Galois Representations Attached to Curves

Ricky Magner

1 Motivation and Definitions

Galois representations have become a central part of modern number theory. They have provided a uniform language for generalizing reciprocity laws, studying rational points on varieties, and describing characteristics of certain natural L-functions. One of the most famous applications comes from the modularity theorem, from which Fermat's Last Theorem was deduced as a consequence.

Notation. Throughout, we will let F be a finite extension of $\mathbb{Q}$, and fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Identify $\overline{F}$ with $\overline{\mathbb{Q}}$ and let $G_F = \mathrm{Gal}(\overline{F}/F)$.

Definition 1. *A representation of G_F (over K) is a finite dimensional K-vector space along with a group homomorphism $\rho : G_F \to GL(V)$.*

The first source of these comes from E/F a finite Galois extension. Then E is a finite dimensional F-vector space, so the canonical action of G_F on E gives a representation which factors through $\mathrm{Gal}(E/F)$, a discrete group. In general, G_F is a profinite group, equipped with the natural topology. So when K is a topological field, we will assume all of our representations are continuous where $GL(V)$ inherits the topology of $GL_n(K)$.

The second source of Galois representations will be the focus of this paper. These are the ones which come from geometry. For this, we give an example to illustrate the principle.

Example. Let E be an elliptic curve over F. Write $E[n]$ for the subgroup of n-torsion points of E. Then the coordinates of $E[n]$ are defined over a Galois extension of F, and the natural action on the coordinates commutes with the group law on E. Thus we have a group action of G_F on $E[n]$. But we also know that $E[n] \simeq (\mathbb{Z}/n\mathbb{Z})^2$, so when $n = p$ is prime, $E[p]$ is a 2-dimensional $\mathbb{F}_p$-vector space. This means that $E[p]$ is a 2-dimensional representation of G_F over $\mathbb{F}_p$.

For concreteness, we will compute a specific example. Let $E : y^2 = x^3 + 6$. Then the third division polynomial is $x^4 + 24x = 0$, so the x-coordinates of

the 3-torsion are 0 and all cube roots of -24. Let ω be a nontrivial cube root of unity. Then

$$E[3] = \{(0, \pm\sqrt{6}), (-2\sqrt[3]{3}, \pm 3\sqrt{-3}), (-2\omega\sqrt[3]{3}, \pm 3\sqrt{-3}), (-2\omega^2\sqrt[3]{3}, \pm 3\sqrt{-3}), \mathcal{O}\}.$$

If we write $L = \mathbb{Q}(E[3])$ for the number field generated by the coordinates above, we see that $L = \mathbb{Q}(\omega, \sqrt[3]{3}, \sqrt{6})$, a degree 12 extension. Hence the map $G_{\mathbb{Q}} \to E[3]$ factors through $\mathrm{Gal}(L/\mathbb{Q}) \to E[3]$ and has image of size 12 in $\mathrm{GL}_2(\mathbb{F}_3)$ (after choosing a basis for $E[3]$).

We can do a similar computation for $E[n]$ for any n, but the computations become unwieldy to perform by hand quickly. Theoretically, however, we can form the group $E[p^n]$ for all n, and these fit together into an inverse system under the map $E[p^{n+1}] \to E[p^n]$ by multiplication by p. By identifying each with $(\mathbb{Z}/p^n\mathbb{Z})^2$ and taking an inverse limit, we form the Tate module $T_p(E) := \varprojlim_n E[p^n]$. This inherits a (continuous) action of G_F on $T_p(E) \simeq \mathbb{Z}_p^2$. Tensoring with $\mathbb{Q}_p$ gives $V_p(E) := T_p(E) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

The surprising fact is that the Galois representation $V_p(E)$ contains a huge amount of information about E.

