
University of Bordeaux 1

algant master thesis

# Galois Representations Attached to Elliptic Curves

*Author:*
Can Ozan OGUZ

*Supervisor:*
Jean Gillibert

July 10, 2012

## Contents

## Introduction

This work focuses on a paper of Serre called "Les propriétés galoisiennes des points des torsions des courbes elliptiques"[1] where he proves a theorem about the image of Galois representations attached to elliptic curves defined over number fields without complex multiplication and poses a question which will be referred as "Serre's uniformity question". The proof of the theorem is in the section 4 of his paper, where he uses all the tools he has built in previous chapters and in his book "Abelian l-adic representations"[2]. I want to put that proof in an easy to follow format, by giving all the used results, emphasizing the underlying ideas and omitting some proofs in the sake of making the big picture more admissible.

Here is a vague idea of the proof. To study the images of the representations $\varphi_l$, Serre first studies the subgroups of $Aut(E[n]) = GL_2(\mathbb{Z}/n\mathbb{Z})$. He also studies the structure of the inertia subgroup $I_w$ of $G = Gal(\overline{K}/K)$ related to a place $w$ of $\overline{K}$. Since we are dealing with finite groups here, by using cardinality arguments, Serre eliminates some possiblites for the image of $\varphi_l$. Then, in chapter 3, he introduces an algebraic group $S_m$ with the help of local class field theory, which gives rise to an infinite family of abelian $l$-adic representations. He begins his proof by assuming existence of an infinite family $L$ of primes such that the for every $l \in L$, the representations $\varphi_l$ are not surjective and assuming futher that the elliptic curve has no complex multiplication. He proves that for an infinite number of primes, the representaions $\varphi_l$ are isomorphic to representations coming from the algebraic group $S_m$, hence their images are abelian. This suffices to conclude his proof since existence of infinitely many such representations implies that the elliptic curve has complex multiplication. All the constructions are made in order to arrive to a contradiction with the hypothesis of E having complex multiplication.

We have a nice theorem about the algebraic structure of n-torsion points on an elliptic curve defined over an algebraically closed field of characteristic 0. They form a free module over $\mathbb{Z}/n\mathbb{Z}$ of rank two. In order to study an elliptic curve over an arbitrary number field, we first take an algebraic closure of that field, look at the elliptic curve over the algebraic closure and take into account the action of the galois group of the algebraic closure over our number field.

Serre's theorem states the existence of a positive integer $n(E, K)$, depending on the elliptic curve $E$ and the number field $K$, such that for every prime $l > n(E, K)$, the representation $\varphi_l$ is surjective. Then Serre asks the question if there exists an integer $n(K)$ which depends

only on the number field $K$ and is independent of the elliptic curve $E$ such that for every prime $l$ bigger then $n(K)$, the representation $\varphi_l$ is surjective. This is the so called "Serre's uniformity question".

A weaker version of this question is finding primes where the representaions $\varphi_l$ are reducible. We will study a paper of Nicolas Billerey named "Critères d'irréductibilité pour les représentations des courbes elliptiques"[3], where he deals with the question of finding explicitly the primes $l$ such that the representation $\varphi_l$ is reducible. He calles such primes "reducible primes" for an elliptic curve $E$ defined over a number field $K$. He denotes the set of such primes $Red(E/K)$. An important result is that the set $Red(E/K)$ is finite if and only if $E$ has no complex multiplication. Then he gives an algorithm to calculate this set explicitly and discusses its complexity.

We will investigate Serre's work in the first 7 sections. In first 5 chapters, we focus on understanding the tools that will be used in the proof of his main theorem. The steps of his proof is given in section 6. There are some examples in concrete cases in section 9. The rest of the article is about Billerey's work on reducible primes, again with concrete examples in section 11.

## 1. Preliminaries

1.1. **Elliptic curves.** In this section, we will fix our notation, give some basic definitions and remind some known properties of elliptic curves defined over number fields. For more details about elliptic curves and missing proofs, the reader may refer to [4],[5].

We will denote by $\mathbb{Z}$ the usual ring of integers, by $\mathbb{Q}$ its field of fractions, by $\overline{\mathbb{Q}}$ an algebraic closure of $\mathbb{Q}$ inside the complex numbers $\mathbb{C}$. We will let $K$ be a number field or a local field in this section.

**Definition 1.** *An elliptic curve defined over $K$ is a non-singular projective curve $E$ over $K$ of genus one with a distinguished point $O \in E(K)$.*

We denote by $E(K)$ the $K$-rational points of $E$. On an elliptic curve, one can define a commutative group law where the distinguished point $O$ is the identity element. The Mordell-Weil theorem states that for an elliptic curve $E$ defined over a number field $K$, its $K$-rational points form a finitely generated abelian group. We will be interested in the torsion part of this group.

We denote by $[n] : E \to E$ the map of multiplication by $n$, where $n$ is a positive non-zero integer. This map sends a point $A$ on the elliptic curve $E$ to the point $n.A := A + A + ... + A$ where the plus operation is

the group law on the curve. We will be interested in the kernel of this map, denoted $E[n]$, which consists of $n$-torsion points on the curve.

On an algebraically closed field with characteristic zero, $E[n]$ is a free $\mathbb{Z}/n\mathbb{Z}$-module of rank 2.

Now let $l$ be a prime number and consider the sets $E[l^n]$ of $l^n$-torsion points for $n \geq 1$. We have morphisms

$$E[l^{n+1}] \to E[l^n]$$

and we can define their projective limit

$$T_l = \varprojlim E[l^n]$$

which is called the Tate module of $E$. This is a free $\mathbb{Z}_l$-module of rank 2, where $\mathbb{Z}_l$ is the ring of $l$-adic integers.

For an elliptic curve defined over K, the endomorphism group $End(E)$ is either $\mathbb{Z}$ or a 2 dimensional free $\mathbb{Z}$-module. In the first case, we say that the elliptic curve is without complex multiplication over $K$ and if this holds true for any extension of $K$, we say that the elliptic curve $E$ is without complex multiplication. We will be interested mostly in this case.

Let $E$ be an elliptic curve defined over $K$. Then $E$ is isomorphic to a curve defined by a Weierstrass equation

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

where the coefficients $a_1, a_2, a_3, a_4, a_6$ are in $K$, and the distinguished point is $(0, 1, 0)$. Conversely, every non-singular cubic curve C given by a Weierstrass equation is an elliptic curve defined over $K$ with the distinguished point $(0, 1, 0)$. There is a quantity attached to every Weiestrass equation called the discriminant, denoted as $\Delta$, which serves us to see if the curve is singular. If the discriminant is not zero, then the Weierstrass equation defines an elliptic curve(i.e it is non-singular). The discriminant of an elliptic curve is not an invariant of the curve, since different Weierstrass equations can give rise to isomorphic elliptic curves.

If our Weierstrass equation defines an elliptic curve, then we attach to it another quantitiy, called the $j$-invariant. This is an invariant of the curve. Moreover, two elliptic curves have the same $j$-invariant if and only if they are isomorphic over an algebraic closure of $K$.

If $char(K) \neq 2, 3$, which is our case for number fields, we can write the Weierstrass equation over the affine plane as

$$y^2 = x^3 + ax + b,$$

where $a, b \in O_K$.

Then the discriminant is given by the formula $\Delta = -16(4a^3 + 27b^2)$ and the $j$-invariant is equal to $1728(4a^3)/(4a^3 + 27b^2)$.

1.1.1. *Reduction of elliptic curves.* Let $(K, v)$ be a local field, $O_K$ its ring of integers and $\mathfrak{m}$ its maximal ideal.

If $E$ is an elliptic curve over $K$, it has a Weierstrass equation with coefficients in $O_K$. This equation is not unique, but we can take it with minimal discriminant. By a minimal discriminant, we mean the discriminant which has the smallest valuation among all possible discriminants. Then we can look at the reduction of this elliptic curve at the maximal ideal $\mathfrak{m}$, where we take the same Weierstrass equation with coefficients in the field $O_K/\mathfrak{m}$.

Now the question is whether this reduced formula gives us again an elliptic curve. This may not be the case since the non-singularity condition might not hold in this situation(i.e $\Delta = 0 \pmod{\mathfrak{m}}$). If we get an elliptic curve, then the next question is the structure of the group defined over the new reduced curve.

If the reduced curve is still an elliptic curve, we say that $E$ has good reduction at $\mathfrak{m}$. If this is not the case, we say that $E$ has bad reduction at $\mathfrak{m}$. The important fact is that an elliptic curve $E$ has bad reduction at $\mathfrak{m}$ if and only if $\mathfrak{m}$ divides the discriminant of $E$.

If a curve $E$ has bad reduction, we have two cases to consider. Either it has a cusp, and we have a cuspidal (or additive) reduction, or it has a node, and we have a nodal (or multiplicative) reduction.

Now suppose that $K = \mathbb{Q}_p$. We say that $E$ has bad reduction of additive type if the reduced curve has a double point with exactly one tangent. For $p \neq 2, 3$, we have the additive reduction when $p|4a^3+27b^2$ and $p| - 2ab$. In this case, if we denote the non-singular points of the reduced curve by $\overline{E}^{ns}$, we have $\overline{E}^{ns} = \mathbb{G}_a$, where $\mathbb{G}_a$ is the additive algebraic group.

We say that $E$ has bad reduction of multiplicative type if the reduced curve has a double point with two distinct tangents. For $p \neq 2, 3$, we have the multiplicative reduction if and only if $p|4a^3 + 27b^2$ and $p$ does not divide $-2ab$. Here we have either $\overline{E}^{ns} = \mathbb{G}_m$ or $\overline{E}^{ns} = \mathbb{G}_m[-2\overline{ab}]$, where $\mathbb{G}_m$ is the multiplicative algebraic group and $\overline{ab}$ is the reduction of $ab$ modulo $p$.

Now suppose that $E$ has good reduction. Then we have two cases:

(1) Good reduction of height 1(ordinary reduction):

This is the case where the $j$-invariant of the reduced curve $\overline{E}$ is not zero. We have an exact sequence

$$0 \to X_p \to E_p \to \overline{E}_p \to 0$$

where $E_p \to \overline{E}_p$ is the reduction morphism. Its kernel $X_p$ is cyclic of order $p$. The group $G$ fixes $X_p$.

(2) Good reduction of height 2(supersingular reduction):

This is the case where the $j$-invariant of the reduced curve $\overline{E}$ is zero. The curve $\overline{E}$ does not have any points of order $p$, and each element of $E_p$ is sent to the identity element of $E$.

1.1.2. *Galois representations attached to elliptic curves.*

Let $E$ be an elliptic curve defined over a number field $K$. Take an algebraic closure $\overline{K}$ of the field $K$ inside the complex numbers $\mathbb{C}$. Then the Galois group of $\overline{K}/K$ acts on the group $E[n]$ of $n$-torsion points of the curve over the algebraic closure $\overline{K}$. This gives us a representation of $Gal(\overline{K}/K)$:

$$\varphi_n : Gal(\overline{K}/K) \to Aut(E[n]) \simeq GL_2(\mathbb{Z}/n\mathbb{Z})$$

The group $\varphi_n(G)$ is the Galois group of the extension of $K$ obtained by adding the coordinates of the points of $E[n]$.

Let $E_\infty$ be the torsion part of $E(\overline{K})$. The group $Aut(E_\infty)$ is the projective limit of groups $Aut(E[n])$, which is a profinite group isomorphic to

$$\varprojlim GL_2(\mathbb{Z}/n\mathbb{Z}) = GL_2(\hat{\mathbb{Z}})$$

where $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$.

Now let $l$ be a prime number and let $E_{l^\infty}$ be the union of $E_{l^n}$ for $n \geq 1$. This is the $l$-primary part of $E_\infty$. Its automorphism group is isomorphic to $GL_2(\mathbb{Z}_l)$ where $\mathbb{Z}_l$ is the ring of $l$-adic integers.

We have

$$E_\infty = \bigoplus_{l \in P} E_{l^\infty}$$

and

$$Aut(E_\infty) = \prod_{l \text{ prime}} Aut(E_{l^\infty}) \simeq \prod_{l \text{ prime}} GL_2(\mathbb{Z}_l).$$

1.2. **Class field theory.** This theory plays a very important role in understanding the abelian $l$-adic representations, which are themselves important in understanding the representations attached to elliptic curves. For more details and proofs, the reader may refer to [6].

