Galois representations associated to classical modular forms of weight at least 2: Deligne's theorem

Laia Amorós Carafí

Abstract

These are notes attached to the talk "Galois representations associated to classical modular forms of weight at least 2: Deligne's theorem" given at the 29th Barcelona Number Theory Seminar. The aim of these notes is to give a quick introduction to Galois representations of modular forms, gathering the essential results from different sources to be able to state Deligne's theorem and give a sketch of the proof in the case $k = 2$ (case due to Shimura).

The first section is intended to introduce the notion of Galois representation and give some examples. After that, we motivate why in the case of Galois representations of number fields it is necessary to have some kind of notion of compatible representations. In section 2 we introduce modular forms and Hecke operators, and give the results that will be needed later for our purpose. Section 3 is devoted to give a sketch of how one can attach a Galois representation to a modular form of weight $k = 2$. The last section is just a brief mention to the case $k > 2$.

Contents

1 Introduction to ℓ-adic Galois representations

We start by giving some basic definitions and examples. Then we will continue by introducing the notion of compatible systems of Galois representations. We will treat Galois representations with ground field a number field. In this case, Frobenius elements are defined, and one has the notion of *rational* ℓ-adic Galois representation: one for which their characteristic polynomials have rational coefficients (instead of merely ℓ-adic ones). Two representations corresponding to different primes are *compatible* if the characteristic polynomial of their Frobenius elements are the same (at least almost everywhere). Most of this section can be found in [Se68] and [Di05].

1.1 Definitions and examples

Let G be a profinite group and k a topological field. An **n-dimensional representation** of G is a continuous homomorphism of groups

$$\rho : G \to \mathrm{GL}_n(k).$$

The representation is called an **ℓ-adic representation** if $k \subseteq \overline{\mathbb{Q}}_\ell$. Let K be a field and denote by G_K the **absolute Galois group of** K, i.e., the Galois group of the separable closure of K. A representation of G_K over k is called a **Galois representation**.

A basic tool to provide examples of Galois representations is the *Tate module*. Let A denote some abelian group an let ℓ be some fixed prime. Denote by $A[\ell^n]$ the ℓ^n-torsion of A. One may construct an inverse system $\psi : A[\ell^{n+1}] \twoheadrightarrow A[\ell^n]$, and its inverse limit,

$$\mathrm{T}_\ell(A) := \varprojlim_n A[\ell^n],$$

is known as the **Tate module of A at ℓ**.

For the next examples, let K be a field of characteristic p, with p either a prime number or 0, and denote by $\overline{K}$ its separable closure. Let ℓ be some prime different from p.

Example 1.1 (The ℓ-adic cyclotomic character)**.** By choosing a compatible system of roots of unity μ_{ℓ^n}, we have an inverse system $\mu_{\ell^n}(\overline{K}) \twoheadrightarrow \mu_{\ell^{n-1}}(\overline{K})$ given by $x \mapsto x^\ell$, and we can define the **ℓ-adic Tate module of $\overline{K}^\times$**,

$$\mathrm{T}_\ell(\overline{K}^\times) = \varprojlim_n \mu_{\ell^n}(\overline{K}) \cong \varprojlim_n (\mathbb{Z}/\ell^n\mathbb{Z}) \cong \mathbb{Z}_\ell.$$

The absolute Galois group G_K acts compatibly on $\mu_{\ell^n}(\overline{K})$ for all n, so we can define a Galois representation:

$$\begin{array}{rccl} \chi_\ell : & G_K & \to & \mathrm{Aut}(\mathrm{T}_\ell(\overline{K}^\times)) \cong \mathbb{Z}_\ell^\times = \mathrm{GL}_1(\mathbb{Z}_\ell) \hookrightarrow \mathrm{GL}_1(\mathbb{Q}_\ell). \\ & \sigma & \mapsto & x \mapsto \sigma(x) \end{array}$$

It is called the **ℓ-adic cyclotomic character** (over $\overline{K}$).

Example 1.2 (Galois representations and elliptic curves)**.** Let E be an elliptic curve over K. Consider the inverse system $E[\ell^n] \twoheadrightarrow E[\ell^{n-1}]$ given by $P \mapsto \ell \cdot P$. The **ℓ-adic Tate module of E** is the resulting inverse limit $\mathrm{T}_\ell(E) = \varprojlim(E[\ell^n])$, which turns out to satisfy $\mathrm{T}_\ell(E) \cong \mathbb{Z}_\ell^2$ as

an abelian group. For each n, the field $\mathbb{Q}(E[\ell^n])$ is a Galois number field, giving a restriction map and an injection

$$\begin{array}{ccccc} G_{\mathbb{Q}} & \twoheadrightarrow & \mathrm{Gal}(\mathbb{Q}(E[\ell^n])/\mathbb{Q}) & \hookrightarrow & \mathrm{Aut}(E[\ell^n]). \\ \sigma & \mapsto & \sigma|_{\mathbb{Q}(E[\ell^n])} & & \end{array}$$

These maps are compatible in the sense that, for each n, the following diagram commutes

$$\begin{array}{ccc} & G_{\mathbb{Q}} & \\ \swarrow & & \searrow \\ \mathrm{Aut}(E[\ell^n]) & \longleftarrow & \mathrm{Aut}(E[\ell^{n+1}]) \end{array}$$

Choosing basis (P_n, Q_n) of $E[\ell^n]$ for each n, compatible in the sense that each basis is a lift of the predecessor, one can determine an isomorphism $\mathrm{Aut}(E[\ell^n]) \cong \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$, and these combine to give $\mathrm{Aut}(\mathrm{T}_\ell(E)) \xrightarrow{\sim} \mathrm{GL}_2(\mathbb{Z}_\ell)$. Since $G_{\mathbb{Q}}$ acts on $\mathrm{T}_\ell(E)$, we obtain a Galois representation

$$\rho_{E,\ell} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell) \subset \mathrm{GL}_2(\mathbb{Q}_\ell),$$

known as the **2-dimensional ℓ-adic Galois representation associated to** E.

Example 1.3 (Galois representations and abelian varieties)**.** Let A be an abelian variety of dimension g over K. Consider the inverse system $A[\ell^n] \twoheadrightarrow A[\ell^{n-1}]$ given by $P \mapsto \ell \cdot P$ and define the **ℓ-adic Tate module of** A, $\mathrm{T}_\ell(A) = \varprojlim A[\ell^n]$. One can compatibly identify $A[\ell^n]$ with $(\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$, yielding an isomorphism $\mathrm{T}_\ell(A) \cong (\mathbb{Z}_\ell)^{2g}$ of abelian groups.

In order to kill the torsion and make computations easier, one often considers the $\mathbb{Q}_\ell$-vector space $V_\ell(A) := \mathrm{T}_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong \mathbb{Q}_\ell^{2g}$. The Galois group G_K acts on $\mathrm{T}_\ell(A)$ and on $V_\ell(A)$. This yields to the **ℓ-adic Galois representation associated to** A,

$$\rho_{A,\ell} : G_K \to \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(A)) \cong \mathrm{GL}_{2g}(\mathbb{Q}_\ell).$$

Example 1.4 (Cohomology representations)**.** Let Y be an algebraic variety over K, and put $X = Y \otimes_K \overline{K}$. In order to associate Galois representations to X one uses the étale cohomology of Artin-Grothendieck. First attach to X the cohomology groups $\mathrm{H}^i(X_{et}, \mathbb{Z}/\ell^n\mathbb{Z})$ for each integer i, where X_{et} denotes the *étale site of* X or the *Grothendieck category* and $\mathbb{Z}/\ell^n\mathbb{Z}$ is thought as the "system of constant sheaves with coefficients in $\mathbb{Z}/\ell^n\mathbb{Z}$ ". Then one defines

$$\mathrm{H}^i(X, \mathbb{Z}_\ell) := \varprojlim \mathrm{H}^i(X_{et}, \mathbb{Z}/\ell^n\mathbb{Z}), \quad \text{and} \quad \mathrm{H}^i_\ell(X, \mathbb{Q}_\ell) := \mathrm{H}^i(X, \mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

The group $\mathrm{H}^i_\ell(X, \mathbb{Q}_\ell)$ is a $\mathbb{Q}_\ell$-vector space on which G_K acts (via the action of G_K on X). It is finite dimensional if $\mathrm{char}(K) = 0$ or if X is proper. One thus gets an ℓ-adic representation of G associated to $\mathrm{H}^i_\ell(X, \mathbb{Q}_\ell)$, the **$i$-th ℓ-adic Galois representation associated to** X, for $0 \leq i \leq 2\dim(X)$.