Definition 2. *Let V be a variety over $\mathbb{F}_q$ for $q = p^n$. Then the zeta function $Z(V, T)$ associated to V is defined as*

$$Z(V, T) = \exp\left(\sum_{i=1}^{\infty} \#V(\mathbb{F}_{q^i})T^i/i\right).$$

The Weil conjectures tell us a lot of valuable information about $Z(V, T)$ in general, but the story for elliptic curves was known long ago (conjectured by Artin and proven by Hasse). Specifically, in the case of E over $\mathbb{F}_p$, we have

$$Z(E, T) = \frac{1 - a_pT + pT^2}{(1 - T)(1 - pT)},$$

for some $a_p \in \mathbb{Z}$ with $|a_p| \leq 2\sqrt{p}$. The relation to Galois representations comes from the fact that a_p is actually the trace of the (conjugacy class of) Frob_p acting on $V_p(\tilde{E})$ for $\tilde{E}$ some elliptic curve over F whose reduction is E modulo p. But at the same time, we also have $|\#E(\mathbb{F}_p) - (p + 1)| = |a_p|$, so the Tate module counts points on $\tilde{E}$ modulo various primes (of good reduction).

The Tate module can be generalized to any algebraic variety via the étale cohomology. Specifically, for X a projective variety over F, ℓ a prime, there exist (nonzero) finite dimensional $\mathbb{Q}_\ell$-vector spaces $H^i_{\text{ét}}(X, \mathbb{Q}_\ell)$ associated to X functorially. Given $\sigma \in G_F$, we have a morphism $\sigma : X \to X$ in the natural

way, so we get an induced map $\sigma^* : H^i_{\text{ét}}(X, \mathbb{Q}_\ell) \to H^i_{\text{ét}}(X, \mathbb{Q}_\ell)$. In other words, $H^i_{\text{ét}}(X, \mathbb{Q}_\ell)$ is a Galois representation, and it turns out $H^1_{\text{ét}}(E, \mathbb{Q}_\ell) \simeq V_\ell(E)^*$ (the dual space of the Tate module) in the case where $X = E$ is an elliptic curve.

2 Theoretical Results

In this section we will present some known results regarding the above constructions, particularly in the case of curves. The following theorem was a consequence of Faltings's proof of the Mordell conjecture.

Theorem 3. *Let A and B be abelian varieties over the number field F. If $V_p(A) \simeq V_p(B)$ as G_F-representations, then A and B are isogenous (over $\overline{F}$).*

This says that the Galois representations associated to abelian varieties should "know" all of their isogeny invariants. However, the question of how to access those from the Galois representation alone is answered by a few major theorems, and in some cases still only conjecturally. We will provide a few here, continuing with the theme of counting points modulo p.

2.1 Counting Points

As was motivated with the example of elliptic curves above, Galois representations can be used to count points on varieties over finite fields.

Theorem 4. *Let C be a curve of genus g over F with good reduction at $\mathfrak{p} \subset \mathcal{O}_F$, and $\mathcal{O}_F/\mathfrak{p} \simeq \mathbb{F}_q$. Let $\{\alpha_i\}_{i=1}^{2g}$ be the eigenvalues of $Frob_\mathfrak{p}$ acting on $H^1_{ét}(C, \mathbb{Q}_\ell)$ for $\mathfrak{p} \nmid \ell$. Then if $\overline{C}$ is the reduction of C modulo $\mathfrak{p}$, we have $|\#\overline{C}(\mathbb{F}_q) - (q+1)| = |\sum_{i=1}^{2g} \alpha_i|$.*

This follows from some formalism of étale cohomology (in particular the Lefschetz fixed point theorem). The Weil conjectures tell us about the eigenvalues mentioned in the theorem. In particular, we have $|\#\overline{C}(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}$ where g is the genus of C.

We can apply this to counting points on Jacobians of curves over finite fields as well. Let $P_C(T)$ be the numerator of the zeta function attached to $\overline{C}$. Write $J(C)$ for the Jacobian of C. Then we have $\#\overline{J(C)}(\mathbb{F}_q) = P_C(1)$. The right side can be computed as an expression in the eigenvalues of Frobenius elements acting on a vector space as described in the theorem. This result comes from the fact that $H^n_{\text{ét}}(J(C), \mathbb{Q}_\ell) = \wedge^n H^1(C, \mathbb{Q}_\ell)$ (using a theorem about Hopf algebras) and the Lefschetz fixed point theorem.

2.2 Endomorphism Rings

Let $\mathrm{End}(E)$ be the endomorphism ring of an elliptic curve E over F a number field. Then it is known either $\mathrm{End}(E)$ is an order in an imaginary quadratic extension of $\mathbb{Q}$ ("E has CM") or $\mathrm{End}(E) = \mathbb{Z}$ ("E doesn't have CM"). Elliptic curves with CM have various special properties. One of them is the following application to Galois theory.

