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

Laia Amorós i Carafí
Universitat de Barcelona, University of Luxembourg

January 2015

1. **Introduction to Galois representations**
2. **Introduction to modular forms**
3. **Shimura's construction for weight $k = 2$**
4. **Deligne's construction for weight $k \geq 2$**

1. INTRODUCTION TO GALOIS REPRESENTATIONS

Introduction to ℓ-adic Galois representations

Let $\mathbf{G}$ be a profinite group and let k be a topological field. We will study ℓ-**adic Galois representations**, which are defined as follows:

- a **representation** of $\mathbf{G}$ (of dimension n) is a continuous homomorphism of groups

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

- ρ is a **Galois** representation when $\mathbf{G} = \mathbf{G}_K =$ absolute Galois group of a field K,
- is an ℓ-**adic** representation when $k \subseteq \overline{\mathbb{Q}}_\ell$,
- and ℓ is just some prime number.

Introduction to ℓ-adic Galois representations

Let $\mathbf{A}$ denote some abelian group and $\mathbf{A}[\ell^n]$ its ℓ^n-torsion. One may construct an inverse system $\mathbf{A}[\ell^{n+1}] \twoheadrightarrow \mathbf{A}[\ell^n]$. Its inverse limit

$$T_\ell(\mathbf{A}) := \varprojlim_n \mathbf{A}[\ell^n],$$

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

Example (The ℓ-adic cyclotomic character)

Let K be a field of characteristic p and $\overline{K}$ its separable closure. Let $\ell \neq p$ be a prime. 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 $\overline{K}^\times$**,

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

Example (The ℓ-adic cyclotomic character)

Let K be a field of characteristic p and $\overline{K}$ its separable closure. Let $\ell \neq p$ be a prime. 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 $\overline{K}^\times$**,

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

$\mathbf{G}_K$ acts compatibly on $\mu_{\ell^n}(\overline{K})$ for all n. We have a Galois representation:

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

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

Example (Galois representations and elliptic curves)

Let $\mathbf{E}$ be an elliptic curve over K and $\ell \neq p$. Consider the inverse system $\mathbf{E}[\ell^n] \twoheadrightarrow \mathbf{E}[\ell^{n-1}]$ given by $P \mapsto \ell \cdot P$ and the corresponding ℓ-**Tate module of E**, $\mathrm{T}_\ell(\mathbf{E}) = \varprojlim \mathbf{E}[\ell^n] \cong \mathbb{Z}_\ell^2$. For each n, the field $\mathbb{Q}(\mathbf{E}[\ell^n])$ is a Galois number field, giving a restriction map and an injection

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

These maps are compatible for each n.

Example (Galois representations and elliptic curves)

Let $\mathbf{E}$ be an elliptic curve over K and $\ell \neq p$. Consider the inverse system $\mathbf{E}[\ell^n] \twoheadrightarrow \mathbf{E}[\ell^{n-1}]$ given by $P \mapsto \ell \cdot P$ and the corresponding **ℓ-Tate module of E**, $\mathrm{T}_\ell(\mathbf{E}) = \varprojlim \mathbf{E}[\ell^n] \cong \mathbb{Z}_\ell^2$. For each n, the field $\mathbb{Q}(\mathbf{E}[\ell^n])$ is a Galois number field, giving a restriction map and an injection

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

These maps are compatible for each n.

Choosing basis of $\mathbf{E}[\ell^n]$ for each n in a compatible way one can determine isomorphisms $\mathrm{Aut}(\mathbf{E}[\ell^n]) \cong \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$, and these combine to give $\mathrm{Aut}(\mathrm{T}_\ell(\mathbf{E})) \xrightarrow{\sim} \mathrm{GL}_2(\mathbb{Z}_\ell)$. Since $\mathbf{G}_K$ acts on $\mathrm{T}_\ell(\mathbf{E})$, we obtain a Galois representation

$$\rho_{\mathbf{E},\ell} : \mathbf{G}_K \longrightarrow GL_2(\mathbb{Z}_\ell) \subset \mathrm{GL}_2(\mathbb{Q}_\ell),$$

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

Example (Galois representations and abelian varieties)

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

Example (Galois representations and abelian varieties)

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

Consider $V_\ell(A) := \mathrm{T}_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong \mathbb{Q}_\ell^{2g}$. The Galois group $\mathbf{G}_K$ acts on $\mathrm{T}_\ell(\mathbf{A})$ and on $V_\ell(\mathbf{A})$. This yields to the **ℓ-adic Galois representation associated to A**,

$$\rho_{\mathbf{A},\ell} : \mathbf{G}_K \to \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(\overline{K})) \cong \mathrm{GL}_{2g}(\mathbb{Q}_\ell).$$

Introduction to ℓ-adic Galois representations

Example (Cohomology representations)

Let $\mathbf{X}$ be an algebraic variety over $\overline{K}$ and $\ell \neq p$. Attach to $\mathbf{X}$ the étale cohomology groups $\mathrm{H}^i(\mathbf{X}_{et}, \mathbb{Z}/\ell^n\mathbb{Z}),\ i \in \mathbb{Z}$. Then, one defines

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

Example (Cohomology representations)

Let $\mathbf{X}$ be an algebraic variety over $\overline{K}$ and $\ell \neq p$. Attach to $\mathbf{X}$ the étale cohomology groups $\mathrm{H}^i(\mathbf{X}_{et}, \mathbb{Z}/\ell^n\mathbb{Z})$, $i \in \mathbb{Z}$. Then, one defines

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

The group $\mathrm{H}^i_\ell(\mathbf{X}, \mathbb{Q}_\ell)$ is a $\mathbb{Q}_\ell$-vector space on which $\mathbf{G}_K$ acts. It is finite dimensional, at least if $\mathrm{char}(K) = 0$ or if $\mathbf{X}$ is proper.

