Modularity of Rigid Galois Representations

Sachin Kumar
University of Waterloo, Faculty of Mathematics

April 2023

Notation

Let K be a number field and let $G_K = \text{Gal}(\overline{K}/K)$ be absolute Galois group. Let $K(t)$ be the function field of $\mathbb{P}^1/K$ and set $G_{K(t)}$ to be the Galois group $\text{Gal}(\overline{K(t)}/K(t))$. Identifying, $\text{Gal}(\overline{K(t)}/\overline{K}(t))$ with G_K, we obtain the exact sequence,

$$1 \to G_{\overline{K}(t)} \to G_{K(t)} \to G_K \to 1$$

Let p be an odd prime number and let $\mathbb{F}$ denote a finite field of characteristic p. Given a point $x \in \mathbb{P}^1(K)$, we have an associated decomposition group $G_X \subset G_{K(t)}$ and inertia subgroup $I_X \subset G_X$. There is a natural isomorphism $G_X/I_X \xrightarrow{\sim} G_K$. A continuous Galois representation $\varrho : G_{K(t)} \to GL_2(E)$ is said to be unramified at x if $I_X \subset \ker \varrho$. At any point x at which ϱ is unramified, the rigid Galois representation specializes to $\varrho_X : G_K \to GL_2(E)$. Throughout, $\mathbb{Q}(\zeta_n)$ is the cyclotomic field generated by a primitive root of unity ζ_n, and $K_n = \mathbb{Q}(\zeta_n)^+$ is its real subfield.

Rigid Galois representation

Frey representation

Let p, q are r be not neccesarily distinct primes. A Frey representation associated to $x^p + y^q = z^r$ is a Galois representation,

$$\varrho : \varrho_t : G_{K(t)} \to GL_2(\mathbb{F})$$

satisfying ther following conditions:

- The restriction of ϱ to $G_{\overline{K}(t)}$ is irreducible with trivial determinant. We let $\varrho^{\text{geom}} : G_{\overline{K}(t)} \to PSL_2(\mathbb{F})$ be the projectivization of this representation.
- The representation $\varrho^{\text{geom}} : G_{\overline{K}(t)} \to PSL_2(\mathbb{F})$ is unramified away from $\{0, 1, \infty\}$.
- It maps the inertia groups at 0, 1, ∞ to subgroups of $PSL_2(\mathbb{F})$ of order p, q, r respectively.

For each point $x \in \mathbb{P}^1(K) \setminus \{0, 1, \infty\}$ we obtain a Galois representation $\varrho_X : G_K \to GL_2(\mathbb{F})$, thus giving us a 1-parameter family of Galois representations. Given a nontrivial solution (a, b, c) to $x^p + y^q = z^r$, we obtain a Galois representation,

$$\rho = \varrho(a^p/c^r) : G_K \to GL_2(\mathbb{F})$$

A certain quadratic twist of ρ is shown to have very little ramification. Two Frey representation ϱ_1 and ϱ_2 are equivalent if ϱ_1 is conjugate over $\overline{\mathbb{F}}$ to a central twist of ϱ_2.

Given $x \in \mathbb{P}^1(K)$. The inertia group $I_X \cong \widehat{\mathbb{Z}}(1)$. Choosing a topological generator γ_j of I_j for $j \in \{0, 1, \infty\}$, set $\sigma_j \in PSL_2(\mathbb{F})$ to be $\varrho^{\mathrm{geom}}(\gamma_j)$. The decomposition groups and generators γ_j may be chosen so that the relationship $\sigma_0\sigma_1\sigma_\infty = 1$ is satisfied in $PSL_2(\mathbb{F})$. Assuming p, q, r are odd primes, there is a unique lift of $\widetilde{\sigma}_j$ of σ_j to $SL_2(\mathbb{F})$. The representation ϱ is even (resp. odd) if $\widetilde{\sigma}_0\widetilde{\sigma}_1\widetilde{\sigma}_\infty = 1$ (resp. -1).

