Ribet's Level-Lowering Theorem for Modular Representations

Ricky Magner

November 8, 2017

Overview

1. Galois Representations
2. Level-Lowering Theorems
3. Character Groups
4. Shimura Curves and Modular Curves

Outline for section 1

Modular Representations

- Let ℓ be an odd prime and let $\mathbb{F}$ be a finite field of characteristic ℓ. Let $\mathbb{T} = \mathbb{T}_N$ be the Hecke algebra associated to $S(N) := S_2(\Gamma_0(N))$, the space of weight 2 cuspforms of level $\Gamma_0(N)$.

Modular Representations

- Let ℓ be an odd prime and let $\mathbb{F}$ be a finite field of characteristic ℓ. Let $\mathbb{T} = \mathbb{T}_N$ be the Hecke algebra associated to $S(N) := S_2(\Gamma_0(N))$, the space of weight 2 cuspforms of level $\Gamma_0(N)$.
- We say that a (continuous) Galois representation $\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{F})$ is <u>modular of level N</u> if $\det \circ \rho$ is the mod ℓ cyclotomic character, and there is a homomorphism $\omega : \mathbb{T} \to \overline{\mathbb{F}}$ such that

$$\mathrm{tr}(\rho(\mathrm{Frob}_p)) = \omega(T_p)$$

for almost all primes p.

Modular Representations (cont.)

Theorem (Deligne)

Let $f \in S(N)$ be a Hecke eigenform and let E be the number field generated by its Hecke eigenvalues. Let ℓ be prime and pick $\lambda \mid \ell$ a place of E. Then there exists a representation $\rho_f : G_{\mathbb{Q}} \to GL_2(E_\lambda)$, unramified away from ℓN, such that

$$tr(\rho_f(Frob_p)) = a_p, \ \ and \ \det(\rho_f(Frob_p)) = p$$

for all $p \nmid \ell N$.

Modular Representations (cont.)

Theorem (Deligne)

Let $f \in S(N)$ be a Hecke eigenform and let E be the number field generated by its Hecke eigenvalues. Let ℓ be prime and pick $\lambda \mid \ell$ a place of E. Then there exists a representation $\rho_f : G_{\mathbb{Q}} \to GL_2(E_\lambda)$, unramified away from ℓN, such that

$$tr(\rho_f(Frob_p)) = a_p, \text{ and } \det(\rho_f(Frob_p)) = p$$

for all $p \nmid \ell N$.

- For example, if $f \in S(N)$ is a Hecke eigenform, then define $\omega : \mathbb{T} \to \overline{\mathbb{F}}$ by $\omega(T_p) = a_p$ ("mod ℓ") where $T_p f = a_p f$. Then the "reduction" of the representation ρ_f constructed above is modular of level N by our definition.

Outline for section 2

A condition on representations

Definition

Suppose $\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{F})$ is a Galois representation. We say ρ is finite at p if there exists a finite flat $\mathbb{F}$-vector space scheme H over $\mathbb{Z}_p$ such that the representation of $G_{\mathbb{Q}_p}$ arising from $H(\overline{\mathbb{Q}_p})$ is the restriction of ρ to the decomposition group at p.

A condition on representations

Definition

Suppose $\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{F})$ is a Galois representation. We say ρ is _finite at p_ *if there exists a finite flat $\mathbb{F}$-vector space scheme H over $\mathbb{Z}_p$ such that the representation of $G_{\mathbb{Q}_p}$ arising from $H(\overline{\mathbb{Q}_p})$ is the restriction of ρ to the decomposition group at p.*

- For example, if $E/\mathbb{Q}$ is an elliptic curve, then $E[\ell]$ is finite at all primes $p \neq \ell$ such that E has good reduction at p.

The Main Theorem

Theorem (Ribet)

Let $\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{F})$ be an irreducible modular representation of level Mp, with $p \nmid M$ and $\ell =$char$(\mathbb{F})$. Assume ρ is finite at p. Then ρ is modular of level M if at least one of the following hold:

(i) $\ell \nmid M$,

(ii) $p \not\equiv 1 \bmod \ell$.

Deligne's Theorem revisited

- To prove Ribet's theorem, we need to define $\rho_{\mathfrak{m}}$ for $\mathfrak{m} \subset \mathbb{T} = \mathbb{T}_N$ a maximal ideal.