One thus gets an ℓ-adic representation of $\mathbf{G}_K$ associated to $\mathrm{H}^i_\ell(\mathbf{X}, \mathbb{Q}_\ell)$, the ***i*-th ℓ-adic Galois representation associated to X**, for $0 \leq i \leq 2\dim(\mathbf{X})$.

Introduction to ℓ-adic Galois representations

Let **K** be a number field. Then one may find not one, but a family of representations $\{\rho_\ell\}_\ell$ attached to **K**, one for each ℓ,

$$\rho_\ell : \mathsf{Gal}(\mathbf{K}/\mathbb{Q}) \to \mathsf{GL}(\overline{\mathbb{Q}}_\ell).$$

Since they come from the same object, they might be expected to be *compatible* in some sense.

Introduction to ℓ-adic Galois representations

Consider an arbitrary Galois extension $L/K/\mathbb{Q}$ and $\mathfrak{P}/\mathfrak{p}/p$ prime ideals in these fields. Recall the **decomposition group** of $\mathfrak{P}$

$$\mathbf{D}_{\mathfrak{P}} := \{\sigma \in \mathbf{G}_K \mid \mathfrak{P}^\sigma = \mathfrak{P}\} \cong \mathrm{Gal}(\mathbf{L}_{\mathfrak{P}}/\mathbf{K}_{\mathfrak{p}})$$

and the **inertia group** of $\mathfrak{P}$,

$$\mathbf{I}_{\mathfrak{P}} := \{\sigma \in \mathbf{D}_{\mathfrak{P}} \mid x^\sigma \equiv x \pmod{\mathfrak{P}},\ \forall x \in \mathcal{O}_L\}.$$

Introduction to ℓ-adic Galois representations

Consider an arbitrary Galois extension $L/K/\mathbb{Q}$ and $\mathfrak{P}/\mathfrak{p}/p$ prime ideals in these fields. Recall the **decomposition group** of $\mathfrak{P}$

$$\mathbf{D}_{\mathfrak{P}} := \{\sigma \in \mathbf{G}_K \mid \mathfrak{P}^\sigma = \mathfrak{P}\} \cong \mathrm{Gal}(\mathbf{L}_{\mathfrak{P}}/\mathbf{K}_{\mathfrak{p}})$$

and the **inertia group** of $\mathfrak{P}$,

$$\mathbf{I}_{\mathfrak{P}} := \{\sigma \in \mathbf{D}_{\mathfrak{P}} \mid x^\sigma \equiv x \pmod{\mathfrak{P}},\ \forall x \in \mathcal{O}_L\}.$$

There is an isomorphism

$$\mathbf{D}_{\mathfrak{P}}/\mathbf{I}_{\mathfrak{P}} \cong \mathrm{Gal}(\mathbb{F}(\mathfrak{P})/\mathbb{F}(\mathfrak{p})) = \langle \mathrm{Frob}_p \rangle,$$

and any representative in $\mathbf{D}_{\mathfrak{P}}$ mapping to the Frobenius automorphism Frob_p is called a **Frobenius element** of $\mathrm{Gal}(L/K)$, denoted by $\mathbf{Frob}_{\mathfrak{p}}$.

Introduction to ℓ-adic Galois representations

Consider an arbitrary Galois extension $L/K/\mathbb{Q}$ and $\mathfrak{P}/\mathfrak{p}/p$ prime ideals in these fields. Recall the **decomposition group** of $\mathfrak{P}$

$$\mathbf{D}_{\mathfrak{P}} := \{\sigma \in \mathbf{G}_K \mid \mathfrak{P}^\sigma = \mathfrak{P}\} \cong \mathrm{Gal}(\mathbf{L}_{\mathfrak{P}}/\mathbf{K}_{\mathfrak{p}})$$

and the **inertia group** of $\mathfrak{P}$,

$$\mathbf{I}_{\mathfrak{P}} := \{\sigma \in \mathbf{D}_{\mathfrak{P}} \mid x^\sigma \equiv x \pmod{\mathfrak{P}},\ \forall x \in \mathcal{O}_L\}.$$

There is an isomorphism

$$\mathbf{D}_{\mathfrak{P}}/\mathbf{I}_{\mathfrak{P}} \cong \mathrm{Gal}(\mathbb{F}(\mathfrak{P})/\mathbb{F}(\mathfrak{p})) = \langle \mathrm{Frob}_p \rangle,$$

and any representative in $\mathbf{D}_{\mathfrak{P}}$ mapping to the Frobenius automorphism Frob_p is called a **Frobenius element** of $\mathrm{Gal}(L/K)$, denoted by $\mathbf{Frob}_{\mathfrak{p}}$.

Definition

An ℓ-adic Galois representation $\rho_\ell : \mathbf{G}_K \to \mathrm{Aut}(V)$ is called **unramified** at a prime $\mathfrak{p}$ of K if $\mathbf{I}_{\mathfrak{P}} \subset \ker\rho$ for any place $\mathfrak{P}$ of $\overline{K}$ extending $\mathfrak{p}$.

