An introduction to Galois representations and modular forms

Takeshi Saito

Panoramas et Synthèses

Numéro 49

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
Publié avec le concours du Centre national de la recherche scientifique

Panoramas & Synthèses
49, 2016, p. 1–27

AN INTRODUCTION TO GALOIS REPRESENTATIONS AND MODULAR FORMS

by

Takeshi Saito

Abstract. – These notes are based on a series of lectures given at the summer school held on July 17-29, 2006 at IHÉS. 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

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

A goal in number theory is to understand finite extensions of $\mathbb{Q}$. By Galois theory, it is equivalent to understanding 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 their degrees. Class field theory provides us with 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 ℓ-adic characters $G_{\mathbb{Q}} \to \mathbb{Q}_{\ell}^{\times}$ for a prime ℓ, we find more characters. For example, the ℓ-adic cyclotomic character is defined as the composition:

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

2010 Mathematics Subject Classification. – 11F80, 11F03, 11G18.
Key words and phrases. – Galois representations, modular forms, modular curves, elliptic curves, Hecke operators.

The ℓ-adic characters "with motivic origin" are generated by Dirichlet characters and ℓ-adic cyclotomic characters:

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

if we use a fancy terminology "geometric," that will not be explained in this note. For the definition, we refer to [**11**].

When we leave the realm of class field theory, the first representations we encounter are those of degree 2. For ℓ-adic Galois representations of degree 2, we expect to have (cf. [**11**]) a similar equality

$$\{\text{odd "geometric" } \ell\text{-adic representations of } G_{\mathbb{Q}} \text{ of degree 2 with distinct Hodge-Tate weights}\} = \{\ell\text{-adic representations associated to modular form of weight at least 2}\},$$

up to a 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 these notes, we discuss only one direction $\supset$ established by Shimura and Deligne ([**20**], [**4**]). We will not discuss the other direction $\subset$, which is almost established ([**13**]) after the revolutionary work of Wiles, although it has significant consequences including Fermat's last theorem, the modularity of elliptic curves, etc. ([**24**], [**2**]).

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. Some more detail can be found in the books [**15, 16**].

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

I would like to acknowledge on this occasion that many of Japanese participants of the summer school are supported by JSPS Core-to-Core Program 18005 New Developments of Arithmetic Geometry, Motive, Galois Theory, and Their Practical Applications.

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 the $\mathbb{C}$-vector spaces $S_k(N,\varepsilon) \subset M_k(N,\varepsilon)$ of cusp forms and of modular forms of level N, weight k and character ε. We will see later in §3.4 that they are of finite dimension by using compactifications of modular curves. For $\varepsilon = 1$, we write $S_k(N) \subset M_k(N)$ for $S_k(N,1) \subset M_k(N,1)$. For this subsection, we refer to [**10**] 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 $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto d \bmod N$. Their 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 $H = \{\tau \in \mathbb{C} | \mathrm{Im}\ \tau > 0\}$ is defined by

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

for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ 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 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 $q_N = \exp(2\pi i \frac{\tau}{N})$. 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

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

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 **[18]** 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

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