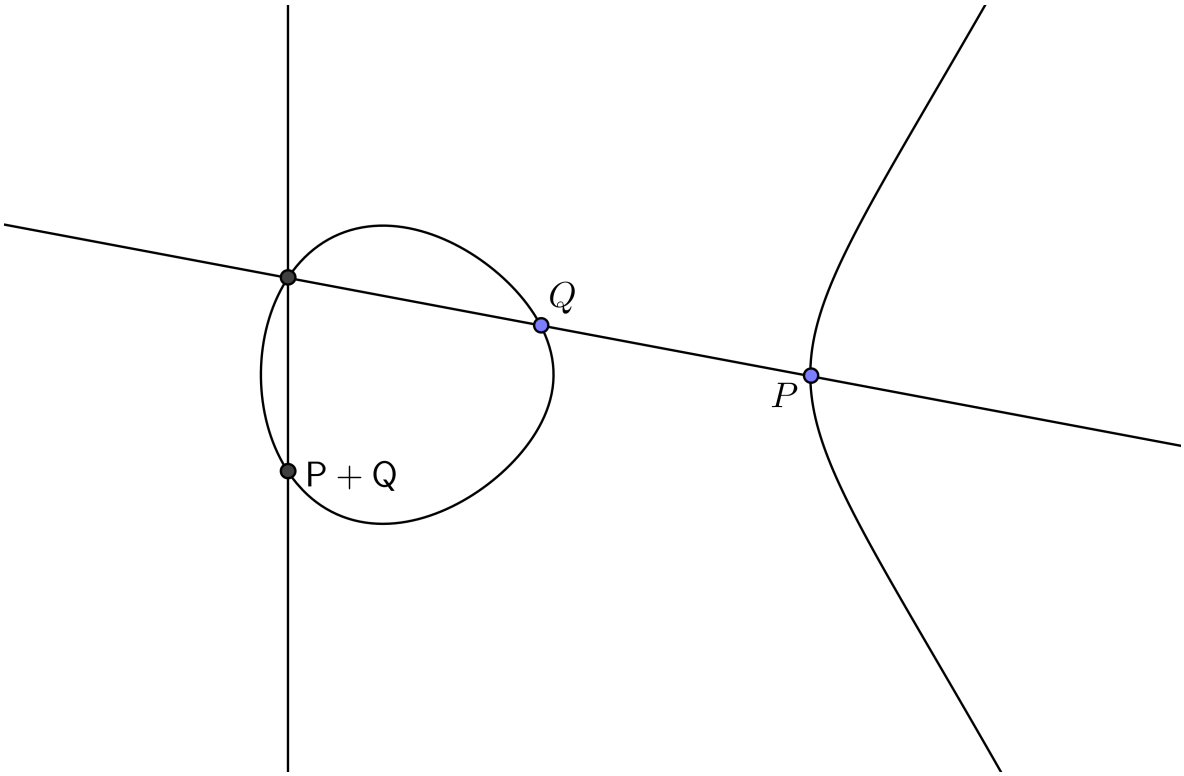
ELLIPTIC CURVES

Sara Arias de Reyna



SUMMER SCHOOL

EXPLICIT AND COMPUTATIONAL APPROACHES TO GALOIS REPRESENTATIONS

3–7 July 2018

University of Luxembourg

Version 14/07/2018

Introduction

These notes correspond to the course *Elliptic Curves* taught at the Summer School *Explicit and computational approaches to Galois representations* that took place at the University of Luxembourg, 3-7 July 2018. This course consisted of three lectures, and is focused on presenting some background material on elliptic curves and introducing the Galois representations attached to their torsion.

As such, these notes hardly contain any proof, and is rather a comprehensive collection of definitions and statements that will allow to formulate some interesting questions concerning these representations for the project sessions (included as Section 12 in these notes), and tackle them computationally. I claim no originality of any of the material presented. In fact, for most of the content, I followed the presentation in the books of Silverman [Sil92] and [Sil94], complemented with some material from Serre's book [Ser98].

I hope these notes are useful as a quick introduction to the compatible system of Galois representations attached to an elliptic curve defined over a number field. Any comments, corrections and remarks are very welcome!

Thanks to Alexander Rahm for several remarks on a previous version of these notes.

Notations

Some notations to be used thoughout the lecture notes:

K will denote a field; most of the time it will be either a number field or a local field. $\overline{K}$ denotes a (fixed) algebraic closure of K, and $G_K := \mathrm{Gal}(\overline{K}/K)$ the absolute Galois group, endowed with the Krull topology. When K is a local field, v will denote the valuation of K, usually normalised in such a way that $v(K^\times) = \mathbb{Z}$. The valuation ring will be denoted by $\mathcal{O}_K$, its maximal ideal by $\mathfrak{m}_K$ and the residue field will be usually denoted by k.

G_K acts on the projective space $\mathbb{P}^n(\overline{K})$ coordinatewise; for any $P \in \mathbb{P}^r(\overline{K})$ and $\sigma \in G_K$, we denote by P^σ the point obtained from P via the action of σ.

Given a curve C defined over a field K, and F/K a field extension, we denote by $C(F)$ the set of points of C defined over F, and $F(C)$ the field of F-rational functions of C. G_K acts on $\overline{K}(C)$ as follows; given $f \in \overline{K}(C)$, we can choose a polynomial representing it; then f^σ is obtained from f by letting σ act on its coefficients.

