ℓ-adic Representations of Elliptic Curves

Naina Praveen

May, 2024

Contents

Introduction

The study of Galois actions on points of finite order on elliptic curves over number fields constitutes a fundamental aspect of arithmetic geometry. Given an elliptic curve E/K over a number field K, the absolute Galois group $G_K := \mathrm{Gal}(\overline{K}/K)$ acts on the torsion subgroup $E[\mathrm{tors}]$ (for example, via $(x, y)^\sigma = (x^\sigma, y^\sigma)$). For any positive integer n, one obtains the *mod - n representation* $\rho_{E,n} : G_K \to \mathrm{Aut}(E[n])$. By passing to the inverse limit on n, the group $\mathrm{Aut}\, E[\mathrm{tors}]$ comprising of all automorphisms of the torsion points of E is obtained, and a continuous homomorphism $\rho_\infty : G \to \mathrm{Aut}(E[\mathrm{tors}])$ is established. Serre in his paper "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques" [1] shows that for an elliptic curve without complex multiplication (CM) the group $\rho_\infty(G_K)$ is open in $\mathrm{GL}_2(\hat{\mathbb{Z}})$.

If one were to rephrase this and let ℓ be any prime in the set of primes $\mathcal{P}$, and let $E[\ell^\infty] = \varprojlim_n E[\ell^n]$, then one has

$$E[\mathrm{tors}] = \bigoplus_{\ell \in \mathcal{P}} E[\ell^\infty]$$

and

$$\mathrm{Aut}\, E[\mathrm{tors}] = \prod_{\ell \in \mathcal{P}} \mathrm{Aut}\, E[\ell^\infty] \cong \prod_{\ell \in \mathcal{P}} \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Serre's open image theorem then states that for elliptic curves without CM, $\rho_\ell : G_K \to \mathrm{GL}_2(\mathbb{F}_\ell)$ is surjective for all but finitely many $\ell \in \mathcal{P}$. This is to say that the degree of its ℓ^{th} division fields $K(E[\ell])$ is "as large as possible", i.e., $[K(E[\ell]) : K] = (\ell^2 - 1)(\ell^2 - \ell)$. This is in contrast with the CM case, where if E is a an elliptic curve with CM over a quadratic field K, then one can show that the image of $\rho_\ell(G)$ is abelian in $\mathrm{Aut}\, T_\ell$. For more details, see [1] §4.5.

The proof heavily relies on the theory established in Serre's antecedent work, "Abelian ℓ-adic Representations" [2]. A key component of this proof is the criterion for irreducibility of non-CM elliptic curves (see [2] Theorem IV 2.2), which states that for almost all prime numbers ℓ, $E[\ell]$ is an irreducible G_K-module. Further, under the assumption that the j-invariant is not an integer in K, Serre proceeds to prove that $\rho_\ell(G_K) = \mathrm{GL}_2(\mathbb{F}_\ell)$ for almost all ℓ (see [2] IV 3.2). He then raises the question of whether one could substitute the condition "j is non-integral" with the weaker requirement that E possesses no CM, which is the principal outcome in [1].

Serre's proof is a proof by contradiction and is not exactly constructive. Hence, identifying examples of surjective ρ_∞ is not straightforward. In the same paper, Serre shows that if $K = \mathbb{Q}$, then in fact, $\rho_\infty(G_\mathbb{Q}) \neq \mathrm{GL}_2(\hat{\mathbb{Z}})$ for any elliptic curve E over $\mathbb{Q}$. In partial answer to that question, Zywina in [3] shows that "most" elliptic curves do have surjective $\rho_{E,\ell}$ when $K \neq \mathbb{Q}$. Zywina's proof involves a very different approach from Serre's – using large sieve methods, one can sieve out certain elliptic curves modulo specific primes and obtain the result.

Chapters 1 and 2 provide technical background and theory behind Serre's proof in [1], Chapter 3 provides a brief overview of the proof along with some explicit examples, and 4 delves into Zywina's methods and proof behind $\rho_{E,\ell}$ being surjective for all ℓ for "most" curves.

Lastly, I would like to thank Prof. Jack Thorne for his constructive feedback that has helped improve this exposition.

1. Background

In this chapter, we introduce elliptic curves and provide some important results about them, primarily drawn from [4], [5]. We then introduce the notion of ℓ-adic representations and define rational and compatible systems of the same. Lastly, we make some remarks on Class Field Theory with further references. Throughout this chapter, and for the rest of this essay, ℓ and p shall denote primes.

1.1 Elliptic curves and Tate modules

An elliptic curve E over a field K is a non-singular, smooth, projective, algebraic curve of genus one, on which there is a specified point O_E at infinity, defined by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

The points $E(K)$ naturally form a geometrically defined group structure, with the point at infinity O_E as the identity element.

An *endomorphism* of E is a morphism from E to itself that fixes O_E. For every integer n, multiplication by n on E yields an endomorphism of E, denoted by $[n]$. $E[n]$ denotes the kernel of the endomorphism $[n]$. If $n \neq 0$, then the endomorphism $[n]$ is nonzero and has degree n^2. When n is prime to the characteristic of K, the kernel of $[n]$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$ (See [4] Proposition III.4.2 and Corollary III.6.4).

Denote $\mathrm{End}_K(E)$ to be the ring of endomorphisms of an elliptic curve E over K. From the previous paragraph, it is evident that $\mathbb{Z} \hookrightarrow \mathrm{End}_K(E)$. Usually, the story ends there and $\mathrm{End}_K(E) \cong \mathbb{Z}$, but if $K = \mathbb{C}$, then certain elliptic curves have endomorphism rings that are larger than just $\mathbb{Z}$. In fact, these rings are isomorphic to an order $\mathcal{O}$ in a totally imaginary quadratic extension (see [4] A.C Proposition 11.1.1 or [5] II.§1.) and elliptic curves with these larger endomorphism rings are called elliptic curves with *complex multiplication.*

In particular, if K has characteristic $p > 0$ (not necessarily finite), then the two aforementioned objects $E[p]$ and $\mathrm{End}(E)$ are intertwined by the following theorem.

Theorem 1.1. *Let K be a field of characteristic p. For integer $r \geq 1$, let*

$$\phi_r : E \longrightarrow E^{p^r} \quad \textit{and} \quad \hat{\phi}_r : E^{p^r} \longrightarrow E$$

be the p^r-power Frobenius map and its dual.

(i) Then the following are equivalent:

(a) $E[p^r] = 0$ for one $r \geq 1$.

(b) The map $[p] : E \to E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$

(c) $\mathrm{End}(E)$ is an order in a quarternion algebra.

(ii) If the conditions in (i) do not hold, then

(a) $E[p^r] = \mathbb{Z}/p^r\mathbb{Z}$ for all $r \geq 1$

(b) If $j(E) \in \overline{\mathbb{F}}_p$, then $\mathrm{End}(E)$ is an order of a quadratic imaginary field.

Proof. See [4] Chapter V Theorem 3.1. □

Definition 1.1. If E satisfies condition in (i), it is said to be *supersingular*. If E satisfies conditions from (ii), it is said to be *ordinary*.

For any prime ℓ (and its powers), $E[\ell]$ enables us to define further interesting objects.

Definition 1.2. Let ℓ be a rational prime. Define the *ℓ-adic Tate Module* to be

$$T_\ell(E) = \varprojlim_n E[\ell^n]$$

the inverse limit with respect to the maps $\ell : E[\ell^{n+1}] \to E[\ell^n]$. If $\operatorname{char} K \neq \ell$, then $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ as a $\mathbb{Z}_\ell$-module. If $p = \operatorname{char} K$, then $T_p(E) \cong \{0\}$ or $\mathbb{Z}_p$ (see [4] III.7 Proposition 7.1). Let $G_K := \operatorname{Gal}(\overline{K}/K)$. The action of G_K on each $E[\ell^n]$ commutes with the multiplication-by-ℓ map used to form the inverse limit, so G_K also acts on $T_\ell(E)$. Further, since the profinite group G_K acts continuously on each finite (discrete) group $E[\ell^n]$, the resulting action on $T_\ell(E)$ is also continuous.

Definition 1.3. For an ℓ-adic Tate module T_ℓ, define

$$V_\ell = T_\ell \left[\frac{1}{\ell}\right] = T_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

T_ℓ is a free $\mathbb{Z}_\ell$-module of rank 2 while V_ℓ is a $\mathbb{Q}_\ell$-vector space of dimension 2. $\mathrm{GL} T_\ell$ is isomorphic to $\mathrm{GL}_2(\mathbb{Z}_\ell)$, while $\mathrm{GL} V_\ell$ is isomorphic to $\mathrm{GL}_2(\mathbb{Q}_\ell)$.

Definition 1.4. The *ℓ-adic representation* (of G_K associated to E) is the homomorphism

$$\rho_\ell : G_K \longrightarrow \mathrm{GL} T_\ell \subset \mathrm{GL} V_\ell$$

induced by the action of G_K on the ℓ^n-torsion points of E.

1.2 Elliptic curves over Local Fields

In this section, let K be a local field, in particular $K = \mathbb{Q}_p$ for some prime p. Let the valuation ring of K be denoted as $\mathcal{O}_K = \{x \in K : v(x) \geq 0\} \cup \{0\}$ and its units be denoted as $\mathcal{O}_K^\times = \{x \in K : v(x) = 0\}$. Let $\mathfrak{p}$ be the unique maximal ideal of K, π the generator of $\mathfrak{p}$, $k = \mathcal{O}_K/\mathfrak{p}$ the residue field of K.

Definition 1.5. A Weierstrass equation of an elliptic curve E over a K with $a_1, \dots, a_6 \in K$ is *integral* is $a_1, \dots, a_6 \in \mathcal{O}_K$. It is *minimal* if $v(\Delta)$ is minimal among all integral Weierstrass equations of E, where Δ denotes the discriminant of E.

The reduction $\tilde{E}$ of E is the curve defined over the residue field k by the Weierstrass equation

$$y^2 + \tilde{a_1}xy + \tilde{a_3}y = x^3 + \tilde{a_2}x^2 + \tilde{a_4}x + \tilde{a_6}$$

where the a_i's are the coefficients of a minimal Weierstrass equation for E and $\tilde{a_i}$ denotes the image of a_i in k. The reduction $\tilde{E}$ is independent up to isomorphism of the particular minimal equation chosen for E ([4] Proposition VII.1.3(b)).

Definition 1.6. Let E/K be an elliptic curve, and let $\tilde{E}$ be the reduction modulo $\mathfrak{p}$ of a minimal Weierstrass equation for E.

(i) E has *good (or stable)* reduction if $\tilde{E}$ is nonsingular.

(ii) E has *multiplicative (or semistable)* reduction if $\tilde{E}$ has a node.

(iii) E has *additive (or unstable)* reduction if $\tilde{E}$ has a cusp.

In cases (ii) and (iii) we say that E has *bad reduction.* A curve E is said to be *semistable* if it has multiplicative reduction at every bad prime. If E has multiplicative reduction, then the reduction is said to be *split* if the slopes of the tangent lines at the node are in k, and otherwise it is said to be *nonsplit.*

The next proposition explains how reduction type behaves under field extensions.

Theorem 1.2 (Semistable reduction theorem)**.** *Let E/K be an elliptic curve.*

(i) Let K'/K be an unramified extension. Then the reduction type of E over K (good, multiplicative, or additive) is the same as the reduction type of E over K'.

(ii) Let K'/K be a finite extension. If E has either good or multiplicative reduction over K, then it has the same reduction type over K'.

(iii) There exists a finite extension K'/K such that E has either good or (split) multiplicative reduction over K'

Proof. See [4] VII.5. Proposition 5.4. □

1.3 ℓ-adic representations

In this section, let K be a number field and let Σ_K denote the set of all finite places of K. Let $k_{\mathfrak{p}}$ denote the residue field of K with respect to a valuation $v_{\mathfrak{p}} \in \Sigma_K$, let p be its characteristic and $N(\mathfrak{p}) = p^{\deg(\mathfrak{p})}$ be its cardinality, where $\deg(\mathfrak{p})$ is the degree of the extension of $k_{\mathfrak{p}}$ over $\mathbb{F}_p$. The *ramification index* $e_{\mathfrak{p}}$ of $\mathfrak{p}$ is $v_{\mathfrak{p}}(p)$.

Let L/K be a Galois extension and $\mathfrak{P} \in \Sigma_L$.

Definition 1.7. The *decomposition group* $D_{\mathfrak{P}}$ is the set of all $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\mathfrak{P}) = \mathfrak{P}$.

As the restriction of $v_{\mathfrak{P}}$ to K is an integral multiple of an element $v_{\mathfrak{p}} \in \Sigma_K$, we abuse language and say $\mathfrak{p}$ is the restriction of $\mathfrak{P}$ in K and denote it as $\mathfrak{P} \mid \mathfrak{p}$ ("$\mathfrak{P}$ divides $\mathfrak{p}$"). Denote $L_{\mathfrak{P}}$ and $K_{\mathfrak{p}}$ to be the completion of L and K with respect to $v_{\mathfrak{P}}$ and $v_{\mathfrak{p}}$ respectively. There is a surjective map

$$res : \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \longrightarrow \mathrm{Gal}(l_{\mathfrak{P}}/k_{\mathfrak{p}})$$

the kernel of which is called the *inertia subgroup* $I_{\mathfrak{P}}$.

Definition 1.8. The valuation corresponding to $\mathfrak{P}$ is called *unramified* if $I_{\mathfrak{P}} = \{1\}$.

Definition 1.9. The quotient $D_{\mathfrak{P}}/I_{\mathfrak{P}}$ is a finite cyclic group generated by the *Frobenius element* $\mathrm{Frob}_{\mathfrak{P}}$.

For more details on the aforementioned groups, the reader may refer to [6] I.§7. We now apply these definitions to the ℓ-adic representations introduced in §1.1, following closely I.§2 from [2]. Prior to that, we remark that the definition of ℓ-adic representation introduced in §1.1 is a specific example of a slightly more general definition given below.

Definition 1.10. Let ℓ be a prime number and V a finite-dimensional vector space over $\mathbb{Q}_\ell$ of ℓ-adic numbers. An *ℓ-adic representation* of a group G is a continuous homomorphism $\rho : G \to \mathrm{Aut}(V)$.

Definition 1.11. let $\rho : G_K \to \mathrm{Aut}(V)$ be an ℓ-adic representation and $\mathfrak{p} \in \Sigma_K$. We say ρ is *unramified* at $\mathfrak{p}$ if $\rho(I_{\mathfrak{P}}) = \{1\}$ for any $\mathfrak{P} \in \Sigma_{\overline{K}}$ extending $\mathfrak{p}$. If A is a set on which G_K acts, A is *unramified* at $\mathfrak{p}$ if the action of $I_{\mathfrak{P}}$ on A for some $\mathfrak{P}$ extending $\mathfrak{p}$ is trivial.

Proposition 1.3. *Let E/K be an elliptic curve such that the reduced curve $\tilde{E}/K$ is non-singular. If n is an integer relatively prime to $\mathrm{char}(k)$, then $E[n]$ is unramified at $\mathfrak{p}$.*

Proof. See [4] VII.4 Proposition 4.1. □

A converse to this statement also holds, proven by Néron, Ogg and Shafarevich, which characterises the non-singularity of $\tilde{E}/k$ in terms of the action of the inertia group on the torsion points.

Theorem 1.4 (Criterion of Néron-Ogg-Shafaverich)**.** *Let E/K be an elliptic curve. Then the following are equivalent:*

(i) E has good reduction at K.

(ii) $E[n]$ is unramfied at all $\mathfrak{p}$ for all integers $n \geq 1$ that are relatively prime to $\mathrm{char}(k)$*.*

(iii) $E[n]$ is unramified at $\mathfrak{p}$ for infinitely many integers $n \geq 1$ that are relatively prime to $\mathrm{char}(k)$

(iv) The Tate module $T_\ell(E)$ is unramified at $\mathfrak{p}$.

Proof. See [4] VII.7 Theorem 7.1. □

There is another Theorem by Shafaverich, that has some important corollaries, in particular that the action of G_K on $E[\ell]$ is irreducible.

Theorem 1.5 (Shafaverich)**.** *Fix an elliptic curve E/K. Then there are only finitely many elliptic curves E/K that are K-isogenous to E.*

Proof. See [4] Chapter IX, §6.1. Corollary 6.2. □

Using this, we can deduce an important corollary, which was one of the main theorems of Serre in [2]. We follow the proof given in [4] Chapter IX Corollary 6.2.

