SERRE'S ADELIC OPEN IMAGE THEOREM FOR NON-CM ELLIPTIC CURVES

TYLER GENAO

These notes follow Pete L. Clark's translation of Serre's *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques* [Ser72], so numbering is slightly off from the original French version. They supplement the talk I gave on this paper in the SeZoom seminar.

Let F be a number field and $E_{/F}$ an elliptic curve. One has an action of the absolute Galois group $G_F := \mathrm{Gal}(\overline{F}/F)$ on $E(\overline{F})$: for $\sigma \in G_F$ and $P = (x, y) \in E(\overline{F})$, the map $P \mapsto \sigma(P) := (\sigma(x), \sigma(y))$ defines an action of G_F on $E(\overline{F})$. For an integer $N \in \mathbb{Z}^+$, this action takes N-torsion to N-torsion, whence we have an action of G_F on $E[N]$,

$$\rho_{E,N} : G_F \to \mathrm{Aut}(E[N]).$$

This action is called the *mod−N Galois representation of E over F*. Choosing a basis P, Q of $E[N]$, one gets a more explicit action,

$$\rho_{E,N,P,Q} : G_F \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

For a prime $\ell \in \mathbb{Z}^+$, one can define the *ℓ-adic Tate module* as an inverse limit of the various ℓ-primary torsion subgroups of $E[\mathrm{tors}]$:

$$T_\ell(E) := \varprojlim E[\ell^n].$$

Consequently, $T_\ell(E)$ is a rank two $\mathbb{Z}_\ell$-module, where $\mathbb{Z}_\ell$ is the ring of ℓ-adic integers. The Galois action on each $E[\ell^n]$ naturally extends to the inverse limit $T_\ell(E)$, whence we have the *ℓ-adic Galois representation* of E

$$\rho_{E,\ell^\infty} : G_F \to \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Finally, one has the adelic Tate module $T(E)$ of E, an inverse limit over all $E[N]$. Consequently, $T(E)$ has rank two over the ring of profinite integers $\hat{\mathbb{Z}}$. This lends us the *adelic Galois representation* of E,

$$\rho_E : G_F \to \mathrm{GL}_2(\hat{\mathbb{Z}}).$$

The main result of Serre's paper [Ser72] is the following.

Theorem 1. *Suppose F is a number field and $E_{/F}$ a non-CM elliptic curve. Then $\rho_E(G_F)$ is open in $GL_2(\hat{\mathbb{Z}})$. Equivalently, for all but finitely many primes $\ell \in \mathbb{Z}^+$, the mod−ℓ Galois representation is surjective,*

$$\rho_{E,\ell}(G_F) = \mathrm{GL}_2(\ell).$$

Date: 4/30/2021.

The above says that for a non-CM elliptic curve $E_{/F}$, almost all degrees of its prime division fields $F(E[\ell])$ are as large as possible, i.e.,

$$[F(E[\ell]) : F] = (\ell^2 - 1)(\ell^2 - \ell)$$

for all but finitely many primes $\ell \in \mathbb{Z}^+$.

Remark. What is the difference between the CM and non-CM case? An important predecessor to Serre's paper [Ser72] is his book [Ser98] on abelian ℓ-adic representations and elliptic curves. As we will see, Serre was able to prove the ℓ-adic open image theorem for non-CM elliptic curves. One key piece of this was [Theorem, IV.2.2 [Ser98]], his irreducibility theorem for non-CM elliptic curves – that for almost all primes $\ell \in \mathbb{Z}^+$, the ℓ-torsion subgroup $E[\ell]$ is an irreducible G_F-module, i.e., $E[\ell]$ has no proper nontrivial G_F-stable submodules. Equivalently, E has no F-rational ℓ-isogenies for sufficiently large ℓ. Assuming further that the curve has non-integral j-invariant, Serre shows that almost all G_ℓ contain $\mathrm{SL}_2(\ell)$, whence almost all $\rho_{E,\ell}(G_F) = \mathrm{GL}_2(\ell)$. Following his proof, Serre asks if "non-integral j-invariant" can be replaced with "no CM." Indeed, this is the main result of [Ser72].

