# Galois representations and modular forms

Takeshi Saito

July 17-22, 2006 at IHES

**Abstract**

This note is based on a series of lectures given at the summer school held on July 17-29, 2006 at IHES. The purpose of the lectures is to explain the basic ideas in the geometric construction of the Galois representations associated to elliptic modular forms of weight at least 2.

## Motivation

The Galois representations associated to modular forms play a central role in the modern number theory. In this introduction, we give a reason why they take such a position.

A goal in number theory is to understand the finite extensions of $\mathbb{Q}$. By Galois theory, it is equivalent to understand the absolute Galois group $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. One may say that one knows a group if one knows its representations.

Representations are classified by the degrees. The class field theory provides us a precise understanding of the representations of degree 1, or characters. By the theorem of Kronecker-Weber, a continuous character $G_{\mathbb{Q}} \to \mathbb{C}^\times$ is a Dirichlet character

$$G_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \to (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$$

for some integer $N \geq 1$. If we consider not only complex continuous characters but also $\ell$-adic characters $G_{\mathbb{Q}} \to \mathbb{Q}_\ell^\times$ for a prime $\ell$, we find more characters. For example, the $\ell$-adic cyclotomic character is defined as the composition:

$$G_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^n}, n \in \mathbb{N})/\mathbb{Q}) = \varprojlim{}_n \mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^n})/\mathbb{Q}) \to \varprojlim{}_n (\mathbb{Z}/\ell^n\mathbb{Z})^\times = \mathbb{Z}_\ell^\times \subset \mathbb{Q}_\ell^\times.$$

The $\ell$-adic characters "with motivic origin" are generated by Dirichlet characters and $\ell$-adic cyclotomic characters:

$$\begin{aligned} &\{\text{"geometric" } \ell\text{-adic character of } G_{\mathbb{Q}}\} \\ = \ &\langle \text{Dirichlet characters, } \ell\text{-adic cyclotomic characters} \rangle \end{aligned}$$

if we use a fancy terminology "geometric", that will not be explained in this note. For the definition, we refer to [13].

When we leave the realm of class field theory, the first representations we encounter are those of degree 2. For $\ell$-adic Galois representation of degree 2, we expect to have (cf. [13]) a similar equality

$$\begin{aligned} & \{\text{odd "geometric" } \ell\text{-adic representation of } G_{\mathbb{Q}} \text{ of degree 2 of distinct Hodge-Tate weight}\} \\ = & \{\ell\text{-adic representation associated to modular form of weight at least 2}\}, \end{aligned}$$

up to twist by a power of the cyclotomic character. In other words, the Galois representations associated to modular forms are the first ones we encounter when we explore outside the domain of class field theory.

In this note, we discuss only one direction $\supset$ established by Shimura and Deligne ([21], [7]). We will not discuss the other direction $\subset$, which is almost established after the revolutionary work of Wiles, although it has significant consequences including Fermat's last theorem, the modularity of elliptic curves, etc. ([24], [1]).

In Section 1, we recall the definition of modular forms and state the existence of Galois representations associated to normalized eigen cusp forms. We introduce modular curves defined over $\mathbb{C}$ and over $\mathbb{Z}[\frac{1}{N}]$ as the key ingredient in the construction of the Galois representations, in Section 2. Then, we construct the Galois representations in the case of weight 2 by decomposing the Tate module of the Jacobian of a modular curve in Section 3. In the final Section 4, we briefly sketch an outline of the construction in the higher weight case.

Proofs will be only sketched or omitted mostly. The author apologizes that he also omits the historical accounts completely.

The author would like to thank the participants of the summer school for pointing out numerous mistakes and inaccuracies during the lectures.

# Contents

# 1 Galois representations and modular forms

## 1.1 Modular forms

Let $N \geq 1$ and $k \geq 2$ be integers and $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a character. We will define $\mathbb{C}$-vector spaces $S_k(N,\varepsilon) \subset M_k(N,\varepsilon)$ of cusp forms and of modular forms of level $N$, weight $k$ and of character $\varepsilon$. We will see later in §3.4 that they are of finite dimension by using the compactification of a modular curve. For $\varepsilon = 1$, we write $S_k(N) \subset M_k(N)$ for $S_k(N,1) \subset M_k(N,1)$. For a reference on this subsection, we refer to [12] Chapter 1.

A subgroup $\Gamma \subset SL_2(\mathbb{Z})$ is called a congruence subgroup if there exists an integer $N \geq 1$ such that $\Gamma \supset \Gamma(N) = \mathrm{Ker}(SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z}))$. In this note, we mainly consider the congruence subgroups

$$\begin{aligned} & \Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \middle| a \equiv 1, c \equiv 0 \bmod N \right\} \\ \subset \quad & \Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \middle| c \equiv 0 \bmod N \right\}. \end{aligned}$$

We identify the quotient $\Gamma_0(N)/\Gamma_1(N)$ with $(\mathbb{Z}/N\mathbb{Z})^\times$ by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d \bmod N$. The indices are given by

$$\begin{aligned} [SL_2(\mathbb{Z}) : \Gamma_0(N)] &= \prod_{p|N} (p+1) p^{\mathrm{ord}_p(N)-1} = N \prod_{p|N} \left(1 + \frac{1}{p}\right), \\ [SL_2(\mathbb{Z}) : \Gamma_1(N)] &= \prod_{p|N} (p^2-1) p^{2(\mathrm{ord}_p(N)-1)} = N^2 \prod_{p|N} \left(1 - \frac{1}{p^2}\right). \end{aligned}$$

The action of $SL_2(\mathbb{Z})$ on the Poincaré upper half plane $H = \{\tau \in \mathbb{C} | \mathrm{Im}\ \tau > 0\}$ is defined by

$$\gamma(\tau) = \frac{a\tau + b}{c\tau + d}$$

for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ and $\tau \in H$. For a holomorphic function $f$ on $H$, we define a holomorphic function $\gamma_k^* f$ on $H$ by

$$\gamma_k^* f(\tau) = \frac{1}{(c\tau + d)^k} f(\gamma\tau).$$

If $k = 2$, we have $\gamma^*(f d\tau) = \gamma_2^*(f) d\tau$.

**Definition 1.1** *Let $\Gamma \supset \Gamma(N)$ be a congruence subgroup and $k \geq 2$ be an integer. We say that a holomorphic function $f : H \to \mathbb{C}$ is a modular form (resp. a cusp form) of weight $k$ with respect to $\Gamma$, if the following conditions* (1) *and* (2) *are satisfied.*

(1) *$\gamma_k^* f = f$ for all $\gamma \in \Gamma$.*

(2) *For each $\gamma \in SL_2(\mathbb{Z})$, $\gamma_k^* f$ satisfies $\gamma_k^* f(\tau + N) = \gamma_k^* f(\tau)$ and hence we have a Fourier expansion $\gamma_k^* f(\tau) = \sum_{n=-\infty}^{\infty} a_{\frac{n}{N}}(\gamma_k^* f) q_N^n$ where $q_N = \exp(2\pi i \frac{\tau}{N})$. We require the condition*

$$a_{\frac{n}{N}}(\gamma_k^* f) = 0$$

*be satisfied for $n < 0$ (resp. $n \leq 0$) for every $\gamma \in SL_2(\mathbb{Z})$.*

We put

$$\begin{aligned} & S_k(\Gamma)_{\mathbb{C}} = \{f | f \text{ is a cusp form of weight } k \text{ w.r.t. } \Gamma\} \\ \subset \ & M_k(\Gamma)_{\mathbb{C}} = \{f | f \text{ is a modular form of weight } k \text{ w.r.t. } \Gamma\} \end{aligned}$$

and define $S_k(N) = S_k(\Gamma_0(N))$. Since $\Gamma_0(N)$ contains $\Gamma_1(N)$ as a normal subgroup, the group $\Gamma_0(N)$ has a natural action on $S_k(\Gamma_1(N))$ by $f \mapsto \gamma_k^* f$. Since $\Gamma_1(N)$ acts trivially on $S_k(\Gamma_1(N))$, we have an induced action of the quotient $\Gamma_0(N)/\Gamma_1(N) = (\mathbb{Z}/N\mathbb{Z})^\times$ on $S_k(\Gamma_1(N))$. The action of $d \in (\mathbb{Z}/N\mathbb{Z})^\times$ on $S_k(\Gamma_1(N))$ is denoted by $\langle d \rangle$ and is called the diamond operator. The space $S_k(\Gamma_1(N))$ is decomposed by the characters

$$S_k(\Gamma_1(N)) = \bigoplus_{\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times} S_k(N, \varepsilon)$$

where $S_k(N, \varepsilon) = \{f \in S_k(\Gamma_1(N)) | \langle d \rangle f = \varepsilon(d) f \text{ for all } d \in (\mathbb{Z}/N\mathbb{Z})^\times\}$. The fixed part $S_k(\Gamma_1(N))^{\Gamma_0(N)} = S_k(N, 1)$ is equal to $S_k(N) = S_k(\Gamma_0(N))$.

## 1.2 Examples

We give some basic examples following [19] Chapter VII. First, we define the Eisenstein series. For an even integer $k \geq 4$, we put

$$G_k(\tau) = \sum_{m,n \in \mathbb{Z}, (m,n) \neq (0,0)} \frac{1}{(m\tau + n)^k}.$$

It is a modular form of weight $k$.

The $q$-expansion of an Eisenstein series is computed as follows. The logarithmic derivative of $\sin \pi\tau = \pi\tau \prod_{n=1}^{\infty} \left(1 - \frac{\tau^2}{n^2}\right)$ gives

$$-2\pi i \left(\frac{1}{2} + \sum_{n=1}^{\infty} q^n\right) = \frac{1}{\tau} + \sum_{n=1}^{\infty} \left(\frac{1}{\tau+n} + \frac{1}{\tau-n}\right).$$

Applying $k-1$-times the operator $q\frac{d}{dq} = \frac{1}{2\pi i}\frac{d}{d\tau}$, one gets

$$\sum_{n=1}^{\infty} n^{k-1} q^n = \frac{(-1)^k (k-1)!}{(2\pi i)^k} \sum_{n \in \mathbb{Z}} \frac{1}{(\tau+n)^k}.$$

For $k \geq 4$ even, by putting $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$ and

$$E_k(q) = 1 + \frac{2}{\zeta(1-k)} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n \in \mathbb{Q}[[q]],$$

we deduce

$$\begin{aligned} \frac{(k-1)!}{(2\pi i)^k} G_k(\tau) &= \frac{(k-1)!}{(2\pi i)^k} (2\zeta(k) + (G_k(\tau) - 2\zeta(k))) \\ &= \zeta(1-k) + 2\sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n = \zeta(1-k) E_k(q). \end{aligned}$$

Recall that the special values of the Riemann zeta function at negative odd integers

$$\zeta(-1) = -\frac{1}{12},\ \zeta(-3) = \frac{1}{120},\ \zeta(-5) = -\frac{1}{252},\ \ldots$$

are non-zero rational numbers (cf. [19] p.71, Chapter VII Proposition 7). The $\mathbb{C}$-algebra of modular forms of level 1 are generated by the Eisenstein series: $\bigoplus_{k=0}^{\infty} M_k(1)_{\mathbb{C}} = \mathbb{C}[E_4, E_6]$ (cf. loc. cit. Section 3.2).

The Delta-function defined by

$$\Delta(q) = \frac{1}{12^3}(E_4^3 - E_6^2) = q \prod_{n=1}^{\infty} (1-q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n$$

is a cusp form of weight 12 and of level 1 (see [19] Chapter VII Sections 4.4, 4.5). The space of cusp forms of level 1 are generated by the Delta-function as a module over the algebra of modular forms: $\bigoplus_{k=0}^{\infty} S_k(1)_{\mathbb{C}} = \mathbb{C}[E_4, E_6] \cdot \Delta$.

The function $f_{11}$ defined by

$$f_{11}(q) = q \prod_{n=1}^{\infty} (1-q^n)^2 (1-q^{11n})^2$$

is a basis of the space of cusp forms $S_2(11)_{\mathbb{C}}$ of level 11 and of weight 2 (see [12] Proposition 3.2.2).

## 1.3 Hecke operators

The space of modular forms has Hecke operators as its endomorphisms. More detail on Hecke opeators can be found in [12] Chapter 5. For every integer $n \geq 1$, the Hecke operator $T_n$ is defined as an endomorphism of $S_k(\Gamma_1(N))$. Here we only consider the case where $n = p$ is a prime. The general case is discussed later in §2.6.

For a prime number $p$, we define the Hecke operator $T_p$ by

$$T_p f(\tau) = \frac{1}{p}\sum_{i=0}^{p-1} f\left(\frac{\tau+i}{p}\right) + \begin{cases} p^{k-1}\langle p\rangle f(p\tau) & \text{if } p \nmid N \\ 0 & \text{if } p|N. \end{cases} \tag{1}$$

In terms of the $q$-expansion $f(\tau) = \sum_n a_n(f)q^n$, we have

$$T_p f(\tau) = \sum_{p|n} a_n(f)q^{n/p} + \begin{cases} p^{k-1}\sum_n a_n(\langle p\rangle f)q^{pn} & \text{if } p \nmid N \\ 0 & \text{if } p|N. \end{cases}$$

The Hecke operators on $S_k(\Gamma_1(N))$ are commutative to each other and formally satisfy the relation

$$\sum_{n=1}^{\infty} T_n n^{-s} = \prod_{p\nmid N}(1 - T_p p^{-s} + \langle p\rangle p^{k-1}p^{-2s})^{-1} \times \prod_{p|N}(1 - T_p p^{-s})^{-1}.$$

A cusp form $f = \sum_{n=1}^{\infty} a_n q^n \in S_k(N, \varepsilon)$ is called a normalized eigenform if $T_n f = \lambda_n f$ for all $n \geq 1$ and if $a_1 = 1$. Since $a_1(T_n f) = a_n(f)$, if $f \in S_k(N, \varepsilon)$ is a normalized eigenform, we have $\lambda_n = a_n$. For a normalized eigenform $f = \sum_{n=1}^{\infty} a_n q^n$, the subfield $\mathbb{Q}(f) = \mathbb{Q}(a_n, n \in \mathbb{N}) \subset \mathbb{C}$ is a finite extension of $\mathbb{Q}$, as we will see later at the end of §2.6.