Theorem

Let $\mathfrak{m} \subset \mathbb{T}$ be a maximal ideal. Then there is a unique semisimple representation $\rho_{\mathfrak{m}} : G_{\mathbb{Q}} \to GL_2(\mathbb{T}/\mathfrak{m})$ unramified away from $\mathfrak{m}N$ such that

$$tr(\rho_{\mathfrak{m}}(Frob_p)) = T_p \bmod \mathfrak{m}, \; \textit{and} \; \det(\rho_{\mathfrak{m}}(Frob_p)) = p \bmod \mathfrak{m}$$

for all primes p away from $\mathfrak{m}N$.

Sketch of the proof

- Let $k = \mathbb{T}/\mathfrak{m}$, and $\mathcal{L}$ be the space of weight 2 cuspforms whose q-expansions at the usual cusp at ∞ lie in $\mathbb{Z}[[q]]$.

Sketch of the proof

- Let $k = \mathbb{T}/\mathfrak{m}$, and $\mathcal{L}$ be the space of weight 2 cuspforms whose q-expansions at the usual cusp at ∞ lie in $\mathbb{Z}[[q]]$.
- The map $(\mathcal{L} \otimes k) \times (\mathbb{T} \otimes k) \to k$ by $(f, T) \mapsto$(the coefficient of q in $f|T$) induces a map $\mathcal{L} \otimes k \to \hom_{\mathbb{Z}}(\mathbb{T}, k)$.

Sketch of the proof

- Let $k = \mathbb{T}/\mathfrak{m}$, and $\mathcal{L}$ be the space of weight 2 cuspforms whose q-expansions at the usual cusp at ∞ lie in $\mathbb{Z}[[q]]$.
- The map $(\mathcal{L} \otimes k) \times (\mathbb{T} \otimes k) \to k$ by $(f, T) \mapsto$(the coefficient of q in $f|T$) induces a map $\mathcal{L} \otimes k \to \hom_{\mathbb{Z}}(\mathbb{T}, k)$.
- By a dimension argument, one can show this map is an isomorphism. Taking the canonical element on the right $\mathbb{T} \to \mathbb{T}/\mathfrak{m}$, we get $f \in \mathcal{L} \otimes k$ whose q-coefficients are $t_n = T_n \bmod \mathfrak{m}$.

Sketch of the proof

- Let $k = \mathbb{T}/\mathfrak{m}$, and $\mathcal{L}$ be the space of weight 2 cuspforms whose q-expansions at the usual cusp at ∞ lie in $\mathbb{Z}[[q]]$.
- The map $(\mathcal{L} \otimes k) \times (\mathbb{T} \otimes k) \to k$ by $(f, T) \mapsto$(the coefficient of q in $f|T$) induces a map $\mathcal{L} \otimes k \to \hom_{\mathbb{Z}}(\mathbb{T}, k)$.
- By a dimension argument, one can show this map is an isomorphism. Taking the canonical element on the right $\mathbb{T} \to \mathbb{T}/\mathfrak{m}$, we get $f \in \mathcal{L} \otimes k$ whose q-coefficients are $t_n = T_n \bmod \mathfrak{m}$.
- By carefully lifting f, we can apply Deligne's theorem to the corresponding eigenform to get $\rho_f =: \rho_{\mathfrak{m}}$, which satisfies the desired properties.

Mazur's Level-Lowering Theorem

- Fix M and $p \nmid M$ an odd prime. Let $\mathbb{T} = \mathbb{T}_{Mp}$, and $\mathfrak{m} \subset \mathbb{T}$ a maximal ideal.

Mazur's Level-Lowering Theorem

- Fix M and $p \nmid M$ an odd prime. Let $\mathbb{T} = \mathbb{T}_{Mp}$, and $\mathfrak{m} \subset \mathbb{T}$ a maximal ideal.

Theorem (Mazur)

Suppose $\rho_{\mathfrak{m}}$ is irreducible, $\ell = char(\mathbb{T}/\mathfrak{m})$ is odd, and $\rho_{\mathfrak{m}}$ is finite at p. If also $p \not\equiv 1 \bmod \ell$, then $\rho_{\mathfrak{m}}$ is modular of level M.

Strategy for the Proof of Main Theorem

- Start with $\rho_{\mathfrak{m}}$ of level Mp, $p \nmid M$ with the assumptions in Ribet's theorem. To show it is of level M, we use three steps:

Strategy for the Proof of Main Theorem

- Start with $\rho_{\mathfrak{m}}$ of level Mp, $p \nmid M$ with the assumptions in Ribet's theorem. To show it is of level M, we use three steps:
    1. **Raise the level** from Mp to Mpq for a convenient choice of odd prime $q \nmid Mp$.

