Le programme de Langlands appliqué à la théorie de Galois inverse

Adrián Zenteno

Centro de Investigación en Matemáticas, A.C. México

XXXII^{es} Journées Arithmétiques

03 juillet 2023

Inverse Galois problem over $\mathbb{Q}$

From Galois Theory, we know that

$$\text{finite Galois extension } K/\mathbb{Q} \rightsquigarrow \text{finite group } G := Gal(K/\mathbb{Q})$$

Question (Inverse Galois Problem)

Let G be a finite group. Does there exist a finite Galois extension $K/\mathbb{Q}$ such that $Gal(K/\mathbb{Q}) \cong G$?

Known cases:

- $G = S_n, A_n$ (Hilbert 1892),
- G a solvable group (Shafarevich 1958),
- G a sporadic group except M_{23} (Matzat,Thompson,... 80's),
- $G = G(\mathbb{F}_{\ell^s})$ a finite Lie type group, when s is small as compared to the rank of G (Matzat, Malle,... 80's).

How to address the problem when s is large?

1. Let's consider a Galois representation

$$\overline{\rho} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_n(\overline{\mathbb{F}}_\ell)$$

2. As $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ is compact, $Im(\overline{\rho})$ is a finite matrix subgroup of $GL_n(\mathbb{F}_{\ell^s})$ for some integer $s > 0$.
3. As $Ker(\overline{\rho})$ is an open normal subgroup of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, there is a finite Galois extension $K/\mathbb{Q}$ such that

$$Ker(\overline{\rho}) \cong Gal(\overline{\mathbb{Q}}/K)$$

4. Then, combining ❷ ❸

$$Im(\overline{\rho}) \cong Gal(\overline{\mathbb{Q}}/\mathbb{Q})/Ker(\overline{\rho}) \cong Gal(\overline{\mathbb{Q}}/\mathbb{Q})/Gal(\overline{\mathbb{Q}}/K) \cong Gal(K/\mathbb{Q})$$

Maximally induced representations

- Let $n = 2m$ be a positive even integer and $p, q > n$ be distinct odd primes such that the order of q modulo p is n.
- $\mathbb{Q}_{q^n}$ be the unique unramified extension of $\mathbb{Q}_q$ of degree n and recall

$$\mathbb{Q}_{q^n}^\times \simeq \langle q \rangle \times \mu_{q^n-1} \times U_1$$

Definition

Let ℓ be a prime distinct from p and q. A character

$$\chi_q : \mathbb{Q}_{q^n} \longrightarrow \overline{\mathbb{Q}}_\ell^\times$$

is of *S-type* (*resp. of O-type*) and order p if satisfies the following conditions:

1. $\chi_q|_{U_1}$ is trivial,
2. $\chi_q|_{\mu_{q^n-1}}$ has order p,
3. $\chi_q(q) = -1$ (resp. $\chi_q(q) = 1$)

Maximally induced representations

By Class Field Theory

Definition

Let ℓ be a prime distinct from p and q. A character

$$\chi_q : Gal(\overline{\mathbb{Q}}_q/\mathbb{Q}_{q^n}) \longrightarrow \overline{\mathbb{Q}}_\ell^\times$$

is of **S-type (resp. of O-type)** and order p if satisfies the following conditions:

1. $\chi_q|_{U_1}$ is trivial,
2. $\chi_q|_{\mu_{q^n-1}}$ has order p,
3. $\chi_q(q) = -1$ (resp. $\chi_q(q) = 1$)

We can construct

$$\rho_q := \mathrm{Ind}_{Gal(\overline{\mathbb{Q}}_q/\mathbb{Q}_{q^n})}^{Gal(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)} \chi_q : Gal(\overline{\mathbb{Q}}_q/\mathbb{Q}_q) \longrightarrow GL_n(\overline{\mathbb{Q}}_\ell)$$

We can construct

$$\rho_q = \mathrm{Ind}_{Gal(\overline{\mathbb{Q}}_q/\mathbb{Q}_{q^n})}^{Gal(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)} \chi_q : Gal(\overline{\mathbb{Q}}_q/\mathbb{Q}_q) \longrightarrow GL_n(\overline{\mathbb{Q}}_\ell)$$

