GALOIS REPRESENTATIONS FROM ELLIPTIC CURVES

JOHN XIAOSHU ZHOU

Abstract. In this paper, we will explain the basics of Galois representations coming from elliptic curves, including examples. We will also give a foundation of the theory of elliptic curves from a scheme-theoretic perspective. We assume some basic algebraic number theory and algebraic geometry. A good reference would be *Algebraic Number Theory* by J. Neukirch for the former and *Algebraic Geometry* by R. Hartshorne for the latter.

Contents

1. Introduction

The absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of $\mathbb{Q}$ is a central object of study for algebraic number theory. One key tool for studying it is the representation theory. To that end, our first task is to give a definition for a Galois representation. In order to fully appreciate the definition, we need to recall some key features of the Krull topology on $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Under the Krull topology, the closed subgroups are $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ for intermediate extensions $\mathbb{Q} \subset K \subset \overline{\mathbb{Q}}$ and the open subgroups are $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ for $K/\mathbb{Q}$ finite. Moreover, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is a topological group with respect to the Krull topology.

Definition 1.1. Let V be a module over a topological ring R. A continuous Galois representation is a continuous homomorphism

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(V)$$

with respect to the Krull topology on $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and the induced topology on V by the topology of R.

Date: AUGUST 14.

Essentially all Galois representations we consider will be continuous, and we will simply call them Galois representations by abuse of notation. Familiar examples of Galois representations include Artin representations (representations of the absolute Galois group on complex vector spaces), adelic Galois representations (representations over modules over $\hat{\mathbb{Z}}$, the profinite completion of the integers), ℓ-adic Galois representations (representations over modules over $\mathbb{Z}_\ell$, the ℓ-adic integers $\mathbb{Z}_\ell$), and Galois representations over finite fields such as $\mathbb{F}_p$.

To demonstrate the usefulness of Galois representations, it is perhaps instructive to consider the easy special case of Artin representations.

Example 1.2. An Artin representation is a continuous homomorphism

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C})$$

for some integer n. Immediately, one sees that an easy way to produce such representations is by first projecting $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ for some finite Galois extension $K/\mathbb{Q}$, and then invoking the representation theory of the finite group $\mathrm{Gal}(K/\mathbb{Q})$ to produce a representation

$$\overline{\rho} : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C}).$$

Surprisingly, this is the only way Artin representation arises. This is largely due to the "continuous" requirement. Notice that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is isomorphic (as a topological group) to a profinite group, and is therefore totally disconnected. As ρ is continuous, the image of ρ must be a compact totally disconnected topological group. However, since the target $\mathrm{GL}_n(\mathbb{C})$ carries the subspace topology of Euclidean space, by basic topology, one concludes that the image of ρ must be finite. In particular, the kernel of ρ must be a closed subgroup of finite index of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and so must be an open subgroup by basic properties of topological groups. By the definition of the Krull topology, one concludes that

$$\ker(\rho) \simeq \mathrm{Gal}(\overline{\mathbb{Q}}/K)$$

for some finite Galois extension $K/\mathbb{Q}$. In particular, the image must be $\mathrm{Gal}(K/\mathbb{Q})$. Hence, any Artin representation must factor through $\mathrm{Gal}(K/\mathbb{Q})$ for some finite Galois extension $K/\mathbb{Q}$. Heuristically, the interaction between the different topologies between the source and target of Galois representations makes the image of Galois representations "simple", which in turn makes Galois representations a particularly useful tool in studying $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. In fact, the difference in topologies is so large in the case of Artin representations that it tells us nothing more than the representation theory of finite Galois groups. In the case of ℓ-adic representations, we will see that the image can actually be infinite.

Another important easy example of Galois representation is the cyclotomic characters.

Example 1.3. Given positive integer n, let μ_n be the group of n^{th} roots of unities. Let ζ_n be a fixed generator. Given $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we must have $\sigma(\zeta_n) = \zeta_n^{\chi_n(\sigma)}$ for some $\chi_n : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$. One easily checks that χ_n is a group homomorphism and is independent of our choice of ζ_n as a generator. In fact, χ_n is the restriction map $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$ (note that $\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$ is canonically isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$). We call χ_n the mod n cyclotomic character. By definition, χ_n is a 1-dimensional Galois representation over the ring $\mathbb{Z}/n\mathbb{Z}$. Now suppose p is a prime. One can check that the diagram

$$\begin{tikzcd}
\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \arrow[r, "\chi_{p^r}"] \arrow[dr, "\chi_p"'] & (\mathbb{Z}/p^r\mathbb{Z})^\times \arrow[d, "\mathrm{mod}\, p"] \\
& (\mathbb{Z}/p\mathbb{Z})^\times
\end{tikzcd}$$

commutes. In particular, we may take a limit and obtain a p-adic cyclotomic character $\chi_{p,\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{Z}_p^\times$. More generally, the above diagram commutes if we replace p and p^r with any m, k such that $m \mid k$. If we take a limit, we then get the adelic cyclotomic character $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \hat{\mathbb{Z}}^\times$, where we have

$$\lim \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) = \lim(\mathbb{Z}/n\mathbb{Z})^\times = \hat{\mathbb{Z}}^\times.$$

The study of such representations is fruitful. The Kronecker-Weber theorem tells us that

$$\mathbb{Q}^{\mathrm{ab}} = \mathrm{colim}\, \mathbb{Q}(\mu_n),$$

where $\mathbb{Q}^{\mathrm{ab}}$ is the maximal abelian extension of $\mathbb{Q}$ and μ_n is the set of n^{th} roots of unity. In particular, we have

$$\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) = \lim \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}).$$

This shows that the adelic cyclotomic character is just the restriction to the maximal abelian extension. In particular, χ tells us the abelianization of all the Galois groups over $\mathbb{Q}$. As a side remark, notice that unlike in Artin representations, all cyclotomic characters are surjective (being reduction maps).

The bulk of Galois representations in nature arise from geometry. The main topics of this paper, Galois representations from elliptic curves, are of such type. The general method for one to obtain Galois representations from elliptic curves (and more generally abelian varieties) is by considering the action of the Galois group on the n-torsion points of the elliptic curve. For special modular forms known as eigenforms, one can obtain an abelian variety called the Jacobian, and obtain Galois representations from the Jacobian. In fact, we have the following result by Khare and Wintenberger (see [3]).

Theorem 1.4 (Serre's Modularity Conjecture)**.** *Any two-dimensional absolutely irreducible odd Galois representation over a finite field arises from a modular form.*

One interpretation of the result is that most reasonable two-dimensional Galois representations come from geometry. Something more precise could be said along those lines.

Given an algebraic variety X over $\mathbb{Q}$, set $X_{\overline{\mathbb{Q}}} = X \times_{\mathbb{Q}} \overline{\mathbb{Q}}$. Then the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the étale cohomology groups $H^i((X_{\overline{\mathbb{Q}}})_{\text{ét}}, \mathbb{Z}/n\mathbb{Z})$, which produces Galois representations. Under this interpretation, we may recover the representation given by torsion points on an abelian variety A by setting $i = 1$ and $X = A$, with suitable coefficient rings. One can then conjecture that all reasonable Galois representations arise in this fashion. The precise statement is known as the Fontaine-Mazur conjecture. Due to the scope of this paper, we will not attempt to state the conjecture. For a precise formulation of the conjecture, see [2].

2. Galois Representations from Elliptic Curves

2.1. **Preliminaries.** We will first survey some basic concepts and properties related to elliptic curves, and then discuss how Galois representations are related to elliptic curves. We would first work over a general field k. For simplicity, we may assume that k is perfect.

Definition 2.1. Let k be a field. An elliptic curve (E, O) over k have the following three equivalent definitions:

(1) A nonsingular irreducible projective plane curve E of degree 3 over k along with a distinguished k-point O;

(2) A nonsingular irreducible projective curve E of genus 1 over k along with a distinguished k-point O;

(3) A projective plane curve E over k defined by the Weierstrass equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

where $a_i \in k$ and $O = [0 : 1 : 0]$.

At an elementary level, the third definition is the most commonly presented. While being the most concrete definition, it is also a bit ad hoc. Its equivalence to the first definition resolves this issue. Elliptic curves are actually the next logical step when one considers solving Diophantine equations (as the degree 1 case is easily solved and the degree 2 case is solved by appealing to the Hasse-Minkowski theorem).

