the conjugation above, and the vertical maps are projections:

$$\begin{tikzcd} X(\Gamma') \arrow[r, "\alpha"] \arrow[d, "\pi_1"'] & X(\Gamma'') \arrow[d, "\pi_2"'] \\ X(\Gamma) & X(\Gamma) \end{tikzcd}.$$

Thus we get a map $T_p(x) = \pi_2 \cdot \alpha \cdot \pi_1^{-1} \in \mathrm{Div}(X(\Gamma))$. This extends linearly to give a map

$$T_p : \mathrm{Div}(X(\Gamma)) \longrightarrow \mathrm{Div}(X(\Gamma)).$$

2. Picard Groups

Henceforth, we fix $\Gamma = \Gamma_0(N)$ for some $N \in \mathbb{N}$ and define $X_0(N) := X(\Gamma_0(N))$.

Definition 2.1. The *Picard group* of an algebraic curve X over a field K is defined to be

$$\mathrm{Pic}^0(X)_K := \mathrm{Div}^0(X/K)/K(X),$$

where $\mathrm{Div}^0(X/K)$ is the space of degree zero divisors and $K(X)$ is the space of principal divisors on $X(K)$.

Using the above, we see that the Hecke action defined on $\mathrm{Div}(X_0(N))$ descends to an action on the Picard group, as T_p preserves both $\mathrm{Div}^0(X_0(N))$ and $K(X)$ (regardless of whether the base field is $\mathbb{C}$ or $\mathbb{Q}$). The Picard group is an abelian variety of dimension g, where $g = g(X_0(N)) = \dim_{\mathbb{C}} S_2(\Gamma)$.

If $\phi : X \to Y$ is a map of algebraic curves, then we get a *pushforward map* $\phi_* : \mathrm{Pic}^0(X) \to \mathrm{Pic}^0(Y)$ induced by the map

$$\phi_*\left(\sum_x n_x x\right) = \sum_x n_x \phi(x).$$

Similarly, there is a *pullback map* $\phi^* : \mathrm{Pic}^0(Y) \to \mathrm{Pic}^0(X)$ given by

$$\phi^*\left(\sum_y n_y y\right) = \sum_y n_y \sum_{x \in \phi^{-1}(y)} e_x x,$$

where e_x is the ramification degree of ϕ at x. Accordingly, if $X = Y$ and ϕ is an endomorphism, then we get two endomorphisms on $\mathrm{Pic}^0(X)$. For suitably 'nice' maps $\phi : X \to Y$ of algebraic curves over K, we have the formula

$$\phi_* \circ \phi^* = \deg(\phi)$$

as endomorphisms on $\mathrm{Pic}^0(Y)$ (where the map $\deg(\phi)$ is scalar multiplication).

Remark: There is another way of thinking about the Picard group. Over $\mathbb{C}$, we can pick a specified basepoint x_0 and consider a point x on the curve as a path from x_0 to x. Then we consider the path integral

$$\int_{x_0}^{x} dz$$

as an element of $\Omega^1_{\mathrm{hol}}(X_0(N))^*$, that is, as an element of the dual space of holomorphic 1-forms on $X_0(N)$. From [DS05], Chapter 3, the space of holomorphic 1-forms on $X_0(N)$ is isomorphic to the space of degree two cusp forms for $\Gamma_0(N)$ via the map $f \mapsto f(z)dz$ for a weight 2 cusp form f. Accordingly, we can define a map

$$\mathrm{Div}(X_0(N)) \longrightarrow S_2(\Gamma_0(N))^*, \quad [x] \longmapsto \int_{x_0}^{x} dz.$$

The $\mathbb{Z}$-span (inside $S_2(\Gamma_0(N))^*$) of the integrals of the form $\int_{x_0}^{x} dz$ for $x \in X_0(N)$ is the homology group $\mathrm{H}^1(X_0(N), \mathbb{Z})$. *Abel's Theorem* then states that there is a canonical isomorphism

$$\mathrm{Jac}(X_0(N)) := S_2(\Gamma_0(N))^*/\mathrm{H}^1(X_0(N), \mathbb{Z}) \cong \mathrm{Pic}^0(X_0(N))$$

induced by the map on divisors given above (see [DS05], Chapter 6). This is another way of seeing that $\dim \mathrm{Pic}^0(X_0(N)) = \dim_{\mathbb{C}} S_2(\Gamma_0(N))$.

3. The Eichler-Shimura Relation

In the study of Galois representations of elliptic curves, we show that for $E/\mathbb{Q}$ an elliptic curve, we have that $\rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{p}})$ (for $\mathfrak{p}|p$ a prime of $\overline{\mathbb{Z}}$) satisfies the equation $X^2 - a_p(E)X + p = 0$ at all primes $p \nmid \ell N$. A similar result exists for the Galois representation attached to a modular curve. To show this, we exploit the Eichler-Shimura relation.