It can be proved that

- If χ_q is of S-type, ρ_q is irreducible and symplectic in the sense that it can be conjugated to take values in $Sp_n(\overline{\mathbb{Q}}_\ell)$.
- If χ_q is of O-type, ρ_q is irreducible and orthogonal in the sense that it can be conjugated to take values in $SO_n(\overline{\mathbb{Q}}_\ell)$.
- In fact, if $\alpha : Gal(\overline{\mathbb{Q}}_q/\mathbb{Q}_q) \longrightarrow \overline{\mathbb{Q}}_\ell^\times$ is an unramified character, then the residual representation

$$\overline{\rho}_q \otimes \overline{\alpha} : Gal(\overline{\mathbb{Q}}_q/\mathbb{Q}_q) \longrightarrow GL_n(\overline{\mathbb{F}}_\ell)$$

(the semi-simplification of the reduction mod ℓ) is also irreducible.

Definition

We say that a Galois representation

$$\rho : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_n(\overline{\mathbb{Q}}_\ell)$$

is **maximally induced of S-type (resp. of O-type)** at q of order p if

$$\rho|_{D_q} \simeq \rho_q \otimes \alpha$$

where ρ_q is constructed from a character χ_q of S-type (resp. of O-type) of order p and α is an unramified character as above.

Theorem

If

$$\rho : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_n(\overline{\mathbb{Q}}_\ell)$$

is a maximally induced Galois representation

- *of S-type at q of order p, then the image of* $\overline{\rho}^{proj}$ *is equal to*

  $$PSp_n(\mathbb{F}_{\ell^s}) \text{ or } PGSp_n(\mathbb{F}_{\ell^s})$$

  for some integer $s > 0$.

- *resp. if* ρ *is of O-type at q of order p, then the image of* $\overline{\rho}^{proj}$ *is equal to*

  $$P\Omega_n^{\pm}(\mathbb{F}_{\ell^s}),\ PSO_n^{\pm}(\mathbb{F}_{\ell^s}),\ PO_n^{\pm}(\mathbb{F}_{\ell^s}) \text{ or } PGO_n^{\pm}(\mathbb{F}_{\ell^s})$$

  for some integer $s > 0$.

Question

Are there maximally induced Galois representations?

Applying Langlands program

1. Let's start with χ_q of S-type, then

$$\rho_q : Gal(\overline{\mathbb{Q}}_q/\mathbb{Q}_q) \longrightarrow Sp_n(\overline{\mathbb{Q}}_\ell).$$

2. By Local Langlands Correspondence (H 2000, HT 2001)

$$\rho_q \rightsquigarrow \tau_q \text{ a supercuspidal representation of } SO_{n+1}(\overline{\mathbb{Q}}_q).$$

3. By globalization of supercuspidal representations of simple quasi-split algebraic groups (KLS 2008), there is

$$\tau = \otimes_v \tau_v$$

a cuspidal automorphic representation of $SO_{n+1}(\mathbb{A}_\mathbb{Q})$ such that if $v = q$ then $\tau_v = \tau_q$.

Applying Langlands program

2. By Local Langlands Correspondence (H 2000, HT 2001)

$$\rho_q \rightsquigarrow \tau_q \text{ a supercuspidal representation of } SO_{n+1}(\overline{\mathbb{Q}}_q).$$

3. By globalization of supercuspidal representations of simple quasi-split algebraic groups (KLS 2008), there is

$$\tau = \otimes_v \tau_v$$

a cuspidal automorphic representation of $SO_{n+1}(\mathbb{A}_{\mathbb{Q}})$ such that if $v = q$ then $\tau_v = \tau_q$.

4. By Langlands Functoriality (A 2013) there is a regular algebraic, essentially self-dual, cuspidal automorphic representation $\pi = \otimes_v \pi_v$ of $GL_n(\mathbb{A}_{\mathbb{Q}})$ such that $\tau_q \cong \pi_q$.