Let $K$ be a number field. If we have two absolute values $|\cdot|_1$ and $|\cdot|_2$, they are said to be equivalent if there exists a fixed $c > 0$ in $K$

such that $|x|_1 = |x|_2^c$ for all $x \in K$. A place of $K$ is an equivalence class of absolute values over $K$. Let $\Sigma_K$ be the set of finite places of $K$. There are two types of places: finite places that can be identified with prime ideals of $O_K$ and infinite places that can be identified with embedings of $K$ into $\mathbb{R}$ and $\mathbb{C}$. For every finite place $v \in \Sigma_K$, we have a completion $K_v$ called the completion of $K$ with respect to $v$. We define its ring of integers $O_v = \{x \in K_v | v(x) \geq 0\}$ and its maximal ideal $m_v = \{x \in K_v | v(x) > 0\}$ . Then the quotient $k_v := O_v/m_v$ is called the residue field, and it is a finite field with characteristic $p_v$.

We also denote by $\Sigma_K^\infty$ the set of infinite places of $K$ and $\overline{\Sigma}_K$ the set of all places of $K$. For $v \in \Sigma_K$, the group of units of $K_v$ is denoted by $U_v$.

**Definition 2.** *The idele group $I$ of $K$ is the subgroup of $\Pi_{v \in \overline{\Sigma}_K} K_v^*$ consisting of families $(a_v)$ with $a_v \in U_v$ for almost all $v$.*

The idele group is endowed with a topology such that the subgroup (with respect to the product topology) $\Pi_{v \in \Sigma_K^\infty} K_v^* \times \Pi_{v \in \Sigma_K} U_v$ will be open.

Then $K^*$ is embedded into $I$ by sending every element $a \in K^*$ onto the idele $(a_v)$, where $a_v = a$ for all $v$. The topology induced on $K^*$ is the discrete topology. The quotient group $C_K = I/K^*$ is called the idele class group of $K$.

**Definition 3.** *A modulus $\mathfrak{m}$ of $K$ is a function*

$$\mathfrak{m} : \overline{\Sigma}_K \to \mathbb{Z}$$

*such that*

*a)$\mathfrak{m}(v) \geq 0$ for all places and $\mathfrak{m}(v) = 0$ for all but finitely many $v \in \overline{\Sigma}_K$,*

*b)$\mathfrak{m}(v) = 0$ or $1$ for real places $v$,*

*c)$\mathfrak{m}(v) = 0$ for complex places of $v$.*

We will use the modulus to control ramification at certain primes. We will be interested only in the ramification at finite places, hence we can suppose that $m(v) = 0$ at infinite places.

**Definition 4.** *The support of a modulus $\mathfrak{m}$ is the set $S = \{v \in \overline{\Sigma}_K | \mathfrak{m}(v) > 0\}$.*

If $v \in \overline{\Sigma}_K$ and $\mathfrak{m}$ is a modulus of support $S$, we let $U_{v,\mathfrak{m}}$ denote :

- the connected component of unity of $K_v^*$ if $v \in \Sigma_K^\infty$,

- the subgroup of $U_v$ consisting of those $u \in U_v$ for which $v(1-u) \geq \mathfrak{m}(v)$ if $v \in S$,

- $U_v$ if $v \in \Sigma_K - S$.

For $v \in S$, the condition $v(1-u) \geq \mathfrak{m}(v)$ is equivalent to $\pi^{\mathfrak{m}(v)}|(1-u_v)$ where $\pi$ is a prime in $K_v$ and $u_v$ is the image of $u$ in $K_v$. If we let $\mathfrak{p}$ be the prime ideal of $O_K$ related to $v$, then our condition is equivalent to saying $u \to 1 \in (O_v/\mathfrak{p}^{\mathfrak{m}(v)})^\times$. In other words, for $v \in S$, we can also define $U_{v,\mathfrak{m}}$ to be $1 + \mathfrak{p}^{\mathfrak{m}(v)}$.

Then we define the group $U_\mathfrak{m} = \Pi_v U_{v,\mathfrak{m}}$ which is an open subgroup of $I$. Let us still denote by $U_\mathfrak{m}$ its image under the map $I \to C_K := I/K^*$. $U_\mathfrak{m}$ is a finite index open subgroup of $C_K$ and we define $C_\mathfrak{m} := C_K/U_\mathfrak{m}$ the ray class group of modulus $\mathfrak{m}$.

We let $E = O_K^*$ be the units of $K$, $E_\mathfrak{m} = E \cap U_\mathfrak{m}$.

Then we get an exact sequence

$$0 \to K^*/E_\mathfrak{m} \to I/U_\mathfrak{m} \to C_\mathfrak{m} \to 0.$$

Let $\overline{K}$ be an algebraic closure of $K$. We denote by $K^{ab}$ the maximal abelian extension of $K$ inside $\overline{K}$. The main theorem of global class theory is the following one:

**Theorem 5.** *(Global Artin homomorphism) We have a global Artin homomorphism*

$$\theta : C_K \to Gal(K^{ab}/K)$$

*which is surjective. Its kernel is the connected component $D_K$ of the identity in $C_K$.*

This gives us an isomorphism

$$\Theta : C_K/D_K \xrightarrow{\sim} Gal(K^{ab}/K).$$

## 2. Inertia groups

Let $K$ be a valued field, $v$ a valuation on $K$ corresponding to a finite place and $L$ a Galois extension of $K$. Let $S_v$ be the set of equivalence classes of extensions of $v$ to L. We denote by $G$ the Galois group of the extension of $L$ over $K$. Then $G$ acts transitively on the set $S_v$. If we think in terms of prime ideals of $O_K$, then the valuation $v$ corresponds to a prime ideal $\mathfrak{p}$ and the set $S_v$ corresponds to the set of prime ideals of $O_L$ appearing in the factorisation of $\mathfrak{p}$ into prime ideals. Then $G$ acts on this set of prime ideals above $\mathfrak{p}$ transitively. For a Galois extension, the exponents of prime ideals appearing in the factorisation of a prime ideal $\mathfrak{p} \in O_K$ over $O_L$ are all equal. We call this number the ramification index of $\mathfrak{p}$ over $L$.

Let $w$ be an extension of $v$ to $L$. Then the decomposition group of $w$, denoted as $D_w$, is the subgroup of $G$ consisting of all elements that

fix the equivalence class $[w] \in S_w$(i.e $D_w = \{\sigma \in G | \sigma.[w] = [w]\}$). If we interpret this in terms of prime ideals again, we see that for a prime ideal $\mathfrak{p}$ of $O_K$, and a prime ideal $\beta$ of $O_L$ containing $\mathfrak{p}$, the decomposition group of $\beta$, denoted as $D_{\beta/\mathfrak{p}}$, is the set $\{\sigma \in G | \sigma(\beta) = \beta\}$.

Now we denote by $l$ the residue field $O_L/\beta$ and by $k$ the residue field $O_K/\mathfrak{p}$. We suppose that $l/k$ is separable. As any element $\sigma \in D(\beta/\mathfrak{p})$ fixes $\beta$, it gives rise to an automorphism of the residue field $l = O_L/\beta$. Since $\sigma$ is in the group $Gal(L/K)$, it fixes $O_K$. Hence $\sigma$ induces an automorphism of the residue field $l$ fixing $k$. This gives us a group homomorphism

$$D_{\beta/\mathfrak{p}} \to Gal(l/k)$$

and the kernel of this homomorphism is called the inertia group of $\beta$, denoted by $I_\beta$. We know that $Gal(l/k)$ is a cyclic group since it is the Galois group of a finite extension of a finite field. Hence, we obtain an isomorphism

$$D_{\beta/\mathfrak{p}}/I_\beta \simeq Gal(l/k)$$

and any generator of this group is called a Frobenius element, denoted by $F_\beta$.

Let $K$ be a local field. We say that an extension $L$ of $K$ is unramified if $[L : K] = [l : k]$, where $l = O_L/\mathfrak{m}_L$ and $k = O_K/\mathfrak{m}_K$ are residue fields of $O_L$ and $O_K$ respectively. This condition means that the ramification index of a uniformiser $\pi_K$ is 1.

In other cases, we say that the extension $L/K$ is ramified. If the ramification index is coprime to the characteristic of the residue field, we say that the ramification is tame. Otherwise we say that the ramification is wild.

For a finite Galois extension $L'/K$, we have a morphism $Gal(L'/K) \to Gal(l'/k)$ whose kernel is the inertia group $I = Gal(K_s/K_{nr})$, where $K_s$ is a separable closure of $K$ and $K_{nr}$ is the maximum non-ramified extension of $K$ inside $K_s$. We also denote by $K_t$ the maximum tamely ramified extension of $K$ inside $K_s$. Then we have $I_p = Gal(K_s/K_t)$ the inertia $p$-group. It is the biggest pro-$p$ group contained in $I$ and we define $I_t = I/I_p = Gal(K_t/K_{nr})$ the tame inertia group of $G$.

We are interested in the tame inertia group because the action of $I_p$ on a vector space over o field of characteristic $p$ is trivial, hence we can take look at the action of $I_t$ instead of the action of the inertia group. This facilitates our work.

**Proposition 6.** [1, Section 1.6, proposition 4]
*Let $V$ be a finite dimensional vector space over a field of characteristic $p$. Let*

$$\rho : G \to GL(V)$$

*be a continuous linear representation of $G$. If $\rho$ is semisimple, then we have $\rho(I_p) = 1$.*

2.1. **The structure of the tame inertia group.**

Let $d$ be a positive integer copime to $p$. Note $\mu_d$ the group of $d$-th roots of unity in $K_{nr}$. Let $x$ be a uniformiser of $K_{nr}$, and let $K_d = K_{nr}(x^{1/d})$. The extension $K_d/K_{nr}$ is totally ramified, tamely ramified and of degre $d$, its Galois group is isomorphic to $\mu_d$. More precisely, if $s \in Gal(K_d/K_{nr})$, there exists a unique $d$-th root of unity $\zeta_d(s)$ such that

$$s(x^{1/d}) = \zeta_d(s)x^{1/d}$$

and the map $\zeta_d : Gal(K_d/K_{nr}) \to \mu_d$ is an isomorphism.

The field $K_t$ is the union of the fields $K_d$ for $(d, p) = 1$. Hence

$$I_t = Gal(K_t/K_{nr}) = \varprojlim Gal(K_d/K_{nr}) \cong \varprojlim \mu_d.$$

Now let $q$ be a power of $p$ and $\mathbb{F}_q$ the finite field with $q$ elements. We have $\mathbb{F}_q^* = \mu_{q-1}$ and the numbers of the form $q - 1$ are cofinite in the set of integers copime to $p$. Therefore the projective system $(\mu_d)$ is equivalent to the projective system $\mu_{q-1}$. Hence we have an isomorphism

$$\theta : I_t \to \varprojlim \mathbb{F}_q^*$$

where $q$ runs through powers of $p$.

2.2. **Characters of the tame inertia group.** We will look at the group $X = Hom(I_t, k_s*)$ of continuous characters of $I_t$ with values in $k_s^*$(the union of groups $F_q^*$).

We already have our morphisms $\theta_d : I_t \to Gal(K_d/K_{nr}) \simeq \mu_d$ which belong to $X$. Let us denote by $(\mathbb{Q}/\mathbb{Z})'$ the set of elements of $\mathbb{Q}/\mathbb{Z}$ whose order are coprime to $p$. Then every element $\alpha \in (\mathbb{Q}/\mathbb{Z})'$ can be written as $\alpha = a/d$ with $a, d \in \mathbb{Z}$ and $(d, p) = 1$. We will note by $\chi_\alpha$ the $a$-th power of $\theta_d$.

