The inverse Galois problem: abelian varieties, modular forms & Goldbach's conjecture

Samuele Anni

Géométrie algébrique, Théorie des nombres et Applications, GTA2021

19th August 2021

Université d'Aix-Marseille, Institut de Mathématiques

The inverse Galois problem

The inverse Galois problem

The inverse Galois problem

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

The inverse Galois problem

The inverse Galois problem

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

The inverse Galois problem: effective version

Let G be a finite group. Can one give an explicit/effective construction of a Galois extension $K/\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q}) \cong G$?

The inverse Galois problem

The inverse Galois problem with contraints

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

The inverse Galois problem

The inverse Galois problem with contraints

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

The inverse Galois problem: uniform version

Let G_n be a parametric family of finite groups. Can one write a unique "object" attached to a family of number fields K_n such that for every n one has $\mathrm{Gal}(K_n/\mathbb{Q}) \cong G_n$?

Theorem

If $G_n \cong \mathbb{Z}/n\mathbb{Z}$ where $n \in \mathbb{Z}_{>1}$, then G_n is a Galois group over $\mathbb{Q}$.

Proof.

□

Theorem

If $G_n \cong \mathbb{Z}/n\mathbb{Z}$ where $n \in \mathbb{Z}_{>1}$, then G_n is a Galois group over $\mathbb{Q}$.

Proof.

□

Theorem

Every finite abelian group is a Galois group over $\mathbb{Q}$.

Theorem

If $G_n \cong S_n$ where $n \in \mathbb{Z}_{>1}$, then G_n is a Galois group over $\mathbb{Q}$.

Theorem

If $G_n \cong S_n$ where $n \in \mathbb{Z}_{>1}$, then G_n is a Galois group over $\mathbb{Q}$.

Proof.

Let K_n be the splitting field of

$$x^n - x - 1$$

over $\mathbb{Q}$. Then, $\mathrm{Gal}(K_n/\mathbb{Q}) \cong S_n$ for every n (uniform realisation). $\square$

The inverse Galois problem: general base

Let G be a finite group and let K be a number field. Does there exist a Galois extension L/K such that $\mathrm{Gal}(L/K) \cong G$?

The inverse Galois problem: general base

Let G be a finite group and let K be a number field. Does there exist a Galois extension L/K such that $\mathrm{Gal}(L/K) \cong G$?

Aims of this talk

1. Show that it is possible to **explicitly** realise for all* $g \in \mathbb{Z}_{\geq 1}$, the group $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ as a Galois group over $\mathbb{Q}$, simultaneously for all odd primes ℓ, using the ℓ-torsion of the Jacobian of the same hyperelliptic curve.
2. Elliptic curves over totally real fields (with a digression on isogenies).

The inverse Galois problem: general base

Let G be a finite group and let K be a number field. Does there exist a Galois extension L/K such that $\mathrm{Gal}(L/K) \cong G$?

Aims of this talk

1. Show that it is possible to **explicitly** realise for all* $g \in \mathbb{Z}_{\geq 1}$, the group $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ as a Galois group over $\mathbb{Q}$, simultaneously for all odd primes ℓ, using the ℓ-torsion of the Jacobian of the same hyperelliptic curve.
2. Elliptic curves over totally real fields (with a digression on isogenies).

Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$ and let $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Let A be a principally polarized abelian variety over $\mathbb{Q}$ of dimension g.

Let ℓ be a prime and $A[\ell]$ the ℓ-torsion subgroup:

$$A[\ell] := \{P \in A(\overline{\mathbb{Q}}) \mid [\ell]P = 0\} \cong (\mathbb{Z}/\ell\mathbb{Z})^{2g}.$$

$A[\ell]$ is a $2g$-dimensional $\mathbb{F}_\ell$-vector space, as well as a $G_{\mathbb{Q}}$-module.

The polarization induces a symplectic pairing, the mod ℓ **Weil pairing** on $A[\ell]$, which is a bilinear, alternating, non-degenerate pairing:

$$\langle\ ,\ \rangle\ :\ A[\ell] \times A[\ell] \to \mu_\ell$$

that is Galois invariant: $\forall \sigma \in G_{\mathbb{Q}}\,,\ \forall v, w \in A[\ell]$

$$\langle \sigma v, \sigma w \rangle = \chi(\sigma)\langle v, w \rangle,$$

where $\chi : G_{\mathbb{Q}} \to \mathbb{F}_\ell^\times$ is the mod ℓ cyclotomic character.

$(A[\ell], \langle\ ,\ \rangle)$ is a symplectic $\mathbb{F}_\ell$-vector space of dimension $2g$. This gives a representation

$$\overline{\rho}_{A,\ell} : G_{\mathbb{Q}} \to \mathsf{GSp}(A[\ell], \langle\ ,\ \rangle) \cong \mathsf{GSp}_{2g}(\mathbb{F}_\ell).$$

Example: $g = 1$

Take $\ell = 3$ and the elliptic curve over $\mathbb{Q}$ given by:

$$E: \quad y^2 = x^3 + 5x + 22 \qquad (53.a1)$$

3-division polynomial ψ_3: polynomial whose roots are the x-coordinates of the non trivial 3-torsion points. In this case the polynomial is

$$\psi_3(x) = 3x^4 + 30x^2 + 264x - 25.$$

One can show that $\psi_3(x)$ is irreducible over $\mathbb{Q}$ and via a Theorem of Reverter and Vila (2000) we have that

$$\overline{\rho}_{E,3} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_3)$$

is surjective.

