Residual modular Galois representations and their images

Samuele Anni

University of Warwick

University of Warwick, Number Theory Seminar
2nd December 2013

Let us fix a positive integer $n \in \mathbb{Z}_{>0}$.

Definition

The **congruence subgroup** $\Gamma_1(n)$ of $\mathrm{SL}_2(\mathbb{Z})$ is the subgroup given by

$$\Gamma_1(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : n \mid a-1 \,,\; n \mid c \right\}.$$

The integer n is called **level** of the congruence subgroup.

Over the upper half plane:

$$\mathbb{H} = \{z \in \mathbb{C} | \operatorname{Im}(z) > 0\}$$

we can define an action of $\Gamma_1(n)$ via **fractional transformations**:

$$\begin{array}{rcl} \Gamma_1(n) \times \mathbb{H} & \to & \mathbb{H} \\ (\gamma, z) & \mapsto & \gamma(z) = \dfrac{az+b}{cz+d} \end{array}$$

where $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
Moreover, if $n \geq 4$ then $\Gamma_1(n)$ acts freely on $\mathbb{H}$.

Escher, Reducing Lizards Tessellation

Definition

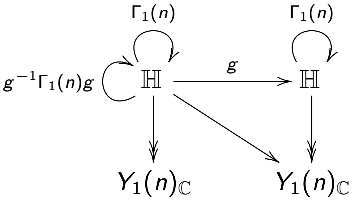
We define the **modular curve** $Y_1(n)_{\mathbb{C}}$ to be the non-compact Riemann surface obtained giving on $\Gamma_1(n)\backslash\mathbb{H}$ the complex structure induced by the quotient map. Let $X_1(n)_{\mathbb{C}}$ be the compactification of $Y_1(n)_{\mathbb{C}}$.

Fact: $Y_1(n)_{\mathbb{C}}$ can be defined algebraically over $\mathbb{Q}$ (in fact over $\mathbb{Z}[1/n]$).

The group $GL_2^+(\mathbb{Q})$ acts on $\mathbb{H}$ via fractional transformation, and its action has a particular behaviour with respect to $\Gamma_1(n)$.

Proposition

For every $g \in GL_2^+(\mathbb{Q})$, the discrete groups $g\Gamma_1(n)g^{-1}$ and $\Gamma_1(n)$ are commensurable



We define operators on $Y_1(n)$ through the correspondences given before:

- the **Hecke operators** T_p for every prime p, using $g = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \in GL_2^+(\mathbb{Q})$;
- the **diamond operators** $\langle d \rangle$ for every $d \in (\mathbb{Z}/n\mathbb{Z})^*$, using $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(n)$, where $\Gamma_0(n)$ is the set of matrices in $\mathrm{SL}_2(\mathbb{Z})$ which are upper triangular modulo n.

For $n \geq 5$ and k positive integers, let ℓ be a prime not dividing n. Following Katz, we define the space of mod ℓ cusp forms as

MOD ℓ CUSP FORMS

$$S(n,k)_{\overline{\mathbb{F}}_\ell} = \mathrm{H}^0(X_1(n)_{\overline{\mathbb{F}}_\ell}, \omega^{\otimes k}(-\,\mathrm{Cusps})).$$

$S(n,k)_{\overline{\mathbb{F}}_\ell}$ is a finite dimensional $\overline{\mathbb{F}}_\ell$-vector space, equipped with Hecke operators T_n $(n \geq 1)$ and diamond operators $\langle d \rangle$ for every $d \in (\mathbb{Z}/n\mathbb{Z})^*$.

Analogous definition in characteristic zero and over any ring where n is invertible.

One may think that mod ℓ modular forms come from reduction of characteristic zero modular forms mod ℓ:

$$S(n,k)_{\mathbb{Z}[1/n]} \to S(n,k)_{\mathbb{F}_\ell}.$$

Unfortunately, this map is **not surjective** for $k=1$.

Even worse: given a character $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ the map

$$S(n,k,\epsilon)_{\mathcal{O}_K} \to S(n,k,\overline{\epsilon})_{\mathbb{F}}$$

is **not** always **surjective** even if $k>1$, where $\mathcal{O}_K$ is the ring of integers of the number field where ϵ is defined, $\mathbb{F}_\ell \subseteq \mathbb{F}$ and
$S(n,k,\epsilon)_{\mathcal{O}_K} = \{f \in S(n,k)_{\mathcal{O}_K} | \forall d \in (\mathbb{Z}/n\mathbb{Z})^*, \langle d\rangle f = \epsilon(d) f\}$.