Theorem 5 (Kronecker's Jugendraum)**.** *Let E be an elliptic curve over a number field F with CM by $\mathcal{O}_K$, where K is an imaginary quadratic extension of $\mathbb{Q}$. Then*

$$K^{ab} = \cup_{n \geq 1} K(j(E), E[n]),$$

where $j(E)$ is the j-invariant of E.

This tells us that adjoining n-torsion of E to K as above generates all abelian extensions of K (after adjoining $j(E)$). But this means that $\rho : G_F \to Aut(E[p]) \simeq \mathrm{GL}_2(\mathbb{F}_p)$ can not be surjective in general ($p > 2$), because the image must be abelian. So if ρ is surjective for some p sufficiently large, E cannot have CM.

Conversely, a famous theorem of Serre tells us more.

Theorem 6. *Let E be an elliptic curve without CM over a number field F. Then $\rho : G_F \to GL_2(\mathbb{F}_p)$ is surjective for p sufficiently large.*

Over finite fields, there is a similar dichotomy. If $\overline{E}$ is an elliptic curve over $\mathbb{F}_q$, then $\mathrm{End}(\overline{E})$ is either an order in an imaginary quadratic field or an order in a quaternion algebra over $\mathbb{Q}$. In the former case $\overline{E}$ is said to be ordinary, and in the latter it is called supersingular. If E is an elliptic curve over F with good reduction at $\mathfrak{p}$ so that $\mathcal{O}_F/\mathfrak{p} \simeq \mathbb{F}_q$ and E reduces to $\overline{E}$, then the Galois representation $T_\ell(E)$ associated to E at ℓ coprime to $\mathfrak{p}$ can tell if $\overline{E}$ is ordinary or supersingular.

Theorem 7. *With notation as above, $\overline{E}$ is supersingular if and only if $a_p \equiv 0 \bmod p$ where a_p is the trace of $Frob_p$ acting on $T_\ell(E)$.*

For $p > 3$, the Hasse bound implies that $a_p \equiv 0 \bmod p$ is equivalent to $a_p = 0$ in $\mathbb{Z}_p$.

2.3 Reduction Type

Galois representations can also tell us when an abelian variety has good or bad reduction at a prime. For example, we have the following criterion.

Theorem 8 (Neron-Ogg-Shafarevich)**.** *Let K be a local field, and ℓ a prime not dividing the residue characteristic. Let A be an abelian variety over K. Then A has good reduction if and only if $T_\ell(A)$ is unramified.*

In the case where $\ell = p$ is the residue characteristic, $T_p(A)$ can still detect if A has good reduction or not. However, being unramified is replaced with the condition of being crystalline.

2.4 Hodge Numbers

An interesting fact is that Galois representations also know a bit of the geometry of algebraic varieties. The following was conjectured by Tate (after being proven in some special cases) and proven by Faltings.

Theorem 9 (Hodge-Tate Decomposition)**.** *Let X be an algebraic variety over a local field K with residue characteristic p. Then*

$$H^n_{\acute{e}t}(X, \mathbb{Q}_p) \otimes \mathbb{C}_p = \oplus_{i+j=n} H^i(X, \Omega^j_{X/\mathbb{C}_p}) \otimes \mathbb{C}_p(-j).$$

The right side of the decomposition has trivial action on the sheaf cohomology tensored with appropriate Tate twists. This theorem shows that upon tensoring with a large enough field, the étale cohomology becomes rather simple, being a direct sum of 1-dimension representations that are understood via class field theory. In addition, we can recover the Hodge numbers $h^{i,j}(X) := \dim H^i(X, \Omega^j_{X/\mathbb{C}_p})$ using the identity

$$(H^n_{\text{ét}}(X, \mathbb{Q}_p) \otimes \mathbb{C}_p(j))^{G_K} = H^i(X, \Omega^j_{X/\mathbb{C}_p})$$

and the fact that $\mathbb{C}_p(j)^{G_K} = K$ if and only if $j = 0$, and 0 otherwise. This implies the Hodge numbers of X are determined by the Galois representations associated to its étale cohomology.