Rigidity Method

Construction and classification

There are two methods of constructing and classifying Frey representations. One method is to use results on rigidity due to Belyi, Fried, Thompson and Matzat. The other method is to consider Galois representations arising from hypergeometric abelian varieties of GL_2-type. The strategy is to first define a Galois representation $\varrho^{\mathrm{geom}} : G_{\overline{K}(t)} \to PSL_2(\mathbb{F})$ which is unramified away from $\{0, 1, \infty\}$. The maximal quotient of $G_{\overline{K}(t)}$ which is unramified away from $\{0, 1, \infty\}$ is isomorphic to the profinite completion of the fundamental group of $\mathbb{P}^1 \setminus \{0, 1, \ infty\}$. Thus, this quotient is topologically generated by 3 loops α_j for $j = 0, 1, \infty$, and are subject to the relation $\alpha_0\alpha_1\alpha_\infty = 1$. In order to specify a Galois representation ϱ^{geom}, it suffices to choose 3 elements $\sigma_j \in PSL_2(\mathbb{F})$ such that $\alpha_j \mapsto \sigma_j$. Rigidity theorems are used (as well as certain cohomological inputs) to extend the Galois representation defined on $G_{\overline{K}(t)}$ to $G_{K(t)}$. Let us briefly summarize results that can be proven via the rigidity theorem.

Frey representation of $x^p + y^p = z^p$

Theorem (Hecke). Let p be a odd prime. Then, there is a unique Frey representation $\varrho_t : G_{\mathbb{Q}(t)} \to GL_2(\mathbb{F}_p)$ associated to $x^p + y^p = z^p$. Futhermore, this representation is odd.

We will see a theorem on the Frey representation of $x^p + y^p = z^r$. The convention is that p is the characteristic of the Frey representation.

Theorem (Darmon). Let p and r be distinct primes. Assume that p is odd. Let $K = \mathbb{Q}(\zeta_r)^+$ and $\mathbb{F}$ be the residue field of K at a prime $\mathfrak{p} \mid p$. There are exactly $(r - 1)$ Frey representations,

$$\varrho_t : G_{K(t)} \to GL_2(\mathbb{F})$$

up to equivalence. When $r \neq 2$, exactly $\frac{r-1}{2}$ representations are even and $\frac{r-1}{2}$ are odd.

We will discuss Frey representation of $x^r + y^r = z^p$. Recall that p is the characteristic of the Frey representation, ie., the finite field $\mathbb{F}$.

Theorem (Darmon). Let p and r be distinct odd primes. Let $K = \mathbb{Q}(\zeta_r)^+$ and $\mathbb{F}$ be the residue field of K at a prime $\mathfrak{p} \mid p$. There are exactly $\frac{(r-1)(r-2)}{2}$ Frey representations,

$$\varrho_t : G_{K(t)} \to GL_2(\mathbb{F})$$

up to equivalence. Exactly $\frac{(r-1)^2}{4}$ representations are odd and $\frac{(r-1)(r-3)}{4}$ are even.

Similarly, we will discuss Frey representation of $x^p + y^q = z^r$, *Theorem (Darmon).* Let p, q and r be distinct primes and assume that p is odd. Let $K = \mathbb{Q}(\zeta_r, \zeta_q)^+$ and $\mathbb{F}$ be the residue field of K at a prime $\mathfrak{p} \mid p$. There are exactly $\frac{(r-1)(q-1)}{2}$ Frey representations,

$$\varrho_t : G_{K(t)} \to GL_2(\mathbb{F})$$

up to equivalence. Exactly $\frac{(r-1)(q-1)}{4}$ representations are odd and $\frac{(r-1)(q-1)}{4}$ are even.

hypergeometric abelian varieties: $x^p + y^p = z^p$

The Frey representations constructed via rigidity are realized as Galois representations associated to certain hypergeometric abelian varities. Consider Legendre family, $J = J(t) : y^2 = x(x-1)(x-t)$, of elliptic curves. The module $J[p] \simeq \mathbb{F}_p \oplus \mathbb{F}_p$ is a module over $G_{\mathbb{Q}(t)}$. The Galois representation,

$$\varrho_t : G_{\mathbb{Q}(t)} \to GL_2(\mathbb{F}_p)$$

is the Frey representation associated to $x^p + y^p = z^p$. Now, let's look at the case when $x^p + y^p = z^2$. let C_2 be the family of elliptic curves, $C_2 = C_2(t) : y^2 = x^3 + 2x^2 + tx$. The mod-$p$ Galois representation, $\varrho_t : G_{\mathbb{Q}(t)} \to GL_2(\mathbb{F}_p)$ arising from $C_2[p]$ is the associated Frey representation. Now, let's discuss when $x^p + y^p = z^r$, when r is a odd prime. Suppose that p and r are distinct odd primes. Let $\omega_j = \zeta_r^j + \zeta_r^{-j}$, and set $\omega = \omega_1$. Note that $K := \mathbb{Q}(\omega)$ is the real subfield of $\mathbb{Q}(\zeta_r)$. The degree $d = [K : \mathbb{Q}]$ is $\frac{r-1}{2}$. Let $g(x) = \prod_j (x + \omega_j)$ be the characteristic polynomial over $-\omega$. Set $f(x) = xg(x^2 - 2)$, and consider the hyperelliptic curves over $\mathbb{Q}(t)$ defined by,