Definition

The **Hecke algebra** $\mathbb{T}(n,k)$ of $S(n,k)_{\mathbb{C}}$ is the $\mathbb{Z}$-subalgebra of $\mathrm{End}_{\mathbb{C}}(S(\Gamma_1(n),k)_{\mathbb{C}})$ generated by Hecke operators T_p for every prime p and by diamond operators $\langle d \rangle$ for every $d \in (\mathbb{Z}/n\mathbb{Z})^*$.

Fact:

$\mathbb{T}(n,k)$ is finitely generated as $\mathbb{Z}$-module.

Given a character $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$, we associate a Hecke algebra $\mathbb{T}_\epsilon(n,k)$ to each $S(n,k,\epsilon)_{\mathbb{C}}$:

$$S(n,k,\epsilon)_{\mathbb{C}} = \{f \in S(n,k)_{\mathbb{C}} | \forall d \in (\mathbb{Z}/n\mathbb{Z})^*, \langle d \rangle f = \epsilon(d) f\}.$$

Theorem (Deligne, Shimura)

Let n and k be positive integers. Let $\mathbb{F}$ be a finite field of characteristic ℓ, with ℓ not dividing n, and $f : \mathbb{T}(n,k) \twoheadrightarrow \mathbb{F}$ a surjective morphism of rings. Then there is a continuous semi-simple representation:

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

unramified outside $n\ell$, such that for all p not dividing $n\ell$ we have:

$$\mathrm{Trace}(\rho_f(\mathrm{Frob}_p)) = f(T_p) \text{ and } \det(\rho_f(\mathrm{Frob}_p)) = f(\langle p \rangle)p^{k-1} \text{ in } \mathbb{F}.$$

Such a ρ_f is unique up to isomorphism.

Computing ρ_f is "difficult", but theoretically it **can be done in polynomial time** in $n, k, \#\mathbb{F}$:

Edixhoven, Couveignes, de Jong, Merkl, Bruin, Bosman ($\#\mathbb{F} \leq 32$); Mascot, Zeng, Tian ($\#\mathbb{F} \leq 41$).

Question

Can we compute the image of a residual modular Galois representation without computing the representation?

Main ingredients:

Theorem (Dickson)

Let ℓ be an odd prime and H a finite subgroup of $\mathrm{PGL}_2(\overline{\mathbb{F}}_\ell)$. Then a conjugate of H is one of the following groups:

- a finite subgroup of the upper triangular matrices;
- $\mathrm{SL}_2(\mathbb{F}_{\ell^r})/\{\pm 1\}$ or $\mathrm{PGL}_2(\mathbb{F}_{\ell^r})$ for $r \in \mathbb{Z}_{>0}$;
- a dihedral group D_{2n} with $n \in \mathbb{Z}_{>1}$, $(\ell, n) = 1$;
- or it is isomorphic to A_4, S_4 or A_5.

Definition

If $G := \rho_f(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ has order prime to ℓ we call the image **exceptional**.

The field of definition of the representation is the smallest field $\mathbb{F} \subset \overline{\mathbb{F}}_\ell$ over which ρ_f is equivalent to all its conjugate. The image of the representation ρ_f is then a subgroup of $\mathrm{GL}_2(\mathbb{F})$.

Let $\mathbb{P}\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{F})$ be the projective representation associated to the representation ρ_f:

$$\begin{array}{ccc} \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \xrightarrow{\rho_f} & \mathrm{GL}_2(\mathbb{F}) \\ & \searrow^{\mathbb{P}\rho_f} & \downarrow \pi \\ & & \mathrm{PGL}_2(\mathbb{F}). \end{array}$$

The representation $\mathbb{P}\rho_f$ can be defined on a different field than the field of definition of the representation. This field is called the **Dickson's field** for the representation.

Theorem (Khare, Wintenberger, Dieulefait, Kisin), Serre's Conjecture

Let ℓ be a prime number and let $\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be an odd, absolutely irreducible, continuous representation. Then ρ is **modular** of level $N(\rho)$, weight $k(\rho)$ and character $\epsilon(\rho)$.

