The inverse Galois problem for symplectic groups

Samuele Anni

IWR - Universität Heidelberg

Arithmetic of Hyperelliptic Curves
ICTP, 5$^{\text{th}}$ September 2017

UNIVERSITÄT
HEIDELBERG
ZUKUNFT
SEIT 1386

The inverse Galois problem

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

Aim of this talk

Show that it is possible to **explicitly** realise for all* $g \in \mathbb{Z}_{\geq 1}$, the group $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$, simultaneously for all odd primes ℓ, using the ℓ-torsion of the Jacobian of the same hyperelliptic curve.

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

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

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.

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 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

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

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 $g \geq 4$?

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 $J = \mathrm{Jac}(C)$.

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

- If $(2G + \epsilon)$ 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	$11, 17, 23$

  Recent preprint of Landesman, Swaminathan, Tao, Xu for $g = 2, 3$.
- Generalization to higher degree number fields (work in progress).
- It is possible to prove that for each g which satisfies $(2G + \epsilon)$ there exists a **positive density** of $f(x) \in \mathbb{Z}[x]$ as in the previous theorem.

Example: $g = 6$

$$
\begin{aligned}
f_0(x) = x^{14} + {}& 112297655051805859275993907 4\, x^{13} + 1024732349070635834864 4352\, x^{12} + \\
+ {}& 1120184609916242124087443456\, x^{11} + 1863982903647860009218867 20\, x^{10} + \\
+ {}& 1685990245699349559300014080\, x^{9} + 3875299526726535859354992 64\, x^{8} + \\
+ {}& 1422826957983635547417870336\, x^{7} + 5859839986254299973080350 72\, x^{6} + \\
+ {}& 607434202225985243206107136\, x^{5} + 1820210247550502007557029888\, x^{4} + \\
+ {}& 533014336994715937945092096\, x^{3} + 595803405154942945879752704\, x^{2} + \\
+ {}& 1276845913825955586899050496\, x + 1323672381818030813822668800.
\end{aligned}
$$

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

$$= 7^2 \cdot 11^2 \cdot 23 \cdot 29 \cdot 19^2 \cdot 41^2 \cdot 37^3 \cdot 17^3 \cdot 2^{14} \cdot 3^2 \cdot 5^2 = 220159075751181643606548 4800$$

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. $f = f_0$).

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

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.

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 $i = 1, 2$.*

Definition

Let $f(x) \in \mathbb{Z}[x]$ be a monic squarefree polynomial. We say that f is of **type** $t - \{q_1, \ldots, q_k\}$ *at a prime p if $f(x) \in \mathbb{Z}_p[x]$ is of type $t - \{q_1, \ldots, q_k\}$.*

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

Back to the example

$$\begin{aligned} f_0(x) = x^{14} &+ 112297655051805859275993907 4\, x^{13} + 102473234907063583486443 52\, x^{12} + \\ &+ 1120184609916242124087443456\, x^{11} + 1863982903647860009218867 20\, x^{10} + \\ &+ 1685990245699349559300014080\, x^{9} + 3875299526726535859354992 64\, x^{8} + \\ &+ 1422826957983635547417870336\, x^{7} + 5859839986254299973080350 72\, x^{6} + \\ &+ 607434202225985243206107136\, x^{5} + 18202102475505020075570298 88\, x^{4} + \\ &+ 533014336994715937945092096\, x^{3} + 5958034051549429458797527 04\, x^{2} + \\ &+ 1276845913825955586899050496\, x + 13236723818180308138226688 00. \end{aligned}$$

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

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

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

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

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

$f_0 \equiv (x^{11} - 17^2) \cdot (x^3 + x + 14) \bmod 17^3$ — type $2 - \{11\}$ 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 $J[\ell]$.

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.

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.

Irreducibility

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

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, away from a finite list of primes, requiring that $f(x)$ has type $2 - \{q_3\}$ at an odd prime p_3, that is a primitive root modulo q_3. In order to conclude for all primes we require "double Goldbach".

The inverse Galois problem for symplectic groups

Samuele Anni

IWR - Universität Heidelberg

Arithmetic of Hyperelliptic Curves
ICTP, 5^{th} September 2017

Thanks!