Applying Langlands program

3. By globalization of supercuspidal representations of simple quasi-split algebraic groups (KLS 2008), there is
$$\tau = \otimes_v \tau_v$$
a cuspidal automorphic representation of $SO_{n+1}(\mathbb{A}_{\mathbb{Q}})$ such that if $v = q$ then $\tau_v = \tau_q$.
4. By Langlands Functoriality (A 2013) there is a regular algebraic, essentially self-dual, cuspidal automorphic representation $\pi = \otimes_v \pi_v$ of $GL_n(\mathbb{A}_{\mathbb{Q}})$ such that $\tau_q \cong \pi_q$.
5. By Global Langlands correspondence (S 2011, CH 2013), there is a self-dual Galois representation
$$\rho_{\pi,\ell} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GSp_n(\overline{\mathbb{Q}}_\ell)$$
such that
$$\rho_{\pi,\ell}\big|_{D_q} \simeq \rho_q \otimes \alpha$$
for some unramified character α as above.

Similarly

1. If we start with χ_q of O-type, we obtain

$$\rho_q : Gal(\overline{\mathbb{Q}}_q/\mathbb{Q}_q) \longrightarrow SO_n(\overline{\mathbb{Q}}_\ell).$$

2. By Local Langlands Correspondence (H 2000, HT 2001)

$$\rho_q \rightsquigarrow \tau_q \text{ a supercuspidal representation of } SO_n(\overline{\mathbb{Q}}_q).$$

3. By globalization of supercuspidal representations of simple quasi-split algebraic groups (KLS 2008), there is

$$\tau = \otimes_v \tau_v$$

a cuspidal automorphic representation of $SO_n(\mathbb{A}_\mathbb{Q})$ such that if $v = q$ then $\tau_v = \tau_q$.

4. By Langlands Functoriality (A 2013) there is a regular algebraic, essentially self-dual, cuspidal automorphic representation $\pi = \otimes_v \pi_v$ of $GL_n(\mathbb{A}_{\mathbb{Q}})$ such that $\tau_q \cong \pi_q$.
5. By Global Langlands correspondence (S 2011, HT 2013), there is a self-dual Galois representation

$$\rho_{\pi,\ell} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GO_n(\overline{\mathbb{Q}}_\ell)$$

such that

$$\rho_{\pi,\ell}|_{D_q} \simeq \rho_q \otimes \alpha$$

for some unramified character α as above.

Consequences

Let ℓ be a (fixed) prime.

- By Chebotarev's Density Theorem, there are infinitely many ways to choose the couple of primes (p, q).
- Then, we can construct infinitely many regular algebraic, essentially self-dual, cuspidal automorphic representations

$$\{\pi_i\}_{i \in \mathbb{N}}$$

  of $GL_n(\mathbb{A}_{\mathbb{Q}})$ as above.
- Hence, there exists a family of Galois representations

$$\{\rho_{\pi_i,\ell}\}_{i \in \mathbb{N}}$$

  of S-type (resp. O-type) such that the size of the image of $\overline{\rho}^{proj}_{\pi_i,\ell}$ is unbounded for running i, because we can choose p as large as we please so that elements of larger and larger orders appear in the inertia images.

Consequences

Corollary

Let ℓ be an odd prime. Then, there are infinitely many integers $s > 0$ such that

- *(AdRDSW 2015) at least one of the following groups:*

$$\{PSp_{2m}(\mathbb{F}_{\ell^s}),\ PGSp_{2m}(\mathbb{F}_{\ell^s})\}$$

can be realized as a Galois group over $\mathbb{Q}$.

- *(Z 2021) at least one of the following groups:*

$$\{P\Omega^{\pm}_{2m}(\mathbb{F}_{\ell^s}),\ PSO^{\pm}_{2m}(\mathbb{F}_{\ell^s}),\ PO^{\pm}_{2m}(\mathbb{F}_{\ell^s}),\ PGO^{\pm}_{2m}(\mathbb{F}_{\ell^s})\}$$

can be realized as a Galois group over $\mathbb{Q}$.

More cases solved

Theorem (KLS 2010)

Let ℓ be an odd prime. Then, there are infinitely many integers $s > 0$ such that

- *at least one of the following groups:*

$$\{\Omega_{2m+1}(\mathbb{F}_{\ell^s}),\ SO_{2m+1}(\mathbb{F}_{\ell^s})\}$$

  can be realized as a Galois group over $\mathbb{Q}$.

- *$G_2(\mathbb{F}_{\ell^s})$ can be realized as a Galois group over $\mathbb{Q}$.*

Thank you for your attention!

Merci pour votre attention!