Since $S_{12}(1) = \mathbb{C}\cdot\Delta$ and $S_2(11) = \mathbb{C}\cdot f_{11}$, the cusp forms $\Delta$ and $f_{11}$ are examples of normalized eigenforms.

For a cusp form $f = \sum_n a_n q^n \in S_k(\Gamma_1(N))$, the $L$-series is defined as a Dirichlet series

$$L(f, s) = \sum_{n=1}^{\infty} a_n n^{-s}.$$

It is known to converge absolutely on $\mathrm{Re}\, s > \dfrac{k+1}{2}$ as a consequence of the Ramanujan conjecture. If $f = \sum_n a_n q^n \in S_k(N, \varepsilon)$ is a normalized eigen form, the $L$-series $L(f, s)$ has an Euler product

$$L(f, s) = \prod_{p\nmid N}(1 - a_p p^{-s} + \varepsilon(p)p^{k-1}p^{-2s})^{-1} \times \prod_{p|N}(1 - a_p p^{-s})^{-1}.$$

## 1.4 Galois representations

To state the existence of a Galois representation associated to a modular form, we introduce some terminologies on Galois representations (cf. [12] Chapter 9). Let $p$ be a prime number. A choice of an embedding $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}_p}$ defines an embedding $G_{\mathbb{Q}_p} = \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \to G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. The Galois group $G_{\mathbb{Q}_p}$ thus regarded as a subgroup of $G_{\mathbb{Q}}$ is called the decomposition group. It is well-defined upto conjugacy.

The intermediate extension $\mathbb{Q}_p \subset \mathbb{Q}_p^{\mathrm{ur}} = \mathbb{Q}_p(\zeta_m; p \nmid m) \subset \overline{\mathbb{Q}_p}$ defines a normal subgroup $I_p = \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p^{\mathrm{ur}}) \subset G_{\mathbb{Q}_p}$ called the inertia subgroup. The quotient $G_{\mathbb{Q}_p}/I_p = \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p)$ is canonically identified with the absolute Galois group $G_{\mathbb{F}_p} = \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ of the residue field $\mathbb{F}_p$. The element $\varphi_p \in G_{\mathbb{F}_p}$ defined by $\varphi(a) = a^p$ for all $a \in \overline{\mathbb{F}_p}$ is called the Frobenius substitution. It is a free generator of $G_{\mathbb{F}_p}$ in the sense that the map $\widehat{\mathbb{Z}} = \varinjlim_n \mathbb{Z}/n\mathbb{Z} \to G_{\mathbb{F}_p}$ defined by sending 1 to $\varphi_p$ is an isomorphism.

Let $\ell$ be a prime, $E_\lambda$ be a finite extension of $\mathbb{Q}_\ell$ and $V$ be an $E_\lambda$-vector space of finite dimension. We call a continuous representation $G_{\mathbb{Q}} \to GL_{E_\lambda} V$ an $\ell$-adic representation of $G_{\mathbb{Q}}$. The group $GL_{E_\lambda} V$ is isomorphic to $GL_n(E_\lambda)$ as a topological group if $n = \dim_{E_\lambda} V$.

We say that an $\ell$-adic representation is unramified at a prime number $p$ if the restriction to the inertia group $I_p$ is trivial. In the following, we only consider $\ell$-adic representations unramified at every prime $p \nmid N\ell$ for some integer $N \geq 1$. For a prime $p \nmid N\ell$, the polynomial $\det(1 - \varphi_p t : V) \in E_\lambda[t]$ is well-defined.

**Definition 1.2** *Let $f = \sum_n a_n q^n \in S_k(N, \varepsilon)$ be a normalized eigen cusp form and $\mathbb{Q}(f) \to E_\lambda$ be an embedding to a finite extension of $\mathbb{Q}_\ell$. A 2-dimensional $\ell$-adic representation $V$ over $E_\lambda$ is said to be associated to $f$ if, for every $p \nmid N\ell$, $V$ is unramified at $p$ and*

$$\mathrm{Tr}(\varphi_p : V) = a_p(f).$$

The goal in this note is to explain the geometric proof of the following theorem.

**Theorem 1.3** *Let $N \geq 1$ and $k \geq 2$ be integers and $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a character. Let $f \in S_k(N, \varepsilon)$ be a normalized eigenform and $\lambda | \ell$ be place of $\mathbb{Q}(f)$. Then, there exists an $\ell$-adic representation $V_{f,\lambda}$ over $\mathbb{Q}(f)_\lambda$ associated to $f$.*

The following is a consequence of the geometric construction and the Weil conjecture.

**Corollary 1.4 (Ramanujan's conjecture** (see Corollary 4.5)**)** *For every prime $p$, we have*

$$|\tau(p)| \leq 2p^{\frac{11}{2}}.$$

Here is a reason why Frobenius's are so important.

**Theorem 1.5 (Cebotarev's density theorem)** *Let $L$ be a finite Galois extension of $\mathbb{Q}$ and $C \subset \mathrm{Gal}(L/\mathbb{Q})$ be a conjugacy class. Then there exist infinitely many prime $p$ such that $L$ is unramifed at $p$ and that $C$ is the class of $\varphi_p$.*

If $L = \mathbb{Q}(\zeta_N)$, this is equivalent to Dirichlet's Theorem on Primes in Arithmetic Progressions.

The following is a consequence of Theorem 1.5. Let $V_1$ and $V_2$ be $\ell$-adic representations of $G_{\mathbb{Q}}$. If there exists an integer $N \geq 1$ such that

$$\mathrm{Tr}(\varphi_p : V_1) = \mathrm{Tr}(\varphi_p : V_2)$$

for every prime $p \nmid N\ell$, the semi-simplifications $V_1^{\mathrm{ss}}$ and $V_2^{\mathrm{ss}}$ are isomorphic to each other. In particular, the $\ell$-adic representation associated to $f$ is unique upto isomorphism, since it is known to be irreducible by a theorem of Ribet [17]. It also follows that we may replace the condition $\mathrm{Tr}(\varphi_p : V) = a_p(f)$ in Definition 1.2 by a stronger one

$$\det(1 - \varphi_p t : V) = 1 - a_p(f)t + \varepsilon(p)p^{k-1}t^2.$$

# 2 Modular curves and modular forms

Modular forms are defined as certain holomorphic functions on the Poincaré upper half plane. To link them to Galois representations, we introduce modular curves. Modular curves are defined as the moduli of elliptic curves.

## 2.1 Elliptic curves

We define elliptic curves. Basic references for elliptic curves are [22], [16] Chapter 2. First, we consider elliptic curves over a field $k$ of characteristic $\neq 2, 3$. An elliptic curve over $k$ is the smooth compactification of an affine smooth curve defined by

$$y^2 = x^3 + ax + b$$

where $a, b \in k$ satisfying $4a^3 + 27b^2 \neq 0$. Or equivalently,

$$y^2 = 4x^3 - g_2 x - g_3$$

where $g_2, g_3 \in k$ satisfying $g_2^3 - 27g_3^2 \neq 0$.

More precisely, $E$ is the curve in the projective plane $\mathbf{P}^2_k$ defined by the homogeneous equation $Y^2 Z = X^3 + aXZ^2 + bZ^3$. The point $O = (0 : 1 : 0) \in E(k)$ is called the 0-section. Precisely speaking, an elliptic curve is a pair $(E, O)$ of a projective smooth curve $E$ of genus 1 and a $k$-rational point $O$. The embedding $E \to \mathbf{P}^2_k$ is defined by the basis $(x, y, 1)$ of $\Gamma(E, \mathcal{O}_E(3O))$. For an elliptic curve $E$ defined by $y^2 = 4x^3 - g_2 x - g_3$, the $j$-invariant is defined by

$$j(E) = 12^3 \frac{g_2^3}{g_2^3 - 27g_3^2}.$$

We define an elliptic curve over an arbitrary base scheme $S$. An elliptic curve over $S$ is a pair $(E, O)$ of a proper smooth curve $f : E \to S$ of genus 1 and a section

$O : S \to E$. We have $f_*\mathcal{O}_E = \mathcal{O}_S$ and $f_*\Omega^1_{E/S} = O^*\Omega^1_{E/S} = \omega_E$ is an invertible $\mathcal{O}_S$-module.

An elliptic curve has a commutative group structure. To define the addition, we introduce the Picard functor ([2] Chapter 8). For a scheme $X$, the Picard group $\mathrm{Pic}(X)$ is the isomorphism class group of invertible $\mathcal{O}_X$-modules. The addition is defined by the tensor product. If $X$ is a smooth proper curve over a field $k$, the Picard group $\mathrm{Pic}(X)$ is equal to the divisor class group

$$\mathrm{Coker}(\mathrm{div} : k(X)^\times \to \bigoplus_{x:\text{closed points of } X} \mathbb{Z}).$$

For a non-zero rational function $f \in k(X)^\times$, its divisor $\mathrm{div} f$ is defined to be $\sum_x \mathrm{ord}_x f \cdot [x]$. The degree map $\deg : \mathrm{Pic}(X) \to \mathbb{Z}$ is induced by the map $\bigoplus_{x:\text{closed points of } X} \mathbb{Z} \to \mathbb{Z}$, whose $x$-component is the multiplication by $[\kappa(x) : k]$.

Let $E$ be an elliptic curve over a scheme $S$. For a scheme $T$ over $S$, the degree map $\deg : \mathrm{Pic}(E \times_S T) \to \mathbb{Z}(T)$ has a section $\mathbb{Z}(T) \to \mathrm{Pic}(E \times_S T)$ defined by $1 \mapsto [\mathcal{O}(O)]$. For an invertible $\mathcal{O}_{E\times_S T}$-module $\mathcal{L}$, its degree $\deg \mathcal{L} : T \to \mathbb{Z}$ is the locally constant function defined by $\deg \mathcal{L}(t) = \deg(\mathcal{L}|_{E\times_T t})$. The pull-back $O^* : \mathrm{Pic}(E \times_S T) \to \mathrm{Pic}(T)$ also has a section $f^* : \mathrm{Pic}(T) \to \mathrm{Pic}(E \times_S T)$. Thus, we have a decomposition

$$\mathrm{Pic}(E \times_S T) = \mathbb{Z}(T) \oplus \mathrm{Pic}(T) \oplus \mathrm{Pic}^0_{E/S}(T)$$

and a functor $\mathrm{Pic}^0_{E/S} : (\text{Schemes}/S) \to (\text{Abelian groups})$ is defined. We define a morphism of functors $E \to \mathrm{Pic}^0_{E/S}$ by sending $P \in E(T)$ to the projection of the class $[\mathcal{O}_{E_T}(P)] \in \mathrm{Pic}(E \times_S T)$.

**Theorem 2.1 (Abel's theorem)** (cf. [16] Theorem 2.1.2) *The morphism $E \to \mathrm{Pic}^0_{E/S}$ of functors is an isomorphism.*

The inverse $\mathrm{Pic}^0_{E/S} \to E$ is defined as follows. For $[\mathcal{L}] \in \mathrm{Pic}^0_{E/S}(T)$, the support of the cokernel of the natural map $f_T^* f_{T*}(\mathcal{L}(O)) \to \mathcal{L}(O)$ defines a section $T \to E \times_S T$.

Since $\mathrm{Pic}^0_{E/S}$ is a sheaf of abelian groups, the isomorphism $E \to \mathrm{Pic}^0_{E/S}$ defines a group structure on the scheme $E$ over $S$. For a morphism $f : E \to E'$, the pull-back map $f^* : \mathrm{Pic}^0_{E'/S} \to \mathrm{Pic}^0_{E/S}$ defines the dual $f^* : E' \to E$. The map $f : E \to E'$ itself is identified with the push-forward map $f_* : E \to E'$ induced by the norm map recalled later in §3.2. We have $f \circ f^* = [\deg f]_{E'}$ and hence $f^* \circ f = [\deg f]_E$.

If an elliptic curve $E$ over a field $k$ is defined by $y^2 = x^3 + ax + b$, the addition on $E(k)$ is described as follows. Let $P, Q \in E(k)$. The line $PQ$ meets $E$ at the third point $R'$. The divisor $[P]+[Q]+[R']$ is linearly equivalent to the divisor $[O]+[R]+[R']$, where $R$ is the opposite of $R'$ with respect to the $x$-axis. Thus, we have $[P] + [Q] + [R'] = [O] + [R] + [R']$ in $\mathrm{Pic}(E)$ and $([P] - [O]) + ([Q] - [O]) = [R] - [O]$ in $\mathrm{Pic}^0(E)$. Hence we have $P + Q = R$ in $E(k)$.