$$C_r^- = C_r^-(t) : y^2 = f(x) + 2 - 4t$$
$$C_r^+ = C_r^+(t) : y^2 = (x+2)(f(x) + 2 - 4t)$$

and let $J_r^\pm$ be the Jacobian of $C_r^\pm$ over $\mathbb{Q}(t)$. These Jacobians have real multiplication by K, ie., $\mathrm{End}_{\overline{\mathbb{Q}}(t)}(J_r^\pm) \simeq \mathcal{O}_K$. Fix $\mathfrak{p} \mid p$ of K and let $\mathbb{F}$ be the residue field of $\mathfrak{p}$. Choose a homomorphism $\varphi : \mathcal{O}_K \to \mathbb{F}$. The module $J_r^\pm[p] \otimes_\varphi \mathbb{F} \simeq \mathbb{F} \oplus \mathbb{F}$ is a module over $G_{K(t)}$, and

$$\varrho_r^\pm = \varrho_r^\pm(t) : G_{K(t)} \to GL_2(\mathbb{F})$$

the associated Galois representation.

Theorem (Darmon). Let $K = \mathbb{Q}(\zeta_r)^+$ and let $\mathbb{F}$ be the residue field of K are a prime $\mathfrak{p} \mid p$. As $\varphi : \mathcal{O}_K \to \mathbb{F}$ ranges over all $\frac{r-1}{2}$ homomorphisms, the representations $\varrho_r^\pm : G_{K(t)} \to GL_2(\mathbb{F})$ give a rise to the $(r-1)$ characteristic p Frey representation for $x^p + y^p = z^r$. The representations ϱ_r^+ are even representation and ϱ_r^- are odd.

We will discuss hypergeometric abelian varieties, where $x^r + y^r = z^p$. Let p and r be distict odd primes. Choose an odd integer $1 \leq j \leq r-2$, and consider the curves over $\mathbb{Q}(t)$ defined by,

$$X_{r,r}^-(t) : y^{2r} = u^2 x^{j-2} \left(\frac{x-1}{x-u}\right)^{j+2}$$
$$X_{r,r}^+(t) : y^r = u^2 x^{j-2} \left(\frac{x-1}{x-u}\right)^{j+2}$$

where $u = \frac{t}{t-1}$. Consider the family of elliptic curves $J = J(t)$ defined by,

$$J(t) : y^2 = u^2 x^{j-2} \left(\frac{x-1}{x-u}\right)^{j+2}$$

There is an involution τ of $X_{r,r}^\pm$ and J defined by, $\tau(x,y) = \left(\frac{u}{x}, \frac{1}{y}\right)$. Maps, $\pi : X_{r,r}^- \to J$ and $\pi_r : X_{r,r}^- \to X_{r,r}^+$ are defined by,

$$\pi(x,y) = (x, y^r)$$
$$\pi_r(x,y) = (x, y^2)$$

Let $C^{\pm}_{r,r} = X^{\pm}_{r,r}/\tau$ and $J' = J/\tau$, the maps π and π_r descend to maps,

$$\pi : C^{-}_{r,r} \to J'$$
$$\pi_r : C^{-}_{r,r} \to C^{+}_{r,r}$$

Set $J^{+}_{r,r}$ to be the jacobian of $C^{+}_{r,r}$. The maps π and π_r induce maps,

$$\pi^* : J' \to \mathrm{Jac}(C^{-}_{r,r})$$
$$\pi_r^* : J^{+}_{r,r} \to \mathrm{Jac}(C^{-}_{r,r})$$

Let$J^{-}_{r,r}$ be defined to be the quotient,

$$J^{-}_{r,r} = \frac{\mathrm{Jac}(C^{-}_{r,r})}{(\pi^*(J') + \pi_r^*(J^{+}_{r,r}))}$$

We have an isomorphism $\mathrm{End}_{K(t)}(J^{+}_{r,r}) \simeq \mathcal{O}_K$.

