Galois representations and modular forms

Takeshi Saito

July 17-22, 2006 at IHES

Introduction

A goal in number theory is to understand

— the finite extensions of $\mathbb{Q}$, or equivalently,

— the absolute Galois group $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, or further equivalently,

— representations of $G_{\mathbb{Q}}$.

Representations are classified by the degree. Representations of degree 1 are called 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 $N \geq 1$. Thus, there are too few continuous characters $G_{\mathbb{Q}} \to \mathbb{C}^\times$. It is more natural to consider ℓ-adic characters for a prime ℓ. ℓ-adic cyclotomic character.

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

$$\begin{aligned} & \{\ell\text{-adic character of } G_{\mathbb{Q}} \text{ potentially cristalline at } \ell\} \\ = \ & \{\text{“geometric” } \ell\text{-adic character of } G_{\mathbb{Q}}\} \\ = \ & \langle \text{Dirichlet characters, } \ell\text{-adic cyclotomic characters} \rangle. \end{aligned}$$

In the case where degree is 2, we expect to have (cf. [7])

$$\begin{aligned} & \{\text{odd } \ell\text{-adic representation of } G_{\mathbb{Q}} \text{ of degree 2 potentially semi-stable at } \ell\} \\ = \ & \{\text{odd “geometric” } \ell\text{-adic representation of } G_{\mathbb{Q}} \text{ of degree 2}\} \\ = \ & \{\ \ell\text{-adic representation associated to modular form}\}. \end{aligned}$$

In this course, we discuss on one direction $\supset$ established by Shimura and Deligne ([14], [5]). The other direction $\subset$ partly established by Wiles and others, which will not be discussed here, has significant consequences including Fermat's last theorem, the modularity of elliptic curves, etc. ([2],[3]).

Contents

1 Galois representations and modular forms

1.1 Modular forms

([14]) 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 space $S_k(N, \varepsilon) \subset M_k(N, \varepsilon)$ of cusp forms and of modular forms of level N, weight k and of character ε. We will see later that they are of finite dimension. For $\varepsilon = 1$, we write $S_k(N) \subset M_k(N)$ for $S_k(N, 1) \subset M_k(N, 1)$.

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 the following, we mainly consider

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

for $N \geq 1$. 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

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

The action of $SL_2(\mathbb{Z})$ on the Poincaré upper half plane $H = \{\tau \in \mathbb{C} | \mathrm{Im}\,\tau > 0\}$. For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ and $\tau \in H$, we put $\gamma(\tau) = \dfrac{a\tau + b}{c\tau + d}$. For a holomorphic function f on H, we define $\gamma_k^* f$ 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 Γ, 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 $q_N = \exp(2\pi i \frac{\tau}{N})$. Here, we impose $a_{\frac{n}{N}}(\gamma_k^* f) = 0$ 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 $S_k(N) = S_k(\Gamma_0(N))$. The group $\Gamma_0(N)$ has a natural action on $S_k(\Gamma_1(N))$ and the subgroup $\Gamma_1(N)$ acts trivially on it. Hence, the space $S_k(\Gamma_1(N))$ has an action of the quotient $\Gamma_0(N)/\Gamma_1(N) = (\mathbb{Z}/N\mathbb{Z})^\times$. 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 is decomposed by the characters

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

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

([12]) Eisenstein series. $k \geq 4$ even.

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

is a modular form of weight k.

q-expansion. By differentiating the logarithms of $\sin \pi\tau = \pi\tau \prod_{n=1}^{\infty} \left(1 - \frac{\tau^2}{n^2}\right)$, one obtains

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

Applying $q\frac{d}{dq} = \frac{1}{2\pi i}\frac{d}{d\tau}$ $k-1$-times, 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 obtain

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

Recall that

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

$\bigoplus_{k=0}^{\infty} M_k(1)_{\mathbb{C}} = \mathbb{C}[E_4, E_6]$.