Here's a quick sketch of the equivalence of these three definitions. Definition (1) implies definition (2) by the degree-genus formula. Definition (2) implies definition (3) by computation of the dimension of the global section of $\mathcal{O}_E(3O)$ via Riemann-Roch, then using a basis $\{1, x, y\}$ of $\mathcal{O}_E(3O)$ to form an embedding $E \setminus \{O\} \to \mathbb{P}^2$ with $P \mapsto [x(P) : y(P) : 1]$ that extends to an embedding $E \to \mathbb{P}^2$ by $O \mapsto [0 : 1 : 0]$, which satisfies the given equation by computation of the dimension of $\Gamma(E, \mathcal{O}_E(6O))$, again by Riemann-Roch. Definition (3) implies definition (1) is immediate by setting $O = [0 : 1 : 0]$. For a complete proof, see [1] page 45.

When k is algebraically closed, E could be viewed as an algebraic variety in the traditional sense and there is no harm in only considering the closed points. When k is not algebraically closed, the closed points of E are in natural bijection with the closed points in $\mathbb{P}^2_{\overline{k}}$ satisfying the defining Weierstrass equation whose coordinates lie in k. For field extensions L/k, one can consider the fiber product $E_L = E \times_k L$, whose closed points can be thought of as the closed points in $\mathbb{P}^2_{\overline{k}}$ satisfying the same Weierstrass equation whose coordinates lie in L. Notice that there can be multiple defining Weierstrass equations for an elliptic curve, via change of coordinates. To each Weierstrass equation, one attaches two quantities, the discriminant Δ and a quantity known as c_4. The discriminant is a handy quantity that can be used to test whether something written in the form of a Weierstrass equation is an elliptic curve or not, i.e., whether or not it is singular. A Weierstrass equation represents a singular elliptic curve if and only if the discriminant is zero. Neither quantity is invariant under change of basis. However, the quantity $j = c_4^3/\Delta$, known as the j-invariant, is independent of basis change. A fact that is often convenient for us is when the characteristic of k is not 2 or 3, we can always change variables to make the Weierstrass equation into

$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

We now proceed to define a central notion of the theory of elliptic curves, the group law. For elliptic curves over algebraically closed fields, there are two ways that one can construct the group law. We first present the more general and abstract way. For an elliptic curve E over a field k, denote its Picard group $\mathrm{Pic}(E)$. As principal divisors have degree 0, we have the natural degree map $\deg : \mathrm{Pic}(E) \to \mathbb{Z}$ inherited from that of the divisor group. We call the kernel of the degree map the degree-0 part of the Picard group and denote it by $\mathrm{Pic}^0(E)$. For a field extension L/k, we denote by $E(L)$ the L-valued points of E. One can then formulate a key observation.

Proposition 2.2. *Let E be an elliptic curve over k and L/k a field extension. There is a natural bijection between $\mathrm{Pic}^0(E_L)$ and $E(L)$.*

Proof. Letting D be a Weil divisor of E_L with degree 0, it suffices to show that there exists a unique L-point (P) of E such that D is linearly equivalent to $(P) - (O)$. We do this by Riemann-Roch. By definition, E has genus 1, so Riemann-Roch tells us that $\dim \mathcal{L}(D + (O)) = 1$. We may pick a nonzero $f \in L(E_L)$ such that $\mathrm{div}(f) \geq -D - (O)$. As the degree of $\mathrm{div}(f)$ is 0, we must have $\mathrm{div}(f) = -D - (O) + (P)$ for some L-point P of E. We have thus demonstrated the existence of such a point. For uniqueness, suppose (P') also has the property. We then have (P') is linearly equivalent to (P). In particular, there exists $f \in L(E_L)$ such that $\mathrm{div}(f) = (P) - (P')$, so $f \in \mathcal{L}((P'))$. By Riemann-Roch, one has $\dim \mathcal{L}((P')) = 1$, but $L \subset \mathcal{L}((P'))$, so we must have that f is a constant, and so $P = P'$, which shows uniqueness. □

The above proposition allows us to identify L-points on E with elements of $\mathrm{Pic}^0(E_L)$, which gives a group structure on $E(L)$. This is known as the *algebraic group law* of $E(L)$.

Correspondingly, there is a *geometric group law* on $E(L)$ given by the following. Choose an embedding $E_L \to \mathbb{P}^2_L$. Let $P, Q \in (E_L)(L) = E(L)$. As E has degree 3, the line connecting P and Q intersects a third L-point R of E by Bézout's theorem. We set $P + Q$ to be the third intersection point of the line connecting R and O with E. One can show that this gives an abelian group structure on E with identity O.

One can also check that if we a priori endow $E(L)$ with the geometric group law, then the map in Proposition 2.2 becomes an isomorphism of groups, i.e., the two group laws agree, and we will from now on refer them as the *group law* on $E(L)$. More generally, one can show that E is a *group variety*, that is, for any k-variety S, the S-valued points of E form a group. Moreover, as we require elliptic curves to be smooth, E is automatically an *abelian variety* over characteristic zero fields. This property is true over arbitrary characteristic and is in fact a defining property. An alternative definition for an elliptic curve would be a 1-dimensional abelian variety.

Remark 2.3. At a higher level, one can construct a k-variety called the *Picard variety* whose set of L-points is exactly $\mathrm{Pic}^0(E_L)$, and there is an isomorphism of k-schemes between the Picard variety of E and E that will induce the bijection of L-points described by Proposition 2.2.

In the simple case where k has characteristic 0, up to change of variables, one can use the differential equation satisfied by the Weierstrass $\wp$-function to create an explicit isomorphism as complex varieties between the analytification of $E \times_k \mathbb{C}$ and the torus $\mathbb{C}/\Lambda$ for some lattice Λ. In this case, the group law on $E(\mathbb{C})$ is simply given by addition in $\mathbb{C}/\Lambda$.

Another good thing about the group law is that it allows us to characterize principal divisors. A divisor is principal if and only if it has degree zero and is in the kernel of the map $\mathrm{Div}^0(E) \to E$. Hence, to check whether a divisor is principal or not, it suffices to compute the degree and to add the points in the elliptic curve according to the group law and see if one gets O.

Now we define the correct notion of "morphisms" between elliptic curves.

Definition 2.4. A morphism between elliptic curves over k is a morphism as k-group schemes.

This is more commonly known as an *isogeny* between elliptic curves. Two elliptic curves E_1 and E_2 over k are said to be *isogenous* if there is an isogeny $\phi : E_1 \to E_2$ that does not factor through the structure morphism $E_1 \to \mathrm{Spec}(k)$. In fact, due to the wonderful properties of elliptic curves, the notion of an isogeny can be weakened.

Proposition 2.5. *Let (E_1, O_1) and (E_2, O_2) be elliptic curves over k and $\phi : E_1 \to E_2$ a morphism of k-schemes that does not factor through the structure morphism of E_1 and maps O_1 to O_2. Then ϕ is an isogeny.*

Proof. This is a direct consequence of the group law on elliptic curves. We will show that such a map induces a group homomorphism on the geometric points. Recall the bijection between $E(\overline{k})$ and $\mathrm{Pic}^0(E_{\overline{k}})$. For the sake of this proof, we denote $\kappa_1 : E_1(\overline{k}) \to \mathrm{Pic}^0(E_{1,\overline{k}})$ and $\kappa_2 : E_2(\overline{k}) \to \mathrm{Pic}^0(E_{2,\overline{k}})$. As ϕ does not factor through the structure morphism, it is finite and induces a group homomorphism $\phi_* : \mathrm{Pic}^0(E_{1,\overline{k}}) \to \mathrm{Pic}^0(E_{2,\overline{k}})$ by point-wise application of ϕ. Moreover, since ϕ maps O_1 to O_2, by checking with the definition of κ_1 and κ_2, we have the following commutative diagram.

$$\begin{tikzcd}
E_1(\overline{k}) \arrow[r, "\kappa_1"] \arrow[d, "\phi"'] & \mathrm{Pic}^0(E_{1,\overline{k}}) \arrow[d, "\phi_*"] \\
E_2(\overline{k}) \arrow[r, "\kappa_2"] & \mathrm{Pic}^0(E_{2,\overline{k}})
\end{tikzcd}$$