Theorem 1.6. *Let E/K be an elliptic curve with no complex multiplication. Then for all but finitely many primes ℓ, the group of ℓ-torsion points $E[\ell]$ has no nontrivial G_K-invariant subgroups. In other words, the representation of G_K on $E[\ell]$ is irreducible for almost all primes ℓ.*

Proof. Suppose $H_\ell \subset E[\ell]$ is a non-trivial G_K-invariant subgroup of $E[\ell]$. As $E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$, H_ℓ is necessarily cyclic of order ℓ. Using the fact that for an elliptic curve E' and a finite subgroup $H \subset E'$ there is a unique elliptic curve E'' and a separable isogeny $\phi : E' \to E''$ satisfying $ker(\phi) = H$ (see [4] III.4.12 for this claim), one can obtain an elliptic curve E_ℓ/K and an isogeny $\phi_\ell : E \to E_\ell$ with kernel $ker(\phi_\ell) = H_\ell$. The Galois invariance of H_ℓ ensures that the curve E_ℓ and ϕ_ℓ are defined over K. As each E_ℓ is K-isogenous to E, Theorem 1.5 says that E_ℓ will fall into finitely many K-isomorphism classes. Suppose $E_\ell \cong E_{\ell'}$ for two primes ℓ and ℓ'. Then, the composition

$$E \xrightarrow{\phi_\ell} E_\ell \cong E_{\ell'} \xrightarrow{\hat{\phi}_{\ell'}} E$$

defines an endomorphism of E of degree $(\deg \phi_\ell)(\deg \hat{\phi_{\ell'}}) = \ell\ell'$. As by assumption E has no complex multiplication, every endomorphism of E has degree n^2 for some $n \in \mathbb{Z}$. This shows that $\ell = \ell'$, and so $E_\ell \not\cong E_{\ell'}$ for $\ell \neq \ell'$. Therefore, there are only finitely many primes ℓ for which such a subgroup H and a curve E_ℓ can exist.

□

Remark 1. Theorem 1.6 is equivalent to the fact that V_ℓ is irreducible for all primes ℓ.

Now, if $\mathfrak{p} \in \Sigma_K$ is unramified with respect to ρ, then $\rho(I_{\mathfrak{P}}) = \{1\}$ for any extension $\mathfrak{P}$ over $\mathfrak{p}$, and the restriction of ρ to $D_{\mathfrak{P}} \subset G_K$ factors through $D_{\mathfrak{P}}/I_{\mathfrak{P}}$. As $D_{\mathfrak{P}}/I_{\mathfrak{P}}$ is generated by $\mathrm{Frob}_{\mathfrak{P}}$, $\rho(\mathrm{Frob}_{\mathfrak{P}}) \in \mathrm{Aut}(T_\ell(E))$ is defined. Call this the *Frobenius of* $\mathfrak{P}$ in the representation ρ, and denote it as $\mathrm{Frob}_{\mathfrak{P},\rho}$. The conjugacy class of $\mathrm{Frob}_{\mathfrak{P},\rho}$ in $\mathrm{Aut}(T_\ell(E))$ only depends on $\mathfrak{p}$, so we may denote it as $\mathrm{Frob}_{\mathfrak{p},\rho}$. Then, for an unramified $\mathfrak{p}$, let $P_{\mathfrak{p},\rho}(T)$ denote the polynomial $\det(1 - \mathrm{Frob}_{\mathfrak{P},\rho} T)$.

Definition 1.12. An ℓ-adic representation of K is said to be *rational* (resp, *integral*) if there exists a finite set $S \subset \Sigma_K$ such that

(i) Any element of $\Sigma_K - S$ is unramified with respect to ρ.

(ii) if $\mathfrak{p} \notin \Sigma_K$, then the coefficients of $P_{\mathfrak{p},\rho}$ lie in $\mathbb{Q}$ (resp. in $\mathbb{Z}$).

The ℓ-adic representation $\rho : G_K \to \mathrm{Aut}(T_\ell(E))$ is rational. Now, we define compatible systems of ℓ-adic representations, a key ingredient in Serre's proof.

Definition 1.13. Let ℓ and ℓ' be distinct primes and let ρ be a ℓ-adic representation of K and ρ' be a ℓ'-adic representation of K. Assume ρ, ρ' are rational. Then, ρ, ρ' are said to be *compatible* if there exists a finite subset S of Σ_K such that ρ and ρ' are unramified outside S and $P_{\mathfrak{p},\rho}(T) = P_{\mathfrak{p},\rho'}(T)$ for all $\mathfrak{p} \in \Sigma_K - S$.

Definition 1.14. If $\rho : G_K \to \mathrm{Aut}(V)$ is a rational ℓ-adic representation of K, then V has a composition series

$$V = V_0 \supset V_1 \supset \ldots \supset V_r = 0$$

of ρ-invariant subspaces with V_i/V_{i+1} $(0 \leq i \leq r-1)$ irreducible (or simple). The ℓ-adic representation ρ^{ss} of K defined by $V' = \sum_{i=0}^{r-1} V_i/V_{i+1}$ is semi-simple, rational and compatible with ρ. ρ^{ss} shall be called the *semi-simplification* of V. In particular, for a 2-dimensional representation ρ, if ρ is irreducible, then $\rho^{ss} = \rho$. Otherwise, if ρ is reducible, then there is a subspace on which ρ acts via a character, so ρ can be expressed as $\begin{pmatrix} \varphi_1 & * \\ 0 & \varphi_2 \end{pmatrix}$. The semisimplification ρ^{ss} is then given by the matrix $\begin{pmatrix} \varphi_1 & 0 \\ 0 & \varphi_2 \end{pmatrix}$.

Serre's proof is a proof by contradiction. It entails constructing two sets of compatible, rational, semi-simple ℓ-adic representations. The subsequent theorem implies that both the constructed sets ought to be the same, that Serre then uses to arrive at a contradiction. The theorem goes as follows.

Theorem 1.7. *Let ρ be an ℓ-adic representation of K, and let ℓ' be another prime. Then, there exists up to isomorphism, at most one ℓ'-adic rational representation ρ' of K which is semi-simple and compatible with ρ.*

Proof. See [1] Chapter I, I-10 Theorem. □

Next, we state an important density theorem, the Chebotarev density theorem that is utilized in the proof of the theorem above, and in proofs to come.

Theorem 1.8 (Chebotarev Density Theorem)**.** *Let L/K be a finite Galois extension of a number field K, with Galois group* $\mathrm{Gal}(L/K)$*. Let X be a subset of* $\mathrm{Gal}(L/K)$*, stable under conjugation. Let P_X be the set of places $\mathfrak{p} \in \Sigma_K$, unramified in L, such that the Frobenius class* $\mathrm{Frob}_\mathfrak{p}$ *is contained in X. Then P_X has density equal to* $\mathrm{Card}(X)/\mathrm{Card}(\mathrm{Gal}(L/K))$*.*

Proof. See [2] I.2.3 Theorem. □

1.4 Class Field Theory

In this section, let Σ_K denote the set of finite places of a number field K and let Σ_K^∞ denote the set of archimedean absolute values of K. Set $\overline{\Sigma}_K := \Sigma_K \cup \Sigma_K^\infty$. Let $\mathfrak{p}$ be a prime of K, finite or infinite. Then $K_\mathfrak{p}$, the completion of K with respect to $\mathfrak{p}$, is either a p-adic field for some prime p, $\mathbb{R}$ or $\mathbb{C}$. Let $\pi_\mathfrak{P}$ denote the maximal ideal of $K_\mathfrak{P}$. Let $k_\mathfrak{p}$ denote the residue field of K with respect to $\mathfrak{p}$. Let S be a finite subset of Σ_K. Then, a modulus of support S is a family $\mathfrak{m} = (m_\mathfrak{p})_{\mathfrak{p}\in S}$ where $m_\mathfrak{p}$ are integers greater than 1.

Definition 1.15. The group $\mathbb{I}_K$ of *idèles* is the topological group

$$\prod_{\mathfrak{p}\in\overline{\Sigma}_K}^{res} (K_\mathfrak{p}^\times, \mathcal{O}_{K_\mathfrak{p}}^\times) = \{(x_\mathfrak{p}) : x_\mathfrak{p} \in \mathcal{O}_{K_\mathfrak{p}}^\times \text{ for all but finitely many } \mathfrak{p} \in \overline{\Sigma}_K\} \subset \prod K_\mathfrak{p},$$

where, $\mathcal{O}_{K_\mathfrak{p}} = K_\mathfrak{p}$ if $\mathfrak{p}$ is infinite. It is endowed with a topology that decrees that the subgroup (with respect to the product topology)

$$\prod_{\mathfrak{p}\in\Sigma_K^\infty} K_\mathfrak{p}^\times \times \prod_{\mathfrak{p}\in\Sigma_K} \mathcal{O}_{K_\mathfrak{p}}$$

is open.

Clearly, $K^\times$ can be embedded into $\mathbb{I}_K$ be sending $a \in K^\times$ into the idèle $(a_\mathfrak{p})$ where $a_\mathfrak{p} = a$ for all $\mathfrak{p}$. The *idèle class group* is the quotient group $\mathbb{C} := \mathbb{I}_K/K^\times$.

For a modulus $\mathfrak{m} = \prod_\mathfrak{p} \mathfrak{p}^{r_\mathfrak{p}}$, write

$$U_\mathfrak{p}^{r_\mathfrak{p}} = \begin{cases} \mathcal{O}_{K_\mathfrak{p}}^\times & \text{if } \mathfrak{p} \text{ is finite, } r_\mathfrak{p} = 0 \\ 1 + \mathfrak{p}^{r_\mathfrak{p}} & \text{if } \mathfrak{p} \text{ is finite, } r_\mathfrak{p} \geq 0 \\ \mathbb{R}^\times = K_\mathfrak{p}^\times & \text{if } \mathfrak{p} \text{ is real, } r_\mathfrak{p} = 0 \\ \mathbb{R}^+ \subset K_\mathfrak{p}^\times & \text{if } \mathfrak{p} \text{ is real, } r_\mathfrak{p} = 1 \\ \mathbb{C}^\times = K_\mathfrak{p}^\times & \text{if } \mathfrak{p} \text{ is complex,} \end{cases}$$

For any modulus $\mathfrak{m}$, write $\alpha \equiv 1 \mod \mathfrak{m}$ if $\alpha_\mathfrak{p} \equiv 1 \mod \mathfrak{p}^{r_\mathfrak{p}}$ for all $\mathfrak{p}$.

Definition 1.16. $\mathbb{I}_K(\mathfrak{m}) = \{\alpha \in \mathbb{I}_K : \alpha \equiv 1 \mod \mathfrak{m}\}$

Then, $\mathbb{I}_K(\mathfrak{m}) = \prod_\mathfrak{p} U_\mathfrak{p}^{r_\mathfrak{p}} \subset \mathbb{I}_K$.

Definition 1.17. $C_K(\mathfrak{m}) = \mathbb{I}_K(\mathfrak{m})K^\times/K^\times \subset C_K$ is the *congruence subgroup modulo* $\mathfrak{m}$.

Definition 1.18. The quotient $C_\mathfrak{m} = C_K/C_K(\mathfrak{m}) = \mathbb{I}_K/K^\times\mathbb{I}_K(\mathfrak{m})$ is called the *ray class group modulo* $\mathfrak{m}$.

Theorem 1.9. *There is an exact sequence*

$$1 \longrightarrow K^\times/\mathbb{I}_K(\mathfrak{m}) \cap K^\times \longrightarrow \mathbb{I}_K/\mathbb{I}_K(\mathfrak{m}) \longrightarrow C_\mathfrak{m} \longrightarrow 1. \tag{1.1}$$

Furthermore, $C_\mathfrak{m}$ is a finite group.

Proof. See [7] Theorem Chapter V Theorem 1.7. □

The reason one studies these ray class groups modulo $\mathfrak{m}$ is to use it to understand statements from global Class Field theory. From the Artin Reciprocity Theorem (see [7] Chapter V Theorem 3.5, 3.6, 5.3), for any number field K, the Artin Map

$$\Phi_K : \mathbb{I}_K \longrightarrow \mathrm{Gal}(K^{ab}/K)$$

is surjective and gives is a canonical isomorphism

$$\varprojlim_{\mathfrak{m}} C_\mathfrak{m} \xrightarrow{\sim} \mathrm{Gal}(K^{ab}/K). \tag{1.2}$$

Let ∞ denote the set of infinite primes of K and let $K_\mathfrak{p}^+$ denote the connected component of $K_\mathfrak{p}^\times$. Clearly, $\prod_{\mathfrak{p}|\infty} K_\mathfrak{p}^+ \subset \mathrm{Ker}(\phi_K)$. By definition, $K^\times \subset \mathrm{Ker}(\phi_K)$, and so $K^\times \cdot \left(\prod_{\mathfrak{p}|\infty} K_\mathfrak{p}^+\right) \subset \mathrm{Ker}(\phi_K)$. But ϕ_K is a continuous homomorphism and $\mathrm{Gal}(K^{ab}/K)$ is Hausdorff (under the Krull topology), and so the kernel is a closed subgroup. Thus, $\mathrm{Ker}(\phi_K)$ contains the closure of $K^\times \cdot \left(\prod_{\mathfrak{p}|\infty} K_\mathfrak{p}^+\right)$. It is a theorem that this is precisely the kernel. The image of the closure of $K^\times \cdot \left(\prod_{\mathfrak{p}|\infty} K_\mathfrak{p}^+\right)$ in C_K is the connected component of C_K containing 1.

For every finite abelian extension L of K, the Artin map defines and isomorphism $C_K/\,\mathrm{N}(C_L) \to \mathrm{Gal}(L/K)$, where N is the norm map. When we pass to the inverse limit over L, we get an isomorphism with $\mathrm{Gal}(K^{ab}/K)$ on the right. For now, we shall call the kernel of this isomorphism D. This group shall be used in Section 2.1 to construct a compatible system of ℓ-adic representations. For more details on local Class Field Theory and the claims above, see [7].

2. Preliminaries for Serre's Proof

The goal of this chapter is to set the groundwork before we delve into Serre's proof. First, we construct a commutative set $S_{\mathfrak{m}}$ that allows us to construct a system of abelian ℓ-adic representations. Then, we go on a bit of a detour and classify the subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$. Lastly, we describe the tame inertia groups and its characters.

2.1 Construction of $S_{\mathfrak{m}}$

The purpose of this section is to construct a projective family $(S_{\mathfrak{m}})$ of commutative algebraic groups over $\mathbb{Q}$. In order to construct such a group, one must first look at an algebraic construction called the Weil restriction (or the "restriction of scalars"). The section introducing Weil restrictions largely follows from [8] Chapter 4, §4.6., while the section on constructing $S_{\mathfrak{m}}$ follows from [2] Chapter II.

The motivation behind Weil restrictions is that for a field extension L/K and a L-variety X, one can find a canonical way of obtaining a K-variety, say $R_{L/K}(X)$ that "behaves the same way" over K as X does over L. More specifically, if L is a number field and X is a L-variety, then one can use the Weil restriction to work over the field of rationals instead of L. Further, if X is an algebraic group, then $R_{L/K}(X)$ has the structure of an algebraic K-group.

Before stating the definitions, it might be insightful to look at an example first.

Example 1. Let $\mathbb{C}/\mathbb{R}$ be the field extension and let $\mathbb{G}_m := \mathbb{C}[X, X^{-1}]$ be the multiplicative group over $\mathbb{C}$ (equivalently, $\mathbb{G}_m = \mathbb{C}[X, X^{-1}] = \mathbb{C}[X][X^{-1}] = \mathbb{C}[X_1, X_2]/(X_1X_2 - 1) \cong \mathbb{A}^1\backslash\{0\}$). Using $\{1, i\}$ as a basis for $\mathbb{C}/\mathbb{R}$, one can write $X_1 = V_1 + iV_2$ and $X_2 = V_3 + iV_4$. Then, $X_1X_2 - 1$ simplifies to the following to relations

$$V_1V_4 + V_2V_3 = 0$$
$$V_1V_3 - V_2V_4 = 1$$

Then, the Weil restriction $R_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_m)$ is given by

$$R_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_m) = \frac{\mathbb{R}[X_1, X_2, X_3, X_4]}{(X_1X_4 + X_2X_3)(X_1X_3 - X_2X_4 - 1)}.$$

Later, we will show this is actually a torus isomorphic to $\mathbb{C}^\times$.

