A brief introduction to Galois representations attached to Elliptic Curves

Alejandro Argáez-García
A.Argaez-Garcia@warwick.ac.uk

University of Warwick

06 November 2013.

- Galois Representations - Gabor Wiese.
- Galois Representations - Richard Taylor.
- What is a Galois Representation? - Mark Kisin.

Index:

During this talk we will use K as a field of characteristic 0.

Definition

Let K be a field and let $\overline{K}$ its algebraic closure. We call $G_K = \mathrm{Gal}(\overline{K}/K)$ the *absolute Galois group* of K.

Recall that G_K is a profinite topological group with its natural Krull topology; more precisely, $G_K = \varprojlim \mathrm{Gal}(L/K)$ as L runs over finite Galois extensions of K contained in $\overline{K}$.

Definition

Let G be a profinite group and let k be a topological field. By an *n-dimensional representation* of G we mean a continuous homomorphism of groups

$$\rho : G \to \mathrm{GL}_n(k)$$

There are three types of representations.

Definition

Let ρ be an n-dimensional representation of G over k.

(a) The representation ρ is called

- an *Artin representation* if $k \subseteq \mathbb{C}$ (topological subfield),
- an *ℓ-adic representation* if $k \subseteq \overline{\mathbb{Q}}_\ell$,
- a *mod ℓ representation* if $k \subseteq \overline{\mathbb{F}}_\ell$.

(b) The representation ρ is called

- *abelian* if $\rho(G)$ is an abelian group.
- *dihedral* if $\rho(G)$ is a dihedral group, etc.

Definition

Let ρ be an n-dimensional representation of G over k.

(*a*) The representation ρ is called

- an *Artin representation* if $k \subseteq \mathbb{C}$ (topological subfield),
- an *ℓ-adic representation* if $k \subseteq \overline{\mathbb{Q}}_\ell$,
- a *mod ℓ representation* if $k \subseteq \overline{\mathbb{F}}_\ell$.

(*b*) The representation ρ is called

- *abelian* if $\rho(G)$ is an abelian group.
- *dihedral* if $\rho(G)$ is a dihedral group, etc.

Definition

Let ρ be an n-dimensional representation of G over k.

(a) The representation ρ is called

- an *Artin representation* if $k \subseteq \mathbb{C}$ (topological subfield),
- an *ℓ-adic representation* if $k \subseteq \overline{\mathbb{Q}}_\ell$,
- a *mod ℓ representation* if $k \subseteq \overline{\mathbb{F}}_\ell$.

(b) The representation ρ is called

- *abelian* if $\rho(G)$ is an abelian group.
- *dihedral* if $\rho(G)$ is a dihedral group, etc.

Definition

Let ρ be an n-dimensional representation of G over k.

(a) The representation ρ is called

- an *Artin representation* if $k \subseteq \mathbb{C}$ (topological subfield),
- an *ℓ-adic representation* if $k \subseteq \overline{\mathbb{Q}}_\ell$,
- a *mod ℓ representation* if $k \subseteq \overline{\mathbb{F}}_\ell$.

(b) The representation ρ is called

- *abelian* if $\rho(G)$ is an abelian group.
- *dihedral* if $\rho(G)$ is a dihedral group, etc.

Definition

Let ρ be an n-dimensional representation of G over k.

(*a*) The representation ρ is called

- an *Artin representation* if $k \subseteq \mathbb{C}$ (topological subfield),
- an *ℓ-adic representation* if $k \subseteq \overline{\mathbb{Q}}_\ell$,
- a *mod ℓ representation* if $k \subseteq \overline{\mathbb{F}}_\ell$.

(*b*) The representation ρ is called

- *abelian* if $\rho(G)$ is an abelian group.
- *dihedral* if $\rho(G)$ is a dihedral group, etc.

Definition

Let ρ be an n-dimensional representation of G over k.

(*a*) The representation ρ is called

- an *Artin representation* if $k \subseteq \mathbb{C}$ (topological subfield),
- an *ℓ-adic representation* if $k \subseteq \overline{\mathbb{Q}}_\ell$,
- a *mod ℓ representation* if $k \subseteq \overline{\mathbb{F}}_\ell$.