Hence, ϕ induces a group homomorphism on the level of geometric points. □

The set of isogenies between E_1 and E_2 is denoted $\mathrm{Hom}(E_1, E_2)$, and is, in fact, an abelian group. However, the addition operation is a bit hard to define. On the level of $\overline{k}$-points, it is clear that the addition should just be point-wise addition. One way to proceed is to check that the map of $\overline{k}$-points satisfies a certain polynomial equation, and then invoke the property of the elliptic curves being a k-variety to show that there must be exactly one morphism of schemes that represents the sum. However, this method is not natural. With the above proposition, one can formulate a much more natural addition law. Consider the category of "based k-varieties", which we denote as $\mathrm{Var}_k^\bullet$, with objects diagrams of form

$$\begin{tikzcd}
\mathrm{Spec}(k) \arrow[r] & X \arrow[r] & \mathrm{Spec}(k)
\end{tikzcd}$$

with X a k-variety and morphisms commutative diagrams

$$\begin{tikzcd}
\mathrm{Spec}(k) \arrow[r] \arrow[dr] & X \arrow[r] \arrow[d] & \mathrm{Spec}(k) \\
 & Y \arrow[ur] &
\end{tikzcd}$$
.

By Proposition 2.5,

$$\mathrm{Hom}(E_1, E_2) \simeq \mathrm{Hom}_{\mathbf{Var}_k^\bullet}(E_1, E_2).$$

By Yoneda's lemma,

$$\mathrm{Hom}_{\mathbf{Var}_k^\bullet}(E_1, E_2) \simeq \mathrm{Nat}_{\mathrm{Fun}(\mathbf{Var}_k^\bullet, \mathbf{Sets})}(h_{E_1}, h_{E_2}),$$

where $h_E : (\mathbf{Var}_k^\bullet)^{\mathrm{op}} \to \mathbf{Sets}$ is the representable functor given by

$$h_E(X) = \mathrm{Hom}_{\mathbf{Var}_k^\bullet}(X, E).$$

As elliptic curves are abelian varieties, $h_E(X)$ is an abelian group, and h_E is in fact a representable functor to the category of abelian groups. In particular, we have

$$\mathrm{Nat}_{\mathrm{Fun}(\mathbf{Var}_k^\bullet, \mathbf{Sets})}(h_{E_1}, h_{E_2}) \simeq \mathrm{Nat}_{\mathrm{Fun}(\mathbf{Var}_k^\bullet, \mathbf{AbGrps})}(h_{E_1}, h_{E_2}).$$

Notice that the abelian group structure on this set is clearly definable point-wise. This pulls back to an abelian group structure on $\mathrm{Hom}(E_1, E_2)$.

In the special case where E_1 and E_2 coincide, $\mathrm{Hom}(E, E) = \mathrm{End}(E)$ is a ring with multiplication given by composition. If we restrict to isomorphisms, we have the automorphism group $\mathrm{Aut}(E)$.

Moreover, notice that for any elliptic curve E over k, there is a natural homomorphism $\mathrm{Gal}(\overline{k}/k) \to \mathrm{Aut}(E_L)$ for any Galois extension L/k. Let $\sigma \in \mathrm{Gal}(\overline{k}/k)$, set $\sigma_L = \sigma|_L$ and $\mathrm{Spec}(\sigma_L) : \mathrm{Spec}(L) \to \mathrm{Spec}(L)$ the induced map of affine schemes, and

$$\sigma_{E,L} = \mathrm{id}_E \times_k \mathrm{Spec}((\sigma_L)^{-1})$$

the map $E_L \to E_L$. One can easily check that the map $\sigma \mapsto \sigma_{E,L}$ defines a homomorphism $\mathrm{Gal}(\overline{k}/k) \to \mathrm{Aut}(E_L)$. This homomorphism gives a natural action of $\mathrm{Gal}(\overline{k}/k)$ on $\mathrm{Hom}(E_{1,L}, E_{2,L})$.

Let E_1 and E_2 be two elliptic curves over k, $\sigma \in \mathrm{Gal}(\overline{k}/k)$, $f \in \mathrm{Hom}(E_{1,L}, E_{2,L})$, and L/k a Galois extension. We have a natural action of $\mathrm{Gal}(\overline{k}/k)$ on $\mathrm{Hom}(E_{1,L}, E_{2,L})$ by

$$\sigma(f) = \sigma_{E_2,L} \circ f \circ \sigma_{E_1,L}^{-1}.$$

Diagrammatically, one has the following.

$$\begin{tikzcd}
E_{1,L} \arrow[r, "\sigma_{E_1,L}^{-1}"] \arrow[d, "\sigma(f)"'] & E_{1,L} \arrow[d, "f"] \\
E_{2,L} \arrow[r, "\sigma_{E_2,L}^{-1}"] \arrow[d] & E_{2,L} \arrow[d] \\
\mathrm{Spec}(L) \arrow[r, "\sigma_L^{-1}"'] & \mathrm{Spec}(L)
\end{tikzcd}$$

For an algebraic extension L/k, we say that an isogeny $E_{1,\overline{k}} \to E_{2,\overline{k}}$ is defined over L if it is fixed by the action of $\mathrm{Gal}(\overline{k}/L)$ and denote the set of isogenies over L to be $\mathrm{Hom}_L(E_1, E_2)$. In other words, we have

$$\mathrm{Hom}_L(E_1, E_2) = \mathrm{Hom}(E_{1,\overline{k}}, E_{2,\overline{k}})^{\mathrm{Gal}(\overline{k}/L)}$$

and similarly for $\mathrm{End}_L(E)$ and $\mathrm{Aut}_L(E)$. One can check that

$$\mathrm{Hom}_L(E_1, E_2) \simeq \mathrm{Hom}(E_{1,L}, E_{2,L}).$$

Indeed, via base change, it suffices to show that

$$\operatorname{Hom}_k(E_1, E_2) \simeq \operatorname{Hom}(E_1, E_2).$$

For proof, consider the following diagram of pullback squares.

$$\begin{tikzcd}
E_{1,\overline{k}} \arrow[r, "\sigma_{E_1}^{-1}"] \arrow[d, "\sigma(f)"'] & E_{1,\overline{k}} \arrow[r] \arrow[d, "f"] & E_1 \arrow[d, "g"] \\
E_{2,\overline{k}} \arrow[r, "\sigma_{E_2}^{-1}"] \arrow[d] & E_{2,\overline{k}} \arrow[r] \arrow[d] & E_2 \arrow[d] \\
\operatorname{Spec}(\overline{k}) \arrow[r, "\sigma^{-1}"'] & \operatorname{Spec}(\overline{k}) \arrow[r] & \operatorname{Spec}(k)
\end{tikzcd}$$

Given $g \in \operatorname{Hom}(E_1, E_2)$, we see that the induced isogeny $f : E_{1,\overline{k}} \to E_{1,\overline{k}}$ is fixed by $\operatorname{Gal}(\overline{k}/k)$ because $\sigma_{E_1}^{-1}$ is invertible so by the universal property of pullback squares, the structure map $E_{1,\overline{k}} \to E_1$ is invariant under composition by $\sigma_{E_1}^{-1}$, and so $\sigma(f) = f$ by universal property as all the other maps are obviously the same.

This shows that $\operatorname{Hom}_L(E_1, E_2)$ is also an abelian group. Moreover, this shows that it suffices to study $\operatorname{Hom}(E_1, E_2)$.

Notice that the group law gives a natural family of isogenies. Let E be an elliptic curve over k and m be a natural number, we denote $[m] \in \operatorname{End}(E)$ the morphism given by m copies of the identity morphism of E added together under the group structure of $\operatorname{End}(E)$ as we have established before. One can show that $\operatorname{Hom}(E_1, E_2)$ is torsion-free. To do so, we first recall the following definition.

Definition 2.6. Let $f : X \to Y$ be a finite surjective morphism of k-varieties. The degree of f is $\deg(f) = [k(X) : f^*(k(Y))]$.