Remark 1.5. For abelian varieties, the first ℓ-adic cohomology group is the dual of the Tate module, and the higher cohomology groups are given by its exterior powers. For curves, the first cohomology group is the first cohomology group of its Jacobian.

Suppose K is a field of characteristic zero. Then one may find not one, but a family of representations $\{\rho_{E,\ell}\}_\ell$. Since they come from the same object, they might be expected to be *compatible* in some sense. We will discuss this in the next section.

1.2 ℓ-adic Galois representations of number fields. Compatible systems.

Let K be a number field and $\mathfrak{p}$ a finite place of K. We denote by $K_\mathfrak{p}$ its completion with respect to $\mathfrak{p}$, by $\mathcal{O}_{K_\mathfrak{p}} = \mathcal{O}_\mathfrak{p}$ the discrete valuation ring of $K_\mathfrak{p}$, by $\hat{\mathfrak{p}}$ (or just $\mathfrak{p}$) its valuation ideal, and by $\mathbb{F}_q = \mathbb{F}_{p^f} = \mathcal{O}_\mathfrak{p}/\hat{\mathfrak{p}}$ its residue field, with $\mathrm{N}(\mathfrak{p}) = q$. Denote by Σ_K the set of all finite places of K.

Let L/K be a finite Galois extension of number fields and $\mathfrak{P}/\mathfrak{p}/p$ prime ideals in these fields. The **decomposition group** of $\mathfrak{P}$ is defined as

$$D(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

We have the natural isomorphism $D(\mathfrak{P}/\mathfrak{p}) \cong \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{P})$. Whenever we have a Galois extension of local fields $L_\mathfrak{P}/K_\mathfrak{p}$, we can consider the reduction mod $\mathfrak{P}$ of all field automorphisms in $\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$, since each of them fixes the valuation rings. The reduction map

$$\pi(L_\mathfrak{P}/K_\mathfrak{p}) = \pi(\mathfrak{P}/\mathfrak{p}) \ : \ \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p}) \to \mathrm{Gal}(\mathbb{F}_{q'}/\mathbb{F}_q)$$

is surjective. A canonical generator for $\mathrm{Gal}(\mathbb{F}_{q'}/\mathbb{F}_q)$ is given by the (**arithmetic**) **Frobenius endomorphism**, also called **Frobenius element** $\mathrm{Frob}(L_\mathfrak{P}/K_\mathfrak{p}) = \mathrm{Frob}(\mathfrak{P}/\mathfrak{p})$, which is defined as $x \mapsto x^q$. The kernel of the reduction map is the **inertia group** $I(L_\mathfrak{P}/K_\mathfrak{p}) = I(\mathfrak{P}/\mathfrak{p})$, so that we have the exact sequence

$$0 \longrightarrow I(L_\mathfrak{P}/K_\mathfrak{p}) \longrightarrow \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p}) \overset{\pi(L_\mathfrak{P}/K_\mathfrak{p})}{\longrightarrow} \mathrm{Gal}(\mathbb{F}_{q'}/\mathbb{F}_q) \to 0.$$

The field extension $L_\mathfrak{P}/K_\mathfrak{p}$ (or the prime $\mathfrak{P}$ above $\mathfrak{p}$) is **unramified** if and only if $I(L_\mathfrak{P}/K_\mathfrak{p})$ is trivial. In this case the reduction map $\pi(\mathfrak{P}/\mathfrak{p})$ is an isomorphism, and we can consider $\mathrm{Frob}(L_\mathfrak{P}/\mathfrak{p})$ as an element of $D(\mathfrak{P}/\mathfrak{p})$. We have

$$\mathrm{Frob}(\sigma(\mathfrak{P}/\mathfrak{p})) = \sigma \circ \mathrm{Frob}(\mathfrak{P}/\mathfrak{p}) \circ \sigma^{-1},$$

so the Frobenius elements of the primes lying over $\mathfrak{p}$ form a conjugacy class in $\mathrm{Gal}(L/K)$. We will write $\mathrm{Frob}_\mathfrak{p}$ for either this conjugacy class or any element in it.

Now we pass to infinite Galois extensions. If L is an arbitrary algebraic extension of $\mathbb{Q}$, one defines Σ_L to be the projective limit of the sets Σ_{L_α}, where L_α ranges over the finite subextensions of $L/\mathbb{Q}$. Consider L/K an arbitrary Galois extension of the number field K and take $\mathfrak{P} \in \Sigma_L$. One defines $D_\mathfrak{P}, I_\mathfrak{P}$ and $\mathrm{Frob}_\mathfrak{P}$ as before. If $\mathfrak{p}$ is an unramified place of K and $\mathfrak{P}$ is a place of L extending $\mathfrak{p}$, we denote by $\mathrm{Frob}_\mathfrak{p}$ the conjugacy class of $\mathrm{Frob}_\mathfrak{P}$ in $G = \mathrm{Gal}(L/K)$.

Definition 1.6. Let $\rho : G_K \to \mathrm{Aut}(V)$ be an ℓ-adic Galois representation of K, and let $\mathfrak{p} \in \Sigma_K$. We say that ρ is **unramified** at $\mathfrak{p}$ if $I_\mathfrak{P} \subset \ker\rho$ for any place $\mathfrak{P}$ of $\overline{K}$ extending $\mathfrak{p}$.

If the representation ρ is unramified at $\mathfrak{p}$, then the restriction of ρ to $D_\mathfrak{P}$ factors through $D_\mathfrak{P}/I_\mathfrak{P}$ for any $\mathfrak{P} \mid \mathfrak{p}$. Hence $\rho(\mathrm{Frob}_\mathfrak{P}) \in \mathrm{Aut}(V)$ is defined, and we call $\rho(\mathrm{Frob}_\mathfrak{P})$ the **Frobenius of $\mathfrak{P}$ in the representation** ρ, an we denote it by $\mathrm{Frob}_{\mathfrak{P},\rho}$ (or $\mathrm{Frob}_\mathfrak{P}$). The conjugacy class of $\mathrm{Frob}_{\mathfrak{P},\rho}$ in $\mathrm{Aut}(V)$ depend only on $\mathfrak{p}$; it is denoted by $\mathrm{Frob}_{\mathfrak{p},\rho}$ (or $\mathrm{Frob}_\mathfrak{p}$). If L/K is the extension of K corresponding to $H = \mathrm{Ker}(\rho)$, then ρ is unramified at $\mathfrak{p}$ if and only if $\mathfrak{p}$ is unramified in L/K.

Recall the **Frobenius automorphism in characteristic** p,

$$\sigma_p : \mathbb{F}_q \to \mathbb{F}_q, \quad x \mapsto x^q.$$

The action of $\mathrm{Frob}_{\mathfrak{p}}$ on a number field K restricted to $\mathcal{O}_K$ descends to $\mathbb{F}_q$, where it is the action of the Frobenius automorphism σ_p. When ρ is unramified, making $I_{\mathfrak{p}}$ trivial, $\mathrm{Frob}_{\mathfrak{p}}$ is unique.