(*b*) The representation ρ is called

- *abelian* if $\rho(G)$ is an abelian group.
- *dihedral* if $\rho(G)$ is a dihedral group, etc.

Proposition

Let G be a profinite group, k a topological field and $\rho : G \to GL_n(k)$ a representation. The image of ρ is finite in any of the three cases:

(a) *ρ is an Artin representation,*

(b) *ρ is a mod ℓ representation,*

(c) *G is a pro-p-group and ρ is an ℓ-adic representation with $\ell \neq p$.*

Proposition

Let G be a profinite group, k a topological field and $\rho : G \to GL_n(k)$ a representation. The image of ρ is finite in any of the three cases:

(a) *ρ is an Artin representation,*

(b) *ρ is a mod ℓ representation,*

(c) *G is a pro-p-group and ρ is an ℓ-adic representation with $\ell \neq p$.*

Proposition

Let G be a profinite group, k a topological field and $\rho : G \to GL_n(k)$ a representation. The image of ρ is finite in any of the three cases:

(a) *ρ is an Artin representation,*

(b) *ρ is a mod ℓ representation,*

(c) *G is a pro-p-group and ρ is an ℓ-adic representation with $\ell \neq p$.*

A representation of G_K over k is called a *(n-dimensional) Galois representation* and is given by

$$\rho : G_K \to \mathrm{GL}_n(k)$$

Index:

Class field theory ([Chi09]) provides us a precise understanding of 1-dimensional Galois representation (in this case, characters). For example, over $\mathbb{Q}$, by the Kronecker-Weber Theorem [DF04], a continuous character χ from $G_{\mathbb{Q}}$ to $\mathbb{C}^{\times}$ is a Dirichlet character

$$G_{\mathbb{Q}} \longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^{\times} \longrightarrow \mathbb{C}^{\times}$$

for some integer $n \geq 1$, where ζ_n is an $n-$root of unity.

Index:

The objective of this talk is about 2-dimensional Galois representations mod ℓ attached to elliptic curves, in specific

$$\rho_{E,\ell} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\ell)$$

where $\mathbb{F}_\ell$ is the finite group with ℓ elements, with ℓ prime.

Let K be a field. An *elliptic curve* E over K is the locus of an equation

$$E : y^2 = x^3 + ax + b$$

called the *(short) Weierstrass equation* of E where $a, b \in K$, together with a point ∞ defined over K (whose homogeneous coordinates are $[0 : 1 : 0]$), called *the point at infinity*.

Consider the set of *K-rational points* of the elliptic curve as the set

$$E(K) = \{(x, y) \in K^2 | y^2 = x^3 + ax + b\} \cup \{\infty\}.$$

This set is naturally a group and the group law is given as follows: the sum of three points equals zero (the point at infinity) if and only if the points lie on the same line. With respect to this law $(E(K), \infty)$ becomes an additive abelian group. For an explicit description of the group law, see [Sil09].

Consider the set of *K-rational points* of the elliptic curve as the set

$$E(K) = \{(x, y) \in K^2 | y^2 = x^3 + ax + b\} \cup \{\infty\}.$$

This set is naturally a group and the group law is given as follows: the sum of three points equals zero (the point at infinity) if and only if the points lie on the same line. With respect to this law $(E(K), \infty)$ becomes an additive abelian group. For an explicit description of the group law, see [Sil09].

Índice:

Let m be an integer. We define the *multiplication-by-m* map for an elliptic curve E by

$$[m] : E \to E$$
$$P \mapsto mP$$

where $mP = P + \cdots + P$, m times. The kernel of this map, denoted by $E[m]$, is called the *m-torsion subgroup* of E and is given by

$$E[m] = \{P \in E(\overline{K}) : mP = \infty\}$$

where the points P in $E[m]$ are called *m-torsion points*. This subgroup $E[m]$ of E can be seen as

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}.$$

We note that $E[m] \subset E(\overline{K})$.

