GALOIS ACTIONS ON TORSIONS OF ELLIPTIC CURVES

TARIKA MANE

Abstract. Our first focus is proving that field extensions of $\mathbb{Q}$ generated by torsion points of elliptic curves are Galois over $\mathbb{Q}$. To do so, we study the structure torsion points and finite extensions of $\mathbb{Q}$. We then analyze their Galois groups through representations and prove the representation is a one-to-one group homomorphism between the Galois group and the general linear group $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.

Contents

1. Introduction

Our goal is to prove that extension generated by coordinates of torsion points on a rational elliptic curve is Galois over $\mathbb{Q}$, and outline a method for computing the representation. We begin by examining the algebraic structure of the complex points on the elliptic curve $E(\mathbb{C})$. We define a group law on $E(\mathbb{C})$ and layout an isomorphism between $E(\mathbb{C})$ and a complex torus, to obtain torsion groups.

The focus then diverges to general theory of number fields that are Galois over $\mathbb{Q}$. We examine splitting fields, cyclotomic fields, and the Fundamental Theorem of Galois theory. We converge on the relationship between Galois extensions of $\mathbb{Q}$ and elliptic curves by looking at the interactions between the automorphisms of the Galois group and E. We are then able to prove that the field generated by n-torsion point coordinates is Galois over $\mathbb{Q}$.

We conclude with studying the Galois groups of these extensions by computing the representation. We further show that the representation is a one-to-one group homomorphism from the Galois group to the general linear group of 2×2 invertible matrices with coefficients in $\mathbb{Z}/n\mathbb{Z}$.

Date: August 25th, 2020.

Here, we begin by defining an elliptic curve, and looking at its structure in the projective plane:

Definition 1.1 (Elliptic Curve)**.** An *elliptic curve* E over some field F, where $\text{char}F \neq 2$, is a smooth, projective, non-singular algebraic curve of genus 1. It is given by the homogenous equation

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3 \tag{1.2}$$

with $a, b, c \in F$.

If $F = \mathbb{Q}$ then E is a *rational elliptic curve.* All elliptic curves considered in this paper are rational.

Any projective point $(X\colon Y\colon Z) \in \mathbb{P}^2$ can be associated with the point $(X/Z, Y/Z)$ in the affine plane $\mathbb{A}^2$. If $Z = 0$ then $(X\colon Y\colon 0)$ can be associated with $(X\colon Y)$ in the projective line $\mathbb{P}^1$. Then we can view E as the affine curve

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

along with points at infinity. The affine curve is similarly non-singular, i.e. $f(x)$ has distinct roots.

The points at infinity in (1.2) occur when $Z = 0$. Setting $Z = 0$ gives one point at infinity, namely $\mathcal{O} = (0\colon 1\colon 0)$, and is considered to be the point where all vertical lines meet in the xy-plane. A line connecting a point $P \in \mathbb{A}^2$ to $\mathcal{O}$ is then the vertical line through P. Details about projective geometry are in Appendix A of [2].

Definition 1.3. Let $E\colon y^2 = f(x) = x^3 + ax^2 + bx + c$ be a rational elliptic curve. The set of K-rational points for a field K, denoted as $E(K)$, is

$$\{(x, y) \in F \times F \mid y^2 = f(x)\}.$$

2. The Elliptic Group Law

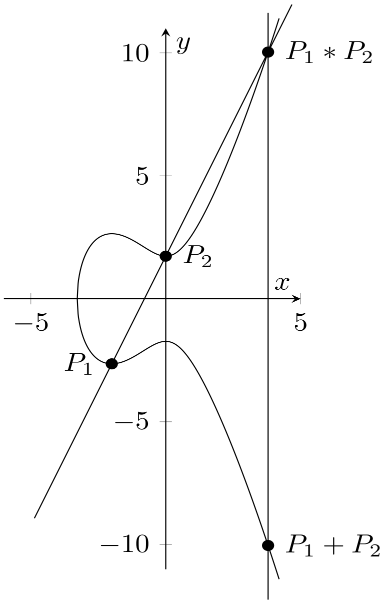
A crucial fact about rational elliptic curves is that the complex points $E(\mathbb{C})$ are, algebraically, an abelian group. To obtain a group structure, we first need that a line passing through two points on E intersects the curve at a third point.

Theorem 2.1 (Bézout's Theorem [2, Theorem A.2])**.** *Two projective curves C_1 and C_2 of degree m and n respectively intersect a total of mn times.*

Since E is degree 3 and the line l connecting two distinct points P_1 and P_2 on E has degree 1, l intersects the curve at a third point by Bézout's Theorem. This point is denoted as $P_1 * P_2$. The set $E(\mathbb{C})$ can then be made into a group with the following operation:

Definition 2.2 (Group Law)**.** Let E be a rational elliptic curve and take P_1 and P_2 on E. The map $+\colon E(\mathbb{C}) \times E(\mathbb{C}) \to E(\mathbb{C})$ is defined as follows: Consider the point $P_1 * P_2$,. The line connecting $\mathcal{O}$ and $P_1 * P_2$ intersects E at another point $\mathcal{O} * (P_1 * P_2) = P_3$. Then $P_1 + P_2$ is P_3.

Remark 2.3. If $P_1 = P_2$ then take the tangent line through P_1. The tangent line is considered to intersect the curve twice at P_1 and a third time at a $P_1 * P_1$.



The Group Law.

Theorem 2.4 ([2, Pgs. 12-15])**.** *Let E be a rational elliptic curve. Then $(E(\mathbb{C}), +)$ is an abelian group, with group operation $+$ from Definition 2.2, and $\mathcal{O}$ as the identity.*

Proof. For commutativity, take $P_1, P_2 \in E(\mathbb{C})$. Since the line connecting P_1 to P_2 is the same as the line connecting P_2 to P_1, they yield the same third intersection point.

To show $\mathcal{O}$ is the identity, join P_1 to $\mathcal{O}$, and take the third intersection point, $P_1 * \mathcal{O}$. This line intersects the curve at $\mathcal{O}, P_1$, and $P_1 * \mathcal{O}$. So, connecting $P_1 * \mathcal{O}$ to $\mathcal{O}$ and then taking the third intersection point yields P_1. Thus, $\mathcal{O}$ is the identity. Furthermore, $(P * \mathcal{O}) + P = \mathcal{O}$, so there exists an inverse $-P = P * \mathcal{O}$.

For associativity, details can be found in Chapter 1 of [2]. □

3. Torsion Points

With a group law now defined over $E(\mathbb{C})$, we can construct methods to find torsion points. We start with 2-torsion points and compute higher torsions by defining an isomorphism between $E(\mathbb{C})$ and a complex torus.