Definition 2.1. Let L/K be a field extension and let X be a L-variety. The Weil restriction $R_{L/K}(X) = \mathfrak{X}$, if it exists, is a K-variety characterised by the existence of bijections between $\mathrm{Hom}_K(S, \mathfrak{X}) \to \mathrm{Hom}_L(S \times_L L, X)$ for each K-scheme S varying functorially.

But, what exactly does this mean? "Varying functorially in S" means that for any K morphism $f : S \to T$, the diagram

$$\begin{tikzcd}
\mathrm{Hom}_K(T, \mathfrak{X}) \arrow[r] \arrow[d] & \mathrm{Hom}_L(T \times_L L, X) \arrow[d] \\
\mathrm{Hom}_K(S, \mathfrak{X}) \arrow[r] & \mathrm{Hom}_L(S \times_L L, X)
\end{tikzcd}$$

is induced by f and its base extension $f_L : S \times_K X \to T \times_K X$ (i.e., the map given by precomposing with f gives a contravariant functor) commutes. In other words, for a K-variety Y, $\mathrm{Mor}_L(Y_{/L}, X) = \mathrm{Mor}_K(Y, \mathfrak{X})$.

In particular, if X is an affine L-variety, then one can explicitly describe the construction of $\mathfrak{X}$. Say $X = \mathrm{Spec}(L(Y_1 \dots, Y_n))/J$, let $d = [L : K]$ and $a_1, \dots a_d$ be a K basis for L. Then one can make the substitution

$$Y_i = a_1 V_{i1} + ... + a_d V_{id},$$

thus replacing each Y_i by a linear expression in d new variables V_{ij}. Moreover, suppose $J = \langle g_1, ..., g_m \rangle$; then substituting each of the above equations into $g_k(Y_1, ..., Y_n)$, we get a polynomial in the V-variables, however still with L-coefficients. Now, using the fixed basis of L/K, consider a single polynomial with L-coefficients as a vector of d polynomials with K coefficients. Thus, we end up with md generating polynomials in the V-variables, say generating an ideal I in $K[V_{ij}]$. Then, put $R_{L/K}(X) = \mathrm{Spec}\, K[V_{ij}]/I$.

Theorem 2.1 (Weil, [8] Chapter 4 §4.6.)**.** *Let L/K be a finite Galois extension with Galois group G. Let X be a L variety. If $R_{L/K}(X) = \mathfrak{X}$ exists, then*

$$\mathfrak{X}_L = \prod_{\sigma \in G} X^\sigma$$

as L-varieties.

Going back to Example 1, from the above theorem, the Weil restriction $R_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_m) \times_{\mathbb{R}} \mathbb{C} = \prod_{\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})} \mathbb{G}_m$, and so by definition is a torus.

With the definition of Weil restriction established, one can now proceed to construct $S_{\mathfrak{m}}$.

Let K be a number field and $\mathbb{G}_m$ the multiplicative group over K. Define $T = R_{K/\mathbb{Q}}(\mathbb{G}_m)$. If A is a commutative $\mathbb{Q}$-algebra, then the points of T with values in A form the multiplicative group $(K \otimes_{\mathbb{Q}} A)^\times$ of invertible elements $K \otimes_{\mathbb{Q}} A$. In particular, $T(\mathbb{Q}) = K^\times$. From Theorem 2.1, it is clear that if $d = [K : \mathbb{Q}]$, then T is a torus of dimension d, i.e., $T_{/\overline{\mathbb{Q}}} = T \times_{\mathbb{Q}} \overline{\mathbb{Q}}$ is isomorphic to $\mathbb{G}_{m/\overline{\mathbb{Q}}} \times \ldots \times \mathbb{G}_{m/\overline{\mathbb{Q}}}$ (d times).

In order to construct $S_{\mathfrak{m}}$, one actually "enlarges" a quotient of the torus T described above. We make this more precise below.

Let k be a field and A a commutative algebraic group over k and suppose

$$0 \longrightarrow Y_1 \longrightarrow Y_2 \longrightarrow Y_3 \longrightarrow 0$$

is an exact sequence of commutative groups, with Y_3 finite. Let $\varepsilon : Y_1 \to A(k)$ be a homomorphism of Y_1 into the set of k-rational points of A. The goal is to construct a group B, together with a morphism of algebraic groups $A \to B$ and a homomorphism of Y_2 into $B(k)$ such that

(i) the diagram

$$\begin{tikzcd} Y_1 \arrow[r] \arrow[d] & A(k) \arrow[d] \\ Y_2 \arrow[r] & B(k) \end{tikzcd}$$

is commutative.

(ii) B is universal with respect to A.

Such a group universal B can be constructed, details of which can be found in [2] Chapter II-1.3. Thus, for an extension k'/k, one obtain an exact sequence

$$0 \longrightarrow A(k') \longrightarrow B(k') \longrightarrow Y_3 \to 0$$

and a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & Y_1 \arrow[r] \arrow[d] & Y_2 \arrow[r] \arrow[d] & Y_3 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A(k') \arrow[r] & B(k') \arrow[r] & Y_3 \arrow[r] & 0
\end{tikzcd}$$

The algebraic group B is thus an *extension* of the algebraic group Y_3 by A.

One can now apply this construction to the exact sequence (1.1) (i.e., let $Y_1 = K^\times/\mathbb{I}_K(\mathfrak{m}) \cap K^\times, Y_2 = \mathbb{I}_k/\mathbb{I}_K(\mathfrak{m})$ and $Y_3 = C_\mathfrak{m}$). Note that $C_\mathfrak{m}$ is finite from Theorem 1.9. However, before that we must "cut down" the torus $T = R_{K/\mathbb{Q}}(\mathbb{G}_m)$ defined earlier in this section. Set $E_\mathfrak{m} = \mathbb{I}_K(\mathfrak{m}) \cap K^\times$, and let $\overline{E}_\mathfrak{m}$ be the Zariski closure of in T. Set the commutative group A to be $T_\mathfrak{m} = T/\overline{E}_\mathfrak{m}$. Then the construction described above yields an "enlarged" $\mathbb{Q}$-algebraic group $S_\mathfrak{m}$ with an algebraic morphism $T_\mathfrak{m} \to S_\mathfrak{m}$ and a group homomorphism $\varepsilon : \mathbb{I}_K/\mathbb{I}_K(\mathfrak{m}) \to S_\mathfrak{m}(\mathbb{Q})$. The sequence

$$1 \longrightarrow T_\mathfrak{m} \longrightarrow S_\mathfrak{m} \longrightarrow C_\mathfrak{m} \longrightarrow 1 \tag{2.1}$$

is exact, and the diagram

$$\begin{tikzcd}
1 \arrow[r] & K^\times/\mathbb{I}_K(\mathfrak{m}) \cap K^\times \arrow[r] \arrow[d] & \mathbb{I}_K/\mathbb{I}_K(\mathfrak{m}) \arrow[r] \arrow[d, "\varepsilon"] & C_\mathfrak{m} \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & T_\mathfrak{m}(\mathbb{Q}) \arrow[r] & S_\mathfrak{m}(\mathbb{Q}) \arrow[r] & C_\mathfrak{m} \arrow[r] & 1
\end{tikzcd} \tag{2.2}$$

is commutative.

2.2 Abelian ℓ-adic representations

With $S_\mathfrak{m}$ constructed, the canonical ℓ-adic representation of K with values in $S_\mathfrak{m}$ can now be constructed. Let ℓ be a prime number and $\mathfrak{m}$ a modulus. Let $\pi : T \to T_\mathfrak{m} \to S_\mathfrak{m}$ be the algebraic morphisms from the previous section and also call $\varepsilon : \mathbb{I}_K \to \mathbb{I}_K/\mathbb{I}_K(\mathfrak{m}) \to S_\mathfrak{m}(\mathbb{Q})$. By taking points with values in $\mathbb{Q}_\ell$, π defines a homomorphism

$$\pi_\ell : T(\mathbb{Q}_\ell) \longrightarrow S_\mathfrak{m}(\mathbb{Q}_\ell).$$

As $K \otimes_\mathbb{Q} \mathbb{Q}_\ell = \prod_{\mathfrak{p}|\ell} K_\mathfrak{p}$, the group $T(\mathbb{Q}_\ell)$ can be identified with $K_\ell^\times = \prod_{\mathfrak{p}|\ell} K_\mathfrak{p}^\times$, and is therefore a direct factor of the idèle class group $\mathbb{I}$. Let pr_ℓ denote the projection of $\mathbb{I}_K$ onto this factor $T(\mathbb{Q}_\ell)$. Then, the map

$$\alpha_\ell = \pi_\ell \circ pr_\ell : \mathbb{I}_K \to T(\mathbb{Q}_\ell) \to S_m(\mathbb{Q}_\ell)$$

is a continuous homomorphism (since π_ℓ and pr_ℓ are).

Lemma 2.2. *α_ℓ and ε coincide on $K^\times$.*

Proof. This is clear from the commutative diagram 2.2. □

With the help of this Lemma, define $\varepsilon_\ell : \mathbb{I}_K \to S_\mathfrak{m}(\mathbb{Q}_\ell)$ by

$$\varepsilon_\ell(a) : \varepsilon(a)\alpha_\ell(a^{-1})) \tag{2.3}$$

i.e., $\varepsilon_\ell = \varepsilon.\alpha_\ell^{-1}$ (note, this is multiplication and not composition). From Lemma 2.2, this is identity on $K^\times$. Since the idèle class group is $C = \mathbb{I}_K/K^\times$, ε_ℓ defines a map from $C \to S_\mathfrak{m}(\mathbb{Q}_\ell)$. Let α_ℓ denote the ℓ^{th} component of the idèle a. Then as $S_\mathfrak{m}(\mathbb{Q}_\ell)$ is totally disconnected, it is trivial on the connected component D of C_K from §1.4. As C_K/D is isomorphic to $\mathrm{Gal}(K^{ab}/K)$, we end up with the homomorphism

$$\varepsilon_\ell : \mathrm{Gal}(K^{ab}/K) \longrightarrow S_\mathfrak{m}(\mathbb{Q}_\ell) \tag{2.4}$$

i.e, an ℓ-adic representation of K with values in $S_\mathfrak{m}$!

The following properties can be deduced about this system of representations:

Proposition 2.3. *(i) The representation $\varepsilon_\ell : \mathrm{Gal}(K^{ab}/K) \to S_{\mathfrak{m}}(\mathbb{Q}_\ell)$ is a rational representation.*

(ii) ε_ℓ is unramified outside $\{\mathfrak{p} \mid \mathfrak{m}\} \cup S_\ell$ where $S_\ell = \{\mathfrak{p} : \mathrm{char}\, k_{\mathfrak{p}} = \ell\}$.

(iii) If $\mathfrak{p} \notin \{\mathfrak{p} \mid \mathfrak{m}\} \cup S_\ell$, then the Frobenius element $\mathrm{Frob}_{v,\varepsilon_\ell}$ is equal to $\mathrm{Frob}_{\mathfrak{p}} \in S_{\mathfrak{m}}(\mathbb{Q}_\ell)$.

(iv) The representations ε_ℓ form a system of strictly compatible ℓ-adic representations with values in $S_{\mathfrak{m}}$.

Proof. See [2] Chapter II §2.3 Proposition.

□

While this construction is undeniably intriguing, it begs the question of how this abstract group its representations are related to anything that this essay hopes to proves. The subsequent section aims to shed some light on this matter.

Let W_0 be a finite dimensional vector space over $\mathbb{Q}$, and let $\varphi_0 : S_{\mathfrak{m}} \to \mathrm{GL}W_0$ be a linear representation of $S_{\mathfrak{m}}$. For each prime number ℓ, let $W_\ell = W_0 \otimes \mathbb{Q}_\ell$ and $S_{\mathfrak{m}/\mathbb{Q}_\ell} = S_{\mathfrak{m}} \times \mathbb{Q}_\ell$. We then obtain a linear representation $\varphi_{0/\ell} : S_{\mathfrak{m}/\mathbb{Q}_\ell} \to \mathrm{GL}W_\ell$, which defines a homomorphism $\varphi_{0/\ell} : S_{\mathfrak{m}}(\mathbb{Q}_\ell) \to \mathrm{Aut}\, W_\ell$. By composing the map $\varepsilon_\ell : \mathrm{Gal}(K^{ab}/K) \to S_{\mathfrak{m}}(\mathbb{Q}_\ell)$, we obtain

$$\varphi_\ell = \varphi_{0/\ell} \circ \varepsilon_\ell : \mathrm{Gal}(K^{ab}/K) \to \mathrm{Aut}\, W_\ell \tag{2.5}$$

an ℓ-adic representation of K in W_ℓ. φ_ℓ is *abelian* (i.e., $\varphi_\ell(\mathrm{Gal}(K^{ab}/K)$ is abelian) because $S_{\mathfrak{m}}$ is abelian by construction (see [2] Remark II-5). We can deduce the following about φ_ℓ:

Theorem 2.4. *(i) The φ_ℓ form a strictly compatible system of abelian semisimple ℓ-adic representations.*

(ii) For each $v \notin \mathrm{Supp}(\mathfrak{m})$, the Frobenius element of v with respect to the system (φ_ℓ) is the element $\varphi(\mathrm{Frob}_v)$ of $\mathrm{Aut}\, W_0$.

(iii) There exist infinitely many primes ℓ such that φ_ℓ is diagonalisable over $\mathbb{Q}_\ell$.

Proof. See [2] II-20 §2.5 Theorem 1. □

Recall the $\mathbb{Q}_\ell$-vector space denoted by V_ℓ as defined in Definition 1.3. Specifically, by setting $W_\ell = V_\ell$, we have constructed an abelian ℓ-adic representation $\varphi_\ell : \mathrm{Gal}(K^{ab}/K) \to \mathrm{Aut}(V_\ell)$. This brings us closer to our objective of investigating ℓ-adic representations of elliptic curves; however, there is an opportunity for further refinement. Let $\overline{\mathbb{Q}}$ (resp. $\overline{\mathbb{Q}_\ell}$) be the algebraic closure of $\mathbb{Q}$ (resp. $\mathbb{Q}_\ell$). We shall now present a criterion for determining when any given system of ℓ-adic representations (subject to certain assumptions) is isomorphic to the system (φ_ℓ) established previously. In order to do so, we first delve into character groups.

Let $X(T) = \mathrm{Hom}_{\overline{\mathbb{Q}}}(T_{/\overline{\mathbb{Q}}}, \mathbb{G}_{m/\overline{\mathbb{Q}}})$. If Γ is the set of embeddings of K into $\overline{\mathbb{Q}}$, then each $\sigma \in \Gamma$ extends to a homomorphism $K \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$ and defines a morphism $[\sigma] : T_{/\overline{\mathbb{Q}}} \to \mathbb{G}_{m/\overline{\mathbb{Q}}}$. The set of $[\sigma]$'s form the basis of the *character group* $X(T)$ of T. Every element $\phi \in X(T)$ can be uniquely expressed as

$$\phi = \prod_{\sigma \in \Gamma} [\sigma]^{n(\sigma)}, \qquad \text{with } n(\sigma) \in \mathbb{Z},$$

and we call $n(\sigma)$ the *exponents* of ϕ. As $T_{\mathfrak{m}} = T/\overline{E}_{\mathfrak{m}}$, the group $X(T_{\mathfrak{m}})$ can actually be identified as a subgroup of $X(T)$ formed by characters of the above type such that

$$\phi(x) = \prod_{\sigma \in \Gamma} \sigma(x)^{n(\sigma)} = 1, \qquad \text{for all } x \in E_{\mathfrak{m}}.$$

But, we are interested in characters of $S_{\mathfrak{m}}$. So, taking the dual of (2.1), we obtain a dual exact sequence

$$0 \longrightarrow \mathrm{Hom}(C_{\mathfrak{m}}, \overline{\mathbb{Q}}^{\times}) \longrightarrow X(S_{\mathfrak{m}}) \longrightarrow X(T_{\mathfrak{m}}) \longrightarrow 0,$$

and so every character ϕ of $T_{\mathfrak{m}}$ can be extended to a character of $S_{\mathfrak{m}}$ in precisely $h_{\mathfrak{m}} = \#C_{\mathfrak{m}}$ ways.

With characters of $X(S_{\mathfrak{m}})$ in place, we would now like to express representations of $\mathrm{Gal}(K^{ab}/K)$ via characters of $S_{\mathfrak{m}}$.