If C_1, C_2 are curves defined over K and $\phi : C_1 \to C_2$ a morphism of curves, then ϕ can be written as $(\phi_1, \ldots, \phi_r)$ for some $r \in \mathbb{N}$, $\phi_1, \ldots, \phi_r \in \overline{K}(C_1)$; G_K acts on ϕ coordinatewise. We denote by ϕ^σ the morphism obtained from ϕ by the action of $\sigma \in G_K$.

The image in the title page was drawn using GeoGebra 4 (`http://www.geogebra.org`)

Contents

1 Weierstrass equations

Definition 1.1. *Let K be a field. An* elliptic curve *E/K is a genus 1 curve*[1]*, endowed with a rational point $O_E \in E(K)$.*

Every elliptic curve E/K can be expressed as a plane curve given by a homogeneous equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{1.1}$$

where $a_1, a_2, a_3, a_4, a_6 \in K$ and where the point O_E corresponds to the projective point $[0 : 1 : 0]$. Such an equation is called a *Weierstrass equation for* E. Since the only point of E belonging to the infinity hyperplane $\{Z = 0\}$ is the point O_E, we will usually work with the dehomogeneization of Equation (1.1) with respect to Z, that is,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.2}$$

Weierstrass equations for E are not unique. In general, if we perform the change of variables

$$\begin{cases} x = u^2x' + r \\ y = u^3y' + u^2sx' + t \end{cases} \tag{1.3}$$

we obtain another Weierstrass equation for E. If the characteristic of K is different from 2 or 3, we can perform a particularly nice change of variables to obtain an equation of the shape

$$y^2 = x^3 + Ax + B, \tag{1.4}$$

with $A, B \in K$.

It is not true that any equation of the shape (1.2) defines an elliptic curve, since the geometric locus of the points satisfying the equation (together with the point O_E at infinity) could be a singular curve. There are two important quantities attached to a Weierstrass equation; one is the *discriminant* Δ, and another one is the *j-invariant*. Both quantities can be defined in terms of the coefficients a_1, a_2, a_3, a_4, a_6 of the equation as follows:

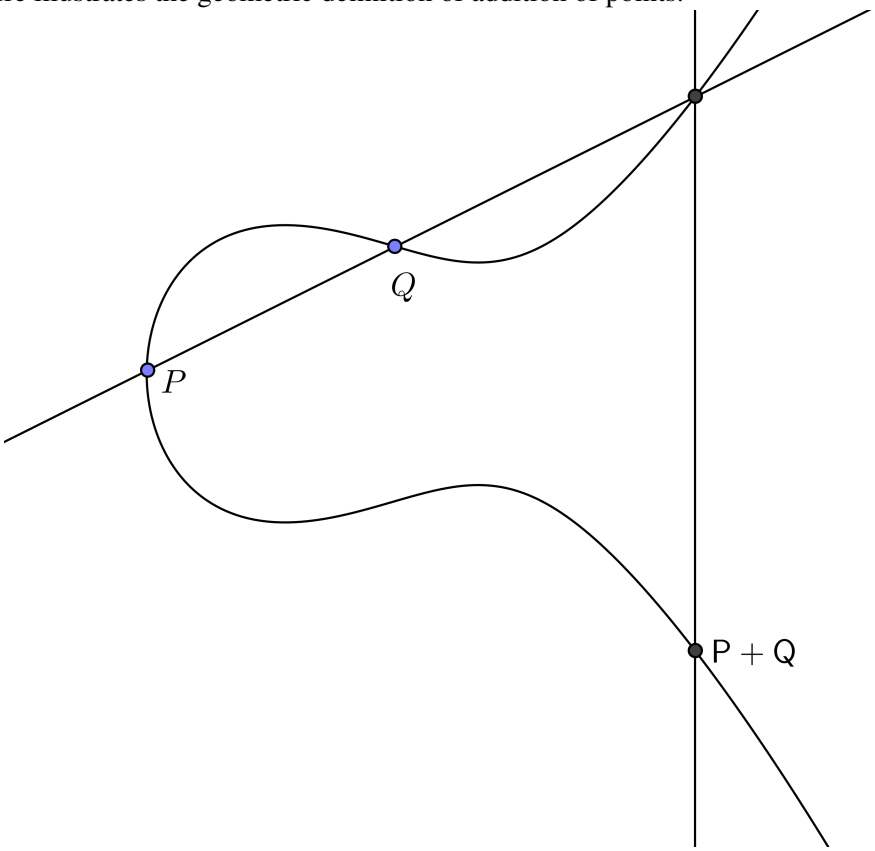
$$\begin{aligned} b_2 &:= a_1^2 + 4a_2; \\ b_4 &:= 2a_4 + a_1a_3; \\ b_6 &:= a_3^2 + 4a_6; \\ b_8 &:= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2; \\ c_4 &:= b_2^2 - 24b_4; \\ c_6 &:= b_2^3 + 36b_2b_4 - 216b_6; \\ \Delta &:= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6; \\ j &:= c_4^3/\Delta; \end{aligned}$$

[1] By a curve, we mean a smooth, projective, algebraic variety of dimension 1.

The curve defined by (1.2) is nonsingular (thus an elliptic curve) if and only if $\Delta \neq 0$. The j-invariant classifies elliptic curves up to $\overline{K}$-isomorphisms; if the j-invariant of two equations coincide, then there is an isomorphism, defined over $\overline{K}$, between the curves defined by the two equations. Thus, we can speak of the j-invariant of the elliptic curve, since it does not depend on the Weierstrass equation of the curve. For each $j_0 \in \overline{K}$ there exists an elliptic curve E defined over $K(j_0)$ such that the j-invariant of E is j_0; thus, there is a bijection between the set of equivalence classes of elliptic curves defined over $\overline{K}$ (up to isomorphism) and the set $\overline{K}$.

