GALOIS REPRESENTATIONS AND STATISTICS

COURSE: SAMUELE ANNI AND RENÉ SCHOOF
NOTES: ROSS PATERSON

Lecture 1 (Schoof)

1. Elliptic Curves

Let E/F be an elliptic curve over a number field. We take the notation:

- $E(\overline{F})$ is the group of points over the algebraic closure;
- for a prime $\ell \in \mathbb{Z}_{\geq 1}$ write $E[\ell]$ for the ℓ-torsion points in $E(\overline{F})$, which is isomorphic to $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ as an abelian group;
- $F_\ell := F(E[\ell])$;
- Note that $\mathrm{Gal}(\overline{F}/F)$ acts on $E[\ell]$, and so we obtain a map

$$\mathrm{Gal}(\overline{F}/F) \to \mathrm{Aut}(E[\ell]) \cong \mathrm{GL}_2(\mathbb{F}_\ell).$$

We denote by $G_\ell \cong \mathrm{Gal}(F_\ell/F)$ the image of Galois under this map.

Example 1. $E : y^2 + y = x^3 + x$ over $F = \mathbb{Q}$. We begin by looking at division polynomials $f_\ell(x) \in \mathbb{Z}[x]$ using the recursive `elldivpol` algorithm in PARI. By definition, $f_\ell(x) = 0$ if and only if x is the x-coordinate of a nonzero ℓ-division point. For ℓ an odd prime we have $\deg(f_\ell) = \frac{\ell^2-1}{2}$. Now for some explicit examples.

- For $\ell = 2$: `elldivpol` gives us $f_2(x) = 4x^3 - 4x + 1$, and then using `Galoisgroup` we see that this polynomial has Galois group isomorphic to $S_3 \cong \mathrm{GL}_2(\mathbb{F}_2)$. Thus $G_2 = \mathrm{GL}_2(\mathbb{F}_2)$.
- For $\ell = 3$: `elldivpol` gives us that $f_3(x) = 3x^4 - 6x^2 + 3x - 1$, and then using `Galoisgroup` we get that this polynomial has Galois group S_4. For 3-torsion points the x coordinates correspond to the lines in $E[3]$, so points in $\mathbb{P}_1(\mathbb{F}_3)$. Thus $\mathrm{Gal}(f)$ can be viewed as a subgroup of $\mathrm{PGL}_2(\mathbb{F}_3)$, and since it is $S_4 \cong \mathrm{PGL}_2(\mathbb{F}_3)$ we see that it is acting as the full $\mathrm{PGL}_2(\mathbb{F}_3)$ on this space. In particular, using Exercise 2 below, $G_3 = \mathrm{GL}_2(\mathbb{F}_3)$.

Exercise 2. Show that if $H \leq \mathrm{GL}_2(\mathbb{F}_3)$ surjects onto $\mathrm{PGL}_2(\mathbb{F}_3)$ (under the natural projection $\mathrm{GL}_2(\mathbb{F}_3) \to \mathrm{PGL}_2(\mathbb{F}_3)$) then $H = \mathrm{GL}_2(\mathbb{F}_3)$

Example 3. $E' : y^2 = x^3 + x^2 - 2x - 1$, let ζ_7 be a fixed primitive 7th root of unity.

- For $\ell = 2$: The zeroes of the cubic are Galois conjugates of $\zeta_7 + \zeta_7^{-1}$. Thus the points in $E[2]$ generate the totally real subfield of $\mathbb{Q}(\zeta_7)$, which is a cyclic gubic extension of $\mathbb{Q}$, and so $G_2 \cong C_3 \subseteq \mathrm{GL}_2(\mathbb{F}_2)$.
- For $\ell = 3$: the 3-division polynomial is $(x-2)(3x^3 + 10x^2 + 8x + 4)$. The cubic is an S_3-cubic whose splitting field has quadratic subfield $\mathbb{Q}(\sqrt{-3})$. The linear factor corresponds to the points $(2, \pm\sqrt{7})$. Note that this is sufficient to show that the order of the Galois image is at least $6 \times 2 = 12$.

Moreover, if $P = (2, \sqrt{7})$ then $\langle P \rangle \leq E[3]$ is a Galois stable subgroup. Thus the image of Galois is contained in the group of matrices of the form

$$\begin{pmatrix} \psi & * \\ 0 & \omega \end{pmatrix}.$$

Where ψ is the sign character on $\mathrm{Gal}(\mathbb{Q}(\sqrt{7})/\mathbb{Q})$, and ω is some character of $\mathrm{Gal}(\mathbb{Q}(E[3])/\mathbb{Q})$ (since the determinant is a character). There are at most 12 possible matrices of this form, and so this whole group must be the image of Galois.