Theorem. Let $p \neq r$ be distinct odd primes. Let $K = \mathbb{Q}(\zeta_r)^+$, and let $\mathbb{F}$ the residue field of K at a prime $\mathfrak{p} \mid p$. The representation $\varrho^{\pm}_{r,r} : G_{K(t)} \to GL_2(\mathbb{F})$ associated to $J^{\pm}_{r,r}$ as φ ranges over homomorphisms $\mathcal{O}_K \to \mathbb{F}$ are the characteristic p Frey representations associated to $x^r + y^r = z^p$.

Modular Lifting conjecture

Let K be a totally real field and p an odd prime. Let E be an finite extension of $\mathbb{Q}_p$ with valuation ring $\mathcal{O}_E$ and $\mathbb{F} = \mathcal{O}_E/\varpi$ the residue field. A continuous Galois representation $\rho : G_K \to GL_2(E)$ is said to be modular if it arises from a Hilbert modular form on $GL_2(K)$. In greater detail, this means that there is a Hecke eigencuspform f on $GL_2(K)$ and a prime $\mathfrak{p} \mid p$ in the field of Fourier coefficients of f such that $\rho_{f,\mathfrak{p}} \simeq \rho$. Modular Galois representations satisfy some characteristic properties. If the Galois representation ρ is modular then, ρ satisfies some additional conditions:

- ρ is unramified away from a finite set of primes of K.
- The resrictions of ρ to the decomposition groups at the primes of K above p are all potentially semistable.

Given a continuous Galois representation $\rho : G_K \to GL_2(E)$, let $V_\rho \simeq E \oplus E$ be the underlying vector space. There exists a Galois stable $\mathcal{O}_E$-lattice $L \subset V_E$ for the action of G_K. Let $\rho : G_K \to GL_2(\mathcal{O}_E)$ be the associated Galois representation on L and $\overline{\rho} : G_K \to GL_2(\mathbb{F})$, the mod-$\varpi$ reduction of ρ. The semisimplification of $\overline{\rho}$ is independent of the choice of Lattice L. We say that $\overline{\rho}$ is modular if (up to semisimplification) it arises from a Hecke eigencuspform g for $GL_2(K)$.

Conjecture (Darmon). Let p be an odd prime and $\rho : G_K \to GL_2(\mathcal{O}_E)$ a Galois representation such that ρ is unramified at all but finitely many primes of K and ρ is potentially semistable when restricted all primes $\mathfrak{p} \mid p$ of K. Suppose $\overline{\rho}$ is modular, then ρ itself is modular.

Let $\varrho = \varrho_t : G_{K(t)} \to GL_2(\mathcal{O}_E)$ be an irreducible Galois representation. We say that ρ is rigid if it is unramified at all points, $x \in \mathbb{P}^1(\overline{K}) - \{0, 1, \infty\}$. For $j \in \{0, 1, \infty\}$, let γ_j be a generator of the inertia group I_j and let $\sigma_j = \varrho(\gamma_j) \in GL_2(\mathcal{O}_E)$. The semisimplification of σ_j is finite of order n_j. Let $n = \mathrm{lcm}(n_0, n_1, n_\infty)$. The field K is necessarily contains $K_n = \mathbb{Q}(\zeta_n)^+$. In the event that K strictly contains K_n, then after a twist, we may in fact extend ϱ_t to $\varrho_t : G_{K_n(t)} \to GL_2(\mathcal{O}_E)$.

Theorem (Darmon). Let ϱ be the rigid Galois representation, and assume that at least one of the σ_j is unipotent, and that 8 does not divide $n(\varrho) = \mathrm{lcm}(n_0, n_1, n_\infty)$. Suppose that the modularity lifting conjecture is true, then ϱ_x arises from a Hilbert modular form on $GL_2(K)$ form for all $x \in \mathbb{P}^1(\mathbb{Q}) \setminus \{0, 1, \infty\}$.