Let ρ be an ℓ-adic Galois representation of a number field K. If $\mathfrak{p} \in \Sigma_K$ is unramified with respect to ρ, we define the **characteristic polynomial of Frobenius of ρ at $\mathfrak{p}$ as**

$$P_{\mathfrak{p},\rho}(T) := \det(1 - T\ \mathrm{Frob}_{\mathfrak{p},\rho}) \in \mathbb{Q}_\ell[T].$$

Definition 1.7. An ℓ-adic representation ρ is said to be **rational** (resp. **integral**) if there exists a finite subset $S \subset \Sigma_K$ such that:

(a) any element of $\Sigma_K - S$ is unramified with respect to ρ,

(b) if $\mathfrak{p} \notin S$, the coefficients of $P_{\mathfrak{p},\rho}(T)$ belong to $\mathbb{Q}$ (resp. to $\mathbb{Z}$).

We will consider from now on *rational* ℓ-adic representations, so we will be able to compare different rational representations (even over different completions) just by comparing those polynomials.

Examples 1.8. The ℓ-adic representations of G_K given in examples 1,2,3 are integral representations. In the first example one can take as S the set S_ℓ of places ν in K such that $p_\nu = \ell$. The corresponding Frobenius is $\mathrm{N}(\nu)$, the norm of ν.

In examples 2 and 3 one can take for S the union of S_ℓ and the set S_A, where A has bad reduction. The fact that the corresponding Frobenius has an integral characteristic polynomial (which is independent of ℓ) is a consequence of Weil's results on endomorphisms of abelian varieties.

Example 4 is true if $K = \overline{\mathbb{F}}_q$ (Weil's conjectures), and it is a well known open question in general.

Definition 1.9. Let ℓ' be a prime, and consider an ℓ'-adic Galois representation ρ' of G_K. Assume that ρ and ρ' are rational. Then ρ and ρ' are said to be **compatible** if there exists a finite subset $S \subset \Sigma_K$ such that ρ and ρ' are unramified outside S and

$$P_{\mathfrak{p},\rho}(T) = P_{\mathfrak{p},\rho'}(T), \quad \text{for all } \mathfrak{p} \in \Sigma_K - S.$$

(In other words, the characteristic polynomials of the Frobenius elements are the same for ρ and ρ' for almost all $\mathfrak{p}$).

If $\rho : G_K \to \mathrm{Aut}(V)$ is a rational ℓ-adic Galois representation, then V has a composition series $0 = V_q \subset \ldots \subset V_1 \subset V_0 = V$ of ρ-invariant subspaces with V_i/V_{i+1} simple. The ℓ'-adic representation ρ' of G_K defined by $V' = \sum_{i=0}^{q-1} V_i/V_{i+1}$ is semi-simple, rational, and compatible with ρ. It is called the **semi-simplification** of ρ.

Theorem 1.10. *There exists a unique (up to isomorphism) rational, semisimple ℓ-adic representation compatible with ρ.*

Let's finally define a **compatible system of rational representations** of G_K as a collection $\{\rho_\ell\}_\ell$ such that any two ρ_ℓ and $\rho_{\ell'}$ are compatible for all primes ℓ, ℓ'. The system $\{\rho_\ell\}_\ell$ is said to be **strictly compatible** if there exists a finite subset $S \subset \Sigma_K$ such that:

(a) If we let $S_\ell = \{\nu \mid p_\nu = \ell\}$, then for every $\nu \notin S \cup S_{\ell'}$ the representation ρ_ℓ is unramified at ν and $P_{\nu,\rho_\ell}(T)$ has rational coefficients.

(b) $P_{\nu,\rho_\ell}(T) = P_{\nu,\rho'_\ell}(T)$ if $\nu \notin S \cup S_\ell \cup S_{\ell'}$.

When a system $\{\rho_\ell\}_\ell$ is strictly compatible, there is a smallest finite set S having properties (a) and (b). We call it the **exceptional set** of the system.

The idea behind this notion is that a compatible system of representations does not depend on ℓ at the end. We are constructing a bunch of representations, one for each ℓ, of some Galois group G to end up with an object, which is the same for almost all representations, namely the characteristic polynomial.

Examples 1.11. The systems of ℓ-adic representations given in examples 1,2 and 3 are strictly compatible. The exceptional set of the first one is empty. The exceptional set of example 2 (resp. 3) is the set of places where the elliptic curve (resp. abelian variety) has bad reduction.

We can summarise the results that we have seen until here for the 2 first examples.

Theorem 1.12. *Let χ_ℓ be the cyclotomic character over $\overline{\mathbb{Q}}$. It is a 1-dimensional global Galois representation, which is unramified at all primes $p \neq \ell$ and is characterised there by*

$$\chi_\ell(\mathrm{Frob}_p) = p.$$

Theorem 1.13. *Let ℓ be a prime and let E be an elliptic curve over $\mathbb{Q}$ with conductor N. The Galois representation*

$$\rho_{E,\ell} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Q}_\ell)$$

is unramified at every prime $p \nmid \ell N$. For any such p, let $\mathfrak{p} \subseteq \overline{\mathbb{Z}}$ be any maximal ideal over p. Then the characteristic equation of $\rho_{E,\ell}(\mathrm{Frob}_\mathfrak{p})$ is

$$x^2 - a_p(E)x + p = 0, \quad \text{where } a_p = p + 1 - \#E(\mathbb{F}_p)$$

The Galois representation is irreducible.

Proof. **Unramified:** Let $p \nmid \ell N$ and let $\mathfrak{p}$ lie over p. There is a commutative diagram

$$\begin{array}{ccc} D_\mathfrak{p} & \xrightarrow{\quad f \quad} & \mathrm{Aut}(E[\ell^n]) \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle g'} \\ G_{\mathbb{F}_\mathfrak{p}} & \xrightarrow[\quad f' \quad]{} & \mathrm{Aut}(\widetilde{E}[\ell^n]) \end{array}$$

where f restricts the action of $G_{\mathbb{Q}}$ on E to $D_\mathfrak{p}$, and f' is given by the action of $G_{\mathbb{F}_p}$ on $\widetilde{E}$. The inertia group $I_\mathfrak{p}$ is contained in $\ker(f' \circ g)$. The map g' is an isomorphism, since the condition $p \nmid \ell N$ means that E has good reduction at p and the reduction preserves ℓ^n-torsion structure. Consequently $I_\mathfrak{p}$ is contained in the kernel of f. Since n is arbitrary, this means that $I_\mathfrak{p} \subset \ker\rho_{E,\ell}$, i.e., $\rho_{E,\ell}$ is unramified at every $p \nmid N\ell$.

Characteristic polynomial: We need to compute $\det\rho_{E,\ell}(\mathrm{Frob}_\mathfrak{p})$ and $\mathrm{tr}\rho_{E,\ell}(\mathrm{Frob}_\mathfrak{p})$ for $p \nmid \ell N$. For the determinant, let $\rho_n : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ be the nth entry of $\rho_{E,\ell}$ for $n \in \mathbb{Z}^+$.