Using (2.1) along with the fact that $X(S_{\mathfrak{m}}) = \mathrm{Hom}(S_{\mathfrak{m}/\overline{\mathbb{Q}}}, \overline{\mathbb{Q}}^{\times})$ and $S_{\mathfrak{m}} = T/\overline{E}_{\mathfrak{m}}$, we can write an element of $X(S_{\mathfrak{m}})$ as a pair (ψ, f), where $\psi \in X(T)$ and $f \in \mathrm{Hom}(\mathbb{I}_K, \overline{\mathbb{Q}}^{\times})$. For $\phi = \prod_{\sigma\in\Gamma}[\sigma]^{n(\sigma)}$ an element of $X(T)$, let ϕ_ℓ denote the the homomorphism of $K_\ell^{\times} = T_{/\mathbb{Q}_\ell}$ into $\overline{\mathbb{Q}}_\ell$ defined by

$$\phi_\ell(x) = \prod_{\sigma\in\Gamma} \sigma_\ell(x)^{n(\sigma)}$$

where $\sigma_\ell : K_\ell \to \overline{\mathbb{Q}}_\ell$ is a linear extension of $\sigma : K \to \mathbb{Q}$.

Then, an ℓ-adic character of $\mathrm{Gal}(K^{ab}/K)$ attached to character of $S_{\mathfrak{m}}$ can be given as follows:

Let $\psi = (\phi, f)$ be an element of $X(S_{\mathfrak{m}})$. If a is an idèle of K, put

$$\psi_\ell(a) = f(a)\phi_\ell(a_\ell^{-1}),$$

from which we obtain a homomorphism $\psi_\ell : \mathbb{I}_K \to \overline{\mathbb{Q}}_\ell^{\times}$. Using the same construction as for ε_ℓ, we can obtain a continuous homomorphism $\psi_\ell : \mathrm{Gal}(K^{ab}/K) \to \overline{\mathbb{Q}}_\ell^{\times}$!

Considering this modulo π_ℓ we obtain

$$\tilde{\psi}_\ell : \mathrm{Gal}(K^{ab}/K) \to k_\ell^{\times}; \qquad \tilde{\psi}_\ell(a) \equiv \prod_{\sigma\in\Gamma} \sigma_\ell(a_\ell^{-1})^{n(\sigma)} \mod \pi_\ell.$$

We now approach the final result of this section:

Theorem 2.5. *Let $\rho_\ell : G_K \to \mathrm{GL}W_\ell$, where W_ℓ is a $\mathbb{Q}_\ell$ vector space. Suppose (ρ_ℓ) is a semisimple, rational, strictly compatible system of ℓ-adic representations. Let P denote the set of primes. Then, if there is an integer N and an infinite subset L of P satisfying the property that for all $\ell \in L$, the reduction ρ_ℓ^{ss} of ρ_ℓ modulo ℓ is abelian, and, for any associated character $\theta_\ell^{(i)} : \mathbb{I}_K \to k_\ell^{\times}$ there are integers $n(\sigma,\ell,i)_{\sigma\in\Gamma}$ less than N in absolute value such that*

$$\theta_\ell^{(i)}(a) \equiv \prod_{\sigma\in\Gamma} \sigma_\ell(a^{-1})^{n(\sigma,\ell,i)} \mod \pi_\ell \qquad \textit{for all } a \in \mathbb{I}_K(\mathfrak{m}),$$

then, the system (ρ_ℓ) is isomorphic to the system (φ_ℓ) associated to a representation $\varphi_o : S_{\mathfrak{m}} \to \mathrm{GL}W_0$.

Proof. See [1] Theorem 1. □

Note, that the hypothesis does not require ρ_ℓ to abelian – however, the conclusion of the theorem states that (ρ_ℓ) must be isomorphic to (φ_ℓ) if such an N exists, implying that (ρ_ℓ) must be abelian!

2.3 Subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$

In this section, let V be a 2-dimensional vector space over $\mathbb{F}_p$. As V is 2-dimensional, it can be written as the direct sum of two distinct lines $V = D_1 \oplus D_2$. The definitions can be found in [9] or [1] §2.

Definition 2.2. Any subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ which up to conjugation is of the form

$$\left\{\begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} : a, c \in \mathbb{F}_p, ac \neq 0\right\}$$

is called a *split Cartan* subgroup. The subgroup is abelian of type $(p-1, p-1)$. Equivalently, if C is a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ consisting of elements s such that $sD_1 = D_1$ and $sD_2 = D_2$, then it is a split Cartan subgroup defined by $\{D_1, D_2\}$.

Definition 2.3. Let C_1 be a subgroup of matrices that acts trivially on D_1. This is a cyclic subgroup of order $p-1$, with matrix representation $\begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix}$. Such a subgroup is called a *semi-split Cartan.*

Definition 2.4. . Let $\varepsilon \in \mathbb{F}_p^\times$ be a non-square element. Then any subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ which up to conjugation is of the form

$$\left\{ \begin{pmatrix} a & \varepsilon b \\ b & a \end{pmatrix} : a, b \in \mathbb{F}_p, a^2 - \varepsilon b^2 \neq 0 \right\}$$

is a *nonsplit Cartan* subgroup. Every nonsplit Cartan subgroup is isomorphic to $F_{p^2}^\times$.

Definition 2.5. Any subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ which up to conjugation is of the form

$$\left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{F}_p, ac \neq 0 \right\}$$

is called a *Borel* subgroup. Equivalently, it is the subgroup of $\mathrm{GL}(V)$ consisting of all elements s such that $sD = D$. It has order $p(p-1)^2$, and D is the unique line stabilised by the Borel subgroup.

Remark 2. For a number field K with absolute Galois group G_K and an ℓ-adic representation ρ, if $\rho(G_K)$ is contained in a split Cartan subgroup, then it is a subgroup of matrices of the form $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ and so it is already semi-simple and abelian. If $\rho(G_K)$ is contained in a nonsplit Cartan subgroup, then the elements of a nonsplit Cartan are diagonalisable over $\mathbb{F}_{p^2}$ and not $\mathbb{F}_p$, so the representation ρ is still semisimple and abelian. If $\rho(G_K)$ is contained in a Borel subgroup, then let D be the line left fixed by the Borel subgroup. Then,

$$G \to V/D \oplus D \cong \mathbb{F}_p \oplus \mathbb{F}_p$$

is the semisimplification and is abelian.

With the help of the following theorem, Serre classifies all the subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ (for the specifics of $p = 2, 3, 5$, see [1] §2).

Theorem 2.6. *Let p be a positive prime and let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$.*

(i) If $p \mid \#G$, then one of the following holds

(a) G contains $\mathrm{SL}_2(\mathbb{F}_p)$.

(b) G is contained in a Borel subgroup of $\mathrm{GL}(\mathbb{F}_p)$.

(ii) If $p \nmid \#G$, then

(a) G is contained in a Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$.

(b) G is properly contained in the normaliser of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$.

(c) The image of G in $\mathrm{PGL}_2(\mathbb{F}_p) := \mathrm{GL}_2(\mathbb{F}_p)/\mathbb{F}_p^\times$ is isomorphic to one of the exceptional groups A_4, A_5 or S_4.

Proof. (i) By Jordan Normal form, every element of order p of $GL_2(\mathbb{F}_p)$ can be expressed as $\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$ and hence pointwise fixes a unique line D_x corresponding to each x. If all the lines D_x corresponding to every p order element are the same line, say D, then G stabilises D and is contained in a Borel subgroup. If there are at least 2 different lines D_x and D_y, then pick a basis such that the basis vectors lie on these lines. Then G contains elements

$$x = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}, \qquad u = \begin{bmatrix} 1 & 0 \\ b & 1 \end{bmatrix}.$$

But, $SL_2(\mathbb{F}_p)$ is generated by these elements, and so the first part of the proposition follows. In particular, if G contains a Cartan subgroup and we are in the latter case, then $\det G \in \mathbb{F}_p^\times$, implying $G = \mathrm{GL}_2(\mathbb{F}_p)$.

(ii) To prove this, we first make the following claim:

Lemma 2.7. *Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ of order prime to p, and let $H = \phi(G)$ be its image in $\mathrm{PGL}_2(\mathbb{F}_p)$ under $\phi : \mathrm{GL}_2(\mathbb{F}_p) \to \mathrm{PGL}_2(\mathbb{F}_p)$. Then*

(a) if H is cyclic, then G contained in a Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$.

(b) if H is dihedral, then G is contained in the normaliser of a Cartan subgroup.

(c) H is isomorphic to A_4, S_4 or A_5.

Proof. If H is cyclic, then let $H = \langle h \rangle$. Let $A, B \in G$ be such that $\phi(A) = h = \phi(B)$. Then $A \sim B$ and as every non-scalar lies in a unique Cartan and the intersection of any two Cartans are the non-scalars, A and B must be in the same Cartan subgroup. If $H = \langle x, y : x^n = y^2 = 1, yxy^{-1} = x^{-1} \rangle$ is dihedral, then $\phi^{-1}(H)$ is the normaliser of $\phi^{-1}(\langle x \rangle)$ in $\phi^{-1}(H)$. Then using the first part $\phi^{-1}(\langle x \rangle)$ is contained in a Cartan, which implies that G lies in the normaliser of a Cartan. Lastly, if H is a finite subgroup of $\mathrm{PGL}_2(\mathbb{F}_p)$ of order prime to p and H is neither cyclic or dihedral, then H is isomorphic to A_4, S_4 or A_5 (see [1] Proposition 16).

□

So, from the above lemma, it is now clear that if G contains a Cartan subgroup C, it is sufficient to show that H is cyclic or or dihedral, i.e., it is not isomorphic to A_4,A_5 or S_4. This is obvious if $p \leq 3$. Suppose $p \geq 5$. Then the image of C in $\mathrm{PGL}_2(\mathbb{F}_p)$ is cyclic of order $p+1 \geq 6$ (because $p \geq 7$ if C is split). But none of A_4, A_5 or S_4 contain any elements of order at least 6.

□

2.4 On Tame Inertia groups and characters

The purpose of this section is to give results of a local nature, mainly concerning the tame inertia group and its action on torsion points of elliptic curves. This action can be given by *fundamental characters* with exponents bounded by the ramification index of the local fields considered; the existence of this bound will play a key role in the proof that follows.

Let $\overline{\mathbb{Q}}_p$ be the separable closure of $\mathbb{Q}_p$ (which is the same as the algebraic closure). There is a unique maximal unramified extension denoted as $\mathbb{Q}_p^{nr}$. Let $\mathbb{Q}_p^t/\mathbb{Q}_p^{nr}$ denote the maximal tamely ramified extension of $\mathbb{Q}_p$. Then, there is the following sequence of containment:

$$\overline{\mathbb{Q}}_p \supset \mathbb{Q}_p^t \supset \mathbb{Q}_p^{nr} \supset \mathbb{Q}_p.$$

Set

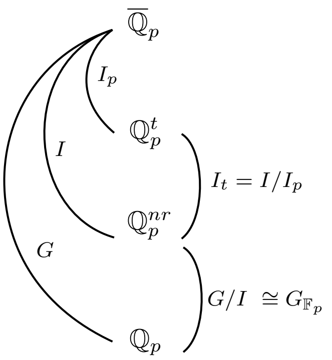
$$G = \mathrm{Aut}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p), \quad I = \mathrm{Aut}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^{nr}), \quad I_p = \mathrm{Aut}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^t), \quad I_t = I/I_p = \mathrm{Aut}(\mathbb{Q}_p^t/\mathbb{Q}_p^{nr})$$

Then, $G \supset I \supset I_p$. The group I is called the *inertia group* and the group I_p is called the *wild inertia group*. The group $G/I = \mathrm{Aut}(\mathbb{Q}_p^{nr}/\mathbb{Q}_p)$ is identified with $G_{\mathbb{F}_p} = \mathrm{Aut}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. The quotient $I_t = I/I_p$ is called the *tame inertia group* of G.

Remark 3. I_p is the largest prop-p group contained in I: it is a Sylow-p subgroup because each finite Galois extension of $\mathbb{Q}^t$ has degree a power of p, and the order of I_t is prime to p; it is unique because it is the kernel of $\mathrm{Gal}(\mathbb{Q}_p/\mathbb{Q}_p) \to \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^t)$, hence normal.

Remark 4. All the claims made in this section are easily generalisable to any number field K, with the replacement of $\overline{\mathbb{Q}}_p$ by K^{sep}, the separable closure of K.

The setting looks something like this:



For more details on these extensions and groups, see [10]. From now, let $q = p^m$ for some prime p and positive integer m.

Lemma 2.8. *There is an isomorphism*

$$\theta : I_t \to \varprojlim_q \mathbb{F}_q^\times$$

where $\mathbb{F}_q$ ranges over the finite subfields of $\overline{\mathbb{Q}}_p$ and where the transition maps are given by the norm map

$$N : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q^\times, \quad N(\alpha) = \alpha^{1+q+\dots q^{m-1}}.$$

Proof. Let x be a uniformiser of $\mathbb{Q}_p^{nr}$. The field $\mathbb{Q}_p^t$ is the union of all totally and tamely ramified extensions of $\mathbb{Q}_p^{nr}$ and since all such extensions are of the form $\mathbb{Q}_p^{nr}(\sqrt[d]{x})$ for all integers $\gcd(d, m) = 1$, we deduce

$$\mathbb{Q}_p^t = \varprojlim_{p \nmid d} \mathbb{Q}_p(\sqrt[d]{x}). \tag{2.6}$$

Similarly, since the unramified extensions of $\mathbb{Q}_p$ are the extensions $\mathbb{Q}_p(\zeta_m)$ for integers $p \nmid m$, we deduce

$$\mathbb{Q}_p^{nr} = \varprojlim_{p \nmid m} \mathbb{Q}_p(\zeta_m) \tag{2.7}$$

Kummer theory gives a canonical isomorphism

$$\mathrm{Gal}(\mathbb{Q}_p^{nr}(\sqrt[d]{x})/\mathbb{Q}_p^{nr}) \to \mu_d, \quad \sigma \mapsto \sigma(\sqrt[d]{x})/\sqrt[d]{x} \tag{2.8}$$

where μ_d is the group of d^{th} roots of unity, each of which are contained in $\mathbb{Q}_p^{nr}$ by (2.7). Each such isomorphism lifts to a map $\theta_d : I_p \to \mu_d$ which factors through I_t due to (2.6). Thus, we obtain an identification

$$I_t = \mathrm{Gal}(\mathbb{Q}_p^t/\mathbb{Q}_p^{nr}) = \varprojlim_{p \nmid d} \mathrm{Gal}(\mathbb{Q}_p^{nr}(\sqrt[d]{x})/\mathbb{Q}_p^{nr}) = \varprojlim_{p \nmid d} \mu_d. \tag{2.9}$$

As $\mathbb{F}_q^\times = \mu_{q-1}$, the inverse system (μ_d) is equivalent to the inverse system formed by $\mathbb{F}_q^\times$ and the norm maps $N : \mathbb{F}_{q^m} \to \mathbb{F}_q^\times, N(\alpha) = \alpha^{1+q+\dots q^{m-1}}$, and so the result follows.

□

Proposition 2.9. *Let V^{ss} denote the semi-simplification of V as a G-module (i.e., the direct sum of the Jordan-Hölder constituents of V). Then I_p acts trivially on V^{ss}.*

Proof. As we only need to prove that I_p acts trivially on the direct summands of V^{ss}, we may reduce to the case that $V = V^{ss}$ is simple. The continuity of ρ ensures that ρ kills an open (hence finite index) subgroup of G, so that ρ factors through a finite discrete quotient. As I_p is a pro p-group, the image $\rho(I_p)$ is a finite p-group. Let $W = V^{I_p}$ be the subspace on which I_p acts trivially. Since W is a p-torsion abelian group on which a finite p-group acts, we claim that $W \neq 0$. Indeed, as I_p is a pro-p group, its orbits have size 1 or powers of p. The orbit $\{0\}$ has size 1, and $|V|$ is a power of p. Since the orbits partition V, there must be at least $p-1$ other singleton orbits, in other words, there are at least $p-1$ non-trivial points that are fixed by I_p. So W is non-trivial. But, I_p is a normal subgroup of G, so W is a nontrivial G-stable subspace of V. However, since V is simple by hypothesis, $W = V$ and I_p acts trivially on V. □

By Proposition 2.9, $I_t = I/I_p$ acts on V^{ss}. The identification (2.9) shows that I_t is abelian, and so I_t acts on V^{ss} via two characters

$$\psi_1, \psi_2 : I_t \to \overline{\mathbb{F}}_p^\times$$

We are thus motivated to understand the group $\mathrm{Hom}\left(I_t, \overline{\mathbb{F}}_p^\times\right)$.