For the case of isogenies of elliptic curves, one can show that they are all finite surjective morphisms, and the notion of degree is well-defined. Further, a morphism between elliptic curves has degree zero if and only if the map is the constant map that maps the source to O. One property of $[m]$ is that it is nonconstant. In particular, $\operatorname{Hom}(E_1, E_2)$ is torsion-free by the multiplicativity of degree. As $\operatorname{End}(E)$ is torsion-free, one sees that $\mathbb{Z}$ embeds into $\operatorname{End}(E)$. For proof of the above facts, see [4, Chapter III]. It turns out that for most elliptic curves, $\operatorname{End}(E) = \mathbb{Z}$, which leads to the following definition.

Definition 2.7. An elliptic curve E over k is said to have complex multiplication or CM if $\operatorname{End}(E) \neq \mathbb{Z}$.

We will see that elliptic curves with CM enjoy various nice properties.

2.2. **The Tate Module.**

Now we proceed to an important construction of elliptic curves, the Tate module.

Definition 2.8. Let E be an elliptic curve over k. The kernel of $[m]$ is called the m-torsion points of E and is denoted $E[m]$.

The m-torsion points of E is a finite group scheme. For our purposes, we need only consider the $\overline{k}$-valued points of $E[m]$. As the functor of points is a Hom functor, it is left exact and thus commutes with kernels. In particular, $E[m](\overline{k}) = E(\overline{k})[m]$, where $E(\overline{k})[m]$ is the kernel of the induced map on $E(\overline{k})$ by $[m]$. The structure of the group $E(\overline{k})[m]$ is well-known.

Proposition 2.9. *Given an elliptic curve (E, O) over k a field and $m \in \mathbb{Z}$. If $\mathrm{char}(k) = 0$ or $0 < p = \mathrm{char}(k) \nmid m$, then $E(\overline{k})[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. If $\mathrm{char}(k) = p > 0$, then either $E[p^e] = \{O\}$ for all $e \geq 1$ or $E[p^e] = \mathbb{Z}/p^e\mathbb{Z}$ for all $e \geq 1$.*

Proof. See [4], page 86, Corollary 6.4. □

When $K = \mathbb{C}$, then E is isomorphic to the torus $\mathbb{C}/\Lambda$, and the above fact is obvious.

For a prime ℓ, notice that there is a natural projective system

$$\cdots \xrightarrow{[\ell]} E(\overline{k})[\ell^{n+1}] \xrightarrow{[\ell]} E(\overline{k})[\ell^n] \xrightarrow{[\ell]} \cdots .$$

Definition 2.10. Given ℓ prime, and E an elliptic curve over k, the ℓ-adic Tate module of E is the inverse limit

$$T_\ell(E) = \varprojlim E(\overline{k})[\ell^n].$$

Each $E(\overline{k})[\ell^n]$ is naturally a $\mathbb{Z}/\ell^n\mathbb{Z}$ module, upon taking limit of the projective system of diagrams, one obtains a natural $\mathbb{Z}_\ell$-module structure for $T_\ell(E)$. Being such, we have an induced topology on $T_\ell(E)$ with base $\{x + \ell^n T_\ell(E)\}_{x \in T_\ell(E)}$, that is equivalent to the limit topology. From the structure of the torsion points of $E(\overline{k})$, one obtains the following by taking limit.

Corollary 2.11. *Given an elliptic curve (E, O) over k a field and ℓ a prime. If $\mathrm{char}(k) = 0$ or $0 < p = \mathrm{char}(k) \neq \ell$, then $T_\ell(E) \simeq \mathbb{Z}_\ell \times \mathbb{Z}_\ell$. If $\mathrm{char}(k) = p > 0$, then either $T_p(E) = 0$ or $T_p(E) \simeq \mathbb{Z}_p$.*

The Tate module is of central importance in the study of Galois representations. We first show some applications to elliptic curves.

Let E_1 and E_2 be elliptic curves over k and $\phi : E_{1,\overline{k}} \to E_{2,\overline{k}}$ be an isogeny, then we know that it induces a group homomorphism on the level of closed points. In particular, ϕ maps m-torsion points to m-torsion points. By taking the limit, we have an induced map $\phi_\ell : T_\ell(E_1) \to T_\ell(E_2)$ of $\mathbb{Z}_\ell$-modules. We thus have a group homomorphism $\mathrm{Hom}_{\overline{k}}(E_1, E_2) \to \mathrm{Hom}(T_\ell(E_1), T_\ell(E_2))$ given by $\phi \mapsto \phi_\ell$. One can show that the map is injective. In fact, one can show something stronger.

Proposition 2.12. *Let E_1 and E_2 be elliptic curves over k, $\ell \neq \mathrm{char}(k)$ a prime, then*

$$\mathrm{Hom}_{\overline{k}}(E_1, E_2) \otimes \mathbb{Z}_\ell \to \mathrm{Hom}(T_\ell(E_1), T_\ell(E_2))$$

given by $\phi \otimes 1 \mapsto \phi_\ell$, is injective.

Proof. See [4], page 107, Theorem 7.4. □

Corollary 2.13. *Let E_1 and E_2 be elliptic curves over k. Then $\mathrm{Hom}_{\overline{k}}(E_1, E_2)$ is a free $\mathbb{Z}$-module of rank at most 4.*

Proof. One notes that $\mathrm{Hom}_{\overline{k}}(E_1, E_2)$ is torsion-free and $\mathbb{Z}$ is a PID, so to show that it is free, it suffices to show that it is finitely-generated. By the flatness of $\mathbb{Z}_\ell$ over $\mathbb{Z}$, it suffices to show that $\mathrm{Hom}_{\overline{k}}(E_1, E_2) \otimes \mathbb{Z}_\ell$ is finitely generated. By the above embedding, $\mathrm{Hom}_{\overline{k}}(E_1, E_2) \otimes \mathbb{Z}_\ell$ is a submodule of $\mathrm{Hom}(T_\ell(E_1), T_\ell(E_2))$. Since the Tate modules are free $\mathbb{Z}_\ell$-modules of rank 2, $\mathrm{Hom}(T_\ell(E_1), T_\ell(E_2))$ is a free $\mathbb{Z}_\ell$-module of rank 4. As $\mathbb{Z}_\ell$ is a PID, this shows that $\mathrm{Hom}_{\overline{k}}(E_1, E_2) \otimes \mathbb{Z}_\ell$ is a free finitely generated $\mathbb{Z}_\ell$-module, with $\mathbb{Z}_\ell$-rank less than or equal to 4. By the flatness of $\mathbb{Z}_\ell$ over $\mathbb{Z}$, the $\mathbb{Z}$-rank of $\mathrm{Hom}_{\overline{k}}(E_1, E_2)$ is the same as the $\mathbb{Z}_\ell$-rank of $\mathrm{Hom}_{\overline{k}}(E_1, E_2) \otimes \mathbb{Z}_\ell$, and we are done. □

Let E be an elliptic curve over k, L/k an algebraic extension, and ℓ a prime. For any $\sigma \in \mathrm{Gal}(\overline{k}/L) \subset \mathrm{Gal}(\overline{k}/k)$, we have a corresponding $\sigma_{E,\overline{k},\ell} \in \mathrm{Aut}_{\overline{k}}(E)$. As before, this gives a Galois action of $\mathrm{Gal}(\overline{k}/L)$ on $\mathrm{Hom}(T_\ell(E_1), T_\ell(E_2))$ given by

$$\sigma(f) = \sigma_{E_2,\overline{k},\ell} \circ f \circ \sigma^{-1}_{E_2,\overline{k},\ell}.$$

We define $\mathrm{Hom}_L(T_\ell(E_1), T_\ell(E_2))$ to be the $\mathbb{Z}_\ell$-linear maps between the Tate modules that are fixed by the Galois action of $G_{\overline{k}/L}$.

By restricting the source and target, one obtains the natural map

$$\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell \to \mathrm{Hom}_k(T_\ell(E_1), T_\ell(E_2)),$$

which is injective by the previous proposition. In fact, it is oftentimes an isomorphism.

Theorem 2.14 (Isogeny Theorem). *Let $\ell \neq \mathrm{char}(k)$ be prime and E_1 and E_2 be elliptic curves over k. Then the natural map*

$$\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell \to \mathrm{Hom}_k(T_\ell(E_1), T_\ell(E_2))$$

is an isomorphism if k is finite or a number field.