2.5 Global Rational Points

Let A be an abelian variety over a number field F. Then we can associate to it an L-function $L(A, s)$ which is a product of local L-factors at every prime of F. In the case of an elliptic curve, this is just the product of the numerators of the zeta functions at the good primes, plus finitely many at the bad primes. In other words, it is built out of data associated to the Galois representation associated to A. Miraculously, it seems that this function, coming from local data, knows about global rational points as well.

Conjecture 10 (Birch and Swinnerton-Dyer)**.** *Let $L(A, s)$ be the L-function attached to an abelian variety A over F. Then $L(A, s)$ has an analytic continuation to the entire complex plane, and the order of vanishing at $s = 1$ equals the rank of $A(F)$.*

In the case where $A = E$ is an elliptic curve of rank 0 or 1 over $\mathbb{Q}$, this is known to be true. This gives a relatively simple way to determine if an elliptic curve over $\mathbb{Q}$ has finitely many rational points by computing $L(E, 1)$ to enough precision and proving it is nonzero. But the conjecture gives no way of producing any rational points on the abelian variety in question.

2.6 Coefficients of Modular Forms

Let $f(\tau)$ be a weight $k \geq 2$ normalized eigenform of level $\Gamma_1(N)$ of Nebentype ε. Let K be the number field obtained by adjoining all Fourier coefficients of f to $\mathbb{Q}$ (the fact that this is a finite extension is part of the theory of modular forms). Let K_ℓ be the completion of K at a place dividing $\ell \in \mathbb{Q}$ prime. Then Deligne proved the following result.

Theorem 11. *There exists a continuous Galois representation $\rho_{f,\ell} : G_{\mathbb{Q}} \to GL_2(K_\ell)$ unramified away from $\ell \cdot N$ which satisfies (for p unramified)*

$$\det(T - \rho_f(Frob_p)) = T^2 - a_p T + p^{k-1}\varepsilon(p)$$

where a_p is the pth Fourier coefficient of f.

So this theorem recognizes the coefficients of f as the traces of Frobenius at prime places. Swinnerton-Dyer in (8) uses this to explain some congruences among coefficients of modular forms originally observed by Ramanujan.

The theorem allowed for the formulation of an important conjecture, now proven, in terms of Galois representations.

Theorem 12. *Let E be an elliptic curve over $\mathbb{Q}$. Then there exists a normalized eigenform f of weight 2 and level $\Gamma_1(N)$ where N is the conductor of E such that*

$$L(E, s) = L(f, s)$$

where $L(f, s) = \sum_{n \geq 1} a_n/n^s$ for a_n the Fourier coefficients of f.

By the theory of Hecke operators, it was known $L(f, s)$ has an Euler product similar to the one defining $L(E, s)$. However, it was not previously known that $L(E, s)$ should extend analytically beyond $\Re(s) > 3/2$, an important corollary and piece of conjecture 10.

In fact, the equivalence of L-functions is equivalent to saying the Galois representations associated to E and f have the same Artin L-functions.

2.7 Inverse Galois Problem

It is an old conjecture that every finite group appears as a Galois group $\mathrm{Gal}(F/\mathbb{Q})$ for some finite extension $F/\mathbb{Q}$. The decomposition theorem of finite abelian groups and Dirichlet's theorem on primes verifies this for finite abelian groups. In addition, class field theory allows one to deduce that the conjecture is true for any finite solvable group.

Given any surjective homomorphism $\rho : G_{\mathbb{Q}} \to H$ we see that $F := \overline{\mathbb{Q}}^{\ker \rho}$ will be Galois with group $\mathrm{Gal}(F/\mathbb{Q}) \simeq H$. Thus if H appears as the image of a Galois representation, this verifies the inverse Galois problem for H. In particular, theorem 6 implies that $\mathrm{GL}_2(\mathbb{F}_p)$ appears as a Galois group for all p. (First for sufficiently large p, but effective bounds allow us to check directly that it is true.) Later we will explore some recent results of this flavor, where certain finite groups are realized as Galois groups by a similar geometric argument.

3 Computational Aspects

Now that we have seen how prolific Galois representations are in number theory and how much information they contain about geometric objects, we will discuss some results regarding computing these representations, especially those coming from hyperelliptic curves.

3.1 Subgroups of $\mathbf{GL}_2(\mathbb{F}_p)$

In this section, we record some results of group theory about the subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$, the codomain of mod p representations. Understanding the type of subgroup which is the image of a mod p representation will give information about the curve it originates from.