Let m be an integer. We define the *multiplication-by-m* map for an elliptic curve E by

$$[m] : E \to E$$
$$P \mapsto mP$$

where $mP = P + \cdots + P$, m times. The kernel of this map, denoted by $E[m]$, is called the *m-torsion subgroup* of E and is given by

$$E[m] = \{P \in E(\overline{K}) : mP = \infty\}$$

where the points P in $E[m]$ are called *m-torsion points*. This subgroup $E[m]$ of E can be seen as

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}.$$

We note that $E[m] \subset E(\overline{K})$.

Let m be an integer. We define the *multiplication-by-m* map for an elliptic curve E by

$$[m] : E \to E$$
$$P \mapsto mP$$

where $mP = P + \cdots + P$, m times. The kernel of this map, denoted by $E[m]$, is called the *m-torsion subgroup* of E and is given by

$$E[m] = \{P \in E(\overline{K}) : mP = \infty\}$$

where the points P in $E[m]$ are called *m-torsion points*. This subgroup $E[m]$ of E can be seen as

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}.$$

We note that $E[m] \subset E(\overline{K})$.

The torsion subgroup of E, denoted by E_{tors}, is the set of points of finite order,

$$E_{tors} = \bigcup_{m=1}^{\infty} E[m].$$

If $E[m]$ is defined over K, then $E_{tors}(K)$ denotes the (rational) points of finite order in $E(K)$.

How does G_K acts on $E[m]$? Let $\sigma \in G_K$ and consider $P = (x, y)$ on the elliptic curve $E : y^2 = x^3 + ax + b$. It is not difficult to see that for P satisfying E, $\sigma(P)$ also satisfies E, i.e.,

$$\sigma(y)^2 = \sigma(x)^3 + a\sigma(x) + b.$$

In fact, for any two points P and Q on the elliptic curve we will obtain that

$$\sigma(P+Q) = \sigma(P) + \sigma(Q).$$

The reason is that the "+" is given by rational functions with all its coefficients in K. In this way, σ induces group homomorphism $E(\overline{K}) \to E(\overline{K})$, hence group homomorphism $E[m] \to E[m]$ and we can consider $\mathrm{Aut}(E[m])$.

In fact, for any two points P and Q on the elliptic curve we will obtain that

$$\sigma(P+Q) = \sigma(P) + \sigma(Q).$$

The reason is that the "+" is given by rational functions with all its coefficients in K. In this way, σ induces group homomorphism $E(\overline{K}) \to E(\overline{K})$, hence group homomorphism $E[m] \to E[m]$ and we can consider $\mathrm{Aut}(E[m])$.

In fact, for any two points P and Q on the elliptic curve we will obtain that

$$\sigma(P+Q) = \sigma(P) + \sigma(Q).$$

The reason is that the "$+$" is given by rational functions with all its coefficients in K. In this way, σ induces group homomorphism $E(\overline{K}) \to E(\overline{K})$, hence group homomorphism $E[m] \to E[m]$ and we can consider $\mathrm{Aut}(E[m])$.

Now we will discuss how $\mathrm{Aut}(E[m])$ and $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ are related when G_K acts on them. Choose a basis

$$\{P_1, P_2\}$$

$(P_i \in E(\overline{K}))$ for $E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \oplus (\mathbb{Z}/m\mathbb{Z})$. This means that every element of $E[m]$ is expressible in the form $a_1P_1 + a_2P_2$ with integers a_1, a_2. Let

$$\alpha : E(\overline{K}) \longrightarrow E(\overline{K})$$

be an automorphism from E to itself, then α maps $E[m]$ into $E[m]$, where we have the homomorphism $\alpha_m : E[m] \to E[m]$.

Now we will discuss how $\mathrm{Aut}(E[m])$ and $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ are related when G_K acts on them. Choose a basis

$$\{P_1, P_2\}$$

$(P_i \in E(\overline{K}))$ for $E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \oplus (\mathbb{Z}/m\mathbb{Z})$. This means that every element of $E[m]$ is expressible in the form $a_1P_1 + a_2P_2$ with integers a_1, a_2. Let

$$\alpha : E(\overline{K}) \longrightarrow E(\overline{K})$$

be an automorphism from E to itself, then α maps $E[m]$ into $E[m]$, where we have the homomorphism $\alpha_m : E[m] \to E[m]$.