What about the CM case? Say $E_{/F}$ has CM by an order $\mathcal{O}$; write its fraction field as $K := \mathcal{O} \otimes \mathbb{Q}$. For simplicity, let us assume that $K \subseteq F$. Then one can show that $\rho_{E,N}(G_F)$ is an abelian subgroup of $\mathrm{GL}_2(\ell)$ (more precisely, $E[\ell]$ is a free, rank one $\mathcal{O}/\ell\mathcal{O}$-module). In particular, for any integer $N > 1$ the image $\rho_{E,N}(G_F)$ will not equal $\mathrm{GL}_2(\ell)$. Still, there is a similar "open image theorem" for CM elliptic curves if one changes the target group from $\mathrm{GL}_2(\ell)$ to $\mathrm{GL}_1(\mathcal{O}/\ell\mathcal{O}) = (\mathcal{O}/\ell\mathcal{O})^\times$. For more details on the CM case, see e.g. [BC20].

1. Abelian ℓ-Adic Representations and Elliptic Curves

Preceding Serre's paper [Ser72] is his book [Ser98]. The main result of his text is the ℓ-adic open image theorem for non-CM elliptic curves, see [Theorem, IV.2.2 [Ser98]].

Theorem 2. *Suppose F is a number field and $E_{/F}$ a non-CM elliptic curve. Then for all primes $\ell \in \mathbb{Z}^+$, $\rho_{E,\ell^\infty}(G_F)$ has finite index in $\mathrm{GL}_2(\mathbb{Z}_\ell)$.*

1.1. Variations of G_{ℓ^∞} and G_ℓ with ℓ.

For the remainder of this section, we'll follow the last two sections of [Ser98], which precede the open image theorem of [Ser72].

Here is the "Main Proposition" of section IV.3 [Ser98]. It concerns openness of the adelic Galois representation of a non-CM elliptic curve defined over a number field. This will be used to prove Theorem 1 later on.

Proposition 3. *Suppose that F is a number field and $E_{/F}$ is a non-CM elliptic curve. Let $G := \rho_E(G_F)$, $G_{\ell^\infty} := \rho_{E,\ell^\infty}(G_F)$ and $G_\ell := \rho_{E,\ell}(G_F)$.*

The following are equivalent:

1. *G is open in $\mathrm{GL}_2(\hat{\mathbb{Z}}) \cong \prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell)$;*
2. *$G_{\ell^\infty} = \mathrm{GL}_2(\mathbb{Z}_\ell)$ for all but finitely many primes $\ell \in \mathbb{Z}^+$;*
3. *$G_\ell = \mathrm{GL}_2(\ell)$ for all but finitely many primes $\ell \in \mathbb{Z}^+$;*
4. *$G_\ell \supseteq \mathrm{SL}_2(\ell)$ for all but finitely many primes $\ell \in \mathbb{Z}^+$.*

The implications 1. $\Rightarrow$ 2. $\Rightarrow$ 3. $\Rightarrow$ 4. are immediate. The implication 4. $\Rightarrow$ 1. requires the Main Theorem (Theorem 2) and the following "Main Lemma". The Main Lemma is purely group-theoretical.

Lemma 4 (Main Lemma)**.** *Let G be a closed subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}}) \cong \prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell)$. Let $G_{\ell^\infty} := \pi_{\ell^\infty}(G)$ and $G_\ell := \pi_\ell(G) = \pi_\ell(G_{\ell^\infty})$ denote its images in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ and $\mathrm{GL}_2(\ell)$, respectively. Suppose the following properties hold:*

1. *G_{ℓ^∞} is open in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ for all primes ℓ;*
2. *$\det(G) \subseteq \hat{\mathbb{Z}}^\times$ is open;*
3. *G_ℓ contains $\mathrm{SL}_2(\ell)$ for all but finitely many ℓ.*

Then G is open in $\mathrm{GL}_2(\hat{\mathbb{Z}})$. Equivalently, it has finite index in $\mathrm{GL}_2(\hat{\mathbb{Z}})$.