2 Group law and torsion points

The main feature of an elliptic curve E/K is that, for any field extension F/K, the set of F-points of E is endowed with the structure of a commutative group, where O_E is the neutral element. The next figure illustrates the geometric definition of addition of points.



The fact that $E(F)$, together with the addition defined geometrically, is a group, can be proved in a completely elementary way (but the proof of associativity requires a great amount of patience).

Given a Weierstrass equation (1.2) for E, and the (affine) coordinates of the points $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, we can express the coordinates of the sum $P_3 = (x_3, y_3) := P_1 \oplus P_2$ in terms of

The image was drawn using GeoGebra 4 (`http://www.geogebra.org`)

x_1, y_1, x_2, y_2 as follows:

$$\begin{cases} x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2; \\ y_3 = -(\lambda + a_1)x_3 - \nu - a_3; \end{cases} \tag{2.5}$$

where

$$\begin{cases} \lambda = \frac{y_2 - y_1}{x_2 - x_1}; \\ \nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}; \end{cases}$$

if $x_2 - x_1 \neq 0$; otherwise

$$\begin{cases} \lambda = \frac{3x_1 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3}; \\ \nu = \frac{-x_1^3 + a_4 x_1 + 2a_6 - a_3 y_1}{2y_1 + a_1 x_1 + a_3}; \end{cases}$$

if $x_2 = x_1$ and $2y_1 + a_1 x_1 + a_3 \neq 0$. In case $x_1 = x_2$ and $2y_1 + a_1 x_1 + a_3 = 0$ we have $P_1 + P_2 = O_E$.

From this formulae, one can see that the map $\oplus : E(\overline{K}) \times E(\overline{K}) \to E(\overline{K})$ is in fact a morphism of algebraic varieties, except at the points (P, P), $(P, -P)$, (P, O_E), (O_E, P), (O_E, O_E), where different formulae hold. However, one can check that, in fact, it is a morphism of algebraic varieties (cf. [Sil92, Remark 3.6.1, Chapter III]). The oposite of an (affine) point (x_0, y_0) can be computed as follows: $-P = (x_0, -y_0 - a_1 x_0 - a_3)$. Thus, the map $- : E(\overline{K}) \to E(\overline{K})$ mapping P to $-P$ is also a morphism of algebraic varieties.

Another way to introduce the addition law on E is by means of divisors. Given E/K an elliptic curve, we define the group $\mathrm{Div}(E)$ as the free abelian group generated by the points of $E(\overline{K})$. Denoting by (P) the divisor corresponding to the point P, any divisor D can be expressed as a finite sum

$$D = \sum_{i=1}^{n} a_n (P_n),$$

where $n \in \mathbb{N}$, $a_1, \ldots, a_n \in \mathbb{Z}$, $P_1, \ldots, P_n \in E(\overline{K})$. For such a divisor D we define its degree as $\deg D = \sum_{i=1}^{n} a_n \in \mathbb{Z}$; the subset of degree-0 divisors is a subgroup of $\mathrm{Div}(E)$, denoted by $\mathrm{Div}^0(E)$.

Given a rational function $f \in \overline{K}(E)$, which is not constantly equal to zero, one can attach to it a divisor in the following way: if $P_1, \ldots, P_n$ are the points where f vanishes and $Q_1, \ldots, Q_m$ are the points where f has a pole, we set

$$\mathrm{div}(f) := \sum_{i=1}^{n} a_i (P_i) - \sum_{j=1}^{m} b_j (Q_j),$$

where for each $i = 1, \ldots, n$, a_i is the order of vanishing of f at P_i, and for each $j = 1, \ldots, m$, b_j is the order of f at the pole Q_j. The divisors of the form $D = \mathrm{div}(f)$ for $f \in \overline{K}(E) \setminus \{0\}$ are called *principal divisors*, and they for a subgroup of $\mathrm{Div}(E)$. It holds that, for any $f \in \overline{K}(E)$ not identically zero, $\deg \mathrm{div}(f) = 0$ (cf. [Har77, (II.6.10)]).

Now we can define an equivalence relation in $\mathrm{Div}(E)$ as follows: $D_1 \sim D_2$ if and only if there exists $f \in \overline{K}(E)$, non-identically zero, such that $D_1 = D_2 + \mathrm{div}(f)$. The quotient group, denoted by $\mathrm{Pic}(E)$, is called the *Picard group* of E. Since the subgroup of principal divisors is contained in

$\mathrm{Div}^0(E)$, we can also consider the quotient $\mathrm{Pic}^0(E)$ of $\mathrm{Div}^0(E)$ by the equivalence relation above; we obtain a subgroup $\mathrm{Pic}^0(E) \subset \mathrm{Pic}(E)$.