Introduction to ℓ-adic Galois representations

Let $\mathfrak{p}$ be an unramified prime with respect to some representation ρ_ℓ.
One defines the **characteristic polynomial of Frobenius of ρ_ℓ at $\mathfrak{p}$ as**

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

Introduction to ℓ-adic Galois representations

Let $\mathfrak{p}$ be an unramified prime with respect to some representation ρ_ℓ.
One defines the **characteristic polynomial of Frobenius of ρ_ℓ at $\mathfrak{p}$ as**

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

The representation ρ_ℓ is called **rational** (resp. **integral**) if

- it is unramified at all primes except for a finite set S, and
- $P_{\mathfrak{p},\rho_\ell}(T) \in \mathbb{Q}[T]$ (resp. $\mathbb{Z}[T]$).

Let $\mathfrak{p}$ be an unramified prime with respect to some representation ρ_ℓ.
One defines the **characteristic polynomial of Frobenius of ρ_ℓ at $\mathfrak{p}$ as**

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

The representation ρ_ℓ is called **rational** (resp. **integral**) if

- it is unramified at all primes except for a finite set S, and
- $P_{\mathfrak{p},\rho_\ell}(T) \in \mathbb{Q}[T]$ (resp. $\mathbb{Z}[T]$).

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

The ℓ-adic Galois representations $\chi_\ell, \rho_{\mathbf{E},\ell}$ and $\rho_{\mathbf{A},\ell}$ of $\mathbf{G}_K$ are integral representations.

Introduction to ℓ-adic Galois representations

Examples

The ℓ-adic Galois representations $\chi_\ell, \rho_{\mathbf{E},\ell}$ and $\rho_{\mathbf{A},\ell}$ of $\mathbf{G}_K$ are integral representations.

In the first case one can take as S the set S_ℓ of places in K that lie over ℓ. In the second and third cases, one can take as S the union of S_ℓ and the set of primes of bad reduction of $\mathbf{E}$ (resp. $\mathbf{A}$).

Introduction to ℓ-adic Galois representations

Examples

The ℓ-adic Galois representations $\chi_\ell, \rho_{\mathbf{E},\ell}$ and $\rho_{\mathbf{A},\ell}$ of $\mathbf{G}_K$ are integral representations.

In the first case one can take as S the set S_ℓ of places in K that lie over ℓ. In the second and third cases, one can take as S the union of S_ℓ and the set of primes of bad reduction of **E** (resp. **A**).

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.

Examples

The ℓ-adic Galois representations $\chi_\ell, \rho_{\mathbf{E},\ell}$ and $\rho_{\mathbf{A},\ell}$ of $\mathbf{G}_K$ are integral representations.

In the first case one can take as S the set S_ℓ of places in K that lie over ℓ. In the second and third cases, one can take as S the union of S_ℓ and the set of primes of bad reduction of $\mathbf{E}$ (resp. $\mathbf{A}$).

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.

Cohomology representations of $\mathbf{G}_K$ are known to be integral if $K = \overline{\mathbb{F}}_q$ (Weil conjectures), and it is a well known open question in general.

Introduction to ℓ-adic Galois representations

Let ℓ' be a prime, and consider an ℓ'-adic Galois representation ρ' of $\mathbf{G}_K$. Assume that ρ and ρ' are rational. Then, ρ and ρ' are **compatible** if

- there exists a finite subset of primes S such that ρ and ρ' are unramified outside S and
- $P_{\mathfrak{p},\rho}(T) = P_{\mathfrak{p},\rho'}(T), \quad$ for all primes outside S.

Introduction to ℓ-adic Galois representations

Let ℓ' be a prime, and consider an ℓ'-adic Galois representation ρ' of $\mathbf{G}_K$. Assume that ρ and ρ' are rational. Then, ρ and ρ' are **compatible** if

- there exists a finite subset of primes S such that ρ and ρ' are unramified outside S and
- $P_{\mathfrak{p},\rho}(T) = P_{\mathfrak{p},\rho'}(T), \quad$ for all primes outside S.

Given a rational ℓ-adic Galois representation $\rho : \mathbf{G}_K \to \mathrm{Aut}(V)$ it is always possible to find a compatible representation with ρ which is semisimple. It is unique (up to isomorphism) and is called the **semisimplification** of ρ.

Introduction to ℓ-adic Galois representations

For each prime ℓ, let ρ_ℓ be a rational ℓ-adic representation of G_K. The system $\{\rho_\ell\}_\ell$ is called a **compatible system** if any two ρ_ℓ and $\rho_{\ell'}$ are compatible for any primes ℓ, ℓ'.

Introduction to ℓ-adic Galois representations

For each prime ℓ, let ρ_ℓ be a rational ℓ-adic representation of G_K. The system $\{\rho_\ell\}_\ell$ is called a **compatible system** if any two ρ_ℓ and $\rho_{\ell'}$ are compatible for any primes ℓ, ℓ'.

Let $S_\ell = \{\text{primes over } \ell\} \subset \mathcal{O}_K$. The system $\{\rho_\ell\}_\ell$ is said to be **strictly compatible** if there exists a finite subset $S \subset \mathcal{O}_K$ of primes such that

- for every $\mathfrak{p} \notin S \cup S_\ell$, ρ_ℓ is unramified at $\mathfrak{p}$ and $P_{\mathfrak{p},\rho_\ell}(T) \in \mathbb{Q}(T)$.
- $P_{\mathfrak{p},\rho_\ell}(T) = P_{\mathfrak{p},\rho'_\ell}(T)$, for $\mathfrak{p} \notin S \cup S_\ell \cup S_{\ell'}$.