We introduce the Weil pairing (cf. [16] Section 2.8). For an elliptic curve $f : E \to S$ and an integer $N \geq 1$, the Weil pairing is a non-degenerate alternating pairing

$(\ ,\ )_{E[N]} : E[N] \times E[N] \to \mu_N$. Here and in the following, $E[N]$ and $\mu_N$ denote the kernels of the multiplications $[N] : E \to E$ and $[N] : \mathbf{G}_m \to \mathbf{G}_m$. Non-degerate means that the induced map $E[N] \to E[N]^* = Hom(E[N], \mu_N)$ to the Cartier dual (see [4] Chapter V Section (3.8)) is an isomorphism of finite group schemes.

Let $P \in E[N](S)$ be an $N$-torsion point and $\mathcal{L}$ be an invertible $\mathcal{O}_E$-module corresponding to $P$. Since $[[N]^*\mathcal{L}] = NP = 0$, the invertible $\mathcal{O}_E$-module $[N]^*\mathcal{L}$ is canonically isomorphic to the pull-back of an invertible $\mathcal{O}_S$-module $f_*[N]^*\mathcal{L}$. For another $N$-torsion point $Q \in E[N](S)$, the translation $Q+$ satisfies $[N] \circ (Q+) = [N]$. Hence it induces an automorphisms $Q^*$ of $[N]^*\mathcal{L}$ and of $f_*[N]^*\mathcal{L}$ by pull-back. Thus we obtain a morphism $(P,\ )_{E[N]} : E[N] \to \mu_N \subset \mathbf{G}_m = \mathrm{Aut}\ f_*[N]^*\mathcal{L}$ sending $Q$ to $Q^*$, that defines a bilinear pairing $(\ ,\ )_{E[N]} : E[N] \times E[N] \to \mu_N$.

## 2.2 Elliptic curves over $\mathbb{C}$

To give an elliptic curve over $\mathbb{C}$ is equivalent to give a complex torus of dimension 1, as follows. For more detail, see [22] Chapter VI and [12] Section 1.4.

Let $E$ be an elliptic curve over $\mathbb{C}$. Then, $E(\mathbb{C})$ is a connected compact abelian complex Lie group of dimension 1. The tangent space $\mathrm{Lie}\ E$ of $E(\mathbb{C})$ at the origin is a $\mathbb{C}$-vector space of dimension 1. The exponential map $\exp : \mathrm{Lie}\ E \to E(\mathbb{C})$ is surjective and the kernel is a lattice of $E(\mathbb{C})$ and is identified with the singular homology $H_1(E(\mathbb{C}), \mathbb{Z})$. A lattice $L$ of a complex vector space $V$ of finite dimension is a free abelian subgroup generated by an $\mathbb{R}$-basis.

Conversely, let $L$ be a lattice of $\mathbb{C}$. The $\wp$-function is defined by

$$x = \wp(z) = \frac{1}{z^2} + \sum_{\omega \in L, \omega \neq 0} \left( \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Since

$$y = \frac{d\wp(z)}{dz} = -2 \sum_{\omega \in L} \frac{1}{(z-\omega)^3},$$

they satisfy the Weierstrass equation

$$y^2 = 4x^3 - g_2 x - g_3$$

where $g_2 = 60 \displaystyle\sum_{\omega \in L, \omega \neq 0} \frac{1}{\omega^4}$ and $g_3 = 140 \displaystyle\sum_{\omega \in L, \omega \neq 0} \frac{1}{\omega^6}$. If $L = \mathbb{Z} + \mathbb{Z}\tau$ for $\tau \in H$, we have

$$\begin{aligned} g_2 &= 60 G_4(\tau) = 60 \cdot \frac{(2\pi i)^4}{3!} \frac{1}{120} E_4 = \frac{(2\pi i)^4}{12} E_4, \\ g_3 &= 140 G_6(\tau) = 140 \cdot \frac{(2\pi i)^6}{5!} \left( -\frac{1}{252} \right) E_6 = -\frac{(2\pi i)^6}{6^3} E_6 \end{aligned}$$

and hence

$$g_2^3 - 27 g_3^2 = (2\pi i)^{12} \frac{1}{12^3} (E_4^3 - E_6^2) = (2\pi i)^{12} \Delta \neq 0.$$

Thus the equation $y^2 = 4x^3 - g_2x - g_3$ defines an elliptic curve $E$ over $\mathbb{C}$. The map $\mathbb{C}/L \to E(\mathbb{C})$ defined by $z \mapsto (\wp(z), \wp'(z))$ is an isomorphism of compact Riemann surfaces.

We show that the Weil pairing $(P, Q) \in \mu_N(\mathbb{C})$ for the $N$-torsion points $P = \frac{1}{N}, Q = \frac{\tau}{N} \in E = \mathbb{C}/\langle 1, \tau\rangle$ is equal to $\exp \frac{2\pi\sqrt{-1}}{N}$. The elliptic function

$$f(z) = \frac{\sigma(z)}{\sigma(z-1)} \prod_{i,j=1,\dots,N} \frac{\sigma(z - \frac{1}{N}(i + j\tau + \frac{1}{N}))}{\sigma(z - \frac{1}{N}(i + j\tau))}$$

is a basis of $[N]^*\mathcal{L}$ for $\mathcal{L} = \mathcal{O}_E(P - O)$ where $\sigma$ denotes the Weierstrass's $\sigma$-function for the lattice $\langle 1, \tau\rangle$ (for the definition, see [22] p. 156). Hence, the Weil pairing $(P, Q)$ is equal to the ratio $\dfrac{f(z + \frac{\tau}{N})}{f(z)}$. We see that it is equal to $\exp \dfrac{\eta(1)\tau - \eta(\tau)1}{N}$, by using the formula $\dfrac{\sigma(z+\omega)\sigma(w)}{\sigma(z)\sigma(w+\omega)} = \exp(\eta(\omega)(z-w))$ for $z, w \in \mathbb{C}$ and $\omega \in \langle 1, \tau\rangle$ ([23] Proposition 5.4 (b)). where $\eta$ denotes the Dedekind $\eta$-function (for the definition, see loc. cit. p. 65). Thus the assertion follows from the Legendre relation $\eta(1)\tau - \eta(\tau)1 = 2\pi\sqrt{-1}$ (loc. cit. Proposition 5.2 (d)).

## 2.3 Modular curves over $\mathbb{C}$

The set of isomorphism classes of elliptic curves over $\mathbb{C}$ has a one-to-one correspondence with the quotient of the Poincaré upper half plane by $SL_2(\mathbb{Z})$. The $j$-invariant defines an isomorphism $SL_2(\mathbb{Z})\backslash H \to \mathbb{C}$ of Riemann surfaces. Modular curves over $\mathbb{C}$ are defined as finite coverings of an algebraic curve $SL_2(\mathbb{Z})\backslash H$ over $\mathbb{C}$. More detail is found in [12] Chapters 2 and 3.

We put

$$\mathcal{R} = \{\text{lattices in } \mathbb{C}\}, \quad \widetilde{\mathcal{R}} = \{(\omega_1, \omega_2) \in \mathbb{C}^{\times 2} | \mathrm{Im}\frac{\omega_1}{\omega_2} > 0\}.$$

The multiplication defines an action of $\mathbb{C}^\times$ on $\mathcal{R}$ and on $\widetilde{\mathcal{R}}$. We consider the map $\widetilde{\mathcal{R}} \to \mathcal{R}$ sending $(\omega_1, \omega_2)$ to the lattice $\langle \omega_1, \omega_2\rangle$ generated by $\omega_1, \omega_2$. A natural action of $SL_2(\mathbb{Z})$ on $\widetilde{\mathcal{R}}$ is defined by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} a\omega_1 + b\omega_2 \\ c\omega_1 + d\omega_2 \end{pmatrix}$. It induces a bijection $SL_2(\mathbb{Z})\backslash\widetilde{\mathcal{R}} \to \mathcal{R}$. The map $H \to \widetilde{\mathcal{R}} : \tau \to (\tau, 1)$ is compatible with the action of $SL_2(\mathbb{Z})$ and induces bijections

$$H \to \mathbb{C}^\times\backslash\widetilde{\mathcal{R}}, \quad SL_2(\mathbb{Z})\backslash H \to (SL_2(\mathbb{Z}) \times \mathbb{C}^\times)\backslash\widetilde{\mathcal{R}} \to \mathbb{C}^\times\backslash\mathcal{R}.$$

The map sending a lattice $L$ to the isomorphism class of the elliptic curve $\mathbb{C}/L$ defines bijections

$$SL_2(\mathbb{Z})\backslash H \to \mathbb{C}^\times\backslash\mathcal{R} \to \{\text{isomorphism classes of elliptic curves over } \mathbb{C}\}.$$

The quotient $Y(1)(\mathbb{C}) = SL_2(\mathbb{Z})\backslash H$ is called the modular curve of level 1. The map

$$j : SL_2(\mathbb{Z})\backslash H \to \mathbb{C}$$

defined by the $j$-invariant

$$j(\tau) = 1728\frac{g_2(\tau)^3}{g_2(\tau)^3 - 27g_3(\tau)^2} = \frac{E_4^3}{\Delta}$$

is an isomorphism of Riemann surfaces ([19] Chapter 7 Proposition 5).

For an integer $N \geq 1$, similarly the map sending $(\omega_1, \omega_2) \in \widetilde{\mathcal{R}}$ to the pair $(E, P) = \left(\mathbb{C}/\langle\omega_1, \omega_2\rangle, \dfrac{\omega_2}{N}\right)$ defines a bijection

$$\begin{aligned} \Gamma_1(N)\backslash H &\to (\Gamma_1(N) \times \mathbb{C}^\times)\backslash\widetilde{\mathcal{R}} \\ &\to \left\{\begin{matrix}\text{isom. classes of pairs } (E, P) \text{ of an elliptic curve} \\ E \text{ over } \mathbb{C} \text{ and a point } P \in E(\mathbb{C}) \text{ of order } N\end{matrix}\right\}. \end{aligned}$$

Note that $\dfrac{c\omega_1 + d\omega_2}{N} \equiv \dfrac{\omega_2}{N} \bmod \langle\omega_1, \omega_2\rangle$ since $c \equiv 0, d \equiv 1 \bmod N$ for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$. The quotient $\Gamma_1(N)\backslash H$ is denoted by $Y_1(N)(\mathbb{C})$ and is called the modular curve of level $\Gamma_1(N)$.

The diamond operators act on $Y_1(N)(\mathbb{C})$. For $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, the action of $\langle d\rangle$ is given by $\langle d\rangle(E, P) = (E, dP)$. The quotient $\Gamma_0(N)\backslash H = (\mathbb{Z}/N\mathbb{Z})^\times\backslash Y_1(N)(\mathbb{C})$ is denoted by $Y_0(N)(\mathbb{C})$ and is called the modular curve of level $\Gamma_0(N)$. We have a natural bijection

$$\Gamma_0(N)\backslash H \to \left\{\begin{matrix}\text{isom. classes of pairs } (E, C) \text{ of an elliptic curve } E \\ \text{over } \mathbb{C} \text{ and a cyclic subgroup } C \subset E(\mathbb{C}) \text{ of order } N\end{matrix}\right\}.$$

We have finite flat maps $Y_1(N) \to Y_0(N) \to Y(1) = \mathbf{A}^1$ of open Riemann surfaces. The degrees of the maps are given by

$$[Y_1(N) : Y_0(N)] = \sharp(\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\} = \begin{cases} \varphi(N)/2 & \text{if } N \geq 3 \\ 1 & \text{if } N \leq 2, \end{cases}$$

and $[Y_0(N) : Y(1)] = [SL_2(\mathbb{Z}) : \Gamma_0(N)]$.

Let $X_1(N)$ and $X_0(N)$ be the compactifications of $Y_1(N)$ and $Y_0(N)$. The maps $Y_1(N) \to Y_0(N) \to Y(1) = \mathbf{A}^1$ are uniquely extended to finite flat maps $X_1(N) \to X_0(N) \to X(1) = \mathbf{P}^1$ of compact Riemann surfaces, or equivalently of projective smooth curves over $\mathbb{C}$.

We identify $f \in S_2(N)$ with $f \cdot 2\pi i d\tau \in \Gamma(X_0(N), \Omega^1)$ and $S_2(N) = \Gamma(X_0(N), \Omega^1)$. Applying the Riemann-Hurwitz formula to the map $j : X_0(N) \to X(1) = \mathbf{P}^1$, we obtain the genus formula

$$g(X_0(N)) = g_0(N) = 1 + \frac{1}{12}[SL_2(\mathbb{Z}) : \Gamma_0(N)] - \frac{1}{2}\varphi_\infty(N) - \frac{1}{3}\varphi_6(N) - \frac{1}{4}\varphi_4(N)$$

where

$$\varphi_6(N) = \begin{cases} 0 & \text{if } 9|N \text{ or if } \exists p|N, p \equiv -1 \bmod 3 \\ 2^{\sharp\{p|N \,:\, p \equiv 1 \bmod 3\}} & \text{if otherwise,} \end{cases}$$

$$\varphi_4(N) = \begin{cases} 0 & \text{if } 4|N \text{ or if } \exists p|N, p \equiv -1 \bmod 4 \\ 2^{\sharp\{p|N \,:\, p \equiv 1 \bmod 4\}} & \text{if otherwise.} \end{cases}$$

and $\varphi_\infty(NM) = \varphi_\infty(N)\varphi_\infty(M)$ if $(N, M) = 1$ and, for a prime $p$ and $e > 0$,

$$\varphi_\infty(p^e) = \begin{cases} 2p^{(e-1)/2} & \text{if } e \text{ odd} \\ (p+1)p^{e/2-1} & \text{if } e \text{ even.} \end{cases}$$

We have $g_0(11) = 1$ and hence $X_0(11)$ is an elliptic curve, defined by the equation $y^2 = 4x^3 - \frac{124}{3}x - \frac{2501}{27}$, where $\Delta = \left(\frac{124}{3}\right)^3 - 27\left(\frac{2501}{27}\right)^2 = -11^5$. The space $S_2(11) = \Gamma(X_0(11), \Omega^1)$ of cusp forms of weight 2 and level 11 is generated by the differential form $\dfrac{dx}{y}$ corresponding to $f_{11}$.