Example: $g = 1$

$$\overline{\rho}_{E,3} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_3)$$

is surjective so there exists a number field $K/\mathbb{Q}$, the kernel of the representation, such that $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_3)$.

K is the splitting field of

$$x^8 + 3x^7 + 7x^6 + \frac{29}{3}x^5 + \frac{26}{3}x^4 + 4x^3 + x^2 + \frac{5}{9}X - \frac{7}{27}.$$

Theorem (Serre)

Let $A/\mathbb{Q}$ be a principally polarized abelian variety of dimension g. Assume that $g = 2, 6$ or g is odd and, furthermore, assume that $\mathrm{End}_{\overline{\mathbb{Q}}}(A) = \mathbb{Z}$. Then there exists a bound B_A such that for all primes $\ell > B_A$ the representation $\overline{\rho}_{A,\ell}$ is surjective.

The conclusion of the theorem is known to be false for general g (counterexample by Mumford for $g = 4$).

Open question

Is it possble to have a **uniform bound** B_g depending only on g?

Genus 1

The Galois representation attached to the ℓ-torsion of the **elliptic curve**

$$y^2 + y = x^3 - x \qquad (37a1)$$

is surjective for all prime ℓ. This gives a realization $\mathrm{GL}_2(\mathbb{F}_\ell)$ as Galois group for all prime ℓ.

Genus 1

The Galois representation attached to the ℓ-torsion of the **elliptic curve**

$$y^2 + y = x^3 - x \qquad (37a1)$$

is surjective for all prime ℓ. This gives a realization $\mathrm{GL}_2(\mathbb{F}_\ell)$ as Galois group for all prime ℓ.

Genus 2 (Dieulefait)

Let C be the **genus** 2 **hyperelliptic curve** given by

$$y^2 = x^5 - x + 1 \qquad (45904.d.734464.1)$$

and let J denotes its Jacobian. This gives a realization $\mathrm{GSp}_4(\mathbb{F}_\ell)$ as Galois group for all odd prime ℓ.

Genus 3 (A., Lemos and Siksek)

Let $C/\mathbb{Q}$ be the following genus 3 hyperelliptic curve,

$$C \ : \ y^2 + (x^4 + x^3 + x + 1)y = x^6 + x^5.$$

and write J for its Jacobian. Then

$$\overline{\rho}_{J,\ell}(G_{\mathbb{Q}}) = \mathsf{GSp}_6(\mathbb{F}_\ell)$$

for all odd prime ℓ. Moreover, $\overline{\rho}_{J,2}(G_{\mathbb{Q}}) \cong S_5 \times C_2 \subseteq S_8$.

Genus 3 (A., Lemos and Siksek)

Let $C/\mathbb{Q}$ be the following genus 3 hyperelliptic curve,

$$C \ : \ y^2 + (x^4 + x^3 + x + 1)y = x^6 + x^5.$$

and write J for its Jacobian. Then

$$\overline{\rho}_{J,\ell}(G_{\mathbb{Q}}) = \mathsf{GSp}_6(\mathbb{F}_\ell)$$

for all odd prime ℓ. Moreover, $\overline{\rho}_{J,2}(G_{\mathbb{Q}}) \cong S_5 \times C_2 \subseteq S_8$.

Higher genera

What about $g \geq 4$?

Main result

Theorem (A., Dokchitser V.)

Let g be a positive integer such that $2g+2$ satifies hypothesis $(2\mathrm{G}+\epsilon)$. Then there exist an explicit $N \in \mathbb{Z}$ and an explicit $f_0(x) \in \mathbb{Z}[x]$ monic of degree $2g+2$ such that if

1. $f(x) \equiv f_0(x) \bmod N$, *and*
2. $f(x) \bmod p$ *has no roots of multiplicity* ≥ 2 *for all primes* $p \nmid N$,

then $\mathrm{Gal}(\mathbb{Q}(J[\ell])/\mathbb{Q}) \cong \begin{cases} \mathrm{GSp}_{2g}(\mathbb{F}_\ell) \text{ for all primes } \ell \neq 2 \\ S_{2g+2} \text{ for } \ell = 2. \end{cases}$

Double Goldbach conjecture

Let $g \in \mathbb{Z}_{\geq 0}$.

Hypothesis $(2\mathrm{G} + \epsilon)$: Double Goldbach conjecture

There exist primes q_1, q_2, q_3, q_4, q_5 such that:

$2g + 2 = q_1 + q_2 = q_4 + q_5, \qquad 2g + 2 > q_3 > q_5 > q_2 \geq q_1 > q_4.$

Hypothesis $(2\mathrm{G} + \epsilon)$ has been verified for g up to 10^7: the only exceptions are $0, 1, 2, 3, 4, 5, 7$ and 13.