It will be important to look at the ring of endomorphisms of E over F. In fact $\mathrm{End}_{\overline{F}}(E) \cong \mathbb{Z}$ or $\mathcal{O}$ where $\mathcal{O}$ is an order in an imaginary quadratic field.

Case: Defined CM. Assuming that $\mathrm{End}_F(E) \cong \mathcal{O}$ for $\mathcal{O}$ an order in an imaginary quadratic field. Then

$$\mathcal{O} = \mathrm{End}(E) \to \mathrm{End}_{\mathrm{ab}}(E[\ell]).$$

The kernel of this map is $\ell\mathrm{End}(E)$. Indeed: if $f|_{E[\ell]} = 0$ then $\ker([\ell]) \subseteq \ker(f)$, meaning that

$$f = g \circ [\ell] = [\ell] \circ g \in \ell\mathrm{End}(E).$$

Thus we have an injection

$$\mathcal{O}_\ell\mathcal{O} \to \{2 \times 2\text{-matrices over } \mathbb{F}_\ell\} =: M_{2\times 2}(\mathbb{F}_\ell).$$

The condition that every element of $\mathcal{O}$ is defined over F gives us that the image of $\mathcal{O}/\ell\mathcal{O}$ in $M_{2\times 2}(\mathbb{F}_\ell)$ must commute with the image of G_ℓ. That is to say, G_ℓ must be contained in the centraliser of $(\mathcal{O}/\ell\mathcal{O})^\times \subseteq M_{2\times 2}(\mathbb{F}_\ell)$.

Exercise 4. Show that $(\mathcal{O}/\ell\mathcal{O})^\times$ is its own centralizer, and so $G_\ell \subseteq (\mathcal{O}/\ell\mathcal{O})^\times$.

Based on the splitting type of ℓ in $\mathcal{O}$ we see:

- if ℓ is split then $\mathcal{O}_\ell/\mathcal{O}_\ell^\times = \mathbb{F}_\ell^\times \times \mathbb{F}_\ell^\times$ (split Cartan)
- if ℓ is inert then $\mathcal{O}_\ell/\mathcal{O}_\ell^\times = \mathbb{F}_{\ell^2}^\times$ (nonsplit Cartan)
- if ℓ is split then $\mathcal{O}_\ell/\mathcal{O}_\ell^\times = \mathbb{F}_\ell[\varepsilon]$

Case: Undefined CM. Assuming that $\mathrm{End}_F(E) \subsetneq \mathrm{End}(E) \cong \mathcal{O}$ for $\mathcal{O}$ an order in an imaginary quadratic field. Then we have a surjection

$$\mathrm{Gal}(\overline{F}/F) \to \mathrm{Aut}(\mathcal{O}) = \{\mathrm{Id}, c\}$$

Thus the endomorphisms are defined over a degree 2 extension F'/F. Moreover $G_\ell \subset$normaliser of $\mathcal{O}/\ell\mathcal{O}^\times$. The size of the Galois image can be

$$\begin{cases} 2(\ell-1)^2 & \text{if normaliser of split cartan} \\ 2(\ell^2-1) & \text{if normaliser of non split cartan} \\ (\ell-1)^2\ell & \text{if Borel} = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \end{cases}$$

Non-CM. In the case of non-CM elliptic curves, we have the following theorem of Serre.

Theorem 5 (Serre 1972)**.** *Let E/F be an elliptic curve over a number field without CM (i.e.* $\mathrm{End}(E) \cong \mathbb{Z}$*). Then there is a constant C, depending on E, such that for all $\ell > C$ the image of*

$$\mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_2(\mathbb{F}_\ell)$$

is surjective

Conjecture 6 (Serre)**.** *The constant above can be chosen uniformly in E.*

Weil Pairing. An important concept related to the Galois image is the Weil pairing.

Definition 7. There is a nondegenerate alternating bilinear pairing called the Weil pairing

$$e_\ell : E[\ell] \times E[\ell] \to \mu_\ell,$$

which is defined over F (meaning it is $\mathrm{Gal}(\overline{F}/F)$-equivariant).

Since the pairing is nondegenerate, note that if P, Q is a basis of $E[\ell]$ then $e_\ell(P,Q) = \zeta_\ell$ for a primitive ℓth root of unity ζ_ℓ. In particular since the left hand side is invariant under $\mathrm{Gal}(\overline{F}/F_\ell)$ we must have $F(\zeta_\ell) \subseteq F_\ell$.