The universal elliptic curves over the modular curves $Y_1(N)$ for $N \geq 4$ are defined as follows. We consider the semi-direct product $\Gamma_1(N) \ltimes \mathbb{Z}^2$ with respect to the left action by ${}^t\gamma^{-1}$. We define an action of $\mathbb{C}^\times \times \Gamma_1(N) \ltimes \mathbb{Z}^2$ on $\widetilde{\mathcal{R}} \times \mathbb{C}$ by

$$\begin{aligned} c((\omega_1, \omega_2), z) &= ((c\omega_1, c\omega_2), cz) \\ \gamma((\omega_1, \omega_2), z) &= ((a\omega_1 + b\omega_2, c\omega_1 + d\omega_2), z) \\ (m, n)((\omega_1, \omega_2), z) &= ((\omega_1, \omega_2), z + m\omega_1 + n\omega_2). \end{aligned}$$

for $c \in \mathbb{C}^\times$, $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$ and $(m, n) \in \mathbb{Z}^2$. The projection $\widetilde{\mathcal{R}} \times \mathbb{C} \to \widetilde{\mathcal{R}}$ is compatible with the projection $\mathbb{C}^\times \times \Gamma_1(N) \ltimes \mathbb{Z}^2 \to \mathbb{C}^\times \times \Gamma_1(N)$.

Assume $N \geq 4$. By taking the quotient, we obtain

$$E_{Y_1(N)} = (\Gamma_1(N) \ltimes \mathbb{Z}^2)\backslash(H \times \mathbb{C}) \to Y_1(N) = \Gamma_1(N)\backslash H.$$

The fiber at $\tau \in H$ is the elliptic curve $\mathbb{C}/\mathbb{Z}+\mathbb{Z}\tau$. If $N = 1, 2$, we have $-1 \in \Gamma_1(N)$ and the general fiber is the quotient of $\mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau$ by the involution $-1$ and is isomorphic to $\mathbf{P}^1$. For $N = 3$, the fibers at primitive cubic roots $\tau = \omega, \omega^{-1}$ are also isomorphic to $\mathbf{P}^1$.

The universal elliptic curve $E_{Y_1(N)}$ has the following modular interpretation.

**Lemma 2.2** *Assume $N \geq 4$. Let $f : E \to S$ be a holomorphic family of elliptic curve and $P : S \to E$ be a section of exact order $N$. Then, there exists a unique morphism $S \to Y_1(N)$ such that $(E, P)$ is isomorphic to the pull-back of the universal elliptic curve $E_{Y_1(N)}$ and the section defined by $z = \dfrac{\omega_2}{N}$.*

*Sketch of Proof.* Since the question is local on $S$, we may take basis of $\omega = O^*\Omega^1_{E/S}$ and of $R^1f_*\mathbb{Z}$. Then, they give a family of lattices in $\mathbb{C}$ parametrized by $S$ and define a map $S \to \widetilde{\mathcal{R}}$. The induced map $S \to Y_1(N) = (\Gamma_1(N) \times \mathbb{C}^\times)\backslash\widetilde{\mathcal{R}}$ is well-defined and satisfies the condition. ■

## 2.4 Modular curves and modular forms

The definition of modular forms given in Section 1.1 is rephrased in terms of the universal elliptic curves as follows. For more detail, we refer to [6] Chapitre VII, Sections 3 and 4 and also [11] Sections 12.1, 12.3.

Let $N \geq 4$. Let $\omega_{Y_1(N)}$ be the invertible sheaf $O^*\Omega_{E_{Y_1(N)}/Y_1(N)}$ where $O : Y_1(N) \to E_{Y_1(N)}$ is the 0-section of the universal elliptic curve. Then, we have

$$\{f : H \to \mathbb{C} | f \text{ is holomorphic and satisfies (1) in Definition 1.1}\} = \Gamma(Y_1(N), \omega^{\otimes k})$$

by identifying $f$ with $f \cdot (2\pi\sqrt{-1}dz)^{\otimes k}$. By the isomorphism $\omega^{\otimes 2} \to \Omega_{Y_1(N)}$ sending $(2\pi\sqrt{-1}dz)^{\otimes 2} \mapsto 2\pi\sqrt{-1}d\tau$, the left hand side is identified with $\Gamma(Y_1(N), \omega^{\otimes k-2} \otimes \Omega_{Y_1(N)})$.

Assume $N \geq 5$. Then the universal elliptic curve $E_{Y_1(N)} \to Y_1(N)$ is uniquely extended to a smooth group scheme $\overline{E}_{Y_1(N)} \to X_1(N)$ whose fibers at cusps are $\mathbf{G}_m$. Let $\omega_{X_1(N)} = O^*\Omega_{\overline{E}_{Y_1(N)}/X_1(N)}$. Since $2\pi\sqrt{-1}d\tau = \dfrac{dq}{q}$, the isomorphism $\omega^{\otimes 2} \to \Omega_{Y_1(N)}$ on $Y_1(N)$ is extended to an isomorphism $\omega^{\otimes 2}_{X_1(N)} \to \Omega_{X_1(N)}(\log(\text{cusps}))$ on $X_1(N)$. By the isomorphism $\omega^{\otimes 2}_{X_1(N)} \to \Omega_{X_1(N)}(\log(\text{cusps}))$, we may identify

$$M_k(\Gamma_1(N)) = \Gamma(X_1(N), \omega^{\otimes k}) \supset S_k(\Gamma_1(N)) = \Gamma(X_1(N), \omega^{\otimes k-2} \otimes \Omega_{X_1(N)}).$$

Since $X_1(N)$ is compact, the $\mathbb{C}$-vector spaces $M_k(\Gamma_1(N))$ and $S_k(\Gamma_1(N))$ are of finite dimension.

For $N \geq 5$, there exists a constant $C$ satisfying $\deg \omega = C \cdot [SL_2(\mathbb{Z}) : \Gamma_1(N)]$. The isomorphism $\omega^{\otimes 2} \to \Omega^1_{X_1(N)}(\log \text{cusps})$ implies

$$2g_1(N) - 2 + \frac{1}{2}\sum_{d|N} \varphi(\frac{N}{d})\varphi(d) = 2C \cdot [SL_2(\mathbb{Z}) : \Gamma_1(N)].$$

In particular, for $p \geq 5$, we have

$$2g_1(p) - 2 + p - 1 = 2C \cdot (p^2 - 1).$$

Since $g_1(5) = 0$, we have $C = \frac{1}{24}$ and

$$\dim S_2(\Gamma_1(N)) = g_1(N) = \begin{cases} 1 + \dfrac{1}{24}[SL_2(\mathbb{Z}) : \Gamma_1(N)] - \dfrac{1}{4}\displaystyle\sum_{d|N} \varphi(\frac{N}{d})\varphi(d) & \text{if } N \geq 5, \\ 0 & \text{if } N \leq 4. \end{cases}$$

By Riemann-Roch, we have

$$\begin{aligned} \dim S_k(\Gamma_1(N)) &= \deg(\omega^{\otimes(k-2)} \otimes \Omega^1) + \chi(X_1(N), \mathcal{O}) = (k-2)\deg\omega + g_1(N) - 1 \\ &= \frac{k-1}{24}[SL_2(\mathbb{Z}) : \Gamma_1(N)] - \frac{1}{4}\sum_{d|N} \varphi(\frac{N}{d})\varphi(d) \end{aligned}$$

for $k \geq 3, N \geq 5$.

## 2.5 Modular curves over $\mathbb{Z}[\frac{1}{N}]$

To construct Galois representations associated to modular forms, we descend the definition field of modular curves to $\mathbb{Q}$ and consider their integral models over $\mathbb{Z}[\frac{1}{N}]$.

Let $N \geq 1$ be an integer and $T$ be a scheme over $\mathbb{Z}[\frac{1}{N}]$. We say a section $P : T \to E$ of an elliptic curve $E \to T$ is exactly of order $N$, if $NP = 0$ and if $P_t \in E_t(t)$ is of order $N$ for every point $t \in T$. We define a functor $\mathcal{M}_1(N) : (\text{Scheme}/\mathbb{Z}[\frac{1}{N}]) \to (\text{Sets})$ by

$$\mathcal{M}_1(N)(T) = \left\{ \begin{matrix} \text{isomorphism classes of pairs } (E, P) \text{ of an elliptic curve} \\ E \to T \text{ and a section } P \in E(T) \text{ exactly of order } N \end{matrix} \right\}.$$

**Theorem 2.3** ([16] Corollaries 2.7.3 and 4.7.1) *For an integer $N \geq 4$, the functor $\mathcal{M}_1(N)$ is representable by a smooth affine curve over $\mathbb{Z}[\frac{1}{N}]$.*

Namely, there exist a smooth affine curve $Y_1(N)_{\mathbb{Z}[\frac{1}{N}]}$ over $\mathbb{Z}[\frac{1}{N}]$ and a pair $(E, P)$ of elliptic curves $E \to Y_1(N)_{\mathbb{Z}[\frac{1}{N}]}$ and a section $P : Y_1(N)_{\mathbb{Z}[\frac{1}{N}]} \to E$ exactly of order $N$ such that the map

$$\mathrm{Hom}_{\text{Scheme}/\mathbb{Z}[\frac{1}{N}]}(T, Y_1(N)_{\mathbb{Z}[\frac{1}{N}]}) \to \mathcal{M}_1(N)(T)$$

sending $f : T \to Y_1(N)_{\mathbb{Z}[\frac{1}{N}]}$ to the class of $(f^*E, f^*P)$ is a bijection for every scheme $T$ over $\mathbb{Z}[\frac{1}{N}]$.

If $N \leq 3$, the functor $\mathcal{M}_1(N)$ is not representable because there exists a pair $(E, P) \in \mathcal{M}_1(N)(T)$ with a non-trivial automorphism. More precisely, by étale descent, there exist 2 distinct elements $(E, P), (E', P') \in \mathcal{M}_1(N)(T)$ whose pull-backs are the same for some étale covering $T' \to T$.

*Proof of Theorem for $N = 4$.* Let $E \to T$ be an elliptic curve over a scheme $T$ over $\mathbb{Z}[\frac{1}{2}]$ and $P$ be a section of exact order 4. We take a coordinate of $E$ so that $2P = (0, 0), P = (1, 1), 3P = (1, -1)$ and let $dy^2 = x^3 + ax^2 + bx + c$ be the equation defining $E$. Then the line $y = x$ meets $E$ at $2P$ and is tangent to $E$ at $P$. Thus we have $x^3 + (a-d)x^2 + bx + c = x(x-1)^2$. Namely, $E$ is defined by $dy^2 = x^3 + (d-2)x^2 + x$. The moduli $Y_1(4)_{\mathbb{Z}[\frac{1}{4}]}$ is given by $\mathrm{Spec}\mathbb{Z}[\frac{1}{4}][d, \frac{1}{d(d-4)}]$. ■

To prove the general case, we consider the following variant. For an elliptic curve $E$ and an integer $r \geq 1$, let $E[r] = \mathrm{Ker}([r] : E \to E)$ denote the kernel of the multiplication by $r$. We define a functor $\mathcal{M}(r) : (\mathrm{Scheme}/\mathbb{Z}[\frac{1}{r}]) \to (\mathrm{Sets})$ by

$$\mathcal{M}(r)(T) = \left\{ \begin{array}{l} \text{isom. classes of pairs } (E,(P,Q)) \text{ of an elliptic curve } E \to T \\ \text{and } P, Q \in E(T) \text{ defining an isomorphism } (\mathbb{Z}/r\mathbb{Z})^2 \to E[r] \end{array} \right\}.$$

**Theorem 2.4** *For an integer $r \geq 3$, the functor $\mathcal{M}(r)$ is representable by a smooth affine curve $Y(r)_{\mathbb{Z}[\frac{1}{r}]}$ over $\mathbb{Z}[\frac{1}{r}]$.*

*Sketch of Proof.* If $r = 3$, the functor $\mathcal{M}(r)$ is representable by the smooth affine curve $Y(3) = \mathrm{Spec}\ \mathbb{Z}[\frac{1}{3}, \zeta_3][\mu, \frac{1}{\mu^3 - 1}]$ over $\mathrm{Spec}\ \mathbb{Z}[\frac{1}{3}]$. The universal elliptic curve $E \subset \mathbf{P}^2$ is defined by $X^3 + Y^3 + Z^3 - 3\mu XYZ$ and the origin is $O = (0, 1, -1)$. The basis of $E[3]$ is given by $P = (0, 1, -\omega^2)$ and $Q = (1, 0, -1)$.

Next we consider the case $r = 4$. Let $E$ be the universal elliptic curve over $Y_1(4)$ and $P$ be the universal section of order 4. Then, the Weil pairing $(P, \ )$ defines a map $E[4] \to \mu_4$. The modular curve $Y(4)$ is the inverse image of the complement of the open and closed subscheme $\mu_2 \subset \mu_4$.