Remarks

Remarks

- If $(2\mathrm{G}+\epsilon)$ does not hold, it is still possible to obtain the same conclusion as in the theorem except for a finite list of primes ℓ:

Genus	primes excluded
2	$3, 5$
3	$3, 5, 7$
4	$5, 7$
5	$5, 7, 11$
7	$5, 11, 13$
13	$11, 17, 23$

Remarks

- If $(2\mathrm{G}+\epsilon)$ does not hold, it is still possible to obtain the same conclusion as in the theorem except for a finite list of primes ℓ:

Genus	primes excluded
2	$3, 5$
3	$3, 5, 7$
4	$5, 7$
5	$5, 7, 11$
7	$5, 11, 13$
13	$11, 17, 23$

- Generalization to number fields (in progress: A. and Yvon).

Remarks

- If $(2\mathrm{G}+\epsilon)$ does not hold, it is still possible to obtain the same conclusion as in the theorem except for a finite list of primes ℓ:

Genus	primes excluded
2	$3, 5$
3	$3, 5, 7$
4	$5, 7$
5	$5, 7, 11$
7	$5, 11, 13$
13	$11, 17, 23$

- Generalization to number fields (in progress: A. and Yvon).
- For each g which satisfies $(2\mathrm{G}+\epsilon)$ there exists a **positive density** of $f(x) \in \mathbb{Z}[x]$ as in the previous theorem.

Remarks

- If $(2\mathrm{G}+\epsilon)$ does not hold, it is still possible to obtain the same conclusion as in the theorem except for a finite list of primes ℓ:

Genus	primes excluded
2	$3, 5$
3	$3, 5, 7$
4	$5, 7$
5	$5, 7, 11$
7	$5, 11, 13$
13	$11, 17, 23$

- Generalization to number fields (in progress: A. and Yvon).
- For each g which satisfies $(2\mathrm{G}+\epsilon)$ there exists a **positive density** of $f(x) \in \mathbb{Z}[x]$ as in the previous theorem.

Notation: let $C/\mathbb{Q} : y^2 = f(x)$ be an hyperelliptic curve with $f(x) \in \mathbb{Z}[x]$ monic, squarefree and of degree $2g+2$. Let $J = \mathrm{Jac}(C)$.

Example: $g = 6$

$$\begin{aligned} f_0(x) = x^{14} + & \quad 1122976550518058592759939074\, x^{13} + \quad 10247323490706358348644352\, x^{12} + \\ + & \quad 1120184609916242124087443456\, x^{11} + \quad 18639829036478600092188672 0\, x^{10} + \\ + & \quad 1685990245699349559300014080\, x^{9} + \quad 38752995267265358593549926 4\, x^{8} + \\ + & \quad 1422826957983635547417870336\, x^{7} + \quad 58598399862542999730803507 2\, x^{6} + \\ + & \quad 607434202225985243206107136\, x^{5} + \quad 18202102475505020075570298 88\, x^{4} + \\ + & \quad 533014336994715937945092096\, x^{3} + \quad 59580340515494294587975270 4\, x^{2} + \\ + & \quad 127684591382595558689905049 6\, x + \quad 13236723818180308138226688 00. \end{aligned}$$

$$N = p_t^2 \cdot p_t'^2 \cdot p_{lin} \cdot p_{irr} \cdot p_2^2 \cdot p_2'^2 \cdot p_3^3 \cdot p_3'^3 \cdot 2^{2g+2} \cdot \prod_{3 \le p \le g} p^2 =$$

$$= 7^2 \cdot 11^2 \cdot 23 \cdot 29 \cdot 19^2 \cdot 41^2 \cdot 37^3 \cdot 17^3 \cdot 2^{14} \cdot 3^2 \cdot 5^2 = 2201590757511816436065484800$$

For all $f(x) \in \mathbb{Z}[x]$ such that

1. $f(x) \equiv f_0(x) \bmod N$, and
2. C is semistable at all primes $p \nmid N$ (e.g. $f = f_0$).

$$\mathrm{Gal}(\mathbb{Q}(J[\ell])/\mathbb{Q}) \cong \begin{cases} \mathrm{GSp}_{12}(\mathbb{F}_\ell) & \text{for all primes } \ell \neq 2 \\ S_{14} & \text{for } \ell = 2. \end{cases}$$

Subgroups of $\mathsf{GSp}_{2g}(\mathbb{F}_\ell)$

Transvection

Definition

Let $(V, \langle\ ,\ \rangle)$ *be a finite-dimensional symplectic vector space over* $\mathbb{F}_\ell$*. A* **transvection** *is an element* $T \in \mathrm{GSp}(V, \langle\ ,\ \rangle)$ *which fixes a hyperplane* $H \subset V$*.*

Transvection

Definition

Let $(V, \langle\ ,\ \rangle)$ be a finite-dimensional symplectic vector space over $\mathbb{F}_\ell$. A **transvection** *is an element $T \in \mathrm{GSp}(V, \langle\ ,\ \rangle)$ which fixes a hyperplane $H \subset V$.*

When does $\overline{\rho}_{J,\ell}(G_{\mathbb{Q}})$ contain a transvection?

Let $p \neq \ell$ be an odd prime such that

Transvection

Definition

Let $(V, \langle\ ,\ \rangle)$ be a finite-dimensional symplectic vector space over $\mathbb{F}_\ell$. A **transvection** *is an element $T \in \mathrm{GSp}(V, \langle\ ,\ \rangle)$ which fixes a hyperplane $H \subset V$.*

When does $\overline{\rho}_{J,\ell}(G_{\mathbb{Q}})$ contain a transvection?