The above theorem is highly nontrivial, and we will omit the proof. For a historical note, the finite field case is proven by Tate in [5] and the number field case is proven by Faltings in [6]. One should note that the theorem fails easily over other fields, for instance local fields.

2.3. **The Weil Pairing.** The Weil pairing is a natural pairing one can define on the m-torsion points on elliptic curves. We now construct it.

Let E be an elliptic curve over a field k and $P, Q \in E(\overline{k})[m]$. Consider the divisor

$$\sum_{n=1}^{m} (P + nQ) - (nQ).$$

It is clear that it has degree zero and the sum of the points with respect to the group law on E is O, so it is a principal divisor of some $f \in \overline{k}(E)$. Set $\tau_Q : E(\overline{k}) \to E(\overline{k})$ to be given by $R \mapsto R + Q$ under the group law. Then $f \circ \tau_Q \in \overline{k}(E)$. Moreover,

$$(f \circ \tau_Q) = \sum_{n=1}^{m} (P + (n+1)Q) - ((n+1)Q) = (f)$$

since $P, Q \in E(\overline{k})[m]$. Hence, $e_m(P, Q) = f \circ \tau_Q / f$ is a constant. Repeating this argument, one has $(f \circ \tau_Q / f)^m = f \circ \tau_Q^m / f = 1$, so we have $e_m : E[m] \times E[m] \to \mu_m$. Moreover, one can show that it is Galois-invariant. That is, for some $\sigma \in G_{\overline{K}/K}$, $\sigma(e_m(P, Q)) = e_m(\sigma(P), \sigma(Q))$. In addition, one can show that it is nondegenerate antisymmetric, and bilinear. By those properties, we can easily check that the following is a compatible projective system.

$$\begin{tikzcd}
\cdots \arrow[r] & E(\overline{k})[\ell^{n+1}] \times E(\overline{k})[\ell^{n+1}] \arrow[r, "{[\ell]\times[\ell]}"] \arrow[d, "e_{\ell^{n+1}}"] & E(\overline{k})[\ell^{n}] \times E(\overline{k})[\ell^{n}] \arrow[r] \arrow[d, "e_{\ell^{n+1}}"] & \cdots . \\
\cdots \arrow[r] & \mu_{\ell^{n+1}} \arrow[r] & \mu_{\ell^{n}} \arrow[r] & \cdots
\end{tikzcd}$$

Therefore, we may take a limit and obtain the ℓ-adic Weil pairing $e : T_\ell(E) \times T_\ell(E) \to \mathbb{Z}_\ell$.

2.4. **Galois Representations and Elliptic Curves.** Now we are ready to discuss in detail how Galois representations arise naturally from elliptic curves. As mentioned before, one does this by considering the torsion points on the elliptic curve. Let us first consider the following motivating example.

Example 2.15. Consider the multiplicative group scheme $\mathbb{G}_m = \operatorname{Spec} \mathbb{Q}[t, t^{-1}]$ over $\mathbb{Q}$. Denote by $\mathbb{G}_m(\overline{\mathbb{Q}})$ the $\overline{\mathbb{Q}}$-valued points of $\mathbb{G}_m$. Notice that one can interpret the mod n cyclotomic character as being induced by the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the group of $\overline{\mathbb{Q}}$-points of order dividing n, which we call the n-torsion points and denote as $\mathbb{G}_m(\overline{\mathbb{Q}})[n]$. One can also note that as a curve, $\mathbb{G}_m$ has genus 0 and is isomorphic to the non-singular part of the nodal elliptic curve cut out by

$$Y^2Z = X^3 + X^2Z,$$

which implies that somehow $\mathbb{G}_m$ is “almost” an elliptic curve. This is a strong hint that we should consider the same approach for getting Galois representations from elliptic curves.

Let E be an elliptic curve over a field k and $P \in E(\overline{k})[m]$, σ an element of $\mathrm{Gal}(\overline{k}/k)$, and $\mathrm{char}(k) = p \nmid m$. Notice that we have $[m](\sigma(P)) = \sigma([m]P) = O$ as $[m]$ is defined over k. In particular, $\mathrm{Gal}(\overline{k}/k)$ acts on $E(\overline{k})[m]$. This gives a Galois representation $\mathrm{Gal}(\overline{k}/k) \to \mathrm{Aut}(E(\overline{k})[m]) \simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ upon choosing a basis for $E(\overline{k})[m]$. This is known as the mod m representation associated to the elliptic curve E.

As is with the cyclotomic characters, we can now let $\ell \neq p$ be a prime and take the limit over the projective system

$$\begin{tikzcd}
\cdots \arrow[r, "{[\ell]}"] & E(\overline{k})[\ell^{n+1}] \arrow[r, "{[\ell]}"] & E(\overline{k})[\ell^{n}] \arrow[r, "{[\ell]}"] & \cdots .
\end{tikzcd}$$

and obtain the ℓ-adic representation $\rho_{E,\ell} : \mathrm{Gal}(\overline{k}/k) \to \mathrm{Aut}(T_\ell(E)) \simeq \mathrm{GL}_2(\mathbb{Z}_\ell)$ of $\mathrm{Gal}(\overline{k}/k)$ with respect to E. If we further compose with the natural embedding $\mathrm{Aut}(T_l(E)) \mapsto \mathrm{Aut}(T_l(E)) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \simeq \mathrm{Aut}(V_\ell(E))$, where $V_\ell(E) \simeq T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, we obtain a representation $\mathrm{Gal}(\overline{k}/k) \to \mathrm{GL}_2(\mathbb{Q}_l)$, which we also denote by $\rho_{E,\ell}$ by abuse of notation.

We have seen previously that the 1-dimensional Galois representations coming from studying the torsion points of $\mathbb{G}_m$, i.e., the cyclotomic characters, are always surjective. This is not true for 2-dimensional representations coming from elliptic curves, and we will see counterexamples when we have more tools. For the special case where k is a number field and E is an elliptic curve without CM, one has the following.

Theorem 2.16. *Let k be a number field and E and elliptic curve over k without complex multiplication. Then $\mathrm{im}(\rho_{E,\ell})$ has finite index in $\mathrm{Aut}(T_\ell(E))$ for all $\ell \neq \mathrm{char}(k)$ and $\mathrm{im}(\rho_{E,\ell}) = \mathrm{Aut}(T_\ell(E))$ for almost all ℓ.*

Proof. See [7]. □

We are nowhere near giving a sketch of the above theorem. Instead, we will try to explain more about how one may compute images of Galois representations. For simplicity, we only consider mod m representations.

We start with an explicit method. Let E be an elliptic curve over $\mathbb{Q}$. Notice that the image of any Galois representation must be the Galois group of some Galois extension k of $\mathbb{Q}$. The kernel must then be $\mathrm{Gal}(\overline{\mathbb{Q}}/k)$, whose elements must fix $E(\overline{\mathbb{Q}})[m]$. If one chooses an embedding of E in $\mathbb{P}^2_{\mathbb{Q}}$ by Riemann-Roch, say $E \cap \mathbb{A}^2_{\mathbb{Q}}$ is cut out by

$$Y^2 = X^3 + aX + b,$$

where $a, b \in \mathbb{Q}$, one may identify elements of $E(\overline{\mathbb{Q}})[m]$ with certain points in $\overline{\mathbb{Q}}^2$ along with the point at infinity. Under this identification, the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E(\overline{\mathbb{Q}})[m]$ is just coordinate-wise application, i.e., $\sigma((x, y)) = (\sigma(x), \sigma(y))$ for $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and $(x, y) \in \overline{\mathbb{Q}}^2$. In particular, k must be the normal closure of $\mathbb{Q}$ adjoined with the coordinates of the non-identity elements of $E(\overline{\mathbb{Q}})[m]$ (as O is a $\mathbb{Q}$-point by definition), which we denote as $\mathbb{Q}(E(\overline{\mathbb{Q}})[m])$. It turns out that k is exactly equal to $\mathbb{Q}(E(\overline{\mathbb{Q}})[m])$ because $\mathbb{Q}(E(\overline{\mathbb{Q}})[m])/\mathbb{Q}$ is Galois, due to the following analog of cyclotomic polynomials.

