Galois Representations and Elliptic Curves

AJ Bull

December 14, 2018

1 Introduction

When looking at a field, it is natural to wonder how we can move elements into a subfield, while still maintaining the properties and laws of that subfield. That is, if we take a field F, and a field $K \supset F$, what numbers $k_1, \ldots, k_n \in K$ can we adjoin to F, and what field does this make? A heavily explored example is $\mathbb{C}$, specifically with finite extensions of the subfield $\mathbb{Q}$. In particular, we can look at **algebraic extensions** of $\mathbb{Q}$, where all numbers adjoined to $\mathbb{Q}$ from $\mathbb{C}$ are the roots of some polynomial in $Q[X]$, or polynomials with rational coefficients.

We can study these fields in the context of Galois Theory, where we look at the field homomorphisms of an extension, and the automorphisms of a field extension as a group under composition. Of particular interest are Galois Extensions, where every field homomorphism is an automorphism. Galois Theory gives a clear connection between field theory and group theory, and through it a clearer understanding of these field extensions.

Functions in (x,y) where $y^2 = f(x)$ for a cubic polynomial f, otherwise known as **elliptic curves**, can help us find such extensions. Beyond that, elliptic curves give us an easy way to put Galois extensions into the context of linear algebra, by using representation theory. This transforms what can be a very complex field of study into a simpler one. This paper includes a cursory overview of Galois Theory, assumes knowledge of elliptic curves, and touches on Representation Theory in order to display a beautiful connection all three share.

2 Galois Groups

In Galois Theory, the core idea is to look at a field extension K of F and its automorphisms. That is, for $f \in F$, a field, if K is a finite extension of F, the Galois Group is the set of homomorphisms

$$\begin{aligned} \sigma\ : K &\longrightarrow \mathbb{C} \\ f &\longmapsto f \end{aligned}$$

In other words, the homomorphisms which preserve the ring structures (addition and multiplication) and embed K into $\mathbb{C}$, fixing F. Since this is a ring homomorphism, then this map is injective.

Suppose $\sigma(k) = \sigma(k')$. $\sigma(k) - \sigma(k') = \sigma(k - k') = 0$. If $k - k' \neq 0$, $\exists (k-k')^{-1} \Rightarrow \sigma((k-k')(k-k')^{-1}) = \sigma(1) = 1$. But, $\sigma((k-k')(k-k')^{-1}) = 0 \cdot \sigma(k-k')^{-1} = 0$. So $k = k'$.

Since σ is injective, it must preserve subfields, since for $k \in K \setminus F$, $f \in F$,

$$kf \neq 1 \Rightarrow \sigma(kf) = \sigma(k)\sigma(f) \neq 1.$$

It is clear then that $\text{Aut}(K)$ is a group under composition. It is possible for a field homomorphism to take K to K', where K' is some different finite extension of F. This makes studying of the field harder, since there is some function which we might stumble upon that would take us out of the context we had been studying. However, if every field homomorphism is an automorphism, then we call K a **Galois** extension of F, and denote

$$\text{Aut}(K) = \text{Gal}(K/F)$$

and call this the Galois Group of K over F. We might also say K is Galois over F. The group law defined here is the composition of automorphisms. Since each automorphism is injective, it has an inverse, thus making elements of this set invertible. If K is not Galois over F, we can take the Galois Closure of K, where for each algebraic number in K, we collect the algebraic numbers they go to under homomorphisms and include them in the generation of a new K'.

What are the ways we can find Galois extensions, particularly of $\mathbb{Q}$? We can add members of $\mathbb{C}$, say $\alpha_1, \dots \alpha_n$, and take the smallest field containing all of these, calling it $\mathbb{Q}(\alpha_1, \dots \alpha_n) = K$. Then, we can check K is Galois by looking at embeddings $K \to \mathbb{C}$, which of these are field homomorphisms, and if said field homomorphisms are isomorphisms. But, this can be rather tedious. Instead, we will defer to a set of functions whose properties will simply yield us Galois extensions through manipulation of solution groups.