Strategy for the Proof of Main Theorem

- Start with $\rho_{\mathfrak{m}}$ of level Mp, $p \nmid M$ with the assumptions in Ribet's theorem. To show it is of level M, we use three steps:
  1. **Raise the level** from Mp to Mpq for a convenient choice of odd prime $q \nmid Mp$.
  2. **Lower the level** using Ribet's main work to go from Mpq to Mq.

Strategy for the Proof of Main Theorem

- Start with $\rho_{\mathfrak{m}}$ of level Mp, $p \nmid M$ with the assumptions in Ribet's theorem. To show it is of level M, we use three steps:
  1. **Raise the level** from Mp to Mpq for a convenient choice of odd prime $q \nmid Mp$.
  2. **Lower the level** using Ribet's main work to go from Mpq to Mq.
  3. **Use Mazur's theorem** to get rid of q in the level to get level M.

Strategy for the Proof of Main Theorem

- Start with $\rho_{\mathfrak{m}}$ of level Mp, $p \nmid M$ with the assumptions in Ribet's theorem. To show it is of level M, we use three steps:
  1. **Raise the level** from Mp to Mpq for a convenient choice of odd prime $q \nmid Mp$.
  2. **Lower the level** using Ribet's main work to go from Mpq to Mq.
  3. **Use Mazur's theorem** to get rid of q in the level to get level M.
- As a diagram:

$$Mp \xrightarrow{\text{Raise Level}} Mpq \xrightarrow{\text{Ribet}} Mq \xrightarrow{\text{Mazur}} M$$

Ribet's Arrow

So what we need to show now is

Theorem (Ribet)

Suppose $\ell \nmid qM$ and $\rho_{\mathfrak{m}}$ (of level Mpq) is finite at p. Assume $q \not\equiv 1 \bmod \ell$. Then $\rho_{\mathfrak{m}}$ is modular of level Mq.

Note that by Mazur's theorem, we can assume $p \equiv 1 \bmod \ell$, so in particular, $\ell \nmid Mpq$.

Outline for section 3

Reductions of Curves

- Let C be a curve over a p-adic field K. Let $\mathscr{C}$ be the regular minimal model over $\mathcal{O}_K$. Write $\mathscr{C}_k$ for the special fiber.

Reductions of Curves

- Let C be a curve over a p-adic field K. Let $\mathscr{C}$ be the regular minimal model over $\mathcal{O}_K$. Write $\mathscr{C}_k$ for the special fiber.
- Suppose the gcd of the multiplicity of the irreducible components of $\mathscr{C}_k$ is 1 and all singular points of $\mathscr{C}_k$ are ordinary double points (i.e. look like $xy = 0$ locally).
- (These conditions will be satisfied in our applications.)

Character Groups Associated to Reductions

- The normalization of $\mathscr{C}_k$ is the disjoint union of some nonsingular curves D_j inducing a surjection

$$Pic^0(\mathscr{C}_k) \to \prod_j Pic^0(D_j)$$

whose kernel is a torus T.

Character Groups Associated to Reductions

- The normalization of $\mathscr{C}_k$ is the disjoint union of some nonsingular curves D_j inducing a surjection

$$Pic^0(\mathscr{C}_k) \to \prod_j Pic^0(D_j)$$

whose kernel is a torus T.

- Define $X = X(T)$ to be the character group of T. We call this the character group associated to the reduction of C.

Outline for section 4

From $\rho_{\mathfrak{m}}$ to Shimura Curves

- Let M, p, q, ℓ be as before.

From $\rho_{\mathfrak{m}}$ to Shimura Curves

- Let M, p, q, ℓ be as before.
- Let C be the Shimura curve associated to the norm 1 units in a level M Eichler order in the quaternion algebra over $\mathbb{Q}$ of discriminant pq.

From $\rho_{\mathfrak{m}}$ to Shimura Curves

- Let M, p, q, ℓ be as before.
- Let C be the Shimura curve associated to the norm 1 units in a level M Eichler order in the quaternion algebra over $\mathbb{Q}$ of discriminant pq.
- Set $J = Pic^0(C)$ and let $W = J(\overline{\mathbb{Q}})[\mathfrak{m}]$ be the group of elements of $J(\overline{\mathbb{Q}})$ annihilated by $\mathfrak{m} \subset \mathbb{T}$. In particular, if $\ell = char(\mathbb{T}/\mathfrak{m})$, then $W \subseteq J(\overline{\mathbb{Q}})[\ell]$ as $G_{\mathbb{Q}}$-modules.