The Weil pairing shows that the action of $\sigma \in G_{\mathbb{Q}}$ on the root of unity μ_{ℓ^n} is given by the determinant, but by definition we also have

$$\mu_{\ell^n}^{\sigma} = \mu_{\ell^n}^{det\rho_n(\sigma)} = \mu_{\ell^n}^{\chi_{\ell,n}(\sigma)}.$$

That is, $\det\rho_n(\sigma) = \chi_{\ell,n}(\sigma)$ in $(\mathbb{Z}/\ell^n\mathbb{Z})^*$ for all n, so $\det\rho_{E,\ell}(\sigma) = \chi_\ell(\sigma)$ in $\mathbb{Z}_\ell^*$. In particular,

$$\det\rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{p}}) = p.$$

For the trace, let $A = \rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{p}})$ and recall that a square matrix satisfies its characteristic polynomial. Since $\det A = p$, the characteristic equation is $A^2 - \mathrm{tr}\, A + p\,\mathrm{I}_2 = 0$, where $I_2 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. So $\mathrm{tr}\, A = A + pA^{-1}$. We know that [1] $\sigma_{p,*} + \sigma_p^* = a_p(E)$, and that $\sigma_{p,*}$ acts as σ_p and σ_p^* acts as $p\sigma_p^{-1}$. The previous diagram shows that σ_p acts on $\widetilde{E}[\ell^n]$ as $\mathrm{Frob}_{\mathfrak{p}}$ acts on $E[\ell^n]$. That is,

$$A + pA^{-1} \equiv a_p(E)\,\mathrm{I}_2 \pmod{\ell^n}, \quad \forall n.$$

Since this holds for all n, it follows that $\mathrm{tr}\, A = a_p(E)$, that is,

$$\mathrm{tr}\,\rho_{E,\ell}(\mathrm{frob}_{\mathfrak{p}}) = a_p(E).$$

Irreducible: Too difficult to prove in these notes. □

2 Introduction to modular forms

In this section we introduce some notation and results on modular forms that we will use in the following sections. We will state the moduli interpretation for elliptic curves, and we will introduce two important operators, the diamond operators $\langle d \rangle$ and the Hecke operators T_p, which play a crucial role in what follows. All the definitions and results of this section can be found in [Di05].

2.1 Definitions and examples

To begin with, recall that the **modular group** $\mathrm{SL}_2(\mathbb{Z})$ acts on the **upper half plane** $\mathfrak{h} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) \geq 0\}$ as

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(\tau) = \frac{a\tau + b}{c\tau + d}, \quad \tau \in \mathfrak{h}.$$

[1] Let C be a projective curve over $\mathbb{F}_p$. Then the Frobenius automorphism defines a morphism from C to itself, since $C^{\sigma_p} = C$. The Frobenius map on C is

$$\sigma_p([x_0, \ldots, x_n]) = [x_0^p, \ldots, x_n^p].$$

The forward map of σ_p on C acts on the divisors of C as

$$\sigma_{p,*}(P) = \sigma_p(P),$$

and the reverse induced map acts as

$$\sigma_p^*(P) = p(\sigma_p^{-1}(P)).$$

Definition 2.1. Let k be an integer. A meromorphic function $f : \mathfrak{h} \to \mathbb{C}$ is **weakly modular of weight** k if

$$f(\gamma(\tau)) = (c\tau + d)^k f(\tau), \quad \text{for } \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \text{ and } \tau \in \mathfrak{h}.$$

An holomorphic weakly modular function f of weight k has a Fourier expansion at ∞

$$f(\tau) = \sum_{n=0}^{\infty} a_n q^n, \quad q = \mathrm{e}^{2\pi i \tau}.$$

An holomorphic weakly modular function $f : \mathfrak{h} \to \mathbb{C}$ is called a **modular form of weight** k if moreover f is holomorphic at ∞. If $a_0 = 0$ then f is called a **cusp form of weight** k. The set of modular forms of weight k is denoted by $M_k(\mathrm{SL}_2(\mathbb{Z}))$. It is in fact a finite-dimensional vector space over $\mathbb{C}$, and the sum

$$M(\mathrm{SL}_2(\mathbb{Z})) = \bigoplus_{k \in \mathbb{Z}} M_k(\mathrm{SL}_2(\mathbb{Z}))$$

forms a graded ring. The set of cusp forms is denoted by $S_k(\mathrm{SL}_2(\mathbb{Z}))$. It forms a vector subspace of $M_k(\mathrm{SL}_2(\mathbb{Z}))$ and the graded ring

$$S(\mathrm{SL}_2(\mathbb{Z})) = \bigoplus_{k \in \mathbb{Z}} S_k(\mathrm{SL}_2(\mathbb{Z}))$$

is an ideal in $M(\mathrm{SL}_2(\mathbb{Z}))$.

Example 2.2 (Trivial examples)**.** The zero function on $\mathfrak{h}$ is a modular form of every weight, and every constant function on $\mathfrak{h}$ is a modular form of weight 0.

Example 2.3 (Eisenstein series)**.** For nontrivial examples of modular forms, let $k \geq 2$ be an even integer. Define the **Eisenstein series of weight** k to be a 2-dimensional analog of the Riemann zeta function $\zeta(k) = \sum_{d=1}^{\infty} 1/d^k$,

$$G_k(\tau) = \sum_{(c,d) \neq (0,0)} \frac{1}{(c\tau + d)^k}, \quad \tau \in \mathfrak{h}.$$

It is a modular form of weight k, and its Fourier expansion is

$$G_k(\tau) = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n,$$

where the coefficient $\sigma_{k-1}(n)$ is the function $\sigma_{k-1}(n) = \sum_{m|n, m>0} m^{k-1}$.

Example 2.4 (Discriminant function)**.** Let $g_2(\tau) = 60G_4(\tau)$ and $g_3(\tau) = 140G_6(\tau)$. Define the **discriminant function** $\Delta : \mathfrak{h} \to \mathbb{C}$ as

$$\Delta(\tau) = (g_2(\tau))^3 - 27(g_3(\tau))^2.$$

Then Δ is weakly modular of weight 12 and holomorphic on $\mathfrak{h}$, and $a_0 = 0$, so it is a cusp form.

Replacing the modular group $\mathrm{SL}_2(\mathbb{Z})$ by a subgroup Γ generalises the notion of weak modularity. Let N be a positive integer. The **principal congruence subgroup of level** N is

$$\Gamma(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod{N} \right\}.$$

A subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ is a **congruence subgroup** if $\Gamma(N) \subset \Gamma$ for some $N \in \mathbb{Z}^+$, in which case Γ is a congruence subgroup of **level** N.

Besides the principal congruence subgroups, the most important congruence subgroups are

$$\Gamma_0(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \pmod{N} \right\}$$

and

$$\Gamma_1(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \pmod{N} \right\},$$

which satisfy $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$.

Adapting the previous definitions of modular and cusp forms, we can define the notion of **modular** (or **cusp**) **form of weight** k **with respect to a congruence subgroup** Γ, and denote them by $M_k(\Gamma)$ and $S_k(\Gamma)$, respectively. For a Dirichlet character χ modulo N, define the χ**-eigenspace** of $M_k(\Gamma_1(N))$ as

$$M_k(N, \chi) = \{ f \in M_k(\Gamma_1(N)) : f[\gamma]_k = \chi(d_\gamma) f, \quad \text{for all } \gamma \in \Gamma_1(N) \},$$

and denote by $S_k(N, \chi)$ the corresponding subspace of cusp forms.

2.2 Modular curves, moduli spaces and modularity

A **complex torus** is a quotient of the complex plane by a lattice,

$$\mathbb{C}/\Lambda = \{ z + \Lambda : z \in \mathbb{C} \}.$$

A nonzero holomorphic homomorphism between two complex tori is called an **isogeny**.

For any positive integer N and any lattice Λ, the *multiply-by-N map*

$$\begin{array}{rccc} [N]: & \mathbb{C}/\Lambda & \to & \mathbb{C}/\Lambda \\ & z + \Lambda & \mapsto & Nz + \Lambda. \end{array}$$

is an isogeny. Its kernel is the set of N-torsion points of $\mathbb{C}/\Lambda$, a subgroup isomorphic to $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. If we denote the torus $\mathbb{C}/\Lambda$ by E, this subgroup is denoted by $E[N]$.