3 Elliptic Curves and Points of Finite Order

An elliptic curve is the set of solutions to $C(\mathbb{C}) = \{P = (x,y) | y^2 = ax^3 + bx^2 + cx + d\}$, where $a, b, c, d \in \mathbb{Q}$. These solutions actually form a group law under addition, with the additive identity being a point at infinity. In our cases, for cubics with rational coefficients this ”point at infinity”, denoted O, is the vertical line in the projective plane. We can transform this curve in a way that preserves the group, through a linear transformation, to the form $y^2 = x^3 + ax^2 + bx + c$ (cf. [1, Section 1.3]). We can explicitly list our group laws for addition and doubling, and through them gain an idea of what multiplying a point by any scalar might look like.

For addition, we have for $P = (x_1, y_1)$, $Q = (x_2, y_2)$ distinct points in $C(\mathbb{C})$,

$$P + Q = (x_3,\ y_3)$$

where

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - a - x_1 - x_2,\ y_3 = \frac{y_2 - y_1}{x_2 - x_1}(x_1 - x_3) - y_1.$$

and $2P = 2(x,y) = (x', y')$, where

$$x' = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c},\ y' = \left(\frac{3x^2 + 2ax + b}{2y}\right)(x - x') - y.$$

In particular, this group law is commutative, so multiplication by scalars distributes. For example:

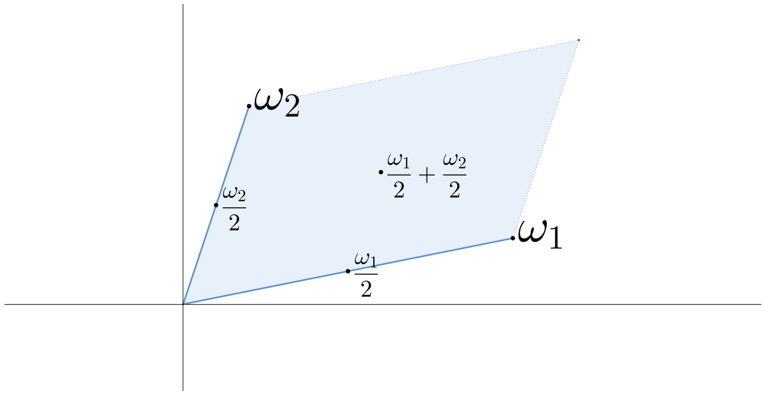
$$n(P+Q) = P+Q+\ldots+P+Q = P+\ldots+P+Q+\ldots+Q = nP+nQ.$$

We can take a subgroup $C[n]$, or the points $P \in C(\mathbb{C})$, the points with coordinates in the complex numbers, such that $nP = O$. In other words, this is the subgroup of points with order dividing n. This group, it turns out, is finite.

Proposition 1:

$$C[n] \cong (\mathbb{Z}/n\mathbb{Z}) \oplus (\mathbb{Z}/n\mathbb{Z})$$

Denote $(\mathbb{Z}/n\mathbb{Z}) \oplus (\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^2$. We know that $C(\mathbb{C}) \cong \mathbb{C}/L$, where $L = \{m_1\omega_1 + m_2\omega_2 \mid m_1, m_2 \in \mathbb{Z},\ \omega_1, \omega_2 \in \mathbb{C}\}$ (cf. [1, Section 2.2]) That is, our points are isomorphic to points inside a parallelogram on the complex plane. If we take the points of order 2, they appear in our parallelogram like so:



where the shaded region is our fundamental domain. Then, if we multiply the points $\frac{\omega_1}{2}$, $\frac{\omega_2}{2}$, and $\frac{\omega_1}{2}+\frac{\omega_2}{2}$ by 2, they go to the corners of our fundamental parallelogram, i.e. they are on the lattice L. We can do this for any n, and can construct an isomorphism by looking at the map

$$\begin{aligned} f\ :\ (\mathbb{Z}/n\mathbb{Z})^2 &\longrightarrow \mathbb{C}/L \\ (a,b) &\longmapsto \frac{a}{n}\omega_1 + \frac{b}{n}\omega_2 \end{aligned}$$

Indeed, a, b both have order dividing n, so the points on the curve correspoinding to $f(a,b)$ for $a, b \in (\mathbb{Z}/n\mathbb{Z})^2$ also have order dividing n, since $nf(a,b) = a\omega_1 + b\omega_2 \in L \Leftrightarrow nf(a,b) = O \in C(\mathbb{C})$. From this map we get all points of order dividing n in $\mathbb{C}/L \cong C(\mathbb{C})$. With this explicit isomorphism, the two groups are isomorphic.