- $N(\rho)$ (the level) is the Artin conductor away from ℓ.
- $k(\rho)$ (the weight) is given by a recipe in terms of $\rho|_{I_\ell}$.
- $\epsilon(\rho)\colon (\mathbb{Z}/N(\rho)\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ is given by:

$$\det \circ \rho = \epsilon(\rho)\chi^{k(\rho)-1}.$$

Algorithm

Input:

- n positive integer;
- ℓ prime such that $(n, \ell) = 1$;
- k positive integer such that $2 \leq k \leq \ell + 1$;
- a character $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$;
- a morphism of ring $f\colon \mathbb{T}_\epsilon(n, k) \to \overline{\mathbb{F}}_\ell$;

Output:

Image of the associated Galois representation ρ_f, up to conjugacy as subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$.

Problems

- ρ_f can arise from lower level or weight, i.e. there exists $g \in S(m,j)_{\overline{\mathbb{F}}_\ell}$ with $m \leq n$ or $j \leq k$ such that $\rho_g \cong \rho_f$
- ρ_f can arise as twist of a representation of lower conductor, i.e. there exist $g \in S(m,j)_{\overline{\mathbb{F}}_\ell}$ with $m \leq n$ or $j \leq k$ and a Dirichlet character χ such that $\rho_g \otimes \chi \cong \rho_f$

Algorithm

- **Step 1** Iteration "down to top", i.e. considering all divisors of n: creation of a database
- **Step 2** Determine minimality with respect to level and with respect to weight.
- **Step 4** Determine minimality up to twisting.

Algorithm

- **Step 1** Iteration "down to top"
- **Step 2** Determine minimality with respect to level and weight.
- **Step 3** Determine whether reducible or irreducible.
- **Step 4** Determine minimality up to twisting.
- **Step 5** Compute the projective image
- **Step 6** Compute the image

Remarks

- Check equality between the system of eigenvalues and the systems coming from specific Eisenstein series.
- The projective image is determined by excluding cases. Each exceptional case is related to a particular equality of mod ℓ modular forms or a particular construction.
- Compute the field of definition of the projective representation, i.e. the Dickson's field: obtained using twists.
- Compute the field of definition of the representation: obtained using coefficients up to a finite explicit bound.

In this talk:

Algorithm

- **Step 1** Iteration “down to top”
- **Step 2** Determine minimality with respect to level and weight
- **Step 3** Determine whether reducible or irreducible
- **Step 4** Determine minimality up to twisting
- **Step 5** Compute the projective image
- **Step 6** Compute the image

How many T_p are needed?

One of the most important features of this algorithm is that, in almost all cases, we have a linear bound in n and k: Sturm Bound for $\Gamma_0(n)$ and weight k:

$$\frac{k}{12} \cdot n \cdot \prod_{p|n \text{ prime}} \left(1 + \frac{1}{p}\right) \ll \frac{k}{12} \cdot n \log \log n$$

while the bound known to compare two semi-simple Galois representation is of the order $\ll \ell^5 n^3$.

Setting $(*)$

- n and k be positive integers;
- ℓ be a prime number not dividing n, such that $2 \leq k \leq \ell + 1$;
- $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character;
- $f : \mathbb{T}_\epsilon(n,k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings;
- $\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the unique, up to isomorphism, continuous semi-simple representation attached to f;
- $\overline{\epsilon} : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be the character defined by $\overline{\epsilon}(a) = f(\langle a \rangle)$ for all $a \in (\mathbb{Z}/n\mathbb{Z})^*$.

Let p be a prime dividing $n\ell$. Let us denote by

- $G_p = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \subset G_\mathbb{Q}$ the decomposition subgroup at p;
- I_p the inertia subgroup, I_t the tame inertia subgroup;
- $G_{i,p}$, with $i \in \mathbb{Z}_{>0}$, the higher ramification subgroups ($I_p = G_{0,p}$).

Lemma (Livné)

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be an odd, continuous representation of conductor $\mathrm{N}(\rho)$, and let k be a positive integer. If $f \in S(n,k)_{\overline{\mathbb{F}}_\ell}$ is an eigenform such that $\rho_f \cong \rho$, then $\mathrm{N}(\rho)$ divides n.