**Proposition 7.** *The map $\alpha \to \chi_\alpha$ is an isomorphism between the groups $(\mathbb{Q}/\mathbb{Z})'$ and $X = Hom(I_t, k_s^*)$.*

Therefore we get a parametrisation of the character group of $I_t$ via our morphisms $\theta_d$. Now let $n$ be an integer $\geq 1$ and $q = p^n$. We define a "fundamental character of level $n$" to be any character obtained as the composition of the character

$$\theta_{q-1} : I_t \to \mu_{q-1} = \mathbb{F}_q^*$$

and an automorphism of the field $\mathbb{F}_q$. Since all automorphisms of $\mathbb{F}_q$ are of the form $x \to x^{p^i}$ for $i = 0, 1..., n-1$, we have $n$ fundamental characters of level $n$:

$$\theta_d^{p^i} \text{ for } i = 0, 1, ..., n-1.$$

More generally, if $k'$ is a field of characteristic $p$, a character of $I_t$ with values in $(k')^*$ is called a fundamental character of level $n$ if it is obtained by composing $\theta_d$ with an embedding of the field $\mathbb{F}_q$ into $k'$.

2.3. **Images of the tame inertia group.** In this section, let $K$ be a complete field for a discrete valuation $v$ of characteristic zero, $k$ its residue field, $E$ an elliptic curve defined over $K$, $\overline{E}$ its reduction modulo the maximal ideal, $E_p$ the kernel of multiplication by $p$ of $E(\overline{K})$, and $\overline{E}_p$ the kernel of multiplication by $p$ of $\overline{E}(\overline{k})$. We denote by $e = v(p)$ the absolute ramification index of $K$.

**Good reduction of height 1**

Recall that this is the case where the $j$-invariant of the reduced curve is not zero. $\overline{E}_p$ is of order $p$. The kernel $X_p$ of the reduction map $E_p \to \overline{E}_p$ is cyclic of order $p$. The group $G = Gal(\overline{K}/K)$ fixes $X_p$. For a basis $(e_1, e_2)$ of $E_p$ such that $X_p = \mathbb{F}_p e_1$, the image of $G$ in $Aut(E_p)$ is contained in a Borel subgroup $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$.The image of $I_p$ is contained in the unipotent subgroup $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$. Therefore, the group $I_t$ acts on the group $X_p$ via a character $\chi_x$ and acts on the group $\overline{E}_p$ via a character $\chi_y$ with values in $\mathbb{F}_p^*$.

**Proposition 8.** *We have $\chi_x = \theta_{p-1}^e$ and $\chi_y = 1$.*

**Corollary 1.** *Suppose that $e = 1$. Then:*

*a) The two characters $\chi_x$ and $\chi_y$ are the trivial character and the fundamental character $\theta_{p-1}$.*

*b) If $I_p$ acts trivially on $E_p$, image of $I$ in $GL(E_p)$ is a cyclic group of order $p-1$, represented by matrices of the form $\left(\begin{smallmatrix} * & 0 \\ 0 & 1 \end{smallmatrix}\right)$.*

*c)If $I_p$ does not act trivially on $E_p$, then image of $I$ in $GL(E_p)$ is of order $p(p-1)$, represented by matrices of the form $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$.*

*Proof.* The assertion a) follows directly from the previous proposition. It implies that $\chi_x : I_t \to \mathbb{F}_p^*$ is surjective, and the image of $I$ is a

multiple of $p-1$. Since the image is contained in a subgroup of $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$, its order is either $p-1$ or $p(p-1)$. □

**Good reduction of height 2**

Recall that this is the case where the $j$-invariant of the reduced curve is zero. The curve $\overline{E}$ has no points of order $p$, hence the cardinality of $X_p$ is $p^2$.

**Proposition 9.** *Suppose that $e = 1$. Then:*

*a) The action of $I_p$ on $E_p$ is trivial.*

*b) On $E_p$, there exists a structure of $\mathbb{F}_{p^2}$-vector space of dimension 1 such that the action of $I_t$ is given by a fundemantal character of level 2 $\theta_{p^2-1}$.*

*c) The image of $I$ in $GL(E_p)$ is a cyclic group $C$ of order $p^2-1$*

*d) The image of $G$ in $GL(E_p)$ is equal to $C$ or to its normaliser $N$.*

**Bad reduction of multiplicative type**

Recall that this is the case where the reduced curve has one singular point with two distinct tangents.

**Proposition 10.** *The image of $I$ in $Aut(E_p)$ is contained in a subgroup of type $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$. The two characters that appear in this representaion are the trivial character and the character $\theta_{p-1}^e$.*

**Corollary 2.** *Suppose that $e = 1$. Then:*

*a) The two characters that gives the action of $I_t$ on the semi-simplification of $E_p$ are the trivial character and $\theta_{p-1}$*

*b) If $I_p$ acts trivially on $E_p$, image of $I$ in $GL(E_p)$ is a cyclic group of order $p-1$, represented by matrices of the type $\left(\begin{smallmatrix} * & 0 \\ 0 & 1 \end{smallmatrix}\right)$.*

*c)If $I_p$ does not act trivially on $E_p$, then image of $I$ in $GL(E_p)$ is of order $p(p-1)$, represented by matrices of the type $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$.*

## 3. Subgroups of $GL_2(\mathbb{F}_p)$

As we mentioned above, for an elliptic curve $E$, the kernel of multpilication by p, denoted $E[p]$ is a dimension 2 vector space over the finite field $\mathbb{F}_p$. Therefore, in order to study the image of the absolute Galois group in $Aut(E[p]) = GL_2(\mathbb{F}_p)$, it is a good idea to study the subgroups of $GL_2(\mathbb{F}_p)$ which is a finite group. Also, since $E[p]$ is a 2 dimensional vector space, we can approach the situation from a geometric point of view.

### 3.1. Cartan subgroups.

Let $V = E[p]$ be a vector space. Let $D_1$ and $D_2$ be two distinct lines of V. We have $V = D_1 \bigoplus D_2$. Let $C$ be the subgroup of $GL(V)$

consisting of elements $s$ stabilising $D_1$ and $D_2$. If we choose a suitable basis, then the group $C$ can be represented by matrices as $\left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right)$. This is the split Cartan subgroup defined by $\{D_1, D_2\}$. The group $C$ is abelian of type $(p-1, p-1)$.

Now let $C_1$ be the subgroup of $C$ acting trivially on $D_1$. This is a cyclic group of order $p-1$, and can be represented by matrices of the type $\left(\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right)$. This subgroup is called the split half Cartan subgroup.

Now, if we have $C'$ a split half Cartan subgroup, we let $C = C' \times \mathbb{F}_p^*$ be the group generated by $C'$ and by homotheties. This group $C$ is the unique split Cartan subgroup containing $C'$. The image of $C$ in the projective group $PGL(V) = GL(V)/\mathbb{F}_p^*$ is the same as the image of $C'$, which is cyclic of order $p-1$.

Now let $k$ be a sub-algebra of $End(V)$, which is a field with $p^2$ elements. The subgroup $k^*$ of $GL(V)$ is cyclic of order $p^2-1$. Its image in the projective group $PGL(V) = GL(V)/\mathbb{F}_p^*$ is cyclic of order $p+1$. Such a subgroup of $GL(V)$ is called a non-split Cartan subgroup.

The intersection of Cartan subgroups is $\mathbb{F}_p^*$. Their union is the set of elements of $GL(V)$ with order coprime to $p$. Let $s \in GL(V)$. Then the caracteristic polynomial of $s$ is $f_s(X) = X^2 - Tr(s)X + det(s)$, and its discriminant is $\Delta_s = Tr(s)^2 - 4det(s)$. If $p \neq 2$ and $\Delta_s \neq 0$, then $s$ belongs to a unique Cartan subgroup. This subgroup is split if and only if $\Delta_s$ is a square in $\mathbb{F}_p$

3.2. **Normaliser of Cartan subgroups.**

Let $C$ be a Cartan subgroup of $GL(V)$ and $N$ its normaliser. Let $k = \mathbb{F}_|[C]$ be the subalgebra of $End(V)$ generated by $C$. This is a commutative algebra. If $s \in N$, then the map $x \to sxs^{-1}$ is an automorphism of $k$. If this automorphism is identity, then $s$ commutes to $k$, so belongs to $k$, which implies that it belongs to $C$. We conclude that $(N : C) = 2$.

**Proposition 11.** [1, Section 2.2, Proposition 14] *Let $C$ be a Cartan subgroup of $GL(V)$ and let $N$ be its normaliser. Let $C'$ be another Cartan subgroup of $GL(V)$ inside $N$. Suppose that $p \geq 5$ if $C'$ is split, and $p \geq 3$ if not. Then we have $C = C'$.*

3.3. **Borel subgroups.**

Let $D$ be a line of $V$. The Borel subgroup $B$ is the group consisting of elements $s$ such that $sD = D$ which is of order $p(p-1)^2$. It can be represented by matrices as $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$. The line $D$ is the only line fixed by B. If a Cartan subgroup is contained in $B$, then this subgroup should be a split Cartan subgroup where $D$ is one of the two lines associated to that split Cartan subgroup.

### 3.4. Subgroups of $GL_2(\mathbb{F}_p)$ containing a Cartan subgroup.

**Proposition 12.** [1, Section 2.7, Proposition 17] *Let $G$ be a subgroup of $GL(V)$ containing Cartan subgroup $C$. We suppose that $p \neq 5$ if $C$ is split. Then one of the following is true:*
*either $G = GL(V)$,*
*or $G$ is contained in a Borel subgroup,*
*or $G$ is contained in the normaliser of a Cartan subgroup.*

## 4. $l$-adic representations

For all details in this section, the reader should refer to [2].

Let $K$ be a number field, and $\overline{K}$ be an algebraic closure of $K$. Let $G = Gal(\overline{K}/K)$ be the Galois group of the extension $K_s/K$. It is endowed with the Krull topology. Let $l$ be a prime number and $V$ be a finite dimensional vector space over the field $\mathbb{Q}_l$ of $l$-adic numbers. The topology of $Aut(V)$ is the one induced by the natural topology of $End(V)$.

**Definition 13.** *An $l$-adic representation of $G$(or of $K$) is a continuous homomorphism $\rho : G \to Aut(V)$.*

**Definition 14.** *Let $\rho : Gal(\overline{K}/K) \to Aut(V)$ be an $l$-adic representation of $K$ and let $v \in \Sigma_K$. We say that $\rho$ is unramified at $v$ if $\rho(I_w) = \{1\}$ for any valuation $w$ of $\overline{K}$ extending $v$.*

If $v \in \Sigma_K$ is unramified with respect to $\rho$, since we have $\rho(I_w) = \{1\}$ for any extension $w$ of $v$, the restriction of $\rho$ to $D_w \subset G$ factors through $D_w/I_w$. $D_w/I_w$ is a finite cyclic group generated by the Frobenius element $F_w$. Therefore $\rho(F_w) \in Aut(V)$ is defined and we denote it by $F_{w,\rho}$. The conjugacy class of $F_{w,\rho}$ in $Aut(V)$ depends only on $v$, and we denote it by $F_{v,\rho}$.

Now we let $v$ be an unramified place with respect to $\rho$ and let $P_{v,\rho}(T)$ denote the polynomial $det(1 - F_{v,\rho}T)$.

**Definition 15.** *An $l$-adic representation $\rho$ of $K$ is said to be rational if there exists a finite subset $S$ of $\Sigma_K$ such that*
*(a) Any element of $\Sigma_K - S$ is unramified with respect to $\rho$*
*(b) If $v \notin S$, the coefficients of $P_{v,\rho}(T)$ belong to $\mathbb{Q}$.*

**Definition 16.** *Let $l, l'$ be primes, $\rho$ be an $l$-adic representation of $K$,$\rho'$ be an $l'$-adic representation of $K$ and assume that $\rho, \rho'$ are rational. Then $\rho$ and $\rho'$ are said to be compatible if there exists a finite subset $S$ of $\Sigma_K$ such that $\rho$ and $\rho'$ are unramified outside of $S$ and $P_{v,\rho}(T) = P_{v,\rho'}(T)$ for any $v \in \Sigma_K - S$.*

**Definition 17.** *For each prime $l$, let $\rho_l$ be a rational $l$-adic representation of $K$. The system $(\rho_l)$ is said to be compatible if $\rho_l, \rho_{l'}$ are compatible for any two primes $l, l'$.*

*The system $(\rho_l)$ is said to be strictly compatible if there exists a finite subset $S$ of $\Sigma_K$ satisfying:*

*a) Let $S_l = \{v | p_v = l\}$. Then, for every $v \notin S \cup S_l$, $\rho_l$ is unramified at $v$ and $P_{v,\rho_l}(T)$ has rational coefficients.*

*b) $P_{v,\rho_l}(T) = P_{v,\rho_{l'}}(T)$ if $v \notin S \cup S_l \cup S_{l'}$.*

If $\rho : Gal(\overline{K}/K) \to Aut(V)$ is a rational $l$-adic representation of $K$, then $V$ has a composition series

$$V = V_0 \subset V_1 \subset V_2 \subset ... \subset V_q = 0$$

of $\rho$-invariant subspaces with $V_i/V_{i+1}$ simple(irreducible) for $0 \leq i \leq q-1$. Then the representation $\rho'$ of $K$ defined by $V' = \Sigma_{i=0}^{q-1} V_i/V_{i+1}$ is semi-simple, rational and compatible with $\rho$. It is called "the semi-simplification of $V$".