There is a smallest finite set S having these properties. We call it the **exceptional set** of the compatible system.

Introduction to ℓ-adic Galois representations

For each prime ℓ, let ρ_ℓ be a rational ℓ-adic representation of G_K. The system $\{\rho_\ell\}_\ell$ is called a **compatible system** if any two ρ_ℓ and $\rho_{\ell'}$ are compatible for any primes ℓ, ℓ'.

Let $S_\ell = \{\text{primes over } \ell\} \subset \mathcal{O}_K$. The system $\{\rho_\ell\}_\ell$ is said to be **strictly compatible** if there exists a finite subset $S \subset \mathcal{O}_K$ of primes such that

- for every $\mathfrak{p} \notin S \cup S_\ell$, ρ_ℓ is unramified at $\mathfrak{p}$ and $P_{\mathfrak{p},\rho_\ell}(T) \in \mathbb{Q}(T)$.
- $P_{\mathfrak{p},\rho_\ell}(T) = P_{\mathfrak{p},\rho'_\ell}(T)$, for $\mathfrak{p} \notin S \cup S_\ell \cup S_{\ell'}$.

There is a smallest finite set S having these properties. We call it the **exceptional set** of the compatible system.

Examples

The systems of ℓ-adic representations $\{\chi_\ell\}_\ell$, $\{\rho_{\mathbf{E},\ell}\}$ and $\{\rho_{\mathbf{A},\ell}\}$ are strictly compatible. The exceptional set of the first one is empty. The exceptional sets of $\{\rho_{\mathbf{E},\ell}\}$ and $\{\rho_{\mathbf{A},\ell}\}$ are the set of places where the elliptic curve (resp. abelian variety) has bad reduction.

Theorem

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

$$\rho_{\mathbf{E},\ell} : \mathbf{G}_{\mathbb{Q}} \to GL_2(\mathbb{Q}_\ell)$$

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 $\rho_{\mathbf{E},\ell}(\mathbf{Frob}_{\mathfrak{p}})$ is

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

The Galois representation is irreducible.

Introduction to ℓ-adic Galois representations

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

$$\begin{array}{ccc} \mathbf{D}_{\mathfrak{p}} & \longrightarrow & \mathrm{Aut}(\mathbf{E}[\ell^n]) \\ \big\downarrow & & \big\downarrow \wr \\ \mathbf{G}_{\mathbb{F}_p} & \longrightarrow & \mathrm{Aut}(\widetilde{\mathbf{E}}[\ell^n]) \end{array}$$

Introduction to ℓ-adic Galois representations

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

$$\begin{array}{ccc} \mathbf{D}_{\mathfrak{p}} & \longrightarrow & \mathrm{Aut}(\mathbf{E}[\ell^n]) \\ \downarrow & & \downarrow \wr \\ \mathbf{G}_{\mathbb{F}_p} & \longrightarrow & \mathrm{Aut}(\widetilde{\mathbf{E}}[\ell^n]) \end{array}$$

The inertia group $\mathbf{I}_{\mathfrak{p}}$ is contained in the kernel of $\downarrow_{\rightarrow}$. Since $p \nmid \ell N$, $\mathbf{E}$ has good reduction at p and the reduction preserves the ℓ^n-torsion structure. Thus $\mathbf{I}_{\mathfrak{p}}$ is contained in the kernel of $\rightarrow_{\downarrow}$ and

$$\mathbf{I}_{\mathfrak{p}} \subset \ker(\mathbf{D}_{\mathfrak{p}} \to \mathrm{Aut}(\mathbf{E}[\ell^n])) = \ker(\mathbf{D}_{\mathfrak{p}} \to \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}))$$

$$\Rightarrow \mathbf{I}_{\mathfrak{p}} \subset \ker(\mathbf{D}_{\mathfrak{p}} \to \mathrm{GL}_2(\mathbb{Z}_\ell)) \subset \ker \rho_{\mathbf{E},\ell}.$$

Characteristic polynomial: Let $p \nmid \ell N$.

- det$\rho_{\mathbf{E},\ell}(\mathrm{Frob}_{\mathfrak{p}})$: Let $\rho_n : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ be the nth entry of $\rho_{\mathbf{E},\ell}$ for $n \in \mathbb{Z}^+$. Using that, for all $\sigma \in G_{\mathbb{Q}}$, det$\rho_n(\sigma) = \chi_{\ell,n}(\sigma)$, we obtain that det$\rho_{\mathbf{E},\ell}(\sigma) = \chi_\ell(\sigma)$ in $\mathbb{Z}_\ell^*$. In particular, det$\rho_{\mathbf{E},\ell}(\mathbf{Frob}_{\mathfrak{p}}) = p$.

Characteristic polynomial: Let $p \nmid \ell N$.