4 Adjoining $C[n]$ to $\mathbb{Q}$

Since $C[n]$ is finite, if we take $C[n] = \{O, (x_1, y_1), \ldots (x_m, y_m)\}$ we can take the finite field extension $\mathbb{Q}(x_1, y_1, \ldots x_m, y_m)$ and see what field we get. To help us, we have the following theorem:

Theorem 1: The numbers x_k, y_k are algebraic for $1 \leq k \leq m$

Proof. For (a), we must show the coordinates of points of finite order are algebraic. Let us start with the x-coordinates. Take a point $P = (x_1, y_1)$ with order dividing n.

Claim: $x(kP) = x_k = \frac{\phi_k(x_1)}{\psi_k(x_1)}$, where $\phi_k, \psi_k \in \mathbb{Q}[x_1]$, i.e. are polynomials in terms of x_1 with rational coefficients depending on i.

Denote $kP = (x_k, y_k)$.

Case $k = 1$: $x(P) = x_1$.

Assume this is true for integers $k \leq n$. Then,

$$x((n+1)P_1) = x(nP + P) = \left(\frac{y_n - y_1}{x_n - x_1}\right)^2 - a - x_1 - x_n$$

By the induction hypothesis, all x_n terms are polynomial in x_1. From there it should be clear how we eliminate everything except $(y_n - y_1)^2$ into polynomials of x_1.

$$(y_n - y_1)^2 = y_n^2 - y_1^2 - y_1 y_n$$

If $f(x)$ is the function defining our elliptic curve, $y_n^2 = f(x_n)$, so it is polynomial in x_n and thus in x_1. Likewise, $y_1^2 = f(x_1)$, so it is polynomial in x_1. Then, we just need to show $y_1 y_n$ is polynomial in x_1. To do this we need the following:

Claim: $y(kP) = \frac{\phi_k'(x_1)}{\psi_k'(x_1)} y_1$, where $\phi_k'(x_1), \psi_k'(x_1) \in \mathbb{Q}[x_1]$.

Case $k = 1$: $y(P) = y_1$.

Assume this is true for all integers $k \leq n - 1$. Then,

$$y(nP) = y((n-1)P + P) = \frac{y_{n-1} - y_1}{x_{n-1} - x_1}(x_1 - x_n) - y_1 = y_1 \left(\frac{y_{n-1} y_1^{-1} - 1}{x_{n-1} - x_1}(x_1 - x_n) - 1\right)$$

Then, by our secondary induction hypothesis, $y_{n-1} y_1^{-1} = \frac{\phi_{n-1}'(x_1)}{\psi_{n-1}'(x_1)} y_1 y_1^{-1} = \frac{\phi_{n-1}'(x_1)}{\psi_{n-1}'(x_1)}$, so the equation in the parenthesis balances to a division of polynomials in x_n, x_{n-1}, and x_1, which by our primary induction hypothesis are all polynomial in x_1. Then,

$$y(nP) = \frac{\phi_n'(x_1)}{\psi_n'(x_1)} y_1 \Rightarrow x(nP) = y_1 y_n = \frac{\phi_n'(x_1)}{\psi_n'(x_1)} y_1^2 = \frac{\phi_n'(x_1)}{\psi_n'(x_1)} f(x_1)$$

which proves our claim for the addition formula. For the duplication formula, the process is obvious for x-coordinates, since they do not rely on y. For y-coordinates,

$$y(2P) = \left(\frac{3x_1^2 + 2ax_1 + b}{2y_1}\right)(x_1 - x_2) - y_1 = y_1 \left(\left(\frac{3x_1^2 + 2ax_1 + b}{2y_1^2}\right)(x_1 - x_2) - 1\right)$$

$$= y_1 \left(\left(\frac{3x^2 + 2ax + b}{2f(x_1)}\right)(x - x') - 1\right).$$

From this it is clear our previous induction would also work here. Since P is a point of finite order, there is some n for which $\psi_n(x_1) = 0$, which is how we get the identity element in our elliptic curve group. In other words, x_1 is the root of some polynomial with rational coefficients, so it is algebraic. Then, the x-coordinates of multiples of P are also algebraic. Since y coordinates can be written in terms of polynomials of x-coordinates, in particular via $C : y^2 = x^3 + ax^2 + bx + c$, these are also algebraic for points of finite order. Thus, all coordinates of points of finite order are algebraic.