We have the following exact sequence

$$1 \to \overline{K} \setminus \{0\} \to \overline{K}(E) \setminus \{0\} \to \mathrm{Div}^0(E) \to \mathrm{Pic}^0(E) \to 0.$$

Given a field extension F/K, the Galois group $\mathrm{Gal}(\overline{K}/F)$ acts naturally on $E(\overline{K})$. This action carries through to an action on $\mathrm{Div}(E)$, and we can consider the subset $\mathrm{Div}_F(E) = \{D \in \mathrm{Div}(E) : D^\sigma = D \text{ for all } \sigma \in \mathrm{Gal}(\overline{K}/F)\}$. Since the group of principal divisors is preserved by the Galois action, we can also consider the subset $\mathrm{Pic}_F(E) = \{[D] \in \mathrm{Pic}(E) : D \in \mathrm{Div}_F(E)\}$ (where $[D]$ denotes the equivalence class of D in the quotient group) and $\mathrm{Pic}^0_F(E) = \{[D] \in \mathrm{Pic}^0(E) : D \in \mathrm{Div}_F(E)\}$. All these subsets are subgroups. Moreover, it can be proved (but is not trivial, cf. [Sil92, Ex. II.2.13]) that $\mathrm{Pic}^0_F(E)$ is the quotient group of $\mathrm{Div}^0_F(E)$ by $F(E) \setminus \{0\}$.

Now, $\mathrm{Div}^0(E)$ and $\mathrm{Div}^0_F(E)$ are naturally abelian groups, and we can make use of this group law to define a group law on the set of points in the elliptic curve. We need the following proposition (cf. [Sil92, (III.3.4(a))]).

Proposition 2.1. *For every $D \in \mathrm{Div}^0(E)$ there exists a unique point $P \in E(\overline{K})$ such that $D \sim (P) - (O_E)$. Thus, we obtain a bijection*

$$\Psi : \mathrm{Pic}^0(E) \to E(\overline{K})$$

such that $\Psi((P) - (O_E)) = P$.

Using the bijection Ψ, we can define a group law $\oplus : E(\overline{K}) \times E(\overline{K}) \to E(\overline{K})$ by $P_1 \oplus P_2 = \Psi(\Psi^{-1}(P_1) + \Psi^{-1}(P_2))$. It turns out that this addition law coincides with the addition law defined geometrically using a Weierstrass equation (2.5). Note that, in particular, this result shows that the addition law defined in terms of the coefficients of a Weierstrass equation for E does not depend on the choice of equation, but is an intrinsic feature of the curve.

3 Isogenies

In this section we consider morphisms between elliptic curves. We start with the definition of isogeny.

Definition 3.1. *Let $E_1, E_2/\overline{K}$ be elliptic curves. An* isogeny *between E_1 and E_2 is a morphism of algebraic varieties, $\phi : E_1 \to E_2$, such that $\phi(O_{E_1}) = O_{E_2}$.*

Remark 3.2. *In the definition of isogeny, we are not asking that ϕ induces a group morphism between $E_1(\overline{K})$ and $E_2(\overline{K})$. However, it turns out that every isogeny is also a group morphism; this is a consequence of the definition of isogeny (cf. [Sil92, (III.4.8)]).*

Remark 3.3. *Let $\phi : E_1 \to E_2$ be an isogeny. There are two possibilities: either ϕ is a constant map (thus constantly equal to O_{E_2}), or else it is a* surjective *map (cf. [Har77, (II.6.8)]). Assume we are in*

the second case. Recall that ϕ, as a morphism of algebraic varieties, defines a map ϕ^* from the field of rational functions of E_2 to the field of rational functions of E_1 by composition, $\phi^* : \overline{K}(E_2) \to \overline{K}(E_1)$, $f \mapsto f \circ \phi$. Since ϕ is surjective, the map ϕ^* is an injection, thus we obtain an inclusion of fields $\phi^*(\overline{K}(E_2)) \subset \overline{K}(E_1)$. This extension of fields has finite degree (cf. [Har77, (II.6.8)]); the degree of *ϕ is defined as*

$$\deg \phi := [\overline{K}(E_1) : \phi^* \overline{K}(E_2)].$$

We can write $\deg \phi$ as the product of the separable degree $\deg_s \phi$ (defined as the separable degree of the extension $\overline{K}(E_1)/\phi^*\overline{K}(E_2)$) and the inseparable degree $\deg_i(\phi)$ (defined as the inseparability degree of $\overline{K}(E_1)/\phi^*\overline{K}(E_2)$).

When ϕ is a non-constant isogeny, it holds that $\ker(\phi) = \phi^{-1}(O_{E_2})$ is a finite group, whose cardinality coincides with $\deg_s \phi$ (cf. [SZ14, Theorem 1.4.1] for a proof in the separable case).

If E_1, E_2 are elliptic curves defined over K, we can consider the isogenies defined over K, that is to say, the set of isogenies $\phi : E_1 \to E_2$ such that, for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$, $\phi^\sigma = \phi$.

Example 3.4. *Let E/K be an elliptic curve. For any $m \in \mathbb{Z}$, we can define a map:*

$$\begin{aligned} [m] : E(\overline{K}) &\to E(\overline{K}) \\ P &\mapsto P + \underbrace{\cdots}_{m \text{ times}} + P. \end{aligned}$$

Since the addition in E is a morphism of algebraic varieties, $[m]$ is also a morphism of algebraic varieties from E to E. Clearly, $[m](O_E) = O_E$. Thus, $[m]$ is an isogeny. If $m \neq 0$, the isogeny $[m]$ is not constant, of degree m^2 (cf. [Sil92, (III.6.2-(d))]).