If $r$ is divisible by $s = 3$ or $4$, one can construct $Y(r)_{\mathbb{Z}[\frac{1}{r}]}$ as a finite étale scheme over $Y(s)_{\mathbb{Z}[\frac{1}{r}]}$. For general $r \geq 5$, the modular curve $Y(r)_{\mathbb{Z}[\frac{1}{r}]}$ is obtained by patching the quotient $Y(r)_{\mathbb{Z}[\frac{1}{sr}]} = Y(sr)_{\mathbb{Z}[\frac{1}{sr}]}/\mathrm{Ker}(GL_2(\mathbb{Z}/rs\mathbb{Z}) \to GL_2(\mathbb{Z}/r\mathbb{Z}))$ for $s = 3, 4$. ■

By the Weil pairing, the scheme $Y(r)_{\mathbb{Z}[\frac{1}{r}]}$ is naturally a scheme over $\mathbb{Z}[\frac{1}{r}, \zeta_r]$. For $r = 1, 2$, the modular curves $Y(r)_{\mathbb{Z}[\frac{1}{r}]}$ are also defined by patching the quotients. The $j$-invariant defines an isomorphism $Y(1)_{\mathbb{Z}} \to \mathbb{A}^1_{\mathbb{Z}}$. The Legendre curve $y^2 = x(x-1)(x-\lambda)$ defines an isomorphism $\mathrm{Spec}\mathbb{Z}[\frac{1}{2}][\lambda, \frac{1}{\lambda(\lambda-1)}] \to Y(2)_{\mathbb{Z}[\frac{1}{2}]}$.

By regarding $P, Q \in E[N]$ as a map $(\mathbb{Z}/N\mathbb{Z})^2 \to E[N]$, we define a natural right action of $GL_2(\mathbb{Z}/N\mathbb{Z})$ on $\mathcal{M}(N)$ and hence on $Y(N)$ as that induced by the natural action of $GL_2(\mathbb{Z}/N\mathbb{Z})$ on $(\mathbb{Z}/N\mathbb{Z})^2$.

The modular curve $Y_1(N)_{\mathbb{Z}[\frac{1}{N}]}$ is constructed as the quotient

$$Y(N)_{\mathbb{Z}[\frac{1}{N}]} \Big/ \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}/N\mathbb{Z}) \middle| a = 1, c = 0 \right\}.$$

The modular curve $Y_1(N)_{\mathbb{Z}[\frac{1}{N}]}$ for $N \leq 3$ are also defined as the quotients.

The Atkin-Lehner involution $w_N : Y_1(N)_{\mathbb{Z}[\frac{1}{N}, \zeta_N]} \to Y_1(N)_{\mathbb{Z}[\frac{1}{N}, \zeta_N]}$ is defined by sending $(E, P)$ to $(E/\langle P \rangle, Q)$ where $Q \in E[N]/\langle P \rangle \subset (E/\langle P \rangle)[N]$ is the inverse image of $\zeta_N \in \mu_N$ by the isomorphism $(P, \ ) : E[N]/\langle P \rangle \to \mu_N$.

The affine smooth curve $Y_1(N)_{\mathbb{Z}[\frac{1}{N}]}$ is uniquely embedded in a proper smooth curve $X_1(N)_{\mathbb{Z}[\frac{1}{N}]}$ over $\mathbb{Z}[\frac{1}{N}]$ ([6] Chapitre IV 4.14, [11] Section 9). The universal elliptic curve $E_{Y_1(N)_{\mathbb{Z}[\frac{1}{N}]}}$ over $Y_1(N)_{\mathbb{Z}[\frac{1}{N}]}$ is uniquely extended to a smooth group scheme $E_{X_1(N)_{\mathbb{Z}[\frac{1}{N}]}}$ over $X_1(N)_{\mathbb{Z}[\frac{1}{N}]}$ such that the fiber at every geometric point in the complement $X_1(N)_{\mathbb{Z}[\frac{1}{N}]} \setminus Y_1(N)_{\mathbb{Z}[\frac{1}{N}]}$ is isomorphic to $\mathbf{G}_m$ (loc. cit.). We define an invertible sheaf $\omega_{X_1(N)_{\mathbb{Z}[\frac{1}{N}]}}$ to be the inverse image $O^*\Omega^1_{E_{X_1(N)_{\mathbb{Z}[\frac{1}{N}]}}/X_1(N)_{\mathbb{Z}[\frac{1}{N}]}}$. The $\mathbb{Q}$-vector space $S_k(\Gamma_1(N))_{\mathbb{Q}} = \Gamma(X_1(N)_{\mathbb{Q}}, \omega^{\otimes k-2} \otimes \Omega^1)$ gives a $\mathbb{Q}$-structure of the $\mathbb{C}$-vector space $S_k(\Gamma_1(N))_{\mathbb{C}} = \Gamma(X_1(N)_{\mathbb{C}}, \omega^{\otimes k-2} \otimes \Omega^1)$.

## 2.6 Hecke operators

In this subsection, we give an algebraic definition of the Hecke operators. For more detail, we refer to [12] Section 7.9.

For integers $N, n \geq 1$, we define a functor $\mathcal{T}_1(N,n)_{\mathbb{Z}[\frac{1}{N}]} : (\text{Schemes}/\mathbb{Z}[\frac{1}{N}]) \to (\text{Sets})$ by

$$\begin{aligned} &\mathcal{T}_1(N,n)_{\mathbb{Z}[\frac{1}{N}]}(T) \\ = &\left\{ \begin{array}{c} \text{isom. classes of triples } (E,P,C) \text{ of an elliptic curve } E \text{ over } T, \text{ a} \\ \text{section } P : T \to E \text{ exactly of order } N \text{ and a subgroup scheme} \\ C \subset E \text{ finite flat of degree } n \text{ over } T \text{ such that } \langle P \rangle \cap C = O \end{array} \right\} \end{aligned}$$

and a morphism $s : \mathcal{T}_1(N,n)_{\mathbb{Z}[\frac{1}{N}]} \to \mathcal{M}_1(N)_{\mathbb{Z}[\frac{1}{N}]}$ of functors sending $(E,P,C)$ to $(E,P)$. The functor $\mathcal{T}_1(N,n)_{\mathbb{Z}[\frac{1}{N}]}$ is representable by a finite flat scheme $T_1(N,n)_{\mathbb{Z}[\frac{1}{N}]}$ over $Y_1(N)_{\mathbb{Z}[\frac{1}{N}]}$, if $N \geq 4$. The map $T_1(N,n)_{\mathbb{Z}[\frac{1}{N}]} \to Y_1(N)_{\mathbb{Z}[\frac{1}{N}]}$ is uniquely extended to a finite flat map of proper normal curves $s : \overline{T}_1(N,n)_{\mathbb{Z}[\frac{1}{N}]} \to X_1(N)_{\mathbb{Z}[\frac{1}{N}]}$.

For an elliptic curve $E \to T$ and a subgroup scheme $C \subset E$ finite flat of degree $n$, the quotient $E' = E/C$ is defined and the induced map $E \to E'$ is finite flat of degree $n$. The structure sheaf $\mathcal{O}_{E'}$ is the kernel of $pr_1^* - \mu^* : \mathcal{O}_E \to \mathcal{O}_{E \times_T C}$ where $\mathrm{pr}_1, \mu : E \times_T C \to E$ denote the projection and the addition respectively. By this construction, we may identify the set $\mathcal{T}_1(N,n)_{\mathbb{Z}[\frac{1}{N}]}(T)$ with

$$\left\{ \begin{array}{c} \text{isom. classes of pairs } (\varphi : E \to E', P) \text{ of finite flat morphism} \\ \varphi : E \to E' \text{ of elliptic curves over } T \text{ of degree } n \text{ and a section} \\ P : T \to E \text{ exactly of order } N \text{ such that } \langle P \rangle \cap \mathrm{Ker}(E \to E') = O \end{array} \right\}.$$

We define a morphism $t : \mathcal{T}_1(N,n)_{\mathbb{Z}[\frac{1}{N}]} \to \mathcal{M}_1(N)_{\mathbb{Z}[\frac{1}{N}]}$ of functors sending $(\varphi : E \to E', P)$ to $(E', \varphi(P))$, It also induces a finite flat map of proper curves $t : \overline{T}_1(N,n)_{\mathbb{Z}[\frac{1}{N}]} \to X_1(N)_{\mathbb{Z}[\frac{1}{N}]}$.

For an integer $n \geq 1$, we define the Hecke operator $T_n : S_k(\Gamma_1(N)) \to S_k(\Gamma_1(N))$ as $s_* \circ \varphi^* \circ t^*$. Here

$$t^* : S_k(\Gamma_1(N)) = \Gamma(X_1(N), \omega^{\otimes k-2} \otimes \Omega^1) \to \Gamma(\overline{T}_1(N,n), t^*\omega^{\otimes k-2} \otimes \Omega^1),$$

$$s_* : \Gamma(\overline{T}_1(N,n), s^*\omega^{\otimes k-2} \otimes \Omega^1) \to \Gamma(X_1(N), \omega^{\otimes k-2} \otimes \Omega^1) = S_k(\Gamma_1(N))$$

are induced by the maps $s, t : \overline{T}_1(N,n)_{\mathbb{Z}[\frac{1}{N}]} \to X_1(N)_{\mathbb{Z}[\frac{1}{N}]}$ defined above respectively. The push-forward map $s_*$ is induced by the trace map. Since $s^*\omega = \omega_E$ and $t^*\omega = \omega_{E'}$, the map $\varphi : E \to E'$ induces

$$\varphi^* : \Gamma(\overline{T}_1(N,n), t^*\omega^{\otimes k-2} \otimes \Omega^1) \to \Gamma(\overline{T}_1(N,n), s^*\omega^{\otimes k-2} \otimes \Omega^1).$$

The group $(\mathbb{Z}/N\mathbb{Z})^\times$ has a natural action on the functor $\mathcal{M}_1(N)$. Hence it acts on $S_k(\Gamma_1(N))$. For $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, the action is denoted by $\langle d\rangle$ and called the diamond operator.

We verify the equality (1) in §1.3 for $T_p$. For $\tau \in H$, the point $P = \frac{1}{N} \in E = \mathbb{C}/\langle 1, \tau\rangle$ is of order $N$. The elliptic curve $E = \mathbb{C}/\langle 1, \tau\rangle$ has $p+1$ subgroups $\langle \frac{\tau+i}{p}\rangle, i = 0, \dots, p-1$ and $\langle \frac{1}{p}\rangle$ of order $p$. If $p \nmid N$, each of them defines a point of $T_1(N,p)$ and they are the inverse image of $\tau \in H$ by $s$. If $p|N$, the subgroup $\langle \frac{1}{p}\rangle$ is a subgroup of $\langle \frac{1}{N}\rangle$ and does not define a point of $T_1(N,p)$. The other $p$ subgroups define points of $T_1(N,p)$ and they are the inverse image of $\tau \in H$ by $s$. For $i = 0, \dots, p-1$, the subgroups $\langle \frac{\tau+i}{p}\rangle$ define $E \to \mathbb{C}/\langle 1, \frac{\tau+i}{p}\rangle$ and the image of $P$ is $\frac{1}{N}$. Thus their images by $t$ are $\frac{\tau+i}{p}$. If $p \nmid N$, the subgroup $\langle \frac{1}{p}\rangle$ define $E \to \mathbb{C}/\langle \frac{1}{p}, \tau\rangle$. The multiplication by $p$ induces an isomorphism $\mathbb{C}/\langle \frac{1}{p}, \tau\rangle \to \mathbb{C}/\langle 1, p\tau\rangle$ and the image of $P$ is $\frac{p}{N}$. Thus its image by $t$ is $\langle p\rangle p\tau$. From this the equality (1) follows immediately.

We define the Hecke algebra by

$$T_k(\Gamma_1(N)) = \mathbb{Q}[T_n, n \in \mathbb{N}, \langle d\rangle, d \in (\mathbb{Z}/N\mathbb{Z})^\times] \subset \mathrm{End} S_k(\Gamma_1(N)).$$

It is a finite commutative $\mathbb{Q}$-algebra.