## 5. The algebraic group $S_{\mathfrak{m}}$

Lets start by recalling the definition of an algebraic group, and giving some well-known examples. Let $K$ be a field.

**Definition 18.** *An algebraic group $A$ over $K$ is an algebraic variety over $K$ which has a group structure defined on it where the group operation is a morphism of algebraic varieties $A \times A \to A$.*

Elliptic curves are examples of algebraic groups. First of all, they are algebraic varieties. Furthermore we can define a commutative group law on them by taking the point at infinity $(0 : 1 : 0)$ as the identity element. The idea is that if three points on the curve are aligned, they sum up to the identity element.

Returning to algebraic groups, we have the so called "multiplicative (algebraic) group", denoted by $\mathbb{G}_m$ , which is the same as $GL_1(K)$ or $K^*$, the invertible elements of the field $K$. They form an open subset of $K$ or $\mathbb{P}^1(K)$, defined by $xy = 1$. It is also called "the algebraic torus of dimension 1".

Another example is the additive group denoted by $\mathbb{G}_a$, which is formed by seeing the field $K$ as a set, and forming an additive group with it's usual addition operation.

Now let $G$ be a finite group. We will try to endow it with an algebraic group structure. Taking as many points from a field $K$ as the order of $G$, we can see it as an algebraic variety over $K$. The group law on this variety is defined by the group law on $G$. Therefore we obatined

an algebraic group. This is called the constant algebraic group related to $G$. Over any field with characteristic zero $K$, we have $G(K) = G$, hence the word constant.

5.1. **Weil Restriction.**

In this section, we will see a way of obtaining an algebraic variety defined over $\mathbb{Q}$ from an algebraic variety defined over $K$, where $K$ is a number field. In doing so, we will obtain an algebraic variety over $\mathbb{Q}$ whose $\mathbb{Q}$-rational points are the $K$-rational points of the original variety defined over $K$. The motivation behind this construction is that, while studying algebraic varieties over number fields for example, we can obtain new algebraic varieties defined over $\mathbb{Q}$ for each one of them, which makes our study easier since then all our varieties are defined over the same field.

This construction is called "Weil restriction", where we restrict the scalars from $K$ to $\mathbb{Q}$.

**Definition 19.** *Let $K$ be a number field and let $X$ be an algebraic variety defined over $K$. Weil restriction is a functor from $\mathbb{Q}-schemes^{op}$ to sets defined by*

$$Res_{K/\mathbb{Q}}X(A) = X(A \bigotimes_{\mathbb{Q}} K).$$

If our variety $X$ is affine of projective, Weil restriction gives us a variety over $\mathbb{Q}$. Now we take $X = \mathbb{G}_m(K)$ as our algebraic variety and put $T = Res_{K/\mathbb{Q}}(\mathbb{G}_m(K))$. This is an algebraic group over $\mathbb{Q}$ obtained from the multiplicative group $\mathbb{G}_m(K)$ by restriction of the scalars from $K$ to $\mathbb{Q}$.

If we have $[K : Q] = d$, then the group $T$ is a torus of dimension $d$, meaning that if we extend the scalars of $T$ from $\mathbb{Q}$ to $\overline{\mathbb{Q}}$ by setting $T_{\overline{\mathbb{Q}}} = T \bigotimes_{\mathbb{Q}} \overline{\mathbb{Q}}$, then $T_{\overline{\mathbb{Q}}}$ is isomorphic to $\mathbb{G}_m \times ... \times \mathbb{G}_m$ ($d$ times) over $\overline{\mathbb{Q}}$.

5.2. **Extension of groups.**

Here we will see a homological construction. We will be working only with commutative groups and commutative algebraic groups.We will start with a short exact sequence of groups, and a morphism from one of these groups to an algebraic group. Using the exact sequence of groups, we will obtain an exact sequence of algebraic groups. Then we will apply this construction to the exact sequence

$$1 \to K^*/E_{\mathfrak{m}} \to I_{\mathfrak{m}} \to C_{\mathfrak{m}} \to 1,$$

which is coming from idele class theory.

Here is the explicit construction of the algebraic group $B$. Let

$$0 \to Y_1 \to Y_2 \to Y_3 \to 0$$

be an exact sequence of groups with $Y_3$ finite.

Let $A$ be an algebraic group over $\mathbb{Q}$ and let

$$\epsilon : Y_1 \to A(\mathbb{Q})$$

be a homomorphism of $Y_1$ into the $\mathbb{Q}$-rational points of $A$. Now we want to construct an algebraic group $B$ with a morphism of algebraic groups $A \to B$ and a morphsim of $Y_2$ into $B(\mathbb{Q})$ such that

a) the diagram

$$\begin{array}{ccc} Y_1 & \longrightarrow & Y_2 \\ \downarrow & & \downarrow \\ A(\mathbb{Q}) & \longrightarrow & B(\mathbb{Q}) \end{array}$$

is commutative,

b) $B$ is universal with respect to a).

Here by the universality of $B$, we mean that for any algebraic group $B'$ over $\mathbb{Q}$ and morphisms $A \to B'$, $Y_2 \to B'(\mathbb{Q})$ such that a) is true, there exists a unique algebraic group homomorphism $f : B \to B'$ such that the given maps $A \to B'$ and $Y_2 \to B(\mathbb{Q})$ can be obtained by composing those of $B$ with $f$.

At the end, we obtain an exact sequence

$$0 \to A(\mathbb{Q}) \to B(\mathbb{Q}) \to Y_3 \to 0$$

where we see $Y_3$ as a constant algebraic group and obtain a commmutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Y_1 & \longrightarrow & Y_2 & \longrightarrow & Y_3 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A(\mathbb{Q}) & \longrightarrow & B(\mathbb{Q}) & \longrightarrow & Y_3 & \longrightarrow & 0. \end{array}$$

We call the algebraic group $B$ an extension of the constant algebraic group $Y_3$ by $A$.

Let $\overline{y}$ be a representative of $y \in Y_3$ in $Y_2$. For $y, y' \in Y_3$, we get

$$\overline{y} + \overline{y'} = \overline{y + y'} + c(y, y')$$

where $c(y, y')$ is an element of $Y_1$.

Now let $B$ be the disjoint union of copies $A_y$ of $A$ indexed by $y \in Y_3$.We define a group law on $B$ by using the maps

$$\pi_{y,y'} : A_y \times A_{y'} \to A_{y+y'}$$

$$(a, a') \to a + a' + \epsilon c(y, y')$$

Then we define the maps $A \to B$ and $Y_2 \to B(\mathbb{Q})$ as follows:

For the map $A \to B$, we have a natural injection of $A$ into $B$ via $A \to A_0$. We define our map as the composition of this injection and translation by $-c(0, 0)$,

For the map $Y_2 \to B(\mathbb{Q})$, we map an element $\overline{y} + z$, $y \in Y_3$, $z \in Y_1$ onto the image of $z$ in $A_y$.

5.3. **Obtaining $S_{\mathfrak{m}}$.**

Now we apply our construction to the sequence

$$1 \to K^*/E_{\mathfrak{m}} \to I_{\mathfrak{m}} \to C_{\mathfrak{m}} \to 1$$

as promised, where we take our algebraic group $A = T_{\mathfrak{m}} := T/\overline{E_{\mathfrak{m}}}$. Here $E_{\mathfrak{m}} = E \bigcap U_{\mathfrak{m}}$ as before, and $\overline{E_{\mathfrak{m}}}$ is the Zariski closure of $E_{\mathfrak{m}}$ in $T$.

This allows us to construct an algebraic group that we will denote by $S_{\mathfrak{m}}$, which satisfies the properties defined in the above section, that is we have an algebraic group morphism $T_{\mathfrak{m}} \to S_{\mathfrak{m}}$ and a group morphism $I_{\mathfrak{m}} \to S_{\mathfrak{m}}(Q)$.

This gives us an exact sequence of algebraic groups

$$1 \to T_{\mathfrak{m}} \to S_{\mathfrak{m}} \to C_{\mathfrak{m}} \to 1$$

and a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K^*/E_{\mathfrak{m}} & \longrightarrow & I/U_{\mathfrak{m}} & \longrightarrow & C_{\mathfrak{m}} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & T_{\mathfrak{m}}(\mathbb{Q}) & \longrightarrow & S_{\mathfrak{m}}(\mathbb{Q}) & \longrightarrow & C_{\mathfrak{m}} & \longrightarrow & 1. \end{array}$$

Then we say that the group $S_{\mathfrak{m}}$ is an extension of the finite group $C_{\mathfrak{m}}$ (considered as the constant algebraic group) by $T_{\mathfrak{m}}$.

5.4. **What were we doing exactly?**

Throughout this section, we tried to obtain an algebraic group $S_m$ which is related to the idele group via a commutative diagram. The reason we wanted to obtain such an algebraic group is, it gives rise to abelian $l$-adic representations which are isomorphic to representations coming from elliptic curves. This in turn implies that the elliptic curve has complex multiplication.

We want to obtain representations of $Gal(K^{ab}/K)$ over $\overline{\mathbb{Q}}_l^*$. To do so, we will first obtain a morphism $Gal(K^{ab}/K) \to S_m(\mathbb{Q}_l)$ and then a morphism from $S_m(\mathbb{Q}_l)$ to $\overline{\mathbb{Q}}_l^*$.

We have a morphism $\epsilon' : I_{\mathfrak{m}} \to S_{\mathfrak{m}}(\mathbb{Q})$ by the diagram above. We will also denote $\epsilon : I \to I_{\mathfrak{m}} \to S_{\mathfrak{m}}(\mathbb{Q})$. Let $\mathfrak{m}$ be a modulus and let $l$ be a prime number. We have another morphism $\pi : T \to T_{\mathfrak{m}} \to S_{\mathfrak{m}}$ and by taking values in $\mathbb{Q}_l$, we get a morphism

$$\pi_l : T(\mathbb{Q}_l) \to S_{\mathfrak{m}}(\mathbb{Q}_l).$$

We know that $T(\mathbb{Q}_l)$ is the invertible elements of $K \bigotimes_{\mathbb{Q}} \mathbb{Q}_l$, and $K \bigotimes_{\mathbb{Q}} \mathbb{Q}_l = \Pi_{v|l} K_v$. Therefore $T(\mathbb{Q}_l)$ is a direct factor of the idele group $I$. If we denote by $pr_l$ the projection from the idele group $I$ to this direct factor, then we get:

$$\alpha_l = \pi_l \circ pr_l : I \to T(\mathbb{Q}_l) \to S_{\mathfrak{m}}(\mathbb{Q}_l)$$

which is a continuous morphism.

This means that we have two maps $\epsilon : I \to S_{\mathfrak{m}}(\mathbb{Q})$ and $\alpha_l : I \to S_{\mathfrak{m}}(\mathbb{Q}_l)$.

Now we let $\epsilon_l : I \to S_{\mathfrak{m}}(\mathbb{Q}_l)$ be defined by

$$\epsilon_l(a) = \epsilon(a)\alpha_l(a^{-1}),$$

that is $\epsilon_l = \epsilon.\alpha_l^{-1}$.