Definition 3.1. For $m \in \mathbb{N}$, a point P has order m if $m \cdot P = \mathcal{O}$ and $m' \cdot P \neq \mathcal{O}$ for all $1 \leq m' \leq m$. If such an m exists then P has order m. If the order of P divides $n \in \mathbb{N}$ then P is an n-torsion point.

3.1. **Points of Order 2.**

Let $E\colon y^2 = f(x) = x^3 + ax^2 + bx + c$ be a rational elliptic curve. The points of order two are unique because their x-coordinates are exactly the roots of $f(x)$.

Each point of order 2 satisfies $2P = \mathcal{O}$, or rather, $P = -P$. By Theorem 2.4, if $P = (x, y)$ then $-P = (x, -y)$ so $y = -y$, implying that $y = 0$. By definition, an elliptic curve is non-singular so $f(x)$ has three distinct (complex) roots, $\alpha_1, \alpha_2, \alpha_3$. Including $\mathcal{O}$, the set of points of order 2 is $\{\mathcal{O}, P_1, P_2, P_3\}$ where $P_i = (\alpha_i, 0)$.

Example 3.2. Let $p \in \mathbb{N}$ be prime and consider the curve $E : y^2 = x^3 - p$. Let ζ_3 be a primitive cube root of unity and $\beta = \sqrt[3]{p}$. Then

$$\{\text{roots of } x^3 - p\} = \{\beta, \zeta_3\beta, \zeta_3^2\beta\}.$$

The points of order 2 are

$$\{\mathcal{O}, (\beta, 0), (\zeta_3\beta, 0), (\zeta_3^2\beta, 0)\}.$$

The points of order 2 are therefore quite nice, as they come from the roots of f. For higher order torsion groups, there is a method to compute them, outlined in the next subsection.

3.2. **An Elliptic Curve as a Complex Torus.**

Points of higher order (than 2) can be difficult to compute via the group law. By converting $E(\mathbb{C})$ into a quotient group of $\mathbb{C}$ modulo a lattice $\mathcal{L}$, finding the group of n-torsion points becomes more efficient. Many results are stated without proof and computational details can be found in Chapter 6 of [3].

Definition 3.3. A *lattice* $\mathcal{L}$ is an additive subgroup of $\mathbb{C}$ generated by two $\mathbb{R}$-linearly independent periods ω_1 and ω_2 :

$$\mathcal{L} = \{\omega_1\mathbb{Z} + \omega_2\mathbb{Z}\}.$$

The quotient group $\mathbb{C}/\mathcal{L}$ for some lattice $\mathcal{L}$ is topologically a torus and forms an abelian group. The group law is defined by complex addition modulo the periods of $\mathcal{L}$. Each point in $\mathbb{C}/\mathcal{L}$ can be mapped to a point in $E(\mathbb{C})$. To create a mapping, we need a Weierstrass $\wp$-function.

Definition 3.4 (Weierstrass $\wp$-function)**.** Let $\mathcal{L} \subset \mathbb{C}$ be a lattice. Then the *Weierstrass $\wp$-function* relative to $\mathcal{L}$ is

$$\wp(u, \mathcal{L}) = \frac{1}{u^2} + \sum_{\substack{\omega \in \mathcal{L} \\ \omega \neq 0}} \left(\frac{1}{(u-\omega)^2} - \frac{1}{\omega^2} \right).$$

With the use of the $\wp$-function, and it's derivative, we are able to define a map between $\mathbb{C}$ and $E(\mathbb{C})$.

Theorem 3.5 ([3, Corollary 5.1.1])**.** *For a rational elliptic curve E, $\mathbb{R}$-linearly independent periods ω_1 and ω_2 can be chosen to define the lattice $\mathcal{L}$ such that for each $u \in \mathbb{C}$, the point $P(u) = (\wp(u, \mathcal{L}), \wp'(u, \mathcal{L}))$ is on E. If $u \in \mathcal{L}$ then $P(u) = \mathcal{O}$.*

The function $\wp(u, \mathcal{L})$ is doubly periodic: $\wp(u + \omega_1, \mathcal{L}) = \wp(u, \mathcal{L})$ and $\wp(u + \omega_2, \mathcal{L}) = \wp(u, \mathcal{L})$ for all $u \in \mathbb{C}$. Thus, $\wp(u + \omega, \mathcal{L}) = \wp(u, \mathcal{L})$ for all $\omega \in \mathcal{L}$. For $u, v \in \mathbb{C}$ where $u - v \in \mathcal{L}$, $P(u) = P(v)$. Therefore, P descends to a well-defined map $\mathbb{C}/\mathcal{L} \to E(\mathbb{C})$. This map turns out to be a bijection.

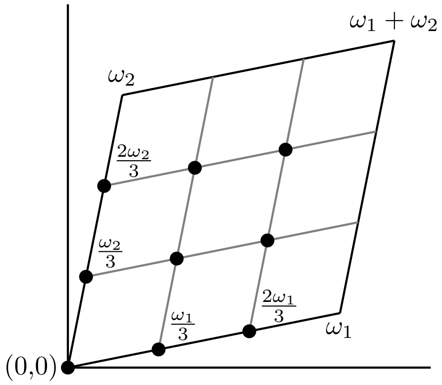
Theorem 3.6 ([3, Corollary 5.1.1])**.** *Let E be a rational elliptic curve and $\mathcal{L}$ be a lattice associated with E from Theorem 3.5. The map $u \mapsto P(u)$, where $P(u) = (\wp(u, \mathcal{L}), \wp'(u, \mathcal{L}))$, from $\mathbb{C}/\mathcal{L} \to E(\mathbb{C})$ is a group isomorphism.*

It follows that the map $u \mapsto P(u)$ from $\mathbb{C} \to E(\mathbb{C})$ is a group homomorphism so

$$P(u + v) = P(u) + P(v).$$

The kernel of this homomorphism is the lattice $\mathcal{L}$, and the quotient group of the complex u-plane modulo $\mathcal{L}$ is isomorphic to the group $E(\mathbb{C})$. Thus, for any $u \in \mathbb{C}/\mathcal{L}$ where $mu \in \mathcal{L}$, $P(u)$ is an m-torsion point. So the set of m-torsion points is

$$\left\{ \frac{a\omega_1 + b\omega_2}{m} \mid a, b \in \mathbb{Z}/m\mathbb{Z} \right\}.$$



The Group of Points of Order Dividing Three.