**Proposition 2.5** *The map*

$$S_k(\Gamma_1(N))_{\mathbb{C}} \to \mathrm{Hom}_{\mathbb{Q}}(T_k(\Gamma_1(N)), \mathbb{C}) \tag{2}$$

*sending a cusp form $f$ to the linear form $T \mapsto a_1(Tf)$ is an isomorphism of $\mathbb{Q}$-vector spaces.*

*Proof.* Suffices to show that the pairing $S_k(\Gamma_1(N))_{\mathbb{C}} \times T_k(\Gamma_1(N))_{\mathbb{C}} \to \mathbb{C}$ defined by $(T, f) \mapsto a_1(Tf)$ is non-degenerate. If $f \in S_k(\Gamma_1(N))_{\mathbb{C}}$ is in the kernel, $a_n(f) = a_1(T_n f) = 0$ for all $n$ and $f = \sum_n a_n(f) q^n = 0$. If $T \in T_k(\Gamma_1(N))$ is in the kernel, $Tf$ is in the kernel for all $f \in S_k(\Gamma_1(N))_{\mathbb{C}}$ since $a_1(T'Tf) = a_1(TT'f) = 0$ for all $T' \in T_k(\Gamma_1(N))$. Hence $Tf = 0$ and $T = 0$. ■

**Corollary 2.6** *The isomorphism* (2) *induces a bijection of finite sets*

$$\{f \in S_k(\Gamma_1(N))_{\mathbb{C}} | \text{normalized eigenform}\} \to \mathrm{Hom}_{\mathbb{Q}\text{-algebra}}(T_k(\Gamma_1(N)), \mathbb{C}) \tag{3}$$

*Proof.* We prove the bijectivity. Let $\varphi$ be the linear form corresponding to $f$. The condition $\varphi(1) = 1$ is equivalent to $a_1(f) = 1$. If $\varphi$ is a ring homomorphism, we have $a_n(Tf) = a_1(T_n Tf) = \varphi(T_n T) = \varphi(T)\varphi(T_n) = \varphi(T) a_1(T_n f) = \varphi(T) a_n(f)$ for every $n \geq 1$ and for $T \in T_k(\Gamma_1(N))$. Thus, we have $Tf = \sum_n a_n(Tf) q^n = \sum_n \varphi(T) a_n(f) q^n = \varphi(T) f$ and $f$ is a normalized eigenform. Conversely, if $f$ is a normalized eigenform and $Tf = \lambda_T f$ for each $T \in T_k(\Gamma_1(N))$, we have $\varphi(T) = a_1(Tf) = a_1(\lambda_T f) = \lambda_T a_1(f) = \lambda_T$. Thus $\varphi$ is a ring homomorphism.

Since $T_k(\Gamma_1(N))$ is finite over $\mathbb{Q}$, the right hand side is a finite set. ■

For a normalized eigenform $f \in S_k(\Gamma_1(N))_{\mathbb{C}}$, the subfield $\mathbb{Q}(f) \subset \mathbb{C}$ is the image of the corresponding $\mathbb{Q}$-algebra homomorphism $\varphi_f : T_k(\Gamma_1(N)) \to \mathbb{C}$ and hence is a finite extension of $\mathbb{Q}$.

# 3 Construction of Galois representations: the case $k = 2$

We will construct Galois representations associated to modular forms in the case $k = 2$, using the Tate module of the Jacobian of a modular curve.

## 3.1 Galois representations and finite étale group schemes

To construct Galois representations, it suffices to define group schemes, in the following sense. For a field $K$, we have an equivalence of categories

$$(\text{finite étale commutative group schemes over } K) \to (\text{finite } G_K\text{-modules})$$

defined by $A \mapsto A(\overline{K})$. The inverse is given by $M \mapsto \mathrm{Spec}(\mathrm{Hom}_{G_K}(M, \overline{K}))$.

In the case $K = \mathbb{Q}$, it induces an equivalence

$$(\text{finite étale commutative group schemes over } \mathbb{Z}[\frac{1}{N}]) \to \begin{pmatrix} \text{finite } G_{\mathbb{Q}}\text{-modules} \\ \text{unramified at } p \nmid N \end{pmatrix}$$

for $N \geq 1$.

**Lemma 3.1** *Let $N \geq 1$ be an integer and $A$ be a finite étale group scheme over* Spec $\mathbb{Z}[\frac{1}{N}]$. *For a prime number $p \nmid N$, the action of $\varphi_p$ on $A(\overline{\mathbb{Q}}) = A(\overline{\mathbb{F}_p})$ is the same as that defined by the geometric Frobenius endomorphism $Fr : A_{\mathbb{F}_p} \to A_{\mathbb{F}_p}$.*

*Proof.* Clear from the commutative diagram

$$\begin{array}{ccc} \mathcal{O}_{A_{\mathbb{F}_p}} & \longrightarrow & \overline{\mathbb{F}}_p \\ {\scriptstyle a\mapsto a^p}\downarrow & & \downarrow{\scriptstyle x\mapsto x^p} \\ \mathcal{O}_{A_{\mathbb{F}_p}} & \longrightarrow & \overline{\mathbb{F}}_p. \end{array}$$

■

To define an $\ell$-adic representation of $G_{\mathbb{Q}}$ unramified at $p \nmid N\ell$, it suffices to construct an inverse system of finite étale $\mathbb{Z}/\ell^n\mathbb{Z}$-module group schemes over $\mathbb{Z}[\frac{1}{N}]$.

## 3.2 Jacobian of a curve and its Tate module

First, we consider the case $g_0(N) = 1$, e.g. $N = 11$. Then, $E = X_0(N)$ is an elliptic curve and the Tate module $V_\ell E = \mathbb{Q}_\ell \otimes \varprojlim_n E[\ell^n](\overline{\mathbb{Q}})$ defines a 2-dimensional $\ell$-adic representation. To construct the Galois representation for general $N$, we will introduce the Jacobian.

Let $f : X \to S$ be a proper smooth curve with geometrically connected fibers of genus $g$. For simplicity, we assume $f : X \to S$ admits a section $s : S \to X$. We define a functor $\mathrm{Pic}^0_{X/S} : (\mathrm{Schemes}/S) \to (\text{Abelian groups})$ by

$$\mathrm{Pic}^0_{X/S}(T) = \frac{\mathrm{Ker}(\deg : \mathrm{Pic}(X \times_S T) \to \mathbb{Z}(T))}{\mathrm{Im}(f^* : \mathrm{Pic}(T) \to \mathrm{Pic}(X \times_S T))}.$$

A section $s : S \to X$ provides a decomposition

$$\mathrm{Pic}(X \times_S T) = \mathbb{Z}(T) \oplus \mathrm{Pic}(T) \oplus \mathrm{Pic}^0_{X/S}(T)$$

depending on the choice of a section.

**Theorem 3.2** ([2] Proposition 9.4/4) *The functor $\mathrm{Pic}^0_{X/S}$ is representable by a proper smooth scheme $J = \mathrm{Jac}_{X/S}$ with geometrically connected fibers of dimension $g$.*

The proper group scheme (=abelian scheme) $\mathrm{Jac}_{X/S}$ is called the Jacobian of $X$. If $g = 1$, Abel's theorem says that the canonical map $E \to \mathrm{Jac}_{E/S}$ is an isomorphism.

Let $f : X \to Y$ be a finite flat morphism of proper smooth curves. The pull-back of invertible sheaves defines the pull-back map $f^* : \mathrm{Jac}_{Y/S} \to \mathrm{Jac}_{X/S}$. We also have a push-forward map defined as follows. The norm map $f_* : f_*\mathbf{G}_{m,X} \to \mathbf{G}_{m,Y}$ defines a push-forward of $\mathbf{G}_m$-torsors and a map $\mathrm{Pic}(X) \to \mathrm{Pic}(Y)$, for a finite flat map $f : X \to Y$ of schemes (see [10] 7.1). They define a map of functors and hence a morphism $f_* : \mathrm{Jac}_{X/S} \to \mathrm{Jac}_{Y/S}$ (see loc. cit. 7.2). The composition $f_* \circ f^*$ is the multiplication by $\deg f$.

If $f : X \to Y$ is a finite flat map of proper smooth curves over a field, then the isomorphism $\mathrm{Coker}(\mathrm{div} : k(X)^\times \to \bigoplus_x \mathbb{Z}) \to \mathrm{Pic}(X)$ has the following compatibility. The pull-back $f^* : \mathrm{Pic}(Y) \to \mathrm{Pic}(X)$ is compatible with the inclusion $f^* : k(Y)^\times \to k(X)^\times$ and the map $\bigoplus_y \mathbb{Z} \to \bigoplus_x \mathbb{Z}$ sending the class $[y]$ to $\sum_{x \mapsto y} e(x/y) \cdot [x]$ where $e(x/y)$ denotes the ramification index. The push-forward $f_* : \mathrm{Pic}(X) \to \mathrm{Pic}(Y)$ is compatible with the norm map $f_* : k(X)^\times \to k(Y)^\times$ and the map $\bigoplus_x \mathbb{Z} \to \bigoplus_y \mathbb{Z}$ sending the class $[x]$ to $[\kappa(x) : \kappa(y)] \cdot [y]$ where $y = f(x)$.

We define the Weil pairing. Let $N \geq 1$ be an integer invertible on $S$. Then, a non-degenerate pairing $J_{X/S}[N] \times J_{X/S}[N] \to \mu_N$ of finite étale groups schemes is defined as follows. First, we recall that, for invertible $\mathcal{O}_X$-modules $\mathcal{L}$ and $\mathcal{M}$, the pairing $\langle \mathcal{L}, \mathcal{M} \rangle$ is defined as an invertible $\mathcal{O}_S$-module. It is characterized by the bilinearity, the compatibility with base change and by the property $\langle \mathcal{L}, \mathcal{M} \rangle = f_{D*}(\mathcal{L}|_D)$ if $\mathcal{M} = \mathcal{O}_X(D)$ for a divisor $D \subset X$ finite flat over $S$. If $\mathcal{L} = f^*\mathcal{L}_0$, we have $\langle \mathcal{L}, \mathcal{M} \rangle = \mathcal{L}_0^{\otimes \deg \mathcal{M}}$.

If $N[\mathcal{L}] = 0 \in \mathrm{Pic}^0_{X/S}(S)$, we have $\mathcal{L}^{\otimes N} = f^*\mathcal{L}_0$ for some $\mathcal{L}_0 \in \mathrm{Pic}(S)$. Hence, for $\mathcal{M} \in \mathrm{Pic}(X)$ of degree 0, we have a trivialization $\langle \mathcal{L}, \mathcal{M} \rangle^{\otimes N} = \langle \mathcal{L}^{\otimes N}, \mathcal{M} \rangle = \langle f^*\mathcal{L}_0, \mathcal{M} \rangle = f^*\mathcal{L}_0^{\otimes \deg \mathcal{M}} = \mathcal{O}_S$. If $N[\mathcal{M}] = 0 \in \mathrm{Pic}^0(X/S)$, we have another trivialization $\langle \mathcal{L}, \mathcal{M} \rangle^{\otimes N} = \mathcal{O}_S$. By comparing them, we obtain an invertible function $\langle \mathcal{L}, \mathcal{M} \rangle_N$ on $S$, whose $N$-th power turns out to be 1. Thus the Weil pairing $\langle \mathcal{L}, \mathcal{M} \rangle_N \in \Gamma(S, \mu_N)$ is defined. In the case $X = E$ is an elliptic curve, this is the same as the Weil pairing defined before.

For a proper smooth curve over $\mathbb{C}$, the Jacobian has an analytic description as a compact complex torus (cf.[12] Sections 6.1, 6.2). Let $X$ be a smooth proper curve over $\mathbb{C}$, or equivalently a compact Riemann surface. The canonical map

$$H_1(X,\mathbb{Z}) \to \mathrm{Hom}(\Gamma(X,\Omega),\mathbb{C})$$

is defined by sending a 1-cycle $\gamma$ to the linear form $\omega \mapsto \int_\gamma \omega$. It is injective and the image is a lattice. A canonical map

$$\mathrm{Pic}^0(X) = J_X(\mathbb{C}) \to \mathrm{Hom}(\Gamma(X,\Omega),\mathbb{C})/\mathrm{Image}\ H_1(X,\mathbb{Z}) \tag{4}$$

is defined by sending $[P]-[Q]$ to the class of the linear form $\omega \mapsto \int_Q^P \omega$. This is an isomorphism of compact complex tori. Thus, in this case, the $N$-torsion part $\mathrm{Jac}_{X/\mathbb{C}}[N]$ of the Jacobian is canonically identified with $H_1(X,\mathbb{Z}) \otimes \mathbb{Z}/N\mathbb{Z}$.

For a finite flat map $f : X \to Y$ of curves, the isomorphism (4) has the following functoriality. The pull-back $f^* : \mathrm{Pic}^0(Y) \to \mathrm{Pic}^0(X)$ is compatible with the dual of the push-forward map $f_* : \Gamma(X,\Omega) \to \Gamma(Y,\Omega)$ and the pull-back map $H_1(Y,\mathbb{Z}) \to H_1(X,\mathbb{Z})$. The push-forward $f_* : \mathrm{Pic}^0(X) \to \mathrm{Pic}^0(Y)$ is compatible with the dual of the pull-back map $f^* : \Gamma(Y,\Omega) \to \Gamma(X,\Omega)$ and the push-forward map $H_1(X,\mathbb{Z}) \to H_1(Y,\mathbb{Z})$.

The isomorphism $\mathrm{Jac}_{X/\mathbb{C}}[N] \to H_1(X,\mathbb{Z}) \otimes \mathbb{Z}/N\mathbb{Z}$ is compatible with the pull-back and the push-forward for a finite flat morphism. By the isomorphism $\mathrm{Jac}_{X/\mathbb{C}}[N] \to H_1(X,\mathbb{Z}) \otimes \mathbb{Z}/N\mathbb{Z}$, the Weil pairing $\mathrm{Jac}_{X/\mathbb{C}}[N] \times \mathrm{Jac}_{X/\mathbb{C}}[N] \to \mu_N$ is identified with the pairing induced by the cap-product $H_1(X,\mathbb{Z}) \times H_1(X,\mathbb{Z}) \to \mathbb{Z}$.

Now, we introduce the Tate module of the Jacobian a curve. Let $X$ be a proper smooth curve over a field $k$ with geometrically connected fiber of genus $g$. For a prime number $\ell$ invertible in $k$, we define the $\ell$-adic Tate module by

$$T_\ell\ \mathrm{Jac}_{X/k} = \varprojlim{}_n \mathrm{Jac}_{X/k}[\ell^n](\bar{k}) = \varprojlim{}_n \mathrm{Pic}(X_{\bar{k}})[\ell^n]$$

and $V_\ell\ \mathrm{Jac}_{X/k} = \mathbb{Q}_\ell \otimes T_\ell\ \mathrm{Jac}_{X/k}$.