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

is a cusp form of weight 12, level 1. $\bigoplus_{k=0}^{\infty} S_k(1)_{\mathbb{C}} = \mathbb{C}[E_4, E_6] \cdot \Delta$.

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

is a basis of $S_2(11)_{\mathbb{C}}$.

1.3 Hecke operators

([14]) The Hecke operator T_n is defined as an endomorphism of $S_k(\Gamma_1(N))$. Here we only consider the case $n = p$ is a prime. The general case is discussed later.

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

If $f(\tau) = \sum_n a_n(f)q^n$, 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

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

$f \in S_k(N, \varepsilon)$ is called a normalized eigenform if $T_n f = \lambda_n f$ for all $n \geq 1$ and $a_1 = 1$. 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 $f = \sum_n a_n q^n$, 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.

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

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

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

It converges absolutely on Re $s > \dfrac{k+1}{2}$. If $f = \sum_n a_n q^n \in S_k(N, \varepsilon)$ is a normalized eigen form, we have 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

([13]) p prime. 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.

$\mathbb{Q}_p \subset \mathbb{Q}_p^{\mathrm{ur}} \subset \overline{\mathbb{Q}_p}$ 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

$G_{\mathbb{F}_p} = \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$. The map $\widehat{\mathbb{Z}} = \varinjlim_n \mathbb{Z}/n\mathbb{Z} \to G_{\mathbb{F}_p}$ defined by sending 1 to the Frobenius substitution $\varphi_p; \varphi(a) = a^p$ for all $a \in \overline{\mathbb{F}_p}$ is an isomorphism.

V ℓ-adic representation of $G_{\mathbb{Q}}$. E_λ a finite extension of $\mathbb{Q}_\ell$. ℓ is a prime. V E_λ vector space of finite dimension. $G_{\mathbb{Q}} \to GL_{E_\lambda} V$ continuous representation.

There exists an integer $N \geq 1$ such that V is unramified at $p \nmid N\ell$.

Unramified: restriction to I_p is trivial.

For $p \nmid N\ell$, $\det(1 - \varphi_p t : V) \in E_\lambda[t]$ is well-defined.

Definition 1.2 *A 2-dimensional ℓ-adic representation V is said to be associated to a normalized eigen cusp form $f = \sum_n a_n q^n \in S_k(N, \varepsilon)$ if, for every $p \nmid N\ell$, V is unramified at p and*

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

for an embedding $\mathbb{Q}(f) \to E_\lambda$.

We may replace the condition by

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

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

Theorem 1.3 *Let $N \geq 1, k \geq 2$ 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 ℓ-adic representation $V_{f,\lambda}$ associated to f.*

A consequence of the geometric construction and the Weil conjecture.

Corollary 1.4 (Ramanujan's conjecture)

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

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 φ_p.*

A generalization of Dirichlet's Theorem on Primes in Arithmetic Progressions.

Consequence: V_1, V_2 ℓ-adic representations. 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^{ss} and V_2^{ss} are isomorphic to each other. In particular, the ℓ-adic representation associated to f is unique upto isomorphism, since it is irreducible by a theorem of Ribet.

2 Modular curves and modular forms

2.1 Elliptic curves

([15]) k field 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 $\mathbf{P}^2_k$ defined by the homogeneous equation $Y^2Z = X^3 + aXZ^2 + bZ^3$. 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 $y^2 = 4x^3 - g_2x - g_3$, the j-invariant is defined by

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

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

Addition. For a scheme X, the Picard group $\mathrm{Pic}(X)$ is the isomorphism class group of invertible $\mathcal{O}_X$-modules. If X is a smooth proper curve over a field k, the Picard group $\mathrm{Pic}(X)$ is equal to the divisor class group

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

where for a non-zero rational function $f \in k(X)^\times$ its divisor $\mathrm{div} f$ is $(\mathrm{ord}_x f)_x$. The degree map $\deg : \mathrm{Pic}(X) \to \mathbb{Z}$ is induced by the degree 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 $0^* : \mathrm{Pic}(E \times_S T) \to \mathrm{Pic}(T)$ 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 $[\mathcal{O}_{E_T}(P)]$.