Recall: in showing the above, we note that, letting σ_p denote the Frobenius map induced by $x \mapsto x^p$,

$$|\overline{E}(\mathbb{F}_p)| = \ker(\sigma_p - 1) = \deg(\sigma_p - 1) = (\sigma_p - 1)_* \circ (\sigma_p - 1)^*$$

(as endomorphisms on $\mathrm{Pic}^0(\overline{E})$)

$$= p + 1 - (\sigma_{p,*} + \sigma_p^*),$$

so that as endomorphisms of $\mathrm{Pic}^0(\overline{E})$, $a_p = p + 1 - |\overline{E}(\mathbb{F}_p)|$ acts as $\sigma_{p,*} + \sigma_p^*$. The Eichler-Shimura relation says something similar for modular curves.

Henceforth (unless otherwise specified) we work exclusively over $\mathbb{Q}$ using the rational model of $X_0(N)$, and write $\mathrm{Pic}^0(X_0(N)) = \mathrm{Pic}^0(X_0(N))_{\mathbb{Q}}$, dropping the subscript. Reducing curves and maps modulo a prime p is technical and messy at the level of varieties; thus I'll just state some facts about the reduction of modular curves:

- For all $p \nmid N$, there is a non-singular projective curve $\overline{X_0(N)}$ (the *reduction of* $X_0(N)$ *at* p) and a surjective redution map

  $$X_0(N) \longrightarrow \overline{X_0(N)}.$$

  We say that $X_0(N)$ has *good reduction* at these primes. (Note that this is nothing other than base change of the integral model of $X_0(N)$ as a scheme over $\mathbb{Z}[1/N]$ to F_p).

- There is an operator $\overline{T_p}$ on $\overline{X_0(N)}$ making the following commute:

$$\begin{tikzcd} \mathrm{Pic}^0(X_0(N)) \arrow[r, "T_p"] \arrow[d] & \mathrm{Pic}^0(X_0(N)) \arrow[d] \\ \mathrm{Pic}^0(\overline{X_0(N)}) \arrow[r, "\overline{T_p}"] & \mathrm{Pic}^0(\overline{X_0(N)}) \end{tikzcd}.$$

Theorem 3.1 (Eichler-Shimura)**.** *Let σ_p be the Frobenius map on $\overline{X_0(N)}$. Then $\overline{T_p} = \sigma_{p,*} + \sigma_p^*$ as endomorphisms of* $\mathrm{Pic}^0(\overline{X_0(N)})$.

Proof. See [DS05], Chapter 8.7. As an outline: *Igusa's theorem* says that the reduction of $X_0(N)$ is compatible with its interpretation as a moduli space. Then we look at the action of T_p on this moduli space to obtain the result, examining the explicit action of the Hecke operators on elliptic curves, reducing mod p to find the link to Frobenius. □

4. The Galois Representation of a Modular Curve

We will need two further facts about compatibility of torsion in Picard groups. These are stated (but not proved) in [DS05], Chapter 9.5.

Facts: (i) The natural inclusion $\mathrm{Pic}^0(X_0(N)_{\mathbb{Q}})[\ell^n] \longrightarrow \mathrm{Pic}^0(X_0(N)_{\mathbb{C}})[\ell^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$ is an isomorphism.

(ii) For any prime $p \nmid N$, the natural surjection $\mathrm{Pic}^0(X_0(N)_{\mathbb{Q}})[\ell^n] \longrightarrow \mathrm{Pic}^0(\overline{X_0(N)})[\ell^n]$ is an isomorphism.

We are now in a position to define the Galois representation attached to a modular curve. In short, this will be the Tate module of the Picard group.

Definition 4.1. Define the *ℓ-adic Tate module* of $\mathrm{Pic}^0(X_0(N))$ to be the inverse limit

$$\mathrm{T}_\ell\mathrm{Pic}^0(X_0(N)) := \varprojlim_n \mathrm{Pic}^0(X_0(N))[\ell^n] \cong \mathbb{Z}_\ell^2 g,$$

where $g = \dim \mathrm{Pic}^0(X_0(N)) = \dim_{\mathbb{C}} S_2(\Gamma_0(N)) = g(X_0(N))$, and the last isomorphism follows from fact (i) above.

There is a natural action of $G_{\mathbb{Q}}$ on the modular curve $X_0(N)$; each $\sigma \in G_{\mathbb{Q}}$ preserves the curve as it is defined over $\mathbb{Q}$, so by acting on the co-ordinates of the points we obtain the desired action. This then gives a natural action on divisors via

$$\sigma \cdot \sum_x n_x[x] = \sum_x n_x[\sigma(x)].$$

It's easy to see that this action descends to an action on the Picard group, as for any $f \in \mathbb{Q}(X_0(N))$ we have $\sigma(d(f)) = d(\sigma(f))$ (that is, the action takes principal divisors to principal divisors). As the action is linear, this induces actions on $\mathrm{Pic}^0(X_0(N))[\ell^n]$ for any prime ℓ and integer n. This action commutes with the natural projection maps $\mathrm{Pic}^0(X_0(N))[\ell^m] \to \mathrm{Pic}^0(X_0(N))[\ell^n]$ for $m \geq n$, and accordingly we see that $G_{\mathbb{Q}}$ acts on $\mathrm{T}_\ell\mathrm{Pic}^0(X_0(N))$, giving rise to a Galois representation.