Definition 2.6. Let $\phi : I_t \to \overline{\mathbb{F}}_p^\times$ be a continuous character. ϕ is of *level* m if m is the smallest integer such that ϕ factors through $\mathbb{F}_{p^m}$.

$$\begin{tikzcd}
I_t \cong \varprojlim_d \mathbb{F}_{p^d}^\times \arrow[rr, "\phi"] \arrow[dr] & & \overline{\mathbb{F}}_p \\
& \mathbb{F}_{p^m}^\times \arrow[ur] &
\end{tikzcd}$$

The continuity of ϕ ensures that such an m exists, and the level of ϕ is a factor of any other such m. There is a convenient set of generators for the group of characters of I_t of level m that we now describe.

Definition 2.7. Let $q = p^m$. A *fundamental character* of I_t of level m with values in $\mathbb{F}_q^\times$ is a character that is the composition of

$$\theta_{q-1} : I_t \to \mu_{q-1}\left(\mathbb{Q}_p^{\mathrm{nr}}\right) \cong \mathbb{F}_q^\times$$

with a field isomorphism of $\mathbb{F}_q$. Here, θ_{q-1} is the map defined by (2.8). Clearly there are m fundamental characters of level m as such a character is conjugate over $\mathbb{F}_p$ to θ_{q-1} and can be written as

$$\xi = \theta_{q-1}^{p^i}, \quad i = 0, 1, \ldots, m.$$

Remark 5. It is fairly straightforward to see that $\mathrm{Hom}(I_t, \overline{\mathbb{F}}_p^\times)$ can be parametrised by the set of characters $\theta_d : I_t \to \mu_d$. For more details, see [1] §1.7 Proposition 6.

Lemma 2.10. *The fundamental characters of level n generate the set of all characters of level n.*

Proof. See [1] Proposition 5. □

In particular, we now consider the cyclotomic character $\chi : G \to \mathrm{Aut}\,(\mu_p) \cong \mathbb{F}_p^\times$ – the character giving the action of G on the p^{th} roots of unity. As $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ is tamely ramified, χ gives a character of I_t. We claim:

Proposition 2.11. *The character $\chi : I_t \to \mu_p$ is the e^{th} power of $\theta_{p-1} : I_t \to \mu_p$ (recall, e is the ramification index of p).*

Proof. Let $\Phi_p(X)$ be the cyclotomic polynomial and ζ_p a p^{th} root of unity. Then, $v_{\mathfrak{p}}(p) = v_{\mathfrak{p}}(\Phi_p(1)) = \sum_{n=1}^{p-1} v_{\mathfrak{p}}(\zeta_p^n - 1) = (p-1)(\zeta_p - 1)$. So, for $x \in \mu_p \setminus \{1\}$, $v_{\mathfrak{p}}(x-1) = e/(p-1) = \alpha$. This implies that the map $x \mapsto x - 1$ induces an injective homomorphism into V_α, and since all characters of I_t can be parametrised by θ_d's (see Remark 5 or [1] §1.8 Proposition 7), it must follow that $\chi = \theta_{p-1}^e$. □

Corollary 1. *If $e = 1$, then $\chi = \theta_{p-1}$.*

We may now readily apply the properties from above to the particular scenario where V is the set of p-torsion points of an elliptic curve. Let E be an elliptic curve over a complete, normalised discretely valued field K of characteristic 0. Let the residue field be k with maximal ideal π and $\mathrm{char}\, k = p$. Let $E[p]$ denote its kernel under the multiplication by p map in $E(K^{sep})$ - this is a vector space of dimension 2 over $\mathbb{F}_p$. One also knows due to the Weil pairing that $\wedge^2 E[p] \cong \mu_p$. Let $\rho : G \to \mathrm{Aut}(E[p]) = \mathrm{GL}_2(\mathbb{F}_p)$ be a representation. Let $\tilde{E}[p]$ denote the reduction modulo π of $E[p]$ in k. From Definition 1.6, we split into three cases.

Case I: Ordinary Good Reduction

If E has good reduction, there are two possibilities – ordinary reduction and supersingular reduction. First, assume E has ordinary reduction. Then, there is an exact sequence

$$0 \longrightarrow X[p] \longrightarrow E[p] \longrightarrow \tilde{E}[p] \longrightarrow 0 \tag{2.10}$$

where $E[p] \longrightarrow \tilde{E}[p]$ is the reduction map and $X[p]$ is the kernel of this map, which is cyclic of order p as E has good ordinary reduction.

Let $\langle e_1, e_2\rangle = E[p]$ be choice of basis such that $X[p] = \langle e_1\rangle_{\mathbb{F}_p}$. As $X[p]$ is stable under the action of G, the image $\rho(G)$ is contained in a subgroup conjugate to $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$, which implies that the image is contained in a Borel subgroup.

Further, $\rho(I_p)$ is a finite quotient of a pro-p group, it must be of p-power order. As the Sylow p-subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ consists of upper triangular matrices which is generated by $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$, $\rho(I_p)$ must lie in the unipotent group $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$.

The group I_t acts on $X[p]$ (resp. $\tilde{E}[p] = E[p]/X[p]$) by means of a character χ_X (resp. χ_Y) with values in $\mathbb{F}_p^\times$. From this we obtain the first piece of information about the Galois module $E[p]$:

Proposition 2.12.

$$\chi_X = \theta_{p-1}^e, \qquad \textit{and} \qquad \chi_Y = 1.$$

Proof. $\chi_Y = 1$ as G acts on $\tilde{E}[p]$ via the canonical homomorphism $G = \mathrm{Gal}(K^{sep}/K) \to \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. The product $\chi_X\chi_Y$ is the determinant of the action of I_t on $E[p]$ and by Proposition 2.11 is θ_{p-1}^e. □

An immediate corollary to this if $e = 1$ is as follows.

Corollary 2 (Good ordinary reduction)**.** *Suppose $e = 1$. Then,*

(a) The two characters giving the action of I_t on the semisimplification of $E[p]$ are the trivial character and the fundamental character θ_{p-1}.

(b) If I_p acts trivially on $E[p]$, the image of I in $\mathrm{GL}_2(\mathbb{F}_p)$ is a cyclic group of order $p-1$, representable by $\begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix}$ with a choice of basis $\langle e_1, e_2\rangle$ such that $X[p] = \langle e_1\rangle$.

(c) If I_p does not act trivially on $E[p]$, then the image of I in $\mathrm{GL}_2(\mathbb{F}_p)$ has order $p(p-1)$, and is given by $\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$.

Proof. The first claim is clear from 2.12 as $E[p]/X[p] = \tilde{E}[p]$. For the second, notice that as the χ_X must be surjective, the image of I must have order divisible by $p-1$. Since this image must be a subgroup of $\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$, its order is either $p(p-1)$ or $p-1$, which corresponds to either of the two cases. □

Case II: Supersingular Reduction

Now, we consider the second case, that is if E has supersingular reduction. In this case, $\tilde{E}$ has no points of order p and every element of $E[p]$ reduces to the identity element of $\tilde{E}$.

Proposition 2.13 (Good supersingular reduction)**.** *Suppose $e = 1$.*

(a) The action of I_p on $E[p]$ is trivial.

(b) There exists on $E[p]$ the structure of a one-dimensional $\mathbb{F}_{p^2}$-vector space such that the action of I_t is given by the fundamental character θ_{p^2-1} of level 2.

(c) *The image of I in $\mathrm{GL}_2(\mathbb{F}_p)$ is a cyclic group of order p^2-1 (non-split Cartan subgroup)*

(d) *The image of G in $\mathrm{GL}_2(\mathbb{F}_p)$ is contained in a Cartan subgroup or in its normaliser N.*

Proof. The proof of the first, third and fourth parts are in the same vein to Corollary 2. The second uses some elementary theory from formal groups, but is essentially just a straightforward generalisation of Proposition 2.11. For more details, see [1] Proposition 13. □

Case III: Multiplicative Bad Reduction

In this case, assume E has multiplicative bad reduction. To study the Galois representation $E[p]$, it is easiest to study the theory of Tate curves. For a quick overview on Tate curves, see [4] Appendix C.14, and for more detailed treatment, see [5] Chapter V. §3.

In summary, from the theory of Tate curves, there is a unique $q \in K^\times$ with $|q|_v < 1$ such that there is a curve $E(q) = \mathbb{G}_m/q^{\mathbb{Z}}$ which is isomorphic to E over K or isomorphic to E over a quadratic extension L/K (See [4] Appendix C.14 Theorem 14.1). Over this extension, the p-torsion $E[p]$ contains μ_p as a Galois sub-module, with the quotient $E[p]/\mu_p$ being generated by the image of $q^{1/p}$. As any Galois conjugate of $q^{1/p}$ is equal to $\zeta q^{1/p}$ for some $\zeta \in \mu_p$, the Galois action on $q^{1/p}$ modulo μ_p is trivial. This gives an exact sequence

$$0 \to \mu_p \to E[p] \to \mathbb{Z}/p\mathbb{Z} \to 0.$$

Then, similar to the previous cases, we can identify μ_p to be the kernel of reduction. The action of I_p on the kernel of reduction is given by the upper left corner of the matrices $\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$. So we conclude:

Proposition 2.14 (Multiplicative Bad Reduction)**.** *The image of th inertia group I in $\mathrm{GL}_2(\mathbb{F}_p)$ is contained in a subgroup of the type $\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$. The two characters of I_t associated to this epresentation are the unit character and the character θ_{p-1}^e.*

Corollary 3. *Suppose $e = 1$. Then*

(a) *The two characters giving the action of I_t on the semisimplification of $E[p]$ are the trivial character 1 and the character θ_{p-1}.*

(b) *If I_p acts trivially on $E[p]$, the image of I in $\mathrm{GL}_2(\mathbb{F}_p)$, is cyclic of order $p-1$. and has matrix representation $\begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix}$.*

(c) *If I_p does not act trivially on $E[p]$, the image of I has matrix representation $\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$.*

With this, one has all the background required to proceed with Serre's proof. One might ask why we have paid particular attention to the $e = 1$ case, and so far not considered the case of additive reduction. The reason for this is that if E is an elliptic curve over F, then the semistable reduction theorem (c.f. Theorem 1.2 (iii)) can be used to work over a quadratic extension of K/F such that E has only multiplicative bad reduction or good reduction. Further, as only finitely many primes of F ramify in K, one can remove that finite subset of primes and assume that every element of K is at least 7 and unramified in F.

3. Serre's Proof

The goal of this chapter is to provide a sketch of Serre's proof using all the theory covered in the prior chapters. We then provide some explicit examples of how to compute the ℓ-adic images of these Galois representations in certain situations. Lastly, we consider the specific case of $K = \mathbb{Q}$ and define Serre curves.

3.1 Proof (briefly)

In this section, we tie everything covered thus far, to prove the main theorem from Serre's paper [1]. Before we delve into the proof, we first state the two main claims from Serre's antecedent work [2].

Let ℓ be a prime and n an integer. Let E be an elliptic curve over a number field K. Let $E[\ell^\infty] = \varprojlim_n E[\ell^n]$. Then,

$$E[\text{tors}] = \bigoplus_{\ell \in \mathcal{P}} E[\ell^\infty]$$

and

$$\operatorname{Aut} E[\text{tors}] = \prod_{\ell \in \mathcal{P}} \operatorname{Aut} E[\ell^\infty] \cong \prod_{\ell \in \mathcal{P}} \mathrm{GL}_2(\mathbb{Z}_\ell).$$

For $G = \mathrm{Gal}(\overline{K}/K)$, define

$$\begin{aligned}
\rho_n &: G \longrightarrow \operatorname{Aut} E[n] \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \\
\rho_\ell &: G \longrightarrow \operatorname{Aut} E[\ell] \cong \mathrm{GL}_2(\mathbb{F}_\ell) \\
\rho_{\ell^\infty} &: G \longrightarrow \operatorname{Aut} E[\ell^\infty] \cong \mathrm{GL}_2(\mathbb{Z}_\ell) \\
\rho_\infty &: G \longrightarrow \operatorname{Aut} E[\text{tors}] \cong \mathrm{GL}_2(\hat{\mathbb{Z}})
\end{aligned}$$

Proposition 3.1 ([2] IV-19 §3.1 Proposition)**.** *The following are equivalent:*

1. *$\rho_\infty(G)$ is open in $\prod_\ell T_\ell \cong \mathrm{GL}_2(\hat{\mathbb{Z}})$.*
2. *$\rho_{\ell^\infty}(G) = \operatorname{Aut} T_\ell$ for almost all ℓ.*
3. *$\rho_\ell(G) = \operatorname{Aut} E[\ell]$ for almost all ℓ.*
4. *$\rho_\ell(G)$ contains $\mathrm{SL}E[\ell]$ for almost all ℓ.*

Theorem 3.2 ([2] IV-11 §2.2 Theorem)**.** *If E has no complex multiplication over $\overline{K}$, then $\rho_\ell(G)$ is open in $\operatorname{Aut} T_\ell$.*

Theorem 3.1 uses the fact that for an elliptic curve with no CM, if $\rho_\ell(G)$ were abelian, semisimple and rational, we would be able to find a prime ℓ' such that a compatible ℓ'-adic representation $V_{\ell'}$ would be the direct sum of one-dimensional subspaces stable under G_K, contradicting the fact that V_ℓ is irreducible for all primes ℓ if E has no CM (see Theorem 1.6 and Remark).

Recall that $T_\ell = \varprojlim_n E[\ell^n]$. So, in order to show that $\rho_\infty(G)$ is open in $\mathrm{GL}_2(\hat{\mathbb{Z}})$, it is sufficient to show $\rho_\ell : G \to \mathrm{GL}_2(\mathbb{F}_\ell)$ is surjective for almost all ℓ. Thus, in this section, we shall be proving the following theorem:

Theorem 3.3. *Let E be an elliptic curve over F. Suppose E has no complex multiplication over $\overline{F}$. Then, for almost every prime number ℓ, the homomorphism $\rho_\ell : \mathrm{Gal}(\overline{F}/F) \to \mathrm{Aut}\, E[\ell]$ is surjective.*

In the last 2 chapters, we have

- Constructed a rational, semisimple, abelian, strictly compatible system (φ_ℓ) of ℓ-adic representations.
- Given a criteria of when any other semisimple, rational, strictly compatible ℓ-adic system must be isomorphic to (φ_ℓ), and in particular, abelian (Theorem 2.5).
- Given a characterisation of the inertia group on the p-torsion $E[p]$ of an elliptic curve under different types of reduction.
- Identified the possible subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$.

As most of the groundwork is done, the proof proceeds by first assuming E has no CM. Then, comparing the action of the inertia group with the subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$, we zone down on two possibilities for where $\rho_\ell(G)$ must lie. We eliminate one possibility by arriving at a contradiction using Chebotarev Density Theorem. For the second case, we show that the semisimplification $\rho_\ell^{ss} : G \to \mathrm{GL}_2(\mathbb{F}_\ell)$ enjoys certain properties that enables us to show that ρ_ℓ is abelian, implying E must have CM, arriving at a contradiction.

Proof of Theorem 3.3. First, some reduction are in order. One can replace F with a finite extension K/F from Theorem 1.2 for which E attains semistable reduction. Next, we proceed by contradiction: suppose it were the case that there was infinite subset L of primes such that for every $\ell \in L$, $\rho_\ell(G) \neq \mathrm{GL}_2(\mathbb{F}_\ell)$ (we shall show that this hypothesis implies E has complex multiplication). By removing a finite subset of L, one can assume $\ell \in L$ to be such that ℓ are at least 7, unramified in $\mathbb{Q}$ and $\mathbb{E}[\ell]$ is irreducible (see Corollary 1.6). Then as $\ell \nmid \#G$, we are in case ii) of Theorem 2.6.

Let $\ell \in L$ and let v be a place of K lying over ℓ. Choose w to be a place of $\overline{K}$ that extends v. Let I_w be a corresponding inertia subgroup of G. Further, as E is semistable over K, E has either ordinary good reduction, supersingular good reduction or multiplicative bad reduction. Then, from Corollary 2 and Corollary 3, $\rho_\ell(I_w)$ is up to conjugacy of the form $\begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix}$, or $\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$. In particular, the size of the image of the wild inertia subgroup is $\ell - 1$ or $\ell(\ell-1)$, respectively.