To prove Proposition 3, Serre combines the Main Lemma with another lemma concerning the determinants of adelic Galois representations of elliptic curves.

Lemma 5. *Let F be a number field and $E_{/F}$ an elliptic curve. Then for the adelic representation $G := \rho_E(G_F) \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$, we have the following:*

1. *$\det(G)$ is open in $\hat{\mathbb{Z}}^\times$.*
2. *For all but finitely many primes $\ell \in \mathbb{Z}^+$, we have both $\det(G_{\ell^\infty}) = \mathbb{Z}_\ell^\times$ and $\det(G_\ell) = \mathbb{F}_\ell^\times$.*

In particular, with this lemma and the Main Theorem, we can finish the proof of the implication 4. $\Rightarrow$ 1. from the Main Proposition. To see this, note that if $E_{/F}$ is a non-CM elliptic curve, then for the conditions of the Main Lemma, 1. holds by the ℓ-adic open image theorem, 2. holds by Lemma 5 above, and 3. holds by assumption. Then the Main Lemma implies that G is open in $\mathrm{GL}_2(\hat{\mathbb{Z}})$.

Let us shorten Proposition 3 as a corollary, to highlight its application in Theorem 1).

Corollary 6. *Suppose that $E_{/F}$ is a non-CM elliptic curve defined over a number field. Then G is open in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ iff G_ℓ contains $\mathrm{SL}_2(\ell)$ for all but finitely many ℓ.*

Remark. It is worth explicitly mentioning why for almost all primes $\ell \in \mathbb{Z}^+$, $G_\ell \supseteq \mathrm{SL}_2(\ell)$ iff $G_\ell = \mathrm{GL}_2(\ell)$. This follows by surjectivity of the mod$-\ell$ cyclotomic character. Recall that the Weil pairing implies

$$\det G_\ell = \chi_\ell,$$

the mod$-\ell$ cyclotomic character. Furthermore, if ℓ is unramified in F then χ_ℓ surjects onto $\mathbb{F}_\ell^\times$. Therefore, for all ℓ unramified in F, one has $G_\ell \supseteq \mathrm{SL}_2(\ell)$ iff $G_\ell = \mathrm{GL}_2(\ell)$ since $\mathrm{SL}_2(\ell)$ is the kernel of the determinant map on $\mathrm{GL}_2(\ell)$.

1.2. **The case of non-integral j-invariant.** What Serre shows in [Ser98] is that for any elliptic curve $E_{/F}$ over a number field, if its j-invariant $j(E)$ is not integral, then it satisfies the Main Proposition and thus has surjective mod$-\ell$ Galois representation for almost all prime $\ell \in \mathbb{Z}^+$. Observe that the family of non-integral j-invariant elliptic curves is a subset of the family of non-CM elliptic curves.

Serre uses the theory of Tate curves to show that an elliptic curve $E_{/F}$ with non-integral j-invariant will have open adelic image. If $\ell \nmid v(j)$ – here, v is a finite place of

F for which $v(j) < 0$ – then for the inertia group $I_v \subseteq G_F$, its image $\rho_{E,\ell}(I_v)$ contains the transvection $\gamma := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, see [Lemma 1, IV.3.2 [Ser98]]. Then [Lemma 2, IV.3.2 [Ser98]] shows that if G_ℓ acts on $\mathbb{F}_\ell \times \mathbb{F}_\ell$ irreducibly, then also $\gamma^T = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \in G_\ell$. Since $\mathrm{SL}_2(\ell)$ is generated by γ and γ^T, we conclude that $\mathrm{SL}_2(\ell) \subseteq G_\ell$ when $E[\ell]$ is irreducible. But we already know by [Theorem, IV.2.2 [Ser98]] that for any non-CM elliptic curve $E_{/F}$ over a number field, one has that almost all $E[\ell]$ are irreducible. Therefore, we conclude the following.