Theorem 2.1 (Abel's theorem) *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 $f^* : E' \to E$. we have $f^* \circ f = [\deg f]_E$ and $f \circ f^* = [\deg f]_{E'}$.

For an elliptic curve E over a field k, 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 $E(k)$.

2.2 Elliptic curves over $\mathbb{C}$

([15]) To give an elliptic curve over $\mathbb{C}$ is equivalent to give a complex torus of dimension 1, as follows.

Let E be an elliptic curve over $\mathbb{C}$. Then, $E(\mathbb{C})$ is a connected compact abelian complex Lie group of dimension 1. Let Lie E be the tangent space of $E(\mathbb{C})$ at the origin. It 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

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

Since

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

it satisfies the Weierstrass equation

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

where $g_2 = 60 \sum_{\omega \in L}{}' \frac{1}{\omega^4}$ and $g_3 = 140 \sum_{\omega \in L}{}' \frac{1}{\omega^6}$. 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

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

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.

2.3 Modular curves over $\mathbb{C}$

([14]) 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 $\widetilde{\mathcal{R}}$. The map $H \to \widetilde{\mathcal{R}} : \tau \to (\tau, 1)$ induces a bijection $H \to \mathbb{C}^\times\backslash\widetilde{\mathcal{R}}$. We consider the map $\widetilde{\mathcal{R}} \to \mathcal{R}$ sending (ω_1, ω_2) to $\langle\omega_1, \omega_2\rangle$ and an action of $SL_2(\mathbb{Z})$ on $\widetilde{\mathcal{R}}$ 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 sending a lattice L to the isomorphism class of the elliptic curve $\mathbb{C}/L$ defines bijections

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

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.

For an integer $N \geq 1$, similarly the map sending $(\omega_1, \omega_2) \in \widetilde{\mathcal{R}}$ to the pair $(E, P) = \left(\mathbb{C}/\langle\omega_1, \omega_2\rangle, \frac{\omega_2}{N}\right)$ 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 $\frac{c\omega_1 + d\omega_2}{N} \equiv \frac{\omega_2}{N} \bmod \langle\omega_1, \omega_2\rangle$ since $c \equiv 0, d \equiv 1 \bmod N$. 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

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

We have finite flat maps $Y_1(N)\to Y_0(N)\to Y(1)=\mathbf{A}^1$ of open Riemann surfaces. The degree 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 have $S_2(N)=\Gamma(X_0(N),\Omega^1)$. 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 $e>0$,

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

$g_0(11)=1$ 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 $\Delta=\left(\frac{124}{3}\right)-27\left(\frac{2501}{27}\right)^2=-11^5$. We have $S_2(11)=\Gamma(X_0(11),\Omega^1)=\mathbb{C}\frac{dx}{y}$.

Universal elliptic curve. 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 $\mathbb{C}^\times \times \Gamma_1(N) \ltimes \mathbb{Z}^2 \to \mathbb{C}^\times \times \Gamma_1(N)$.

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

$$E_1(N) = (\Gamma_1(N) \ltimes \mathbb{Z}^2)\backslash(H \times \mathbb{C}) \to Y_1(N) = \Gamma_1(N)\backslash H.$$

The fiber at $\tau \in H$ is the elliptic curve $\mathbb{C}/\mathbb{Z}+\mathbb{Z}\tau$. It has the following modular interpretation. For a holomorphic family $E \to S$ of elliptic curve together with a section $P : S \to E$ of order N, 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 $E_1(N)$ and the section defined by $z = \dfrac{\omega_2}{N}$.

