Galois Representations for Siegel Modular Forms

Angus McAndrew

The University of Melbourne

(Supervised by Alex Ghitza)

AustMS

Overview

Thank you to the AustMS Student Support Scheme for the funding to attend this conference.

You sure know how to make a guy feel special.

Goal

Describe some features of the correspondence between modular forms and Galois representations.

Goal

Describe some features of the correspondence between modular forms and Galois representations.

Goal

A walking tour of some Langlands material.

Goal

Describe some features of the correspondence between modular forms and Galois representations.

Goal

A speedwalking tour of some Langlands material.

Galois Representation

We are interested in the group

$$\mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \{\mathbb{Q}\text{-automorphisms of } \overline{\mathbb{Q}}\}.$$

In particular, we would like to understand the representations

$$\rho : \mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathsf{GL}(V).$$

We will do this by considering the images $\rho(\mathrm{Frob}_\ell)$.

Modular Forms

Definition (Modular Form)

A *modular form of weight k, level N and character ε* is a holomorphic function $f : \mathfrak{H}_1 \to \mathbb{C}$ such that

$$f\left(\frac{az+b}{cz+d}\right) = \varepsilon(d)(cz+d)^k f(z) \quad \text{for} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N),$$

where

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| c \equiv 0 \pmod{N} \right\},$$

and f is *holomorphic at infinity*.

The Basic Theory

Modular forms relate to many interesting objects in number theory, but why would that help us?

In fact, modular forms are extremely explicit and nice to study. For example, when $N = 1$ we have the following classification.

Example

$$M_*(\mathrm{SL}_2(\mathbb{Z}); \mathbb{C}) = \mathbb{C}[E_4, E_6],$$

where

$$E_k(q) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n.$$

Back to Galois Representations

Theorem (Deligne)

Let $f \in M_k(\Gamma_1(N), \varepsilon; \overline{\mathbb{F}}_p)$ be a normalised eigenform with $f(q) = \sum a(n)q^n$. There exists a semisimple continuous Galois representation

$$\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

which is unramified for all primes $\ell \nmid pN$ and

$$\mathrm{charpoly}(\rho_f(\mathrm{Frob}_\ell)) = X^2 - a(\ell)X + \varepsilon(\ell)\ell^{k-1}.$$

But amazingly...

Theorem (Serre's Conjecture, Khare-Wintenberger)

Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ be an irreducible, odd Galois representation. Then there exist integers k_ρ, N_ρ, a character ε_ρ and a cusp form $f \in S_{k_\rho}(\Gamma_1(N_\rho), \varepsilon_\rho; \overline{\mathbb{F}}_p)$ such that $\rho \cong \rho_f$.

Where ρ_f refers to the Galois representation attached to f by the theorem of Deligne.

Still unconvinced?

Fermat's Last Theorem

Incredibly, Serre's conjecture $\Rightarrow$ Fermat's Last Theorem.

The idea is as follows

$$\begin{aligned} \text{Solution } (a,b,c) &\longmapsto \text{Elliptic curve } y^2 = x(x-a^p)(x+b^p) \\ &\longmapsto \text{Galois Representation from } E[p] \\ &\longmapsto \text{Modular Form } f \in S_2(\Gamma_0(2); \overline{\mathbb{F}}_p) \end{aligned}$$

However, the space $S_2(\Gamma_0(2); \overline{\mathbb{F}}_p) = \{0\}$, so only the zero solution can exist.

Ok, water break!

Siegel Modular Forms

Definition (Siegel Modular Form)

Let $\kappa : \mathrm{GL}_g(\mathbb{C}) \to \mathrm{GL}_m(\mathbb{C})$ be a rational representation. A *Siegel modular form of degree g, weight κ and level N* is a holomorphic function $F : \mathfrak{H}_g \to \mathbb{C}^m$ such that

$$F((A\mathbf{z}+B)(C\mathbf{z}+D)^{-1}) = \kappa(C\mathbf{z}+D)F(\mathbf{z}), \quad \text{for} \quad \gamma \in \Gamma^g(N),$$

where

$$\Gamma^g(N) = \ker\left(\ \mathrm{Sp}_{2g}(\mathbb{Z}) \to \mathrm{Sp}_{2g}(\mathbb{Z}/N\mathbb{Z}) \ \right)$$

The "Basic" Theory

Here things are more tricky. There are quite a few obstacles in even computing examples. There are still some nice qualities, like the following when $\kappa = \det^k$ and $g = 2$, $N = 1$.

Theorem (Igusa Generators)

$$M_*(\mathrm{Sp}_4(\mathbb{Z}); \mathbb{C}) = \mathbb{C}[\phi_4, \phi_6, \chi_{10}, \chi_{12}, \chi_{35}]/R$$

Note that we can construct spaces like

$$M_\kappa(\Gamma^g(N); \overline{\mathbb{F}}_p)$$

as before.