If E has supersingular reduction, then from Proposition 2.13, then $\rho_\ell(I_w)$ is a non-split Cartan subgroup itself, or a normaliser of a non-split Cartan subgroup and has order $\ell^2 - 1$. So, combined together with Theorem 2.6 we are left with two possibilities

(a) $\rho_\ell(G)$ is contained in a Borel subgroup or a Cartan subgroup.

(b) ρ_ℓ is contained in the normaliser of a Cartan subgroup C_ℓ, and is not contained in C_ℓ.

We shall first show that (b) can occur for only finitely many values of ℓ (if E does not have complex multiplication).

Let N_ℓ denote the normaliser of the Cartan subgrpoup C_ℓ. As C_ℓ has index 2 in its normaliser and as case (b) implies the containment of groups $C_\ell \subseteq \rho_\ell(G) \subseteq N_\ell$, we have the following composition series

$$G \xrightarrow{\rho_\ell} N_\ell \longrightarrow N_\ell/C_\ell \xrightarrow{\sim} \{\pm 1\} \tag{3.1}$$

and, so this cuts out a quadratic extension, say $K_{\ell'}$ over K. Let (3.1) be denoted as a character of order 2, say $\epsilon_\ell : G \to \{\pm 1\}$.

Lemma 3.4. *The extension $K_{\ell'}/K$ is unramified.*

Proof. Let v be a place of K that extends to w. There are 3 cases to check:

(i) If v lies above ℓ, then $\rho_\ell(I_w)$ is a semi-split Cartan subgroup or a non-split Cartan subgroup. Since $\rho_\ell(I_w) \subset \rho_\ell(G)$, and $\rho_\ell(G)$ is contained in N_ℓ, by [1] Proposition 14, $\rho_\ell(I_w) \subseteq C_\ell$. In particular, $\epsilon_\ell(I_w) = 1$, so K' is unramified at v.

(ii) If v does not lie above ℓ and E has good reduction at v, then ρ_ℓ is unramified by Theorem 1.4 (Néron-Ogg-Shafarevich) and so $\epsilon_\ell(I_w) = 1$.

(iii) If v does not lie above ℓ and E has multiplicative reduction at v. Similar to Case III in §2.4, there exists an exact sequence

$$0 \longrightarrow \mu_\ell \longrightarrow E[\ell] \longleftarrow \mathbb{Z}/\ell\mathbb{Z} \longrightarrow 0.$$

which is compatible with the action on I_w. So $\rho_\ell(I_w)$ must be trivial or of order ℓ, and the latter is not possible $\rho_\ell(G)$ is contained in N_ℓ and $\ell \nmid \# N_\ell$. For more details, see [1] §4.2 Lemma 2.

□

Now suppose there is an infinite subset $L' \subset L$ for which $\rho_{\ell'}(G)$ is of type (b). By Hermite's Theorem (see [11] Chapter III Theorem 2.13), there are only finitely many quadratic extensions of K, so there is one such extension K' which is equal to $K_{\ell'}$ for infinitely many $\ell' \in L'$ by the pigeonhole principle. With the help of this extension, we shall show that E actually has complex multiplication, hence eliminating case (b). In lieu of this, note that whenever $v \in \Sigma_K$ is inert in K' and E has good reduction at v, $\tilde{E}_v$ must be supersingular. Indeed, if $\ell \neq \operatorname{char} k_v$, then $\rho(I_w) = \{1\}$ and ρ_ℓ is unramified at v. If δ_w denotes the Frobenius element associated to the extension w of v, then $\operatorname{Tr} F_v \equiv \operatorname{Tr} \delta_w \mod \ell$ and $\delta_w \in N_\ell$ (because we are in case (b) and $\rho(I_w) = \{1\}$). Moreover, suppose $\ell \in L'$ and $K_{\ell'} = K'$. As v is inert in K' and $\delta_w \in N_\ell$, $\epsilon_\ell(\delta_w) = -1$, i.e, $\delta_w \in N_\ell \backslash C_\ell$. However, elements of $N_\ell \backslash C_\ell$ have trace 0, so

$$\operatorname{Tr} F_v \equiv \operatorname{Tr} \delta_w \equiv 0 \mod \ell.$$

As this congruence holds for infinitely many ℓ, it must be the case that $\operatorname{Tr} F_v = 0$ which implies that $\tilde{E}_v$ is supersingular (as $\#\tilde{E}_v = Nv + 1 + \operatorname{Tr} F_v$).

Now, as we know that $v \in \Sigma_K$ inert implies that $\tilde{E}_v$ is supersingular, let Σ'_K be the set of such places. By Chebotarev Density Theorem (Theorem 1.8), the density of Σ'_K is 1/2. But, if E has no complex multiplication, then the places of supersingular reduction has density 0 (See [4] Chapter V Theorem 4.7) This is a contradiction, and so it must be the case that E has complex multiplication.

So now, we can focus on case (a).

Let $\rho_\ell : G \to \mathrm{GL}_2(\mathbb{F}_\ell)$ and let ρ_ℓ^{ss} denote the representation of G obtained from its semisimplification. As we are in (a), a Borel or Cartan subgroup is abelian and so ρ_ℓ^{ss} must be abelian, which implies that we can diagonalise it by extending scalars and obtain two characters $\theta_\ell^{(1)}$ and $\theta_\ell^{(2)}$ such that

$$\theta_\ell^{(i)} : \mathrm{Gal}(K^{ab}/K) \longrightarrow k_\ell^\times.$$

We can identify these with homomorphisms from $\mathbb{I}_K$ into $k_\ell^\times$, just as done for (2.4).

Lemma 3.5. *Let $\mathfrak{m}$ be a modulus of support $S = \varnothing$. Let Γ be the set of embeddings of K into $\overline{\mathbb{Q}}$. Then there is a family of integers $n(\sigma, \ell, i)$ for $i = 1, 2$, $\sigma \in \Gamma$ taking values 0 or 1 such that*

$$\theta_\ell^{(i)}(a) \equiv \prod_{\sigma \in \Gamma} \sigma_\ell(a_\ell^{-1})^{n(\sigma,\ell,i)} \mod \pi_\ell$$

for all $i = 1, 2$ and $a \in \mathbb{I}_K(\mathfrak{m})$.

Proof. The first task is to check for the hypotheses of Theorem 2.5. For that, we first show that ρ_ℓ^{ss} is unramified for each $v \in \Sigma_K$ not dividing ℓ. If E has good reduction, that is clear from Theorem 1.4. Otherwise, E has multiplicative reduction, in which case the arguments in Lemma 3.4 show that $\rho_\ell(I_w)$ corresponding to v is either trivial or of order ℓ, and the semisimplification of such a group must be trivial, so $\rho^{ss}(I_w)$ is trivial. But as $\theta_\ell^{(i)}$ were obtained from ρ^{ss}, $\theta_\ell^{(i)}$ must also be unramified outside places that divide ℓ.

Now in order to show the claim in Theorem 2.5, it is equivalent to find exponents $n(\sigma, \ell, i)$ equal to 0 or 1 such that

$$\theta_\ell^{(i)}(a) \equiv \prod_{\sigma \in \Gamma} \sigma_\ell(a^{-1})^{n(\sigma,\ell,i)} \qquad \forall a \in \mathbb{I}_K(\ell). \tag{3.2}$$

Let each embedding corresponding to v (i.e., $v_\ell \circ \sigma = v$) be denoted by $\Gamma(v)$, then each $\Gamma(v)$ partitions Γ for $v \mid \ell$, and so using the fact that $\mathbb{I}_K(\ell) = \prod_{v|\ell} \mathbb{I}_K(v)$, the formula (3.2) is equivalent to

$$\theta_\ell^{(i)}(a) \equiv \prod_{\sigma \in \Gamma(v)} \sigma_\ell(a^{-1})^{n(\sigma,\ell,i)} \qquad \forall a \in \mathbb{I}_K(v), \tag{3.3}$$

which makes everything now local on v. As v is unramified over $\mathbb{Q}$ we have $[K : \mathbb{Q}_\ell] = f_v$ where f_v is the residue degree of v and $\#\Gamma(v) = f_v$. Using this fact, local class field theory and results from §2.4, (3.3) is equivalent to saying that the reduction of $\theta_\ell^{(i)}$ to the inertia groups I_v at v is the product of the fundamental characters of level f_v with exponents 0 or 1. So, the following cases arise:

(i) If E has ordinary good reduction at v, by Corollary 2, the restrictions of $\theta_\ell^{(i)}$ are either trivial or the fundamental character of level 1. In the first case, take $n(\sigma, \ell, i) = 0$ and in the second case take it as 1.

(ii) If E has supersingular reduction at v, then by Proposition 2.13, we have we have 2 characters of level 2 that are obtained by composing the fundamental character $\theta_{\ell^2-1} : I_v \to \mathbb{F}_{\ell^2}^\times$ with the two embeddings of $\mathbb{F}_{\ell^2}^\times$ into k_v. So, $n(\sigma, \ell, i) = 1$ if the reduction mod char k_v of σ extends the embedding, and 0 otherwise.

(iii) If E has bad reduction of the multiplicative type, then the case is the same as in the case of ordinary good reduction by Corollary 3.

Further, as ρ_ℓ is rational, semisimple and form a strictly compatible system, (ρ_ℓ) satisfies the hypothesis of Theorem 2.5 by taking the integer $N = 1$. So, it is isomorphic to (φ_ℓ), implying that ρ_ℓ is abelian, which by the contrapositive of Theorem 3.2 implies E must have complex multiplication, yet again, arriving at a contradiction. □

□

3.2 Explicit examples

The easiest case is that of semistable elliptic curves. Serre shows an easy criteria to determine the ℓ-adic image for most semistable elliptic curves. Let S_E denote the set of primes p at which E has bad reduction.

Proposition 3.6. *Let $E/\mathbb{Q}$ be a semistable elliptic curve, and let ℓ be a prime number. Suppose*

(a) $\rho_\ell \neq \operatorname{Aut} E[\ell]$; and

(b) Either $\ell \neq 2, 3, 5$ or ℓ does not divide $v_p(j)$ for some $p \in S_E$.

Then,

(i) $\rho_\ell(G)$ is contained in a Borel subgroup of $\operatorname{Aut} E[\ell]$;

(ii) The G-module $E[\ell]$ has Jordan-Hölder sequence with quotients isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$ and μ_ℓ;

(iii) $t_p \equiv 1 + p \mod \ell$ for all $p \in P \backslash S_E$.

Proof. See [1] Proposition 21. □

Serre gives a lot of numerical examples in §5.5. Here are some more examples:

Example 2 (Semistable curve)**.**

$$E : y^2 + xy + y = x^3 + x^2$$

This elliptic curve has conductor N, j-inariant j and discriminant Δ as follows:

$$N = 15 = 3 \cdot 5, \qquad j = \frac{-1}{15}, \qquad \Delta = -15 = -1 \cdot 3 \cdot 5.$$

As $S_E = \{3, 5\}$, by calculating c_4, one can see that it has multiplicative reduction at both 3 and 5. As

$$-v_3(j) = v_3(\Delta) = -1, \qquad -v_5(j) = v_5(\Delta) = -1,$$

and as $\ell \nmid -1$ for any prime ℓ, for $p \neq 3, 5$, there should exist some p such that $A_p = 1 + p + t_p$ (we are trying to show the contrapositive of Proposition 3.6). For $p = 2$, $A_2 = 4$, and so for all $\ell \neq 2$, φ_ℓ must have maximal image. $\ell = 2$ is an exception as $(0, 0)$ is a point of order 4, and so its image must be representable by a matrix of the form $\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$.

Example 3 (Semistable curve)**.**

$$y^2 + xy + y = x^3 - 11x + 12$$

This elliptic curve has conductor N, j-invariant j and discriminant Δ as follows:

$$N = 14 = 2 \cdot 7, \qquad j = \frac{5^3 \cdot 101^3}{2 \cdot 7^2}, \qquad \Delta = 98 = 2 \cdot 7^2.$$

As $S_E = \{2, 7\}$, by calculating c_4, one can see that it has multiplicative reduction at both 2 and 7. Just as above, as

$$-v_2(j) = v_2(\Delta) = 1, \qquad -v_7(j) = v_7(\Delta) = 2,$$

no ℓ divides 1 or 2 for $\ell \geq 5$.

Now, as $A_3 = 6$, the ℓ-adic image is maximal for all $\ell \neq 2, 3$. As $(0, 3)$ is a point of order 6, the image for $\ell = 2, 3$ is representable by a matrix of the form $\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$.

Example 4 (Non-integral j)**.**

$$E : y^2 = x^3 + x^2 + 8x + 8$$

This elliptic curve has conductor N, j-invariant j and discriminant Δ as follows:

$$N = 96 = 2^5 \cdot 3, \qquad j = \frac{2^3 \cdot 24^3}{3^4}, \qquad \Delta = -41472 = -2^9 \cdot 3^4.$$

This curve is has bad reduction at primes $2, 3$. We wish to find $E[2]$. As $E : y^2 = f(x)$, setting $y = 0$, we obtain $x = -1, \pm 2\sqrt{-2}$. So $E[2] = \{O_E, (-1, 0), (2\sqrt{-2}, 0), (-2\sqrt{-2})\}$ and $\mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{-2})$, which has degree 2 over $\mathbb{Q}$. Thus, the mod-2 Galois representation is cyclic of order 2. Set $2\sqrt{-2}$ to be θ. Set basis $P = (-1, 0)$ and $Q = (\theta, 0)$. Then, $P + Q = (\overline{\theta}, 0)$. So any automorphism $\sigma \in G_\mathbb{Q}$ will acts on $E[2]$ via $P \mapsto P$ and

$$Q \mapsto \begin{cases} Q & \text{if } \sigma(\theta) = \theta \\ P + Q & \text{if } \sigma(\theta) = \overline{\theta} \end{cases}$$

So, the Galois representation with respect to the basis $\{P, Q\}$ is given by

$$\rho_{E,2}(G) = \left\{ I, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\},$$

which implies $\rho_{E,2}(G)$ is not surjective.

For other primes ℓ, we claim that $\rho_{E,\ell}(G)$ is surjective in $\mathrm{GL}_2(\mathbb{F}_\ell)$. Using [2] IV-20 §3.2 Lemma 1 and 2, we can deduce that $\rho_{E,\ell}(G) = \mathrm{GL}_2(\mathbb{F}_\ell)$ if and only if $E[\ell]$ is irreducible. As $E[\ell]$ is irreducible if and only if there exists a $\mathbb{Q}$-rational ℓ-isogeny from E to some other E', say $\phi : E \to E'$. Then, just as in the proof of Corollary 1.6, for another isogeny $\psi : E' \to E$, we must have $\deg(\psi \circ \phi) = \ell \deg(\psi)$ to be a square. E corresponds to curve 8 in Ogg's list [12], and as E has conductor 96, E' must be curves $7, 9$ or 10 in Ogg's list. But, Ogg has shown that for such a curve there is an isogeny of order degree $1, 2$ or 4. So, the map $E \to E' \to E$ would then be an endomorphism of degree $\ell, 2\ell$ or 4ℓ, and this is impossible for $\ell \neq 2$ since E has no complex multiplication so $\operatorname{End} E = \mathbb{Z}$.

Example 5 (Integral j-invariant)**.** As E is not semistable at p, a finite group Φ_p can be introduced that measures the failure of semistability at p. As j is integral, there is potentially good reduction of E over p. Then, the group Φ_p can be thought of as $\mathrm{Aut}(L/\mathbb{Q}_p^{nr})$, where L is the smallest extension over $\mathbb{Q}_p^{nr}$ such that E acquires semistable reduction. For more details on how to exactly calculate these groups, see [1] §5.6.