Corollary 7. *Suppose $E_{/F}$ is an elliptic curve over a number field, such that E has non-integral j-invariant. Then $\rho_{E,\ell}(G_F) = \mathrm{GL}_2(\ell)$ for almost all primes $\ell \in \mathbb{Z}^+$. (Equivalently, $G := \rho_E(G_F)$ is open in $\mathrm{GL}_2(\hat{\mathbb{Z}})$.)*

1.3. **Examples with non-integral j-invariant.** A pleasant consequence of the above proof showing that non-integral j-invariant implies open image in $\mathrm{GL}_2(\hat{\mathbb{Z}})$, is that one can work with explicit examples of such elliptic curves and deduce what their mod$-\ell$ Galois representations look like.

As an example, Serre consider the elliptic curve

$$E'_{/\mathbb{Q}} : y^2 + x^3 + x^2 + x = 0.$$

With the automorphism $(x, y) \mapsto (-x, y)$, this equation becomes

$$E_{/\mathbb{Q}} : y^2 = x^3 - x^2 + x.$$

Its j-invariant is $2^{11}/3$, which is not an integer. Thus Corollary 7 tells us that $\rho_{E,\ell}(G_{\mathbb{Q}}) = \mathrm{GL}_2(\ell)$ for all but finitely many primes $\ell \in \mathbb{Z}^+$. What do we explicitly know about the various $G_\ell := \rho_{E,\ell}(G_{\mathbb{Q}})$ in this case?

We take a slightly different approach than Serre. First, we observe that the 2-torsion subgroup of E is $E[2] = \{O, (0,0), (\zeta_6^{\pm 1}, 0)\}$ where $\zeta_6 := \frac{1+\sqrt{-3}}{2}$ is a primitive 6'th root of unity. It follows that the 2-division field $\mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{-3})$, which has degree 2 over $\mathbb{Q}$; thus, we see that the mod-2 Galois representation $G_2 := \rho_{E,2}(G_{\mathbb{Q}})$ is cyclic of order 2. We can be more explicit: fix the basis $P := (0,0)$ and $Q := (\zeta_6, 0)$ of $E[2]$; consequently, $(\zeta_6^{-1}, 0) = P + Q$. Then any automorphism $\sigma \in G_{\mathbb{Q}}$ will act on $E[2]$ via $P \mapsto P$ and

$$Q \mapsto \begin{cases} Q & \text{if } \zeta_6^\sigma = \zeta_6 \\ P + Q & \text{if } \zeta_6^\sigma = \zeta_6^{-1}. \end{cases}$$

We deduce that the Galois representation w.r.t. the basis $\{P, Q\}$ is

$$\rho_{E,2}(G_{\mathbb{Q}}) = \left\{ I, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\}.$$

In particular, $\rho_{E,2} : G_{\mathbb{Q}} \to \mathrm{GL}_2(2)$ is not surjective.

What about G_ℓ for odd primes ℓ? We claim that for $\ell > 2$ one has $G_\ell = \mathrm{GL}_2(\ell)$. To show this, let us first take note of two facts about $E_{/\mathbb{Q}}$:

1. For all primes $\ell \in \mathbb{Z}^+$, the mod$-\ell$ cyclotomic character $\chi_\ell : G_\mathbb{Q} \to \mathbb{F}_\ell^\times$ is surjective. This is because ℓ is (trivially) unramified in $\mathbb{Q}$. In particular, since $\det \rho_{E,\ell} = \chi_\ell$ (Weil pairing), this implies that $\det : G_\ell \to \mathbb{F}_\ell^\times$ is surjective.
2. The 3-adic valuation $v_3 : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ is so that $v_3(j(E)) = -1$. Thus the theory of Tate curves kicks in, and for all ℓ with $E[\ell]$ irreducible we have $\mathrm{SL}_2(\ell) \subseteq G_\ell$ (see again [Lemma 1 and 2, IV.3.2 [Ser98]]).

