Images of residual modular Galois representations

Samuele Anni

Heeze, 27th may 2011

Reducing Lizards upper half plane tessellation by M.C. Escher.

Universiteit Leiden

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*

$$\Gamma_1(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a \equiv d \equiv 1 \,,\, c \equiv 0 \bmod n \right\}.$$

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

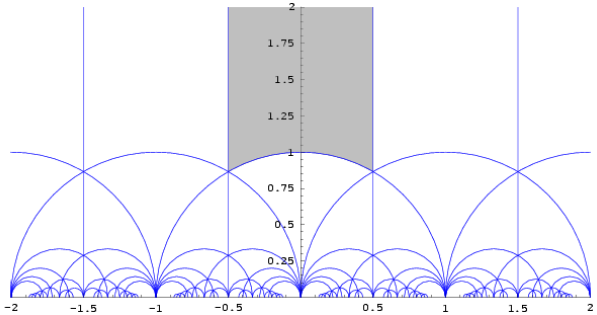
Let us consider the upper half plane:

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

we can define an action of $\Gamma_1(n)$ on $\mathbb{H}$ 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 $\Gamma_1(n)$ acts freely on $\mathbb{H}$ if $n \geq 4$.



Fundamental domain for $\Gamma_1(n)$, Verrill webpage.

Definition

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

Let G be a group. The collection of all G-**modules**, i.e. all abelian group M equipped with a group action of G on M, is a category.

Sending each module M to the group of invariants M^G respect to the action of G yields a **functor** from this category to the category of abelian groups.

This functor is left exact, so we can form its **right derived functors**; their values are abelian groups and they are denoted by $H^n(G, M)$, i.e. the n-th **cohomology group** of G with coefficients in M. $H^0(G, M)$ is identified with M^G.

Fix a prime ℓ such that $(\ell, n) = 1$, and fix $k \in \mathbb{Z}$, $k \geq 2$.

Let $\mathbb{F}_\ell$ be the finite field $\mathbb{Z}/\ell\mathbb{Z}$.

We can consider the **first cohomology group** of $\Gamma_1(n)$ with coefficients in $\mathbb{F}_\ell [x, y]_{k-2}$

$$\boxed{W_{n,k} := H^1(\Gamma_1(n), \mathbb{F}_\ell [x, y]_{k-2}).}$$

$\mathbb{F}_\ell[x,y]_{k-2}$ is a $\Gamma_1(n)$- module, in fact:

- $\Gamma_1(n)$ acts on $\mathbb{F}_\ell^2$: given $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$$\begin{array}{rcl} \Gamma_1(n) \times \mathbb{F}_\ell^2 & \to & \mathbb{F}_\ell^2 \\ (\gamma, \begin{pmatrix} m \\ n \end{pmatrix}) & \mapsto & \gamma(\begin{pmatrix} m \\ n \end{pmatrix}) = \begin{pmatrix} am+bn \\ cm+dn \end{pmatrix} \end{array}$$

- $\mathbb{F}_\ell^2 \xrightarrow{\sim} \mathbb{F}_\ell x \oplus \mathbb{F}_\ell y \hookrightarrow \mathbb{F}_\ell[x,y]$;

- $Sym^{k-2}(\mathbb{F}_\ell) \xrightarrow{\sim} \mathbb{F}_\ell[x,y]_{k-2}$ the vector space of homogeneous polynomials of degree $k-2$ in 2 variables.

Since $\Gamma_1(n)$ has a finite presentation, then it is possible to prove that $W_{n,k}$ is a **finite** dimensional $\mathbb{F}_\ell$-vector space.

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

Proposition

$\forall g \in GL_2^+(\mathbb{Q})$ the discrete groups $g\Gamma_1(n)g^{-1}$ and $\Gamma_1(n)$ are commensurable, i.e. $g\Gamma_1(n)g^{-1} \cap \Gamma_1(n)$ is a subgroup of finite index in $g\Gamma_1(n)g^{-1}$ and $\Gamma_1(n)$.

We can define operators on $W_{n,k}$ considering the action of $GL_2^+(\mathbb{Q})$ on $\mathbb{H}$ thanks to the previous proposition, in particular we have:

- the **Hecke operators** T_p for every prime p:

$$\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \leftrightarrow T_p \quad p \text{ prime.}$$

- the **diamond operators** $\langle d \rangle$ for every $d \in (\mathbb{Z}/n\mathbb{Z})^*$:

$$\begin{pmatrix} d & 0 \\ 0 & d \end{pmatrix} \leftrightarrow \langle d \rangle \text{ for every } d \in (\mathbb{Z}/n\mathbb{Z})^*$$

Definition

The Hecke algebra $\mathbb{T}$ is the $\mathbb{F}_\ell$-subalgebra of $\mathrm{End}_{\mathbb{F}_\ell}(W_{n,k})$ generated by the Hecke operators and the diamond operators.