From $\rho_{\mathfrak{m}}$ to Shimura Curves

- Let M, p, q, ℓ be as before.
- Let C be the Shimura curve associated to the norm 1 units in a level M Eichler order in the quaternion algebra over $\mathbb{Q}$ of discriminant pq.
- Set $J = Pic^0(C)$ and let $W = J(\overline{\mathbb{Q}})[\mathfrak{m}]$ be the group of elements of $J(\overline{\mathbb{Q}})$ annihilated by $\mathfrak{m} \subset \mathbb{T}$. In particular, if $\ell = char(\mathbb{T}/\mathfrak{m})$, then $W \subseteq J(\overline{\mathbb{Q}})[\ell]$ as $G_{\mathbb{Q}}$-modules.
- If V is the underlying vector space of $\rho_{\mathfrak{m}}$, one can show $V \hookrightarrow W$ as $\mathbb{T}/\mathfrak{m}[G_{\mathbb{Q}}]$-modules.

From $\rho_{\mathfrak{m}}$ to Shimura Curves

- Let M, p, q, ℓ be as before.
- Let C be the Shimura curve associated to the norm 1 units in a level M Eichler order in the quaternion algebra over $\mathbb{Q}$ of discriminant pq.
- Set $J = Pic^0(C)$ and let $W = J(\overline{\mathbb{Q}})[\mathfrak{m}]$ be the group of elements of $J(\overline{\mathbb{Q}})$ annihilated by $\mathfrak{m} \subset \mathbb{T}$. In particular, if $\ell = char(\mathbb{T}/\mathfrak{m})$, then $W \subseteq J(\overline{\mathbb{Q}})[\ell]$ as $G_{\mathbb{Q}}$-modules.
- If V is the underlying vector space of $\rho_{\mathfrak{m}}$, one can show $V \hookrightarrow W$ as $\mathbb{T}/\mathfrak{m}[G_{\mathbb{Q}}]$-modules.
- As V is finite at $p \neq \ell$, V is unramified at p. Hence we can identify it with a subgroup of $J(\overline{\mathbb{F}_p})$.

Character Groups for Modular Curves

- Let X be the character group associated to the reduction of $X_0(Mq)$ mod q, and L the character group associated to the reduction of $X_0(Mpq)$ mod q.

Character Groups for Modular Curves

- Let X be the character group associated to the reduction of $X_0(Mq)$ mod q, and L the character group associated to the reduction of $X_0(Mpq)$ mod q.
- The natural degeneracy maps $X_0(Mpq) \to X_0(Mq)$ yield a map $L \to X \oplus X$, which is surjective. Let Y be the kernel.

From Modular to Shimura Curves

- Let Z be the character group associated to the reduction of the Shimura curve C defined earlier mod p. Let Ψ be the component group of J mod p.

From Modular to Shimura Curves

- Let Z be the character group associated to the reduction of the Shimura curve C defined earlier mod p. Let Ψ be the component group of J mod p.

Theorem

There is a Hecke-equivariant isomorphism $Z \cong Y$.

From Modular to Shimura Curves

- Let Z be the character group associated to the reduction of the Shimura curve C defined earlier mod p. Let Ψ be the component group of J mod p.

Theorem

There is a Hecke-equivariant isomorphism $Z \cong Y$.

- Combining this with some facts about the group X associated to $X_0(Mq)$ mod q, we get

From Modular to Shimura Curves

- Let Z be the character group associated to the reduction of the Shimura curve C defined earlier mod p. Let Ψ be the component group of J mod p.

Theorem

There is a Hecke-equivariant isomorphism $Z \cong Y$.

- Combining this with some facts about the group X associated to $X_0(Mq)$ mod q, we get

Theorem

There is an exact sequence of Hecke modules

$$0 \to K \to (X \oplus X)/\gamma(X \oplus X) \to \Psi \to C \to 0$$

for some groups K and C, and $\gamma = (T_p)^2 - 1 \in \mathbb{T}$.

The Proof in One Case

- If $V \subset J(\overline{\mathbb{F}_p})$ is not zero in Ψ, the component group of the reduction, then $\mathfrak{m}$ is in the support of Ψ.

The Proof in One Case

- If $V \subset J(\overline{\mathbb{F}_p})$ is not zero in Ψ, the component group of the reduction, then $\mathfrak{m}$ is in the support of Ψ.
- By the earlier exact sequence, this implies $\mathfrak{m}$ lies in the support of $X \oplus X$ as a Hecke module.