We denote by $\mathrm{Hom}(E_1, E_2)$ the set of isogenies from E_1 to E_2. This set is endowed with the structure of an abelian group; namely, for each $\phi_1, \phi_2 \in \mathrm{Hom}(E_1, E_2)$, we can define $\phi_1 + \phi_2$ by the formula $(\phi_1 + \phi_2)(P) := \phi_1(P) + \phi_2(P)$. It turns out that $\mathrm{Hom}(E_1, E_2)$ is a torsion-free $\mathbb{Z}$-module (cf. [Sil92, (III.4.2-(b))]).

If we look at isogenies from an elliptic curve into itself, we obtain the group of endomorphisms of E, denoted by $\mathrm{End}(E)$. In this group there is another operation, namely the composition of isogenies. Thus, $\mathrm{End}(E)$ is endowed with the structure of a (non-necessarily commutative) ring. Example 3.4 provides an injection $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$. If $\mathrm{End}(E)$ is strictly larger than $\mathbb{Z}$, we say that E has *complex multiplication*. Note that, for all $\phi \in \mathrm{End}(E)$ and $m \in \mathbb{Z}$, it holds that

$$[m] \circ \phi = \phi \circ [m].$$

If there exists a non-constant isogeny between two elliptic curves E_1 and E_2, we say that E_1 and E_2 are *isogenous*. Being isogenous is an equivalence relationship. The reflexive and transitive properties are clear (because the identity is an isogeny, and the composition of two isogenies is an isogeny). The fact that the symmetric property holds is more interesting: if there is an isogeny $\phi : E_1 \to E_2$, then there is another isogeny $\psi : E_2 \to E_1$. In fact, one can prove the following (cf. [Sil92, III.6.1] for a proof in the separable case).

Proposition 3.5. *Let $\phi : E_1 \to E_2$ be a non-constant isogeny of degree m. Then there is a unique isogeny, called the* dual isogeny*,*

$$\widehat{\phi} : E_2 \to E_1$$

such that $\widehat{\phi} \circ \phi = [m]$.

Moreover, if E_1, E_2 and ϕ are defined over K, it can be shown that $\widehat{\phi}$ is also defined over K (because ϕ is surjective and $[m]$ is defined over K). It holds that

$$\widehat{\widehat{\phi}} = \phi.$$

4 Torsion points of E

Let E/K be an elliptic curve. For each $m \in \mathbb{Z}_{>0}$, we can consider the set of *m-torsion points of E*,

$$E[m] := \ker[m] = \{P \in E(\overline{K}) : P + \underbrace{\cdots}_{m \text{ times}} + P = O_E\}.$$

By definition, this set is a subgroup of $E(\overline{K})$, whose structure is given as follows (cf. [Sil92, (III.6.4)])

Proposition 4.1. *1. If $\mathrm{char}K = 0$ or $\mathrm{char}K$ does not divide m, then*

$$E[m] \simeq (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$$

2. If $\mathrm{char}K = p > 0$, there are two possibilities for $E[p]$:

(a) $E[p] = \{O_E\}$ or

(b) $E[p] \simeq \mathbb{Z}/p\mathbb{Z}$.

In the first case, $E[p^e] = \{0\}$ for all $e \in \mathbb{Z}_{>0}$; in the second case, $E[p^e] \simeq \mathbb{Z}/p^e\mathbb{Z}$ for all $e \in \mathbb{Z}_{>0}$.

Since $[m]$ is defined over K, the group $E[m]$ is stable under the action of G_K. In particular, when $m = \ell$ is a prime number, different from $\mathrm{char}K$, then $E[\ell]$ is a 2-dimensional $\mathbb{F}_\ell$-vector space, and the action of G_K gives rise to a representation

$$\overline{\rho}_{E,\ell} : G_K \to \mathrm{GL}(E[\ell]) \simeq \mathrm{GL}_2(\mathbb{F}_\ell).$$

Let $K(E[\ell])$ be the field extension generated over K by the coordinates of the ℓ-torsion points of E. It is clear that the above representation factors through $\mathrm{Gal}(K(E[\ell])/K)$, thus $\overline{\rho}_{E,\ell}$ is *continuous* with respect to the Krull topology on the left hand side and the discrete topology on the right hand side.

Remark 4.2. *Note that $\mathrm{Gal}(K(E[\ell])/K) \simeq \mathrm{Im}\overline{\rho}_{E,\ell}$. Thus, the group $\mathrm{Im}\overline{\rho}_{E,\ell}$ can be realized as a Galois group over the field K. For example, Serre proves [Ser72, Example 5.5.6] that the elliptic curve defined over $\mathbb{Q}$ by the Weierstrass equation $y^2 + y = x^3 + x$ satisfies that, for all prime $\ell \geq 2$, $\mathrm{Im}\overline{\rho}_{E,\ell} \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$. Thus, all these groups can be realized as Galois groups over $\mathbb{Q}$.*

When E is an elliptic curve defined over a number field, the study of $\mathrm{Im}\overline{\rho}_{E,\ell}$ (for ℓ a prime number) is an active research topic. We have the following fundamental result of Serre (cf. [Ser72]).

Theorem 4.3 (Serre, 1972)**.** *Let K be a number field and E/K be an elliptic curve without complex multiplication. Then $\overline{\rho}_{E,\ell}$ is surjective for all except finitely many primes ℓ.*

For more details, look at the first project in Section 12.