Let $p \neq \ell$ be an odd prime such that

- p does not divide the leading coefficient of f

Transvection

Definition

Let $(V, \langle\ ,\ \rangle)$ be a finite-dimensional symplectic vector space over $\mathbb{F}_\ell$. A **transvection** *is an element $T \in \mathrm{GSp}(V, \langle\ ,\ \rangle)$ which fixes a hyperplane $H \subset V$.*

When does $\overline{\rho}_{J,\ell}(G_{\mathbb{Q}})$ contain a transvection?

Let $p \neq \ell$ be an odd prime such that

- p does not divide the leading coefficient of f
- f modulo p has one root in $\overline{\mathbb{F}}_p$ having multiplicity precisely 2, with all other roots simple

Transvection

Definition

Let $(V, \langle\ ,\ \rangle)$ *be a finite-dimensional symplectic vector space over* $\mathbb{F}_\ell$. *A* **transvection** *is an element* $T \in \mathrm{GSp}(V, \langle\ ,\ \rangle)$ *which fixes a hyperplane* $H \subset V$.

When does $\overline{\rho}_{J,\ell}(G_{\mathbb{Q}})$ contain a transvection?

Let $p \neq \ell$ be an odd prime such that

- p does not divide the leading coefficient of f
- f modulo p has one root in $\overline{\mathbb{F}}_p$ having multiplicity precisely 2, with all other roots simple

then $\overline{\rho}_{J,\ell}(G_{\mathbb{Q}})$ contains a transvection (Grothendieck, Hall).

Classification of subgroups of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ with a transvection

Theorem (Arias-de-Reyna, Dieulefait and Wiese; Hall)

Let $\ell \geq 5$ be a prime and let V a symplectic $\mathbb{F}_\ell$-vector space of dimension $2g$. Let G be a subgroup of $\mathrm{GSp}(V)$ such that:

(*i*) *G contains a* **transvection**;

(*ii*) *V is an $\mathbb{F}_\ell$* **irreducible** *G-module;*

(*iii*) *V is a* **primitive** *G-module.*

Then G contains $\mathrm{Sp}(V)$. The same holds true for $\ell = 3$, provided that $V \otimes \overline{\mathbb{F}}_3$ is an irreducible and primitive G-module.

Classification of subgroups of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ with a transvection

Theorem (Arias-de-Reyna, Dieulefait and Wiese; Hall)

Let $\ell \geq 5$ be a prime and let V a symplectic $\mathbb{F}_\ell$-vector space of dimension $2g$. Let G be a subgroup of $\mathrm{GSp}(V)$ such that:

(*i*) *G contains a* **transvection**;

(*ii*) *V is an $\mathbb{F}_\ell$* **irreducible** *G-module;*

(*iii*) *V is a* **primitive** *G-module.*

Then G contains $\mathrm{Sp}(V)$. The same holds true for $\ell = 3$, provided that $V \otimes \overline{\mathbb{F}}_3$ is an irreducible and primitive G-module.

Transvection: it is enough to require that $f(x)$ has type $1 - \{2\}$ at some prime.

Type $t - \{q_1, \ldots, q_k\}$

Definition

Let $t \in \mathbb{Z}_{>0}$. We say that

$$f(x) = \sum_{i=0}^{m} a_i x^i \in \mathbb{Z}_p[x]$$

is a t-Eisenstein polynomial of degree $m \in \mathbb{Z}_{>0}$ if

- *$f(x)$ is monic,*
- *$\mathrm{ord}_p(a_i) \geq t$ for all $i \neq m$,*
- *$\mathrm{ord}_p(a_0) = t$.*

Definition

Let q be prime number and let $t \in \mathbb{Z}_{>0}$. Let $f(x) \in \mathbb{Z}_p[x]$ be a monic squarefree polynomial.

Then $f(x)$ is of type $t - \{q\}$ if

$$f(x) = h(x)\, g(x - \alpha) \text{ over } \mathbb{Z}_p[x], \text{ where}$$

- $\alpha \in \mathbb{Z}_p$
- $g(x) \in \mathbb{Z}_p[x]$ *is a t-Eisenstein polynomial of degree q,*
- *the reduction of h, denoted by $\overline{h}(x)$, is separable and $\overline{h(\alpha)} \neq 0$.*

Definition

Let q_1, q_2 be prime numbers and let $t \in \mathbb{Z}_{>0}$. Let $f(x) \in \mathbb{Z}_p[x]$ be a monic squarefree polynomial.

Then $f(x)$ is of type $t - \{q_1, q_2\}$ if

$$f(x) = h(x)\, g_1(x - \alpha_1)\, g_2(x - \alpha_2) \text{ over } \mathbb{Z}_p[x], \text{ where}$$

- *for some $\alpha_1, \alpha_2 \in \mathbb{Z}_p$ with $\overline{\alpha}_1 \neq \overline{\alpha}_2$ (reduction)*
- *$g_1(x) \in \mathbb{Z}_p[x]$ is a t-Eisenstein polynomial of degree q_1,*
- *$g_2(x) \in \mathbb{Z}_p[x]$ is a t-Eisenstein polynomial of degree q_2,*
- *$\overline{h}(x)$ is separable and such that $\overline{h(\alpha_i)} \neq 0$ for $i = 1, 2$.*

Congruences

The notion of type can be expressed in terms of congruence conditions.