Definition 2.17. Let a, b be free variables. The division polynomials associated to (a, b) are defined recursively as follows:

$$\begin{aligned}
&\psi_0 = 0,\\
&\psi_1 = 1,\\
&\psi_2 = 2Y,\\
&\psi_3 = 3X^4 + 6aX^2 + 12bX - a^2,\\
&\psi_4 = 4Y(X^6 + 5aX^4 + 20bX^3 - 5a^2X^2 - 4abX - 8b^2 - a^3),\\
&\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{m-1}\psi_{m+1}^3 \text{ for } n \geq 2,\\
&\psi_{2n} = \left(\frac{\psi_n}{2Y}\right) \cdot (\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \text{ for } n \geq 3.
\end{aligned}$$

We call ψ_m the m-division polynomial associated to (a, b).

The division polynomials are analogs of the cyclotomic polynomials because for an elliptic curve over $\mathbb{Q}$ with Weierstrass equation $Y^2 = X^3 + aX + b$, the elements of $E(\overline{\mathbb{Q}})[m]$, besides from O, are exactly the solutions of ψ_m associated to (a, b) and the Weierstrass equation. In general, one has $\psi_{2n+1} \in \mathbb{Z}[X, a, b]$ and $\psi_{2n} \in 2Y\mathbb{Z}[X, a, b]$, and it is easily seen that $\mathbb{Q}(E(\overline{\mathbb{Q}})[m])/\mathbb{Q}$ is Galois. Therefore, to compute the image of a mod m Galois representation associated to an elliptic curve over $\mathbb{Q}$, it suffices to find the Galois group of $\mathbb{Q}(E(\overline{\mathbb{Q}})[m])/\mathbb{Q}$, which is the splitting field of certain polynomials. Hence, we may reduce the problem of finding images of Galois representations to finding Galois groups of splitting fields. However, this method does not always work as well as we want because it is quite hard to find splitting fields in general and our division polynomials are defined recursively, making it even harder. To establish a general theory, one can study the distribution of the traces and determinants of the Frobenius elements.

We first recall some definitions.

Definition 2.18. Let $K/\mathbb{Q}$ be a Galois extension and $\mathcal{O}_K$ denote its ring of integers and $\mathfrak{p} \subset \mathcal{O}_K$ a nonzero prime ideal above $(p) \subset \mathbb{Z}$ for some prime number p. A Frobenius element at $\mathfrak{p}$ is an element $\varphi_{\mathfrak{p}} \in \mathrm{Gal}(K/\mathbb{Q})$ such that

$$\varphi_{\mathfrak{p}}(a) \equiv a^p \bmod \mathfrak{p}$$

for all $a \in \mathcal{O}_K$.

Notice that the above definition also works for $K = \overline{\mathbb{Q}}$. A Frobenius element of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is called an absolute Frobenius and (up to conjugation and inertia) will be denoted as Frob_p is it is over $\mathfrak{p}$ and $(p) = \mathfrak{p} \cap \mathbb{Z}$. In fact, any Frobenius element of $\mathrm{Gal}(K/\mathbb{Q})$ for some finite Galois extension $K/\mathbb{Q}$ is the restriction of some Frobenius element of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to K. The Chebotarev density theorem roughly says that for a finite Galois extension $K/\mathbb{Q}$, every element of $\mathrm{Gal}(K/\mathbb{Q})$ is a Frobenius element for (infinitely many) primes of K. In particular, for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and finite Galois $K/\mathbb{Q}$, one can always find a Frobenius element $\varphi_{\mathfrak{p}} \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $\sigma|_K = \varphi_{\mathfrak{p}}|_K$. In other words, we have the following.

Theorem 2.19. *The set of Frobenius elements in* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *is dense in* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

As Galois representations are continuous, the above theorem says that the values of $\rho_{E,\ell}$ on Frobenius elements completely determine the Galois representation. To this end, the following proposition comes in handy.

Theorem 2.20. *Let E be an elliptic curve over $\mathbb{Q}$, p a prime of good reduction for E. Then for any $\ell \neq p$,*

$$\det(\rho_{E,\ell}(\mathrm{Frob}_p)) = p \quad \textit{and} \quad \mathrm{tr}(\rho_{E,\ell}(\mathrm{Frob}_p)) = p + 1 - \#E(\mathbb{F}_p),$$

where $\#E(\mathbb{F}_p)$ denotes the number of $\mathbb{F}_p$-points of E.

Proof. See [4]. □

Remark 2.21. Notice that the determinant and trace of images of Frobenii would be the same regardless of the chosen ℓ. This tells us a lot of information about the Galois representation.

2.5. **Elliptic Curves over Local Fields.** In this section, we give a sketch of the basic theory of elliptic curves over local fields. We refer the reader to [4, Chapter VII] for a detailed exposition. Throughout, K is a local field, R its valuation ring, $\mathfrak{m}$ is the maximal ideal, π is a uniformizer, k is the residue field, and v is the additive valuation, normalized so that $v(\pi) = 1$.

One operation we would like to perform on an elliptic curve E over a local field K is to reduce modulo the unique maximal ideal of the valuation ring R, or a uniformizer π. However, it does not a priori make sense as the defining Weierstrass equation may have coefficients not in R. Fortunately, one can always clear denominators to make the Weierstrass equation have coefficients in R. One has to caution, however, that if we multiply by a power of π too high, the equation becomes zero after reduction, which is undesirable. We thus choose the equation such that the coefficients lie in R and the discriminant has minimal valuation. This is the *minimal Weierstrass equation* of E. One checks that the equation is unique up to change of coordinates over R.

Definition 2.22. Let E be an elliptic curve over local field K, then its reduction modulo π is the projective plane curve $\tilde{E}$ over k defined by a minimal Weierstrass equation for E with coefficients reduced modulo π.

To give a cleaner construction, one can first construct a Néron model E_R for E, which is "the best" approximation of E as a R-scheme. The reduction is then $E_R \times_R k$.

Notice that the reduced curve may fail to be an elliptic curve because it may fail to be nonsingular. The K-points of E get mapped to k-points of $\tilde{E}$. If we assume that $\tilde{E}$ is nonsingular, then the reduction $E(\overline{K})[m] \to \tilde{E}(\overline{k})$ is in fact injective for m relatively prime to the residue characteristic. We now use the Galois action on E to formulate this into a necessary and sufficient condition for when $\tilde{E}$ is nonsingular.

Definition 2.23. Let E be an elliptic curve over K and $\tilde{E}$ be its reduction. We set $\tilde{E}_{\text{ns}}(\overline{k})$ to be the set (group) of nonsingular geometric points of $\tilde{E}$ over k and $E_0(\overline{K})$ its preimage under reduction. We also denote $E_1(\overline{K})$ the kernel of the reduction $E_0(\overline{K}) \to \tilde{E}_{\text{ns}}(\overline{k})$.

We have the following exact sequence

$$0 \to E_1(\overline{K}) \to E_0(\overline{K}) \to \tilde{E}_{\text{ns}}(\overline{k}) \to 0.$$

Some important facts to note are that $E_0(K)$ always has finite index in $E(\overline{K})$ and $E_1(\overline{K})$ is torsion-free.

Definition 2.24. Let K^{nr} be the maximal unramified extension of K and $I_v = \text{Gal}(\overline{K}/K^{\text{nr}})$ be the inertia subgroup.

Definition 2.25. Let S be a $\text{Gal}(\overline{K}/K)$-set, then S is unramified if the action of I_v on S is trivial.

In the case where L is a global field. Let v be a finite place. Then we may extend the above definition. As $\text{Gal}(\overline{L_v}/L_v) \subset \text{Gal}(\overline{L}/L)$, any $\text{Gal}(\overline{L}/L)$-set is a $\text{Gal}(\overline{L_v}/L_v)$-set, and we say that a $\text{Gal}(\overline{L}/L)$-set is unramified at v if the inertia subgroup I_v of $\text{Gal}(\overline{L_v}/L_v)$ acts trivially on the set.

We have seen before that $\text{Gal}(\overline{K}/K)$ acts on the torsion points and the Tate module of elliptic curves, which allows us to use our language to formulate the following.

