Constructing Galois representations ramified at one prime

Anwesh Ray

University of British Columbia

anweshray@math.ubc.ca

November 9, 2021

Motivation

- Let p be a prime number and G a smooth group–scheme over $\mathbb{Z}_p$ (example $G = \mathrm{GL}_n$).
- The *inverse Galois problem* asks if $G(\mathbb{F}_p)$ is realizable as the Galois group $\mathrm{Gal}(K/\mathbb{Q})$.
- This is open for GL_n, however for $n = 2$, many $\mathrm{GL}_2(\mathbb{F}_p)$-extensions are cut out by the torsion in rational elliptic curves.

Galois actions arising from geometry

- Given a prime p and an elliptic curve $E_{/\mathbb{Q}}$, the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on $E[p] \subset E(\bar{\mathbb{Q}})$.
- This gives rise to a representation

$$\rho_{E,p} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}).$$

- The field $\mathbb{Q}(E[p])$ is fixed by the kernel of $\rho_{E,p}$, and $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_p)$ if $\rho_{E,p}$ is surjective.
- If E does not have complex-multiplication, then $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_p)$ for all but finitely many primes p.
- For example, for the elliptic curve $E : y^2 + xy + y = x^3 + x^2 - 2160x - 39540$ (with Cremona label 15a1), $\rho_{E,p}$ is surjective for all primes $p > 2$.

Galois representations

- Let $A_{/\mathbb{Q}}$ be an abelian variety of dimension m and p a prime.
- The p-adic Tate-module is the inverse limit

$$T_p(A) := \varprojlim_n A[p^n],$$

and is isomorphic to $\mathbb{Z}_p^{2m}$.
- The Galois representation on $T_p(A)$:

$$\rho_{A,p^\infty} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_{2m}(\mathbb{Z}_p).$$

- In fact, its image lies in the subgroup $\mathrm{GSp}_{2m}(\mathbb{Z}_p)$.

A result of Greenberg

- A prime p is *regular* if p does not divide the class number of $\mathbb{Q}(\mu_p)$. It is *irregular* otherwise.
- Let M be the maximal pro-p extension of $\mathbb{Q}(\mu_p)$ which is unramified at all primes $\ell \neq p$.

Theorem (Shafarevich)

If p is an regular prime, then $\mathrm{Gal}\,(M/\mathbb{Q}(\mu_p))$ is free pro-p with $\frac{p+1}{2}$ generators.

Theorem (Greenberg)

Let p be an odd regular prime such that $p \geq 4\lfloor n/2 \rfloor + 1$. Then, there is an infinite Galois extension $K \subset M$ such that $\mathrm{Gal}(K/\mathbb{Q})$ injects into $\mathrm{GL}_n(\mathbb{Z}_p)$ and contains a finite-index subgroup of $\mathrm{SL}_n(\mathbb{Z}_p)$.

What about irregular primes?

- Greenberg's result motivates the following question:

Question

Let p be a prime and $n > 1$. Does there exist a continuous Galois representation $\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{Z}_p)$ with suitably large image? If so, can one control the set of primes at which it may ramify?

Eigenspace decomposition

- Denote by
$$\chi : \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \to \mathbb{F}_p^\times$$
the mod-p cyclotomic character. This encodes the action of the Galois group on μ_p, the p-th roots of 1.
- Let $\mathcal{C} := \mathrm{Cl}(\mathbb{Q}(\mu_p)) \otimes \mathbb{F}_p$ be the mod-p class group of $\mathbb{Q}(\mu_p)$.
- There is an action of $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ on $\mathcal{C}$, and $\mathcal{C}$ decomposes into eigenspaces
$$\mathcal{C} = \bigoplus_{i=0}^{p-2} \mathcal{C}(\bar{\chi}^i),$$
where $\mathcal{C}(\bar{\chi}^i) = \{x \in \mathcal{C} \mid g \cdot x = \bar{\chi}^i(g)x\}$.

The index of irregularity

- The number of non-vanishing eigenspaces $\mathcal{C}(\bar{\chi}^i)$ is the *index of irregularity*.
- It is expected that the density of irregular primes with index of irregularity equal to r should equal $e^{-1/2}/(2^r r!)$.
- Among the first million primes, the highest index of irregularity observed is 6, for the prime $p = 527377$.

Main result

Theorem

Let $n > 1$, $e \geq 0$ and p be a prime number such that

1. $p \geq 2^{n+2+2e} + 3$,
2. *the index of irregularity of p is $\leq e$.*

There are infinitely many continuous representations $\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mathrm{GL}_n(\mathbb{Z}_p)$ unramified at all primes $\ell \neq p$, such that the image of ρ contains $\ker\left(\mathrm{SL}_n(\mathbb{Z}_p) \rightarrow \mathrm{SL}_n(\mathbb{Z}/p^4)\right)$.