Exercise 8. Use the Galois equivariance of the Weil pairing to check that the diagram below commutes:

$$\begin{array}{ccc} G_\ell = \mathrm{Gal}(F_\ell/F) & \longrightarrow & \mathrm{GL}_2(\mathbb{F}_\ell) \\ \big\downarrow{\scriptstyle \mathrm{res}} & & \big\downarrow{\scriptstyle \det} \\ \mathrm{Gal}(F(\zeta_\ell)/F) & \longrightarrow & \mathbb{F}_\ell^\times. \end{array}$$

In particular, if $F(\zeta_\ell)/F$ has degree $\ell - 1$ then this means that the determinant map must be surjective and so our Galois image must not be too small! Moreover, this assumption on the degree always holds for all but finitely many ℓ since F is a number field.

Proposition 9. *If $H \leq \mathrm{GL}_2(\mathbb{F}_\ell)$, and $\det(H) = \mathbb{F}_\ell^\times$, then one of the following is true*

- *$H \subseteq$normaliser of Cartan (split or nonsplit)*
- *$H \subseteq$Borel*
- *The image of H in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ is an exceptional subgroup A_4, S_4, A_5 in $\mathrm{PGL}_2(\mathbb{F}_\ell)$*

Proof. If $\ell \mid \#H$ then H contains an element σ of order ℓ. In particular, there is an element $\sigma \in H$ such that $\sigma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. If there is a $\tau \in H$ which fixes another point in $\mathbb{F}_\ell \times \mathbb{F}_\ell$ then we can show that it can be moved around to get that $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ is in H. It is an exercise to show that these two matrices generate $\mathrm{SL}_2(\mathbb{F}_\ell)$. Thus $H \supseteq \mathrm{SL}_2(\mathbb{F}_\ell)$, and since the determinant map is assumed to be surjective then $H = \mathrm{GL}_2(\mathbb{F}_\ell)$. If τ does not exist then we leave it as an exercise to show [?].

If $\ell \nmid \#H$ then all $\sigma \in H$ are diagonalisable, and writing $\overline{\sigma}$ =image of $\sigma \in \mathrm{PGL}_2(\mathbb{F}_\ell)$ we see that every $\overline{\sigma}$ im the image of H in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ must have two fixed points in $\mathbb{P}^1(\mathbb{F}_\ell)$. It is then an exercise to copy the proof over $\mathbb{C}$ that shows we are in one of the cases above. □

1.1. **Finding Elements.** Finding elements in $G_\ell \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$ might be hard, but finding characteristic polynomials (of Frobenius elements $\mathrm{Frob}_\mathfrak{p}$) is not so hard. It is standard theory that F_ℓ/F is unramified outside of the set of bad primes of E

and ℓ, so we consider these unramified $\mathfrak{p}$. We denote

$$\begin{aligned} \mathrm{Gal}(F_\ell/F) &\to \mathrm{GL}_2(\mathbb{F}_\ell) \\ \mathrm{Frob}_\mathfrak{p} &\mapsto A_\mathfrak{p}. \end{aligned}$$

Then the characteristic polynomial of $A_\mathfrak{p}$ is $X^2 - a_p X + p \in \mathbb{F}_\ell[X]$ where $p + 1 - a_p = \#E(k_\mathfrak{p})$.

Example 10. $E : y^2 + y = x^3 - x$, $F = \mathbb{Q}$, $p = 3$. Then $\#E(\mathbb{F}_3) = 7$ so $a_3 = 3$ and the characteristic polynomial is $x^2 - 3x + 3$.

For $\ell = 2$: $G_2 \subseteq \mathrm{GL}_2(\mathbb{F}_2)$ has $\mathrm{Frob}_3 \mapsto A_3$ with characteristic polynomial $x^2 + x + 1$ so has order 3.

For $p = 5$, $\ell = 2$: Characteristic polynomial is $X^2 + 1$ and so the Frobenius at 5 is order 2.

If $G_\ell = \mathrm{GL}_2(\mathbb{F}_\ell)$ then all possible characteristic polynomials are those of some $A \in G_\ell$. The converse is true if $\ell \neq 3$.

Theorem 11 (Serre's Criterion)**.** *($\ell \geq 5$). Let E/F be an elliptic curve over a number field and $H = G_\ell$ be the image of Galois in $\mathrm{GL}_2(\mathbb{F}_\ell)$. Assume that all of the following hold:*

- *$\exists \sigma \in H$ with characteristic polynomial $X^2 - tX + p$ for which the discriminant is a nonzero square and $t \neq 0$;*
- *$\exists \sigma \in H$ with characteristic polynomial $X^2 - tX + p$ for which the discriminant is a nonsquare and $t \neq 0$;*
- *$\exists \sigma \in H$ with characteristic polynomial $X^2 - tX + p$ for which $t^2/\det(\sigma) \neq 0, 1, 2, 4, \frac{3 \pm \sqrt{5}}{2}$.*

Then $H = \mathrm{GL}_2(\mathbb{F}_\ell)$.