Consider the curve

$$E : y^2 = x^3 - 3x - 34;$$

$$N = 216 = 2^3 \cdot 3^3, \qquad j = -6 = 2 \cdot 3, \qquad \Delta = -497664 = -2^{11} \cdot 3^5.$$

Then, as $v_2(\Delta) = 11$, $v_3(\Delta) = 5$, and $\#\Phi_p v_p \equiv 0 \mod 12$, running through the possibilities of cardinalities of Φ_2 and Φ_3, we conclude $\#\Phi_2 = 24$ and $\#\Phi_3 = 12$. So, $\Phi_2 \cong \mathrm{SL}_2(\mathbb{F}_3)$. For $\ell \geq 3$, we claim that $\rho_\ell(G) = \operatorname{Aut} E[\ell]$. Theorem 1.4 implies that Φ_2 acts faithfully on $E[\ell]$ for all $\ell \geq 3$. So, if Φ_2 was contained in a Borel subgroup, then its derived subgroup would be contained in $B' = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ – which would imply Φ_2' is trivial or cyclic of order ℓ. But, $\mathrm{SL}_2(\mathbb{F}_3)'$ has cardinality 8, so this is not possible. If Φ_2 were contained in the normaliser of a Cartan, say N_ℓ of C_ℓ, then consider the sequence $\Phi_2 \to N_\ell \to N_\ell / C_\ell$. The kernel would be contained in C, which is abelian, implying $\mathrm{SL}_2(\mathbb{F}_3)$ has an abelian subgroup of index at most 2, which we know is not true. Now, from the inertia group I, Corollary 2 and Proposition 2.13 imply that $\rho_{E,\ell}(G)$ must contain a Cartan or semi-Cartan subgroup. Then, by Proposition 2.6 (more precisely, [1] Proposition 17) for $\ell \neq 5$, $\rho_{E,\ell}(G) = \operatorname{Aut} E[\ell]$. For $\ell = 2$, as Φ_3 has order 12 and its image in $\operatorname{Aut} E[2] = \Phi_3/\{\pm 1\}$, we have $\rho_{E,2}(G) = \operatorname{Aut} E[2]$. Lastly, for $\ell = 5$, by [1] Proposition 17 Remark, we take $s = \pi_{23}$. Then, as $\#\tilde{E}_{23} = 22$, we have $a_{23} = 2$ and so $\mathrm{Tr}(s)^2/\det(s) = 4/23 \equiv 3 \mod 5$, which implies $\rho_{E,5}(G) = \operatorname{Aut} E[5]$. Thus, we have $\rho_{E,\ell}(G) = \operatorname{Aut} E[\ell]$ for all ℓ.

3.3 When $K = \mathbb{Q}$

Based on the proof of the main theorem in Serre's paper and the examples given above, it is a natural question to ask if it is possible that if $\rho_n(G) = \operatorname{Aut} E[n]$ for all $n \geq 1$ (or equivalently

$$\rho_\infty : G \to \operatorname{Aut} E[\mathrm{tors}] \cong \mathrm{GL}_2(\hat{\mathbb{Z}})$$

where P is the set of all primes) implies that ρ_∞ is surjective. Unfortunately, the answer to the same is negative, as Serre answers in his own paper with the following counterexample.

Proposition 3.7. *For every elliptic curve E over $\mathbb{Q}$, the image of*

$$\rho_\infty : G \to \operatorname{Aut} E[tors]$$

is contained in an index 2 subgroup of $\operatorname{Aut} E[tors]$.

Proof. Let $\ell = 2$ and let the 2-torsion points be $\{e_1, e_2, e_3\}$. As $\operatorname{Aut} E[2] \cong \mathrm{GL}_2(\mathbb{F}_2)$, it can be identified with the symmetric group S_3 which permutes $\{e_1, e_2, e_3\}$. Then, one can define a character $\varepsilon : S_3 \to \{\pm 1\}$ that maps to the signature of an element in S_3. Composing with $\rho_2 : G \to \operatorname{Aut} E[2]$, one obtains the character $\chi_\Delta : G \to \{\pm 1\}$ that corresponds to an extension of the base field of degree at most 2, namely $\mathbb{Q}(\sqrt{\Delta})$. As every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension, one can find an integer m such that χ_Δ is the composition of the canonical homomorphism

$$G \to \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = (\mathbb{Z}/m\mathbb{Z})^\times$$

and a character

$$\alpha_\Delta : (\mathbb{Z}/m\mathbb{Z})^\times \to \{\pm\},$$

which we can rewrite as

$$\varepsilon(\rho_2(\sigma)) = \alpha_\Delta(\det(\rho_m(\sigma))) \qquad \text{for all } \sigma \in G.$$

Essentially, there is a commutative diagram

$$\begin{tikzcd}
G \arrow[r, "\rho_m"] \arrow[d, "\rho_2"'] & \mathrm{Aut}\, E[m] \arrow[r, "\det"] & (\mathbb{Z}/m\mathbb{Z})^\times \arrow[d, "\alpha_\Delta"] \\
\mathrm{Aut}\, E[2] \arrow[rr, "\varepsilon"] & & \{\pm 1\}
\end{tikzcd}$$

Let a_m denote the image of $a \in E[\text{tors}]$ in $\mathrm{Aut}\, E[m]$. Then, the image of ρ_∞ is contained in $H_\Delta \subset \mathrm{Aut}\, E[\text{tors}]$ formed by elements a such that

$$\varepsilon(a_2) = \alpha_\Delta(\det a_m)$$

i.e, it is the kernel of the map to $\{\pm 1\}$ given by $a \mapsto \varepsilon^{-1}(a_2)\alpha_\Delta(\det a_m)$, hence is a subgroup. H_Δ is either all of $\mathrm{Aut}(E[\text{tors}])$ or is an index 2 subgroup because the target has size 2. However, the map to ± 1 is surjective as can be seen form the commutative diagram above, so it is an index two subgroup. It is open as it is the composition of continuous homomorphisms into a discrete target. □

Definition 3.1. An elliptic curve for which $\rho_{E,\infty}(G)$ is as large as possible, i.e., $[\mathrm{GL}_2(\hat{\mathbb{Z}}) : \rho_{E,\infty}(G)] = 2$, is called a *Serre curve.*

So far, we have observed that Serre's result is qualitative, lacking precise information on how exactly to calculate the image of a given curve. Consequently, one might be interested in determining the prevalence of elliptic curves whose ℓ-adic Galois representation achieves maximal image across *all* primes ℓ. Zywina offers a partial answer to this question by demonstrating that the ℓ-adic Galois representation of a "random" elliptic curve attains maximal image for all primes ℓ. The details of these methods will be discussed in the subsequent chapter.

4. More on Galois representations and torsion points of elliptic curves

4.1 Maximal image for all ℓ?

The goal in this chapter is to give a brief overview of Zywina's theorem from [3] and methods of proof involved. As mentioned in the previous chapter, Zywina shows that for any "random" elliptic curve, its ℓ-adic Galois representation has maximal image for all ℓ. However, it is necessary to first establish a precise notion of what "random" means in this context. Let K be a number field and let $\mathcal{O}_K$ denote its ring of integers. For $a, b \in \mathcal{O}_K^2$, define $\Delta_{a,b} = -16(4a^3 + 27b^2)$ and if $\Delta_{a,b} \neq 0$, define the elliptic curve $E(a, b)$ by the Weierstrass equation

$$E(a, b) : y^2 = x^3 + ax + b.$$

Fix a norm on $\mathbb{R} \otimes_{\mathbb{Z}} \mathcal{O}_K^2 \cong \mathbb{R}^{[K:\mathbb{Q}]}$, and for each real number $x \geq 0$, define the radius x ball

$$B_K(x) := \{(a, b) \in \mathcal{O}_K^2 : \Delta_{a,b} \neq 0, \|(a, b)\| \leq x)\}.$$

Further, let $\mathbb{Q}^{cyc} = \cup_{n=1}^{\infty} \mathbb{Q}(\zeta_n) \subset \overline{K}$ be the cyclotomic extension of $\mathbb{Q}$ for some choice of isomorphism $\overline{\mathbb{Q}} \cong \overline{K}$, $G = \mathrm{Gal}(\overline{K}/K)$ and $\rho_{E(a,b)} : G \to \mathrm{GL}_2(\hat{\mathbb{Z}})$ the ℓ-adic representation of $E(a, b)$. The theorem then states the following.

Theorem 4.1. *Suppose $K \cap \mathbb{Q}^{cyc} = \mathbb{Q}$ and $K \neq \mathbb{Q}$. Then,*

$$\lim_{x \to \infty} \frac{|\ \{(a, b) \in B_K(x) : \rho_{E(a,b)}(G) = \mathrm{GL}_2(\hat{\mathbb{Z}})\}\ |}{|\ B_K(x)\ |} = 1. \tag{4.1}$$

Heuristically, what this attempts to say is that for a "randomly" chosen pair $(a, b) \in \mathcal{O}_K^2$, the elliptic curve $E(a, b)$ satisfies $\rho_{E(a,b)} = \mathrm{GL}_2(\hat{\mathbb{Z}})$.

Just as in Proposition 3.7, there is a cyclotomic character $\chi_K : G \to \hat{\mathbb{Z}}^\times$, which is given by $\det \circ \rho_E$ for each elliptic curve E over K. The criteria $K \cap \mathbb{Q}^{cyc} = \mathbb{Q}$ is necessary for Theorem 4.1. To see this, note that $\mathrm{Gal}(\mathbb{Q}^{cyc}/\mathbb{Q}) = \varinjlim(\mathbb{Z}/n\mathbb{Z})^\times = \hat{\mathbb{Z}}^\times$. If $\chi_K(G) = H \subsetneq \mathrm{GL}_2(\hat{\mathbb{Z}})$, then

$$K \cap \mathbb{Q}^{cyc} = \overline{K}^{\chi_K^{-1}(H)} = (\mathbb{Q}^{cyc})^H \neq \mathbb{Q}.$$

One can generalise Theorem 4.1 further, in lieu of which one defines the group

$$H_K := \{A \in \mathrm{GL}_2(\hat{\mathbb{Z}}) : \det(A) \in \chi_K(G_K)\}.$$

Then,

Theorem 4.2. *Let $K \neq \mathbb{Q}$ be a number field. Then,*

$$\frac{|\ \{(a, b) \in B_K(x) : \rho_{E(a,b)}(G_K) \neq H_K\}\ |}{|\ B_K(x)\ |} \ll_{K,\|\cdot\|} \frac{\log x}{\sqrt{x}} \tag{4.2}$$

In other words, this theorem essentially says that the proportion of elliptic curves $E(a, b)$ such that $\rho_{E(a,b)}(G_K) = H_K$ quickly approaches 1 as a function of x. Here $f \ll g$ means that there are positive constants c_1 and c_2 such that $|f(x)| \leq c_2|g(x)|$ for $x \geq c_1$ (alternatively, the rest of this essay also uses the notation $O(f)$ to represent an unspecified function g with $g \ll f$.)

The proof broadly involves the following steps, that we shall delve into in greater detail in the following sections.

> *Step I:* Using a group theoretic argument, show that for any fixed elliptic curve E, $\rho_E(G_K) = H_K$ is equivalent to having $\rho_{E,\ell}(G_{K^{cyc}}) \supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for $\ell \geq 5$ and $\rho_{E,m}(G_{K^{cyc}}) = \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ for $m = 4, 9$ under certain assumptions.
>
> *Step II:* For a fixed integer m and conjugacy class C of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, show that the image $\rho_{E,m}(G_K) \cap C$ is almost never empty using a large sieve inequality and a theorem by Jones. As the number of conjugacy classes are finite, this must mean that almost all curves have their mod-m images lying in H_K for every m.
>
> *Step III:* As we wish to understand the image of $\rho_{E,\ell}(G)$ for every ℓ, use a theorem by Masser and Wüstholz to reduce and bound the number of ℓ's to be considered.
>
> *Step IV:* Lastly, verify that the hypotheses in Step I are true for most elliptic curves, again using large sieves.

4.2 Useful results from around about

In this section, we briefly state some theorems that are used in Zywina's proof, along with further references.

Large sieves

Sieve theory generally focuses on determining the asymptotic values of averages of arithmetic functions over integers, subject to congruence restrictions modulo specific prime numbers. Suppose the congruence conditions permit only integers n with residues modulo a prime p not belonging to a specified set Ω_p, say. If Ω_p contains few residue classes (typically, a bounded number as p increases), the setting is that of a "small" sieve. Conversely, if the size of Ω_p increases, it characterizes a "large" sieve situation. It is this latter case that will be used to prove Theorem 4.1. For details on sieve theory and it formalisations, see [13] Chapter 2.

The following theorem by Serre ([14] Chapter 12, §12.1, Theorem) gives a large sieve inequality which be used in the proof.

Theorem 4.3. *Let K be a number field, Λ be a free $\mathcal{O}_K$-module of rank n. Let $\|\cdot\|$ be a norm over $\Lambda_{\mathbb{R}} = \mathbb{R} \otimes_{\mathbb{Z}} \Lambda$. Fix a subset Y of Λ. We impose bounds on the "size" of Y both from the archimedean and non-archimedean viewpoints. More precisely, let x, Q be real numbers such that $x \geq 1, Q > 0$. For every prime ideal $\mathfrak{p} \in \Sigma_K$, let $\omega_{\mathfrak{p}}$ be a real number in $[0, 1)$. Let $\Sigma_K(Q)$ consist of all $\mathfrak{p} \in \Sigma_K$ such that $N(\mathfrak{p}) \leq Q$. Assume*

- *The set Y is contained in a ball of diameter x. i.e, there is a_0 in $\Lambda_{\mathbb{R}}$ such that $|a - a_0| \leq x$ for all $a \in Y$.*
- *For every $\mathfrak{p} \in \Sigma_K(Q)$, the image $Y_{\mathfrak{p}}$ of Y in $\Lambda/\mathfrak{p}\Lambda$ by reduction modulo $\mathfrak{p}$ satisfies*

$$|Y_{\mathfrak{p}}| \leq (1 - \omega_{\mathfrak{p}})|\Lambda/\mathfrak{p}\Lambda|.$$

Then,

$$|Y| \ll_{K,\Lambda,\|\cdot\|} \frac{x^{[K:\mathbb{Q}]n} + Q^{2n}}{L(Q)},$$

where

$$L(Q) := \sum_{\substack{\mathfrak{a} \subseteq \mathcal{O}_K \\ squarefree \\ N(\mathfrak{a}) \leq Q}} \prod_{\mathfrak{p}|\mathfrak{a}} \frac{w_{\mathfrak{p}}}{1 - \omega_{\mathfrak{p}}}.$$

Assumption 2 implies that a proportion $\omega_{\mathfrak{p}}$ of the classes modulo $\mathfrak{p}$ are missing from $Y_{\mathfrak{p}}$, in other words, they have been "sieved out".

To see a quick example of this theorem in action, consider $K = \mathbb{Q}$, $\Lambda = \mathbb{Z}$, $n = 1$, and some $x \in \mathbb{R}_{>1}$. Let Y be the set of squares in $[1, x]$ and set w_p to be near $1/2$ for every prime p. Then, $\sum_{\mathbb{Q}}(Q)$ would consist of primes $p < Q$. As there are $(p-1)/2$ squares in $(\mathbb{Z}/p\mathbb{Z})^{\times}$, the assumptions of Theorem 4.3 are satisfied. By letting $Q \sim x^{1/2}$ and approximating $L(Q) \sim Q$[1], the Theorem yields $|Y| \ll x^{1/2}$.

In our case, we shall let $\Lambda = \mathcal{O}_K^2$ and $\| \cdot \|$ to be the fixed norm on $\mathbb{R} \otimes_{\mathbb{Z}} \mathcal{O}_K^2$.

Theorems by Masser-Wüstholz and Jones

The next two theorems will be particularly useful while proving Steps II and III.

Theorem 4.4 (Masser and Wüstholz)**.** *Let E be an elliptic curve defined over a number field K and assume E does not have complex multiplication. Then, there are positive absolute constants c and γ such that if $\ell > c(\max\{[K : \mathbb{Q}], h(j(E))\})^{\gamma}$, then $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \subseteq \rho_{E,\ell}(G_K)$.*

For the following theorem by Jones, let E be an elliptic curve over $\mathbb{F}_p$, and let $\rho_{E,m} : \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ be a Galois representation arising from the m-torsion of E. Let $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ be the p^{th} power Frobenius auomorphism. For a conjugacy class $C \in \mathrm{GL}_2(\mathbb{Z}/mZ)$ define

$$\Omega_C(p) := \{(r, s) \in \mathbb{F}_p^2 : \Delta_{r,s} \neq 0, \rho_{E(r,s),m}(\mathrm{Frob}_p) \in C\}.$$

This is the set of elliptic curves whose images of m-torsion lie in the same conjugacy class. The following theorem gives an estimate on the cardinality of this set.