The group of n-torsion points in $E(\mathbb{C})$ is also the direct sum of two cyclic groups of order n, an important result for Section 6.

Theorem 3.7 ([3, Proposition 5.4])**.** *Let E be a rational elliptic curve and let $E[n]$ denote the n-torsion points in $E(\mathbb{C})$. Then, $E[n] \cong (\mathbb{Z}/n\mathbb{Z}) \oplus (\mathbb{Z}/n\mathbb{Z})$.*

Proof. First, by Theorem 3.6, $E(\mathbb{C})$ is isomorphic to $\mathbb{C}/\mathcal{L}$ for some lattice $\mathcal{L}$ with periods ω_1 and ω_2. The point $P(u)$ for some $u \in \mathbb{C}/\mathcal{L}$ is in $E[n]$ if and only if $nu \in \mathcal{L}$. Thus,

$$(a_1, a_2) \mapsto P\left(\frac{a_1}{n}\omega_1 + \frac{a_2}{n}\omega_2\right)$$

with P from Theorem 3.5, is an isomorphism from $(\mathbb{Z}/n\mathbb{Z}) \oplus (\mathbb{Z}/n\mathbb{Z})$ to $E[n]$.

This map is surjective because each $Q \in E[n]$ is produced by some $u \in \mathbb{C}/L$ where $nu \in L$. So $u = \dfrac{\alpha\omega_1 + \beta\omega_2}{n}$ for some $\alpha, \beta \in \mathbb{Z}/n\mathbb{Z}$ and corresponds to the pair $(\alpha, \beta) \in (\mathbb{Z}/n\mathbb{Z}) \oplus (\mathbb{Z}/n\mathbb{Z})$. This map is also injective: since P is an isomorphism, if $P\left(\frac{a_1}{n}\omega_1 + \frac{a_2}{n}\omega_2\right) = P\left(\frac{a_3}{n}\omega_1 + \frac{a_4}{n}\omega_2\right)$ then $\frac{a_1}{n}\omega_1 + \frac{a_2}{n}\omega_2 \equiv \frac{a_3}{n}\omega_1 + \frac{a_4}{n}\omega_2 \mod \mathcal{L}$. Then, because ω_1 and ω_2 are $\mathbb{R}$-linearly independent, $(a_1, a_2) \equiv (a_3, a_4) \mod \mathcal{L}$. □

A method for calculating ω_1 and ω_2 is described in Chapter 6 of [3], and can be quickly approximated by computer algorithms. All computer calculations in this paper are done via SageMath. Once such periods are found, the set of n-torsion points $E[n]$ can be computed.

Example 3.8. Consider the curve $E\colon y^2 = f(x) = x^3 - 9x + 9$. The associated lattice $\mathcal{L}$ is generated by the periods $\omega_1 \approx 1.931$ and $\omega_2 \approx -i1.391$. This yields

$$\wp(u, \mathcal{L}) = u^{-2} - \frac{9}{5}u^2 - \frac{9}{7}u^4 + \frac{27}{25}u^6 + O(u^8).$$

So $P(\omega_1/3, \mathcal{L})$ gives the 3-torsion point $(3, 3)$. For each $(a_1, a_2) \in (\mathbb{Z}/n\mathbb{Z}) \oplus (\mathbb{Z}/n\mathbb{Z})$, the point $P(\frac{a_1}{n}\omega_1 + \frac{a_2}{n}\omega_2)$ has order dividing n.

4. Finite Field Extensions of $\mathbb{Q}$

We have constructed a method towards finding torsion points, which often have non-rational coordinates. We can generate interesting field extensions of $\mathbb{Q}$ using these coordinates. However, to understand the extensions they produce, we break away from elliptic curves and examine how to obtain number fields that are Galois over $\mathbb{Q}$.

A field K, with $\mathbb{Q} \subset K \subset \mathbb{C}$, can be viewed as a vector space over $\mathbb{Q}$. The degree of K over $\mathbb{Q}$ is the dimension of K as a vector space over $\mathbb{Q}$, denoted as $[K\colon \mathbb{Q}]$.

Definition 4.1 (Number field)**.** A field extension K, of $\mathbb{Q}$, is a *number field* if $[K\colon \mathbb{Q}]$ is finite.

A simple extension of $\mathbb{Q}$ is created through adjoining an algebraic number, α, to get the field extension $\mathbb{Q}(\alpha)$. A number field can always be thought of as a simple extension of $\mathbb{Q}$.

Lemma 4.2 ([1, Ch. 31 Theorem 2])**.** *Let K be a number field. Then there exists an algebraic number α such that $K = \mathbb{Q}(\alpha)$.*

The set of field homomorphisms $\sigma\colon K \to \mathbb{C}$ provides useful insight into number fields. By definition, $\sigma(1) = 1$, so $\sigma(q) = q$ for all $q \in \mathbb{Q}$, so $\mathbb{Q}$ is fixed by σ. So if $f \in \mathbb{Q}[x]$ and $\gamma \in K$ is a root of f then $\sigma(f(\gamma)) = f(\sigma(\gamma)) = 0$. Thus, $\sigma(\gamma)$ is also a root of f. If $K = \mathbb{Q}(\alpha_1, \cdots, \alpha_n)$ then σ is determined by where it maps $\alpha_1, \cdots, \alpha_n$.

Theorem 4.3. *Let K be a number field. Then the number of field homomorphisms $\sigma\colon K \to \mathbb{C}$ is $[K\colon \mathbb{Q}]$.*

Proof. By Lemma 4.2, $K = \mathbb{Q}(\alpha)$ for some algebraic number α. Consider a map $\sigma\colon K \to \mathbb{C}$ with $\sigma(q) = q$ for all $q \in \mathbb{Q}$, $\sigma(\beta_1\beta_2) = \sigma(\beta_1)\sigma(\beta_2)$ and $\sigma(\beta_1 + \beta_2) = \sigma(\beta_1) + \sigma(\beta_2)$ for all $\beta_1, \beta_2 \in K$. Since K as a vector-space over $\mathbb{Q}$ has the basis $\{1, \alpha, \cdots, \alpha^{n-1}\}$, σ is determined by its mapping of α. If f is the minimal polynomial of α over $\mathbb{Q}$ (i.e. the monic polynomial that has the lowest degree in $\mathbb{Q}[x]$ with α as a root), then f has degree $[K\colon \mathbb{Q}] = n$. So

$$f = (x - \alpha_1) \cdots (x - \alpha_n).$$

Also, $\sigma(f(\alpha)) = f(\sigma(\alpha))$, so $\sigma(\alpha)$ must be a root of f.