- $\det\rho_{\mathbf{E},\ell}(\mathrm{Frob}_{\mathfrak{p}})$: Let $\rho_n : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ be the nth entry of $\rho_{\mathbf{E},\ell}$ for $n \in \mathbb{Z}^+$. Using that, for all $\sigma \in G_{\mathbb{Q}}$, $\det\rho_n(\sigma) = \chi_{\ell,n}(\sigma)$, we obtain that $\det\rho_{\mathbf{E},\ell}(\sigma) = \chi_\ell(\sigma)$ in $\mathbb{Z}_\ell^*$. In particular, $\det\rho_{\mathbf{E},\ell}(\mathbf{Frob}_{\mathfrak{p}}) = p$.
- $\mathrm{tr}\rho_{\mathbf{E},\ell}(\mathbf{Frob}_{\mathfrak{p}})$: the characteristic equation of $\rho_{E,\ell}(\mathbf{Frob}_{\mathfrak{p}}) =: A$ is $A^2 - \mathrm{tr}\,A + p = 0$, so $\mathrm{tr}\,A = A + pA^{-1}$. Using that

$$a_p(E) = \mathrm{Frob}_p + p(\mathrm{Frob}_p^{-1}) \in \mathrm{End}(\mathrm{Pic}^0(\widetilde{\mathbf{E}})),$$

and that Frob_p acts on $\widetilde{\mathbf{E}}[\ell^n]$ as $\mathbf{Frob}_{\mathfrak{p}}$ acts on $\mathbf{E}[\ell^n]$, we have that

$$a_p(\mathbf{E}) = \mathrm{Frob}_p + p\mathrm{Frob}_p^{-1} \equiv \mathbf{Frob}_{\mathfrak{p}} + p\mathbf{Frob}_{\mathfrak{p}}^{-1} \pmod{\ell^n},\ \forall n.$$

$$\Leftrightarrow a_p(\mathbf{E}) \equiv A + pA^{-1} \pmod{\ell^n},\ \forall n.$$

$$\Leftrightarrow \mathrm{tr}\,A = a_p(\mathbf{E}) \Leftrightarrow \mathrm{tr}\,\rho_{\mathbf{E},\ell}(\mathbf{Frob}_{\mathfrak{p}}) = a_p(\mathbf{E}).$$

2. INTRODUCTION TO MODULAR FORMS

Introduction to modular forms

Recall the **modular group** $\mathrm{SL}_2(\mathbb{Z})$ and its congruence subgroups for $N \in \mathbb{Z}_{>0}$:

$$\begin{aligned}
&\Gamma_0(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) (\mathrm{mod}\ N) \right\}, \\
&\cup \\
&\Gamma_1(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) (\mathrm{mod}\ N) \right\}, \\
&\cup \\
&\Gamma(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) (\mathrm{mod}\ N) \right\}.
\end{aligned}$$

They act on the **upper half plane** $\mathfrak{h} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) \geq 0\}$.

<u>Notation</u>:

For any matrix $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ define the **factor of automorphy** $j(\gamma, \tau) \in \mathbb{C}$ for $\tau \in \mathfrak{h}$ to be $j(\gamma, \tau) = c\tau + d$, and for any integer k, define the **weight-k operator** $[\gamma]_k$ on functions $f : \mathfrak{h} \to \mathbb{C}$ by

$$(f[\gamma]_k)(\tau) = j(\gamma, \tau)^{-k} f(\gamma(\tau)), \quad \tau \in \mathfrak{h}.$$

Definition

Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$ and let k be an integer. A function $f : \mathfrak{h} \to \mathbb{C}$ is a **modular of weight k with respect to Γ** if

- f is holomorphic,
- f is weight-k invariant under Γ, i.e., $f[\gamma]_k = f, \ \forall \gamma \in \Gamma$,
- $f[\alpha]_k$ is holomorphic at ∞ for all $\alpha \in SL_2(\mathbb{Z})$.

If in addition,

- $a_0 = 0$ in the Fourier expansion of $f[\alpha]_k$ for all $\alpha \in SL_2(\mathbb{Z})$,

then f is a **cusp form** of weight k with respect to Γ.

The set of modular forms of weight k with respect to Γ is denoted by $\mathcal{M}_k(\Gamma)$, the cusp forms $\mathcal{S}_k(\Gamma)$.

Let's recall the modular interpretation for the congruence subgroups $\Gamma_0(N)$ and $\Gamma_1(N)$.

Theorem (Modular interpretation)

Let N be a positive integer. Then there are isomorphisms

$$\begin{array}{ccc} \Gamma_0(N)/\mathfrak{h} & \xrightarrow{\sim} & Y_0(N)(\mathbb{C}) \\ \Gamma_0(N)\tau & \longmapsto & [\mathbb{C}/\Lambda_\tau, \langle [\frac{1}{N}]_{\Lambda_\tau} \rangle] \end{array}$$

and

$$\begin{array}{ccc} \Gamma_1(N)/\mathfrak{h} & \xrightarrow{\sim} & Y_1(N)(\mathbb{C}) \\ \Gamma_1(N)\tau & \longmapsto & [\mathbb{C}/\Lambda_\tau, [\frac{1}{N}]_{\Lambda_\tau}]. \end{array}$$

Introduction to modular forms

A nonzero modular form $f \in \mathcal{M}_k(\Gamma_1(N))$ that is an eigenform for the Hecke operators T_n and $\langle n \rangle$ for all $n \in \mathbb{Z}^+$ is a **Hecke eigenform** or simply **eigenform**. The eigenform $f(\tau) = \sum_{n=0} a_n(f)q^n$ is **normalised** when $a_1(f) = 1$. A **newform** is a normalised eigenform in $\mathcal{S}_k(\Gamma_1(N))^{\text{new}}$.

Introduction to modular forms

A nonzero modular form $f \in \mathcal{M}_k(\Gamma_1(N))$ that is an eigenform for the Hecke operators T_n and $\langle n \rangle$ for all $n \in \mathbb{Z}^+$ is a **Hecke eigenform** or simply **eigenform**. The eigenform $f(\tau) = \sum_{n=0} a_n(f) q^n$ is **normalised** when $a_1(f) = 1$. A **newform** is a normalised eigenform in $\mathcal{S}_k(\Gamma_1(N))^{\mathrm{new}}$.