Let C be a cyclic subgroup of $E[N]$. As a set, C forms a superlattice of Λ. The *cyclic quotient map*

$$\begin{array}{rccc} \pi: & \mathbb{C}/\Lambda & \to & \mathbb{C}/C \\ & z + \Lambda & \mapsto & NZ + C \end{array}$$

is an isogeny with kernel C.

Every isogeny $\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ is a composition of the examples already given:

$$\varphi : \mathbb{C}/\Lambda \xrightarrow{[n]} \mathbb{C}/\Lambda \xrightarrow{\pi} \mathbb{C}/nK \xrightarrow{\sim} \mathbb{C}/\Lambda',$$

where K denotes the kernel of φ and $K \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/nn'\mathbb{Z}$.

The **dual isogeny** of φ is denoted by $\hat{\varphi} : \mathbb{C}/\Lambda' \to \mathbb{C}/\Lambda$ and satisfies

$$\hat{\varphi} \circ \varphi = \varphi \circ \hat{\varphi} = [\deg(\varphi)] = [\deg(\hat{\varphi})].$$

A complex torus $\mathbb{C}/\Lambda$ can also be viewed as an **elliptic curve**, denoted by E, using the Weierstrass $\mathcal{P}$-function.

Two elliptic curves $\mathbb{C}/\Lambda$ and $\mathbb{C}/\Lambda'$ are holomorphically group-isomorphic if and only if $m\Lambda = \Lambda'$ for some $m \in \mathbb{C}$. Viewing to such curves as equivalent gives a quotient set of equivalence classes of complex elliptic curves. Similarly, two points $\tau, \tau' \in \mathfrak{h}$ are considered equivalent if and only it $\gamma(\tau) = \tau'$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Consider the resulting quotient as well. Then there is a bijection from the first quotient to the second. That is, the equivalence classes of points in the upper half plane under the action of the modular group are described by the isomorphism classes of complex elliptic curves.

Let N be a positive integer. An **enhanced elliptic curve for** $\Gamma_0(N)$ is an ordered pair (E, C) where E is a complex elliptic curve and C is a cyclic subgroup of E of order N. Two such pairs (E, C) and (E', C') are **equivalent**, $(E, C) \sim (E', C')$, if some isomorphism $E \xrightarrow{\sim} E'$ takes C to C'. The set of equivalence classes is denoted by

$$\mathrm{S}_0(N) = \{\text{enhanced elliptic curves for } \Gamma_0(N)\}/\sim .$$

An **enhanced elliptic curve for** $\Gamma_1(N)$ is a pair (E, Q) where E is a complex elliptic curve and Q is a point of E of order N. Two such pairs (E, Q) and (E', Q') are **equivalent** if some isomorphism $E \xrightarrow{\sim} E'$ takes Q to Q'. The set of equivalence classes is denoted by

$$\mathrm{S}_1(N) = \{\text{enhanced elliptic curves for } \Gamma_1(N)\}/\sim .$$

For any congruence subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ acting on $\mathfrak{h}$ form the left, the **modular curve** $Y(\Gamma)$ is defined as the quotient space of orbits under Γ, $Y(\Gamma) = \Gamma \setminus \mathfrak{h}$. The modular curves for $\Gamma_0(N), \Gamma_1(N)$ and $\Gamma(N)$ are denoted

$$Y_0(N) = \Gamma_0(N) \setminus \mathfrak{h}, \quad Y_1(N) = \Gamma_1(N) \setminus \mathfrak{h}, \quad Y(N) = \Gamma(N) \setminus \mathfrak{h}.$$

It turns out that modular curves are Riemann surfaces and they can be compactified. The resulting compact Riemann surfaces for $Y_0(N), Y_1(N)$ and $Y(N)$ are denoted by $X_0(N), X_1(N)$ and $X(N)$.

Theorem 2.5. *Let N be a positive integer.*

(a) *The moduli space for $\Gamma_0(N)$ is*

$$S_0(N) = \{[E_\tau, \langle\ 1/N + \Lambda_\tau\rangle] : \tau \in \mathfrak{h}\}.$$

Two points $[E_\tau, \langle\ 1/N + \Lambda_\tau\rangle]$ and $[E_{\tau'}, \langle\ 1/N + \Lambda_{\tau'}\rangle]$ are equal if and only if $\Gamma_0(N)\tau = \Gamma_0(N)\tau'$. Thus there is a bijection

$$\begin{array}{rcl} \mathrm{S}_0(N) & \xrightarrow{\sim} & Y_0(N) \\ [\mathbb{C}/\Lambda_\tau, \langle 1/N + \Lambda_\tau\rangle] & \mapsto & \Gamma_0(N)\tau. \end{array}$$

(b) *The moduli space for* $\Gamma_1(N)$ *is*

$$S_1(N) = \{[E_\tau,\ 1/N + \Lambda_\tau] : \tau \in \mathfrak{h}\}.$$

Two points $[E_\tau,\ 1/N+\Lambda_\tau]$ *and* $[E_{\tau'},\ 1/N+\Lambda_{\tau'}]$ *are equal if and only if* $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$. *Thus there is a bijection*

$$\begin{array}{rcl} \mathrm{S}_1(N) & \xrightarrow{\sim} & Y_1(N) \\ [\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau] & \mapsto & \Gamma_1(N)\tau. \end{array}$$

Proof. [Di05] pg. 38. □

Every elliptic curve E has a well defined **modular invariant**, denoted by $j(E)$. Complex analytically, the Modularity Theorem says that all elliptic curves with rational invariants come from such modular curves via holomorphic maps, viewing both kinds of curves as compact Riemann surfaces.

Theorem 2.6. *Let* E *be a complex elliptic curve with* $j(E) \in \mathbb{Q}$. *Then for some positive integer* N *there exists a surjective holomorphic function of compact Riemann surfaces*

$$X_0(N) \to E.$$

2.3 Hecke operators and their modular interpretation

Definition 2.7. For congruence subgroups $\Gamma_1, \Gamma_2 \subset \mathrm{SL}_2(\mathbb{Z})$ and $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$, the **weight** k $\Gamma_1\alpha\Gamma_2$ **operator** takes functions $f \in M_k(\Gamma_1)$ to

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

where $\{\beta_j\}$ are orbit representatives.

The map

$$\begin{array}{rcl} \Gamma_0(N) & \to & (\mathbb{Z}/N\mathbb{Z})^* \\ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) & \mapsto & d \pmod N \end{array}$$

is a surjective homomorphism with kernel $\Gamma_1(N)$. This shows that $\Gamma_1(N)$ is normal in $\Gamma_0(N)$ and induces an isomorphism

$$\begin{array}{rcl} \Gamma_0(N)/\Gamma_1(N) & \xrightarrow{\sim} & (\mathbb{Z}/N\mathbb{Z})^* \\ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) & \longmapsto & d \pmod N. \end{array}$$

To define the first type of operator, take any $\alpha \in \Gamma_0(N)$, set $\Gamma_1 = \Gamma_2 = \Gamma_1(N)$, and consider the weight-k double coset operator $[\Gamma_1\alpha\Gamma_2]_k$. Since $\Gamma_1(N) \triangleleft \Gamma_0(N)$, the operator is an isomorphism

$$f[\Gamma_1\alpha\Gamma_2]_k = f[\alpha]_k, \quad \alpha \in \Gamma_0(N).$$

Thus the group $\Gamma_0(N)$ acts on $M_k(\Gamma_1(N))$, and since its subgroup $\Gamma_1(N)$ acts trivially, this is really an action of the quotient $(\mathbb{Z}/N\mathbb{Z})^*$. The action of $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, determined by $d \pmod N$ and denoted by $\langle d \rangle$, is

$$\begin{array}{rccl} \langle d \rangle : & M_k(\Gamma_1(N)) & \to & \mathcal{M}_k(\Gamma_1(N)) \\ & f & \mapsto & \langle d \rangle f = f[\alpha]_k, \end{array}$$

for any $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ with $\delta \equiv d \pmod N$. It is called a **diamond operator**.