By the two points above, we deduce that $G_\ell = \mathrm{GL}_2(\ell)$ iff $E[\ell]$ is irreducible. Thus, our question becomes: for which $\ell > 2$ is $E[\ell]$ irreducible? Observe that $E[\ell]$ is reducible iff there exists a $\mathbb{Q}$-rational ℓ-isogeny from E to some E', say $\phi : E \to E'$. One way to rule this case out is to note that up to isomorphism there are finitely many elliptic curves defined over $\mathbb{Q}$ which are $\mathbb{Q}$-isogenous to E (e.g. Theorem 5 [Maz78]), and then determine such isogenous curves and *their* isogenies. Then for any other rational isogeny $\varphi : E' \to E$, the composition $\varphi \circ \phi$ is an endomorphism of E, a non-CM elliptic curve. This forces $\deg(\varphi \circ \phi) = \ell \deg(\varphi)$ to be a square. One can check if this is possible. The way Serre does this is by noting that isogenous elliptic curves share the same conductor; this specific elliptic curve has conductor $N = 24$. Serre then cites a list of Ogg which gives all possible elliptic curves of conductor 24, and it can be checked that each such elliptic curve only has rational isogenies of degree $1, 2, 4$ or 8. It follows then that no such ϕ exists, whence $E[\ell]$ is irreducible for all odd primes $\ell \in \mathbb{Z}^+$.

1.4. **The non-CM case.** Following Corollary 7, Serre hypothesizes in 1968 [Ser98] that "non-integral j-invariant" can be replaced with "non-CM". A few years later, he proves this in [Ser72] – this is Theorem 1 stated at the beginning of these notes.

2. Galois Properties of Points of Finite Order on Elliptic Curves: An Overview

Throughout the rest of these notes, unless otherwise stated we let F be a number field, $E_{/F}$ an elliptic curve defined over F without CM and $G := \rho_E(G_F)$ its adelic Galois representation.

2.1. **Some equivalencies via profinite group theory.** This paper is concerned with showing that G is open in $\mathrm{GL}_2(\hat{\mathbb{Z}})$, which by basic profinite group theory is equivalent to G having finite index in $\mathrm{GL}_2(\hat{\mathbb{Z}})$. We note that for a topological group G, one has that G is compact iff for any (and all) normal subgroups $N \trianglelefteq G$ one has that both N and G/N are compact. In our context, the topological group G_F is profinite, whence compact (and so closed). For our adelic representation

$$\rho_E : G_F \to \mathrm{GL}_2(\hat{\mathbb{Z}}),$$

we already know that $\ker \rho_E$ is a normal subgroup of G_F. Therefore, the quotient $G_F/\ker \rho_E \cong \mathrm{Gal}(\overline{F}^{\ker \rho_E}/F)$ is a compact subgroup, hence closed. This is one way to see that the image G of our adelic representation is closed in $\mathrm{GL}_2(\hat{\mathbb{Z}})$.

That G has finite index in $\mathrm{GL}_2(\hat{\mathbb{Z}})$, is equivalent to the index of all mod$-N$ Galois representations $G_N := \rho_{E,N}(G_F) \subseteq \mathrm{GL}_2(N)$ being bounded independently of $N \in \mathbb{Z}^+$. By more profinite group theory, another equivalency to G being open in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ is for G

to contain some basic open neighborhood around $I \in \mathrm{GL}_2(\hat{\mathbb{Z}})$; such open neighborhoods are of the form $\pi_m^{-1}(1_{E[m]})$. In particular, G being open is equivalent to G containing all automorphisms of $E[\mathrm{tors}]$ which act trivially on $E[m]$, for some $m \in \mathbb{Z}^+$.

2.2. **Subgroups of $\mathbf{GL}_2(\ell)$.** As noted in Corollary 6, to show that the adelic representation G is open, it is equivalent to show that G_ℓ contains $\mathrm{SL}_2(\ell)$ for all but finitely many ℓ.

The following proposition is a step towards this.