The set of newforms in $\mathcal{S}_k(\Gamma_1(N))^{\mathrm{new}}$ is an orthogonal basis of this space. Each such newform lies in an eigenspace $\mathcal{S}_k(N, \chi)$ and satisfies

$$T_n f = a_n(f) f, \quad \text{for all } n \in \mathbb{Z}^+,$$

i.e., its Fourier coefficients are its T_n-eigenvalues.

Introduction to modular forms

A nonzero modular form $f \in \mathcal{M}_k(\Gamma_1(N))$ that is an eigenform for the Hecke operators T_n and $\langle n \rangle$ for all $n \in \mathbb{Z}^+$ is a **Hecke eigenform** or simply **eigenform**. The eigenform $f(\tau) = \sum_{n=0} a_n(f) q^n$ is **normalised** when $a_1(f) = 1$. A **newform** is a normalised eigenform in $\mathcal{S}_k(\Gamma_1(N))^{\text{new}}$.

The set of newforms in $\mathcal{S}_k(\Gamma_1(N))^{\text{new}}$ is an orthogonal basis of this space. Each such newform lies in an eigenspace $\mathcal{S}_k(N, \chi)$ and satisfies

$$T_n f = a_n(f) f, \quad \text{for all } n \in \mathbb{Z}^+,$$

i.e., its Fourier coefficients are its T_n-eigenvalues.

Let $f \in \mathcal{S}_2(\Gamma_1(N))$ be a normalised eigenform for the Hecke operators T_p. Then the eigenvalues $a_n(f)$ are algebraic integers.

The **Hecke algebra over** $\mathbb{Z}$ is the algebra of endomorphisms of $\mathcal{S}_2(\Gamma_1(N))$

$$\mathbb{T}_{\mathbb{Z}} := \mathbb{Z}[\{T_n, \langle n \rangle : n \in \mathbb{Z}^+\}].$$

3. SHIMURA'S CONSTRUCTION FOR WEIGHT $k = 2$

Shimura's construction

We will see that one may associate a 2-dimensional Galois representation of $\mathbf{G}_{\mathbb{Q}}$ to each normalised cuspidal eigenform. The following theorem is due to Shimura for $k = 2$ and due to Deligne for $k \geq 2$.

Shimura's construction

We will see that one may associate a 2-dimensional Galois representation of $\mathbf{G}_{\mathbb{Q}}$ to each normalised cuspidal eigenform. The following theorem is due to Shimura for $k = 2$ and due to Deligne for $k \geq 2$.

Theorem

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

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

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 $\rho_{f,\lambda}(\mathbf{Frob}_{\mathfrak{p}})$ is

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

Shimura's construction

We will sketch the construction of $\rho_{f,\lambda}$ for a modular form $\mathbf{f}$ of weight 2. Let N be a positive integer and ℓ be a prime. Consider the modular curve $\mathbf{X}_1(N)$ and let g denote its genus. The curve $\mathbf{X}_1(N)_{\mathbb{C}}$ can also be viewed as a compact Riemann surface, and its Jacobian is a g-dimensional complex torus

$$\mathbf{J}_1(N) = \mathrm{Jac}(\mathbf{X}_1(N)_{\mathbb{C}}) \stackrel{\text{def}}{=} \mathcal{S}_2(\Gamma_1(N))^\wedge / H_1(\mathbf{X}_1(N)_{\mathbb{C}}, \mathbb{Z}) \cong \mathbb{C}^g/\Lambda_g.$$

The **Picard group** of $\mathbf{X}_1(N)$ is the abelian group of divisor classes on the points of $\mathbf{X}_1(N)$,

$$\mathrm{Pic}^0(\mathbf{X}_1(N)) = \mathrm{Div}^0(\mathbf{X}_1(N))/\mathrm{DivP}(\mathbf{X}_1(N)).$$

We can think of $\mathrm{Pic}^0(\mathbf{X}_1(N))$ as a subgroup of $\mathrm{Pic}^0(\mathbf{X}_1(N)_{\mathbb{C}})$, and using *Abel's theorem* we have a natural isomorphism

$$\mathrm{Pic}^0(\mathbf{X}_1(N)_{\mathbb{C}}) \cong \mathrm{Jac}(\mathbf{X}_1(N)_{\mathbb{C}}).$$

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

$$\iota_n : \mathrm{Pic}^0(\mathbf{X}_1(N))[\ell^n] \hookrightarrow \mathrm{Pic}^0(\mathbf{X}_1(N)_{\mathbb{C}})[\ell^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z})^{2g}.$$

Shimura's construction

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

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

It turns out that both ι_n and π_n are isomorphisms. Consider the **ℓ-adic Tate module of $\mathbf{X}_1(N)$**, $\mathrm{T}_\ell(\mathrm{Pic}^0(\mathbf{X}_1(N))) := \varprojlim_n \{\mathrm{Pic}^0(\mathbf{X}_1(N))[\ell^n]\}$. Choosing bases of $\mathrm{Pic}^0(\mathbf{X}_1(N))$ compatibly for all n shows that

$$\mathrm{T}_\ell(\mathrm{Pic}^0(\mathbf{X}_1(N))) \cong \mathbb{Z}_\ell^{2g}.$$

Any automorphism $\sigma \in G_{\mathbb{Q}}$ defines an automorphism of $\mathrm{Div}^0(\mathbf{X}_1(N))$, $(\sum n_P(P))^\sigma = \sum n_P(P^\sigma)$. Since $\mathrm{div}(f)^\sigma = \mathrm{div}(f^\sigma)$ for any $f \in \overline{\mathbb{Q}}(\mathbf{X}_1(N))$, the automorphism descends to $\mathrm{Pic}^0(\mathbf{X}_1(N))$.