Given a modular, odd, continuous 2-dimensional Galois representation ρ of conductor $\mathrm{N}(\rho)$, there are **infinitely many** mod ℓ modular forms of level multiple of the conductor such that the associated 2-dimensional Galois representation are equivalent to ρ.

If the representation ρ is **irreducible**, then, by Khare-Wintenberger Theorem there exists a modular form of level $\mathrm{N}(\rho)$ and weight $k(\rho)$ such that the associated representation is equivalent to ρ.

If we restrict to mod ℓ modular forms with weight between 2 and $\ell+1$ then, given a modular, odd, continuous 2-dimensional Galois representation ρ, there exist **at most two** mod ℓ modular forms of level $\mathrm{N}(\rho)$ and weight between 2 and $\ell+1$ with associated 2-dimensional Galois representation equivalent to ρ.

Two different mod ℓ modular forms can give rise to the same Galois representation: the coefficients indexed by the primes dividing the level and the characteristic may differ. Hence,

- either we solve this problem mapping the forms to a higher level (or twisting it) but this is computationally expensive,
- or we study how to describe the coefficients at primes dividing the level and the characteristic so that we can list all possibilities.

Notation: given a residual representation ρ, we will denote as $\mathrm{N}_p(\rho)$ the valuation at p of the Artin conductor of ρ.

Theorem

Assume setting $(*)$. Let p be a prime dividing n. The following holds:

(A) *if $\mathrm{N}_p(\rho_f) = 0$, let $\overline{\alpha}$ and $\overline{\beta}$ be the eigenvalues of $\rho_f(\mathrm{Frob}_p)$, then*
- *if $\mathrm{N}_p(n) = 1$ then $f(T_p) \in \{\overline{\alpha}, \overline{\beta}\}$;*
- *if $\mathrm{N}_p(n) > 1$ then $f(T_p) \in \{0, \overline{\alpha}, \overline{\beta}\}$.*

(B) *if $\mathrm{N}_p(\rho_f) > 0$ and $f(T_p) \neq 0$, then there exists a unique unramified quotient line for the representation and $f(T_p)$ is the eigenvalue of Frob_p on it.*

Moreover, if $f(T_\ell) \neq 0$ then then $f(T_\ell) = \mu$, where μ is the scalar representing the action of Frob_ℓ on an unramified quotient line for the representation, meanwhile if $f(T_\ell) = 0$ there exist no such line.

Let $f : \mathbb{T}(n, k) \to \overline{\mathbb{F}}_\ell$ and $g : \mathbb{T}(m, k) \to \overline{\mathbb{F}}_\ell$ be two Katz modular forms such that $m = \mathrm{N}(\rho_g)$, the integer n is a multiple of m not divisible by ℓ and $2 \leq k \leq \ell + 1$.

Definition

The **old-space** given by g at level n is the subspace of $M(n, k)_{\overline{\mathbb{F}}_\ell}$ given by g through the degeneracy maps from level m to level n.

Theorem

If ρ_f is ramified at ℓ then $\rho_f \cong \rho_g$ if and only if f is in the subspace of the old-space given by g at level n.

A similar statement holds in the unramified case.

Associated to the algorithm there is a database which stores all the data obtained.

The algorithm is cumulative and built with a **bottom-up** approach: for any new level n, we will store in the database the system of eigenvalues at levels dividing n and weights smaller than the weight considered, so that there will be no need to re-do the computations if the representation arises from lower level (or weight).

Local representation at ℓ

Theorem (Deligne)

Assume setting $(*)$. Suppose that $f(T_\ell) \neq 0$. Then $\rho_f|_{G_\ell}$ is reducible, and up to conjugation in $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, we have

$$\rho_f|_{G_\ell} \cong \begin{pmatrix} \chi_\ell^{k-1}\lambda(\overline{\epsilon}(\ell)/f(T_\ell)) & * \\ 0 & \lambda(f(T_\ell)) \end{pmatrix}$$

where $\lambda(a)$ is the unramified character of G_ℓ taking $\mathrm{Frob}_\ell \in G_\ell/I_\ell$ to a, for any $a \in \overline{\mathbb{F}}_\ell^*$.