2.4 Modular curves and modular forms

Let $N \geq 4$. Let $\omega_{Y_1(N)}$ be the invertible sheaf $0^*\Omega_{E_1(N)/Y_1(N)}$ where $0 : Y_1(N) \to E_1(N)$ is the 0-section of the universal elliptic curve. Then, we have

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

By the isomorphism $\omega^{\otimes 2} \to \Omega_{Y_1(N)} : dz^{\otimes 2} \mapsto d\tau$, 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 $E_1(N) \to Y_1(N)$ is uniquely extended to a smooth group scheme $\overline{E}_1(N) \to X_1(N)$ whose fibers at cusps are $\mathbf{G}_m$. Let $\omega_{X_1(N)} = O^*\Omega_{\overline{E}_1(N)/X_1(N)}$. Then we have $\omega^{\otimes 2} = \Omega(\log(\text{cusps}))$ and

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

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 $\mathbb{Z}[\frac{1}{N}]$

Let $N \geq 1$ be an integer. 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 2.2 *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

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

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 equal 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 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 $dy^2 = x^3 + (d-2)x^2 + x$. $Y_1(4)_{\mathbb{Z}[\frac{1}{4}]}$ is given by $\text{Spec}\mathbb{Z}[\dfrac{1}{4}][d, \dfrac{1}{d(d-4)}]$.

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

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

Theorem 2.3 *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 $\mathbb{Z}[\frac{1}{r}]$.*

Proof for $r = 3$. $Y(3) = \mathrm{Spec}\mathbb{Z}[\frac{1}{3}][\mu, \frac{1}{\mu^3-1}]$. $E \subset \mathbf{P}^2$ is defined by $X^3 + Y^3 + Z^3 - 3\mu XYZ$ and $O = (0, 1, -1), P = (0, 1, -\omega^2), Q = (1, 0, -1)$.

$r = 4$. Let E be the universal elliptic curve over $Y_1(4)$. Then, $Y(4)$ is the open and closed subscheme of $E[4]$ defined by the condition that (P,Q) defines an isomorphism $(\mathbb{Z}/4\mathbb{Z})^2 \to E[4]$.

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 $Y(s)_{\mathbb{Z}[\frac{1}{r}]}$. In general, $Y(r)_{\mathbb{Z}[\frac{1}{r}]}$ 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 $s = 3, 4$.

$Y(r)_{\mathbb{Z}[\frac{1}{r}]}$ for $r = 1, 2$ are also defined as the quotients. The j-invariant defines an isomorphism $Y(1) \to \mathbb{A}^1_{\mathbb{Z}}$. 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 the Weil pairing recalled below, the scheme $Y(r)_{\mathbb{Z}[\frac{1}{r}]}$ is naturally a scheme over $\mathbb{Z}[\frac{1}{r}, \zeta_r]$. For $P, Q \in E[r](S)$ and $\mathcal{L}$ be an invertible $\mathcal{O}_E$-module corresponding to P. Since $[r]^*\mathcal{L} = 0$, a canonical isomorphism $Q^*[r]^*\mathcal{L} = O^*[r]^*\mathcal{L}$ is defined. Since $[r](Q) = 0$, we have another canonical isomorphism $Q^*[r]^*\mathcal{L} = 0^*\mathcal{L} = O^*[r]^*\mathcal{L}$. By comparing them, we obtain an invertible function $(P,Q)_N$ on S. Its N-th power is 1 and hence $(P,Q)_N \in \mu_N$.

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

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

$Y_1(N)_{\mathbb{Z}[\frac{1}{N}]}$ 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 $(E/\langle P\rangle, \text{Image of } Q)$ such that $(P,Q)_N = \zeta_N$.

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

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

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

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 $N \geq 4$. It 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

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

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 $(E \to E', P)$ to $(E', \text{Image of } P)$, 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 $s_* \circ t^*$ where $s, t : \overline{T}_1(N,n)_{\mathbb{Z}[\frac{1}{N}]} \to X_1(N)_{\mathbb{Z}[\frac{1}{N}]}$ are the maps defined above. The push-forward map s_* is induced by the trace map. 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 define the Hecke algebra by

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

Proposition 2.4 *The map*

$$S_k(\Gamma_1(N))_{\mathbb{C}} \to \mathrm{Hom}_{\mathbb{Q}}(T_k(\Gamma_1(N)), \mathbb{C}) \tag{1}$$

sending a cusp form f to the linear form $T \mapsto a_1(Tf)$ is an isomorphism.