Remark 4.4. *For the second project in Section 12, we will need the following fact: If $\phi : E_1 \to E_2$ is a nonzero isogeny defined over K, and if $m \in \mathbb{Z}_{\geq 2}$ is such that $\gcd(m, \mathrm{char}(K)) = 1$, $\gcd(m, \deg\varphi) = 1$, then ϕ induces an isomorphism of Galois modules between $E_1[m]$ and $E_2[m]$. Indeed, we have that $[\deg\phi] : E_1[m] \to E_1[m]$ is an isomorphism of Galois modules, and $\phi \circ \widehat{\phi} = \widehat{\phi} \circ \phi = [\deg\phi]$.*

5 The Tate module of E

Let ℓ be a prime. Informally, we can define the *ring* of ℓ-adic integers as the set of infinite ℓ-adic expansions

$$\mathbb{Z}_\ell := \left\{ \sum_{n=0}^{\infty} a_n \ell^n : a_0, a_1, \cdots \in \{0, \ldots, \ell - 1\} \right\},$$

endowed with a natural addition and product (these operations are well defined, since to compute the n-th term of the sum or product of two infinite series, only a finite number of operations is involved).

In a formal way, we can consider the collection of rings $\{\mathbb{Z}/\ell^n\mathbb{Z} : n \in \mathbb{N}\}$ and the connecting maps between them:

$$\pi_{n+1} : \mathbb{Z}/\ell^{n+1}\mathbb{Z} \to \mathbb{Z}/\ell^n\mathbb{Z}.$$
$$x + \ell^{n+1}\mathbb{Z} \mapsto x + \ell^n\mathbb{Z}$$

Then we can form the inverse limit

$$\varprojlim_{n\to\infty} \mathbb{Z}/\ell^n\mathbb{Z}.$$

In a similar way, we want to collect all the G_K-modules $E[\ell^n]$, for $n \in \mathbb{N}$, attached to an elliptic curve E/K, into a single object.

Definition 5.1. *Consider the collection of groups $\{E[\ell^n] : n \in \mathbb{N}\}$ and the connecting maps $[\ell] : E[\ell^{n+1}] \to E[\ell^n]$ among them. We define the* ℓ-adic Tate module *of E as*

$$T_\ell(E) = \varprojlim_{n\to\infty} E[\ell^n].$$

By definition, $T_\ell(E)$ has a $\mathbb{Z}$-module structure, since it is the inverse limit of groups. It is easy to check that this structure extends to a $\mathbb{Z}_\ell$-module structure; if $(\alpha_n + \ell^n\mathbb{Z})_{n\in\mathbb{N}} \in \varprojlim \mathbb{Z}/\ell^n\mathbb{Z}$ and $(P_n)_{n\in\mathbb{N}} \in T_\ell(E)$, then we can define the product

$$(\alpha_n)_{n\in\mathbb{N}} \cdot (P_n)_{n\in\mathbb{N}} := ([\alpha_n]P_n)_{n\in\mathbb{N}}.$$

If $\ell \neq \mathrm{char}(K)$, we have that $T_\ell(E)$ is a free $\mathbb{Z}_\ell$-module of rank 2. Moreover, $T_\ell(E)$ is endowed with an action of G_K, where each $\sigma \in G_K$ acts as $(P_n)_{n\geq 0} \mapsto (P_n^\sigma)_{n\geq 0}$. Thus, we obtain a Galois representation

$$\rho_{E,\ell} : G_K \to \mathrm{GL}(T_\ell(E)) \simeq \mathrm{GL}_2(\mathbb{Z}_\ell).$$

It holds that $\rho_{E,\ell}$ is a continuous Galois representation, when we consider on $\mathrm{GL}_2(\mathbb{Z}_\ell)$ the ℓ-adic topology (cf. [Sil92, Section III.7]).

Since the representations theory of a group with coefficients in a field is easier than if we take coefficients on $\mathbb{Z}_\ell$, we consider also the $\mathbb{Q}_\ell$-vector space $V_\ell(E) = \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell(E)$, and extend the representation $\rho_{E,\ell}$ to a representation (denoted in the same way) $\rho_{E,\ell} : G_K \to \mathrm{GL}(V_\ell(E)) \simeq \mathrm{GL}_2(\mathbb{Q}_\ell)$.

For each prime ℓ, we have a representation $\rho_{E,\ell}$. These representations are related to each other in a very precise way; namely, they form a so-called strongly compatible system (see Definition 8.4 below). In order to formulate the definition of this concept, we need to make a review of the ramification theory of extensions of number fields (see Section 7), as well as the theory of reduction of elliptic curves (see Section 6).

Endomorphisms of the elliptic curve E give rise to endomorphisms of $T_\ell(E)$ as a $\mathbb{Q}_\ell$-vector space. For future use, we state the following result (cf. [Sil92, (III.8.6)]):

Proposition 5.2. *Let E/K be an elliptic curve, $\phi \in \mathrm{End}_K(E)$. For $\ell \neq \mathrm{char}(K)$ a prime number, let $\phi_\ell : T_\ell(E) \to T_\ell(E)$ be the morphism induced on the ℓ-adic Tate module, and denote by $\mathrm{trace}(\phi_\ell)$, $\det(\phi_\ell)$ the trace and determinant of ϕ_ℓ as a morphism of $\mathbb{Q}_\ell$-vector spaces. Then*

$$\begin{aligned} \det(\phi_\ell) &= \deg(\phi) \\ \mathrm{trace}(\phi_\ell) &= 1 + \deg(\phi) - \deg(1-\phi) \end{aligned} \tag{5.6}$$

In particular, the elements $\mathrm{trace}(\phi_\ell), \det(\phi_\ell) \in \mathbb{Z}$ and are independent of ℓ.