**Corollary 3.3** *Let $N \geq 1$ be an integer and $X$ be a proper smooth curve over $\mathbb{Z}[\frac{1}{N}]$ with geometrically connected fibers of genus $g$. Then, $V_\ell\ \mathrm{Jac}_{X_\mathbb{Q}/\mathbb{Q}}$ is an $\ell$-adic representation of $G_\mathbb{Q}$ of degree $2g$ unramified at $p \nmid N\ell$.*

*Proof.* The multiplication $[\ell^n] : \mathrm{Jac}_{X/\mathbb{Z}[\frac{1}{N\ell}]} \to \mathrm{Jac}_{X/\mathbb{Z}[\frac{1}{N\ell}]}$ is finite étale. Hence $\mathrm{Jac}_{X/\mathbb{Q}}[\ell^n](\overline{\mathbb{Q}}) = \mathrm{Jac}_{X/\mathbb{Q}}[\ell^n](\mathbb{C}) = H_1(X,\mathbb{Z}) \otimes \mathbb{Z}/\ell^n\mathbb{Z}$ is isomorphic to $(\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$ as a $\mathbb{Z}/\ell^n\mathbb{Z}$-module and $V_\ell\ \mathrm{Jac}_{X_\mathbb{Q}/\mathbb{Q}}$ is isomorphic to $H_1(X,\mathbb{Z}) \otimes \mathbb{Q}_\ell \simeq \mathbb{Q}_\ell^{2g}$ as a $\mathbb{Q}_\ell$-vector space. Since $\mathrm{Jac}_{X/\mathbb{Z}[\frac{1}{N\ell}]}[\ell^n]$ is a finite étale scheme over $\mathbb{Z}[\frac{1}{N\ell}]$, the $\ell$-adic representation $V_\ell\ \mathrm{Jac}_{X_\mathbb{Q}/\mathbb{Q}}$ is unramified at $p \nmid N\ell$. ■

In the rest of the subsection, we will see that the zeta function of a curve is expressed by the Tate module of the Jacobian. Let $f : X \to X$ be an endomorphism of a proper smooth curve over a field $k$. Let $\Gamma_f, \Delta \subset X \times X$ be the graphs of $f$ and of the identity and let $(\Gamma_f, \Delta_X)_{X\times_k X} \in \mathbb{Z}$ be the intersection number. Then, for a prime number $\ell$ invertible in $k$, the Lefschetz trace formula (cf. §4.1) gives us

$$(\Gamma_f, \Delta_X)_{X\times_k X} = 1 - \mathrm{Tr}(f_* : T_\ell J_X) + \deg f.$$

Assume $k = \mathbb{F}_p$ and apply the Lefschetz trace formula to the iterates $F^n$ of the Frobenius endmorphism $F : X \to X$. Then we obtain

$$\mathrm{Card}\ X(\mathbb{F}_{p^n}) = 1 - \mathrm{Tr}(F_*^n : T_\ell J_X) + p^n.$$

Thus the zeta function defined by

$$Z(X, t) = \exp \sum_{n=1}^{\infty} \frac{\mathrm{Card} X(\mathbb{F}_{p^n})}{n} t^n$$

satisfies

$$Z(X, t) = \frac{\det(1 - F_* t : T_\ell J_X)}{(1-t)(1-pt)}.$$

Thus, for a proper smooth curve $X$ over $\mathbb{Z}[\frac{1}{N}]$ and a prime $p \nmid N\ell$, we have

$$\det(1 - \varphi_p t : T_\ell J_X) = Z(X \otimes_{\mathbb{Z}[\frac{1}{N}]} \mathbb{F}_p, t)(1-t)(1-pt).$$

**Theorem 3.4 (Weil)** *Let $\alpha$ be an eigenvalue of $\varphi_p$ on $T_\ell J_X$. Then, $\alpha$ is an algebraic integer and its conjugates have complex absolute values $\sqrt{p}$.*

## 3.3 Construction of Galois representations

Now we construct a Galois representation associated to a modular form. For more detail, we refer to [12] Chapter 9.

We recall the Eichler-Shimura isomorphism.

**Proposition 3.5** *The canonical isomorphism*

$$H_1(X_1(N), \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{R} \to \mathrm{Hom}(S_2(\Gamma_1(N)), \mathbb{C}) = \mathrm{Hom}(\Gamma(X_1(N), \Omega), \mathbb{C})$$

*is an isomorphism of $T_2(\Gamma_1(N))_{\mathbb{R}}$-modules.*

*Proof.* The $T_2(\Gamma_1(N))$-module structure is defined by $T^*$ on $S_2(\Gamma_1(N))$ and is defined by $T_*$ on $H_1(X_1(N), \mathbb{Q})$ for $T \in T_2(\Gamma_1(N))$. Thus, it follows from the equality $\int_{f_*\gamma} \omega = \int_\gamma f^*\omega$. ■

Define the integral Hecke algebra $T_2(\Gamma_1(N))_{\mathbb{Z}}$ to be the $\mathbb{Z}$-subalgebra $\mathbb{Z}[T_n, n \geq 1;\ \langle d\rangle, d \in (\mathbb{Z}/N\mathbb{Z})^\times] \subset \mathrm{End}\ H_1(X_1(N), \mathbb{Z})$. The $\mathbb{Z}$-algebra $T_2(\Gamma_1(N))_{\mathbb{Z}}$ is commutative and finite flat over $\mathbb{Z}$. It follows from Proposition 3.5 that the Fourier coefficients $a_n(f)$ lie in the image of the ring homomorphism $\varphi_f : T_2(\Gamma_1(N))_{\mathbb{Z}} \to \mathbb{C}$ for a normalized eigenform $f$. Hence they are algebraic integers in the number field $\mathbb{Q}(f)$.

For an integer $N \geq 1$, let $J_1(N)$ denote the Jacobian $\mathrm{Jac}_{X_1(N)/\mathbb{Q}}$ of the modular curve $X_1(N)$ over $\mathbb{Q}$.

**Corollary 3.6** (cf. [12] Lemma 9.5.3) *The $T_2(\Gamma_1(N))_{\mathbb{Q}_\ell}$-module $V_\ell(J_1(N))$ is free of rank 2.*

*Proof.* By Propositions 2.5 and 3.5 and by fpqc descent, $H_1(X_1(N),\mathbb{Q})$ is a free $T_2(\Gamma_1(N))_{\mathbb{Q}}$-module of rank 2. Hence $V_\ell(J_1(N)) = H_1(X_1(N),\mathbb{Q}) \otimes \mathbb{Q}_\ell$ is also free of rank 2. ■

For a place $\lambda|\ell$ of $\mathbb{Q}(f)$, we put

$$V_{f,\lambda} = V_\ell(J_1(N)) \otimes_{T_2(\Gamma_1(N))_{\mathbb{Q}_\ell}} \mathbb{Q}(f)_\lambda.$$

The $\mathbb{Q}(f)_\lambda$-vector space $V_{f,\lambda}$ is a 2-dimensional $\ell$-adic representation unramified at $p \nmid N\ell$.

**Theorem 3.7** (cf. [12] Theorem 9.5.4) *The $\ell$-adic representation $V_{f,\lambda}$ is associated to $f$. Namely, for $p \nmid N\ell$, we have*

$$\det(1-\varphi_p t : V_{f,\lambda}) = 1 - a_p(f)t + \varepsilon_f(p)pt^2.$$

Proof will be given in the next subsection.

**Corollary 3.8** *If we put $1-a_p(f)t+\varepsilon_f(p)pt^2 = (1-\alpha t)(1-\beta t)$, the complex absolute values of $\alpha$ and $\beta$ are $\sqrt{p}$.*

*Proof.* By Lemma 3.1, the left hand side $\det(1-\varphi_p t : V_{f,\lambda})$ is equal to $\det(1-Fr_p t : V_\ell(J_1(N)_{\mathbb{F}_p}) \otimes \mathbb{Q}(f)_\lambda)$. Thus it follows from Theorem 3.4. ■

**Lemma 3.9** *The map $H_1(X_1(N),\mathbb{Q}) \to \mathrm{Hom}(H_1(X_1(N),\mathbb{Q}),\mathbb{Q})$ sending $\alpha$ to the linear form $\beta \mapsto \mathrm{Tr}(\alpha \cap w_N\beta)$ is an isomorphism of $T_2(\Gamma_1(N))$-modules.*

*Proof.* It suffices to show $T_* \circ w = w \circ T^*$. We define $\tilde{w} : T_1(N,n) \to T_1(N,n)$ by sending $(E,P,C) \to (E',Q',C')$ where $E' = E/(\langle P\rangle + C)$, $Q' \in (E/C[N])/\langle\overline{P}\rangle \subset E'[N]$ is the inverse image of $\zeta_N$ by the isomorphism $(\overline{P},\ ) : (E/C[N])/\langle\overline{P}\rangle \to \mu_N$ where $\overline{P} \in E/C[N]$ is the image of $P$ and $C'$ is the kernel of the dual of $E/\langle P\rangle \to E'$. Then, we have $s \circ \tilde{w} = w \circ t$, $t \circ \tilde{w} = w \circ s$ and hence $T_* \circ w = w \circ T^*$. ■

## 3.4 Congruence relation

Let $S$ be a scheme over $\mathbb{F}_p$ and $E$ be an elliptic curve over $S$. The commutative diagram

$$\begin{array}{ccc} E & \xrightarrow{Fr_E} & E \\ \downarrow & & \downarrow \\ S & \xrightarrow{Fr_S} & S \end{array}$$

defines a map $F : E \to E^{(p)} = E \times_{S \swarrow Fr_S} S$ called the Frobenius. The dual $V = F^* : E^{(p)} \to E$ is called the Verschiebung. We have $V \circ F = [p]_E, F \circ V = [p]_{E^{(p)}}$.

**Lemma 3.10**

$$\det(1 - Fr_p t : V_\ell(J_1(N)_{\mathbb{F}_p})) = \det(1 - \langle p\rangle Fr_p^* t : V_\ell(J_1(N)_{\mathbb{F}_p})).$$

*Proof.* First, we show $Fr \circ w = \langle p\rangle \circ w \circ Fr$. We have

$$Fr \circ w(E,P) = Fr(E/\langle P\rangle, Q) = (E^{(p)}/\langle P^{(p)}\rangle, Q^{(p)}),$$

$$\langle p\rangle \circ w \circ Fr(E,P) = \langle p\rangle \circ w(E^{(p)}, P^{(p)}) = (E^{(p)}/\langle P^{(p)}\rangle, pQ')$$

where $Q' \in E'[N]$ is characterized by $(P^{(p)}, Q')_N = (P,Q)_N$. Since $(P^{(p)}, Q^{(p)})_N = (P,Q)_N^p = (P^{(p)}, pQ')_N$, we have $Fr \circ w = \langle p\rangle \circ w \circ Fr$. Hence, we have $w \circ Fr = Fr \circ \langle p\rangle^{-1} \circ w$.

By Lemma 3.9, it suffices to show that $\langle p\rangle Fr_p^*$ is the dual of $Fr_p$ with respect to the pairing $\langle \alpha, w\beta\rangle$ on $V_\ell J_1(N)_{\mathbb{F}_p}$. For $\alpha, \beta \in J_1(N)_{\mathbb{F}_p}[\ell^n]$, we have

$$\begin{aligned}\langle F_*\alpha, w\beta\rangle &= \langle w\circ F_*\alpha, \beta\rangle = \langle (w\circ F)_*\alpha, \beta\rangle \\ &= \langle (Fr\circ\langle p\rangle^{-1}\circ w)_*\alpha, \beta\rangle = \langle \alpha, w\langle p\rangle_* F^*\beta\rangle\end{aligned}$$

and the assertion follows.

Let $N \geq 1$ be an integer and $p \nmid N$ be a prime number. We define two maps

$$a, b : \mathcal{M}_1(N)_{\mathbb{F}_p} \to \mathcal{T}_1(N,p)_{\mathbb{F}_p}$$

by sending $(E,P)$ to $(E, P, F : E \to E^{(p)})$ and to $(E^{(p)}, P^{(p)}, V : E^{(p)} \to E)$ respectively. The compositions are given by

$$\begin{pmatrix} s\circ a & s\circ b \\ t\circ a & t\circ b\end{pmatrix} = \begin{pmatrix} \mathrm{id} & F \\ F & \langle p\rangle\end{pmatrix}. \tag{5}$$

The maps $a, b : \mathcal{M}_1(N)_{\mathbb{F}_p} \to \mathcal{T}_1(N,p)_{\mathbb{F}_p}$ induce closed immersions $a, b : X_1(N)_{\mathbb{F}_p} \to \overline{\mathcal{T}}_1(N,p)_{\mathbb{F}_p}$.