Theorem (Fontaine)

Assume setting (∗). Suppose that $f(T_\ell) = 0$. Then $\rho_f|_{G_\ell}$ is irreducible, and up to conjugation in $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, we have

$$\rho_f|_{I_\ell} \cong \begin{pmatrix} \varphi'^{k-1} & 0 \\ 0 & \varphi^{k-1} \end{pmatrix}$$

where $\varphi', \varphi\colon I_t \to \overline{\mathbb{F}}_\ell^*$ are the two fundamental characters of level 2.

Local representation at primes dividing the level

Theorem (Gross-Vignéras, Serre: Conjecture 3.2.6?)

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}(V)$ be a continuous, odd, irreducible representation of the absolute Galois group over $\mathbb{Q}$ to a 2-dimensional $\overline{\mathbb{F}}_\ell$-vector space V. Let $n = \mathrm{N}(\rho)$ and $k = k(\rho)$, let $f \in S(n,k)_{\overline{\mathbb{F}}_\ell}$ be an eigenform such that $\rho_f \cong \rho$. Let p be a prime divisor of ℓn.

(1) *If $f(T_p) \neq 0$, then there exists a stable line $D \subset V$ for the action of G_p, the decomposition subgroup at p, such that the inertia group at p acts trivially on V/D. Moreover, $f(T_p)$ is equal to the eigenvalue of Frob_p which acts on V/D.*

(2) *If $f(T_p) = 0$, then there exists no stable line $D \subset V$ as in (1).*

Proposition

Assume setting $(*)$ and that ρ_f is irreducible and it does not arise from lower level. Let p be a prime dividing n such that $f(T_p) \neq 0$.
Then $\rho_f|_{G_p}$ is decomposable if and only if $\rho_f|_{I_p}$ is decomposable.

This proposition is proved using representation theory.

Proposition

Assume setting $(*)$ and that ρ_f is irreducible and it does not arise from lower level. Let p be a prime dividing n, such that $f(T_p) \neq 0$. Then:

(A) $\rho_f|_{I_p}$ *is decomposable if and only if* $\mathrm{N}_p(\rho_f) = \mathrm{N}_p(\overline{\epsilon})$;

(B) $\rho_f|_{I_p}$ *is indecomposable if and only if* $\mathrm{N}_p(\rho_f) = 1 + \mathrm{N}_p(\overline{\epsilon})$.

Proof I

The valuation of $\mathrm{N}(\rho_f)$ at p is given by:

$$\mathrm{N}_p(\rho_f) = \sum_{i \geq 0} \frac{1}{[G_{0,p} : G_{i,p}]} \dim(V/V^{G_{i,p}}) = \dim(V/V^{I_p}) + b(V),$$

where V is the two-dimensional $\overline{\mathbb{F}}_\ell$-vector space underlying the representation, $V^{G_{i,p}}$ is its subspace of invariants under $G_{i,p}$, and $b(V)$ is the wild part of the conductor.
Since $f(T_p) \neq 0$, the representation restricted to the decomposition group at p is reducible. Hence, after conjugation,

$$\rho_f|_{G_p} \cong \begin{pmatrix} \epsilon_1 \chi_\ell^{k-1} & * \\ 0 & \epsilon_2 \end{pmatrix}, \ \ \rho_f|_{I_p} \cong \begin{pmatrix} \epsilon_1|_{I_p} & * \\ 0 & 1 \end{pmatrix},$$

where ϵ_1 and ϵ_2 are characters of G_p with ϵ_2 unramified, χ_ℓ is the mod ℓ cyclotomic character and $*$ belongs to $\overline{\mathbb{F}}_\ell$.

Proof II

$$\rho_f|_{I_p} \cong \begin{pmatrix} \epsilon_1|_{I_p} & * \\ 0 & 1 \end{pmatrix}.$$

If $\rho_f|_{I_p}$ is indecomposable then V^{I_p} is either $\{0\}$ if ϵ_1 is ramified, or $\overline{\mathbb{F}}_\ell \cdot \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ if ϵ_1 is unramified. The wild part of the conductor is equal to the wild part of the conductor of ϵ_1. Hence, we have that

$$\mathrm{N}_p(\rho_f) = \begin{cases} 1 = 1 + \mathrm{N}_p(\epsilon_1) & \text{if } \epsilon_1 \text{ is unramified,} \\ 2 + b(\epsilon_1) = 1 + \mathrm{N}_p(\epsilon_1) & \text{if } \epsilon_1 \text{ is ramified.} \end{cases}$$

The determinant of the representation is given by $\det(\rho_f) = \overline{\epsilon}\chi_\ell^{k-1}$, then $\det(\rho_f)|_{I_p} = \overline{\epsilon}|_{I_p}$. This implies that $\epsilon_1|_{I_p} = \overline{\epsilon}|_{I_p}$. Therefore, we have that if $\rho_f|_{I_p}$ is indecomposable $\mathrm{N}_p(\rho_f) = 1 + \mathrm{N}_p(\overline{\epsilon})$.