Definition 13. *Let C_s be the subgroup of diagonal matrices*

$$C_s = \left\{ \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \right\} \subset GL_2(\mathbb{F}_p),$$

called the split Cartan subgroup. Let C_{ns} be the subgroup

$$C_{ns} = \left\{ \begin{pmatrix} x & \varepsilon y \\ y & x \end{pmatrix} \right\} \subset GL_2(\mathbb{F}_p),$$

called the non-split Cartan subgroup. Write B for the subgroup of upper triangular matrices, and call it and its conjugates Borel subgroups.

Given these, we have a classification theorem.

Theorem 14. *Let G be a subgroup of $GL_2(\mathbb{F}_p)$ for p an odd prime, and write H for its image in $PSL_2(\mathbb{F}_p)$. Then one of the following hold:*

1. *G contains an element of order p, and then $G \subseteq B$ or $G \supseteq SL_2(\mathbb{F}_p)$,*
2. *H is cyclic and G is in a Cartan subgroup,*
3. *H is dihedral and G lies in the normalizer of a Cartan group, but not in any Cartan subgroup,*
4. *$H \simeq A_4, S_4$, or A_5, and G is not in any normalizer of a Cartain subgroup.*

3.2 Non-CM Elliptic Curves

For this section, let E be an elliptic curve over $\mathbb{Q}$ without CM. By theorem 6, we know that there are finitely many primes such that the residual representation $\rho_p : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ is not surjective. Let S_E be the finite set of such primes.

Definition 15. *We write $A(E)$ for*

$$A(E) := 2 \cdot 3 \cdot 5 \cdot \prod_{\ell \in S_E} \ell$$

and call this Serre's constant associated to E.

It is possible to show that the representations $\rho_k : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z})$ are surjective for k coprime to $A(E)$. An unconditional upper bound on the largest prime divisor of $A(E)$ is found in (4) in terms of the conductor N of E. The strategy for this goes back to Serre. From the classification of subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$, ρ_p being surjective is equivalent to H (the image in $\mathrm{PSL}_2(\mathbb{F}_p)$) not being contained in a Borel subgroup, nor a split-Cartan subgroup, nor being isomorphic to A_4, S_4, A_5, nor being contained in the normalizer of a Cartan subgroup with $H \not\subseteq C$ (a Cartan subgroup).

Serre himself showed the first three of these are satisfied whenever $p \geq 19$ and $p \neq 37$. In the last case, write G for the image of ρ_p. If N is the normalizer of the Cartan subgroup C which contains G, then composition gives a map $\varepsilon : G_{\mathbb{Q}} \to N/C \simeq \{\pm 1\}$ which is a quadratic character. Assuming GRH, Serre uses this to show there exists a constant c_1 such that

$$A(E) \leq c_1(\log(N))(\log\log(2N))^3.$$

An unconditional variant is given in (4), which we state here.

Theorem 16. *With notation as above, let p be a prime satisfying*

$$p \geq \frac{4\sqrt{6}}{3} N \prod_{\ell | N} \left(1 + \frac{1}{\ell}\right)^{1/2} + 1,$$

where the product runs over prime divisors of the conductor. Then ρ_p is surjective. Also, $A(E) << N(\log(N))^{1/2}$.

The proof uses the Modularity Theorem i.e. theorem 12, showing that for p above that lower bound, G cannot be contained in the normalizer of a Cartan subgroup.

It is conjectured in (9) that when E is an elliptic curve over $\mathbb{Q}$ without CM that ρ_p is surjective for $p > 17$ and $p \neq 37$. More specifically, we have the following.

Conjecture 17. *If $p > 13$ and $(p, j(E)) \notin S_0 := \{(17, -17^2 \cdot 101^3/2), (17, -17 \cdot 373^3/2^{17}), (37, -7 \cdot 11^3), (37, -7 \cdot 137^2 \cdot 2083^3)\}$ then ρ_p is surjective.*

The conjecture was verified for conductors up to 360000 in the same paper, using an algorithm introduced in the paper for computing a finite set S of prime such that for $p \notin S$, ρ_p is surjective and then testing the elements of S directly to see if the representation was surjective.