Shimura's construction

For each n, there is a commutative diagram

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

This leads to a continuous homomorphism

$$\rho_{\mathbf{X}_1(N),\ell} : \mathbf{G}_{\mathbb{Q}} \to \mathrm{GL}_{2g}(\mathbb{Z}_\ell) \subset \mathrm{GL}_{2g}(\mathbb{Q}_\ell).$$

This is the $2g$-**dimensional representation associated to** $\mathbf{X}_1(N)$.

The representation $\rho_{\mathbf{X}_1(N),\ell}$ 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 $\rho_{\mathbf{X}_1(N),\ell}(\mathbf{Frob}_{\mathfrak{p}})$ satisfies the polynomial equation

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

(To be proved later)

Shimura's construction

To continue, we consider a normalised eigenform $\mathbf{f} \in \mathcal{S}_2(N, \chi)$ and denote by $\mathbf{A}_f$ the abelian variety associated to $\mathbf{f}$. There is an isomorphism

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

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

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

The action of $\mathcal{O}_{\mathbf{f}}$ on $\mathbf{A}_{\mathbf{f}}$ is defined on ℓ-power torsion and thus extends to an action on $\mathrm{T}_\ell(\mathbf{A}_{\mathbf{f}})$. Using that the map

$$\mathrm{Pic}^0(\mathbf{X}_1(N))[\ell^n] \twoheadrightarrow \mathbf{A}_{\mathbf{f}}[\ell^n]$$

is a surjection, one can deduce that $\mathbf{G}_{\mathbb{Q}}$ acts on $\mathbf{A}_{\mathbf{f}}[\ell^n]$ and therefore on $T_\ell(\mathbf{A}_{\mathbf{f}})$ as well.

Shimura's construction

The action of $\mathbf{G}_{\mathbb{Q}}$ commutes with the action of $\mathcal{O}_{\mathbf{f}}$ since the $\mathbf{G}_{\mathbb{Q}}$-action and the $\mathbb{T}_{\mathbb{Z}}$-action commute on $\mathrm{T}_\ell(\mathrm{Pic}^0(\mathbf{X}_1(N)))$. Choosing coordinates appropriately it gives a Galois representation

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

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

- It is continuous because $\rho_{\mathbf{X}_1(N),\ell}$ is continuous and

$$\rho^{-1}_{\mathbf{X}_1(N),\ell}(U(n,g)) \subset \rho^{-1}_{\mathbf{A_f},\ell}(U(n,d)),$$

  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

$$\ker \rho_{\mathbf{X}_1(N),\ell} \subseteq \ker \rho_{\mathbf{A}_\ell,\ell}.$$

- 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 $a_p(\mathbf{f})$ and $\langle p \rangle$ acts as $\chi(p)$, $\rho_{\mathbf{A}_f,\ell}(\mathbf{Frob}_{\mathfrak{p}})$ satisfies the polynomial equation

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

Shimura's construction

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

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

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

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

We have proved the following.

Shimura's construction

Theorem

Let $\mathbf{f} \in \mathcal{S}_2(N, \chi)$ *be a normalised eigenform with number field* $K_{\mathbf{f}}$*. Let* ℓ *be a prime. For each maximal ideal* λ *of* $\mathcal{O}_{K_{\mathbf{f}}}$ *lying over* ℓ *there is a 2-dimensional Galois representation*

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

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* $\rho_{\mathbf{f},\lambda}(\mathbf{Frob}_{\mathfrak{p}})$ *satisfies the polynomial equation*

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

In particular, if $\mathbf{f} \in \mathcal{S}_2(\Gamma_0(N))$*, the relation is* $x^2 - a_p(\mathbf{f})x + p = 0$*.*

Shimura's construction

Lemma

The characteristic equation of $\rho_{\mathbf{X}_1(N),\ell}(\mathbf{Frob}_{\mathfrak{p}})$ *is*

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

In order to do this, we need a description of the Hecke operator T_p at the level of Picard groups of reduced modular curves,

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

Suppose this reduction exists, i.e., that there is a commutative diagram

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

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

Shimura's construction

The way to compute the reduction $\widetilde{T}_p$ on $\mathrm{Pic}^0(\widetilde{\mathbf{X}}_1(N))$ is to compute it first in the moduli space environment.

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

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

If $\mathbf{E}$ has good reduction at $\mathfrak{p}$, then so do all the curves $\mathbf{E}/C$. We will describe the right-hand side over $\overline{\mathbb{F}}_p$ rather than over $\overline{\mathbb{Q}}$.

Let C_0 denote the kernel of the reduction map $\mathbf{E}[p] \to \widetilde{\mathbf{E}}[p]$, an order p subgroup of $\mathbf{E}$. Then, for any order p subgroup C of $\mathbf{E}$,

$$[\widetilde{\mathbf{E}/C}, \widetilde{Q + C}] = \begin{cases} [\widetilde{\mathbf{E}}^{\mathrm{Frob}_p}, \widetilde{Q}^{\mathrm{Frob}_p}] & \text{if } C = C_0 \\ [\widetilde{\mathbf{E}}^{\mathrm{Frob}_p^{-1}}, [p]\widetilde{Q}^{\mathrm{Frob}_p^{-1}}] & \text{if } C \neq C_0 \end{cases}$$

Shimura's construction

Define the moduli space diamond operator in characteristic p to be

$$\widetilde{\langle d \rangle} : \begin{array}{ccc} \widetilde{\mathbf{Y}}_1(N) & \to & \widetilde{\mathbf{Y}}_1(N) \\ [\mathbf{E}, Q] & \mapsto & [\mathbf{E}, [d]Q], \quad (d, N) = 1. \end{array}$$

There are $p+1$ order p subgroups C of $\mathbf{E}$, one of which is C_0.