Back to the example

$$
\begin{aligned}
f_0(x) = x^{14} + & \quad 112297655051805859275993907 4 \, x^{13} + & 10247323490706358348644352 \, x^{12} + \\
+ & \quad 112018460991624212408744345 6 \, x^{11} + & 18639829036478600092188672 0 \, x^{10} + \\
+ & \quad 168599024569934955930001408 0 \, x^{9} + & 38752995267265358593549926 4 \, x^{8} + \\
+ & \quad 142282695798363554741787033 6 \, x^{7} + & 58598399862542999730803507 2 \, x^{6} + \\
+ & \quad 607434202225985243206107136 \, x^{5} + & 18202102475505020075570298 88 \, x^{4} + \\
+ & \quad 533014336994715937945092096 \, x^{3} + & 59580340515494294587975270 4 \, x^{2} + \\
+ & \quad 127684591382595558689905049 6 \, x + & 13236723818180308138226688 00.
\end{aligned}
$$

$$f_0 \equiv (x^{12} + 2x^8 + \cdots + 3) \cdot (x^2 - 7) \bmod 7^2 \qquad \text{type } 1 - \{2\} \quad \text{at } 7$$

$$f_0 \equiv (x^{12} + x^8 + \cdots + 2) \cdot (x^2 - 11) \bmod 11^2 \qquad \text{type } 1 - \{2\} \quad \text{at } 11$$

$$f_0 \equiv (x^7 - 19) \cdot ((x-1)^7 - 19) \bmod 19^3 \qquad \text{type } 1 - \{7,7\} \quad \text{at } 19$$

$$f_0 \equiv (x^{11} - 41) \cdot ((x-1)^3 - 41) \bmod 41^3 \qquad \text{type } 1 - \{3,11\} \quad \text{at } 41$$

$$f_0 \equiv (x^{13} - 37^2) \cdot (x+1) \bmod 37^3 \qquad \text{type } 2 - \{13\} \quad \text{at } 37$$

$$f_0 \equiv (x^{11} - 17^2) \cdot (x^3 + x + 14) \bmod 17^3 \qquad \text{type } 2 - \{11\} \quad \text{at } 17$$

Transvection: if $f(x)$ has type $1 - \{2\}$ at some prime $p \neq \ell$ then the local Galois group at p contains a transvection in its action on $J[\ell]$.

Overview of the proof

Main Idea: study inertia

Study the Galois representations $H^1_{\acute{e}t}(C, \mathbb{Q}_\ell)$ and $J[\ell]$ as representations of local Galois groups.

$\ell \neq p$: we use the method of clusters, recently introduced by Dokchitser T., Dokchitser V., Maistret and Morgan.

$\ell = p$: theory of fundamental characters (Serre, Raynaud).

If $f(x)$ is of **type** $t - \{q_1, \ldots, q_k\}$ at a prime p then we have control over the **image of the inertia subgroup** at p.

Theorem (Arias-de-Reyna, Dieulefait and Wiese; Hall)

Let $\ell \geq 5$ be a prime and let V a symplectic $\mathbb{F}_\ell$-vector space of dimension $2g$. Let G be a subgroup of $\mathrm{GSp}(V)$ such that:

(*i*) *G contains a* **transvection**; $\Longleftarrow$ *type* $1 - \{2\}$

(*ii*) *V is an $\mathbb{F}_\ell$* **irreducible** *G-module;* $\Longleftarrow$ *types and* $(2\mathrm{G} + \epsilon)$

(*iii*) *V is a* **primitive** *G-module.* $\Longleftarrow$ *quasi-unramified, p-admissibility*

Then G contains $\mathrm{Sp}(V)$. The same holds true for $\ell = 3$, provided that $V \otimes \overline{\mathbb{F}}_3$ is an irreducible and primitive G-module.

We cannot always guarantee that $H^1_{\acute{e}t}(C, \mathbb{Q}_\ell)$ and $J[\ell]$ are locally irreducible so we use the notion of type.

Irreducibility

Lemma

Let p_2 be an odd prime. Suppose that $f \in \mathbb{Z}_{p_2}[x]$ has type $1 - \{q_1, q_2\}$ where q_1, q_2 are odd primes, coprime to p_2, and such that $2g + 2 = q_1 + q_2$. Suppose that p_2 is a primitive root modulo q_1 and modulo q_2. Then for every prime $\ell \neq p_2, q_1, q_2$ we have

$$(J[\ell] \otimes_{\mathbb{F}_\ell} \overline{\mathbb{F}}_\ell)_{ss} = M_1 \oplus M_2$$

where M_i are $(q_i - 1)$-dimensional irreducible $G_{\mathbb{Q}}$-subrepresentations.

We prove irreducibility by requiring that $f(x)$ has type $2 - \{q_3\}$ at an odd prime p_3, primitive root modulo q_3. In order to conclude for all primes we require "double Goldbach".

Generalisations: number fields

Totally real fields

The inverse Galois problem over a totally real field

Let G be a finite group and let K be totally real field. Does there exist a Galois extension L/K such that $\mathrm{Gal}(L/K) \cong G$?

Totally real fields

The inverse Galois problem over a totally real field

Let G be a finite group and let K be totally real field. Does there exist a Galois extension L/K such that $\mathrm{Gal}(L/K) \cong G$?

Let us pick a prime ℓ and consider $G = \mathrm{GL}_2(\mathbb{F}_\ell)$.