Now we will discuss how $\mathrm{Aut}(E[m])$ and $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ are related when G_K acts on them. Choose a basis

$$\{P_1, P_2\}$$

$(P_i \in E(\overline{K}))$ for $E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \oplus (\mathbb{Z}/m\mathbb{Z})$. This means that every element of $E[m]$ is expressible in the form $a_1P_1 + a_2P_2$ with integers a_1, a_2. Let

$$\alpha : E(\overline{K}) \longrightarrow E(\overline{K})$$

be an automorphism from E to itself, then α maps $E[m]$ into $E[m]$, where we have the homomorphism $\alpha_m : E[m] \to E[m]$.

Moreover, there are $a, b, c, d \in \mathbb{Z}/m\mathbb{Z}$ such that

$$\alpha(P_1) = aP_1 + cP_2, \alpha(P_2) = bP_1 + dP_2.$$

Therefore each homomorphism $\alpha_m : E[m] \longrightarrow E[m]$ is represented by a 2×2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and, from linear algebra, we have $\mathrm{Aut}(E[m]) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Thus we obtain a homomorphism

$$\rho_{E,m} : G_K \longrightarrow \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$$
$$\sigma \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

which is called the *Galois representation mod m* attached (associated) to E.

Moreover, there are $a, b, c, d \in \mathbb{Z}/m\mathbb{Z}$ such that

$$\alpha(P_1) = aP_1 + cP_2, \alpha(P_2) = bP_1 + dP_2.$$

Therefore each homomorphism $\alpha_m : E[m] \longrightarrow E[m]$ is represented by a 2×2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and, from linear algebra, we have $\mathrm{Aut}(E[m]) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Thus we obtain a homomorphism

$$\rho_{E,m} : G_K \longrightarrow \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$$
$$\sigma \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

which is called the *Galois representation mod m* attached (associated) to E.

Moreover, there are $a, b, c, d \in \mathbb{Z}/m\mathbb{Z}$ such that

$$\alpha(P_1) = aP_1 + cP_2, \alpha(P_2) = bP_1 + dP_2.$$

Therefore each homomorphism $\alpha_m : E[m] \longrightarrow E[m]$ is represented by a 2×2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and, from linear algebra, we have $\mathrm{Aut}(E[m]) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Thus we obtain a homomorphism

$$\rho_{E,m} : G_K \longrightarrow \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$$
$$\sigma \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

which is called the *Galois representation mod m* attached (associated) to E.

There is an important observation to remark here: some authors define the Galois representation as we did, but there are others who define it as

$$\rho_{E,m} : \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$$

the motivation to do this is that

$$\mathrm{Im}(\rho_{E,m}) \cong \frac{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}{\ker(\rho_{E,m})} \cong \frac{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(E[m]))} \cong \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}),$$

where $\mathbb{Q}(E[m])$ is the field obtained by adjoining to $\mathbb{Q}$ the $x-$ and $y-$coordinates of the points in $E[m]$; called the $m-$ *division* field of E.

There is an important observation to remark here: some authors define the Galois representation as we did, but there are others who define it as

$$\rho_{E,m} : \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$$

the motivation to do this is that

$$\mathrm{Im}(\rho_{E,m}) \cong \frac{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}{\ker(\rho_{E,m})} \cong \frac{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(E[m]))} \cong \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}),$$

where $\mathbb{Q}(E[m])$ is the field obtained by adjoining to $\mathbb{Q}$ the $x-$ and $y-$coordinates of the points in $E[m]$; called the $m-$ *division* field of E.

There is an important observation to remark here: some authors define the Galois representation as we did, but there are others who define it as

$$\rho_{E,m} : \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$$

the motivation to do this is that

$$\mathrm{Im}(\rho_{E,m}) \cong \frac{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}{\ker(\rho_{E,m})} \cong \frac{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(E[m]))} \cong \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}),$$

where $\mathbb{Q}(E[m])$ is the field obtained by adjoining to $\mathbb{Q}$ the $x-$ and $y-$coordinates of the points in $E[m]$; called the $m-$ *division* field of E.