The second type of operator is also a weight k double coset operator $[\Gamma_1 \alpha \Gamma_2]_k$, where again $\Gamma_1 = \Gamma_2 = \Gamma_1(N)$, but now $\alpha = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$ with p prime. This operator is called **Hecke operator** and denoted by T_p. Thus, T_p is given by

$$\begin{array}{rccl} T_p: & \mathcal{M}_k(\Gamma_1(N)) & \to & \mathcal{M} \\ & f & \mapsto & T_p f = f[\Gamma_1(N)\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)\Gamma_1(N)]_k. \end{array}$$

The double coset here is

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

The modular curve interpretation of T_p is

$$\begin{array}{rccl} T_p: & \mathrm{Div}(X_1(N)) & \to & \mathrm{Div}(X_1(N)) \\ & \Gamma_1(N)\tau & \mapsto & \sum_j \Gamma_1(N)\beta_j(\tau), \end{array}$$

with the matrices β_j taken as

$$\beta_j = \left(\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right) \text{ for } 0 \le j < p, \quad \beta_\infty = \left(\begin{smallmatrix} m & n \\ N & p \end{smallmatrix}\right)\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) \text{ if } p \nmid N, \text{ where } mp - nN = 1.$$

The moduli space interpretation is

$$\begin{array}{rccl} T_p: & \mathrm{Div}(\mathrm{S}_1(N)) & \to & \mathrm{Div}(\mathrm{S}_1(N)) \\ & [E, Q] & \mapsto & \sum_C [E/C, Q + C], \end{array}$$

where the sum is taken over all order p subgroups $C \subset E$ such that $C \cap \langle Q \rangle = \{0_E\}$.

3 Galois representations and modular forms of weight $k = 2$

In this section we relate the world of Galois representations and the one of modular forms (of weight 2). We will sketch how one can associate a Galois representations (with certain properties) to a (normalised, cuspidal) modular form of weight 2. In this section we mostly follow the proof done in [Di05].

3.1 The Eichler-Shimura Relation

Here we give a description of the Hecke operator T_p at the level of Picard groups of reduced modular curves, with $p \nmid N$,

$$\widetilde{T}_p : \mathrm{Pic}^0(\widetilde{X}_1(N)) \to \mathrm{Pic}^0(\widetilde{X}_1(N)).$$

The resulting description of $\widetilde{T}_p$ is called the Eichler-Shimura relation.

Denote by

$$\sigma_p : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p, \quad x \mapsto x^p$$

the **Frobenius map on** $\overline{\mathbb{F}}_p$. We can extend it to a Frobenius map on a projective curve C over $\overline{\mathbb{F}}_p$,

$$\sigma_p : C \to C^{\sigma_p}, \quad [x_0, \ldots, x_n] \mapsto [x_0^p, \ldots, x_n^p].$$

This map acts on the divisors as

$$\sigma_{p,*} : (P) \mapsto (\sigma_p(P)).$$

Since σ_p is bijective and is ramified everywhere with ramification degree p, the reverse induced map acts on divisors of C as

$$\sigma_p^* : (P) \mapsto p(\sigma_p^{-1}(P)).$$

Proposition 3.1. *Let E be an elliptic curve over $\mathbb{Q}$ and let p be a prime such that E has good reduction modulo p. Let $\sigma_{p,*}$ and σ_p^* be the forward and reverse maps of $\mathrm{Pic}^0(\widetilde{E})$ induced by σ_p. Then*

$$a_p(E) = \sigma_{p,*} + \sigma_p^*$$

as endomorphisms of $\mathrm{Pic}^0(\widetilde{E})$ (where the left side means multiplication by $a_p(E)$).

Proof. [Di05], pg. 325. □

The Diamond operator $\langle d \rangle$ on $X_1(N)$ reduces modulo p and passes to Picard groups to give a commutative diagram

$$\begin{array}{ccc} \mathrm{Pic}^0(X_1(N)) & \xrightarrow{\langle d \rangle_*} & \mathrm{Pic}^0(X_1(N)) \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(\widetilde{X}_1(N)) & \xrightarrow{\widetilde{\langle d \rangle}_*} & \mathrm{Pic}^0(\widetilde{X}_1(N)). \end{array}$$

For the Hecke operator T_p on $X_1(N)$ we want a similar diagram

$$\begin{array}{ccc} \mathrm{Pic}^0(X_1(N)) & \xrightarrow{T_p} & \mathrm{Pic}^0(X_1(N)) \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(\widetilde{X}_1(N)) & \xrightarrow{\widetilde{T}_p} & \mathrm{Pic}^0(\widetilde{X}_1(N)). \end{array}$$

We want to compute the reduction of T_p. The expression for $\widetilde{T}_p$ is what is known as the **Eichler-Shimura relation**.

Theorem 3.2 (Eichler-Shimura Relation)**.** *Let $p \nmid N$. The following diagram commutes*

$$\begin{array}{ccc} \mathrm{Pic}^0(X_1(N)) & \xrightarrow{T_p} & \mathrm{Pic}^0(X_1(N)) \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(\widetilde{X}_1(N)) & \xrightarrow{\sigma_{p,*} + \widetilde{\langle p \rangle} \sigma_p^*} & \mathrm{Pic}^0(\widetilde{X}_1(N)). \end{array}$$

Proof. [Di05], pg. 354. □

3.2 Shimura's construction

We will see in this section that one may associate a 2-dimensional Galois representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to each normalised cuspidal eigenform. The following theorem is due to Shimura for $k = 2$ and due to Deligne for $k \geq 2$.

Theorem 3.3. *Let $f \in S_k(N, \chi)$ be a normalised eigenform with number field K_f. Let ℓ be prime. For each maximal ideal λ of $\mathcal{O}_{K_f}$ lying over ℓ there is an irreducible 2-dimensional Galois representation*

$$\rho_{f,\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_{f,\lambda}).$$

This representation is unramified at all primes $p \nmid \ell N$. For any $\mathfrak{p} \subset \overline{\mathbb{Z}}$ lying over such p, the characteristic equation of $\rho_{f,\lambda}(\mathrm{Frob}_{\mathfrak{p}})$ is

$$x^2 - a_p(f)x + \chi(p)p^{k-1} = 0.$$

We will sketch here the construction of $\rho_{f,\lambda}$ in the case of weight $k = 2$. Let N be a positive integer and let ℓ be a prime. The modular curve $X_1(N)$ is a projective nonsingular algebraic curve over $\mathbb{Q}$. Let g denote its genus. The curve $X_1(N)_{\mathbb{C}}$ over $\mathbb{C}$ defined by the same equations can also be viewed as a compact Riemann surface. The Jacobian of the modular curve is a g-dimensional complex torus

$$J_1(N) = \mathrm{Jac}(X_1(N)_{\mathbb{C}}) \stackrel{def}{=} S_2(\Gamma_1(N))^{\wedge}/H_1(X_1(N)_{\mathbb{C}}, \mathbb{Z}) \cong \mathbb{C}^g/\Lambda_g.$$