These results apply only to elliptic curves over $\mathbb{Q}$. Sutherland in (7) provides some probabilistic methods for computing images of Galois representations attached to elliptic curves over some number field F. We'll provide a summary of these methods here.

Fix an elliptic curve E over the number field F. Let p be prime. Write G_p for the image of G_F under $\rho_p : G_F \to Aut(E[p]) \simeq \mathrm{GL}_2(\mathbb{F}_p)$.

Definition 18. *Let $g \in GL_2(\mathbb{F}_p)$. Then we define the signature of g, written $sig(g)$ to be the triple $(\det(g), tr(g), \dim_1(g))$ where $\dim_1(g) \in \{0, 1, 2\}$ is the dimension of the 1-eigenspace of g. For G a subgroup of $GL_2(\mathbb{F}_p)$, we write $sig(G) = \{sig(g) : g \in G\}$.*

The motivation for this definition is to switch from tracking subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ and studying signatures instead, motivated by the following lemma which applies to many cases.

Lemma 19. *Let p be a prime such that $F \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$. Then G_p is determined up to isomorphism by its signature.*

If we let $z(G) = \#\{g \in G : tr(g) = 0\}/\#G$ for $G \subseteq \mathrm{GL}_2(\mathbb{F}_p)$, then it turns out *any* $G \subseteq \mathrm{GL}_2(\mathbb{F}_p)$ is determined by $\mathrm{sig}(G)$ and $z(G)$ up to local conjugacy and isomorphism. In other words, for any other such subgroup H, there exists a bijective map $f : H \to G$ such that $f(h)$ is conjugate to h by some element of $\mathrm{GL}_2(\mathbb{F}_p)$.

The next theorem shows that if we allow ambiguity up to local conjugacy (instead of full conjugacy), then we should consider our elliptic curve defined only up to isogeny.

Theorem 20. *Suppose G' is a subgroup of $GL_2(\mathbb{F}_p)$ which is locally conjugate to G_p but not conjugate to it. Then $G' = G'_p$ for some other elliptic curve E' over F which is related to E by a cyclic isogeny of degree p. The curve E' is unique up to isomorphism.*

The goal of the algorithms given in (7) is to compute the signature of the image G_p by computing signatures of Frobenius elements corresponding to primes $\mathfrak{p}$ of $\mathcal{O}_F$ not dividing primes of bad reduction nor $\mathrm{disc}(F)$. Using some effective bounds from GRH, one can compute the signatures of a finite number of Frobenius elements to determine the signature of the image. Altogether we have the following theorem.

Theorem 21. *Let E be an elliptic curve over $\mathbb{Q}(\alpha)$ given by $y^2 = f(x)$ for $f(x) \in \mathbb{Z}[\alpha][x]$. Assume GRH, and that E does not have CM. Then there is a Las Vegas algorithm which returns a bound L such that $G_p = GL_2(\mathbb{F}_p)$ for all $p > L$ and a list of generators for G'_p when $p \leq L$ for G'_p a subgroup of $GL_2(\mathbb{F}_p)$ locally conjugate to G_p.*

This result is of theoretical importance because, being a Las Vegas algorithm, the results are provably true when the algorithm is successful. However, (7) also contains a Monte Carlo algorithm which is generally faster, with the cost of introducing the possibility the result is incorrect (with a specific assigned probability).

Theorem 22. *With the same assumptions as the last theorem, there exists a Monte Carlo algorithm which computes G_p up to local conjugacy with probability greater than 2/3.*

(7) also gives bounds on the runtimes of each algorithm in terms of f.

3.3 Hyperelliptic Curves

In this section, C will be a hyperelliptic curve of genus g over $\mathbb{Q}$ with Jacobian $J = J(C)$. The Weil pairing on $J[p]$ is symplectic and preserved by the Galois

action, so we get a representation $\rho_p : G_{\mathbb{Q}} \to GSp_{2g}(\mathbb{F}_p)$ by choosing a basis for $J[p]$. (In general, the image is restricted in this way for a principally polarized abelian variety, which a Jacobian of a curve is always an example of.)

We have that theorem 6 generalizes to this setting.