Proposition 2.26. *Let E be an elliptic curve over K whose reduction is nonsingular over k. Then for m relatively prime to* $\text{char}(k)$*, $E(\overline{K})[m]$ is unramified.*

Proof. We know that $E(\overline{K})[m]$ is finite, so by adjoining the coordinates of $E(\overline{K})[m]$, one has a finite extension K'/K such that $E(\overline{K})[m] \subset E(K')$. Set the residue field of K' to be k' and the valuation on K' to be v'. Since the reduction $\tilde{E}$ of E is nonsingular, one must be able to choose a Weierstrass equation for E such that the discriminant Δ is coprime to π, or $v(\Delta) = 0$. By basic properties of extension of local fields, $v'(\Delta) = 0$. In particular, $\tilde{E}$ is nonsingular over k'. We then have the reduction map $E(\overline{K'})[m] = E(\overline{K})[m] \to \tilde{E}(k')$ is injective. Let $\sigma \in I_v$, then σ acts trivially on $\tilde{E}(k')$, so for $P \in E(\overline{K})[m]$, the reduction of $\sigma(P) - P$ is the reduction of O. By the injectivity of reduction, we have $\sigma(P) = P$, so $E(\overline{K})[m]$ is unramified as desired. □

Corollary 2.27. *Let ℓ be a prime not equal to* $\text{char}(k)$*. Then $T_\ell(E)$ is unramified.*

Proof. One simply applies the previous proposition to ℓ^n and takes a limit. □

The above two conditions are in fact both equivalent to E having nonsingular reduction. This fact will be established shortly and is part of what is known as the Néron-Ogg-Shafarevich criterion.

Definition 2.28. Let E be an elliptic curve over K and $\tilde{E}$ its reduction. We say that E has good reduction if $\tilde{E}$ is nonsingular over k. Otherwise, E has bad reduction. If E has bad reduction, we say that E has multiplicative reduction if $\tilde{E}$ has a node, and E has additive reduction if $\tilde{E}$ has a cusp.

Moreover, in the case that E has good reduction, $\tilde{E}$ is an elliptic curve over a field of characteristic p, and so $\tilde{E}(\overline{k})[p] \simeq \mathbb{Z}/p\mathbb{Z}$ or $\tilde{E}(\overline{k})[p] \simeq 0$. We say that E has ordinary reduction in the first case and supersingular reduction in the second.

Proposition 2.29. *Let E be an elliptic curve over K with a fixed minimal Weierstrass equation. Then*

(1) E has good reduction if and only if the discriminant has valuation equal to 0.

(2) E has multiplicative reduction if and only if $v(\Delta) > 0$ and $v(c_4) = 0$. In this case, $\tilde{E}_{\mathrm{ns}}(\overline{k}) \simeq \overline{k}^{\times}$.

(3) E has additive reduction if and only if $v(\Delta) = 0$ and $v(c_4) > 0$. In this case, $\tilde{E}_{\mathrm{ns}} \simeq \overline{k}$.

Proof. The part that does not concern the group structure of $\tilde{E}_{\mathrm{ns}}(k)$ is immediate. For the group structure, one can construct explicit isomorphisms between the two groups, which can be found in [4, Chapter VII.5], Proposition 5.1. □

Now we can prove the Néron-Ogg-Shafarevich criterion.

Theorem 2.30 (The Néron-Ogg-Shafarevich Criterion)**.** *Let E be an elliptic curve over K. Then the following are equivalent.*

(a) E has good reduction over K.

(b) $E(\overline{K})[m]$ is unramified for all $m \geq 1$ relatively prime to char(k).

(c) The Tate module $T_\ell(E)$ is unramified for some prime $\ell \neq$ char(k).

(d) $E(\overline{K})[m]$ is unramified for infinitely many $m \geq 1$ relatively prime to char(k).

Proof. By our previous work, we have already established $(a) \Rightarrow (b) \Rightarrow (c)$. Note that (c) implies (d) since $T_\ell(E)$ is unramified if and only if $E(\overline{K})[\ell^n]$ is unramified for all n, and that's infinitely many numbers.

Now we proceed to show that $(d) \Rightarrow (a)$. By the fact that $E(\overline{K})/E_0(\overline{K})$ is finite and (d), we may pick integer m relatively prime to the residue characteristic and larger than $|E(K^{\mathrm{nr}})/E_0(K^{\mathrm{nr}})|$ such that $E(\overline{K})[m]$ is unramified. In particular, this implies that $E(\overline{K})[m] \subset E(K^{\mathrm{nr}})$. We know that $E(\overline{K})[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$, so $E(K^{\mathrm{nr}})$ contains a subgroup isomorphic to $(\mathbb{Z}/m\mathbb{Z})^2$. By assumption, $|E(K^{\mathrm{nr}})/E_0(K^{\mathrm{nr}})| < m$, so $E_0(K^{\mathrm{nr}})$ contains a subgroup of $E(\overline{K})[m]$ of index less than m. In particular, it must contain a subgroup of form $(\mathbb{Z}/\ell\mathbb{Z})^2$, where $\ell \mid m$ so is prime to char(k). Now we consider the exact sequence

$$0 \to E_1(K^{\mathrm{nr}}) \to E_0(K^{\mathrm{nr}}) \to \tilde{E}_{\mathrm{ns}}(\overline{k}) \to 0.$$

We know that $E_1(K^{\mathrm{nr}})$ is torsion-free, so $\tilde{E}_{\mathrm{ns}}(\overline{k})$ must contain a subgroup isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2$. We know the structure of the group $\tilde{E}_{\mathrm{ns}(\overline{k})}$ when E has bad reduction. In particular, if E has additive reduction, then $\tilde{E}_{\mathrm{ns}(\overline{k})}$ is torsion-free, and so cannot contain $(\mathbb{Z}/\ell\mathbb{Z})^2$. If E has multiplicative reduction, then the ℓ-torsion points of $\tilde{E}_{\mathrm{ns}(\overline{k})}$ are the ℓ^{th} roots of unities, and can't contain $(\mathbb{Z}/\ell\mathbb{Z})^2$. Hence, E must have good reduction over K, as desired. □

Notice that any elliptic curve over $\mathbb{Q}$ may be viewed as one over $\mathbb{Q}_p$, and we say that an elliptic curve over $\mathbb{Q}$ has good (resp. multiplicative, additive) reduction over a prime p if it has good reduction over $\mathbb{Q}_p$. Hence, we have a Néron-Ogg-Shafarevich criterion over $\mathbb{Q}$.

Theorem 2.31 (The Néron-Ogg-Shafarevich Criterion over $\mathbb{Q}$)**.** *Let E be an elliptic curve over $\mathbb{Q}$. Then the following are equivalent.*
(a) E has good reduction at prime p.
(b) $E[m]$ is unramified for all $p \nmid m$.
(c) The Tate module $T_\ell(E)$ is unramified for some (in fact, all) prime $\ell \neq p$.
(d) $E[m]$ is unramified for infinitely many $p \nmid m$.

Now we note that this helps make sense of Theorem 2.19. As the absolute Frobenius Frob_p is well-defined up to conjugation and inertia, it doesn't make sense a priori to consider the quantities $\det(\rho_{E,\ell}(\mathrm{Frob}_p))$ and $\mathrm{tr}(\rho_{E,\ell}(\mathrm{Frob}_p))$. However, by the Néron-Ogg-Shafarevich criterion, the inertia group at p is contained in the kernel of $\rho_{E,\ell}$ because E has good reduction at p. Moreover, both the trace and determinant are conjugacy invariant, so the two quantities indeed make sense.

3. Example: Image of mod 3 Galois Representation from Elliptic Curves

To illustrate the theory we've described in the previous sections, we now consider an example.

Let E be an elliptic curve over K, then we know that the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ acts on the m-torsion points $E(\overline{K})[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ of E, which gives a mod m Galois representation

$$\overline{\rho}_{E,m} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

In this section, we will try to derive some facts about the image of $\overline{\rho}_{E,3}$, with the intended goal being the classification of mod 3 Galois representations.