Theorem 4.5 (Jones)**.** *Fix a positive integer m and a conjugacy class C of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Let d be the element of $(\mathbb{Z}/m\mathbb{Z})^{\times}$ such that $\det(C) = \{d\}$. Then, for all primes p with $p \equiv d \mod m$,*

$$\frac{|\Omega_C(p)|}{p^2} = \frac{|C|}{\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})} + O\left(\frac{|C|}{p^{1/2}}\right).$$

4.3 Proof of Theorem 4.1

The first step in the proof if to identify the condition for which ρ_E has maximal Galois image. Suppose E is an elliptic curve over number field $K \neq \mathbb{Q}$. Then there is an exact sequence

$$\begin{tikzcd} 1 \arrow[r] & \mathrm{SL}_2(\hat{\mathbb{Z}}) \arrow[r] & \mathrm{GL}_2(\hat{\mathbb{Z}}) \arrow[r, "\det"] & \hat{\mathbb{Z}}^{\times} \arrow[r] & 1 \end{tikzcd}$$

and the representation $\det \circ \rho_E : G_K \to \hat{\mathbb{Z}}^{\times}$ is the cyclotomic character χ_K of K. Therefore,

$$\rho_E(G_K) \cap \mathrm{SL}_2(\hat{Z}) = \rho_E(G_{K^{cyc}}).$$

Recall that H_K is defined to be

$$H_K := \{A \in \mathrm{GL}_2(\hat{\mathbb{Z}}) : \det(A) \in \chi_K(G_K)\}.$$

Thus, the equality $\rho_E(G_K) = H_K$ is equivalent to $\rho_E(G_{K^{cyc}}) = \mathrm{SL}_2(\hat{\mathbb{Z}})$.

The following Proposition gives the criteria for maximal Galois action for a *fixed* elliptic curve.

Proposition 4.6. *Let E be an elliptic curve over a number field K and let Δ be the discriminant of E. Suppose the following conditions hold:*

[1] If you're wondering why $L(Q) \sim Q$, note that for large x, approximately $3/4$ of the numbers less than x are not divisible by 4, $8/9$ of the numbers are not divisible by 9 and so on. Using the Chinese Remiander Theorem, one can approximate and obtain $L(Q) \approx (6Q)/\pi^2$.

(a) $\rho_{E,\ell}(G_K) \supseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ *for every prime* $\ell \geq 5$*;*

(b) $\rho_{E,4}(G_K) \supseteq \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$ *an d*$\rho_{E,9}(G_K) \supseteq \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$*;*

(c) $\sqrt{\Delta} \notin K^{cyc}$

(d) $\mu_3 \nsubseteq K$ *or* $\sqrt[3]{\Delta} \notin K^{cyc}$*;*

Then $\rho_E(G_K) = H_K$*.*

Proof. See [3] Proposition 2.1. □

We can now apply the large sieve to show that most elliptic curves have maximal Galois action. For a positive integer m and a conjugacy class C of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, define the set

$$Y_C(x) := \{(a,b) \in B_K(x) : \rho_{E(a,b),m}(G_K) \cap C = \varnothing\}.$$

This is the set of elliptic curves whose mod-m image does not lie in a particular conjugacy class. For $d \in (\mathbb{Z}/m\mathbb{Z})^\times$, let $\sum_K^1(Q;d,m)$ denote the set of $\mathfrak{p} \in \sum_K(Q)$ such that $N(\mathfrak{p})$ prime and $N(\mathfrak{p}) \equiv d \mod m$. Further, define for each positive integer m,

$$B_{K,m}(x) := \{(a,b) \in B_K(x) : \rho_{E(a,b),m}(G_K) \nsupseteq \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})\}.$$

This consists of elliptic curves whose mod-m Galois representation does not have maximal image.

Proposition 4.7. *Let m be a positive integer and C be a conjugacy class of* $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$*. Let d be the unique element of* $(\mathbb{Z}/m\mathbb{Z})^\times$ *such that* $\det(C) = \{d\}$*, and assume* $\chi_K(G_K) \mod m \subseteq (\mathbb{Z}/m\mathbb{Z})^\times$*. Then,*

$$\frac{|Y_C(x)|}{|B_K(x)|} \ll_{K,\|\cdot\|} \frac{|\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})|}{|C|}\left(\sum_K^1(x^{[K:\mathbb{Q}]/2};d,m)| + O_K(m^3 x^{[K:\mathbb{Q}]/4}\right)^{-1}.$$

Proof. (Sketch). This is a straightforward application of Theorem 4.3 and Theorem 4.5. Define $Q := x^{[K:\mathbb{Q}]/2}$ and for each $\mathfrak{p} \in \sum_K^1(Q,d,m)$, define

$$\Omega_\mathfrak{p} = \{(r,s) \in \mathbb{F}_\mathfrak{p}^2 : \Delta_{r,s} \neq 0, \rho_{E(r,s),m}(\mathrm{Frob}_{N(\mathfrak{p})}) \in C\}$$

Let $Y_\mathfrak{p}$ be the image of $Y_C(x)$ in $\mathbb{F}_\mathfrak{p}^2$. After checking that these sets satisfy the hypotheses in Theorem 4.3, for $\mathfrak{p} \notin \sum_K^1(Q,d,m)$ set $\omega_\mathfrak{p} = 0$. For $\mathfrak{p} \in \sum_K^1(Q,d,m)$, Theorem 4.5 gives

$$\omega_\mathfrak{p} = \frac{|C|}{|\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})|} + O\left(\frac{|C|}{N(\mathfrak{p})^{1/2}}\right)$$

Then, combining the bound for $L(Q)$ obtained from Theorem 4.3 along with the fact that $|B_K(x)| \sim bx^{2[K:\mathbb{Q}]}$ for some constant b as $x \to \infty$ yields the result. For more details, see [3] Proposition 5.5. □

Using the fact that there are a finite number of conjugacy classes, and taking their unions, one can say that for a random elliptic curve E, $\rho_{E,m}$ has maximal image. More precisely,

Proposition 4.8. *For a positive integer m,*

$$\frac{|B_{K,m}(x)|}{B_K(x)} \ll_{K,\|\cdot,\|,m} \frac{\log x}{x^{[K:\mathbb{Q}]/2}}$$

Proof. See [3] Proposition 5.7. □

So far, we focused on a fixed positive integer m. However, we wish to understand the image for all primes. Theorem 4.4 gives us a bound on the number of ℓ's that need to be considered. Using bounds from Proposition 4.7 and 4.8, and by setting $\beta = 8\gamma + 1$ (the γ comes from Theorem 4.4), we may deduce

Proposition 4.9. *There is an absolute constant $\beta \geq 1$ such that*

$$\frac{|B_{K,4}(x) \cup B_{K,9}(x) \cup \bigcup_{\ell \geq 5} B_{K,\ell}(x)|}{|B_K(x)|} \ll_{K,\|\cdot\|} \frac{(\log x)^\beta}{x^{[K:\mathbb{Q}]/2}}.$$

Proof. See [3] Proposition 5.2. □

This completes the proof that any "random" elliptic curve has maximal Galois image if the hypotheses in Proposition 4.6 are satisfied. But, the question then remains - do most curves satisfy the hypotheses in Proposition 4.6. The answer is positive, answered by the following

Proposition 4.10. *Fix a number field $K \neq \mathbb{Q}$ and an integer $r \geq 2$ and assume that $\mu_r \subset K$. Then,*

$$\frac{|\{(a,b) \in B_K(x) : \sqrt[r]{\Delta_{a,b}} \in K^{cyc}\}|}{|B_K(x)|} \ll_{K,\|.\|,r} \frac{\log x}{\sqrt{x}}.$$

Proof. (Sketch). The idea is to use the large sieve inequality from Theorem 4.3 again. Define S to be a finite set of primes that satisfy

(i) S contains primes dividing $6r$,

(ii) S contains primes that are ramified in K,

(iii) $\mathcal{O}_S$ is a principal ideal domain, where $\mathcal{O}_S$ is the ring if S' integers where

$$S' = \{\mathfrak{p} \in \Sigma_K : \mathfrak{p} \mid p, \text{ for some } \mathfrak{p} \in S\}.$$

Then, for each $\beta \in \mathcal{O}_S^\times$, define sets

$$W_\beta := \{(a,b) \in \mathcal{O}_K^2 : \Delta_{a,b} = m\alpha^r\beta, \text{ for some } m \in \mathbb{Z}, \alpha \in \mathcal{O}_S\}$$

and $W_\beta(x) = W_\beta \cap B_K(x)$. Let $W_{\beta,p}$ be the image of W_β in $\mathcal{O}_K^2/p\mathcal{O}_K^2$ for each $p \notin S$ and p splits completely in K.

Let I be the set of primes that split completely in K. For each $p \in I$, set $w_p = 1 - \frac{1}{r^{d-1}} + O_{r,d}(p^{-1/2})$, and for $p \notin I$, set $w_p = 0$. Then, W_β and $W_{\beta,p}$ satisfy the assumptions of Theorem 4.3, and so we obtain

$$|W_\beta(x)| \ll_{K,\|\cdot\|} \frac{x^{2d}}{L(\sqrt{x})}, \tag{4.3}$$

where

$$L(\sqrt{c}) := \sum_{\substack{J \subseteq I \text{ finite} \\ \prod_{p\in J} p \leq \sqrt{x}}} \prod_{p \in J} \frac{\omega_p}{1-\omega_p}.$$

Using $r \geq 2$ and $d = [K : \mathbb{Q}] \geq 2$, we obtain

$$L(\sqrt{x}) \geq \sum_{\substack{J \subseteq I \text{ finite} \\ \prod_{p\in J} p \leq \sqrt{x}}} \prod_{p \in J} (1 + O_{r,d}(p^{-1/2})) \geq \sum_{\substack{p \in I \\ p \leq \sqrt{x}}} (1 + O_{r,d}(p^{-1/2})). \tag{4.4}$$

Using (4.3) and (4.4) along with another inequality (see [3] (6.1)) yields the result. □

Finally, we may use these results covered so far to prove Theorem 4.1.

Proof of Theorem 4.1. Define the sets

$$Y_1(x) = B_{K,4}(x) \cup B_{K,9}(x) \cup \bigcup_{\ell \geq 5} B_{K,\ell}(x)$$
$$Y_2(x) = \{(a,b) \in B_K(x) : \sqrt{\Delta_{a,b}} \in K^{cyc}\}$$
$$Y_3 = \{(a,b) \in B_K(x) : \mu_3 \subseteq K \text{ and } \sqrt[3]{\Delta_{a,b}} \in K^{cyc}\}$$

By Proposition 4.6, we have

$$\{(a,b) \in B_K(x) : \rho_{E(a,b)}(G_K) \neq H_K\} \subseteq Y_1(x) \cup Y_2(x) \cup Y_3(x),$$

and so

$$|\{(a,b) \in B_K(x) : \rho_{E(a,b)}(G_K) \neq H_K\}| \leq |Y_1(x)| + |Y_2(x)| + |Y_3(x)|.$$

By Proposition 4.9, we have

$$\frac{|Y_1(x)|}{|B_K(x)|} \ll_{K,\|\cdot\|} \frac{(\log x)^\beta}{x^{[K:\mathbb{Q}]/2}}$$

where $\beta \geq 1$ is an absolute constant. By Proposition 4.10, we have

$$\frac{|Y_2(x)|}{|B_K(x)|} \ll_{K,\|\cdot\|} \frac{\log x}{\sqrt{x}} \qquad \text{and} \qquad \frac{|Y_3(x)|}{|B_K(x)|} \ll_{K,\|\cdot\|} \frac{\log x}{\sqrt{x}}.$$

Combining everything together gives

$$\frac{|\{(a,b) \in B_K(x) : \rho_{E(a,b)}(G_K) \neq H_K\}|}{|B_K(x)|} \ll_{K,\|\cdot\|} \max\left\{\frac{(\log x)^\beta}{x^{[K:\mathbb{Q}]/2}}, \frac{\log x}{\sqrt{x}}\right\} \ll \frac{\log x}{\sqrt{x}}.$$

□

5. Conclusion

Serre's seminal work has paved the way for numerous avenues of research over the past fifty years. In the last chapter, we explored a potential direction stemming from Serre's open image theorem, specifically focusing on determining which elliptic curves exhibit maximal image for all ℓ. On the other hand, a lot of effort has gone into identifying and computing all possible images of $\rho_{E,\ell}$ for all kinds of elliptic curves and values of ℓ. The problem of classifying all possible Galois images over $\mathbb{Q}$ is also often referred to the "Program B" by Mazur. More precisely, "Given a subgroup H of $\mathrm{GL}_2(\hat{\mathbb{Z}}) \cong \prod_p \mathrm{GL}_2(\mathbb{Z}_p)$, classify all elliptic curves $E/\mathbb{Q}$ whose associated Galois representation on torsion points maps $\mathrm{Gal}(\overline{K}/K)$ into $H \leq \mathrm{GL}_2(\hat{Z})$". Substantial progress has been made for both CM and non-CM curves over $\mathbb{Q}$ for prime order, power of prime order and multi prime order - see [15], [16], [17]. On the computational side, substantial progress has been made in effectively computing these images, for example see [18].

One can also view Serre's theorem through a different lens. Another way of rephrasing Theorem 3.3 is to say that there exists a constant $n(E, K)$ such that for all $\ell > n(E, K)$, ρ_ℓ is surjective. One can ask if there exists a constant $n(K)$ that only depends on the number field K and is independent of the choice of elliptic curve E such that Theorem 3.3 holds. This is sometimes dubbed as Serre's uniformity problem, and partial progress has been made in this direction. As seen in §2.3, subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ consist of normalizers of (split and nonsplit) Cartan subgroups, Borel subgroups, and "exceptional" subgroups (those whose projective image is isomorphic to one of the groups A_4, S_4 or A_5). To solve Serre's uniformity problem, one has to show that for sufficiently large n, the image of the Galois representation is not contained in any of the above listed maximal subgroups. Serre himself settled the case of exceptional subgroups in [19], and the work of Mazur [20] on rational isogenies implies Serre uniformity for the Borel subgroups. In the Cartan case, Bilu and Parent [21] answer the question for the split cartan case. The case of the non-split Cartan is actively being researched.

Bibliography

[1] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent Math*, 15:259–331, 1972.

[2] Jean-Pierre Serre. *Abelian ℓ-adic representations and Elliptic curves.* Lecture Notes in Mathematics, 1968.

[3] David Zywina. Elliptic curves with maximal galois action on their torsion points. *Bull. Lond. Math. Soc.*, 42(5):811–826, 2010.

[4] Joseph H. Silverman. *The Arithmetic of Elliptic Curves (2nd ed.).* Springer-Verlag New York, 2009.

[5] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves.* Springer-Verlag New York, 1994.

[6] Jean-Pierre Serre. *Local Fields.* Springer-Verlag New York, 1979.

[7] J.S. Milne. Class field thoery. https://www.jmilne.org/math/CourseNotes/CFT.pdf, 202o. [Online; accessed 6 April 2024].

[8] Bjorn Poonen. *Rational Points on Varieties.* American mathematical Society, 2017.

[9] The LMFDB Collaboration. The L-functions and modular forms database. https://www.lmfdb.org, 2024. [Online; accessed 5 April 2024].

[10] Jean-Pierre Serre. *Local Fields.* Springer New york, 1980.

[11] Jürgen Neukirch. *Algebraic Number Theory.* Springer, Berlin, 1999.

[12] A.P. Ogg. Abelian curves of small conductor. *Journ. für die reine und ang. Math*, 226:204–215, 1967.

[13] E. Kowalski. *The Large Sieve and Its Applications: Arithmetic Geometry, Random Walks and Discrete Groups.* Cambridge University Press, 2008.

[14] Jean-Pierre Serre. *Lectures on the Mordell-Weil Theorem.* Vieweg+Teubner Verlag Wiesbaden, 1997.

[15] Zureick-Brown D Rouse J, Sutherland AV. ℓ -adic images of galois for elliptic curves over $\mathbb{Q}$ (and an appendix with john voight). *Forum of Mathematics, Sigma.*, 10, 2022.

[16] Abbey Bourdon and Pete L. Clark. Torsion points and galois representations on cm elliptic curves. *Pacific J Math.*, 305:43–88, 2020.

[17] Harris B. Daniels and Enrique González-Jiménez. Serre's constant of elliptic curves over the rationals. *Experimental Mathematics*, 31(2):518–536, 2022.

[18] Andrew V. Sutherland. Computing images of galois representations attached to eliptic curves. *Forum of Mathematics, Sigma.*, 4, 2015.

[19] Jean-Pierre Serre. Quelques applications du théorème de densité de chebotarev. *Inst. Hautes Etudes Sci. Publ. Math.*, 54:323–401, 1981.

[20] B. Mazur. Rational isogenies of prime degree. *Invent Math.*, 44:129–162, 1978.

[21] Yuri Bilu and Pierre Parent. Serre's uniformity problem in the split cartan case. *Ann. of Math.*, 173(1):569–584, 2011.