There are at least n maps of this form, $\sigma_1, \cdots, \sigma_n$, where $\sigma_i(\alpha) = \alpha_i$. All field homomorphisms from K to $\mathbb{C}$ must map α to some α_i: if σ does not map α to some root of f, then $\sigma(f(\alpha)) \neq f(\sigma(\alpha))$.

Next, if $\sigma_i(\alpha) = \alpha_i$ and $\sigma_j(\alpha) = \alpha_i$ then $\sigma_i = \sigma_j$: for all $\gamma \in K$, γ is a rational linear combination of $\{1, \alpha, \cdots, \alpha^{n-1}\}$ so $\sigma_i(\gamma) = \sigma_j(\gamma)$. Thus, there are exactly n field homomorphisms from $K \to \mathbb{C}$, each determined by sending α to some α_i. □

It may also hold that a field homomorphism $\sigma\colon K \to \mathbb{C}$ has image $\sigma(K) = K$. Then σ is an automorphism of K. This gives rise to our definition of a Galois extension:

Definition 4.4 (Galois Extension)**.** A number field K is a *Galois extension* of $\mathbb{Q}$ if each homomorphism $\sigma\colon K \to \mathbb{C}$ is an automorphism, so the image $\sigma(K) = K$.

Remark 4.5. If a number field K is a Galois extension of $\mathbb{Q}$, then it is a finite Galois extension of $\mathbb{Q}$. However, there are Galois extensions of $\mathbb{Q}$ which are infinite and will not be discussed.

Let $\mathrm{Aut}(K)$ denote the set of automorphisms of K, which is a group with the following operation: if $\sigma, \tau \in \mathrm{Aut}(K)$ then $(\sigma\tau)(a) = (\sigma(\tau(a))$. If K is a Galois extension of $\mathbb{Q}$, then this group is called the *Galois group of $K/\mathbb{Q}$* and is denoted as $\mathrm{Gal}(K/\mathbb{Q})$.

To find number fields that are Galois over $\mathbb{Q}$, we look at fields generated by roots of polynomials.

Definition 4.6 (Splitting Field)**.** Let F be a field and take a polynomial $f \in F[x]$. Then a field extension K of F is the *splitting field* for f if f splits into linear factors in $K[x]$ and does not completely split into linear factors over any proper subfield of K containing F.

Theorem 4.7. *Let F be a field with $charF = 0$. Take an irreducible polynomial $f \in F[x]$ and let K be the splitting field over F for f. Then $|\mathrm{Aut}(K)| = [K\colon F]$.*

Proof. See Chapter 32 of [1]. The proof is similar to that in Theorem 4.3, where the automorphisms are determined by exchanging roots of minimum polynomial. □

Corollary 4.8. *The splitting field K over $\mathbb{Q}$ for an irreducible polynomial $f \in \mathbb{Q}[x]$ is a Galois extension of $\mathbb{Q}$.*

Proof. By Theorem 4.3, the number of field homomorphisms from $K \to \mathbb{C}$ is equal to $[K\colon \mathbb{Q}]$. Each automorphism is a homomorphism, and by Theorem 4.7, $|\mathrm{Aut}(K)| = [K\colon \mathbb{Q}]$. So each field homomorphism is an automorphism of K, implying K is a Galois extension of $\mathbb{Q}$. □

So a number field K that is the splitting field of some $f \in \mathbb{Q}[x]$ is a Galois Extenion of $\mathbb{Q}$. For each element $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ and root α_i of f, $\sigma(\alpha_i)$ must also be a root of f, so σ induces a permutation on the α_i's.

Example 4.9 (Cyclotomic Fields)**.** A nice example of Galois extensions of $\mathbb{Q}$ arises by considering the splitting field of

$$1 - x^n.$$

Factoring this, with $\zeta = e^{2\pi i/n}$ as the primitive n^{th} root of unity, yields

$$1 - x^n = (1-x)(1-\zeta x)(1-\zeta^2 x)\cdots(1-\zeta^{n-1}x).$$

The field $\mathbb{Q}(\zeta)$ contains all powers of ζ, so it is the splitting field of $1 - x^n$. The field $\mathbb{Q}(\zeta)$ is called a *cyclotomic field.* Thus, $\mathbb{Q}(\zeta)$ is a Galois extension of $\mathbb{Q}$. For any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, $\sigma(\zeta)$ is a primitive n^{th} root of unity. Each primitive n^{th} root of unity is of the form ζ^t where $t \in (\mathbb{Z}/n\mathbb{Z})^*$. There is then a group isomorphism

$$t : \mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^*.$$

It is defined as

$$\sigma(\zeta) = \zeta^{t(\sigma)} \text{ for } \sigma \in \mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}).$$

Details are in Chapter 6 of [2].

Since $(\mathbb{Z}/n\mathbb{Z})^*$ is an abelian group, so is $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, which makes $\mathbb{Q}(\zeta)$ a useful field to study. We can describe subextensions of a cyclotomic field, $\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta)$ through the Fundamental Theorem of Galois theory and the relationship between the Galois groups.

Theorem 4.10 (Fundamental Theorem of Galois Theory [1, Chapter 32])**.** *If L is a finite Galois extension of $\mathbb{Q}$, there is a one-to-one correspondence between the intermediate fields $\mathbb{Q} \subset K \subset L$, and the subgroups of the Galois group,* $\mathrm{Gal}(L/\mathbb{Q})$. *The subgroup H corresponds to the subfield $K = L^H$ that is fixed by the automorphisms in H. The normal subgroups of* $\mathrm{Gal}(L/\mathbb{Q})$ *specifically correspond to subfields K which are Galois over $\mathbb{Q}$.*

A subextension of a cyclotomic field K, is Galois over $\mathbb{Q}$ if and only if $\mathrm{Gal}(\mathbb{Q}(\zeta)/K)$ is a normal subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Since $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is abelian, $\mathrm{Gal}(\mathbb{Q}(\zeta)/K)$ must be a normal subgroup. Thus, $K/\mathbb{Q}$ is Galois. The Galois group $\mathrm{Gal}(K/\mathbb{Q})$ can be described using the following theorem.