The Proof in One Case

- If $V \subset J(\overline{\mathbb{F}_p})$ is not zero in Ψ, the component group of the reduction, then $\mathfrak{m}$ is in the support of Ψ.
- By the earlier exact sequence, this implies $\mathfrak{m}$ lies in the support of $X \oplus X$ as a Hecke module.
- But one can show that the action of $\mathbb{T}$ on $X \oplus X$ is through the p-old quotient! Thus there exists a $\lambda \subset \mathbb{T}_{Mq}$ such that $\rho_{\mathfrak{m}} \cong \rho_{\lambda}$, i.e. $\rho_{\mathfrak{m}}$ is of level Mq.

The Proof in One Case

- If $V \subset J(\overline{\mathbb{F}_p})$ is not zero in Ψ, the component group of the reduction, then $\mathfrak{m}$ is in the support of Ψ.
- By the earlier exact sequence, this implies $\mathfrak{m}$ lies in the support of $X \oplus X$ as a Hecke module.
- But one can show that the action of $\mathbb{T}$ on $X \oplus X$ is through the p-old quotient! Thus there exists a $\lambda \subset \mathbb{T}_{Mq}$ such that $\rho_{\mathfrak{m}} \cong \rho_{\lambda}$, i.e. $\rho_{\mathfrak{m}}$ is of level Mq.
- The case when V is zero in Ψ requires a few more facts....

The Second Case

- If V is zero in Ψ, then one shows that it must be contained in $\hom(Z/\mathfrak{m}Z, \mu_\ell)$, so that $\dim Z/\mathfrak{m}Z \geq 2$ (as a $k = \mathbb{T}/\mathfrak{m}$ vector space).

The Second Case

- If V is zero in Ψ, then one shows that it must be contained in $\hom(Z/\mathfrak{m}Z, \mu_\ell)$, so that $\dim Z/\mathfrak{m}Z \geq 2$ (as a $k = \mathbb{T}/\mathfrak{m}$ vector space).
- Using $Z \cong Y$, we get $\dim_k Y/\mathfrak{m}Y \geq 2$.

The Second Case

- If V is zero in Ψ, then one shows that it must be contained in $\hom(Z/\mathfrak{m}Z, \mu_\ell)$, so that $\dim Z/\mathfrak{m}Z \geq 2$ (as a $k = \mathbb{T}/\mathfrak{m}$ vector space).
- Using $Z \cong Y$, we get $\dim_k Y/\mathfrak{m}Y \geq 2$.
- Assume $\mathfrak{m}$ does not belong to the support of $X \oplus X$ (otherwise the previous argument finishes the proof). But then using

$$0 \to Y \to L \to X \to 0$$

we get $Y/\mathfrak{m}Y \cong L/\mathfrak{m}L$, i.e. $\dim_k L/\mathfrak{m}L \geq 2$.

The Second Case

- If V is zero in Ψ, then one shows that it must be contained in $\hom(Z/\mathfrak{m}Z, \mu_\ell)$, so that $\dim Z/\mathfrak{m}Z \geq 2$ (as a $k = \mathbb{T}/\mathfrak{m}$ vector space).
- Using $Z \cong Y$, we get $\dim_k Y/\mathfrak{m}Y \geq 2$.
- Assume $\mathfrak{m}$ does not belong to the support of $X \oplus X$ (otherwise the previous argument finishes the proof). But then using

$$0 \to Y \to L \to X \to 0$$

  we get $Y/\mathfrak{m}Y \cong L/\mathfrak{m}L$, i.e. $\dim_k L/\mathfrak{m}L \geq 2$.
- But one can show that $\dim_k L/\mathfrak{m}L \leq 1$, so we have a contradiction and $\mathfrak{m}$ belongs to the support of $X \oplus X$.

The Second Case

- If V is zero in Ψ, then one shows that it must be contained in $\hom(Z/\mathfrak{m}Z, \mu_\ell)$, so that $\dim Z/\mathfrak{m}Z \geq 2$ (as a $k = \mathbb{T}/\mathfrak{m}$ vector space).
- Using $Z \cong Y$, we get $\dim_k Y/\mathfrak{m}Y \geq 2$.
- Assume $\mathfrak{m}$ does not belong to the support of $X \oplus X$ (otherwise the previous argument finishes the proof). But then using

$$0 \to Y \to L \to X \to 0$$

  we get $Y/\mathfrak{m}Y \cong L/\mathfrak{m}L$, i.e. $\dim_k L/\mathfrak{m}L \geq 2$.
- But one can show that $\dim_k L/\mathfrak{m}L \leq 1$, so we have a contradiction and $\mathfrak{m}$ belongs to the support of $X \oplus X$.
- This finishes the proof of Ribet's theorem used in the step $Mpq \longrightarrow Mq$.