In particular, $\mathbb{Q}(x_1, y_1, \dots x_m, y_m) = K$ is an algebraic extension of $\mathbb{Q}$. We will call this as the rationals adjoined the n-torsion points of C, or $\mathbb{Q}(C[n])$.

Lemma: Take K' to be the Galois Closure of K.

(a) $C(K')$ is a subgroup of $C(\mathbb{C})$

(b) Take the field automorphism

$$\sigma \; : \; K' \to K',$$

that fixes $\mathbb{Q}$ and define it on the curve C such that

$$\sigma \; : \; C(K') \to C(\mathbb{C})$$

where

$$\sigma(P) = \begin{cases} (\sigma(x), \sigma(y)) & \text{if } P = (x, y) \\ O & \text{if } P = O \end{cases}.$$

Then, σ defines a group homomorphism on $C(K')$. Moreover, $\sigma(P) \in C(K')$ for all $P \in C(K')$.

(c) σ preserves order.

Proof. Part (a): If we look at the duplication and addition formulas, and take P_1 and P_2 with coordinates in K. Since K' is generated by the x and y coordinates of n-torsion points and $\mathbb{Q}$, the group formulas for the elliptic curve tell us the coordinates of $P_1 \pm P_2$ will also be in K', since we are simply performing field operations on these elements. Thus, $P_1 \pm P_2 \in C(K')$.

Part (b): Take $\sigma(P+Q)$ for $P, Q \in C(K)$, with $P = (x_p, y_p)$, $Q = (x_q, y_q)$. If we look at the addition formula, we find

$$\begin{aligned} x(\sigma(P+Q)) &= \sigma\left(\left(\frac{y_q - y_p}{x_q - x_p}\right)^2 - a - x_p - x_q\right) \\ &= \left(\frac{\sigma(y_q) - \sigma(y_p)}{\sigma(x_q) - \sigma(x_p)}\right)^2 - a - \sigma(x_p) - \sigma(x_q) \\ &= x(\sigma(P) + \sigma(Q)) \end{aligned}$$

We can manipulate σ in such a way because it is a field homomorphism of K'. It is easy to see from here that this holds for the y-coordinate, and for the duplication formulas. Then,

$\sigma(P+Q)=\sigma(P)+\sigma(Q)$, and $\sigma(O)=O$, so it is a homomorphism of the group $C(\mathbb{C})$. Since σ is an automorphism of K', the coordinates of $\sigma(P+Q)$ must also be in K', so $\sigma(P+Q)\in C(K')$.

Part (c): Say $P\in C(K')$ has order n, and $\sigma(P)\in C(K')$ has order m. Then,

$$n\sigma(P)=\sigma(nP)=\sigma(O)=O.$$

So, $m|n$. Also, because σ is injective we can take its inverse, so

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

So, $n|m$. Thus $m=n$.

Theorem 2: $K=\mathbb{Q}(x_1,y_1,\dots x_m,y_m)$ is Galois over $\mathbb{Q}$.

Take σ satisfying the hypothesis of our Lemma. Then, since K is generated by the n-torsion points of C, $C[n]=\{O,(x_1,y_1),\dots,(x_m,y_m)\}$, if we take $P\in C(K)$, $\sigma(P)$ is also an n-torsion point. By definition we include all the coordinates of n-torsion points, so the coordinates of $\sigma(P)$ also land in K. In other words, $\sigma(x_k),\sigma(y_k)\in K\ \forall k$, so $\sigma(K)\subset K$. Therefore every field homomorphism of K is an automorphism, so K is Galois over $\mathbb{Q}$.

5 A Basis for $C[n]$

An important conclusion from Proposition 1 is that $C[n]$ can be seen as generated by two elements. These generators must have order n themselves, as a generator for $\mathbb{Z}/n\mathbb{Z}$ as an additive group must have order n. Pick two points of order n, and denote these generating points as P_1 and P_2. Then,

$$C[n]=\{a_1P_1+a_2P_2\mid a_1,a_2\in\mathbb{Z}/n\mathbb{Z}\}.$$

We can look at $\sigma\in\text{Gal}(K/\mathbb{Q})$, where K is $\mathbb{Q}(C[n])=\mathbb{Q}(x_1,y_1,\dots,x_m,y_m)$, as before. If we take σ of any $P\in C[n]$, we find

$$\sigma(P)=\sigma(a_1P_1+a_2P_2)=a_1\sigma(P_1)+a_2\sigma(P_2).$$

So σ is determined solely by where it sends P_1 and P_2, the generators of $C[n]$. Both of these points under σ are part of $C[n]$ themselves, since σ preserves the order of points, so we can say

$$\begin{aligned}\sigma(P_1)=Q_1=\alpha_\sigma P_1+\gamma_\sigma P_2\\ \sigma(P_2)=Q_2=\beta_\sigma P_1+\delta_\sigma P_2\end{aligned}$$