6 Reduction of elliptic curves defined over a local field

Let K_v be a local field, with valuation ring $\mathcal{O}_v$, maximal ideal $\mathfrak{m}_v$, and residue field k_v. For further use, we fix a uniformising element π. Consider an elliptic curve E/K_v. We want to study the reduction of E modulo $\mathfrak{m}_v$. To reduce the curve modulo $\mathfrak{m}_v$, the first thing we need is a Weierstrass equation of E whose coefficients are all in $\mathcal{O}_{K_v}$. We can easily achieve this as follows: fix a Weierestrass equation (1.2), and make a change of variables (1.3) with u divisible by a sufficiently high power of π, say $(x, y) \mapsto (u^{-2}x, u^{-3}y)$; then a_i is replaced by $a_i u^i$. Now that we have an equation whose coefficients are all in $\mathcal{O}_{K_v}$, we can look at the reduction of the equation modulo $\mathfrak{m}_v$, and we obtain a new Weierstrass equation

$$y^2 + \widetilde{a}_1 xy + \widetilde{a}_3 y = x^3 + \widetilde{a}_2 x^2 + \widetilde{a}_4 x + \widetilde{a}_6. \tag{6.7}$$

where $\widetilde{a}_1, \widetilde{a}_2, \widetilde{a}_3, \widetilde{a}_4, \widetilde{a}_6 \in k_v$. If the discriminant $\widetilde{\Delta}$ of this equation is nonzero, then it defines an elliptic curve over k_v, which we will call the *reduction of E*. However, the vanishing of $\widetilde{\Delta}$ depends

on the Weierstrass equation (1.3) chosen, as well as on the change of variables performed. The discriminant Δ of the original equation is replaced by $u^{12}\Delta$; if we replace u by an even higher power of π, we might even get that all coefficients $\widetilde{a}_i$ vanish. We address this issue by defining a *minimal Weierstrass equation for* E to be an equation of the shape (1.2), such that all $a_i \in \mathcal{O}_{K_v}$, and such that $v(\Delta)$ is minimal amongst the possible values of $v(\Delta)$, when Δ is the discriminant of such an equation. Thus, the vanishing of a discriminant of a minimal Weierstrass equation is well-defined. There is a characterisation of minimal Weierstrass equations when $\mathrm{char} k_v \neq 2, 3$ (cf. [Sil92, Remark 1.1, Chapter VII]):

Proposition 6.1. *Let E/K_v be an elliptic curve, defined by a Weierstrass equation* (1.2) *with all $a_i \in \mathcal{O}_{K_v}$. Then the following are equivalent:*

(i) Equation (1.2) *is a minimal Weierstrass equation.*

(ii) $v(\Delta) < 12$ or $v(\Delta) = 12$ and $v(c_4) < 4$.

Definition 6.2. *Let E/K_v be an elliptic curve and Equation* (1.2) *a minimal Weierstrass equation. Then the curve $\widetilde{E}$ defined over k_v by Equation* (6.7) *is called the* reduction of E. *If $\widetilde{\Delta} \neq 0$, then $\widetilde{E}$ is an elliptic curve, and we say that E has good reduction (at v). Otherwise, we say that E has bad reduction (at v).*

In the case when $\widetilde{\Delta} = 0$, the curve $\widetilde{E}$ is a singular curve. According to the type of singularity, we can distinguish two cases:

1. E has multiplicative reduction if $\widetilde{E}$ has a node (two different tangent lines at the singularity). In this case, the reduction is called *split* if the slopes of the tangent lines at the node belong to K_v; otherwise it is called *nonsplit*.

2. E has additive reduction if $\widetilde{E}$ has a cusp (a single tangent line at the singularity).

We will say that E has *semistable reduction* if the reduction of E is either good or multiplicative.

The first case is characterised by the conditions $\widetilde{\Delta} = 0$ and $\widetilde{c}_4 \neq 0$; in the second case $\widetilde{\Delta} = 0 = \widetilde{c}_4$ (cf. [Sil92, (VII.5.1)]). We say that E has *semistable* reduction if E has either good or multiplicative reduction.

Assume L_w/K_v is a finite extension. An elliptic curve E defined over K_v can be considered to be defined over L_w; this is called a *base change* or *extension of scalars*. We denote the elliptic curve obtained from E by extending scalars from K_v to L_w as $L_w \otimes_{K_v} E$, when it is necessary to distinguish it from E. The type of reduction can change after a finite base change, but there are certain rules that are followed (cf. [Sil92, (VII.5.4-(a, b))]).

1. If L_w/K_v is an unramified extension, $L_w \otimes_{K_v} E$ has the same type of reduction (good, multiplicative or additive) as E.

2. If E has good (resp. multiplicative) reduction over K_v, then $L_w \otimes_{K_v} E$ has the good (resp. multiplicative) reduction.