The **Picard group** of $X_1(N)$ is the abelian group of divisor classes on the points of $X_1(N)$,

$$\mathrm{Pic}^0(X_1(N)) = \mathrm{Div}^0(X_1(N))/\mathrm{DivP}(X_1(N)).$$

We can think of $\mathrm{Pic}^0(X_1(N))$ as a subgroup of $\mathrm{Pic}^0(X_1(N)_{\mathbb{C}})$, and using *Abel's theorem* we have a natural isomorphism

$$\mathrm{Pic}^0(X_1(N)_{\mathbb{C}}) \cong \mathrm{Jac}(X_1(N)_{\mathbb{C}}).$$

Thus, there is an inclusion of ℓ^n-torsion,

$$i_n : \mathrm{Pic}^0(X_1(N))[\ell^n] \hookrightarrow \mathrm{Pic}^0(X_1(N)_{\mathbb{C}})[\ell^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z})^{2g}.$$

Denote by $\widetilde{X}_1(N)$ the reduction of $X_1(N)$ at p. By *Igusa's theorem* we know that $X_1(N)$ has good reduction at primes $p \nmid N$, so there is a natural surjective map $\mathrm{Pic}^0(X_1(N)) \to \mathrm{Pic}^0(\widetilde{X}_1(N))$ restricting to

$$\pi_n : \mathrm{Pic}^0(X_1(N))[\ell^n] \to \mathrm{Pic}^0(\widetilde{X}_1(N))[\ell^n].$$

We will use without proof the following facts:

- the inclusion i_n is in fact an isomorphism.
- the surjection π_n is also a surjection, for $p \nmid \ell N$.
- If a curve X over a field k has genus g and M is coprime to $\mathrm{char}(k)$, then $\mathrm{Pic}^0(X)[M] \cong (\mathbb{Z}/M\mathbb{Z})^{2g}$.
- If a curve X over $\mathbb{Q}$ has good reduction at a prime $p \nmid M$, then the reduction map is injective on $\mathrm{Pic}^0(X)[M]$.

Consider the ℓ-**adic Tate module of** $X_1(N)$,

$$\mathrm{T}_\ell(\mathrm{Pic}^0(X_1(N))) := \varprojlim_n \{\mathrm{Pic}^0(X_1(N))[\ell^n]\}.$$

Similarly as before, choosing bases of $\mathrm{Pic}^0(X_1(N))$ compatibly for all n shows that

$$\mathrm{T}_\ell(\mathrm{Pic}^0(X_1(N))) \cong \mathbb{Z}_\ell^{2g}.$$

Any automorphism $\sigma \in G_{\mathbb{Q}}$ defines an automorphism of $\mathrm{Div}^0(X_1(N))$,

$$\Big(\sum n_P(P)\Big)^\sigma = \sum n_P(P^\sigma).$$

Since $\mathrm{div}(f)^\sigma = \mathrm{div}(f^\sigma)$ for any $f \in \overline{\mathbb{Q}}(X_1(N))$, the automorphism descends to $\mathrm{Pic}^0(X_1(N))$,

$$\mathrm{Pic}^0(X_1(N)) \times G_{\mathbb{Q}} \to \mathrm{Pic}^0(X_1(N)).$$

The diagram

$$\begin{array}{ccc} & \mathbf{G}_{\mathbb{Q}} & \\ \swarrow & & \searrow \\ \mathrm{Aut}(\mathrm{Pic}^0(\mathbf{X}_1(N))[\ell^n]) & \longleftarrow & \mathrm{Aut}(\mathrm{Pic}^0(\mathbf{X}_1(N))[\ell^{n+1}]) \end{array}$$

commutes for each n. Again as before, this leads to a continuous homomorphism

$$\rho_{X_1(N),\ell} : G_{\mathbb{Q}} \to \mathrm{GL}_{2g}(\mathbb{Z}_\ell) \subset \mathrm{GL}_{2g}(\mathbb{Q}_\ell).$$

This is the $2g$-**dimensional representation associated to** $X_1(N)$. This representation has the following properties.

Theorem 3.4. *Let ℓ be a prime and let N be a positive integer. The Galois representation $\rho_{X_1(N),\ell}$ is unramified at every prime $p \nmid \ell N$. For any such p, let $\mathfrak{p} \subset \overline{\mathbb{Z}}$ be any maximal ideal over p. Then $\rho_{X_1(N),\ell}(\mathrm{Frob}_\mathfrak{p})$ satisfies the polynomial equation*

$$x^2 - T_p x + \langle p \rangle p = 0.$$

Proof. Let $p \nmid \ell N$ and let $\mathfrak{p}$ lie over p. There is a commutative diagram

$$\begin{array}{ccc} D_\mathfrak{p} & \longrightarrow & \mathrm{Aut}(\mathrm{Pic}^0(X_1(N))[\ell^n]) \\ \downarrow & & \downarrow \pi \\ G_{\mathbb{F}_p} & \longrightarrow & \mathrm{Aut}(\mathrm{Pic}^0(\widetilde{X}_1(N))[\ell^n]). \end{array}$$

The map π is an isomorphism and $I_\mathfrak{p} \subset \ker \rho_{X_1(N),\ell}$. This proves the ramification statement.

For the second part, the Eichler-Shimura relation restricts to ℓ^n-torsion,

$$\begin{array}{ccc} \mathrm{Pic}^0(X_1(N))[\ell^n] & \xrightarrow{T_p} & \mathrm{Pic}^0(X_1(N))[\ell^n] \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(\widetilde{X}_1(N))[\ell^n] & \xrightarrow{\sigma_{p,*} + \widetilde{\langle p \rangle}_* \sigma_p^*} & \mathrm{Pic}^0(\widetilde{X}_1(N))[\ell^n]. \end{array}$$

The diagram

$$\begin{array}{ccc} \mathrm{Pic}^0(X_1(N))[\ell^n] & \xrightarrow{\mathrm{Frob}_\mathfrak{p}+\langle p\rangle p\mathrm{Frob}_\mathfrak{p}^{-1}} & \mathrm{Pic}^0(X_1(N))[\ell^n] \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(\widetilde{X}_1(N))[\ell^n] & \xrightarrow{\sigma_{p,*}+\widetilde{\langle p\rangle}_*\sigma_p^*} & \mathrm{Pic}^0(\widetilde{X}_1(N))[\ell^n]. \end{array}$$

also commutes. Since the vertical arrows are isomorphisms,

$$T_p = \mathrm{Frob}_\mathfrak{p} + \langle p\rangle p\mathrm{Frob}_\mathfrak{p}^{-1} \Leftrightarrow \mathrm{Frob}_\mathfrak{p}^2 - T_p\mathrm{Frob}_\mathfrak{p} + \langle p\rangle p = 0.$$

on $\mathrm{Pic}^0(\widetilde{X}_1(N))[\ell^n]$. This holds for all n, so we can extend the equality to $\mathrm{Ta}_\ell(\mathrm{Pic}^0(\widetilde{X}_1(N)))$. The result follows. □

To proceed from Picard groups to modular forms, consider a normalised eigenform $f \in S_2(N,\chi)$ and denote by A_f the abelian variety associated to f (cf. Appendix I). There is an isomorphism

$$\mathbb{T}_\mathbb{Z}/I_f \xrightarrow{\sim} \mathcal{O}_f = \mathbb{Z}[\{a_n(f) : n \in \mathbb{Z}^+\}].$$

Under this isomorphism, each Fourier coefficient $a_p(f)$ acts on A_f as $T_p + I_f$. The ring $\mathcal{O}_f$ generates the **number field of** f, denoted by K_f. The extension degree $d = [K_f : \mathbb{Q}]$ is also the dimension of A_f as a complex torus. Consider the ℓ-adic Tate module of A_f

$$T_\ell(A_f) = \varprojlim_n \{A_f[\ell^n]\} \cong \mathbb{Z}_\ell^{2d}.$$

The action of $\mathcal{O}_f$ on A_f is defined on ℓ-power torsion and thus extends to an action on $\mathrm{T}_\ell(A_f)$. The following lemma shows that $G_\mathbb{Q}$ acts on $\mathrm{T}_\ell(A_f)$ as well.