**Proposition 3.11** *Let $N \geq 1$ be an integer and $p \nmid N$ be a prime number. Then $s, t : \overline{\mathcal{T}}_1(N,p) \to X_1(N)$ is finite flat of degree $p+1$.*

*The map*

$$a \amalg b : X_1(N)_{\mathbb{F}_p} \amalg X_1(N)_{\mathbb{F}_p} \to \overline{\mathcal{T}}_1(N,p)_{\mathbb{F}_p}$$

*is an isomorphism on a dense open subscheme.*

*Proof.* Since the maps $a, b : X_1(N)_{\mathbb{F}_p} \to \overline{\mathcal{T}}_1(N,p)_{\mathbb{F}_p}$ are sections of projections $\overline{\mathcal{T}}_1(N,p)_{\mathbb{F}_p} \to X_1(N)_{\mathbb{F}_p}$, they are closed immersions. Since both $(1, F) : X_1(N)_{\mathbb{F}_p} \amalg X_1(N)_{\mathbb{F}_p} \to X_1(N)_{\mathbb{F}_p}$ and $\overline{\mathcal{T}}_1(N,p)_{\mathbb{F}_p} \to X_1(N)_{\mathbb{F}_p}$ are finite flat of degree $p+1$, the assertion follows. ■

**Corollary 3.12** (cf. [12] Theorem 8.7.2) *The canonical isomorphism* $\mathrm{Pic}^0(X_1(N))(\overline{\mathbb{Q}})[\ell^n] \to \mathrm{Pic}^0(X_1(N))(\overline{\mathbb{F}_p})[\ell^n]$ *makes the diagram*

$$\begin{tikzcd}
\mathrm{Pic}^0(X_1(N))(\overline{\mathbb{Q}})[\ell^n] \arrow[r, "T_p"] \arrow[d] & \mathrm{Pic}^0(X_1(N))(\overline{\mathbb{Q}})[\ell^n] \arrow[d] \\
\mathrm{Pic}^0(X_1(N))(\overline{\mathbb{F}_p})[\ell^n] \arrow[r, "F_*+\langle p\rangle F^*"] & \mathrm{Pic}^0(X_1(N))(\overline{\mathbb{F}_p})[\ell^n]
\end{tikzcd}$$

*commutative.*

*Proof.* By Proposition, we have a commutative diagram

$$\begin{tikzcd}
\mathrm{Pic}(X_1(N)_{\mathbb{Z}_p^{\mathrm{unr}}}) \arrow[r, "T_p=s_*t^*"] \arrow[d] & \mathrm{Pic}(X_1(N)_{\mathbb{Z}_p^{\mathrm{unr}}}) \arrow[d] \\
\mathrm{Pic}(X_1(N)_{\overline{\mathbb{F}_p}}) \arrow[r, "(t\circ a)_*(s\circ a)^*+(t\circ b)_*(s\circ b)^*"] & \mathrm{Pic}(X_1(N)_{\overline{\mathbb{F}_p}})
\end{tikzcd}$$

By (5), the bottom arrow is $F_* + \langle p\rangle F^*$. ■

*Proof of Theorem 3.7.* By Corollary 3.12, we have

$$(1 - F_*t)(1 - \langle p\rangle F^*t) = (1 - T_pt + \langle p\rangle pt^2).$$

Taking the determinant, we get

$$\det(1 - F_*t)\det(1 - \langle p\rangle F^*t) = (1 - T_pt + \langle p\rangle pt^2)^2.$$

By Lemma 3.10, we get

$$\det(1 - F_*t) = 1 - T_pt + \langle p\rangle pt^2.$$

■

# 4 Construction of Galois representations: the case $k > 2$

To cover the case $k > 2$, we introduce a construction generalizing the torsion part of the Jacobian.

## 4.1 Etale cohomology

In this subsection, we will recall very briefly some basics on etale cohomology. For more detail, we refer to [8] [Arcata].

For a scheme $X$, an étale sheaf on the small étale site is a contravariant functor $\mathcal{F} : (\text{Etale schemes}/X) \to (\text{Sets})$ such that the map

$$\mathcal{F}(U) \to \left\{ (s_i) \in \prod_{i\in I} \mathcal{F}(U_i) \middle| \operatorname{pr}_1^*(s_i) = \operatorname{pr}_2^*(s_j) \text{ in } \mathcal{F}(U_i \times_U U_j) \text{ for } i, j \in I \right\}$$

is a bijection for every family of étale morphisms $(\varphi_i : U_i \to U)_{i\in I}$ satisfying $U = \bigcup_{i\in I} \varphi_i(U_i)$. An étale sheaf on $X$ represented by a finite étale scheme over $X$ is called locally constant.

The abelian étale sheaves form an abelian category with enough injective objects. The étale cohomology $H^q(X,\ )$ is defined as the derived functor of the global section functor $\Gamma(X,\ )$. For a morphism $f : X \to Y$ of schemes, the higher direct image $R^q f_*$ is defined as the derived functor of $f_*$. We write $H^q(X, \mathbb{Q}_\ell) = \mathbb{Q}_\ell \otimes \varprojlim_n H^q(X, \mathbb{Z}/\ell^n\mathbb{Z})$ and $R^q f_* \mathbb{Q}_\ell = \mathbb{Q}_\ell \otimes \varprojlim_n R^q f_* \mathbb{Z}/\ell^n\mathbb{Z}$.

Let $f : X \to S$ be a proper smooth morphism of relative dimention $d$ and let $\mathcal{F}$ be a locally constant sheaf on $X$. Then the higher direct image $R^q f_* \mathcal{F}$ is also locally constant for all $q$ and is 0 unless $0 \le q \le 2d$ and its formation commutes with base change. More generally, assume $f : X \to S$ is proper smooth, $U \subset X$ is the complement of a relative divisor $D$ with normal crossings and $\mathcal{F}$ is a locally constant sheaf on $U$ tamely ramified along $D$. Let $j : U \to X$ be the open immersion. Then, the higher direct image $R^q f_* j_* \mathcal{F}$ is also locally constant and its formation commutes with base change ([8] Appendice 1.3.3 by L. Illusie to [Th. finitude]).

If $f : X \to S$ is a proper smooth curve and if $N$ is invertible on $S$, we have a canonical isomorphism $R^1 f_* \mu_N \to \operatorname{Jac}_{X/S}[N]$.

If $S = \operatorname{Spec} k$ for a field $k$, the category of étale sheaves on $S$ is equivalent to that of discrete sets with continuous $G_k$-actions by the functor sending $\mathcal{F}$ to $\varinjlim_{L\subset \bar{k}} \mathcal{F}(L)$. For a scheme $X$ over $k$, the higher direct image $R^q f_* \mathcal{F}$ is the étale cohomology group $H^q(X_{\bar{k}}, \mathcal{F})$ with the canonical $G_k$-action. If $k = \mathbb{C}$, we have a canonical isomorphism $H^q(X, \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}/N\mathbb{Z} \to H^q(X, \mathbb{Z}/N\mathbb{Z})$ comparing the singular cohomology with the etale cohomology.

Let $X$ be a proper smooth variety over a field $k$ and $f : X \to X$ be an endomorphism. Then, for a prime number $\ell$ invertible in $k$, the Lefschetz trace formula ([8] [Cycle] Proposition 3.3) gives us

$$(\Gamma_f, \Delta_X)_{X\times_k X} = \sum_{q=0}^{2\dim X} (-1)^q \operatorname{Tr}(f^* : H^q(X_{\bar{k}}, \mathbb{Q}_\ell)).$$

Assume $k = \mathbb{F}_p$ and apply the Lefschetz trace formula (loc. cit. Corollaire 3.8) to the iterates of the Frobenius endmorphism $F : X \to X$. Then the zeta function is expressed by the determinant:

$$Z(X, t) = \prod_{q=0}^{2\dim X} \det(1 - F^* t : H^q(X_{\bar{k}}, \mathbb{Q}_\ell))^{(-1)^{q+1}}.$$

**Theorem 4.1 (the Weil conjecture [9])** *Let $\alpha$ be an eigenvalue of $F^*$ on $H^q(X_{\bar{k}}, \mathbb{Q}_\ell)$. Then, $\alpha$ is an algebraic integer and its conjugates have complex absolute values $p^{\frac{q}{2}}$.*

## 4.2 Construction of Galois representations

We briefly sketch the construction in the higher weight case. For more detail, we refer to [7].

Let $N \geq 5$ and $k \geq 2$. Proposition 3.5 is generalized as follows. Let $f : E_{Y_1(N)} \to Y_1(N)$ be the universal elliptic curve and $j : Y_1(N) \to X_1(N)$ be the open immersion.

**Proposition 4.2** *There exists a canonical isomorphism*

$$H^1(X_1(N)_{\mathbb{C}}, j_* S^{k-2} R^1 f_* \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{R} \to S_k(\Gamma_1(N))_{\mathbb{C}}$$

*of $T_k(\Gamma_1(N))_{\mathbb{R}}$-modules.*

**Corollary 4.3** *$H^1(X_1(N)_{\overline{\mathbb{Q}}}, j_* S^{k-2} R^1 f_* \mathbb{Q}_\ell)$ is a free $T_k(\Gamma_1(N))_{\mathbb{Q}_\ell}$-module of rank 2.*

For a place $\lambda | \ell$ of $\mathbb{Q}(f)$, we put

$$V_{f,\lambda} = H^1(X_1(N)_{\overline{\mathbb{Q}}}, j_* S^{k-2} R^1 f_* \mathbb{Q}_\ell) \otimes_{T_k(\Gamma_1(N))_{\mathbb{Q}_\ell}} \mathbb{Q}(f)_\lambda.$$

The $\mathbb{Q}(f)_\lambda$-vector space $V_{f,\lambda}$ is a 2-dimensional $\ell$-adic representation unramified at $p \nmid N\ell$.

**Theorem 4.4** *The dual of the $\ell$-adic representation $V_{f,\lambda}$ is associated to $f$. Namely, for $p \nmid N\ell$, we have*

$$\det(1 - \varphi_p^{-1} t : V_{f,\lambda}) = 1 - a_p(f)t + \varepsilon_f(p) p^{k-1} t^2.$$

**Corollary 4.5** *If we put $1 - a_p(f)t + \varepsilon_f(p)p^{k-1}t^2 = (1 - \alpha t)(1 - \beta t)$, the complex absolute values of $\alpha$ and $\beta$ are $p^{\frac{k-1}{2}}$.*

# References


[1] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over* **Q***: wild 3-adic exercises*, Journal of AMS **14** p. 843-939 (2001).

[2] S. Bosch, W. Lütkebohmert, M. Raynaud, Neron Models, Ergebnisse Der Mathematik Und Ihrer Grenzgebiete. 3. Folge, Springer, 1990. ISBN: 3540505873 .

[3] G. Cornell, J. Silverman (eds.), Arithmetic Geometry, Springer, 1986. ISBN: 0387963111

[4] G. Cornell, J. Silverman, G. Stevens (eds.), Modular Forms and Fermat's Last Theorem, Springer, 1997. ISBN: 0387946098

[5] H. Darmon, F. Diamond, R. Taylor, *Fermat's Last Theorem*, in J. Coates and S. T. Yau (eds.), Elliptic Curves, Modular Forms and Fermat's Last Theorem, 2nd ed. International Press, 1997, 2-140.

[6] P. Deligne, M. Rapoport, *Les schémas de modules de courbes elliptiques,* in W. Kuyk, P. Deligne (eds.), Modular Functions of One Variable II, Lecture Notes in Math., Springer, **349**, 1973, 143-316.

[7] P. Deligne, *Formes modulaires et représentations $\ell$-adiques,* Séminaire Bourbaki no 355, in Lecture Notes in Math., Springer, **179**, 1971, 139-172.

[8] —–, Cohomologie étale, Lecture Notes in Math., Springer, **569**, 1977.

[9] —–, *La conjecture de Weil II*, Publications Mathematiques de l'IHES, 52 (1980), p. 137-252.

[10] —–, *Le déterminant de la cohomologie*, Current trends in arithmetical algebraic geometry, 93–177, Contemp. Math., 67, Amer. Math. Soc., Providence, RI, 1987.

[11] F. Diamond, J. Im, *Modular forms and modular curves*, in Seminar on Fermat's last theorem, CMS conference proceedings **17** pp. 39-133, (1995).

[12] F. Diamond, J. Shurman, A First course in Modular forms, Springer GTM 228 (2005). ISBN:038723229X

[13] J.-M. Fontaine, B. Mazur, *Geometric Galois representations,* in J. Coates and S. T. Yau (eds.), Elliptic Curves, Modular Forms and Fermat's Last Theorem, 2nd ed. International Press, 1997, 41-78.

[14] H. Hida, Modular forms and Galois cohomology, Cambridge studies in advanced math., 69, Cambridge Univ. Press, 2000. ISBN:052177036X

[15] H. Hida, Geometric modular forms and elliptic curves, World Scientific (2000). ISBN:9810243375

[16] N. Katz, B. Mazur, Arithmetic Moduli of Elliptic Curves, Annals of Math. Studies, Princeton Univ. Press, **151**, 1994. ISBN:0691083495

[17] K. Ribet, *The $\ell$-adic representations attached to an eigenform with Nebentypus: a survey*, in Modular Functions of One Variable V, Lecture Notes in Math., Springer, **601**, 1977, 17-61.

[18] T. Saito, Fermat's last theorem (in Japanese), Iwanami Shoten, 1 (2000) ISBN4-00-010659-7, 2 (2008) ISBN4-00-010662-7, .

[19] J-P. Serre, A course in arithmetic, Springer GTM **7** (1973). ISBN:0387900403

[20] —–, Abelian $\ell$-adic representations and Elliptic curves, Benjamin, 1968. ISBN:1568810776

[21] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Functions, Princeton Univ. Press, 1971. ISBN:0691080925

[22] J. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Math., Springer, **106**, 1986. ISBN:0387962034

[23] —–, Advanced Topics in the Arithmetic of Elliptic Curves, Graduate Texts in Math., Springer, **151**, 1994. ISBN:3540943285

[24] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Math., **141**(1995), 443-551.