Semistable elliptic curves

Theorem (Serre)

If $E/\mathbb{Q}$ is a semistable elliptic curve without CM, then $\overline{\rho}_{E,\ell}$ is surjective for any prime $\ell \geq 11$.

Totally real fields

Let K be a totally real field.

Let S be a finite set of non-archimedean places of K.

Totally real fields

Let K be a totally real field.

Let S be a finite set of non-archimedean places of K.

Theorem (A., Siksek)

There are an effectively computable constant $C_{K,S}$, depending only on K and S, and a finite computable set $E_1, \ldots, E_n$ of elliptic curves over K with CM such that the following holds.

If E is an elliptic curve over K semistable outside S, and $\ell > C_{K,S}$ is prime, then either $\overline{\rho}_{E,\ell}$ is surjective, or $\overline{\rho}_{E,\ell} \sim \overline{\rho}_{E_i,\ell}$ for some $i = 1, \ldots, n$.

Totally real fields

Let K be a totally real field.

Let S be a finite set of non-archimedean places of K.

Theorem (A., Siksek)

There are an effectively computable constant $C_{K,S}$, depending only on K and S, and a finite computable set $E_1, \ldots, E_n$ of elliptic curves over K with CM such that the following holds.

If E is an elliptic curve over K semistable outside S, and $\ell > C_{K,S}$ is prime, then either $\overline{\rho}_{E,\ell}$ is surjective, or $\overline{\rho}_{E,\ell} \sim \overline{\rho}_{E_i,\ell}$ for some $i = 1, \ldots, n$.

Over totally real fields we can apply **modularity** and **level lowering** theorems to semistable elliptic curves E/K whose mod ℓ image is contained in the normalizer of a Cartan subgroup.

Modularity

Definition (Modularity)

Let K be a totally real number field, and let E/K be an elliptic curve.

Modularity

Definition (Modularity)

Let K be a totally real number field, and let E/K be an elliptic curve.

E is **modular** *if there exists a Hilbert cuspidal eigenform $\mathfrak{f}$ over K of parallel weight 2, with rational Hecke eigenvalues, such that*

$$L(E/K, s) = L(\mathfrak{f}, s).$$

Modularity

Definition (Modularity)

Let K be a totally real number field, and let E/K be an elliptic curve.

E is **modular** *if there exists a Hilbert cuspidal eigenform $\mathfrak{f}$ over K of parallel weight 2, with rational Hecke eigenvalues, such that*

$$L(E/K, s) = L(\mathfrak{f}, s).$$

It is conjectured that all elliptic curves over totally real fields are modular.

Modularity

Definition (Modularity)

Let K be a totally real number field, and let E/K be an elliptic curve.

E is **modular** *if there exists a Hilbert cuspidal eigenform $\mathfrak{f}$ over K of parallel weight 2, with rational Hecke eigenvalues, such that*

$$L(E/K, s) = L(\mathfrak{f}, s).$$

It is conjectured that all elliptic curves over totally real fields are modular.

Modularity has been proved for elliptic curves over **real quadratic fields** by Freitas, Le Hung and Siksek and over **real cubic fields** by Derickx, Najman and Siksek.

Let K be a totally real field. Let S be a finite set of non-archimedean places of K and let E/K be an elliptic curve semistable outside S.

Let K be a totally real field. Let S be a finite set of non-archimedean places of K and let E/K be an elliptic curve semistable outside S.

Let $\ell \geq 7$ be a prime unramified in K. Suppose that E is semistable at some prime v of K above ℓ.

Let K be a totally real field. Let S be a finite set of non-archimedean places of K and let E/K be an elliptic curve semistable outside S.

Let $\ell \geq 7$ be a prime unramified in K. Suppose that E is semistable at some prime υ of K above ℓ.

Proposition (A., Siksek)

If $\overline{\rho}_{E,\ell}$ is irreducible but not surjective then E is modular.

Isogenies

Extra: isogenies

Theorem (A.)

Let K be a totally real field with $h_K = h_K^+$. Let M be a bound for the order of torsion points for elliptic curves over K. Let $u_1, \ldots, u_n$ be a basis for the totally positive units in K and let

$$B = \gcd(B_T(u_i)) \quad \text{for } 1 \leq i \leq n, T \subset \mathrm{Gal}(K/\mathbb{Q}), T \neq \emptyset.$$

If $\ell > M$ and $\ell \nmid B$ then no semistable elliptic curves over K admits an ℓ-isogeny.

Extra: isogenies

Theorem (A.)

Let K be a totally real field with $h_K = h_K^+$. Let M be a bound for the order of torsion points for elliptic curves over K. Let $u_1, \ldots, u_n$ be a basis for the totally positive units in K and let

$$B = \gcd(B_T(u_i)) \quad \text{for } 1 \leq i \leq n, T \subset \mathrm{Gal}(K/\mathbb{Q}), T \neq \emptyset.$$

If $\ell > M$ and $\ell \nmid B$ then no semistable elliptic curves over K admits an ℓ-isogeny.

Example

Let $p = 5, 7, 11$ or 13 and $K = \mathbb{Q}(\sqrt{p})$, then $B = 1$ and $M = 18$ (Kamienny, Kenku, Momose, Najman).

