Images of Galois representations

Andrea Conti

University of Luxembourg

October 25, 2019

$\overline{\mathbb{Q}}$ = an algebraic closure of $\mathbb{Q}$

$\overline{\mathbb{Q}}$ = an algebraic closure of $\mathbb{Q}$

We study the profinite group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ via its continuous representations:

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(A)$$

where A is a topological ring.

Consider an elliptic curve E defined over $\mathbb{Q}$.

Consider an elliptic curve E defined over $\mathbb{Q}$.

$E(\overline{\mathbb{Q}})$ is equipped with a group structure.

Consider an elliptic curve E defined over $\mathbb{Q}$.

$E(\overline{\mathbb{Q}})$ is equipped with a group structure.

The action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on

$$E[p^\infty] = \varprojlim_n E[p^n]$$

gives a continuous representation

$$\rho_E \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_p).$$

For a “generic” elliptic curve, $\mathrm{End}(E) = \mathbb{Z}$.

For a "generic" elliptic curve, $\mathrm{End}(E) = \mathbb{Z}$.

We say that E has complex multiplication by an imaginary quadratic field K if

$$\mathrm{End}(E) = \text{an order in } K$$

For a "generic" elliptic curve, $\mathrm{End}(E) = \mathbb{Z}$.

We say that E has complex multiplication by an imaginary quadratic field K if

$$\mathrm{End}(E) = \text{an order in } K$$

If E has complex multiplication by K, then

$$\rho_E \cong \rho_E \otimes \chi_K$$

where χ_K is the quadratic character of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $\overline{\mathbb{Q}}^{\ker \chi} = K$.

For a "generic" elliptic curve, $\mathrm{End}(E) = \mathbb{Z}$.

We say that E has complex multiplication by an imaginary quadratic field K if

$$\mathrm{End}(E) = \text{an order in } K$$

If E has complex multiplication by K, then

$$\rho_E \cong \rho_E \otimes \chi_K$$

where χ_K is the quadratic character of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $\overline{\mathbb{Q}}^{\ker \chi} = K$.

For a "generic" elliptic curve, $\mathrm{End}(E) = \mathbb{Z}$.

We say that E has complex multiplication by an imaginary quadratic field K if

$$\mathrm{End}(E) = \text{an order in } K$$

If E has complex multiplication by K, then

$$\rho_E \cong \rho_E \otimes \chi_K$$

where χ_K is the quadratic character of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $\overline{\mathbb{Q}}^{\ker \chi} = K$.

This implies: up to conjugation,

$$\mathrm{Im}\,\rho_E \subset \left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \right\} \cup \left\{ \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix} \right\}$$

For a “generic” elliptic curve, $\mathrm{End}(E) = \mathbb{Z}$.

We say that E has complex multiplication by an imaginary quadratic field K if

$$\mathrm{End}(E) = \text{an order in } K$$

If E has complex multiplication by K, then

$$\rho_E \cong \rho_E \otimes \chi_K$$

where χ_K is the quadratic character of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $\overline{\mathbb{Q}}^{\ker \chi} = K$.

This implies: up to conjugation,

$$\mathrm{Im}\, \rho_E \subset \left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \right\} \cup \left\{ \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix} \right\}$$

The image is “small”.

If E has no CM, Serre proved that the image of ρ_E is “large”:

If E has no CM, Serre proved that the image of ρ_E is "large": up to conjugation,

$$\operatorname{Im}\rho_E \supset \begin{pmatrix} 1+p^n\mathbb{Z}_p & p^n\mathbb{Z}_p \\ p^n\mathbb{Z}_p & 1+p^n\mathbb{Z}_p \end{pmatrix} \cap \mathrm{SL}_2(\mathbb{Z}_p)$$

for some n, i.e., $\operatorname{Im}\rho_E$ contains a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$.

If E has no CM, Serre proved that the image of ρ_E is "large": up to conjugation,

$$\operatorname{Im}\rho_E \supset \begin{pmatrix} 1+p^n\mathbb{Z}_p & p^n\mathbb{Z}_p \\ p^n\mathbb{Z}_p & 1+p^n\mathbb{Z}_p \end{pmatrix} \cap \mathrm{SL}_2(\mathbb{Z}_p)$$

for some n, i.e., $\operatorname{Im}\rho_E$ contains a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$.

In other words: the size of the image of ρ_E detects exactly whether E is "special" or "generic".

We can build representations with coefficients in rings larger than $\mathbb{Z}_p$.

We can build representations with coefficients in rings larger than $\mathbb{Z}_p$.

Given

$$\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(A)$$

we can look at symmetries of the type

$$\rho \otimes \chi \cong \rho \circ \sigma$$

where σ is an automorphism of A.

We can build representations with coefficients in rings larger than $\mathbb{Z}_p$.

Given

$$\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(A)$$

we can look at symmetries of the type

$$\rho \otimes \chi \cong \rho \circ \sigma$$

where σ is an automorphism of A.