Theorem 4.11. *Suppose L and K are finite Galois Extensions of $\mathbb{Q}$, and K is a subfield of L. So $\mathbb{Q} \subset K \subset L$. Then there exists an isomorphism*

$$\frac{\mathrm{Gal}(L/\mathbb{Q})}{\mathrm{Gal}(L/K)} \xrightarrow{\sim} \mathrm{Gal}(K/\mathbb{Q}).$$

Proof. See Chapter 32 in [1]. The important note is that $\mathrm{Gal}(L/\mathbb{Q})$ has some subgroup H which fixes K. Then $\mathrm{Gal}(L/K)$ is specifically H. By taking $\mathrm{Gal}(L/\mathbb{Q})$ modulo H, the remaining automorphisms keep $\mathbb{Q}$ fixed but not K. By restricting the domain from L to K, each $\sigma \in \dfrac{\mathrm{Gal}(L/\mathbb{Q})}{\mathrm{Gal}(L/K)}$ induces an automorphism on K. Thus, we obtain the automorphisms in $\mathrm{Gal}(K/\mathbb{Q})$ precisely from those in $\dfrac{\mathrm{Gal}(L/\mathbb{Q})}{\mathrm{Gal}(L/K)}$. □

So every subfield of a cyclotomic field is therefore a Galois extension of $\mathbb{Q}$ with an abelian Galois group. The Fundamental Theorem of Galois Theory and Theorem 4.11 are helpful when determining the Galois group of some Galois extension K over $\mathbb{Q}$, as seen in the following example.

Example 4.12. Consider the rational elliptic curve $y^2 = f(x) = x^3 - 3x + 1$. Let K be the splitting field of f.

Next, let $\zeta_9 = e^{\pm i2\pi/9}$ be a primitive ninth root of unity. We can show that K is a subfield of $\mathbb{Q}(\zeta_9)$. First,

$$x^9 - 1 = (x^3 - 1)(x^6 + x^3 + 1).$$

Then,

$$\{\text{roots of } x^6 + x^3 + 1\} = \{\zeta_9, \zeta_9^2, \zeta_9^4, \zeta_9^5, \zeta_9^7, \zeta_9^8\}.$$

The splitting field of $x^6 + x^3 + 1$ is then $\mathbb{Q}(\zeta_9)$. Further, if u is a root of $x^6 + x^3 + 1$ then $u + u^{-1}$ is a root of $x^3 - 3x + 1$. So, $\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta_9)$.

Next,

$$\mathrm{Gal}(\mathbb{Q}(\zeta_9)/\mathbb{Q}) \cong (\mathbb{Z}/9\mathbb{Z})^* \cong (\mathbb{Z}/6\mathbb{Z})$$

by the map t from Example 4.9, and since $(\mathbb{Z}/9\mathbb{Z})^* \cong (\mathbb{Z}/6\mathbb{Z})$. By the Fundamental Theorem of Galois Theory, $\mathrm{Gal}(\mathbb{Q}(\zeta_9)/K)$ must correspond to one of the subgroups of $(\mathbb{Z}/6\mathbb{Z})$.

We can denote $\mathrm{Gal}(\mathbb{Q}(\zeta_9)/\mathbb{Q})$ as $\{\sigma_1, \sigma_2, \sigma_4, \sigma_5, \sigma_7, \sigma_8\}$. Using the map t, where $\sigma(\zeta_9) \mapsto \zeta_9^{t(\sigma)}$, gives two subgroups: $\{\sigma_4, \sigma_7, \sigma_1\}$ and $\{\sigma_8, \sigma_1\}$. Then,

$$\begin{array}{rcl} \sigma_8(\zeta_9) & \mapsto & \zeta_9^8 \\ \sigma_8(\zeta_9^8) & \mapsto & \zeta_9. \end{array}$$

Thus, $\zeta_9 + \zeta_9^8 = \sigma_8(\zeta_9 + \zeta_9^8)$, meaning σ_8 fixes $\zeta_9 + \zeta_9^8$. Next, $\zeta_9 + \zeta_9^8$ is of the form $u + u^{-1}$ so $\mathrm{Gal}(\mathbb{Q}(\zeta_9)/K) \cong (\mathbb{Z}/2\mathbb{Z})$. Then

$$\frac{\mathrm{Gal}(\mathbb{Q}(\zeta_9)/\mathbb{Q}}{\mathrm{Gal}(\mathbb{Q}(\zeta_9)/K)} \cong \frac{(\mathbb{Z}/6\mathbb{Z})}{(\mathbb{Z}/2\mathbb{Z})} \cong (\mathbb{Z}/3\mathbb{Z}).$$

By Theorem 4.11, $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/3\mathbb{Z})$.

5. Elliptic Curves over Galois Extensions of $\mathbb{Q}$

We can continue the discussion of field extensions over $\mathbb{Q}$ by focusing on fields generated through the coordinates of n-torsion points on an elliptic curve. We begin be looking at elliptic curves over Galois extensions K of $\mathbb{Q}$.

For some $P \in E(K)$ and $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, let $\sigma(P)$ be the point $(\sigma(x), \sigma(y))$ and $\sigma(\mathcal{O}) = \mathcal{O}$. The interactions between σ and $E(K)$ are useful for proving these extensions are Galois over $\mathbb{Q}$ and for Section 6, where we examine their Galois groups. First, we want the point $\sigma(P)$ to still be contained in $E(K)$.

Proposition 5.1 ([2, Proposition 6.3])**.** *If E is an elliptic curve with rational coefficients and K is a field extension of $\mathbb{Q}$ then $E(K)$ is a subgroup of $E(\mathbb{C})$.*

Theorem 5.2 ([2, Proposition 6.3])**.** *If E is an elliptic curve with rational coefficients and K is a Galois extension of $\mathbb{Q}$ then*

(i) For all $P \in E(K)$ and $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, $\sigma(P) \in E(K)$.
(ii) The group Gal$(K/\mathbb{Q})$ acts on the abelian group $E(K)$.

Proof. For (i), take $P = (x, y) \in E(K)$. Since the coordinates of $\sigma(P)$ are in K, it only needs to be verified that $\sigma(P)$ is on E. First, σ fixes all $q \in \mathbb{Q}$, so

$$\begin{array}{rcl} \sigma(y^2 - x^3 - ax - b) & = & 0 \\ \sigma(y)^2 - \sigma(x)^3 - a\sigma(x) - b & = & 0 \end{array}$$

So then $\sigma(P) \in E(K)$.

For (ii) take $P \in E(K)$ and $\sigma, \tau \in \mathrm{Gal}(K/\mathbb{Q})$. Then

$$\begin{array}{rcl} (\sigma\tau)(P) & = & ((\sigma\tau)(x), (\sigma\tau)(y)) \\ & = & (\sigma(\tau(x)), \sigma(\tau(y)) \\ & = & \sigma(\tau(x), \tau(y)) \\ & = & \sigma(\tau(P)). \end{array}$$

Next, $e(P) = (e(x), e(y)) = (x, y) = P$, where e is the identity in $\mathrm{Gal}(K/\mathbb{Q})$. □

We also want σ to preserve the group structure and maintain the torsion points over $E(K)$.