This way, we can describe all members of $\text{Gal}(K/\mathbb{Q})$ as a change of basis of $C[n]$. We can see this if we look at matrix multiplication on the right:

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

Curiously, if we take $\sigma,\tau\in\text{Gal}(K/\mathbb{Q})$, and look at $\sigma\circ\tau$, we cannot apply the τ matrix, then the σ matrix. Instead, we must compose the matrices. To demonstrate:

$$(\sigma\circ\tau)(P_1)=\sigma(\tau(P_1))=\sigma(\alpha_\tau P_1+\gamma_\tau P_2)=\alpha_\tau\sigma(P_1)+\gamma_\tau\sigma(P_2)$$
$$=\alpha_\tau(\alpha_\sigma P_1+\gamma_\sigma P_2)+\gamma_\tau(\beta_\sigma P_1+\delta_\sigma P_2)=(\alpha_\sigma\alpha_\tau+\beta_\sigma\gamma_\tau)P_1+(\alpha_\tau\gamma_\sigma+\gamma_\tau\delta_\sigma)P_2.$$

The reason for this is that we are looking at members of Gal$(K/\mathbb{Q})$ acting as a group, independently of their effect on $C[n]$. If we look at the matrix multiplication,

$$\begin{bmatrix}\alpha_\sigma & \beta_\sigma\\ \gamma_\sigma & \delta_\sigma\end{bmatrix}\begin{bmatrix}\alpha_\tau & \beta_\tau\\ \gamma_\tau & \delta_\tau\end{bmatrix}=\begin{bmatrix}\alpha_\sigma\alpha_\tau+\beta_\sigma\gamma_\tau & \alpha_\sigma\beta_\tau+\beta_\sigma\delta_\tau\\ \alpha_\tau\gamma_\sigma+\gamma_\tau\delta_\sigma & \beta_\tau\gamma_\sigma+\delta_\sigma\delta_\tau\end{bmatrix}.$$

Then, if we multiply $(P_1\ P_2)$ on the right by this matrix, we find the result in the P_1 place to match $(\sigma\circ\tau)(P_1)$. Note that in all cases, $\alpha,\beta,\gamma,\delta\in\mathbb{Z}/n\mathbb{Z}$. Say we were to look at σ^{-1}. Then, we would want the matrix to be

$$\begin{bmatrix}\alpha_{\sigma^{-1}} & \beta_{\sigma^{-1}}\\ \gamma_{\sigma^{-1}} & \delta_{\sigma^{-1}}\end{bmatrix}=\begin{bmatrix}\alpha_\sigma & \beta_\sigma\\ \gamma_\sigma & \delta_\sigma\end{bmatrix}^{-1}=\frac{1}{\alpha_\sigma\delta_\sigma-\beta_\sigma\gamma_\sigma}\begin{bmatrix}\delta_\sigma & -\beta_\sigma\\ -\gamma_\sigma & \alpha_\sigma\end{bmatrix}$$

Then, when we multiply the matrices for σ and σ^{-1}, we clearly get the identity matrix. This way of looking at members of Gal$(K/\mathbb{Q})$ as matrices naturally gives rise to a group representation.

6 Group Representation of Gal$(\mathbb{Q}(C[n])/\mathbb{Q})$

A Group Representation is a homomorphism of a group G called ρ, where

$$\rho\ :\ G\longrightarrow \mathrm{GL}_n(\mathbb{C})$$

where $\mathrm{GL}_n(\mathbb{C})$ is the set of invertible matrices with complex entries. In particular, we are looking at 2×2 matrices with entries in $\mathbb{Z}/n\mathbb{Z}$ to represent our group Gal(K/bbQ). We know we can send each element of this group to $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, since each member of our group must be invertible. Let us then define the homomorphism

$$\rho_n\ :\ \mathrm{Gal}(\mathbb{Q}(C[n])/\mathbb{Q})\longrightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$
$$\sigma\longmapsto\begin{bmatrix}\alpha_\sigma & \beta_\sigma\\ \gamma_\sigma & \delta_\sigma\end{bmatrix}$$

Our construction in the previous section shows the group operation of composition is respected in the form of matrix multiplication, and inverses go to inverses, so indeed this is a homomorphism.