The other case is analogous.

Remark

If $\rho_f|_{I_p}$ is indecomposable then the image of inertia at p is of order divisible by ℓ and so the image cannot be exceptional.

Let n be a positive integer. Any Dirichlet character of conductor n can be decomposed into local characters, one for each prime divisor of n.

With no loss of generality, we reduce ourselves to study twists of modular Galois representations with Dirichlet characters with prime power conductor.

Question

What is the conductor of the twist?

Shimura gave an upper bound: $\mathrm{lcm}(\mathrm{cond}(\chi)^2, n)$, where n is the level of the form and χ is the character used for twisting.

Proposition

Assume setting $(*)$*. Let* p *be a prime not dividing* $n\ell$*. Let* $\chi : (\mathbb{Z}/p^i\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$*, for* $i > 0$*, be a non-trivial character. Then*

$$\mathrm{N}_p(\rho_f \otimes \chi) = 2\mathrm{N}_p(\chi).$$

Proposition

Assume setting $(*)$ *and that* ρ_f *is irreducible and it does not arise from lower level. Let* p *be a prime dividing* n *and suppose that* $f(T_p) \neq 0$*. Let* $\chi : (\mathbb{Z}/p^i\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$*, for* $i > 0$*, be a non-trivial character. Then*

$$\mathrm{N}_p(\rho_f \otimes \chi) = \mathrm{N}_p(\chi\overline{\epsilon}) + \mathrm{N}_p(\chi).$$

It is also possible to know what is the system of eigenvalues associated to the twist:

Proposition

Assume setting $(*)$. Suppose that ρ_f is irreducible and that $\mathrm{N}(\rho_f) = n$. Let p be a prime dividing n and suppose that $f(T_p) \neq 0$. Let χ from $(\mathbb{Z}/p^i\mathbb{Z})^*$ to $\overline{\mathbb{F}}_\ell^*$, with $i > 0$, be a non-trivial character. Then

(A) *if $\rho_f|_{I_p}$ is decomposable then the representation $\rho_f \otimes \chi$ restricted to G_p, the decomposition group at p, admits a stable line with unramified quotient if and only if $\mathrm{N}_p(\rho_f \otimes \chi) = \mathrm{N}_p(\rho_f)$;*

(B) *if $\rho_f|_{I_p}$ is indecomposable then the representation $\rho_f \otimes \chi$ restricted to G_p does not admit any stable line with unramified quotient.*

Proposition

Assume setting $(*)$*. Suppose that* ρ_f *is irreducible and that* $\mathrm{N}(\rho_f) = n$*. Let* p *be a prime dividing* n *and suppose that* $f(T_p) = 0$*. Then:*

(A) *if* $\rho_f|_{G_p}$ *is reducible then there exists a mod* ℓ *modular form* g *of weight* k *and level at most* np *and a non-trivial character* $\chi : (\mathbb{Z}/p^i\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ *with* $i > 0$ *such that* $g(T_p) \neq 0$ *and* $\rho_g \cong \rho_f \otimes \chi$*;*

(B) *if* $\rho_f|_{G_p}$ *is irreducible then for any non-trivial character* $\chi : (\mathbb{Z}/p^i\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ *with* $i > 0$ *the representation* $\rho_f \otimes \chi$ *restricted to* G_p *does not admit any stable line with unramified quotient.*

The previous propositions motivate the following definition:

Definition

Let n and k be two positive integers, let ℓ be a prime such that $(n, \ell) = 1$ and $2 \leq k \leq \ell + 1$, and let $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character. Let $f : \mathbb{T}_\epsilon(n, k) \to \overline{\mathbb{F}}_\ell$ be a morphism of rings and let $\rho_f : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be the representation attached to f. We say that f is **minimal up to twisting** if for any Dirichlet character $\chi : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$, and for any prime p dividing n

$$\mathrm{N}_p(\rho_f) \leq \mathrm{N}_p(\rho_f \otimes \chi).$$

If f is minimal up to twisting then ρ_f is not isomorphic to a twist of a representation of lower conductor.