Índice:

From now on, let ℓ be a prime number and will be use $\mathrm{GL}_2(\mathbb{F}_\ell)$ to denote $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

Let E be an elliptic curve over $\mathbb{Q}$. If E is an elliptic curve without complex multiplication (CM), $\rho_{E,\ell}$ is usually surjective (below Theorem); but, for $\ell > 2$, if E has *CM*, then $\rho_{E,\ell}$ is never surjective: consider $\rho_{E,\ell} : \mathrm{Gal}(L_\ell/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\ell)$ where $L_\ell = \mathbb{Q}(E[\ell])$, then, by Galois theory, we have that

$$[L_\ell : \mathbb{Q}] \leq |\mathrm{GL}_2(\mathbb{F}_\ell)| = (\ell^2 - \ell)(\ell^2 - 1)$$

By classical results of complex multiplication (Deuring,1941), if E has complex multiplication

$$(\ell - 1)^2 \ll [L_\ell : \mathbb{Q}] \ll \ell^2.$$

Therefore $\rho_{E,\ell}$ cannot be surjective. On the other hand, if E does not have complex multiplication we have a famous result of Serre.

Let E be an elliptic curve over $\mathbb{Q}$. If E is an elliptic curve without complex multiplication (CM), $\rho_{E,\ell}$ is usually surjective (below Theorem); but, for $\ell > 2$, if E has *CM*, then $\rho_{E,\ell}$ is never surjective: consider $\rho_{E,\ell} : \mathrm{Gal}(L_\ell/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\ell)$ where $L_\ell = \mathbb{Q}(E[\ell])$, then, by Galois theory, we have that

$$[L_\ell : \mathbb{Q}] \leq |\mathrm{GL}_2(\mathbb{F}_\ell)| = (\ell^2 - \ell)(\ell^2 - 1)$$

By classical results of complex multiplication (Deuring,1941), if E has complex multiplication

$$(\ell - 1)^2 \ll [L_\ell : \mathbb{Q}] \ll \ell^2.$$

Therefore $\rho_{E,\ell}$ cannot be surjective. On the other hand, if E does not have complex multiplication we have a famous result of Serre.

Let E be an elliptic curve over $\mathbb{Q}$. If E is an elliptic curve without complex multiplication (CM), $\rho_{E,\ell}$ is usually surjective (below Theorem); but, for $\ell > 2$, if E has *CM*, then $\rho_{E,\ell}$ is never surjective: consider $\rho_{E,\ell} : \mathrm{Gal}(L_\ell/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\ell)$ where $L_\ell = \mathbb{Q}(E[\ell])$, then, by Galois theory, we have that

$$[L_\ell : \mathbb{Q}] \leq |\mathrm{GL}_2(\mathbb{F}_\ell)| = (\ell^2 - \ell)(\ell^2 - 1)$$

By classical results of complex multiplication (Deuring,1941), if E has complex multiplication

$$(\ell - 1)^2 \ll [L_\ell : \mathbb{Q}] \ll \ell^2.$$

Therefore $\rho_{E,\ell}$ cannot be surjective. On the other hand, if E does not have complex multiplication we have a famous result of Serre.

Let E be an elliptic curve over $\mathbb{Q}$. If E is an elliptic curve without complex multiplication (CM), $\rho_{E,\ell}$ is usually surjective (below Theorem); but, for $\ell > 2$, if E has *CM*, then $\rho_{E,\ell}$ is never surjective: consider $\rho_{E,\ell} : \mathrm{Gal}(L_\ell/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\ell)$ where $L_\ell = \mathbb{Q}(E[\ell])$, then, by Galois theory, we have that

$$[L_\ell : \mathbb{Q}] \leq |\mathrm{GL}_2(\mathbb{F}_\ell)| = (\ell^2 - \ell)(\ell^2 - 1)$$

By classical results of complex multiplication (Deuring,1941), if E has complex multiplication

$$(\ell - 1)^2 \ll [L_\ell : \mathbb{Q}] \ll \ell^2.$$

Therefore $\rho_{E,\ell}$ cannot be surjective. On the other hand, if E does not have complex multiplication we have a famous result of Serre.

Theorem ([Ser72])

Let K be an algebraic number field, and let E/K be an elliptic curve without complex multiplication. Then, for all but finitely many primes ℓ, $\rho_{E,\ell} : G_K \to GL_2(\mathbb{F}_\ell)$ is surjective.