Proof. Suffices to show that the pairing $(T, f) \mapsto a_1(Tf)$ 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 2.5 *The isomorphism* (1) *induces a bijection of finite sets*

$$\{f \in S_k(\Gamma_1(N))_{\mathbb{C}} | \text{normalized eigenform}\} \to \mathrm{Hom}_{\mathbb{Q}\text{-algebra}}(T_k(\Gamma_1(N)), \mathbb{C}) \qquad (2)$$

Proof. Let φ be the linear form corresponding to f. $\varphi(1) = 1$ is equivalent to $a_1(f) = 1$. If φ is a ring hom, we have $a_n(Tf) = a_1(T_nTf) = \varphi(T_nT) = \varphi(T)\varphi(T_n) = \varphi(T)a_1(T_nf) = \varphi(T)a_n(f)$ for every $n \geq 1$ and $T \in T_k(\Gamma_1(N))$. Thus, $Tf = \sum_n a_n(Tf)q^n = \sum_n \varphi(T)a_n(f)q^n = \varphi(T)f$ 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 φ is a ring homomorphism.

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 $T_k(\Gamma_1(N)) \to \mathbb{C}$ and hence is a finite extension of $\mathbb{Q}$.

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

3.1 Galois representations and finite étale group schemes

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

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

for $N \geq 1$.

Lemma 3.1 *Let $p \nmid N$. The action of φ_p on $A(\overline{\mathbb{Q}}) = A(\overline{\mathbb{F}_p})$ is the same as that defined by the geometric Frobenius endomorphism $Fr : A_{\mathbb{F}_p} \to A_{\mathbb{F}_p}$.*

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

3.2 Jacobian of a curve and its Tate module

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 ℓ-adic representation. To construct the Galois representation in the general case, we need to introduce the Jacobian.

Let $X \to S$ be a proper smooth curve with geometrically connected fibers of genus g. For simplicity, we assume $X \to S$ has a section $s : S \to X$. Similarly as in Section 1.2, we have a decomposition

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

and a functor $\mathrm{Pic}^0_{X/S} : (\text{Schemes}/S) \to (\text{Abelian groups})$ is defined.

Theorem 3.2 *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. They define a map of functors and hence a morphism $f_* : \mathrm{Jac}_{X/S} \to \mathrm{Jac}_{Y/S}$. 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 basis e_y to $\sum_{x \mapsto y} e(x/y) \cdot e_x$. 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 basis e_x to $[\kappa(x) : \kappa(y)]e_y$ for $y = f(x)$.

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 and by $\langle \mathcal{L}, \mathcal{M} \rangle = f_{D*}\mathcal{L}|_D$ 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 $N[\mathcal{L}] = 0 \in \mathrm{Pic}^0(X/S)$, 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.

Jacobian over $\mathbb{C}$. 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 γ to the linear form $\omega \mapsto \int_\gamma \omega$. It is injective and the image is a lattice. A canonical map

$$\mathrm{Pic}^0(X) = J_X(\mathbb{C}) \to \mathrm{Hom}(\Gamma(X, \Omega), \mathbb{C})/\mathrm{Image}\ H_1(X, \mathbb{Z}) \tag{3}$$

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 (3) 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 $H_1(X,\mathbb{Z}) \times H_1(X,\mathbb{Z}) \to \mathbb{Z}$.

The Tate module of Jacobian. Let X be a proper smooth curve over a field k with geometrically connected fiber of genus g and ℓ be a prime number invertible in k. We put

$$V_\ell \,\mathrm{Jac}_{X/k} = \mathbb{Q}_\ell \otimes \varprojlim{}_n \mathrm{Jac}_{X/k}[\ell^n](\bar{k}) = \mathbb{Q}_\ell \otimes \varprojlim{}_n \mathrm{Pic}(X_{\bar{k}})[\ell^n].$$

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 ℓ-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 ℓ-adic representation $V_\ell \,\mathrm{Jac}_{X_\mathbb{Q}/\mathbb{Q}}$ is unramified at $p \nmid N\ell$.