Theorem 5.3 ([2, Proposition 6.3])**.** *Let E be an elliptic curve with rational coefficients and K be a Galois extension of $\mathbb{Q}$. Then*

(i) For all $P, Q \in E(K)$ and $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, $\sigma(P+Q) = \sigma(P) + \sigma(Q)$ and $\sigma(-P) = -\sigma(P)$. So, $\sigma(nP) = n(\sigma(P))$.

(ii) Let $P \in E(K)$ have order n. Then, for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, $\sigma(P)$ has order n.

Proof. For (i), see Chapter 6 in [2]. For (ii) Let $P \in E(K)$ have order n and let the order of $\sigma(P)$ be m. Then

$$n\sigma(P) = \sigma(nP) = \sigma(\mathcal{O}) = \mathcal{O}.$$

So, m divides n. Next,

$$\mathcal{O} = \sigma^{-1}(\mathcal{O}) = \sigma^{-1}(\sigma(mP)) = (\sigma^{-1}\sigma)(mP) = mP.$$

So n divides m. Thus, $n = m$. □

So for a Galois extension K of $\mathbb{Q}$, $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ induces a permutation on the n-torsion points. Consider the set $E[n] = \{P \in E(\mathbb{C}) \mid nP = \mathcal{O}\}$. Let $\mathbb{Q}(E[n])$ denote the field generated over $\mathbb{Q}$ by the coordinates of the points in $E[n]$. We can use the properties from Theorem 5.3 to prove such a field is Galois over $\mathbb{Q}$:

Theorem 5.4 ([2, Proposition 6.5])**.** *Let E be an elliptic curve with rational coefficients. For all $n \geq 2$,*

(i) Let $P = (x_p, y_p) \in E[n]$. Then x_p and y_p are algebraic over $\mathbb{Q}$.

(ii) Let $E[n] = \{P_1, \cdots, P_m, \mathcal{O}\}$ where $P_i = (x_i, y_i)$. Then $\mathbb{Q}(E[n]) = K$ is Galois over $\mathbb{Q}$.

Proof. For (i), details can be found in Chapter 6 of [2]. One proof is done by observing that each field homomorphism $\sigma \colon K \to \mathbb{C}$ is determined by a permutation on the P_i's in $E[n]$. This is because $\sigma(P_i) \in E[n]$, by the same logic in Theorem 5.3. So there is a finite number of homomorphisms. If there existed some x_i or y_i that was not algebraic over $\mathbb{Q}$ then K would have infinite degree over $\mathbb{Q}$, and therefore infinitely many homomorphisms to $\mathbb{C}$.

For (ii), let L be the Galois closure of K over $\mathbb{Q}$ i.e. the smallest field containing K that is Galois over $\mathbb{Q}$. Take $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$. Each P_i is in $E[n]$, so $\sigma(P_i) \in E[n]$ by Theorem 5.3. So $\sigma(P_i) = P_j$ for some $1 \leq j \leq m$. This holds for all $1 \leq i \leq m$. So by restricting the domain of σ to K, then $\sigma(K) \subset K$. Next, since σ induces a permutation on the (x_i, y_i)'s, then for each $\beta \in K$, $\sigma^{-1}(\beta)$ is some $\gamma \in K$. So $\beta = \sigma(\gamma)$ and $K \subset \sigma(K)$. All field homomorphisms from K to $\mathbb{C}$ are obtained by restricting the domain of each $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ to K. Then $\sigma(K) = K$ so each σ is an automorphism. Thus, K is Galois over $\mathbb{Q}$. □

We now know $\mathbb{Q}(E[n])$ is Galois over $\mathbb{Q}$ and how $\sigma \in \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ interacts with the points in $\mathbb{Q}(E[n])$ that are on E. Here we provide some examples of these fields:

Example 5.5. Looking at the curve $E : y^2 = x^3 + x$, the set of 2-torsion points is

$$\{\mathcal{O}, (0,0), (i,0), (-i,0)\}.$$

So the field generated by the coordinates of these points is $\mathbb{Q}(E[2]) = \mathbb{Q}(i)$. Then the Galois group contains two elements: $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) = \{e, \overline{\sigma}\}$ where e is the identity and $\overline{\sigma}$ is complex conjugation.

Example 5.6. For the curve $E\colon y^2 = f(x) = x^3 + 2x$, the points of order 4 are each P where $2P$ has order 2. So the y-coordinate of $2P$ must be 0. Through computation from the group law, the x-coordinates of these points satisfy

$$x^6 + 10x^4 - 20x^2 - 8 = 0. \tag{5.7}$$

Let $\alpha = (\sqrt{2} - 2)i$ and $\upsilon = (\sqrt{2} + 2)i$. Then (5.7) is

$$(x^2 - 2)(x^2 - \alpha^2)(x^2 - \upsilon^2) = 0.$$

Next,

$$f(\pm\sqrt{2}) = \pm 4\sqrt{2}, \quad f(\pm\alpha) = \pm(4\sqrt{2} - 4)\alpha, \quad f(\pm\upsilon) = \pm(-4\sqrt{2} - 4)\upsilon.$$

Since $E[4] \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, there are sixteen points total: $\mathcal{O}$, three 2-torsion points, and two points from each root of (5.7). The points of order 2 are

$$\{(0, 0), (i\sqrt{2}, 0), (-i\sqrt{2}, 0)\}.$$

The points of order 4 are

$$\{(\sqrt{2}, \pm 4\sqrt{2}), (-\sqrt{2}, \pm 4\sqrt{2}), (\alpha, f(\pm\alpha)), (-\alpha, f(\pm\alpha)), (\upsilon, f(\pm\upsilon)), (-\upsilon, f(\pm\upsilon))\}$$

Thus, $\mathbb{Q}(E[4]) = \mathbb{Q}(i, \sqrt{2})$.

6. Representations Given by Torsion

We now know $\mathbb{Q}(E[n])$ is Galois over $\mathbb{Q}$, and we have the tools to explicitly describe the Galois group. Each $\sigma \in \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ induces a permutation on the set $E[n]$. By Theorem 3.7, the set $E[n]$ is also the direct sum of two cyclic groups, each with order n. We can utilize these properties for describing the Galois group. In this section we analyze $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ through its representation.