Essentially $W_{n,k}$ is free of rank 2 as $\mathbb{T}$-module.

$$\begin{pmatrix} \Gamma_1(n) \circlearrowright \mathbb{H} \\ \text{constant sheaf } \underline{\mathbb{F}_\ell[x,y]_{k-2}} \\ H^1(\Gamma_1(n), \mathbb{F}_\ell[x,y]_{k-2}) \end{pmatrix} \longrightarrow \begin{pmatrix} Y_1(n)_{\mathbb{C}} \\ \text{sheaf } \mathcal{F} \\ H^1_{\text{étale}}(Y_1(n), \mathcal{F}) \end{pmatrix}$$

Fact: the second column in this slide can be defined algebraically over $\mathbb{Q}$.

Equation for a model of $Y_1(23)_{\mathbb{C}}$:

$$x^8y^4 + 4x^7y^4 + 2x^7y^3 - 4x^7y^2 + x^7y + x^6y^5 + 10x^6y^4 +$$
$$-2x^6y^3 - 12x^6y^2 + 7x^6y - x^6 + 5x^5y^5 + 14x^5y^4 - 26x^5y^3$$
$$+3x^5y^2 + 7x^5y - 2x^5 + 13x^4y^5 - 6x^4y^4 - 26x^4y^3 +$$
$$23x^4y^2 - 3x^4y - x^4 + 2x^3y^6 + 12x^3y^5 - 31x^3y^4 +$$
$$15x^3y^3 + 6x^3y^2 - 4x^3y + 5x^2y^6 - 6x^2y^5 - 9x^2y^4 +$$
$$16x^2y^3 - 6x^2y^2 + 4xy^6 - 12xy^5 + 12xy^4 - 4xy^3 + y^7 +$$
$$-3y^6 + 3y^5 - y^4$$

Since $Y_1(n)_{\mathbb{C}}$ can be defined algebraically over $\mathbb{Q}$, we have an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the étale cohomology, and this induces a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action on $W_{n,k}$. Shimura and Deligne showed that this action is characterized by:

- it is unramified outside ℓn;
- $\forall p \nmid \ell n$ we have $\mathrm{Tr}(\mathrm{Frob}_p, W_{n,k}) = T_p$.

Theorem (Shimura, Deligne)

Let n and k be positive integers. Let $\mathbb{F}$ be a finite field of characteristic ℓ, $\ell \nmid n$, and $f : \mathbb{T} \twoheadrightarrow \mathbb{F}$ a surjective morphism of rings. Then there is a continuous semi-simple representation: $\rho_f : \mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathsf{GL}_2(\mathbb{F})$ that is unramified outside $n\ell$ such that for all p not dividing $n\ell$ we have, in $\mathbb{F}$:

$$\mathsf{Tr}(\rho_f(\mathsf{Frob}_p)) = f(T_p) \text{ and } \det(\rho_f(\mathsf{Frob}_p)) = f(\langle p \rangle)p^{k-1}.$$

Such a ρ_f is unique up to isomorphism.

For p prime, we let $\mathbb{Q}_p$ denote the topological field of p-adic numbers, and $\overline{\mathbb{Q}_p}$ an algebraic closure.

$$\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \hookrightarrow \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$$

$$0 \to I_p \to \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \to \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$$

Definition

The Frobenius element $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *is the class corresponding to the automorphism of* $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ *that sends* x *to* x^p.

Definition

If the action of the inertia group I_p *is trivial, we say that the representation is unramified at* p.

Computing ρ_f is "difficult", but theoretically it can be done in time polynomial in $n, k, \#\mathbb{F}$, where $\mathbb{F}$ is a finite field of characteristic $\ell, (n, \ell) = 1$.

Reference:

Bas Edixhoven, Jean-Marc Couveignes, Robin de Jong, Franz Merkl, Johan Bosman, *Computational aspects of modular forms and Galois representations*, to appear in the series "Annals of Mathematics Studies" of Princeton University Press.