Theorem 3.1. *Let E be an elliptic curve over a number field K of characteristic zero and Δ its discriminant. Then the image of $\overline{\rho}_{E,3}$ is contained in a Sylow 2-subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ if and only if $x^3 - \Delta = 0$ has a root in K.*

Proof. By our assumption on the characteristic of K, via a change of coordinates, we may assume that E is defined by

$$Y^2 = X^3 + aX + b.$$

The 3-torsion points of E are those whose X-coordinates satisfy the third division polynomial

$$\psi_3(X,Y) = 3X^4 + 6aX^2 + 12bX - a^2.$$

In particular, besides O, there will be a total of eight 3-torsion points, which may be grouped into 4 doubles based on their x-coordinates (the y-coordinates would be inverses of each other). Let the four different x-coordinates be x_1, x_2, x_3, x_4 respectively. By Galois theory, there exists an element $\tau \in \mathrm{Gal}(\overline{K}/K)$ that fixes x_i

and swaps the two y-coordinates corresponding to each x_i. Notice that $\mathrm{Gal}(\overline{K}/K)$ acts on the set $\{x_1, x_2, x_3, x_4\}$, which induces a homomorphism $f : \mathrm{Gal}(\overline{K}/K) \to S_4$. By the parametrization we have chosen, the inverse of $(x, y) \in E(\overline{K})$ under the group law is $(x, -y)$. In particular, $\overline{\rho}_{E,3}(\tau) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. One can also obtain a homomorphism $g : \mathrm{GL}_2(\mathbb{F}_3) \to \mathrm{PGL}_2(\mathbb{F}_3)$. One can check that there is a choice of isomorphism $h : \mathrm{PGL}_2(\mathbb{F}_3) \simeq S_4$ such that $h \circ g = f$. Further, notice that S_4 also acts on the set $\{x_i x_j + x_k x_l\}$ consisting of $\frac{1}{2}\binom{4}{2} = 3$ elements. Hence, we have homomorphisms $S_4 \to S_3$ and $\mathrm{Gal}(\overline{K}/K) \to S_3$. Moreover, we have

Lemma 3.2. *For $\{i, j, k, l\} = \{1, 2, 3, 4\}$, $\Delta^{1/3} = 2a - 3(x_i x_j + x_k x_l)$, where different choices of $\{i, j, k, l\}$ gives different cube roots of Δ.*

Proof. One uses the symmetric polynomial relations of $\{x_1, x_2, x_3, x_4\}$ given by the coefficients of ψ_3 to expand

$$(y - x_1x_2 - x_3x_4)(y - x_1x_3 - x_2x_4)(y - x_1x_4 - x_2x_3) = (y - 2a/3)^3 - 64b^3/27 - 16a^2.$$

We can obtain the desired formula by setting the above to be 0 and solve for $x_i x_j + x_k x_l$. □

Finally, one can check that the action by $\mathrm{Gal}(\overline{K}/K)$ on the three cube roots of Δ coincides with the homomorphism $\mathrm{Gal}(\overline{K}/K)$ we obtained before by identifying the three roots of Δ with $\{x_i x_j + x_k x_l\}$. But since $\Delta^{1/3} \in K$ for one of the cube roots, $\mathrm{Gal}(\overline{K}/K)$ fixes that cube root, so the action is not transitive. Notice that any 3-cycles in S_4 gets sent to a 3-cycle in S_3, so the image of $\overline{\rho}_{E,3}$ does not contain an element of order divisible by 3. On the other hand, if we trace our argument, it is clear that if $\Delta^{1/3} \notin K$, it would lie in the splitting field and thus the image would contain an element of order divisible by 3. In other words, as $\mathrm{GL}_2(\mathbb{F}_3)$ has order 48, the image of $\overline{\rho}_{E,3}$ lies in a Sylow 2-subgroup if and only if $\Delta^{1/3} \in K$. □

A natural next step is to consider images of subgroups of $\mathrm{Gal}(\overline{K}/K)$ under $\overline{\rho}_{E,3}$. In particular, we may consider the decomposition group $\mathrm{Gal}(\overline{K_v}/K_v)$ at a place v of K above 3. We can acquire information about the image of this group under some good circumstances. One way we can narrow down the size of subgroups of general linear groups is to look if they are contained in a Borel subgroup.

Definition 3.3. Let R be a ring. Then a Borel subgroup of $\mathrm{GL}_2(R)$ is any conjugate of the group of upper-triangular matrices in $\mathrm{GL}_2(R)$.

It turns out that under two types of nice conditions, the image of $\mathrm{Gal}(\overline{K_v}/K_v)$ under $\overline{\rho}_{E,3}$ is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$. We now show the first case.

Proposition 3.4. *Let E be an elliptic curve of good ordinary reduction over a local field K with* $\mathrm{char}(K) = 0$ *and residue field k with* $\mathrm{char}(k) = p$. *Then the image of the corresponding Galois representation is contained in a Borel subgroup of* $\mathrm{GL}_2(\mathbb{F}_p)$.

Proof. Notice that it suffices to demonstrate that there exists a nontrivial proper subgroup of $E(\overline{K})[p]$ that is stable under the Galois action. This is because we would then have a cyclic group of order p, and we may pick a generator, complete it to become a basis of $E(\overline{K})[p]$, and the corresponding representation must be upper-triangular. Notice that the kernel of the induced reduction map $E(\overline{K})[p] \to \tilde{E}(\overline{k})[p]$ is exactly such a group. As E has good ordinary reduction, $\tilde{E}(\overline{k})[p] \simeq \mathbb{Z}/p\mathbb{Z}$, so the kernel must have order p, and is a nontrivial proper subgroup of $E(\overline{K})[p]$. Moreover, the kernel is Galois-stable because the reduction map commutes with the Galois action. □

The next case is when E has split multiplicative reduction over v. This case is resolved by a construction called the Tate curve.

Recall that for an archimedean complete discrete valuation field L, such as $\mathbb{C}$ or $\mathbb{R}$, the geometric points of an elliptic curve E over L is isomorphic to the group $\mathbb{C}/\Lambda$ for some lattice $\Lambda = \langle 1, \lambda \rangle$. Through exponentiating, the group is further isomophic to $\mathbb{C}^\times/q^\mathbb{Z}$ for $q = e^{i2\pi\lambda}$, where $0 < |q| < 1$. It turns out that for a nonarchimedean local field K, one can start with such a q and produce an elliptic curve E over K with $E(\overline{K}) \simeq \overline{K}^\times/q^\mathbb{Z}$ as Galois modules. This construction is called the Tate curve.

The structure of the p-torsion group of a Tate curve is especially simple to describe, as we must have $E(\overline{K})[p] \simeq \langle \zeta_p, q^{1/p} \rangle$, where $\zeta_p \in \overline{K}$ is a primitive p^{th} root of unity. Moreover, the subgroup generated by ζ_p is Galois-stable for obvious reasons. Hence, the image of the mod p Galois representation associated to E would lie in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$.

The following theorem tells us when an elliptic curve over a local field K is a Tate curve.

Proposition 3.5. *Let E be an elliptic curve over a local field K of split multiplicative reduction. Then there exists a unique $q \in K^\times$ with $|q| < 1$ such that $E(\overline{K}) \simeq \overline{K}^\times/q^\mathbb{Z}$ as groups.*

Proof. See [8]. □

In particular, if E has split multiplicative reduction over v, its image is also contained in a Borel subgroup. Notice that the above gives examples of Galois representations that are not surjective that we alluded to before.

Acknowledgments

It is a pleasure to thank my mentor, Jinyue Luo, who provided me with numerous excellent resources for me to understand the material, as well as great explanations. I would also like to thank Professor Peter May, who organized the REU program and provided me with an opportunity to interact with my extremely talented peers. Finally, I thank Ruiyou Xia for her invaluable emotional support.

References

[1] J. S. Milne, *Elliptic Curves*, BookSurge Publishers 2006.

[2] J. -M. Fontaine and B. Mazur, Geometric Galois representations, in "Elliptic curves, modular forms and Fermat's last theorem", *International Press* 1995.

[3] C. Khare and J. -P. Wintenberger, Serre's modularity conjecture (I), *Invent. Math.* 178 (2009), 485-504.

[4] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd Edition, Springer Science+Business Media, 2008.

[5] J. Tate, Endomorphisms of abelian varieties over finite fields, *Invent. Math.* 2 (1966), 134–144.

[6] G. Faltings. Endlichkeitssatze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* 73(3)(1983), 349–366.

[7] J.-P. Serre. *Abelian l-adic representations and elliptic curves*, volume 7 of Research Notes in Mathematics. A K Peters Ltd., Wellesley, MA, 1998. With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original.

[8] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics. Vol. 151, Springer-Verlag, 1994.