In general, for any field K we have the following conjecture.

Conjecture

For each number field K there is a uniform bound ℓ_{max} such that $im(\rho_{E,\ell}) = GL_2(\mathbb{F}_\ell)$ for every (non-CM) E/K and every $\ell > \ell_{max}$.

For $K = \mathbb{Q}$, it is generally believed that $\ell_{max} = 37$.

There are some special cases when we can determine with out too much effort when $\rho_{E,\ell}$ is not surjective.

- *If E has a rational point of order ℓ, then $\rho_{E,\ell}$ is not surjective*: Let $\ell | \#E_{tors}(K)$, then exists $P \in E(K)$ such that $\ell P = \infty$. Consider $\sigma \in G_K$, then σ fixes P, i.e., $\sigma(P) = P$. Since $P \in E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$, we can take P to be a basis element of $E[\ell]$. Without loss of generality, let $\{P, Q\}$ be a basis for $E[\ell]$ and $\langle P \rangle$ be a cyclic group of order ℓ. Since $\sigma(P), \sigma(Q) \in E[\ell]$ we can see that

$$\sigma(P) = P \quad \text{and} \quad \sigma(Q) = *P + *Q$$

so, the matrix representation of the ℓ-torsion group is contained in a Borel subgroup,

$$\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \subset \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$$

and therefore the representation is not surjective.

- *If E has a rational point of order ℓ, then $\rho_{E,\ell}$ is not surjective*: Let $\ell | \#E_{tors}(K)$, then exists $P \in E(K)$ such that $\ell P = \infty$. Consider $\sigma \in G_K$, then σ fixes P, i.e., $\sigma(P) = P$. Since $P \in E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$, we can take P to be a basis element of $E[\ell]$. Without loss of generality, let $\{P, Q\}$ be a basis for $E[\ell]$ and $\langle P \rangle$ be a cyclic group of order ℓ. Since $\sigma(P), \sigma(Q) \in E[\ell]$ we can see that

$$\sigma(P) = P \quad \text{and} \quad \sigma(Q) = *P + *Q$$

so, the matrix representation of the ℓ-torsion group is contained in a Borel subgroup,

$$\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \subset \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$$

and therefore the representation is not surjective.

- *If E has a rational point of order ℓ, then $\rho_{E,\ell}$ is not surjective*: Let $\ell | \#E_{tors}(K)$, then exists $P \in E(K)$ such that $\ell P = \infty$. Consider $\sigma \in G_K$, then σ fixes P, i.e., $\sigma(P) = P$. Since $P \in E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$, we can take P to be a basis element of $E[\ell]$. Without loss of generality, let $\{P, Q\}$ be a basis for $E[\ell]$ and $\langle P \rangle$ be a cyclic group of order ℓ. Since $\sigma(P), \sigma(Q) \in E[\ell]$ we can see that

$$\sigma(P) = P \quad \text{and} \quad \sigma(Q) = *P + *Q$$

so, the matrix representation of the ℓ-torsion group is contained in a Borel subgroup,

$$\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \subset \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$$

and therefore the representation is not surjective.

- *If E admits a rational ℓ-isogeny, then $\rho_{E,\ell}$ is not surjective*: For $E/\mathbb{Q}$ without CM, this can only occurs for $\ell \leq 17$ or $\ell = 37$ [Maz78].

On the other hand, $\rho_{E,\ell}$ may be non-surjective even when E does not admit a rational ℓ-isogeny nor a point of order ℓ: the elliptic curve $E_{245.a1} : y^2 = x^3 - 112x + 784$ has torsion order 1 and does not have any ℓ-isogeny, [RV01].

It is important to remark that the image of $\rho_{E,\ell}$ for $\ell = 2$ and 3 are well-known by the experts, and they can be found in the literature of Galois representations.
When the elliptic curve over $\mathbb{Q}$ is **semistable**, everything is well-known [AG10].

Índice:

For the elliptic curve
$E_{1225.b1} : y^2 = x^3 - 269675595x - 1704553285050$ over $\mathbb{Q}$ we have an $37-$isogeny. In fact, the image $\rho_{E,37}(G_{\mathbb{Q}})$ is contained in the a Borel subgroup.