Since $\epsilon_l$ is trivial on $K^*$, it defines a map from $C_K = I/K^*$ to $S_{\mathfrak{m}}(\mathbb{Q}_l)$. Since $S_{\mathfrak{m}}(\mathbb{Q}_l)$ is totally disconnected, the map $C_K = I/K^* \to S_{\mathfrak{m}}(\mathbb{Q}_l)$ factorises through the connected component $D_k$ of $C_K$, and $C_K/D_K$ can be identified with $Gal(K^{ab}/K)$.

At the end, we obtain a moprhism

$$\epsilon_l : Gal(K^{ab}/K) \to S_{\mathfrak{m}}(\mathbb{Q}_l).$$

Now it remains to see the other half of our desired map, from $S_{\mathfrak{m}}(\mathbb{Q}_l)$ to $\overline{\mathbb{Q}}_l^*$. The map we are looking for looks like a character of $S_{\mathfrak{m}}$, and indeed we will see that it is.

If $G$ is an algebraic group over $\mathbb{Q}$, the character group of $G$ denoted by $X(G) = Hom(G_{\mathfrak{m}}, \overline{\mathbb{Q}}^*)$ is the group of $\overline{\mathbb{Q}}$-homomorphisms of $G(\overline{\mathbb{Q}})$ to the multiplicatif group $G_m(\overline{\mathbb{Q}})$. This applies to the algebraic groups $T, T_{\mathfrak{m}}$ and $S_{\mathfrak{m}}$.

The exact sequence $0 \to T_{\mathfrak{m}} \to S_{\mathfrak{m}} \to C_{\mathfrak{m}} \to 0$ gives us another exact sequence:

$$0 \to X(C_{\mathfrak{m}}) \to X(S_{\mathfrak{m}}) \to X(T_{\mathfrak{m}}) \to 0.$$

In particular, each character $\phi$ of $T_{\mathfrak{m}}$ can be extended to a character $(\phi, f)$ of $S_{\mathfrak{m}}$, and the cardinality of different extensions is equal to the cardinality of $C_{\mathfrak{m}}$.

Let $\psi = (\phi, f)$ be a character of $S_{\mathfrak{m}}$. It gives us a morphism from $S_{\mathfrak{m}}(\mathbb{Q}_l)$ to $\overline{\mathbb{Q}}_l^*$.

Finally, by gluing this morphism with $\epsilon_l$, we obtain a continious homomorphism $\psi_l : Gal(K^{ab}/K) \to \overline{\mathbb{Q}}_l^*$.

## 6. The proof(briefly)

Here is the statement of the theorem accompanied by the results used in its proof.

**Theorem 20.** *Let $E$ be an elliptic curve defined over $K$ without complex multiplication over $\overline{K}$. Then for almost all prime number $l$, the morphism $\varphi_l : Gal(\overline{K}/K) \to Aut(E_l)$ is surjective.*

First of all, Serre remarks that we can suppose $E$ to be semistable over a finite extension of our field $K$, which is still a number field[4, Proposition 5.4, p.181]. We will suppose from now on that $E$ is semistable.

Then we suppose the existence of an infinite subset $L$ of prime numbers such that for all $l \in L$ the representations $\varphi_l$ are not surjective. In order to the use the results states in previous sections, we also suppose that every element of $L$ is $\geq 7$ and is not ramified at $K$. We can make this assumption since by doing so, we are just removing a finite number of primes from the set $L$. Now it remains to prove that $E$ has complex multiplication. The idea is to show that these representations are abelian, which will imply that $E$ has complex multiplication according to a result in Serre's book "Abelian l-adic representations"[2].

Here are the steps of the proof:

1) We use our information about the inertia subgroups of $G$ and subgroups of $GL(V)$ to show that we have 2 cases to consider:

(i) $\varphi_l(G)$ is contained in a Borel subgroup or in a Cartan subgroup;

(ii)$\varphi_l(G)$ is contained in the normaliser $N_l$ of a Cartan subgroup $C_l$, and not contained in $C_l$.

2) We show that the second case cannot occur with the help of some lemmas

3) Assuming the first case, we show that our representations are isomorphic to a system of representations arising from the algebraic group $S_{\mathfrak{m}}$, hence they are abelian.

**Step 1:**

Take $l \in L$ , let $v$ be a place of $K$ dividing $l$ and take a place $w$ of $\overline{K}$ extending $v$. Let $I_w$ be the inertia subgroup of $G$ related to $w$. The local study of inertia subgroups applied to $K_v$ gives us the structure of $\varphi_l(I_w)$.

If at $v$, $E$ has good reduction of height 1 or bad reduction of multiplicative type, the order of $\varphi_l(I_w)$ is either $l-1$ or $l(l-1)$. It can

be represented by matrices of the type $\left(\begin{smallmatrix} * & 0 \\ 0 & 1 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$ with respect to some well-chosen basis.

If at $v$, $E$ has good reduction of height 2, $\varphi_l(I_w)$ is cyclic of order $l^2 - 1$.

In the first case, $\varphi_l(G)$ contains a split half Cartan subgroup and in the second case, it contains a non-split Cartan subgroup. Also, by the hypothesis, we know that $\varphi_l(G) \neq Aut(E_l)$. Therefore, proposition(?) leaves us with two possibilities:

(i) $\varphi_l(G)$ is contained in a Borel subgroup or in a Cartan subgroup;

(ii) $\varphi_l(G)$ is contained in the normaliser $N_l$ of a Cartan subgroup $C_l$, and not contained in $C_l$.

**Step 2:**

Suppose that we are in the case (ii), that is we assume $l \in L$ satisfies $\varphi_l(G) \subset N_l$ and $\varphi_l(G) \subsetneq C_l$. If we identify $N_l/C_l$ with the group $\pm 1$, we get a map

$$G \to N_l \to N_l/C_l \simeq \pm 1$$

which can be seen as a character of $G$ of order 2. It corresponds to a quadratic extension $K_l$ of $K$.

**Lemma 21.** [1, Section 4.2, Lemma 2] *The extension $K_l/K$ is unramified.*

Now suppose the existence of an infinite family $L' \subset L$ such that every $l \in L'$ is of type (ii). We know that there exists a finite number of quadratic non-ramified extensions of $K$. Therefore, there exists an extension $K'$ of $K$ which is equal to $K_l$ for an infinity of primes $l \in L'$.

**Lemma 22.** [1, Section 4.2, Lemma 3] *If $v \in \Sigma$ is inert in $K'$ and $E$ has good reduction at $v$, then we have $Tr(F_v) = 0$ and the curve $\overline{E}_v$ is of height 2.*

Here by $F_w$ we denote the Frobenius endomorphism of $\overline{E}_v$ into the field $k_v$.

Let $\Sigma'$ be the set of places $v$ which satisfy the hypotheses of the above lemma. Then the density theorem of Cebotarev says that the density of $\Sigma'$ is $1/2$ in $\Sigma$. On the other hand, if $E$ is without complex multiplication, the set of places for which $\overline{E}_v$ is of height 2 is of density 0. We get a contradiction, hence if we are in the case (ii), $E$ has complex multiplication.

Now it remains to deal with the case (i) and to prove that in that case, E has again complex multiplication.

**Step 3:** Suppose we are in case (i). We let

$$\overline{\varphi_l} : G \to GL_2(\mathbb{F}_l)$$

be a representation of $G$ obtained from the semi-simplification of $\varphi_l$. Since $\varphi_l(G)$ is contained in a Borel subgroup or a Cartan subgroup, we have a composition series $E[l] = V \supset D \supset 0$ of $\varphi_l$ invariant subspaces, where $D$ is a line fixed by the action of the Borel or Cartan subgroup. We know that this semi-simplified representation is abelian since Borel and Cartan subgroups fix at least one line, which implies that the matrix representation of $\overline{\varphi_l}$ is diagonal over an algebraic closure.

Over an algebraic closure $k_l$ of $\mathbb{F}_l$, the representation $\overline{\varphi_l}$ is diagonalisable and is given by two characters

$$\theta_l^{(i)} : Gal(K^{ab}/K) \to k_l^*,$$

$i = 1, 2$; and again by the class field theory, we can identify the characters $\theta_l^i$ to homomorphisms of $I$, the idele group of $K$, to $k_l^*$.

**Lemma 23.** [1, Section 4.2,Lemma 4] *Let $\mathfrak{m}$ be the modulus of $K$ of support $S = \emptyset$. There exists a family of integers $n(\sigma, l, i)$ ($i \in \{1, 2\}, \sigma \in \Gamma$, where $\Gamma$ is the set of embeddings of $K$ into $\overline{\mathbb{Q}}$), equal to 0 or 1 such that*

$$\theta_l^{(i)}(a) = \Pi_{\sigma\in\Gamma}\sigma_l(a_l^{-1})^{n(\sigma,l,i)}$$

*(mod $\mathfrak{p}_l$) for all $i \in \{1, 2\}$ and $a \in U_{\mathfrak{m}}$.*

Once the lemma is proved, we have a situation similar to the one in the following proposition, which is very useful at proving that some representations are abelian:

**Proposition 24.** [1, Section 3.6, Theorem 1] *Let $(\rho_l)$ be a system of $l$-adic semi-simple representations of $K$ with the following properties:*

*(i) If $v \in \Sigma - S_\rho$ and if $l \neq p_v$ , the representation $\rho_l$ is not ramified at $v$,*

*(ii) For all $v \in \Sigma - S_\rho$, there exists a polynomial $P_v(t)$ with coefficients in $\mathbb{Q}$ such that $P_v(t) = P_{v,\rho_l} = det(1 - tF_{w,\rho})$ for all $l \neq p_v$*

*Suppose that there exists a positive integer $N$ and an infinite family $L$ of prime numbers satisfying:*

*($*$) For all $l \in L$, the reduction $\tilde{\rho}_l$ of $\rho_l$(mod $l$) is abelian, and if $\theta_l^{(i)} : I \to k_l^*$ is a caracter appearing in $\tilde{\rho}_l$, there exists integers $n(\sigma, l, i)_{\sigma\in\Sigma}$ smaller than $N$ in absolute value, such that*

$$\theta_l^{(i)}(a) = \Pi_{\sigma\in\Sigma}\sigma_l(a_l^{-1})^{n(\sigma,l,i)} \text{ (mod } p_l) \text{ for all } a \in U_m$$

*Then, the system $(\rho_l)$ is isomorphic to the system $(\Phi_l)$ associated to a representation $\Phi_0 : S_n \to GL_d$ defined over $\mathbb{Q}$.*

*In particular, $\rho_l$ is abelian.*

In fact, the situation in lemma 23 is a particular case of proposition 24. We already have the information that the $\varphi_l$ is rational, semi-simple

and forms a strictly compatible system. Then it is enough to take $N = 1$ in the proposition 24, and this implies that the representations $\varphi_l$ is isomoprhic to a system of representations arising from the algebraic group $S_m$, and in particular that they are abelian.

Now the result of Serre from his previous paper "Abelian $l$-adic representations and Elliptic Curves"[2] is the following one:

**Proposition 25.** [2, p. IV-11] *Let $\varphi_l$ be an $l$-adic representation of $G$. If the elliptic curve $E$ has no complex multiplication, then $\varphi_l(G)$ is open in $Aut(T_l)$, where $T_l = \varprojlim E[l^n]$.*

Therefore, in order to complete the proof, we have to show that the image of $\varphi_l$ is not open in $Aut(T_l)$, which is a direct passage in Serre's paper. We know that $Aut(T_l) \simeq GL_2(\mathbb{Z}_l)$ is a profinite group and the image of $\varphi_l$ is abelian. The open subgruops of $Aut(T_l)$ are of finite index and abelian subgroups of $Aut(T_l)$ cannot be of finite index.

6.1. **Serre's uniformity problem.**

The theorem above proves the existence of a natural number $n(E, K)$ depending on the elliptic curve $E$ and the number field $K$ such that for all prime numbers $l \geq n(E, K)$, the representation $\varphi_l$ is surjective (i.e $\varphi_l(G) = Aut(E_l)$). Then Serre poses the question whether is it possible to find such an integer which only depends on $K$, and does not depend on the elliptic curve $E$. This is called the "Serre's uniformity problem". Mazur showed that for $K = \mathbb{Q}$, we can take $n(K) = 168$. For the other number fields, some upper bounds are obtained in some special cases, but we do not have a general solution.