Proposition 8 (Proposition 16 [Ser72])**.** *Let $G \subseteq \mathrm{GL}_2(\ell)$ be of order divisible by ℓ. Then G either contains $\mathrm{SL}_2(\ell)$ or is contained in a Borel subgroup of $\mathrm{GL}_2(\ell)$.*

We note that [Theorem, IV.2.1 [Ser98]] says that since E has no CM over F, almost all $E[\ell]$ are irreducible. In particular, by the proposition above and Corollary 6, to show that G is open in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ it suffices to show that almost all G_ℓ contain an order ℓ element. Equivalently, we need to show that $\ell \mid \#G_\ell$ for $\ell \gg_{E,F} 0$.

When can we predict that G_ℓ is a subgroup of $\mathrm{GL}_2(\ell)$ which contains an order ℓ element? To help us towards this, Serre gives a classification of subgroups of $\mathrm{GL}_2(\ell)$, see Sections 2.4 and 2.6 [Ser72], essentially due to L. Dickson.

Theorem (Classification of subgroups of $\mathrm{GL}_2(\ell)$)**.** *Let $\ell \in \mathbb{Z}^+$ be prime, and let G be a subgroup of $\mathrm{GL}_2(\ell)$.*

1. *If $\ell \mid \#G$, then one of the following holds:*
   a. *G contains $\mathrm{SL}_2(\ell)$.*
   b. *G is contained in a Borel subgroup of $\mathrm{GL}_2(\ell)$.*
2. *If $\ell \nmid \#G$, then one of the following holds:*
   a. *G is contained in a Cartan subgroup of $\mathrm{GL}_2(\ell)$.*
   b. *G is properly contained in the normalizer of a Cartan subgroup of $\mathrm{GL}_2(\ell)$.*
   c. *The image of G in $\mathrm{PGL}_2(\ell) := \mathrm{GL}_2(\ell)/\mathbb{F}_\ell^\times$ is isomorphic to one of the exceptional groups A_4, S_4 or A_5.*

The first part of this theorem is where Proposition 8 comes from – to emphasize, we know that $E[\ell]$ is irreducible for all but finitely many ℓ, so we can ignore case 1.b.[1] Since we want to show that ℓ divides $\#G_\ell$ for almost all ℓ, we need to show that 2.a, 2.b and 2.c of the theorem also only happen for finitely many ℓ.

2.3. **A sketch of the proof.** Some reductions are in order. First, let us replace F with a finite extension for which E attains semistable reduction, e.g., let us replace F with $F(E[12])$.

Next, we proceed by contradiction: suppose it were the case that infinitely many primes ℓ are with $G_\ell \neq \mathrm{GL}_2(\ell)$; since we can take ℓ arbitrarily large, let us assume that such ℓ are at least 7, are unramified in F and are such that $E[\ell]$ is irreducible. Since $E[\ell]$ is irreducible and ℓ is unramified in F, Proposition 8 implies that $\ell \nmid \#G_\ell$, which puts us into cases 2.a,b,c of Dickson's classification above.

[1] If G_ℓ is Borel, then it is upper triangular up to conjugacy, whence $E[\ell]$ has a nontrivial G_F-stable cyclic subgroup.

Let ℓ be a prime as above, and let w be any prime in $\overline{F}$ lying above ℓ; w is simply a directed union of primes above ℓ, each lying in a unique finite Galois extension of F. Let us set $v := w \cap F$. Let $I_w \subseteq G_F$ be the inertia group of w over v; note that I_w is an inverse limit over the usual finite inertia subgroups from introductory algebraic number theory. A key part of Serre's proof is a thorough study of the "shape" of $\rho_{E,\ell}(I_w)$, which depends on the reduction type of E modulo v.

Since $E_{/F}$ is semistable, E has either ordinary good reduction, supersingular good reduction or multiplicative reduction at v. We have two cases for the "shape" of I_w under $\rho_{E,\ell}$.

(1) E has good ordinary or multiplicative reduction at v: then by Corollaries 7 and 9 [Ser72] $\rho_{E,\ell}(I_w)$ is – up to conjugacy! – a split semi-Cartan subgroup $\left\{\begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} : a \in \mathbb{F}_\ell^\times\right\}$, or a semi-Borel subgroup $\left\{\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : a \in \mathbb{F}_\ell^\times, b \in \mathbb{F}_\ell\right\}$. In particular, the size of the image of inertia is $\ell - 1$ or $\ell(\ell-1)$, respectively.