Definition 6.1. A representation of a group G on a vector space V over a field K is a group homomorphism from G to the general linear group on V, denoted $\mathrm{GL}(V)$:

$$\rho\colon G \to \mathrm{GL}(V).$$

By Theorem 5.3, we have

$$\sigma(P + Q) = \sigma(P) + \sigma(Q), \quad \sigma(-P) = -\sigma(P), \quad \sigma(\mathcal{O}) = \mathcal{O}.$$

By viewing $E[n]$ as an abelian group, each $\sigma \in \mathrm{Gal}(\mathbb{Q}(E[n]/\mathbb{Q})$ is a group homomorphism from $E[n]$ to itself. Each σ also has an inverse so each σ is a group isomorphism from $E[n]$ to itself.

Since $E[n] \cong (\mathbb{Z}/n\mathbb{Z}) \oplus (\mathbb{Z}/n\mathbb{Z})$ by Theorem 3.7, two basis elements P_1, P_2 can be chosen to generate $E[n]$ over $\mathbb{Z}/n\mathbb{Z}$. Then,

$$E[n] = \{aP_1 + bP_2 \mid a, b \in \mathbb{Z}/n\mathbb{Z}\}.$$

Because σ is an isomorphism, then $\sigma(aP_1 + bP_2) = a\sigma(P_1) + b\sigma(P_2)$. So for all $P \in E[n]$, $\sigma(P)$ is determined by $\sigma(P_1)$ and $\sigma(P_2)$. Furthermore, $\sigma(P_1)$ and $\sigma(P_2)$ are some $(\mathbb{Z}/n\mathbb{Z})$-linear combination of P_1 and P_2 :

$$\begin{aligned} \sigma(P_1) &= \alpha_\sigma P_1 + \gamma_\sigma P_2, \\ \sigma(P_2) &= \beta_\sigma P_1 + \delta_\sigma P_2. \end{aligned}$$

So $\sigma(P_1)$ and $\sigma(P_2)$ can be expressed as the matrix product $\begin{pmatrix} P_1 & P_2 \end{pmatrix} \begin{pmatrix} \alpha_\sigma & \beta_\sigma \\ \gamma_\sigma & \delta_\sigma \end{pmatrix}$.

Since σ has an inverse, the matrix is invertible. Furthermore, every 2×2 invertible matrix defines an isomorphism from $E[n]$ to $E[n]$. We can therefore consider the general linear group of 2×2 invertible matrices with coefficients in $\mathbb{Z}/n\mathbb{Z}$, denoted as $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.

Definition 6.2 (Galois Representation)**.** Let E be a rational elliptic curve and fix P_1 and P_2 as the generators of $E[n]$. Then for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$, the constants $\alpha_\sigma, \beta_\sigma, \gamma_\sigma, \delta_\sigma$ are determined by

$$\sigma(P_1) = \alpha_\sigma P_1 + \gamma_\sigma P_2,$$

$$\sigma(P_2) = \beta_\sigma P_1 + \delta_\sigma P_2.$$

The map $\rho_n\colon \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is defined as

$$\rho_n(\sigma) = \begin{pmatrix} \alpha_\sigma & \beta_\sigma \\ \gamma_\sigma & \delta_\sigma \end{pmatrix}.$$

The map ρ_n is the *Galois representation* of $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$.

The representation allows us to understand $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ as a group of matrices. It both preserves the composition law through matrix multiplication and provides a one-to-one group homomorphism.

Theorem 6.3 ([2, Theorem 6.7])**.** *Let E be a rational elliptic curve and take $n \geq 2$. Fix P_1 and P_2 as generators for $E[n]$. Then the map ρ_n from Definition 6.2 is a one-to-one group homomorphism.*

Proof. To prove ρ_n is a group homomorphism, we need $\rho_n(\sigma\tau) = \rho_n(\sigma)\rho_n(\tau)$ for all $\sigma, \tau \in \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$. First,

$$\rho_n(\sigma)\rho_n(\tau) = \begin{pmatrix} \alpha_\sigma & \beta_\sigma \\ \gamma_\sigma & \delta_\sigma \end{pmatrix} \begin{pmatrix} \alpha_\tau & \beta_\tau \\ \gamma_\tau & \delta_\tau \end{pmatrix} = \begin{pmatrix} \alpha_\sigma\alpha_\tau + \beta_\sigma\gamma_\tau & \gamma_\sigma\alpha_\tau + \delta_\sigma\gamma_\tau \\ \alpha_\sigma\beta_\tau + \beta_\sigma\delta_\tau & \gamma_\sigma\beta_\tau + \delta_\sigma\delta_\tau \end{pmatrix}.$$

Next,

$$\begin{aligned} (\sigma\tau)(P_1) &= \sigma(\alpha_\tau P_1 + \gamma_\tau P_2) \\ &= \alpha_\tau\sigma(P_1) + \gamma_\tau\sigma(P_2) \\ &= \alpha_\tau(\alpha_\sigma P_1 + \gamma_\sigma P_2) + \gamma_\tau(\beta_\sigma P_1 + \delta_\sigma P_2) \\ &= (\alpha_\sigma\alpha_\tau + \beta_\sigma\gamma_\tau)P_1 + (\gamma_\sigma\alpha_\tau + \delta_\sigma\gamma_\tau)P_2. \end{aligned}$$

It can similarly be shown that $(\sigma\tau)(P_2) = (\alpha_\sigma\beta_\tau + \beta_\sigma\delta_\tau)(P_1) + (\gamma_\sigma\beta_\tau + \delta_\sigma\delta_\tau)(P_2)$. So $\rho_n(\sigma\tau) = \rho_n(\sigma)\rho_n(\tau)$.

Next, if $\ker(\rho_n) = \{e\}$ where e is the identity isomorphism from $E[n]$ to $E[n]$, then ρ_n is one-to-one. Take $\sigma \in \ker(\rho_n)$ so $\sigma(P_1) = P_1$ and $\sigma(P_2) = P_2$. Then $\sigma(P) = P$ for all $P \in E[n]$ since the generators are fixed. Next, $\sigma((x, y)) = (\sigma(x), \sigma(y))$ by definition, and $\mathbb{Q}(E[n])$ is generated by the coordinates of the points in $E[n]$. So, σ fixes x and y for all $P \in E[n]$ and therefore fixes the generators of $\mathbb{Q}(E[n])$. Thus, all of $\mathbb{Q}(E[n])$ is fixed by σ so σ must be e. So $\ker(\rho_n)$ has only the identity, proving that ρ_n is one-to-one. □

We can now examine Galois representations for various torsions by fixing generators and determining where each isomorphism maps them.