6.2. **The case of complex multiplication.** In his paper, Serre reminds the readers the previous results describing the well known case where the elliptic curve $E$ has complex multiplication.

Let $E$ be an elliptic curve with complex multiplication defined over a number field $K$ and let $R = End_{\overline{K}}(E)$. Recall that $E$ has complex multiplication means that $R \neq \mathbb{Z}$. In this case, $R$ is an order in an imaginary quadratic field $F = \mathbb{Q} \bigotimes R$.

Let $l \in P$ , define $R_l = \mathbb{Z}_l \bigotimes R$ and define $F_l = \mathbb{Q}_l \bigotimes F$. The Tate module $T_l$ is a free $R_l$-module of rank 1 and $V_l$ is a $F_l$ vector space of dimension 1. The image of $G = Gal(\overline{K}/K)$ under

$$\rho_l : G \to GL(T_l)$$

commutes to elements of $R_l$, hence they are contained in $R_l^*$. The important fact is that this image is abelian. Being abelian implies that the representations are never surjective, which will not be the case for the curves with no complex multiplication.

We can identify this representation to a homomorphism

$$\rho_l : I \to R_l^*$$

where $I$ is the idele group of K.

**Theorem 26.** *There exists exactly one continuous homomorphism $\epsilon : I \to F^*$ such that $\epsilon(x) = N_{K/F}(x)$ if $x \in K^*$, and that $\rho_l(a) = \epsilon(a)N_{K_l/F_l}(a^{-1})$ for all $l \in P$ and all $a \in I$.*

**Corollary 3.** *The image of $G$ under $\rho$ is an open subgroup of the product $\Pi_{l\in P}R_l^*$.*

We can also show that to every homomorphism $\epsilon : I \to F^*$ verifying the conditions of the above theorem corresponds an elliptic curve $E$ defined over $K$ such that $End_K(E)$ is an order of $F$. Moreover, $E$ is unique up to $K$-isogeny.

## 7. Serre's calculations

In his paper, Serre makes some calculations for elliptic curves defined over $\mathbb{Q}$. He has two cases to consider, one where the elliptic curve is semi-stable, meaning that if it has a bad reduction at any prime, it is of multiplicative type, and the other is where the curve is not semi-stable, meaning that the curve has a bad reduction of additive type.

We will denote by $S_E$ the set of primes where $E$ has bad reduction. If $p \notin S_E$, there exists a Frobenius endomorphism of the reduced curve at $p$ and we denote by $t_p$ its trace. We have

$$t_p = 1 + p - A_p$$

where $A_p$ is the number of points of the reduced curve over $\mathbb{F}_p$.

**The semi-stable case**

The first case is the easiest one, and for a semi-stable elliptic curve, Serre obtains good upper bounds for the size of the primes for which the representations $\varphi_l$ are not surjective. His most useful result is the following one:

**Proposition 27.** [1, Section 5.4, Corollary 1] *Let $p$ be the smallest prime number where the semi-stable elliptic curve $E$ has good reduction. Then we have $\varphi_l(G) = Aut(E_l)$ for all $l > \left(p^{1/2} + 1\right)^2$.*

Here is another proposition which is very useful in deciding whether for a given curve $E$ over $\mathbb{Q}$, a representation is surjective or not.

**Proposition 28.** [1, Section 5.4, Proposition 21] *Let $E$ be a semi-stable elliptic curve defined over $\mathbb{Q}$ and let $l$ be a prime number. Suppose that*
*a)$\varphi_l(G) \neq Aut(E_l)$*

*b) $l \neq 2, 3$, or $l$ does not divide one of $v_p(j)$ for $p \in S_E$.*
*Then:*
*i) $\varphi_l(G)$ is contained in a Borel subgroup of $Aut(E_l)$;*
*ii) We have $t_p = 1 + p$ (mod $l$) for all $p \in P - S_E$.*

Once we have a semi-stable elliptic curve $E$ over $\mathbb{Q}$, we first check if the condition b) is satisfied, and then it is enough to calculate $t_p$ in (mod $l$) to see if we get a contradiction. If the equivalence (mod $l$) is not satisfied, then it means that our representation $\varphi_l$ is surjective.

**Example 1.** *Let $E$ be the semi-stable curve $y^2 + y = x^3 - x^2$ defined over $\mathbb{Q}$.*

*We have $\Delta_E = -11$ and $j = -2^{12}/11$, which gives us $v_{11}(j) = -1$, so the condition b) is satisfied for all $l$.*

*This curve has a bad reduction at 11, but it is of multiplicative type. So it is stable.*

*Let us check if $1 + p - t_p = A_p$ is divisible by $l$ for $p \notin S_E$, that is for $p \neq 11$.*

*We have $A_2 = 5$. Therefore for all $l \neq 5$, we have that $\varphi_l(G) = Aut(E_l)$. Now it remains to study the case $l = 5$.*

Notice that in the above example there is very little calculation to make in order to see which representations are surjective. In fact, it suffices to calculate the number of points of the reduced curve at only one prime that we choose to be as small as possible. This information is enough to eliminate almost all cases. Here is another example:

**Example 2.** *Let $E$ be the curve defined by the equation $y^2 + xy + y = x^3 - x$ over $\mathbb{Q}$.*

*Here we have $\Delta_E = -2^2 7$ and $j = -5^6/2^2 7$.*

*The only primes where $E$ has bad reduction are 2 and 7, and at these primes, the reduction is of multiplicative type.*

*So our curve is semi-stable. The smallest prime where $E$ has good reduction is 3. We have $A_3 = 6$, so for all $l \neq 2, 3$, we have $\varphi_l(G) = Aut(E_l)$. The only cases left to study are where $l = 2$ and $l = 3$.*

In the above cases, we just calculated $A_2$ and $A_3$, which are very small numbers. Here is another example where our curve has good reduction at 2 and 3. Moreover, we have that $A_2$ and $A_3$ are coprime, which shows us directly that for all prime $l$, $\varphi_l$ is surjective.

**Example 3.** *Let $E$ be the curve defined by the equation $y^2 + y = x^3 - x^2$ over $\mathbb{Q}$.*

*We have $\Delta_E = -43$ and $j = -2^{12}/43$*

*We also have $A_2 = 5$. Now only the case where $l = 5$ remains, but this is easy to study since $A_3 = 7$ implies that in the case where $l = 5$, the representation $\varphi_l$ is surjective.*

**The non semi-stable case**

For the non semi-stable curves, the study is more difficult. If a non-stable elliptic curve $E$ has additive reduction at a prime $p$, the action of the inertia group $I_{\mathfrak{q}}$ for a prime above $\mathfrak{q}$ on $E[p]$ is defined by a finite quotient of $I_{\mathfrak{q}}$, denoted $\Phi_{\mathfrak{q}}$[7]. The definition of $\Phi_{\mathfrak{q}}$ depends whether the j-invariant $j$ is an integer at $p$ or not.

If the $j$-invariant of the curve is an integer, we have 3 cases (see [1, p.312]):

$a_1$) $p \neq 2, 3$. Then the group $\Phi_p$ is cyclic of order $2, 3, 4$, or $6$. More precisely:

$|\Phi_p| = 2 \Leftrightarrow v_p(\Delta) \equiv 6 \pmod{12}$

$|\Phi_p| = 3 \Leftrightarrow v_p(\Delta) \equiv 4 \text{ or } 8 \pmod{12}$

$|\Phi_p| = 4 \Leftrightarrow v_p(\Delta) \equiv 3 \text{ or } 9 \pmod{12}$

$|\Phi_p| = 6 \Leftrightarrow v_p(\Delta) \equiv 2 \text{ or } 10 \pmod{12}$

$a_2$) $p = 3$. Then the group $\Phi_p$ is either cyclic of order $2, 3, 4, 6$, or is non-abelian semi-direct product of a cyclic group of order 4 by a normal subgroup of order 3.

$a_3$) $p = 2$. Then the group $\Phi_p$ is isomorphic to a subgroup of $SL_2(\mathbb{F}_3)$. Its order is $2, 3, 4, 6, 8$ or $24$.

If the $j$-invariant of the curve is not an integer at $p$, we have $\Phi_p \simeq \{\pm 1\}$(see [1, p.312]).

**Proposition 29.** [1, Section 5.6, Proposition 24] *Suppose that $j$ is not an integer. Let $p_0$ be a prime such that $v_{p_0}(j) < 0$ and let $p$ the smallest prime at which $E$ has good reduction. If $l \notin S_E$, $l$ does not divide $v_{p_0}(j)$ and $l > (p^{1/2} + 1)^8$, we have $\varphi_l(G) = Aut(E_l)$.*

Here is another proposition that Serre uses in his calculations. This is a criterion for a subgroup $G$ of $GL(V)$ to be equal to $GL(V)$, where $V$ is a 2-dimensional vector space over $\mathbb{F}_p$.

**Proposition 30.** [1, Section 2.8, Proposition 19] *Let $G$ be a subgroup of $GL(V)$. Suppose that $p \geq 5$ and make the following assumptions:*

*(i) $G$ contains an element $s$ such that $Tr(s)^2 - 4det(s)$ is a square $\neq 0$ in $\mathbb{F}_p$ and $Tr(s) \neq 0$.*

*(ii) $G$ contains an element $s'$ such that $Tr(s')^2 - 4det(s')$ is not a square in $\mathbb{F}_p$ and $Tr(s') \neq 0$.*

*(iii) $G$ contains an element $s''$ such that $u = Tr(s'')^2/det(s'')$ is different from $0, 1, 2$ and $4$ and $u^2 - 3u + u \neq 0$.*

*Then $G$ contains $SL(V) = Ker(det : G \to \mathbb{F}_p^*)$. In particular, if $det : G \to \mathbb{F}_p^*$ is surjective, then we have $G = GL(V)$.*

The hypothesis in this proposition may look strange at first glance, but do not forget that $Tr(s)^2 - 4det(s)$ is the discriminant of the characteristic polynomial of the element $s \in GL(V)$. If this discriminant is not zero, then $s$ belongs to a unique Cartan subgroup, and this subgroup is split if and only if the discriminant is a square in $\mathbb{F}_p$.

## 8. Reducible representations

A weaker version of Serre's surjectivity question is to determine for which primes $l$, the representations $\varphi_l$ are reducible. Remark that if for a prime number $l$ the representation $\varphi_l$ is reducible, then there is a subspace of $E[l]$ fixed by the action of $G$, therefore $\varphi_l(G)$ cannot contain all the elements of $Aut(E[l])$, which implies that the representation $\varphi_l$ is not surjective. However, since not all non-surjective representations should leave a subspace fixed, the solution of this particular case does not provides us the general solution.

We will study a paper of Nicolas Billerey called "Critères d'irreductibilité pour les repriésentations des courbes elliptiques"[3]. He denotes $Red(E/K)$ the set of such primes for an elliptic curve $E$ defined over a number field $K$. He proves that this set is finite if and only if the elliptic curve $E$ has no complex multiplication, and gives an algorithm to determine the members of the set $Red(E/K)$. To do so, he defines a structure of a monoid over the unitary polynomials with non-zero constant terms, defines some unitary polynomials $P_{\mathfrak{q}}$ for some prime ideal $\mathfrak{q}$ above $l$ with the help of this monoid law, and obtains another polynomail $B_l$ with the monoid law using the polynomials $P_{\mathfrak{q}}$. He proves that the elements of $Red(E/K)$ divide certain values of these polynomial functions $B_l$ for every prime $l$.

## 9. Monoid Structure

Let $A$ be an integral ring with the field of fractions $L$, and let $\overline{L}$ be an algebraic closure of $L$. We denote by $M_A$ the subset of $A[X]$ consisting of unitary polynomials with constant terms $\neq 0$.