Admissible triples

An admissible triple $(\sigma_0, \sigma_1, \sigma_\infty)$ is a triple whose elements belong to $SL_2(\mathcal{O}_E)$ such that the following conditions are satisfied:

1. The semisimplification of σ_j is finite of order n_j.
2. The group generated by σ_0, σ_1 and σ_∞ generate an irreducible subgroup of $SL_2(E)$.
3. $\sigma_0\sigma_1\sigma_\infty = 1$

Given an admissible triple $(\sigma_0, \sigma_1, \sigma_\infty)$, there is a rigid Galois representation, $\varrho_t : G_{K_n(t)} \to GL_2(E)$, whose monodromy matrices are σ_0, σ_1 and σ_∞ at 0, 1, ∞ respectively. Here, $n = \mathrm{lcm}(n_0, n_1, n_\infty)$. We will now discuss, hypergeometric abelian varieties with real multiplication. An hypergeometric abelian variety $A/\mathbb{Q}$ is an abelian scheme over $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ of dimension $[K : \mathbb{Q}]$ such that there is a $\mathrm{Gal}(K/\mathbb{Q})$-equivariant isomorphism, $\mathrm{End}_{K(t)}(A) \simeq \mathcal{O}_K$, and the associated Galois representation ϱ_t is irreducible.

Proposition. Let $(\sigma_0, \sigma_1, \sigma_\infty)$ be an admissible triple in $GL_2(\mathcal{O}_{K_n})$. Let E be the completion of K_n at a prime. There exists a hypergeometric abelian variety with multiplications by K_n, such that the associated Galois representation, $\varrho : G_{K_n(t)} \to GL_2(E)$ whose monodromy matrix at j is σ_j for $j \in \{0, 1, \infty\}$.

Let A be a hypergeometric abelian variety with multiplication by K. Letting $(\sigma_0, \sigma_1, \sigma_\infty)$ to be the triple in $SL_2(\mathcal{O}_K)$ defined by letting σ_j be the image of $\gamma_j \in I_j$ acting on the deRham cohomology $H^1_{\mathrm{dR}}(A)$, viewed as a 2-dimensional K vector space. This is an admissible tripple in $SL_2(\mathcal{O}_K)$. Conversely, every admissible triple in $SL_2(\mathcal{O}_K)$ arises in this way.

Inductive aregument

Suppose we are given a rigid Galois representation, $\varrho_t : G_{K_n(t)} \to GL_2(E)$. Let $(\sigma_0, \sigma_1, \sigma_\infty) \in SL_2(\mathcal{O}_E)$ be the associated admissible triple, $n = \mathrm{lcm}(n_0, n_1, n_\infty)$. The admissible triple arises from a hypergeometric abelian variety A with multiplication by $K = K_n$. The triple $(\sigma_0, \sigma_1, \sigma_\infty)$ lies in $SL_2(\mathcal{O}_K)$. It suffices to show that A is modular (in fibres), and the argument is via induction on n. Note that if $n = 1$, then $K = \mathbb{Q}$, and the result follows from the standard results on the modularity of elliptic curves. Assume without loss of generality that $n > 1$, such that $K \neq \mathbb{Q}$. if $n = 2$ or 4, then $K = \mathbb{Q}$, hence n has an odd prime divisor. Let ℓ be an odd prime divisor of n and let $n' = n/\ell$ and $K' = K_{n'}$. Choose a prime $\lambda \mid \ell$ of K and let $\lambda' \mid \ell$ be the prime of K' below λ. Let $\mathbb{F}$ be the residue field of K at λ, since λ' is totally ramified in K, the residue field of λ' is also $\mathbb{F}$. Let $\varphi : \mathcal{O}_K \to \mathbb{F}$ and $\varphi' : \mathcal{O}_{K'} \to \mathbb{F}$ be compatible maps. We may choose a lift $(\sigma'_0, \sigma'_1, \sigma'_\infty)$ of $(\varphi(\sigma_0), \varphi(\sigma_1), \varphi(\sigma_\infty))$ to an admissible triple of $SL_2(\mathcal{O}_{K'})$. Let A' be the abelian variety with multiplication by K' associated to $(\sigma'_0, \sigma'_1, \sigma'_\infty)$. Since $n' < n$, by the inductive hypothesis, A' is modular (in fibres). Since the two triples $(\sigma_0, \sigma_1, \sigma_\infty) \equiv (\sigma'_0, \sigma'_1, \sigma'_\infty) \pmod{\lambda}$, it follows that $A[\ell] \otimes_\varphi \mathbb{F}$ and $A'[\ell] \otimes_{\varphi'} \mathbb{F}$ are isomorphic as $G_{K'(t)}$ representations. Since A' is modular, it follows that $A[\ell] \otimes_\varphi \mathbb{F}$ is modular. By the modularity lifting conjecture, it follows that A is modular, and thus, in particular, the representation ϱ_t is modular (in fibres).