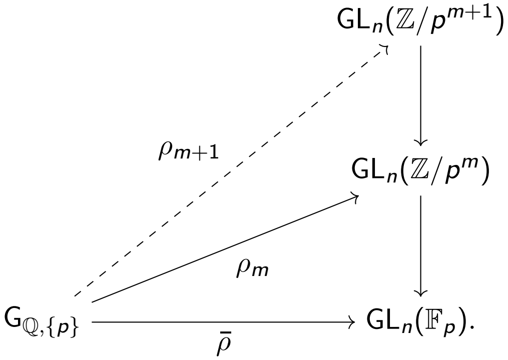
A suitable mod-p representation

- Let $\mathrm{G}_{\mathbb{Q},\{p\}}$ be the maximal quotient of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ unramified away from p.
- Fix a sequence of integers $k_1, k_2, \dots, k_n$ and set $\bar{\rho}$ to denote the mod-p Galois representation which is a direct sum of characters $\bar{\chi}^{k_1} \oplus \cdots \oplus \bar{\chi}^{k_n}$.
- In other words, we have the residual representation

$$\bar{\rho} = \begin{pmatrix} \bar{\chi}^{k_1} & & & \\ & \bar{\chi}^{k_2} & & \\ & & \ddots & \\ & & & \bar{\chi}^{k_n} \end{pmatrix} : \mathrm{G}_{\mathbb{Q},\{p\}} \to \mathrm{GL}_n(\mathbb{F}_p).$$

Lifting to characteristic zero

In order to lift $\bar{\rho}$ to a characteristic zero representation, it suffices to inductively lift it as depicted:



Deformations

- For a local ring R with maximal ideal $\mathfrak{m}_R$, let $\widehat{\mathrm{GL}_n}(R)$ be the group

$$\widehat{\mathrm{GL}_n}(R) := \ker \left\{ \mathrm{GL}_n(R) \xrightarrow{\mathrm{mod}\, \mathfrak{m}_R} \mathrm{GL}_n(R/\mathfrak{m}_R) \right\}.$$

- Two lifts $\rho_m, \rho_m' : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{Z}/p^m)$ of $\bar{\rho}$ are *strictly equivalent* if $\rho_m' = A\rho_m A^{-1}$ for some matrix $A \in \widehat{\mathrm{GL}_n}(\mathbb{Z}/p^m)$.
- A *deformation* is a strict equivalence class of lifts.

The adjoint module

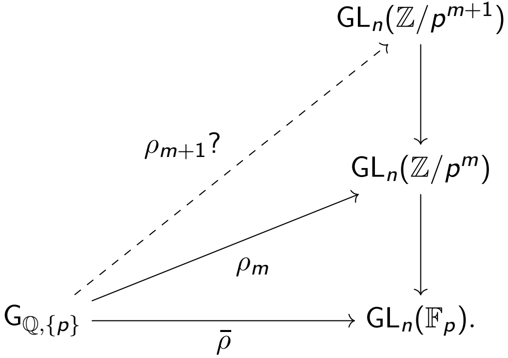
- Set $\operatorname{Ad}\bar{\rho}$ to denote the Galois module whose underlying vector space consists of $n \times n$ matrices with entries in $\mathbb{F}_p$.
- Let $\operatorname{Ad}^0\bar{\rho}$ be the Galois stable submodule of trace zero matrices. The Galois action is as follows: for $g \in \mathrm{G}_{\mathbb{Q},\{p\}}$ and $v \in \operatorname{Ad}\bar{\rho}$, set $g \cdot v := \bar{\rho}(g)v\bar{\rho}(g)^{-1}$.
- The module $\operatorname{Ad}^0\bar{\rho}$ is a direct sum

$$\operatorname{Ad}^0\bar{\rho} = \mathfrak{t} \oplus \left(\bigoplus_{(i,j), i \neq j} \mathbb{F}_p(\bar{\chi}^{k_i - k_j}) \right),$$

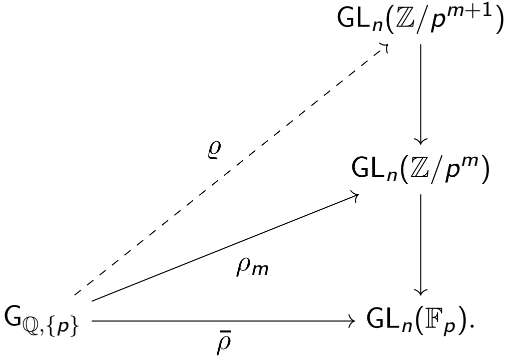
where $\mathfrak{t}$ is the submodule of diagonal matrices and the sum runs over (i,j) with $i \neq j$.