**Lemma 31.** [3, Lemma 2.1] *The map*

$$M_A \times M_A \to A[X]$$

$$(P, Q) \to (P * Q)(X) = Res_Z(P(Z), Q(X/Z)Z^{deg(Q)})$$

*has its image in $M_A$. It defines a commutative monoid law on $M_A$ with identity element $\Psi_1(X) = X - 1$. Moreover, if $P, Q \in M_A$ are written as*

$$P(X) = \Pi_{i=1}^{n}(X - \alpha_i)$$

*and*

$$Q(X) = \Pi_{j=1}^{m}(X - \beta_i)$$

*over $\overline{L}[X]$, then we have*

$$(P * Q)(X) = \Pi_{1\geq i\geq n}^{1\geq j\geq m}(X - \alpha_i\beta_j).$$

In other words, over the algebraic closure, this monoid law gives us a new polynomial $(P*Q)(X)$ whose roots are the product of the roots of $P(X)$ and $Q(X)$. Since the constant term of a polnomial is the product of it's roots up to sign, it becomes clear that the constant term of the new polynomial is not zero, hence the image of the map is in $M_A$.

**Lemma 32.** [3, Lemma 2.2] *Let $r$ be an integer $\geq 1$ and $P \in M_A$. There exists a unique polynomial $P^{(r)} \in M_A$ such that*

$$P^{(r)}(X^r) = (P * \Psi_r)(X)$$

*where $\Psi_r(X) = X^r - 1$. The map $P \to P^{(r)}$ is a morphism of monoids for the $*$ law. Moreover, if $P \in M_A$ factorizes over $\overline{L}$ as $P(X) = \Pi_{i=1}^{n}(X - \alpha_i)$, we have*

$$P^{(r)}(X) = \Pi_{i=1}^{n}(X - {\alpha_i}^r).$$

Here is a result which helps us compare the monoid law defined over different integral rings.

**Lemma 33.** [3, Lemma 2.3] *Let $A$ and $B$ be two integral rings and $\Phi : A \to B$ a morphism of rings. The set*

*$M_A^\Phi = \{P \in M_A | \Phi(P(0)) \neq 0\}$ is stable under the $*$ law. The map $\Phi$ induces a morphism of monoids(still denoted by $\Phi$)*

$$\Phi : M_A^\Phi \to M_B.$$

*Let $P \in M_A^\Phi$ and $r \geq 1$. Then, $P^{(r)} \in M_A^\Phi$ and we have $(\Phi(P))^{(r)} = \Phi(P^{(r)})$.*

This lemma will be used especially in the case of the reduction morphism $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ which is a homomorphism of rings. It will help us carry the monoid structure defined over the $\mathbb{Z}[X]$ for the elliptic curve E defined over K to the reduction of the elliptic curve.

Given a polynomial $P \in M_A$ and an integer $k \geq 1$, we will use the notations $P^{*k} = P * ... * P$ (k times) and $P^{*0} = X - 1$.

9.1. **Definition of the polynomials $P_\mathfrak{q}$.**

Let K be a number field, E an elliptic curve defined over K. If the representation $\Phi_p$ is reducible, we will say that $p$ is a reducible prime for the couple $(E, K)$.

If $p$ is a reducible prime for $(E, K)$, since the representation $\Phi_p$ is reducible and $E[p]$ is a 2-dimensional vector space over $\mathbb{F}_p$, there exists a line $D$ stable under the action of $G_K = Gal(\overline{K}/K)$. Let $\lambda$ be the character giving the action of $G_K$ on the line $D$. In a suitiable basis, the representation $\Phi_p$ can be represented by martices of the type $\left(\begin{smallmatrix} \lambda & * \\ 0 & \lambda' \end{smallmatrix}\right)$.

Now let $p$ be a reducible prime for $(E, K)$ and $\mathfrak{q}$ be a prime ideal of $O_K$. If E has good reduction at $\mathfrak{q}$ and $\mathfrak{q}$ does not divide p, the extension $K(E[p])/K$ is not ramified at $\mathfrak{q}$ by the Neron-Ogg-Shafarevich criterion. We denote by $\sigma_\mathfrak{q}$ a Frobenius morphism at $\mathfrak{q}$ of $Gal(K(E[p])/K)$.

Now suppose that E has good reduction at $\mathfrak{q}$. Then we put

$P_\mathfrak{q}(X) = X^2 - t_\mathfrak{q} X + N(\mathfrak{q}) \in \mathbb{Z}[X]$

where $N(\mathfrak{q})$ is the cardinal of the residue field $O_K/\mathfrak{q}$ and

$t_\mathfrak{q} = N(\mathfrak{q}) + 1 - A_\mathfrak{q}$

where $A_\mathfrak{q}$ is the number of points of the reduced curve at $\mathfrak{q}$ over the residue field $O_K/\mathfrak{q}$.

In other words, the polynomial $P_\mathfrak{q}$ is the characteristic polynomial of the Frobenius endomorphism $\sigma_\mathfrak{q}$.

**Proposition 34.** *(Hasse-Weil) The complex roots of $P_\mathfrak{q}$ are of modulus $N(\mathfrak{q})^{1/2}$. In particular, we have:*

$$|t_\mathfrak{q}| \leq 2N(\mathfrak{q})^{1/2}.$$

*If additionally $\mathfrak{q}$ does not divide $p$, the caracteristic polynomial of $\Phi_p(\sigma_\mathfrak{q})$ is $\overline{P_\mathfrak{q}} = P_\mathfrak{q}(mod\ p) \in \mathbb{F}_p[X]$. In particular, we have $\overline{P_\mathfrak{q}}(\lambda(\sigma_\mathfrak{q})) = 0$.*

## 10. Results of Billerey

Let $l$ be a prime number such that $E$ has good reduction at all prime ideals of $O_K$ above $l$ and let $lO_K = \Pi_{\mathfrak{q}|l}\mathfrak{q}^{v_\mathfrak{q}(l)}$ be its decomposition into prime ideals in $O_K$. Though it is a slight abuse of language, we say that E has good reduction at $l$. If this is the case, we associate a polynomial $P_l^*$ with integer coefficients to $l$:

$$P_l^* = *_{\mathfrak{q}|l}(P_\mathfrak{q}^{(12v_\mathfrak{q}(l))}) \in \mathbb{Z}[X].$$

In other words, for every prime ideal above $l$, we have our polynomial $P_\mathfrak{q}(X) = X^2 - t_\mathfrak{q} X + N(\mathfrak{q})$, whose roots are the eigenvalues of the Frobenius element $\sigma_\mathfrak{q}$ over $\overline{K}$. Let's denote these roots by $\alpha 1_\mathfrak{q}$ and

$\alpha 2_{\mathfrak{q}}$. Then we obtain another polynomial $P_{\mathfrak{q}}^{(12v_{\mathfrak{q}}(l))}$, whose roots are the $(12v_{\mathfrak{q}}(l))$-th powers of $\alpha_{1\mathfrak{q}}$ and $\alpha_{2\mathfrak{q}}$, that is

$$P_{\mathfrak{q}}^{(12v_{\mathfrak{q}}(l))}(X) = (X - \alpha_{1\mathfrak{q}}^{12v_{\mathfrak{q}}(l)})(X - \alpha_{2\mathfrak{q}}^{12v_{\mathfrak{q}}(l)})$$

over $\overline{K}$.

And finally, for every prime ideal $\mathfrak{q}$ above $l$, we take the product of all these polynomials $P_{\mathfrak{q}}^{(12v_{\mathfrak{q}}(l))}$ using the monoid law $*$. This means that we will obtain a polynomial $P_l^*$ whose roots are the multiplication of all the roots of $P_{\mathfrak{q}}^{(12v_{\mathfrak{q}}(l))}$ over the algebraic closure. To sum up, this polynomial $P_l^*$ carries all the information concerning the Frobenius elements $\sigma_{\mathfrak{q}}$ for every prime ideal of $\mathfrak{q}$ of $O_K$ above $l$.

Using this $P_l$ we define the integer:

$$B_l = \Pi_{k=0}^{[d/2]} P_l^*(l^{12k})$$

where $d$ is the degree of $K$ over $\mathbb{Q}$ and $[d/2]$ is the integer part of $d/2$.

Here is the first main result:

**Theorem 35.** [3, Theorem 2.4] *Let $p$ be a reducible prime for $(E, K)$. Then, we are in one of the following situations:*

*1.$p$ divides $6D_K$;*

*2.There exists a prime ideal $\mathfrak{p}$ of $O_K$ above $p$ at which $E$ has a bad reduction of additive type with a potential supersingular good reduction;*

*3. For all prime numbers $l$, the prime $p$ divides the integer $B_l$(if $d = 1$, we suppose $l \neq p$).*

Suppose that $E$ is given by a Weierstrass equation with coefficients in $O_K$. We denote by $\Delta$ the discriminant of $O_K$.

**Corollary 4.** [3, Corollary 2.5] *Let $p$ be a reducible prime for $(E, K)$. Then, we are in one of the two following situations:*

*1.$p$ divides $6D_K N_{K/\mathbb{Q}}(\Delta)$;*

*2. For all prime numbers $l$, the prime $p$ divides the integer $B_l$(if $d = 1$, we suppose $l \neq p$).*

10.1. **Properties of the polynomial $P_l^*$.** Suppose that E has good reduction at a prime $l$ and let $g_l$ be the cardinal of the set of prime ideals above $l$.

**Lemma 36.** [3, Lemma 2.6] *The polynomial $P_l^*$ belongs to $M_{\mathbb{Z}}$ and satisfies $P_l^*(0) = l^{12d2^{g_l-1}}$.*

*It's complex roots are of modulus $l^{6d}$. Moreover, if $l \neq p$, then $P_l^* \in M_Z^{\Phi}$ and we have*

$$\overline{P_l^*}(\Omega) = 0,$$

*where* $\Omega = \Pi_{\mathfrak{q}|l}\lambda(\sigma_{\mathfrak{q}})^{12v_{\mathfrak{q}}(l)} \in \mathbb{F}_p$.

Here is Billerey's second result:

**Theorem 37.** [3, Theorem 2.8] *Let $p$ be a prime number reducible for $(E, K)$. Then, we are in one the following situations:*

*1. $p$ divides $6D_K$.*

*2. There exists a prime ideal $\mathfrak{p}$ of $O_K$ above $p$ at which $E$ has a bad reduction of additive type with potential supersingular good reduction.*

*3.For every prime ideal $\mathfrak{q}$ of good reduction, the prime number $p$ divides the integer*

$$R_{\mathfrak{q}} = \Pi_{k=0}^{[d/2]} Res(P_{\mathfrak{q}}^{(12h),}(\mathfrak{m}_{\gamma_{\mathfrak{q}}}^{(12)})^{*k})$$

*where $\mathfrak{q}^h = \gamma_{\mathfrak{q}}O_K$ and $\mathfrak{m}_{\gamma_{\mathfrak{q}}}$ is the minimal polynomial of $\gamma_{\mathfrak{q}}$ over $\mathbb{Q}$. (If $d = 1$, we suppose that $\mathfrak{q}$ does not divide $p$).*

*Moreover, if $E$ has no complex multiplication over $\overline{\mathbb{Q}}$, then $R_{\mathfrak{q}} \neq 0$ for an infinite number of prime ideals $\mathfrak{q}$.*

## 11. Billerey's Calculations

Billerey gives an algorithm to calculate the set $Red(E/K)$. The set of exceptional primes for Billerey is

$$S_1 = \{\text{prime divisors of } 6D_K N_{K/\mathbb{Q}}(\Delta)\}.$$

First he calculates the elements of this set. Then he takes $l_0$ to be the smallest prime that does not belong to $S_1$ and calculates $B_{l_0}$. Remember that if $p \notin S_1$ is a reducible prime, then it should divide $B_l$ for every prime $l$. The only problem we might encounter is $B_l$ being zero for a prime $l$. Therefore, in Billerey's algorithm, if $B_{l_0} = 0$, then we take the smallest prime $l_1$ such that $l_1 \notin S_1$ , $l_1 > l_0$ and calculate $B_{l_1}$. If $B_{l_1} = 0$, then we repeat this procedure till we find a prime $l_n$ such that $B_{l_n} \neq 0$. If we cannot find such an integer$B_{l_n}$ for a long time, we go to step 2′, if not, we go to step 2.