Example: projective image S_4 in characteristic 3.

Ideas:

- a modular representation which has S_4 as projective image in characteristic 3 has "big" projective image i.e. $\mathrm{PGL}_2(\mathbb{F}_3) \cong S_4$;
- from mod 3 modular forms with projective image S_4, we want to construct characteristic 0 forms;
- use these forms to decide about projective image S_4 in characteristic larger than 3.

Input:

- n positive integer, $(n, 3) = 1$;
- $k \in \{2, 3, 4\}$;
- a character $\epsilon \colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$;
- a morphism of rings $f \colon \mathbb{T}(n, k, \epsilon) \to \overline{\mathbb{F}}_3$.

Suppose the algorithm has certified that ρ_f is absolutely irreducible and that $\mathbb{P}\rho_f \cong S_4$. Suppose also that f is minimal with respect to weight, level and twisting. What else do we know?

- Field of definition of the representation: $\mathbb{F}$;
- Field of definition of the projective representation: $\mathbb{F}_3$;
- Data on the local components;
- Image of the representation: $\rho_f(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \subseteq \mathbb{F}^* \cdot \mathrm{GL}_2(\mathbb{F}_3)$.

Let $\beta : \mathbb{F}^* \cdot \mathrm{GL}_2(\mathbb{F}_3) \to \mathrm{GL}_2(\mathcal{O}_K)$ be a 2-dimensional representation, where $\mathcal{O}_K$ is the ring of integers of a number field.

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho_f} \mathbb{F}^*\,\mathrm{GL}_2(\mathbb{F}_3) \xrightarrow{\beta} \mathrm{GL}_2(\mathcal{O}_K), \qquad \rho_{f_\beta}: \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathcal{O}_K)$$

There exists f_β of weight 1 such that $\rho_{f_\beta} \cong \beta \circ \rho_f$.

Can we determine the level of f_β?

Yes, studying the local representation at primes dividing n and at 3.

Can we determine $f_\beta(T_p)$, $f_\beta(\langle p \rangle)$ for all p?

Yes for the primes dividing the level and 3

No for the unramified primes! Problem: distinguish elements in $\mathrm{GL}_2(\mathbb{F}_3)$ using only traces and determinants is not possible.

Solution:

check in characteristic 2 and 5.

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho_f} \mathbb{F}^* \, \mathrm{GL}_2(\mathbb{F}_3) \xrightarrow{\beta} \mathrm{GL}_2(\mathcal{O}_K) \xrightarrow{\pi} \mathrm{GL}_2(\overline{\mathbb{F}}_2)$$

$$\rho_{f_\beta} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathcal{O}_K), \qquad \rho_{f_{\pi\beta}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$$

$$\rho_{f_{\pi\beta}}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \subseteq \mathbb{F}'^* \times \mathrm{GL}_2(\mathbb{F}_2)$$

$$\mathbb{P}\rho_{f_{\pi\beta}}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \cong S_3$$

There exists a mod 2 modular form $f_{\pi\beta}$ such that $\rho_{f_{\pi\beta}} \cong \pi \circ \beta \circ \rho_f$.

Can we determine the level of $f_{\pi\beta}$?

Yes, we can bound it.

Can we determine $f_\beta(T_p)$, $f_\beta(\langle p \rangle)$ using $f_{\pi\beta}(T_p)$, $f_{\pi\beta}(\langle p \rangle)$ for all p?

Yes for the primes dividing the level and 3.

For the unramified primes there is still a problem but we have candidates i.e. a finite list of mod 2 modular forms with prescribed properties.

How can we solve this problem?

For each candidate we have a power series in characteristic 0. All power series are defined over the same ring of integers so we can reduce them modulo 5 and check if the list we obtain does occur as eigenvalue system or not. Claim: only one power series is a modular form. If this method does not work use Schaeffer's Algorithm.

Residual modular Galois representations and their images

Samuele Anni

University of Warwick

University of Warwick, Number Theory Seminar
2nd December 2013

Thanks!