Reducible representations & isogenies

Goal:

Want to bound ℓ such that $\overline{\rho}_{E,\ell}$ is reducible.

Hypotheses:

1. E/K **semistable** elliptic curve, over K, a Galois totally real field.
2. ℓ rational prime **unramified** in K.
3. If $\overline{\rho}_{E,\ell}$ is reducible: $\overline{\rho}_{E,\ell} \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}$, $\psi_i : G_K \to \mathbb{F}_\ell^\times$.

If $\overline{\rho}_{E,\ell}$ is reducible: $\overline{\rho}_{E,\ell} \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}$, $\psi_i : G_K \to \mathbb{F}_\ell^\times$.

Fact: $v \nmid \ell$, v finite $\implies$ $\overline{\rho}_{E,\ell}|_{I_v} \sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$.

Hence ψ_1, ψ_2 are **unramified** at all finite $v \nmid \ell$ (i.e. $\psi_i|_{I_v} = 1$).

Serre: $v \mid \ell$ $\implies$ $\overline{\rho}_{E,\ell}|_{I_v} \sim \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} 1 & * \\ 0 & \chi \end{pmatrix}$

$\chi : G_K \to \mathbb{F}_\ell^\times$ is the **mod ℓ cyclotomic character:** $\zeta_\ell^\sigma = \zeta_\ell^{\chi(\sigma)}$.

Let

$$S_\ell = \{v : v \mid \ell\}, \qquad S = \{ v \in S_\ell : \psi_1|_{I_v} = \chi|_{I_v} \}.$$

$S = \emptyset$

Lemma

Suppose $h_K^+ = h_K$ and $S = \emptyset$. Then $E(K)[\ell] \neq 0$.

Proof.

$$S = \emptyset \implies \psi_1 : G_K \to \mathbb{F}_\ell^\times \text{ is unramified at all finite places}$$
$$\implies \psi_1 = 1.$$

$$\overline{\rho}_{E,\ell} : G_K \to \mathrm{Aut}(E[\ell]) \cong \mathrm{GL}_2(\mathbb{F}_\ell), \qquad \overline{\rho}_{E,\ell} \sim \begin{pmatrix} 1 & * \\ 0 & \psi_2 \end{pmatrix}.$$

□

Bound on ℓ by Merel's uniform boundedness theorem.

$S = S_\ell$

Lemma

Suppose $h_K^+ = h_K$ and $S = S_\ell$. Then $E'(K)[\ell] \neq 0$, where E' is ℓ-isogenous to K.

Proof.

$$\overline{\rho}_{E,\ell} \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}, \qquad \overline{\rho}_{E',\ell} \sim \begin{pmatrix} \psi_2 & * \\ 0 & \psi_1 \end{pmatrix}.$$

$S = S_\ell \implies \psi_2 : G_K \to \mathbb{F}_\ell^\times$ is unramified at all finite places . . . $\square$

$\emptyset \neq S \subset S_\ell$

- Let $L = K(\psi_1)$. View $\psi_1 : \mathrm{Gal}(L/K) \to \mathbb{F}_\ell^\times$.
- **Local Artin map** $\Theta_v : K_v^\times \to \mathrm{Gal}(L/K)$.
- Let $u \in \mathcal{O}_K$ be a totally positive unit.

$\emptyset \neq S \subset S_\ell$

- Let $L = K(\psi_1)$. View $\psi_1 : \mathrm{Gal}(L/K) \to \mathbb{F}_\ell^\times$.
- **Local Artin map** $\Theta_v : K_v^\times \to \mathrm{Gal}(L/K)$.
- Let $u \in \mathcal{O}_K$ be a totally positive unit.

Compute $\boxed{\psi_1(\Theta_v(u))}$ as v ranges over the places of K.

$\emptyset \neq S \subset S_\ell$

- Let $L = K(\psi_1)$. View $\psi_1 : \mathrm{Gal}(L/K) \to \mathbb{F}_\ell^\times$.
- **Local Artin map** $\Theta_v : K_v^\times \to \mathrm{Gal}(L/K)$.
- Let $u \in \mathcal{O}_K$ be a totally positive unit.

Compute $\boxed{\psi_1(\Theta_v(u))}$ as v ranges over the places of K.

- Suppose $v \mid \infty$. So $\Theta_v(u) = 1$. So $\psi_1(\Theta_v(u)) = 1$.

$\emptyset \neq S \subset S_\ell$

- Let $L = K(\psi_1)$. View $\psi_1 : \mathrm{Gal}(L/K) \to \mathbb{F}_\ell^\times$.
- **Local Artin map** $\Theta_v : K_v^\times \to \mathrm{Gal}(L/K)$.
- Let $u \in \mathcal{O}_K$ be a totally positive unit.

Compute $\boxed{\psi_1(\Theta_v(u))}$ as v ranges over the places of K.

- Suppose $v \mid \infty$. So $\Theta_v(u) = 1$. So $\psi_1(\Theta_v(u)) = 1$.
- Suppose $v \nmid \infty$. By local reciprocity $\Theta_v(u) \in I_v$.

$\emptyset \neq S \subset S_\ell$

- Let $L = K(\psi_1)$. View $\psi_1 : \mathrm{Gal}(L/K) \to \mathbb{F}_\ell^\times$.
- **Local Artin map** $\Theta_v : K_v^\times \to \mathrm{Gal}(L/K)$.
- Let $u \in \mathcal{O}_K$ be a totally positive unit.