Step 2: Now we should find the prime divisors of $B_l \neq 0$ that we found above. This may take some time depending on the integer $B_l$, so we might consider calculating some more integers $B_{l_k}$ as above. Since a reducible prime $p \notin S_1$ should divide all of these integers, we first calculate the greatest common divisor of all these primes and then try to factorise it. We denote by $S_2$ the set of prime divisors of this greatest common divisor, and put $S = S_1S_2$

Step 2': It is possible that it takes a long time to find an integer $B_l \neq 0$. However, since we are considering the case where $E$ has no complex multiplicaiton, by theorem ???, we know the existance of a prime $\mathfrak{q}$ where E has good reduction such that $R_{\mathfrak{q}} \neq 0$. Again, to

make the factorisation faster, we might calculate some integers $R_{\mathfrak{q}} \neq 0$ and try to factorise their greatest common divisor. We denote the set of prime divisors of this greatest common divisor by $S_2$, and we put $S = S_1 S_2$.

Now we have a set $S$ which contains the set $Red(E/K)$, but which might be bigger. In order to eliminate some of the primes that are in $S - Red(E/K)$, we can calculate polynomials $P_{\mathfrak{q}}$ for some primes ideal $\mathfrak{q}$ where $E$ has good reduction. Then for $\mathfrak{q}$ not dividing $p$, if $P_{\mathfrak{q}}$ is irreducible (mod $p$), then $p$ does not belong to $Red(E/K)$. The claim is that the subset $S'$ of $S$, whose elements are the ones that are not eliminated, is small enough in general.

## 11.1. **Examples.**

**Example 4.** *We suppose that $K = \mathbb{Q}(\sqrt{-1})$. Let $E$ be the curve defined by the equation*

*$y^2 = x^3 + 2(3+2\sqrt{-1})x + 2(3+2\sqrt{-1})$. Then the set $Red(E/K)$ is empty.*

*To see this, we first calculate $\Delta = -16(4a^3+27b^2)$ and then $N_{K/\mathbb{Q}}(\Delta) = 2^{12}.3^2.2857$. Let $p$ be a prime number not belonging to set $S_1 = \{2, 3, 2857\}$. The smallest prime not belonging to $S_1$ is $5$, and we know that $p$ divides $B_5$. We hope that $B_5 \neq 0$.*

*In oerder to calculate $B_5$, we need to find polynomials $P_{\mathfrak{q}}$ for $\mathfrak{q}|5$. In $\mathbb{Q}(\sqrt{-1})$, $5$ factorises as $(3+2\sqrt{1})(3-2\sqrt{-1})$, where the factors are primes. This should also make the choice of coefficients of the equation of the curve clear.*

*Remember that we have $P_{\mathfrak{q}}(X) = X^2 - t_{\mathfrak{q}}X + N(\mathfrak{q})$ where $N(\mathfrak{q})$ is the cardinality of the residue field $O_K/\mathfrak{q}$ and $t_{\mathfrak{q}} = N(\mathfrak{q}) + 1 - A_{\mathfrak{q}}$, $A_{\mathfrak{q}}$ being the number of points of the reduction of $E$ at $\mathfrak{q}$ in the field $O_K/\mathfrak{q}$.*

*We have $\{t_{\mathfrak{q}}\}_{\mathfrak{q}|5} = \{-2, 1\}$.*

*Now we should calculate $P_5^* = *_{\mathfrak{q}|5}(P_q^{(12v_{\mathfrak{q}}(5))})$ where $v_{\mathfrak{q}}(5) = 1$ for all $\mathfrak{q}|5$ since $5 = (3+2\sqrt{-1})(3-2\sqrt{-1})$. This gives us $P_5^* = *_{\mathfrak{q}|5}(P_q^{(12)})$.*

*Then we should calculate $B_5 = \Pi_{k=0}^{[d/2]} P_5^*(5^{12k})$. Since we have $d = [K : Q] = 2$ in this case, we get $B_5 = P_5^*(1) \times P_5^*(5^{12})$, which gives us a long list of primes:*

$$B_5 = 2^{28}.3^{16}.5^{39}.11^2.17.61.73.277.397.557.653.757.23833$$

*Now it seems that calculating another integer $B_l$ is a good idea. The next smallest prime we can take is $7$, and $7$ is still a prime in $O_K$.*

*We have* $t_7 = 6$, *and* $N_7 = |O_K/7| = 14$, *so we have* $P_7(X) = X^2 - 6X + 14$. *This also gives us*

$$P_7^* = P_7^{(12v_7(7))} = P_7^{(12)}.$$

*Therefore, we get* $B_7 = P_7^*(1) \times P_7^*(7^12)$, *which gives us again a long list of primes:*

$$B_7 = 2^{14}.3^8.5^2.7^{13}.11.13^5.37^2.2089.2689.3889$$

*But with these two integers* $B_5$ *and* $B_7$, *we get* $S_2 := gcd(B_5, B_7) = 2^{14}.3^8.5^2.11$, *so we just have to deal with the elements of the set* $S = S_1 \cup S_2 = \{2, 3, 5, 11, 2857\}$.

*E has good reduction at the prime ideal* $3O_K$ *and we have* $P_3 = X^2 + 3X + 9$.

*So* $P_3$ *is irreducible modulo* 2,5 *and* 11. *Then* $2, 5, 11$ *do not belong to* $Red(E/K)$.

*Now, for a prime ideal* $\mathfrak{q}_5$ *above* 5, *we have that* $t_\mathfrak{q} = -2$ *or* 1, *that is* $t_{\mathfrak{q}_5} \equiv 1$ *(mod* 3*), and that* $P_{\mathfrak{q}_5}(X) = X^2 + 2X + 2$ *(mod* 3*), which is irreducible modulo* 3, *meaning that* 3 *is not in the set* $Red(E/K)$.

*Finally we have* $P_7(X) = X^2 - 6X + 49$, *which is irreducible modulo* 2857. *Hence, the set* $Red(E/K)$ *is empty.*

**Example 5.** *We take* $K = \mathbb{Q}(\sqrt{2})$,$A = -3^3.5.17^3(428525 + 303032\sqrt{2})$ *and* $B = 2.3^3.5.17^3(62176502533 + 43965551956\sqrt{2})$. *We let E to be the elliptic curve defined by the equation*

$$y^2 = x^3 + Ax + B.$$

*Then* $Red(E/K) = \{13\}$ .

## 12. Billerey's results on the uniformity question

Let $\mathfrak{q}$ be a prime ideal of $O_K$ with residual characteristic $l$. We have

$$N(\mathfrak{q}) = |O_K/\mathfrak{q}| = l^{f_\mathfrak{q}},$$

where $f_\mathfrak{q}$ is the residual degre of $\mathfrak{q}$. We suppose that $E$ has bad reduction of additive type at $\mathfrak{q}$ with potentially good reduction. Then for every prime $p > 3$ such that $p \neq l$, the action of the inertia group $I_\mathfrak{q}$ on $E[p]$ factorises through a finite quotient $\Phi_\mathfrak{q}$ of $I_\mathfrak{q}$:

$$I_\mathfrak{q} \to \Phi_\mathfrak{q} \hookrightarrow Aut(E[p]).$$

Serre also studies the case of non-stable elliptic curves E without complex multiplication via this finite quotient $\Phi_\mathfrak{q}$. His analysis focuses on the curves defined over $\mathbb{Q}$ and in his paper, Billerey extends some of Serre's propositions to the case of number fields.

**Proposition 38.** *Let $E$ be an elliptic curve without complex multiplication defined over $K$ such that $E$ has bad reduction of additive type at $\mathfrak{q}$ with potential good reduction. Suppose that for every integer $n \geq 0$, the order of the group $\Phi_\mathfrak{q}$ does not divide $N(\mathfrak{q})^n(N(\mathfrak{q})-1)$. Then the representation $\phi_p$ is irreducible for all prime numbers $p \geq 3$ such that $p \neq l$.*

Here is a useful corollary of the previous propositon in the case that $\mathfrak{q}$ divides 2:

**Corollary 5.** [3, Corollary 3.4] *We suppose that $\mathfrak{q}$ divides 2 and one of the following two conditions is satisfied:*

*1.The group $\Phi_\mathfrak{q}$ is of order 8 or 24;*

*2.The group $\Phi_\mathfrak{q}$ is of order 3 or 6 and the residue degre $f_\mathfrak{q}$ is an odd number.*

*Then the representation $\phi_p$ is irreducible for all prime number $p \geq 5$.*

And here is another corollary in the case that $\mathfrak{q}$ divides 3:

**Corollary 6.** [3, Corollary 3.5]

*We suppose that $\mathfrak{q}$ divides 3 and one of the following two conditions is satisfied:*

*1.The group $\Phi_\mathfrak{q}$ is of order 12;*

*2.The group $\Phi_\mathfrak{q}$ is of order 4 and the residue degre $f_\mathfrak{q}$ is an odd number.*

*Then the representation $\phi_p$ is irreducible for all prime number $p \geq 5$.*

**Example 6.** *We let $K = \mathbb{Q}(\sqrt{5})$ and consider the elliptic curve $E$ defined by the equation $y^2 = x^3 + 2x^2 + \omega x$ where $\omega_=(1+\sqrt{5})/2$*

*Then $Red(E/K) = 2$.*

*We have $\Delta_E = -2^6\omega$. Since $\omega$ is a unit in $O_K$, we know $E$ has good reduction at all primes $p \neq 2$. At $p = 2$, we have an additive bad reduction since..... Since the extension $K/\mathbb{Q}$ is not ramified, we have $|\Phi_2| = 4$ or $8$..... We deduce that $|\Phi_2| = 8$ and by the above corollary, $\phi_p$ is irreducible for all primes $p \geq 5$.*

*The curve has good reduction at 7 and $t_7 = -12$. We get*

*$P_7(X) = X^2 - t_7X + 49 = X^2 + 1$ (mod 3), which is irreducible modulo 3.*

*Therefore, $\varphi_3$ is irreducible. However, the representation $\varphi_2$ is reducible since $(0,0)$ is a point of order 2.* [2]

## 13. Conclusion

We have studied two articles concerning the Galois representations attached to elliptic curves. Serre's article is written in 1972 and Billerey's

article is written in 2011. In this nearly 40 years period, there has been a great progress on a very important tool that we use today in mathematics: the computers. I believe this is an important fact to consider when comparing these two articles.

Serre was more limited than todays mathematicians in the amount of calculations he could make, and he obtained some results which apply to the case of elliptic curves defined over $\mathbb{Q}$ mostly, but which requires very limited amount of calculations.

On the other hand, Billerey, as we can observe easily from his examples, obtained more general results that works for elliptic curves defined over any number field at the cost of more complicated calculations, which can be done easily with the help of a computer.

Regarding the results proved in these articles, Serre shows that there is a great difference between the Galois representations attached to elliptic curves with complex multiplication and with no complex multiplication. In the first case, their images are never surjective while in the second case, for almost all prime $l$, the representations $\varphi_l$ are surjective.

Another point I want to emphasize is that Billerey's work aims to take a step into solving Serre's uniformity question, which remains unsolved today. A partial solution to this question is give by Pierre Parent and Yuri Bilu in their article "Serre's uniformity problem in the Split Cartan Case"[8].

## References


[1] J. P. Serre, "Les propriétés galoisiennes des points des torsions des courbes elliptiques," *Inventiones mathematicae*, vol. 15, pp. 259–331, 1972.

[2] J.-P. Serre, *Abelian l-adic Representations and Elliptic Curves*. New York:Benjamin, 1968.

[3] N. Billerey, "Critères d'irréductibilité pour les représentations des courbes elliptiques," *Int. J. Number Theory*, pp. 1001–1032, 2011.

[4] J. Silverman, *The Arithmetic of Elliptic Curves*, vol. 106. Springer-Verlag, New York.

[5] J. Milne, *Elliptic Curves*. Booksurge Publishing.

[6] J. Neukirch, *Algebraic Number Theory*. Springer-Verlag.

[7] J.-P. Serre and J. Tate, "Good reduction of abelian varieties," *Ann. of Math.*, vol. 88, pp. 492–517, 1968.

[8] P. Parent and Y. Bilu, "Serre's uniformity problem in the split cartan case," *Ann. of Math.*, vol. 173, pp. 569–584, 2011.