Definition 4.2. Define $\rho_{X_0(N),\ell}$ to be the ℓ-adic Galois representation attached to $X_0(N)$; that is, it is the continuous homomorphism

$$\rho_{X_0(N),\ell} : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(\mathrm{Ta}_\ell\mathrm{Pic}^0(X_0(N))) \cong \mathrm{GL}_{2g}(\mathbb{Z}_\ell)$$

determined by the Galois action (in the sense that $\rho_{X_0(N),\ell}(\sigma)(\alpha) := \sigma \cdot \alpha$ for all $\sigma \in G_{\mathbb{Q}}, \alpha \in \mathrm{Ta}_\ell\mathrm{Pic}^0(X_0(N))$).

We finish with a theorem that describes the image of Frobenius.

Theorem 4.3. *Let p be a prime not dividing ℓN.*

(i) The Galois representation $\rho_{X_0(N),\ell}$ is unramified at p.

(ii) Let $\mathfrak{p}$ be a prime of $\overline{\mathbb{Z}}$ lying above p, and let $\mathrm{Frob}_\mathfrak{p}$ be a Frobenius element at $\mathfrak{p}$. Then $\rho_{X_0(N),\ell}(\mathrm{Frob}_\mathfrak{p})$ satisfies the equation

$$X^2 - T_pX + p = 0.$$

Proof. To prove the first claim, fix some n and look at the commutative diagram

$$\begin{tikzcd} D_\mathfrak{p} \arrow[r, "\rho_{X_0(N),\ell}"] \arrow[d] & \mathrm{Aut}(\mathrm{Ta}_\ell\mathrm{Pic}^0(X_0(N))) \arrow[d] \\ G_{\mathbb{F}_p} \arrow[r, "\rho_{\overline{X_0(N)},\ell}"] & \mathrm{Aut}(\mathrm{Ta}_\ell\mathrm{Pic}^0(\overline{X_0(N)})) \end{tikzcd}.$$

Note that the inertia subgroup $I_\mathfrak{p} \leq D_\mathfrak{p}$ lives in the kernel of the left hand map by definition, whilst the right hand map is an isomorphism using fact (ii) from the start of the section. Thus $I_\mathfrak{p}$ is in the kernel of the top map, which is precisely the statement that $\rho_{X_0(N),\ell}$ is unramified at p.

For the second claim, we use the Eichler-Shimura relation. This restricts to ℓ-torsion to give a commutative diagram

$$\begin{tikzcd} \mathrm{Pic}^0(X_0(N))[\ell^n] \arrow[r, "T_p"] \arrow[d] & \mathrm{Pic}^0(X_0(N))[\ell^n] \arrow[d] \\ \mathrm{Pic}^0(\overline{X_0(N)})[\ell^n] \arrow[r, "\sigma_{p,*} + \sigma_p^*"] & \mathrm{Pic}^0\overline{X_0(N)})[\ell^n] \end{tikzcd}.$$

We can describe completely thepullback map on the Picard group induced by σ_p. As σ_p is a totally ramified map of degree p, we see that it acts on divisors via

$$\sigma_p^*([x]) = p[\sigma_p^{-1}(x)];$$

accordingly, we also have a commutative diagram

$$\begin{tikzcd} \mathrm{Pic}^0(X_0(N))[\ell^n] \arrow[r, "\rho_{X_0(N),\ell}(\mathrm{Frob}_\mathfrak{p}) + p\rho_{X_0(N),\ell}(\mathrm{Frob}_\mathfrak{p}^{-1})"] \arrow[d] & \mathrm{Pic}^0(X_0(N))[\ell^n] \arrow[d] \\ \mathrm{Pic}^0(\overline{X_0(N)})[\ell^n] \arrow[r, "\sigma_{p,*} + \sigma_p^*"] & \mathrm{Pic}^0\overline{X_0(N)})[\ell^n] \end{tikzcd}.$$

As the vertical arrows are isomorphisms, it follows that there is an equality of operators

$$\rho_{X_0(N),\ell}(\mathrm{Frob}_\mathfrak{p}) + p\rho_{X_0(N),\ell}(\mathrm{Frob}_\mathfrak{p}^{-1}) = T_p.$$

As this holds for all $\mathfrak{n}$, we obtain this equality as operators on $\mathrm{Ta}_\ell\mathrm{Pic}^0(X_0(N))$. Applying $\rho_{X_0(N),\ell}(\mathrm{Frob}_\mathfrak{p})$ to this gives the result. $\square$

References

[DS05] Fred Diamond and Jerry Shurman. *A First Course in Modular Forms*. Graduate Studies in Mathematics, 2005.

[Loe14] David Loeffler. Modular curves. Lecture notes, `http://www2.warwick.ac.uk/fac/sci/maths/people/staff/david_loeffler/teaching/modularcurves/lecture_notes.pdf`, 2014.