Compute $\boxed{\psi_1(\Theta_v(u))}$ as v ranges over the places of K.

- Suppose $v \mid \infty$. So $\Theta_v(u) = 1$. So $\psi_1(\Theta_v(u)) = 1$.
- Suppose $v \nmid \infty$. By local reciprocity $\Theta_v(u) \in I_v$.
  - If $v \notin S$ then $\psi_1(\Theta_v(u)) = 1$.

$\emptyset \neq S \subset S_\ell$

- Let $L = K(\psi_1)$. View $\psi_1 : \mathrm{Gal}(L/K) \to \mathbb{F}_\ell^\times$.
- **Local Artin map** $\Theta_v : K_v^\times \to \mathrm{Gal}(L/K)$.
- Let $u \in \mathcal{O}_K$ be a totally positive unit.

Compute $\boxed{\psi_1(\Theta_v(u))}$ as v ranges over the places of K.

- Suppose $v \mid \infty$. So $\Theta_v(u) = 1$. So $\psi_1(\Theta_v(u)) = 1$.
- Suppose $v \nmid \infty$. By local reciprocity $\Theta_v(u) \in I_v$.
  - If $v \notin S$ then $\psi_1(\Theta_v(u)) = 1$.
  - If $v \in S$ then $\psi_1(\Theta_v(u)) = \chi(\Theta_v(u)) = \mathrm{Norm}_{\mathbb{F}_v/\mathbb{F}_\ell}(u)^{-1}$.

$$\text{Global reciprocity} \implies \prod \Theta_v(u) = 1$$
$$\implies \prod_{v \in S} \mathrm{Norm}_{\mathbb{F}_v/\mathbb{F}_\ell}(u) = \overline{1} \quad (\overline{1} \in \mathbb{F}_\ell).$$

Therefore, there is a **non-empty proper** subset $T \subset \mathrm{Gal}(K/\mathbb{Q})$ such that

$$\ell \mid B_T(u) \qquad B_T(u) := \mathrm{Norm}\left(\left(\prod_{\sigma \in T} u^{\sigma}\right) - 1\right).$$

Therefore, there is a **non-empty proper** subset $T \subset \mathrm{Gal}(K/\mathbb{Q})$ such that

$$\ell \mid B_T(u) \qquad B_T(u) := \mathrm{Norm}\left(\left(\prod_{\sigma \in T} u^{\sigma}\right) - 1\right).$$

Lemma (Freitas–Siksek)

For each non-empty proper subset $T \subset \mathrm{Gal}(K/\mathbb{Q})$, there exists totally positive unit u such that $B_T(u) \neq 0$.

Back to the inverse Galois problem, $\mathbb{Q}(\sqrt{101})$

Let $K = \mathbb{Q}(\sqrt{101})$ and let us realise $G = \mathrm{GL}_2(\mathbb{F}_\ell)$ over K.

Back to the inverse Galois problem, $\mathbb{Q}(\sqrt{101})$

Let $K = \mathbb{Q}(\sqrt{101})$ and let us realise $G = \mathsf{GL}_2(\mathbb{F}_\ell)$ over K.
There is an obstruction coming from the Weil pairing:

$$E : y^2 + (\frac{\sqrt{101}+1}{2})y = x^3 + x^2 - 2x - 7 \quad \text{over } \mathbb{Q}(\sqrt{101})$$
$$\overline{\rho}_{E,\ell}(\mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{101}))) \cong \mathsf{GL}_2(\mathbb{F}_\ell) \quad \forall \text{ prime } \ell \neq 101$$
$$\rho_{E,101}(\mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{101}))) \subseteq D \cdot \mathsf{SL}_2(\mathbb{F}_{101})$$

where D is the set of invertible squares in $\mathbb{F}_{101}$.

Back to the inverse Galois problem, $\mathbb{Q}(\sqrt{101})$

We just realised $G = \mathrm{GL}_2(\mathbb{F}_\ell)$ as a Galois group over $\mathbb{Q}(\sqrt{101})$ for every ℓ, except 101, uniformly, using the torsion of the same elliptic curve.

Back to the inverse Galois problem, $\mathbb{Q}(\sqrt{101})$

We just realised $G = \mathrm{GL}_2(\mathbb{F}_\ell)$ as a Galois group over $\mathbb{Q}(\sqrt{101})$ for every ℓ, except 101, uniformly, using the torsion of the same elliptic curve.

How do we realise $\mathrm{GL}_2(\mathbb{F}_{101})$?

We need to use Hilbert modular forms and local types (Weinstein). This is work in progress.

Generalization: other linear groups

Generalization: other linear groups

Question

Inverse Galois problem for groups like $\mathrm{GL}_2(\mathbb{F}_{\ell^2})$ or $\mathrm{PGL}_2(\mathbb{F}_{\ell^2})$?

Theorem (Wiese)

Assume Maeda's conjecture for classical modular forms. Then for every odd integer d, the set of primes ℓ for which there exists $K/\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{PGL}_2(\mathbb{F}_{\ell^d})$ has density 1.

The inverse Galois problem: abelian varieties, modular forms & Goldbach's conjecture

Samuele Anni

Géométrie algébrique, Théorie des nombres et Applications, GTA2021

19th August 2021

Thank you!