Lecture 2 (Schoof)

An alternative formulation of Serre's open image theorem from last time is the following.

Theorem 12 (Serre)**.** *Let E/F be an elliptic curve over a number field. If $G_\ell \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$ is a proper subgroup for infinitely many ℓ then E must have CM.*

Some observations:

- We can extend F to a larger number field without loss of generality. In particular:
  - we may get rid of all of the places of additive reduction and assume that we have semistable reduction (here meaning all reduction types of E are good or split multiplicative); and
  - we may assume that F is complex and Galois over $\mathbb{Q}$.
- We may assume that our infinitely many primes are of good reduction, are unramified in F, and satisfy $\det(G_\ell) = \mathbb{F}_\ell^\times$ (equivalently: that we have $\mathbb{Q}(\zeta_\ell) \cap F = \mathbb{Q}$).

Yesterday we saw that there are infinitely many primes ℓ such that G_ℓ is contained in one of a Borel (meaning upper triangular matrices), normalizer of Cartan or exceptional.

Consider

$$\begin{array}{c} F_\ell \\ \Big| G_\ell \\ F \end{array}$$

Let $I_\mathfrak{l} \subseteq G_\ell$ be the inertia subgroup for $\mathfrak{l} \mid \ell$ (so of good reduction). Then $\#(E \bmod \mathfrak{l})[\ell] = \begin{cases} \ell & \text{ordinary} \\ 1 & \text{supersingular.} \end{cases}$

(1) If ordinary then we have the exact sequene

$$0 \longrightarrow \ker \longrightarrow E[\ell] \xrightarrow{\text{red}} (E \mod \mathfrak{l})[\ell] \longrightarrow 0$$

where $\#\ker = \ell$. Inertia acts trivially on the rightmost group, so must act as

$$\begin{pmatrix} \omega & * \\ 0 & 1 \end{pmatrix}$$

where ω is the cyclotomic character.

Exercise 13. $y^2 = x^3 + x^2 - 2x - 1$ has 3-division polynomial [IMAGE ON PHONE].

(2) If supersingular then take the formal group associated to E over $F_\mathfrak{l}$: let

$$H(z, w) = z + w + (\deg \geq 2),$$

and let $\mathfrak{m}$ be the maximal ideal of the integers of $\overline{\mathbb{Q}_\ell}$. Then $\mathfrak{m}$ is a group using H for composition, and moreover

$$\mathfrak{m} = \left\{ P \in E(\overline{\mathbb{Q}_\ell}) \ : \ P \text{ reduces to } \infty \bmod \mathfrak{l} \right\}.$$

The ℓ-torsion of $\mathfrak{m}$ is precisely

$$\{z \in \mathfrak{m} \ : \ H(z, H(z, H(z, \dots))) = 0\}$$
$$= \ell z + (\text{higher degree}).$$

Formal groups in characteristic ℓ:

$$[\ell]z = H'(z^{\ell^h}$$

where h is the height of the formal group, and $H' = a_1 z + a_2 x^2 + \dots$ and $a_1 \neq 0 \mod \mathfrak{l}$. We are supersingular if and only if $h = 2$.

Now $z \in E[\ell]$ if and only if $\ell z + \ldots + Z^{\ell^2} = 0$, which is equivalent to $z = 0$ or Z is a zero of an Eisenstein polynomial. Thus

$$\#I_\mathfrak{l} = \ell^2 - 1$$

and is cyclic.

Note that

$$I_\mathfrak{l} \subset G_\ell \subset \mathrm{GL}_2(\mathbb{F}_\ell)\overline{I}_\mathfrak{l} \subseteq \mathrm{PGL}_2(\mathbb{F}_\ell)$$

[return and make diagram] so $\#\overline{I}_\mathfrak{l} \geq \ell - 1$

[IMAGE 2]

Thus $G_\ell \subset$exceptional group for only finitely many ℓ.