Index:

As was said before, for any number field K is believed that there is a uniform bound ℓ_{max} such that $\mathrm{im}(\rho_{E,\ell}) = \mathrm{GL}_2(\mathbb{F}_\ell)$ for every (non-CM) E/K and every $\ell > \ell_{max}$.
For $K = \mathbb{Q}$, it is generally believed that $\ell_{max} = 37$ because of all the experimentation done so far (this is an open problem).

Let

$$S_E = \{\ell \text{ prime } | \rho_{E,\ell} \text{ is not surjective } \}.$$

We define the *Serre's constant* attached to an elliptic curve as follows:

Definition

Let E be an non-CM elliptic curve over K. We set

$$A(E) = \prod_{\ell \in S_E} \ell$$

Then $\rho_{E,\ell}$ is surjective for any prime ℓ coprime to $A(E)$.

Let

$$S_E = \{\ell \text{ prime } | \rho_{E,\ell} \text{ is not surjective } \}.$$

We define the *Serre's constant* attached to an elliptic curve as follows:

Definition

Let E be an non-CM elliptic curve over K. We set

$$A(E) = \prod_{\ell \in S_E} \ell$$

Then $\rho_{E,\ell}$ is surjective for any prime ℓ coprime to $A(E)$.

Theorem

Let E be a non-CM elliptic curve over K. Then there exists a finite set S_E, depending on E such that $\rho_{E,\ell}$ is surjective for any prime number $\ell \notin S_E$.

Finding the Serre's constant is a open problem, not only on $\mathbb{Q}$ but also for any field K.

Theorem

Let E be a non-CM elliptic curve over K. Then there exists a finite set S_E, depending on E such that $\rho_{E,\ell}$ is surjective for any prime number $\ell \notin S_E$.

Finding the Serre's constant is a open problem, not only on $\mathbb{Q}$ but also for any field K.

In the last few years there has been some important breakthroughs in the field of Galois representations attached to elliptic curves, among which we can highlight those due William Duke and Alina Cojocaru.

Duke [Duk97] proved that for almost every elliptic curve without complex multiplication over $\mathbb{Q}$ the value of Serre's constant is 1.

Moreover, Cojocaru [Coj05] has proved that there is a bound for the Serre's constant when the elliptic curve over $\mathbb{Q}$ does not have torsion points of order 2, 3 and 5.

Professor Andrew Sutherland from MIT has calculated the image of the Galois representation of every elliptic curve in the Cremona and Stein-Watkins databases for all primes $\ell < 80$. (Workshop on Number Theory, Geometry, and Cryptography at the University of Warwick, June 2013.)

In spite of these accomplishments, there are a lot of open questions regarding Galois representations attached to elliptic curves (and not only for mod m representations), especially when we consider fields other than $\mathbb{Q}$.

Thank you!


Alejandro Argáez-García.
Semistable elliptic curves over $\mathbb{Q}$ and serre's constant.
Master's Thesis, Universidad Autónoma de Yucatán, México, 2010.


Nancy Childress.
Class field theory.
Universitext. Springer, New York, 2009.


Alina Carmen Cojocaru.
On the surjectivity of the Galois representations associated to non-CM elliptic curves.
Canad. Math. Bull., 48(1):16–31, 2005.
With an appendix by Ernst Kani.


David S. Dummit and Richard M. Foote.
Abstract algebra.

John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.

William Duke.
Elliptic curves with no exceptional primes.
C. R. Acad. Sci. Paris Sér. I Math., 325(8):813–818, 1997.

B. Mazur.
Rational isogenies of prime degree (with an appendix by D. Goldfeld).
Invent. Math., 44(2):129–162, 1978.

Amadeu Reverter and Núria Vila.
Images of mod p Galois representations associated to elliptic curves.
Canad. Math. Bull., 44(3):313–322, 2001.

Jean-Pierre Serre.

Propriétés galoisiennes des points d'ordre fini des courbes elliptiques.
Invent. Math., 15(4):259–331, 1972.

Joseph H. Silverman.
The arithmetic of elliptic curves, volume 106 of *Graduate Texts in Mathematics*.
Springer, Dordrecht, second edition, 2009.