We call (σ, χ) a *conjugate self-twist* of ρ.

We can build representations with coefficients in rings larger than $\mathbb{Z}_p$.

Given

$$\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(A)$$

we can look at symmetries of the type

$$\rho \otimes \chi \cong \rho \circ \sigma$$

where σ is an automorphism of A.

We call (σ, χ) a *conjugate self-twist* of ρ.

Conjugate self-twists form a group Σ.

Easy: the size of $\mathrm{Im}\,\rho$ has a natural bound determined by all of its conjugate self-twists:

Easy: the size of $\operatorname{Im}\rho$ has a natural bound determined by all of its conjugate self-twists:

A^{Σ} = subring of A of elements fixed by all conjugate self-twists

Easy: the size of $\mathrm{Im}\,\rho$ has a natural bound determined by all of its conjugate self-twists:

A^{Σ} = subring of A of elements fixed by all conjugate self-twists

(Usually:) There exists an open subgroup H of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that

$$\rho(H) \subset \mathrm{GL}_2(A_0)$$

Easy: the size of $\operatorname{Im}\rho$ has a natural bound determined by all of its conjugate self-twists:

A^{Σ} = subring of A of elements fixed by all conjugate self-twists

(Usually:) There exists an open subgroup H of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that

$$\rho(H) \subset \mathrm{GL}_2(A_0)$$

Question: Is $\operatorname{Im}\rho$ large in $\mathrm{GL}_2(A_0)$?

Easy: the size of $\mathrm{Im}\,\rho$ has a natural bound determined by all of its conjugate self-twists:

A^{Σ} = subring of A of elements fixed by all conjugate self-twists

(Usually:) There exists an open subgroup H of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that

$$\rho(H) \subset \mathrm{GL}_2(A_0)$$

Question: Is $\mathrm{Im}\,\rho$ large in $\mathrm{GL}_2(A_0)$?

(Does the size of $\mathrm{Im}\,\rho$ detect precisely the symmetries of ρ?)

It is known how to build Galois representations from many objects: abelian varieties, modular forms, automorphic representations of reductive groups.

It is known how to build Galois representations from many objects: abelian varieties, modular forms, automorphic representations of reductive groups.

For some of these we have a largeness result.

It is known how to build Galois representations from many objects: abelian varieties, modular forms, automorphic representations of reductive groups.

For some of these we have a largeness result. For instance:

Theorem (Momose 1981, Ribet 1985)

For a non-CM cuspidal modular form f and almost all p, the image of the p-adic Galois representation

$$\rho_{f,p} \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathcal{O})$$

attached to f contains a congruence subgroup of $\mathrm{SL}_2(\mathcal{O}^{\Sigma})$.

It is known how to build Galois representations from many objects: abelian varieties, modular forms, automorphic representations of reductive groups.

For some of these we have a largeness result. For instance:

Theorem (Momose 1981, Ribet 1985)

For a non-CM cuspidal modular form f and almost all p, the image of the p-adic Galois representation

$$\rho_{f,p}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathcal{O})$$

attached to f contains a congruence subgroup of $\mathrm{SL}_2(\mathcal{O}^\Sigma)$.

It is known how to build Galois representations from many objects: abelian varieties, modular forms, automorphic representations of reductive groups.

For some of these we have a largeness result. For instance:

Theorem (Momose 1981, Ribet 1985)

For a non-CM cuspidal modular form f and almost all p, the image of the p-adic Galois representation

$$\rho_{f,p} \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathcal{O})$$

attached to f contains a congruence subgroup of $\mathrm{SL}_2(\mathcal{O}^\Sigma)$.

There are also results for Hilbert and Siegel modular forms (Nekovar, Dieulefait–Zenteno), Hida and Coleman families of modular forms (Hida, J. Lang, C.–Iovita–Tilouine), Siegel–Hida families (Hida–Tilouine).

Bellaïche proves a purely algebraic result:

Theorem (Bellaïche 2017)

Consider a profinite group G, a local pro-p integral domain A and a continuous representation

$$\rho\colon G \to \mathrm{GL}_2(A).$$

Assume that ρ is irreducible, non-induced and "regular". Then there exists a subring A_0 of A such that the image of ρ contains a congruence subgroup of $\mathrm{SL}_2(A_0)$.

Ingredients:

Ingredients:

1. replace representations by pseudorepresentations;

Ingredients:

1. replace representations by pseudorepresentations;
2. replace $\mathrm{GL}_2(A)$ by the units in a *generalized matrix algebra* (GMA);

Ingredients:

1. replace representations by pseudorepresentations;
2. replace $\mathrm{GL}_2(A)$ by the units in a *generalized matrix algebra* (GMA);
3. generalize Pink's Lie algebra theory to GMAs.

Ingredients:

1. replace representations by pseudorepresentations;
2. replace $\mathrm{GL}_2(A)$ by the units in a *generalized matrix algebra* (GMA);
3. generalize Pink's Lie algebra theory to GMAs.