Proposition 14. *There is an extension F'/F with $[F' : F] \leq 2$ such that for infinitely many ℓ the image of $G_{F'}$ is in Borel or Cartan.*

Proof. Suppose that for infinitely many primes ℓ, we have $G_\ell \subset$normaliser of Cartan but not Cartan. Recall that Cartan is the matrices $\left\{\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}\right\}$, and normaliser of this is the Cartan union $\left\{\begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}\right\}$

For each ℓ we get a quadratic extension $F_\ell/F'/F$ depending on ℓ.
Claim: that this extension is everywhere unramified and so (via finiteness of the class group and class field theory) we can choose F' to work for infinitely many ℓ.

Proof of claim. What primes can ramify? Well precisely

(1) $\mathfrak{p} \mid \ell$ of good reduction (by our assumptions on ℓ the good reduction is for free); or
(2) $\mathfrak{p} \nmid \ell$ of bad reduction.

In case 1., if $\mathfrak{p} \mid \ell$ of good reduction then have

$$\begin{array}{c} F_\ell \\ \big| C \\ F' \\ \big| \\ F \end{array}$$

and the total group is contained in $N =$normaliser of Cartan, we want $I_\mathfrak{p} \subset C$. We saw $I_\mathfrak{p} = \begin{pmatrix} \omega & * \\ 0 & 1 \end{pmatrix}$ if ordinary and $\#I_\mathfrak{p} = \ell^2 - 1$ if supersingular. It is then pure group theory: to conclude that $I_\mathfrak{p} \subseteq C$.

In case 2. let $\mathfrak{p} \mid p \neq \ell$ be a bad prime. Our assumptions ensure that $\mathfrak{p}$ is split multiplicative and so we appeal to the Tate curve.

$$\overline{\mathbb{Q}_p}/q^{\mathbb{Z}} \cong E(\overline{\mathbb{Q}_p}).$$

So moreover we have a short exact sequence

$$0 \longrightarrow \mu(\overline{\mathbb{Q}_p}) \longrightarrow E[\ell] \longrightarrow q^{\mathbb{Z}}/q^{\ell\mathbb{Z}} \longrightarrow 0.$$

Thus $I_\mathfrak{p} = \begin{pmatrix} \omega & * \\ 0 & 1 \end{pmatrix}$.[return] □

□

Corollary 15. *Have E/F' and infinitely many primes ℓ for which G_ℓ is contained in either Borel or Cartan (split/nonsplit).*

Remark 16. So in other words we're rid of the exceptional and normaliser of Cartan cases!

Proposition 17. *If G_ℓ is contained in non-split Cartan for infinitely many ℓ then there are also infinitely many ℓ for which G_ℓ is contained in split Cartan (which is contained in Borel).*

Remark 18. This is the hardest part of the proof, we skip it for time.

As a result we now have:

Corollary 19. *For infinitely many primes ℓ we have G_ℓ is contained in Borel.*

Claim: This implies that E has CM.

Proof of claim. We have infinitely many ℓ with G_ℓ contained in Borel, which is the group of upper triangular matrices in $\mathrm{GL}_2(\mathbb{F}_\ell)$. Thus for each such ℓ we have an ℓ-isogeny

$$E \xrightarrow{\varphi_\ell} E_{(\ell)}.$$

However the size of the isogeny class of E over F is finite, so there exists ℓ' with $E_{(\ell)} = E_{(\ell')}$ over F.

$$\begin{array}{ccc} E & \xrightarrow{\varphi_\ell} & E_{(\ell)} \\ & \nwarrow^{\widehat{\varphi}_{\ell'}} & \downarrow \cong \\ & & E_{(\ell')}. \end{array}$$

However $\deg(\widehat{\varphi}_{\ell'}\varphi_\ell) = \ell\ell'$ which is not square, but $\deg([n]) = n^2$ and so $\widehat{\varphi}_{\ell'}\varphi_\ell$ is an endomormphism of E which is not in $\mathbb{Z}$. □

Why was the size of the F-isogeny class of an elliptic curve over F finite? Well one way is to use Faltings (1983), but Serre did not have access to this yet!

Serre: Fix E with good reduction outside of S, then use the result of Shaferevich (1962) that

$$\{E'/F \ : \ E' \text{ is } F\text{-isogenous to } E\} \subseteq \{E'/F \ : \ \text{good reduction outside of } S\}$$

This set is actually finite:

Proof. write $y^2 = x^3 + Ax + B$ for $A, B \in \mathcal{O}_S$ with good reduction. Then the discriminant $4A^3 + 27B^2 \in \mathcal{O}_S^\times/\mathcal{O}_S^{\times 12}$ which is a finite group. Moreover for each allowable discriminant ε we obtain an elliptic curve $4A^3 + 27B^2 = \varepsilon$! What a miracle! Shafarevich then uses a result of Thue (a precursor to Siegel–Mahler) that there are only finitely many solutions. □