Lemma 3.5. *The map*

$$\mathrm{Pic}^0(X_1(N))[\ell^n] \to A_f[\ell^n]$$

is a surjection. Its kernel is stable under $G_\mathbb{Q}$, and $G_\mathbb{Q}$ operates on the kernel.

So $G_\mathbb{Q}$ acts on $A_f[\ell^n]$ and therefore on $T_\ell(A_f)$. The action commutes with the action of $\mathcal{O}_f$ since the $G_\mathbb{Q}$-action and the $\mathbb{T}_\mathbb{Z}$-action commute on $\mathrm{T}_\ell(\mathrm{Pic}^0(X_1(N)))$. Choosing coordinates appropriately gives a Galois representation

$$\rho_{A_f,\ell} : G_\mathbb{Q} \to \mathrm{GL}_{2d}(\mathbb{Q}_\ell).$$

The representation $\rho_{A_f,\ell}$ has the following properties:

- It is continuous because $\rho_{X_1(N),\ell}$ is continuous and

  $$\rho_{X_1(N),\ell}^{-1}(U(n,g)) \subset \rho_{A_f,\ell}^{-1}(U(n,d)),$$

  where $U(n,g) = \ker(\mathrm{GL}_{2g}(\mathbb{Z}_\ell) \to \mathrm{GL}_{2g}(\mathbb{Z}/\ell^n\mathbb{Z}))$.

- It is unramified at all primes $p \nmid \ell N$ since its kernel contains $\ker\rho_{X_1(N),\ell}$.

- For any unramified prime p, let $\mathfrak{p} \subset \overline{\mathbb{Z}}$ be any maximal ideal over p. At the level of Abelian varieties, since T_p acts as $a_p(f)$ and $\langle p\rangle$ acts as $\chi(p)$, $\rho_{A_f,\ell}(\mathrm{Frob}_\mathfrak{p})$ satisfies the polynomial equation

  $$x^2 - a_p(f)x + \chi(\mathrm{Frob}_p)p = 0.$$

The Tate module $\mathrm{T}_\ell(A_f)$ has rank $2d$ over $\mathbb{Z}_\ell$. Since it is an $\mathcal{O}_f$-module, the tensor product $V_\ell(A_f) \otimes \mathbb{Q}$ is a module over $\mathcal{O}_f \otimes \mathbb{Q}_\ell = K_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. It turns out that $G_{\mathbb{Q}}$ acts $K_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-linearly on $V_\ell(A_f)$, and $V_\ell(A_f) \cong (K_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)^2$. Choose a basis of $V_\ell(A_f)$ to get a homomorphism $G_{\mathbb{Q}} \to \mathrm{GL}_2(K_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)$. We have that

$$K_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong \prod_{\lambda|\ell} K_{f,\lambda},$$

so for each λ we can compose the homomorphism with a projection to get a continuous Galois representation

$$\rho_{f,\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_{f,\lambda}).$$

We have proved the following.

Theorem 3.6. *Let $f \in S_2(N, \chi)$ be a normalised eigenform with number field K_f. Let ℓ be a prime. For each maximal ideal λ of $\mathcal{O}_{K_f}$ lying over ℓ there is a 2-dimensional Galois representation*

$$\rho_{f,\lambda} : G_{\mathbb{Q}} \to GL_2(K_{f,\lambda}).$$

This representation is unramified at every prime $p \nmid \ell N$. For any such p let $\mathfrak{p} \subset \overline{\mathbb{Z}}$ be any maximal ideal lying over p. Then $\rho_{f,\lambda}(\mathrm{Frob}_{\mathfrak{p}})$ satisfies the polynomial equation

$$x^2 - a_p(f)x + \chi(p)p = 0.$$

In particular, if $f \in S_2(\Gamma_0(N))$, the relation is $x^2 - a_p(f)x + p = 0$.

3.3 Appendix II: The abelian variety associated to a modular form

Let $f \in S_2(\Gamma_0(N))$ be a normalised eigenform $f = \sum_{n=1}^{\infty} a_n q^n$. Then the eigenvalues $a_n(f)$ are algebraic integers. The field $K_f := \mathbb{Q}(\{a_n\})$ is called the **number field of** f.

The **eigenvalue map** of f is

$$\begin{array}{rccc} \lambda_f : & \mathbb{T}_f & \to & \mathbb{C} \\ & Tf & \mapsto & \lambda_f(T)f, \end{array}$$

and its kernel is $I_f = \ker(\lambda_f) = \{T \in \mathbb{T}_f : Tf = 0\}$. The map $T \mapsto \lambda_f(T)$ induces a $\mathbb{Z}$-module isomorphism

$$\mathbb{T}_{\mathbb{Z}}/I_f \xrightarrow{\sim} \mathbb{Z}[\{a_n(f)\}].$$

Since $\mathbb{T}_{\mathbb{Z}}$ acts on the Jacobian $J_1(M_f)$, the subgroup $I_f J_1(M_f) \subseteq J_1(M_f)$ makes sense.

Definition 3.7. The **abelian variety associated to** f is defined as

$$A_f := J_0(M_f)/I_f J_0(M_f).$$

The $\mathbb{Z}$-module $\mathbb{T}_{\mathbb{Z}}/I_f$ acts on A_f, and thus also the $\mathbb{Z}$-module $\mathbb{Z}[\{a_n(f)\}]$ does. The following diagram commutes

$$\begin{array}{ccc} J_1(M_f) & \xrightarrow{T_p} & J_1(M_f) \\ \downarrow & & \downarrow \\ A_f & \xrightarrow{a_p(f)} & A_f \end{array}$$

We have the following theorem.

Theorem 3.8. *The Jacobian associated to $\Gamma_0(N)$ is isogenus to a direct sum of abelian varieties associated to equivalent classes of newforms*

$$J_1(N) \to \bigoplus_f A_f^{m_f}.$$

Here the sum is taken over a set of representatives $f \in S_2(\Gamma_0(M_f))$ at levels M_f dividing N, and each m_f is the number of divisors of N/M_f.

Proof. [Di05], pg. 244. □

4 Galois representations and modular forms of weight $k \geq 2$

4.1 Deligne's construction

For $k > 2$, the idea of the proof is similar than the $k = 2$ case, but some generalisations have to be made. For example, in the case $k > 2$, the Jacobian variety $J_1(N)$ is changed by a Kuga-Sato variety $W_1(N)$; the abelian variety associated to the modular form f is changed by the Scholl motif M_f associated to f, and $T_p(J_1(N))$ is changed by the étale cohomology of $W_1(N)$.

For a sketch of the general construction see [Wi13].

References

[De68] P. Deligne, *Formes modulaires et représentations ℓ-adiques*, Séminaire Bourbaki **355**, 21 année, 1968/69.

[Di05] Diamond, F., Shurman, J.: *A First Course in Modular Forms*. Springer, 2005. 1, 2, 2.2, 3, 3.1, 3.1, 3.3

[Ma12] Martínez, A. An approach to Galois representations. Master's thesis, Universitat de Barcelona, 2012.

[Mi98] Milne, J., Lectures on Étale Cohomology, 1998

[Se68] Serre, J.-P., *Abelian l-adic representations and elliptic curves*. Benjamin, New York, 1968. 1

[Wi13] Wiese, G. *Modular Galois Representations and Applications*. Lecture notes, Higher School of Economics in Moscow, 2013. 4.1