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 $(\Gamma_f, \Delta_X)_{X \times_k X}$ be the intersection product. Then, for a prime number ℓ invertible in k, the Lefschetz trace formula 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 of the Frobenius endmorphism $F : X \to X$. Then we obtain

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

and

$$Z(X,t) = \exp \sum_{n=1}^{\infty} \frac{\mathrm{Card} X(\mathbb{F}_{p^n})}{n} t^n = \frac{\det(1 - F_* t : T_\ell J_X)}{(1-t)(1-pt)}.$$

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 α be an eigenvalue of φ_p on $T_\ell J_X$. Then, α is an algebraic integer and its conjugates have complex absolute values $\sqrt{p}$.*

3.3 Construction of Galois representations

Eichler-Shimura isomorphism

Proposition 3.5 *The canonical map*

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

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 $\int_{f_*\gamma}\omega=\int_\gamma f^*\omega$.

It follows from Proposition that the Fourier coefficients $a_n(f)$ are integers in the number field $\mathbb{Q}(f)$ for a normalized eigenform f.

Corollary 3.6 *$V_\ell(J_1(N))$ is a free $T_2(\Gamma_1(N))_{\mathbb{Q}_\ell}$-module of rank 2.*

Proof. By Propositions 2.4 and 3.5 and by fpqc descent, $H_1(X_1(N),\mathbb{Q})$ is a free $T_2(\Gamma_1(N))$-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

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

$V_{f,\lambda}$ is a 2-dimensional ℓ-adic representation unramified at $p\nmid N\ell$.

Theorem 3.7 *$V_{f,\lambda}$ is associated to f. Namely, for $p\nmid N\ell$, we have*

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

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 α and β are $\sqrt{p}$.*

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

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 α 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' is the image of $Q\in E/C[N]$ such that (Image of $P,Q)=\zeta_N$ 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 $(P^{(p)}, Q')_N = (P, Q)_N$. 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 $w \circ Fr = Fr \circ \langle p \rangle^{-1} \circ w$.

Thus, 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

$$a, b : \mathcal{M}_1(N)_{\mathbb{F}_p} \to \mathcal{M}_{1,0}(N)_{\mathbb{F}_p}$$

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

$$\begin{pmatrix} s \circ a & s \circ b \\ t \circ a & t \circ b \end{pmatrix} = \begin{pmatrix} \mathrm{id} & F \\ F & \langle p \rangle \end{pmatrix}. \tag{4}$$

The maps $a, b : \mathcal{M}_1(N)_{\mathbb{F}_p} \to \mathcal{M}_{1,0}(N)_{\mathbb{F}_p}$ induce closed immersions $a, b : X_1(N)_{\mathbb{F}_p} \to X_{1,0}(N)_{\mathbb{F}_p}$.

Proposition 3.11 *Let $N \geq 1$ be an integer and $p \nmid N$ be a prime number. Then $s, t : X_{1,0}(N, p) \to X_1(N)$ is finite flat of degree $p + 1$.*

The map

$$a \amalg b : X_1(N)_{\mathbb{F}_p} \amalg X_1(N)_{\mathbb{F}_p} \to X_{1,0}(N, p)_{\mathbb{F}_p}$$

is an isomorphism on a dense open subscheme.

Proof. Since the maps $a, b : X_1(N)_{\mathbb{F}_p} \to X_{1,0}(N,p)_{\mathbb{F}_p}$ are sections of projections $X_{1,0}(N,p)_{\mathbb{F}_p} \to X_1(N)_{\mathbb{F}_p}$, 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 $X_{1,0}(N,p)_{\mathbb{F}_p} \to X_1(N)_{\mathbb{F}_p}$ are finite flat of degree p, the assertion follows.