(2) E has supersingular reduction at v: then Proposition 13 says that $\rho_{E,\ell}(I_w)$ is a non-split Cartan subgroup. This forces G to either be a non-split Cartan subgroup itself, or the normalizer of a non-split Cartan subgroup.

We are assuming that $\ell \nmid \#G_\ell$, which eliminates the case $\rho_{E,\ell}(I_w) = \left\{\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : a \in \mathbb{F}_\ell^\times, b \in \mathbb{F}_\ell\right\}$ (so E has supersingular reduction at v or the wild inertia group I_p acts trivially). In particular, we'll always have that $\rho_{E,\ell}(I_w)$ is cyclic, and of order $\ell - 1$ or $\ell^2 - 1$ depending on whether G_ℓ contains a split semi-Cartan subgroup or a non-split Cartan subgroup. In any case, G_ℓ containing a split semi-Cartan or Cartan subgroup will imply (by Proposition 18 [Ser72]) that the projective image $\overline{G_\ell}$ is not A_4, S_4 or A_5. Therefore, Dickson's classification tells us that G_ℓ is contained in the normalizer of a Cartan subgroup of $\mathrm{GL}_2(\ell)$.

To summarize what we've just shown: G_ℓ contains either a split semi-Cartan subgroup, or the full non-split Cartan subgroup. Furthermore, G_ℓ is contained in the normalizer of a Cartan subgroup. Note that if G_ℓ is contained in the split Cartan subgroup, then G_ℓ is reducible, which is impossible. Thus, either G_ℓ is contained in $C_s^+(\ell)$ but not in $C_s(\ell)$, or is equal to $C_{ns}(\ell)$ or $C_{ns}^+(\ell)$. Let's write what we've just said as two cases:

A. G_ℓ equals a non-split Cartan subgroup.
B. G_ℓ is contained in the normalizer of either a split or non-split Cartan subgroup, but is not contained in the Cartan subgroup itself.

We note that both $C_s(\ell)$ and $C_{ns}(\ell)$ have index two in their normalizers.

Serre reduces Case B to Case A first: suppose $C(\ell)$ is a Cartan subgroup for which $C(\ell) \subseteq G_\ell \subseteq C^+(\ell)$, where $C^+(\ell)$ is the normalizer of $C(\ell)$. Then the composition

$$G_F \xrightarrow{\rho_{E,\ell}} C^+(\ell) \twoheadrightarrow C^+(\ell)/C(\ell) \xrightarrow{\sim} \{\pm 1\}$$

is a surjective quadratic character, which we'll denote by

$$\epsilon_\ell : G_F \twoheadrightarrow \{\pm 1\}.$$

It cuts out a quadratic extension F_ℓ/F, namely $F_\ell := \overline{F}^{\ker \epsilon_\ell}$. Since $\rho_{E,\ell}$ factors through ϵ_ℓ, we have a containment of fixed fields,

$$F_\ell \subseteq \overline{F}^{\ker \rho_{E,\ell}} = F(E[\ell]).$$

We claim that F_ℓ is an unramified extension of F (this is Lemma 8 [Ser72]). To see this, recall that $F(E[\ell])/F$ can only ramify at the primes in F above ℓ, and at the places of bad reduction. Thus F_ℓ/F can only ramify at such places. Recall that we are assuming $E_{/F}$ has semistable reduction, and so bad reduction must be multiplicative.

Let v be an arbitrary finite prime of F; extend v to a prime w of $\overline{F}$. In light of the above, we have three cases to check.