Theorem 23. *Let A be a principally polarized abelian variety over a number field K of dimension $g = 2, 6$ or g is odd. Suppose $End_{\overline{K}}(A) = \mathbb{Z}$. Then there exists $B = B(A, K)$ such that for all $p > B$, the image of ρ_p is equal to $GSp_{2g}(\mathbb{F}_p)$.*

This suggests that for Jacobians with small endomorphism rings, we should expect to see $GSp_{2g}(\mathbb{F}_p)$ as the image of residual Galois representations frequently (although the theorem is not true if the condition on g is removed). In (2), an algorithm is presented for computing a finite set of p for which this happens for special hyperelliptic curves. A major ingredient is a theorem which requires the abelian variety A to satisfy the condition that there exists a prime ℓ such that the Néron model of A over $\mathbb{Q}_\ell$ is semistable with toric dimension 1. This is a technical condition which is always satisfied for J the Jacobian of a curve with a model $C : y^2 = f(x)$ satisfying the properties:

- $f(x)$ has no repeated roots over $\overline{\mathbb{Q}}$,
- all coefficients of f have nonnegative ℓ-adic valuation and the reduction of f mod ℓ has one double root, with the rest simple roots over $\overline{\mathbb{F}}_\ell$.

Then (2) outlines a method for computing certain p with surjective images. In particular, they prove the following.

Proposition 24. *There exists a hyperelliptic curve C such that the mod p representation attached to the Jacobian has $G_p = GSp_6(\mathbb{F}_p)$ for all $11 \leq p \leq 500000$.*

The paper ends with the suggestion that there may be a single hyperelliptic curve which realizes $GSp_6(\mathbb{F}_p)$ as a Galois group for all $p \geq 11$.

Recently, (1) have shown that there do exist hyperelliptic curves with the property that the mod p Galois representation is the general symplectic group for all p. Specifically, they provide a recipe for creating such examples.

Theorem 25. *Suppose $n = 2g + 2$ can we written as a sum of two primes in two different ways, where none of those primes are the largest prime less than n. Then there exist explicit $N \in \mathbb{Z}$ and $f_0(x)$ monic in $\mathbb{Z}[x]$ with the following properties. If $C : y^2 = f(x)$ is a hyperelliptic curve with $f(x) \equiv f_0(x) \bmod N$ with no roots of multiplicity greater than 2 in $\overline{\mathbb{F}}_p$ for $p \nmid N$, then G_p, the image*

of the residual representation attached to $J(C)$, is $GSp_{2g}(\mathbb{F}_p)$ for p odd and S_n for $p = 2$.

An example is provided in (1) of a hyperelliptic curve of genus 6 which satisfies the conditions of the theorem, thus showing $GSp_{12}(\mathbb{F}_p)$ occurs as a Galois group for all p odd.

References

[1] Samuele Anni, Vladimir Dokchitser, "Constructing hyperelliptic curves with surjective Galois representations", arXiv:1701.05915v1 [math.NT]

[2] Sara Arias-de-Reyna, Ccile Armana, Valentijn Karemaker, Marusia Rebolledo, Lara Thomas, Nria Vila, "Galois representations and Galois groups over Q", arXiv:1407.5802v2 [math.NT]

[3] Bhargav Bhatt, "The Hodge-Tate decomposition via perfectoid spaces", notes for AWS 2017.

[4] Alina Carmen Cojocaru and Ernst Kani, On the surjectivity of the Galois representations associated to non-CM elliptic curves, Canad. Math. Bull. 48 (2005), 1631. MR2118760 (2005k:11109)

[5] David A. Cox, *Primes of the Form $x^2 + ny^2$*. John Wiley & Sons, Inc., second edition, 2013.

[6] J. Silverman, *The Arithmetic of Elliptic Curves*, New York: Springer-Verlag (c1986).

[7] Andrew Sutherland, "Computing images of Galois representations attached to elliptic curves", Forum of Mathematics, Sigma 4 (2016), e4 (79 pages)

[8] H.P.F. Swinnerton-Dyer, "On ℓ-adic representations and congruences for coefficients of modular forms", in Modular functions of one variable III (Antwerp, Belgium 1972), P. Deligne and W. Kuyk (Eds.), Lecture Notes in Mathematics 350, Springer, 1973, 156. 3.

[9] David Zywina, "On the surjectivity of mod ℓ representations associated to elliptic curves", arXiv:1508.07661 [math.NT]