Example 6.4. Continuing with the curve $E\colon y^2 = x^3 + x$, the Galois extension of $\mathbb{Q}$ using the 2-torsion points has the Galois group $\{e, \overline{\sigma}\}$ from Example 5.5. The generators can be $P_1 = (0,0)$ and $P_2 = (i, 0)$. Then $e(P_1) = P_1$ and $e(P_2) = P_2$. So, $\rho_2(e) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, which is the identity matrix. Next,

$$\begin{aligned} \overline{\sigma}(P_1) = \overline{\sigma}(0,0) = (0,0) &= P_1 \\ \overline{\sigma}(P_2) = \overline{\sigma}(i,0) = (-i,0) &= P_1 + P_2. \end{aligned}$$

So, $\rho_2(\overline{\sigma}) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Example 6.5. Looking again at the curve $E\colon y^2 = x^3 - 3x + 1$ from Example 4.12, the Galois group $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/3\mathbb{Z})$. Let P_1, P_2, P_3 be the points of order 2. There are 3 isomorphisms in this group, one of them being the identity, and σ and τ where

$$\begin{aligned} \sigma(P_1) &= P_2 & \tau(P_1) &= P_3 \\ \sigma(P_2) &= P_3 & \tau(P_2) &= P_1 \\ \sigma(P_3) &= P_1 & \tau(P_3) &= P_2. \end{aligned}$$

Then the generators can be P_1 and P_2. First, $\rho_2(e) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Next, for $\rho_2(\sigma)$, $\sigma(P_1) = P_2$ and $\sigma(P_2) = P_3 = P_1 + P_2$. So $\rho_2(\sigma) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. Lastly, $\tau(P_1) = P_3 = P_1 + P_2$ and $\tau(P_2) = P_1$ so $\rho_2(\tau) = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$.

For a rational elliptic curve E, the Galois group $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})$ can also be S_3, the permutation group of 3 elements, as in the following example.

Example 6.6. Consider the curve $E : y^2 = x^3 - p$ from Example 3.2, with

$$E[2] = \{\mathcal{O}, (\beta, 0), (\zeta_3\beta, 0), (\zeta_3^2\beta, 0)\}.$$

So $\mathbb{Q}(E[2]) = \mathbb{Q}(\zeta_3, \beta)$. There are two isomorphisms σ and τ where

$$\begin{aligned} \sigma(\beta) &= \zeta_3\beta & \tau(\beta) &= \beta \\ \sigma(\zeta_3) &= \zeta_3 & \tau(\zeta_3) &= \zeta_3^2. \end{aligned}$$

The Galois group $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})$ is S_3, and can be described as $\{e, \sigma, \sigma^2, \sigma\tau, \sigma^2\tau, \tau\}$, where e is the identity. The generators can be $P_1 = (\beta, 0)$ and $P_2 = (\zeta\beta, 0)$. Then,

$$\begin{aligned} \sigma(P_1) = (\sigma(\beta), \sigma(0)) = (\zeta_3\beta, 0) &= P_2 \\ \sigma(P_2) = (\sigma(\zeta_3\beta), \sigma(0)) = (\zeta_3^2\beta, 0) &= P_1 + P_2. \end{aligned}$$

So, $\rho_2(\sigma) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. The matrix $\rho_2(\tau)$ can be found similarly, and is $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. From $\rho_2(\sigma)$ and $\rho_2(\tau)$, the rest of the representation can be found through matrix multiplication.

For higher torsions, the Galois group is more complicated to describe, especially since the representation is not always surjective onto $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Computations for determining the Galois group can be done with the aid of a computer algorithm.

Example 6.7. Consider the curve $E\colon y^2 = f(x) = x^3 - 9x + 9$. In Example 3.8, we found periods ω_1 and ω_2. Looking at the set $E[5]$, the generators can be $P_1 = P(\frac{\omega_1}{5})$ and $P_2 = P(\frac{\omega_2}{5})$, with the map P from Theorem 3.5.

Each $(a_1, a_2) \in (\mathbb{Z}/5\mathbb{Z}) \oplus (\mathbb{Z}/5\mathbb{Z})$ maps to the 5-torsion point

$$P\left(\frac{a_1}{n}\omega_1 + \frac{a_2}{n}\omega_2\right) = a_1P_1 + a_2P_2.$$

So each $\sigma \in \mathrm{Gal}(\mathbb{Q}(E[5])/\mathbb{Q})$ is described by where it sends $\dfrac{\omega_1}{5}$ and $\dfrac{\omega_2}{5}$. In this case,

$$\rho_5(\mathrm{Gal}(\mathbb{Q}(E[5])/\mathbb{Q})) \cong \mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z}).$$

However, if a curve has rational n-torsion points, then the representation cannot be surjective onto $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. The curve E has rational 3-torsion points and every matrix in $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ defines an isomorphism from $E[3]$ to itself [4]. So if an isomorphism moves a rational point in $E[3]$ then it cannot be in $\mathrm{Gal}(\mathbb{Q}(E[3])/\mathbb{Q})$). Thus,

$$\rho_3(\mathrm{Gal}(\mathbb{Q}(E[3])/\mathbb{Q})) \ncong \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}).$$

There are cases where the representation is not isomorphic to the general linear group, even if the torsion points all have non-rational coordinates. This occurred in Example 6.5, where there were only three isomorphisms in the Galois group and six matrices in $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$. Another example is with the curve $T\colon y^2 = x^3 + 9x - 18$. The 5-torsion points are all non-rational, but the representation $\rho_5(\mathrm{Gal}(\mathbb{Q}(T[5])/\mathbb{Q})$ is isomorphic to the symmetric group S_4.

Acknowledgments

I thank my mentor, Seraphina Lee, for her dedication towards answering my numerous questions and for introducing me to multiple new areas of mathematics, especially Galois theory. I also thank participants Jake Zweifler and Logan Quick for multiple discussions on elliptic curves and p-adic numbers. Lastly, I thank Daniil Rudenko for providing a large variety of problems to think through and Peter May for organizing an amazing REU.

References

[1] Charles C. Pinter. *A Book of Abstract Algebra, Second Edition.* Dover Publications. 2010.

[2] Joseph H. Silverman, John T. Tate. *Rational Points on Elliptic Curves, Second Edition.* Springer. 2015.

[3] Joseph H. Silverman. *The Arithmetic of Elliptic Curves, Second Edition.* Springer. 2008.

[4] The LMFDB Collaboration. *The L-functions and Modular Forms Database.* `http://www.lmfdb.org`. [Online; accessed 23 August 2020.]