Johan Bosman produced examples for $\#\mathbb{F} \leq 32$. For the couple $(k, \ell) = (22, 23)$ he got the following polynomial corresponding to the projective representation given by ρ_f:

$$
\begin{aligned}
& x^{24} - 2x^{23} + 115x^{22} + 23x^{21} + 1909x^{20} + 22218x^{19} \\
& +9223x^{18} + 121141x^{17} + 1837654x^{16} - 800032x^{15} \\
& +9856374x^{14} + 52362168x^{13} - 32040725x^{12} \\
& +279370098x^{11} + 1464085056x^{10} + 1129229689x^{9} \\
& +3299556862x^{8} + 14586202192x^{7} + 29414918270x^{6} \\
& +45332850431x^{5} - 6437110763x^{4} - 111429920358x^{3} \\
& -12449542097x^{2} + 93960798341x - 31890957224
\end{aligned}
$$

The Galois group is $\mathbb{P}\,\mathrm{GL}_2(\mathbb{F}_{23})$.

The computation of the Image of a Residual modular Galois representations is a totally different matter than the computation of the representation itself.

In this case, there is no need to know explicitly the representation.

In fact using

- group theory;
- geometry of modular curves;
- number theory: computation of ramification in number fields, characters tables...

it is possible to obtain the image of such representations.

Dickson Theorem

Let ℓ be a prime and H a finite subgroup of $\mathbb{P}\,\mathsf{GL}_2(\overline{\mathbb{F}}_\ell)$. Then a conjugate of H is one of the following groups:

- *finite subgroups of the upper triangular matrices;*
- *$\mathbb{P}\,\mathsf{SL}_2(\mathbb{F}_{\ell^r})$ or $\mathbb{P}\,\mathsf{GL}_2(\mathbb{F}_{\ell^r})$ for $r \in \mathbb{Z}_{>0}$;*
- *dihedral groups;*
- *or it is isomorphic to A_4, S_4 or A_5.*

Example:
Let us consider $\Gamma_1(73)$, $k = 2$, and the associated Hecke algebra $\mathbb{T}$.
There exists a maximal ideal $\mathfrak{m}$ of $\mathbb{T}$ such that the quotient map gives:
$f : \mathbb{T} \to \mathbb{T}/\mathfrak{m} \cong \mathbb{F}_9$.
We can compute explicitly f for some T_p:

T_p	$P(x)$	p
$2i$	$x^2 - 2ix + 2$	$11, 29, 47, 53, 101, 113$
i	$x^2 - ix + 2$	$2, 5, 23, 41, 59, 71, 89, 107, 131$
0	$x^2 + 1$	$7, 97, 139$
2	$x^2 - 2x + 1$	$13, 43, 61, 67, 109$
0	$x^2 + 2$	$17, 83, 103, 137$
1	$x^2 - x + 1$	$19, 31, 37, 79, 127$

where $P(x)$ is the polynomial $x^2 - f(T_p) + f(\langle p \rangle)$ over
$\mathbb{F}_9 \cong \mathbb{F}_3[t]/(t^2 + 1) \cong \mathbb{F}_3[i]$ and p is the prime such that $\rho_f(\mathrm{Frob}_p)$ has $P(x)$ as characteristic polynomial.

Using the fact that the representation can ramify only at $3 \cdot 73$, we are able to prove that the image is $\tilde{A}_4$, in particular the projective image is $A_4 \subset \mathbb{P}\,\mathrm{GL}_2(\mathbb{F}_3)$. To do this we are using number theory and Dickson Theorem at the same time.

Let us remark that in this particular case, even if we have $\rho_f \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_9)$, so $\mathrm{Im}(\rho_f) \subseteq \mathrm{GL}_2(\mathbb{F}_9)$, the projective image is in $\mathbb{P}\,\mathrm{GL}_2(\mathbb{F}_3)$.

Why one should be interested in all this?

- For decades people studied these representations from the theoretical side without making computations. Now we want to show that what they could not prove is actually false, giving explicit examples. For example: Kilford and Wiese approach to Gorenstein properties of the Hecke algebras.
- To obtain explicit answer to question proposed by Serre, Ribet... about for example surjectivity of such representations for elliptic curves. Uniform bound for representations.
- The inverse Galois problem.

- **Algorithm**
  Our aim is to write an algorithm to compute images of residual modular Galois representations.

  We have a partial algorithm ($\Gamma_0(n)$, $k = 2$) implemented in SAGE, able to detect for a given level and a given morphism f as before, the set of primes for which the representation could have small image, according to Dickson Theorem, and the algorithm is able to check if this is the case.
- **Questions**
  How many T_p? Can we optimize the computation maybe modifying N and k?