Ingredients:

1. replace representations by pseudorepresentations;
2. replace $\mathrm{GL}_2(A)$ by the units in a *generalized matrix algebra* (GMA);
3. generalize Pink's Lie algebra theory to GMAs.

1 and 2 are important for treating reducible residual representations, and work in every dimension

Ingredients:

1. replace representations by pseudorepresentations;
2. replace $\mathrm{GL}_2(A)$ by the units in a *generalized matrix algebra* (GMA);
3. generalize Pink's Lie algebra theory to GMAs.

1 and 2 are important for treating reducible residual representations, and work in every dimension

3 only exists in dimension 2

The description of A_0 in terms of the conjugate self-twists of ρ is missing from Bellaïche's result.

The description of A_0 in terms of the conjugate self-twists of ρ is missing from Bellaïche's result.

Theorem (C.–Lang–Medvedovsky 2019)

Consider a profinite group G, a local pro-p integral domain A and a continuous representation

$$\rho\colon G \to \mathrm{GL}_2(A).$$

Assume that ρ is irreducible, non-induced and "regular". Then the image of ρ contains a congruence subgroup of $\mathrm{SL}_2(A^\Sigma)$.

The description of A_0 in terms of the conjugate self-twists of ρ is missing from Bellaïche's result.

Theorem (C.–Lang–Medvedovsky 2019)

Consider a profinite group G, a local pro-p integral domain A and a continuous representation

$$\rho\colon G \to \mathrm{GL}_2(A).$$

Assume that ρ is irreducible, non-induced and "regular". Then the image of ρ contains a congruence subgroup of $\mathrm{SL}_2(A^\Sigma)$.

The description of A_0 in terms of the conjugate self-twists of ρ is missing from Bellaïche's result.

Theorem (C.–Lang–Medvedovsky 2019)

Consider a profinite group G, a local pro-p integral domain A and a continuous representation

$$\rho\colon G \to \mathrm{GL}_2(A).$$

Assume that ρ is irreducible, non-induced and "regular". Then the image of ρ contains a congruence subgroup of $\mathrm{SL}_2(A^\Sigma)$.

We can use this result to recover the known large image results.

Strategy:

Strategy:

- with some tricks one can enlarge the residue field of Bellaïche's ring to get a new ring A_0';

Strategy:

- with some tricks one can enlarge the residue field of Bellaïche's ring to get a new ring A_0';
- conjugate self-twists of ρ can be lifted to conjugate self-twists of the universal deformation ring of $\overline{\rho}$;

Strategy:

- with some tricks one can enlarge the residue field of Bellaïche's ring to get a new ring A'_0;
- conjugate self-twists of ρ can be lifted to conjugate self-twists of the universal deformation ring of $\overline{\rho}$;
- A^{Σ} contains A'_0, it is finite as a A'_0-module, and their fields of fractions coincide.

Strategy:

- with some tricks one can enlarge the residue field of Bellaïche's ring to get a new ring A_0';
- conjugate self-twists of ρ can be lifted to conjugate self-twists of the universal deformation ring of $\overline{\rho}$;
- A^Σ contains A_0', it is finite as a A_0'-module, and their fields of fractions coincide.

Strategy:

- with some tricks one can enlarge the residue field of Bellaïche's ring to get a new ring A'_0;
- conjugate self-twists of ρ can be lifted to conjugate self-twists of the universal deformation ring of $\overline{\rho}$;
- A^Σ contains A'_0, it is finite as a A'_0-module, and their fields of fractions coincide. ($\implies A^\Sigma-$large $= A'_0-$large)

Strategy:

- with some tricks one can enlarge the residue field of Bellaïche's ring to get a new ring A'_0;
- conjugate self-twists of ρ can be lifted to conjugate self-twists of the universal deformation ring of $\overline{\rho}$;
- A^{Σ} contains A'_0, it is finite as a A'_0-module, and their fields of fractions coincide. ($\implies A^{\Sigma}-$large $= A'_0-$large)

Questions:

Strategy:

- with some tricks one can enlarge the residue field of Bellaïche's ring to get a new ring A_0';
- conjugate self-twists of ρ can be lifted to conjugate self-twists of the universal deformation ring of $\overline{\rho}$;
- A^{Σ} contains A_0', it is finite as a A_0'-module, and their fields of fractions coincide. ($\implies A^{\Sigma}-$large $= A_0'-$large)

Questions:

- Can this result be generalized to higher dimension?

Strategy:

- with some tricks one can enlarge the residue field of Bellaïche's ring to get a new ring A'_0;
- conjugate self-twists of ρ can be lifted to conjugate self-twists of the universal deformation ring of $\overline{\rho}$;
- A^Σ contains A'_0, it is finite as a A'_0-module, and their fields of fractions coincide. ($\implies A^\Sigma-$large $= A'_0-$large)

Questions:

- Can this result be generalized to higher dimension?
- How can one characterize the level of the congruence subgroup contained in the image?

Thank you for your attention!