Proposition 2: ρ_n is injective.

It is sufficient to show $\mathrm{Ker}(\rho_n)=\{1\}$. Take some $\sigma\in\mathrm{Ker}(\rho_n)$. Then,

$$\rho_n(\sigma)=\begin{bmatrix}\alpha_\sigma & \beta_\sigma\\ \gamma_\sigma & \delta_\sigma\end{bmatrix}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\Rightarrow\sigma(P_1)=P_1,\sigma(P_2)=P_2.$$

Then, taking $Q=a_1P_1+a_2P_2\in C[n]$,

$$\sigma(Q) = \sigma(a_1P_1 + a_2P_2) = a_1\sigma(P_1) + a_2\sigma(P_2) = a_1P_1 + a_2P_2 = Q.$$

So, if $\sigma \in \text{Ker}(\rho_n)$, $\sigma = 1$, the identity map.

This result is massively important. Not only do we have a way to represent members of a Galois group as relatively simple matrices, but this transformation is robust and gives us a 1-to-1 correspondence in both groups. If we take $\text{Image}(\rho_n) = \rho_n(\text{Gal}(\mathbb{Q}(C[n])/\mathbb{Q})$, we see that the image of this homomorphism is itself a subgroup of $\text{GL}_2(\mathbb{Z}/n\mathbb{Z})$. It is then reasonable to look at the size of this subgroup, which leads us to Serre's Theorem.

Theorem 3 (Serre): Let C be a cubic curve of the form $y^2 = x^3 + ax^2 + bx + c$, with coefficients in $\mathbb{Q}$, without complex multiplication. Then,

(a) $\exists\, M$, dependent on C, such that for all $n \geq 1$,

$$[\text{GL}_2(\mathbb{Z}/n\mathbb{Z}) \ : \ \text{Image}(\rho_n)] < M.$$

(b) $\exists\, N \geq 1$ depending on C, such that for all $n \geq 1$ with the property $\gcd(n,N) = 1$,

$$\rho_n \ : \ \text{Gal}(\mathbb{Q}(C[n])/\mathbb{Q}) \longrightarrow \text{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

is an isomorphism.

We will not show the proof here, but we can at least see the intuition of (b). Given ρ_n is injective, all we would need to show is that for certain n, as proposed, the sizes of the Galois and General Linear groups are equal. To address complex multiplication: this is the idea that in an elliptic curve C, one could multiply a point P by $x + iy = z \in \mathbb{C}$. To gain an idea of how we might do this, we would need a notion of iP, or multiplication of a point by an imaginary number. [1] addresses this topic more in-depth. There is an open problem regarding the generalization of Serre's Theorem, known as Serre's Conjecture.

Conjecture (Serre): For all Weierstrass cubic curves C without complex multiplication, there is some M such that

$$[\text{GL}_2(\mathbb{Z}/n\mathbb{Z}) \ : \ \rho_n(\ \text{Gal}(\mathbb{Q}(C[n])/\mathbb{Q})\ )] < M$$

for all curves C and all $n \geq 1$.

If ever proven true, Serre's Conjecture would provide a great deal of information on the representations of Galois groups, and thus on Galois groups themselves, by letting us know how expressive these Galois Representations are in the space of integer matrices.

7 Conclusion

Recall we started our tour of Galois Representations by simply looking at how Elliptic Curves can give us field extensions. Then, because they give us special field extensions, ones that are Galois, we can use the properties of the Elliptic Curve to say something about the Galois group in terms of well-studied groups, in the form of 2-dimensional matrices over a finite ring. We could even apply this to $\mathbb{F}_p$ if we took the p-torsion points of a curve. There are many paths for this branch of mathematics, including going into topology and further into algebraic geometry. This paper is just a glance at the depth and breadth of Galois Representations, and hopefully has given enough information to aid in further exploration of the topic.

Works Cited

[1] Joseph H. Silverman, John T. Tate, *Rational Points on Elliptic Curves, Second Edition*, Springer International Publishing Switzerland, New York, 2015. DOI 10.1007/978-3-319-18588-0