Corollary 3.12

$$\begin{array}{ccc} \mathrm{Pic}^0(X_1(N))(\overline{\mathbb{Q}})[\ell^n] & \xrightarrow{T_p} & \mathrm{Pic}^0(X_1(N))(\overline{\mathbb{Q}})[\ell^n] \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(X_1(N))(\overline{\mathbb{F}_p})[\ell^n] & \xrightarrow{F_* + \langle p \rangle F^*} & \mathrm{Pic}^0(X_1(N))(\overline{\mathbb{F}_p})[\ell^n] \end{array}$$

is commutative.

By Proposition, we have a commutative diagram

$$\begin{array}{ccc} \mathrm{Pic}(X_1(N)_{\mathbb{Z}_p^{\mathrm{unr}}}) & \xrightarrow{T_p = s_* t^*} & \mathrm{Pic}(X_1(N)_{\mathbb{Z}_p^{\mathrm{unr}}}) \\ \downarrow & & \downarrow \\ \mathrm{Pic}(X_1(N)_{\overline{\mathbb{F}_p}}) & \xrightarrow{(t \circ a)_* (s \circ a)^* + (t \circ b)_* (s \circ b)^*} & \mathrm{Pic}(X_1(N)_{\overline{\mathbb{F}_p}}) \end{array}$$

By (4), the bottom arrow is $F_* + \langle p \rangle F^*$.

Proof of Theorem. By Corollary, we have

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

Taking the determinant, we get

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

By Lemma 3.10, we get

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

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

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

4.1 Etale cohomology

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

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

is a bijection for every family of étale morphisms $(U_i \to U)_{i \in I}$ satisfying $U = \bigcup_{i \in I}$ Image $(U_i \to U)$. 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. 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 and 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.

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

If $S = \mathrm{Spec}\ k$ for a field k, the category of étale sheaves on S is equivalent to that of discrete set with continuous G_k-action 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 $H^q(X, \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}/N\mathbb{Z} \to H^q(X, \mathbb{Z}/N\mathbb{Z})$.

Let X be a proper smooth variety over a field k and $f : X \to X$ is an endomorphism. Then, for a prime number ℓ invertible in k, the Lefschetz trace formula gives us

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

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

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

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

4.2 Construction of Galois representations

Let $N \geq 5$ and $k \geq 2$. Proposition 3.5 is generalized as follows. Let $f : E_1(N) \to Y_1(N)$ 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*

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

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

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

$V_{f,\lambda}$ is a 2-dimensional ℓ-adic representation unramified at $p \nmid N\ell$.

Theorem 4.4 *$V_{f,\lambda}$ is associated to f. Namely, for $p \nmid N\ell$, we have*

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

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 α and β are $p^{\frac{k-1}{2}}$.*

References

[1] G. Cornell, J. Silverman (eds.), Arithmetic Geometry, Springer, 1986.

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

[3] 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.

[4] 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.

[5] P. Deligne, *Formes modulaires et représentations ℓ-adiques,* in Lecture Notes in Math., Springer, **179**, 1971, 139-172.

[6] F. Diamond, J. Shurman, A First course in Modular forms, Springer GTM 228 (2005).

[7] 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.

[8] H. Hida, Modular forms and Galois cohomology, Cambridge studies in advanced math., 69, Cambridge Univ. Press, 2000.

[9] H. Hida, Geometric modular forms and elliptic curves, World Scientific (2000).

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

[11] T. Saito, Fermat's last theorem (in Japanese), Iwanami, 1 (2000), 2 (to be published).

[12] J-P. Serre, A course in arithmetic, Springer GTM **7** (1973).

[13] J.-P. Serre, Abelian ℓ-adic representations and Elliptic curves, Benjamin, 1968.

[14] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Functions, Princeton Univ. Press, 1971.

[15] J. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Math., Springer, **106**, 1986.

[16] J. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Graduate Texts in Math., Springer, **151**, 1994.