The infinitesimal lifting problem

Suppose that ρ_m is a mod-p^m lift. There is a *cohomological obstruction to lifting* ρ_m to ρ_{m+1} as depicted:



It is always possible to pick a continuous lift ϱ (which is not necessarily a homomorphism):



Cohomological obstruction to lifting

- A continuous lift (not necessarily a homomorphism) $\varrho : \mathrm{G}_{\mathbb{Q},\{p\}} \to \mathrm{GL}_n(\mathbb{Z}/p^{m+1})$ of ρ_m does always exist.
- Identify $\mathrm{Ad}^0 \bar{\rho}$ with the kernel of the mod-p^m map $\mathrm{SL}_n(\mathbb{Z}/p^{m+1}) \to \mathrm{SL}(\mathbb{Z}/p^m)$ by associating a vector $X \in \mathrm{Ad}^0 \bar{\rho}$ with $\mathrm{Id} + p^m X$.
- Let $\mathcal{O}(\rho_m)$ be the cohomology class in $H^2(\mathrm{G}_{\mathbb{Q},\{p\}}, \mathrm{Ad}^0 \bar{\rho})$ defined by the 2-cocycle

$$(g, h) \mapsto \varrho(gh)\varrho(h)^{-1}\varrho(g)^{-1}.$$

Vanishing of H^2

- The deformation problem is *unobstructed* if $H^2(\mathrm{G}_{\mathbb{Q},\{p\}}, \mathrm{Ad}^0\,\bar{\rho}) = 0$.
- In this case, ρ_m lifts to ρ_{m+1}, and thus inductively to a characteristic-zero representation

$$\rho : \mathrm{G}_{\mathbb{Q},\{p\}} \to \mathrm{GL}_n(\mathbb{Z}_p).$$

- Note that

$$H^2(\mathrm{G}_{\mathbb{Q},\{p\}}, \mathrm{Ad}^0\,\bar{\rho}) \simeq H^2(\mathrm{G}_{\mathbb{Q},\{p\}}, \mathfrak{t}) \oplus \left(\bigoplus_{(i,j),i\neq j} H^2\left(\mathrm{G}_{\mathbb{Q},\{p\}}, \mathbb{F}_p(\bar{\chi}^{k_i-k_j})\right)\right).$$

- If $k_i - k_j \neq 1 \mod p-1$, then,

$$H^2\left(\mathrm{G}_{\mathbb{Q},\{p\}}, \mathbb{F}_p(\bar{\chi}^{k_i-k_j})\right) \simeq \mathcal{C}(\bar{\chi}^{p-(k_i-k_j)}).$$

Theorem

Let $k_1, \ldots, k_n$ and $\bar{\rho}$ be as above. Assume that the following are satisfied:

1. $0 < k_i < \frac{p-1}{2}$,
2. k_i *is odd for* i *even and even for* i *odd,*
3. $\bar{\chi}^{k_i - k_j}$ *is not equal to* $\bar{\chi}$.
4. *The characters* $\bar{\chi}^{k_i - k_j}$ *for* $i \neq j$ *are all distinct.*
5. *For* (i, j) *such that* $i \neq j$, *we have that* $\mathcal{C}(\bar{\chi}^{p-(k_i - k_j)}) = 0$.

Then there exists a continuous lift $\rho : \mathrm{G}_{\mathbb{Q},\{p\}} \rightarrow \mathrm{GL}_n(\mathbb{Z}_p)$ *of* $\bar{\rho}$ *such that the image of* ρ *contains a finite index subgroup of* $\mathrm{SL}_n(\mathbb{Z}_p)$.

Sketch of proof

1. First, it is shown that there is a mod-p^5 lift $\rho_5 : \mathrm{G}_{\mathbb{Q},\{p\}} \to \mathrm{GL}_n(\mathbb{Z}/p^5)$ such that the image of ρ_5 contains
$$\ker\left\{\mathrm{SL}_n(\mathbb{Z}/p^5) \to \mathrm{SL}_n(\mathbb{Z}/p^4)\right\}.$$
2. Under the hypotheses for $(k_1, \dots, k_n)$, the cohomology group $H^2(\mathrm{G}_{\mathbb{Q},\{p\}}, \mathrm{Ad}^0\,\bar{\rho}) = 0$. It follows that ρ_5 lifts to a characteristic zero continuous representation $\rho : \mathrm{G}_{\mathbb{Q},\{p\}} \to \mathrm{GL}_n(\mathbb{Z}_p)$.
3. Finally, it is shown that the image of ρ contains $\ker\left(\mathrm{SL}_n(\mathbb{Z}_p) \to \mathrm{SL}_n(\mathbb{Z}/p^4)\right)$.

The choice of $(k_1, \ldots, k_n)$

- When $p \geq 2^{n+2+2e} + 3$ and has index of irregularity $\leq e$, one can choose $(k_1, \ldots, k_n)$ satisfying the conditions of the above theorem.
- Recall that we need
$$\mathcal{C}(\bar{\chi}^{p-(k_i-k_j)}) = 0$$
for all $i \neq j$. This is achieved by a pigeon-hole principle argument.

- Consider the $t := n + 2e$ numbers $m_1, \ldots, m_t$:

$$2^2, 2^3 + 1, 2^4, 2^5 + 1, 2^6, 2^7 + 1, \ldots.$$

- We have that $4 = m_1 < m_2 < \cdots < m_t < \frac{p-1}{2}$ and the characters $\bar{\chi}^{p-(m_i - m_j)}$ are all distinct.
- Since it is assumed that the index of irregularity of p is $\leq e$, at most e of the eigenspaces $\bar{\chi}^{p-(m_i - m_j)}$ are non-zero.
- One can choose the tuple $(k_1, \ldots, k_n)$ from $\{m_1, \ldots, m_t\}$ satisfying all of the required conditions.

Thank you!