Summing the previous formula over all order p subgroups $C \subset \mathbf{E}$ gives for a curve $\mathbf{E}$ with ordinary reduction at $\mathfrak{p}$,

$$\begin{aligned} \textstyle\sum_C [\widetilde{\mathbf{E}/C}, \widetilde{Q+C}] &= [\widetilde{\mathbf{E}}^{\mathrm{Frob}_p}, \widetilde{Q}^{\mathrm{Frob}_p}] + \textstyle\sum_C [\widetilde{\mathbf{E}}^{\mathrm{Frob}_p^{-1}}, [p]\widetilde{Q}^{\mathrm{Frob}_p^{-1}}] \\ &= [\widetilde{\mathbf{E}}^{\mathrm{Frob}_p}, \widetilde{Q}^{\mathrm{Frob}_p}] + p\widetilde{\langle p \rangle}\, [\widetilde{\mathbf{E}}^{\mathrm{Frob}_p^{-1}}, \widetilde{Q}^{\mathrm{Frob}_p^{-1}}] \\ &= \mathrm{Frob}_p[\widetilde{\mathbf{E}}, \widetilde{Q}] + p\widetilde{\langle p \rangle}\mathrm{Frob}_p^{-1}[\widetilde{\mathbf{E}}, \widetilde{Q}] \\ &= (\mathrm{Frob}_p + p\widetilde{\langle p \rangle}\mathrm{Frob}_p^{-1})[\widetilde{\mathbf{E}}, \widetilde{Q}] \end{aligned}$$

Shimura's construction

This can be extended to curves with good reduction at $\mathfrak{p}$, and one obtains a commutative diagram (where the primes mean to avoid finitely many points):

$$\begin{array}{ccc}
\mathbf{Y}_1(N)'_{\mathrm{gd}} & \xrightarrow{T_p} & \mathrm{Div}(\mathbf{Y}_1(N)'_{\mathrm{gd}}) \\
\downarrow & & \downarrow \\
\widetilde{\mathbf{Y}}_1(N)'_{\mathrm{gd}} & \xrightarrow{\mathrm{Frob}_p + p\widetilde{\langle p \rangle}\mathrm{Frob}_p^{-1}} & \mathrm{Div}(\widetilde{\mathbf{Y}}_1(N)'_{\mathrm{gd}}).
\end{array}$$

This extends to degree-0 divisors, and to Picard groups:

$$\begin{array}{ccc}
\mathrm{Div}^0(\mathbf{Y}_1(N)'_{\mathrm{gd}}) & \xrightarrow{T_p} & \mathrm{Div}^0(\mathbf{Y}_1(N)'_{\mathrm{gd}}) \\
\downarrow & & \downarrow \\
\mathrm{Div}(\widetilde{\mathbf{Y}}_1(N)'_{\mathrm{gd}}) & \xrightarrow{\mathrm{Frob}_p + p\widetilde{\langle p \rangle}\mathrm{Frob}_p^{-1}} & \mathrm{Div}^0(\widetilde{\mathbf{Y}}_1(N)'_{\mathrm{gd}}) \\
\downarrow & & \downarrow \\
\mathrm{Pic}^0(\widetilde{\mathbf{X}}_1(N)) & \xrightarrow{\mathrm{Frob}_{p,*} + \widetilde{\langle p \rangle}_* \mathrm{Frob}_p^*} & \mathrm{Pic}^0(\widetilde{\mathbf{X}}_1(N)).
\end{array}$$

Shimura's construction

Theorem (Eichler-Shimura Relation)

Let $p \nmid N$. The following diagrams commute

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

$$\begin{array}{ccc} Pic^0(\mathbf{X}_0(N)) & \xrightarrow{T_p} & Pic^0(\mathbf{X}_0(N)) \\ \downarrow & & \downarrow \\ Pic^0(\widetilde{\mathbf{X}}_0(N)) & \xrightarrow{Frob_{p,*} + Frob_p^*} & Pic^0(\widetilde{\mathbf{X}}_0(N)). \end{array}$$

Shimura's construction

The Eichler-Shimura relation restricts to ℓ^n-torsion, and we obtain

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

on $\mathrm{Pic}^0(\mathbf{X}_1(N))[\ell^n]$. This holds for all n, so the equality extends to $\mathrm{T}_\ell(\mathrm{Pic}^0(\widetilde{\mathbf{X}}_1(N)))$.

3. DELIGNE'S CONSTRUCTION FOR WEIGHT $k \geq 2$

Deligne's construction

For $k \geq 2$,

$k = 2$	$k > 2$
$\mathbf{J}_1(N)$	Kuga-Sato variety $\mathbf{W}_1(N)$
$\mathbf{A_f}$	$\mathbf{M_f}$ = Scholl motiv associated to $\mathbf{f}$
$T_p(\mathbf{J}_1(N))$	étale cohomology of $\mathbf{W}_1(N)$

Gràcies!