The Hecke algebra

Consider the local Hecke algebra

$$\mathcal{H}_\ell = \mathcal{H}(\mathrm{GSp}_{2g}(\mathbb{Q}_\ell), \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)).$$

Elements of this algebra are called *Hecke operators* T. These act as linear operators on the vector space $M_\kappa(\Gamma^g(N); \overline{\mathbb{F}}_p)$.

We call a form F an *eigenform* for $\mathcal{H}_\ell$ if it is a simultaneous eigenvector for all $T \in \mathcal{H}_\ell$ and we denote the eigenvalue $\Psi_F(T)$.

The Satake Isomorphism

Theorem (Satake Isomorphism)

We have an isomorphism

$$\mathcal{S}_{p,\ell} : \overline{\mathbb{F}}_p \otimes \mathcal{H}_\ell \xrightarrow{\sim} \overline{\mathbb{F}}_p \otimes R(\mathrm{GSpin}_{2g+1})$$

where

- GSpin_{2g+1} *is the dual group of* GSp_{2g}, *and*
- $R(G)$ *is the representation ring of* G.

Now - back to modular forms!

Satake Parameters

Let $F \in M_\kappa(\Gamma^g(N); \overline{\mathbb{F}}_p)$ be an eigenform. Then we have the eigenvalue character $\Psi_F : \overline{\mathbb{F}}_p \otimes \mathcal{H}_\ell \to \overline{\mathbb{F}}_p$.

We can thus construct a character

$$\Psi_F \circ \mathcal{S}_{p,\ell}^{-1} : \overline{\mathbb{F}}_p \otimes R(\mathrm{GSpin}_{2g+1}) \to \overline{\mathbb{F}}_p.$$

This corresponds to $s_{F,\ell} \in \mathrm{GSpin}_{2g+1}(\overline{\mathbb{F}}_p)$, called the *$\ell$-Satake parameter of F*.

C'mon, Galois representations already!

Galois Representations

Conjecture

Let $F \in M_\kappa(\Gamma^g(N); \overline{\mathbb{F}}_p)$ be an eigenform for each $\mathcal{H}_\ell$ where $\ell \nmid pN$. There exists a representation, unramified for each $\ell \nmid pN$, such that

$$\begin{array}{rccc} \rho_F : & \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \longrightarrow & \mathrm{GSpin}_{2g+1}(\overline{\mathbb{F}}_p) \\ & \mathrm{Frob}_\ell & \longmapsto & s_{F,\ell}. \end{array}$$

This is in fact a theorem in the cases $g = 1$ (seen earlier) and $g = 2$ (due to Taylor, Laumon and Weissauer).

How does one actually play with these?

The Theta Operator

In the classical case, there is a differential operator $\theta : M_k(\Gamma_1(N), \varepsilon; \overline{\mathbb{F}}_p) \to M_{k+p+1}(\Gamma_1(N), \varepsilon; \overline{\mathbb{F}}_p)$. This has the following nice property when related to Galois representations.

Theorem

Let $f \in M_k(\Gamma_1(N), \varepsilon; \overline{\mathbb{F}}_p)$ be an eigenform such that $\theta f \neq 0$. Then

$$\rho_{\theta f} = \chi \otimes \rho_f,$$

where χ is the cyclotomic character (mod p).

This is useful, since it allows one to reduce to the case $k \leq p+1$ and work with low weights.

Siegel Theta Operators

We'd like a similar result for differential operators on Siegel modular forms. As it turns out, there are many generalisations of the theta operator. The crucial feature is how they interact with the Hecke operators T, since those define the Galois representation. For example:

Theorem

- $\Psi_{\theta_{BN}F}(T) = \det(T) \cdot \Psi_F(T)$
- $\Psi_{\theta_{FG}F}(T) = \eta(T) \cdot \Psi_F(T)$

Theta Operators on Galois Representations

Theorem (Ghitza-M.)

Let $\omega_\lambda : \mathrm{GSpin}_{2g+1}(\overline{\mathbb{F}}_p) \to \mathrm{GL}(V)$ *be the representation with highest weight* λ. *Let* ϑ *be such that* ϑF *is an eigenform and*

$$\Psi_{\vartheta F}(T) = \eta(T)^m \cdot \Psi_F(T).$$

Then

$$\omega_\lambda \circ \rho_{\vartheta F} = \chi^{m\cdot\alpha(\lambda)} \otimes (\omega_\lambda \circ \rho_F),$$

where χ *is the cyclotomic character (mod* p*), and* $\alpha(\lambda) = \log_\ell(\eta(\lambda(\ell)))$ *for any prime* $\ell \neq p$.

Thanks for listening!