1. v lies above ℓ. Then the analysis at the start of this subsection implies that $\rho_{E,\ell}(I_w)$ is either a semi split-Cartan subgroup or a non-split Cartan subgroup. Since $\rho_{E,\ell}(I_w) \subseteq G_\ell$ and G_ℓ is contained in $C^+(\ell)$, by Proposition 15 [Ser72] this forces $\rho_{E,\ell}(I_w) \subseteq C(\ell)$. In particular, we get $\epsilon_\ell(I_w) = 1$, and so we conclude that F_ℓ is unramified at v.
2. v doesn't lie above ℓ. Let us set $p := v \cap \mathbb{Q}$. We have two cases, depending on reduction of E at v.
   a. E has good reduction at v. Good reduction implies $\rho_{E,\ell}$ is unramified at v (Néron–Ogg–Shafarevich), whence so is ϵ_ℓ.
   b. E has multiplicative reduction at v. By the theory of Tate curves, we have a short exact sequence of G_F-modules

   $$1 \to \mu_\ell \to E[\ell] \to \mathbb{Z}/\ell\mathbb{Z} \to 0$$

   where $\mathbb{Z}/\ell\mathbb{Z}$ is a trivial G_F-module. In particular, our mod$-\ell$ representation is

   $$G_\ell = \operatorname{im} \begin{bmatrix} \chi_\ell & * \\ 0 & 1 \end{bmatrix}.$$

   (That the two characters on the diagonal are χ_ℓ and 1 follows from $\det(G_\ell) = \operatorname{im} \chi_\ell$.) In particular, since $\rho_{E,\ell}(I_w)$ is contained in G_ℓ it follows that $\#\rho_{E,\ell}(I_w) = 1$ or ℓ. The latter case cannot happen since G_ℓ is contained in $C^+(\ell)$ and $\ell \nmid \#C^+(\ell)$.

We conclude that F_ℓ/F is an unramified quadratic extension. If we replace G_ℓ with $G_\ell := \rho_{E,\ell}(G_{F_\ell})$, then from $\epsilon_\ell(G_{F_\ell}) = 1$ we find that $G_\ell \subseteq \ker \epsilon_\ell = \ker(C^+(\ell) \to C(\ell)) = C(\ell)$, whence we are in Case A for ℓ.

By Hermite's Theorem, there are finitely many unramified quadratic extensions of F. In particular, we let us replace F with the compositum of all such F_ℓ. Our base field F is still a number field, but for $\ell \gg 0$ we now have $G_\ell = C_{ns}(\ell)$.

We already know that for ℓ in consideration, the ℓ-adic representations G_{ℓ^∞} are semisimple; for example, they are irreducible, see [Theorem, IV.2.2 [Ser98]]. Furthermore, this system of ℓ-adic representations is rational and strictly compatible, see §3.6 [Ser72]. For $\ell \gg 0$, the reduction G_{ℓ^∞} mod ℓ equals $C_{ns}(\ell)$, which is abelian. The conclusion is that Theorem 6 [Ser72] holds with $N = 1$, and we have that the system (ρ_{E,ℓ^∞}) is isomorphic to some associated ℓ-adic representation of a representation $\varphi_0 : S_{\mathfrak{m}} \to \mathrm{GL}_d(V_{/\mathbb{Q}})$ of an algebraic group $S_{\mathfrak{m}}$. In particular, for any $\ell \gg 0$ the $\ell-$adic

representation of E is *abelian,* which by the contrapositive of the ℓ-adic open image theorem (see Theorem 2) implies that E must have CM, which is a contradiction. We conclude that only finitely many primes $\ell \in \mathbb{Z}^+$ are such that $G_\ell \neq \mathrm{GL}_2(\ell)$. This concludes the sketch of the proof of Serre's adelic open image theorem for non-CM elliptic curves.

References

[BC20] A. Bourdon and P.L. Clark, *Torsion points and Galois representations on CM elliptic curves*, Pacific J. Math. 305 (2020), 43–88.

[Maz78] B. Mazur, *Rational isogenies of prime degree.* Invent. Math. Vol. 44 (1978), 129–162.

[Ser72] J. P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math 15 (1972), 259 – 331.

[Ser98] J. P. Serre, *Abelian l-adic representations and elliptic curves*, Research Notes in Mathematics (1998).