Efficient irreducibility of residual Galois representations of abelian surfaces with RM over $\mathbb{Q}$

Timo Keller
Universität Bayreuth

Setup and basic properties

- Let A be a principally polarized abelian *surface* over $\mathbb{Q}$ with RM by $\mathcal{O}$ over $\mathbb{Q}$ and $\mathbb{Q}$.
- A is *absolutely simple* and hence $\mathbb{Q}$-isomorphic to $\mathrm{Jac}_{C/\mathbb{Q}}$ for a unique genus-2 curve C (Torelli + $\dim \mathscr{M}_2 = 3 = \dim \mathscr{A}_{2,1,1}$).
- A is of GL_2-type over $\mathbb{Q}$ and hence *modular* of some level N (Ribet + Serre's modularity conjecture).

Computationally feasible effective irreducibility of $\rho_\mathfrak{p}$

Question: Which $\rho_\mathfrak{p} : G_\mathbb{Q} \to \mathrm{Aut}(A[\mathfrak{p}])$ are irreducible for $\mathfrak{p} \mid p$ a finite prime of $\mathcal{O}$?

Theorem [Rib76]**:** All but finitely many $\rho_\mathfrak{p}$ are absolutely irreducible. Disadvantage: *ineffective*

Theorem [DL14]**:** Effective, but *computationally infeasible* upper bound on $|\mathfrak{p}|$ depending on the stable Faltings height of A.

Goal

For a *concretely* given A of **dimension 2**, *efficiently* determine the p with $\rho_\mathfrak{p}$ irreducible for all $\mathfrak{p} \mid p$.

- **Adapt Dieulefait's algorithm** [Die02] for $\mathrm{End}_\mathbb{Q}(A) = \mathbb{Z}$ to real multiplication by $\mathcal{O}$, distinguish by decomposition type of p in $\mathcal{O}$: Either p is inert or it all primes above it have degree 1.
- $A[p]$ is a free $\mathcal{O}/p[\mathrm{Gal}_\mathbb{Q}]$-module of rank 2.
- Need to know the characteristic polynomials of the Frobenii at $\ell \neq p$ acting on $A[p]$: Local zeta function of the associated curve C.
- Raynaud's theorem [Ray74] also holds for $p \parallel N$ of semiabelian reduction! The toric part is unramified.

Theorem (square-free level)

Assume that the level N is *square-free*. If p is a prime for which the localization $\mathcal{O}_\mathfrak{p}$ is a DVR for all $\mathfrak{p} \mid p$, $\rho_\mathfrak{p}$ is reducible for some $\mathfrak{p}$ if and only if $A'(\mathbb{Q})[p] \neq 0$ for some A' $\mathbb{Q}$-isogenous to A (via an isogeny with kernel contained in $A[\mathfrak{p}]$).

- For a prime $2 < \ell \neq p$ of good reduction, $A'(\mathbb{Q})[p] \mid \#A'(\mathbb{F}_\ell) = \#A(\mathbb{F}_\ell)$, so $A'(\mathbb{Q})[p] \neq 0$ can be checked without actually knowing A'. This gives effectively finitely many $\mathfrak{p}$ with $\rho_\mathfrak{p}$ reducible.
- We can also algorithmically treat N not square-free, but with less precise results.

Semistable example: $A = \mathrm{Jac}(X_0(35)/\langle w_7 \rangle)$ (easier)

A is the 2-dimensional isogeny factor of $J_0(35)$. It is semistable and absolutely simple with real multiplication by the ring of integers $\mathcal{O}$ of $\mathbb{Q}(\sqrt{17})$ over $\mathbb{Q}$.

Result

$A(\mathbb{Q})[2] = \mathbb{Z}/2$ and $\rho_\mathfrak{p}$ is reducible exactly for one of the primes over 2 of $\mathcal{O}$.

Corollary: Since $\mathcal{O}$ is a PID, A has no cyclic isogenies of prime power degree other than endomorphisms, except for the prime 2.

Non-semistable example: $A = \mathrm{Jac}(X_0(125)/\langle w_5 \rangle)$ (more diffcult)

A is absolutely simple with real multiplication by the ring of integers $\mathcal{O}$ of $\mathbb{Q}(\sqrt{5})$ over $\mathbb{Q}$, but *not* semistable.

Result

$A(\mathbb{Q})_{\mathrm{tors}} = 0$ and $\rho_\mathfrak{p}$ is irreducible except perhaps for one of the primes over 3 (good reduction) and 5 (split multiplicative reduction) of $\mathcal{O}$.

Corollary: Since $\mathcal{O}$ is a PID, A has no cyclic isogenies of prime power degree other than endomorphisms, except perhaps for the primes 3 and 5.

Computational problem

Either find a means to compute these extra isogenies or prove that they cannot exist.
Calculations on the *Kummer surface* show: For $p = 3$ inert in $\mathcal{O}$, ρ_3 is irreducible.

References

[Die02] Luis V. Dieulefait, *Explicit determination of the images of the Galois representations attached to abelian surfaces with* $\mathrm{End}(A) = \mathbb{Z}$, Experiment. Math. **11** (2002), no. 4, 503–512 (2003).

[DL14] Davide Lombardo, *Explicit surjectivity of Galois representations attached to abelian surfaces and* GL_2*-varieties*, 2014. Preprint, arXiv:1411.1703.

[Ray74] Michel Raynaud, *Schémas en groupes de type* $(p, \ldots, p)$, Bull. Soc. Math. France **102** (1974), 241–280 (French).

[Rib76] Kenneth A. Ribet, *Galois action on division points of Abelian varieties with real multiplications*, Amer. J. Math. **98** (1976), no. 3, 751–804.

LaTeX TikZposter