In general, we will say that E has *potential good reduction* (resp. *potential multiplicative reduction*) if, after a finite base change, the curve acquires good (resp. multiplicative) reduction. An important result, which can be stated and proved in much greater generality, addresses the case of additive reduction (cf. [Sil92, (VII.5.4-(c))]):

Theorem 6.3 (Semistable reduction theorem)**.** *Let E/K_v be an elliptic curve. Then there exists a finite extension L_w/K_v such that $L_w \otimes_{K_v} E$ has semistable reduction.*

These results show that the fact that the (potential) reduction is good or semistable is independent on the base field on which E is defined, and should be read from the j-invariant of the curve. Indeed, this is the case, as the next proposition shows (cf. [Sil92, (VII.5.5)]):

Proposition 6.4. *Let E/K_v be an elliptic curve. Then E has potential good reduction if and only if its j-invariant satisfies $j \in \mathcal{O}_{K_v}$.*

7 Interlude on Galois theory

Let K be a number field, with ring of integers $\mathcal{O}_K$. Each nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ gives rise to a discrete valuation $v_\mathfrak{p}$ on the field K. Such valuations will be called *finite places of K*, and the set of all finite places will be denoted by Σ_K. Further, for each $v = v_\mathfrak{p} \in \Sigma_K$, we denote by k_v the residue field of v, defined as $\mathcal{O}_K/\mathfrak{p}$.

Let L/K be a finite Galois extension and denote by $G := \mathrm{Gal}(L/K)$ its Galois group. For any $v \in \Sigma_K$, there exist only finitely many places $w \in L$ extending the valuation $v \in K$. We write $w|v$ to denote that $w|_K = v$. The subgroup $D_w := \{\sigma \in G : w \circ \sigma = w\}$ is called the *decomposition group of w*. If $w_1, w_2|v$, then D_{w_1} and D_{w_2} are conjugate subgroups. By abuse of notation, we will write D_v to denote a representative in this conjugacy class.

If we denote by K_v (resp. L_w) the completion of K at v (resp. of L at w), the inclusion map $L \hookrightarrow L_w$ induces an isomorphism of groups $\mathrm{Gal}(L_w/K_v) \to D_w$. Thus, to study D_w, we can make use of extensions of local fields, which are much easier to handle than global fields.

The reduction map $\mathcal{O}_{L_w} \to k_w$ from $\mathcal{O}_{L_w}$ into its residue field induces a surjective morphism $\mathrm{Gal}(L_w/K_v) \to \mathrm{Gal}(k_w/k_v)$. Now, the group $\mathrm{Gal}(k_w/k_v)$ has a very easy structure: it is a cyclic group, with a distinguished generator Frob_w, defined as follows: if $\mathrm{card}(k_v) = p^f$, then $\mathrm{Frob}_w(a) = a^{p^f}$. By definition, the kernel of the projection $\mathrm{Gal}(L_w/K_v) \to \mathrm{Gal}(k_w/k_v)$ is the *inertia group at w*, which we denote by I_w. We have an exact sequence:

$$1 \to I_w \to \mathrm{Gal}(L_w/K_v) \to \mathrm{Gal}(k_w/k_v) \to 1.$$

For all except finitely many v, it turns out that $I_w = \{\mathrm{id}\}$, thus $\mathrm{Gal}(L_w/K_v)$ is cyclic, generated by an element projecting onto Frob_w, which by abuse of notation we also denote by Frob_w. Since all

D_w are conjugate for $w|v$, we have a well-defined conjugacy class in $\mathrm{Gal}(L/K)$, which we denote by Frob_v. However, for a finite set of places of K, it can happen that I_w is not trivial; those are the places corresponding to primes $\mathfrak{p}$ of K such that $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^e \cdot \cdots \cdot \mathfrak{P}_r^e$ with $e \neq 1$; in other words, those are the primes that ramify in the extension L/K.

These notions carry through to the case where L is an *infinite* Galois extension of K. In particular, fix an algebraic closure of K. For each $v \in \Sigma_K$, the sets $\{\Sigma_L : L/K \text{ finite Galois}\}$ form a projective system with respect to restriction; we can consider the projective limit $\Sigma_{\overline{K}} = \lim_{\leftarrow} \Sigma_L$. For each $\overline{w} \in \Sigma_{\overline{K}}$, we can define $D_{\overline{w}}$ as before; we have an isomorphism $D_{\overline{w}} \simeq \mathrm{Gal}(\overline{K}_v/K_v)$, and an exact sequence

$$1 \to I_v \to \mathrm{Gal}(\overline{K}_v/K_v) \to \mathrm{Gal}(\overline{k}_v/k_v) \to 1.$$

where I_v is by definition the kernel of the projection. The fixed field of $\overline{K}_v$ by I_v is the maximal unramified subfield of $\overline{K}_v$ containing K_v, denoted by K_v^{unr}; thus

$$I_v = \mathrm{Gal}(\overline{K}_v/K_v^{\mathrm{unr}}).$$

Let p be the residue characteristic of K_v. The *wild inertia group* is the maximal pro-p-subgroup of I_v, denoted I_v^{wild}. We denote by K_v^{tame} the fixed field of $\overline{K}_v$ by I_v^{wild}; it is the maximal tamely ramified subfield of $\overline{K}_v$ containing K_v, and satisfies that $I_v^{\mathrm{wild}} = \mathrm{Gal}(\overline{K}_v/K_v^{\mathrm{tame}})$. If π denotes a uniformising element of K_v, then we can describe K_v^{tame} as

$$K_v^{\mathrm{tame}} = K_v^{\mathrm{unr}}(\{\pi^{1/d} : p \nmid d\}).$$

Finally, we define the tame inertia group I_v^{tame} as the quotient $I_v/I_v^{\mathrm{wild}} \simeq \mathrm{Gal}(K_v^{\mathrm{tame}}/K_v^{\mathrm{unr}})$.

In order to define the conductor of an elliptic curve (Definition 9.1 below), we need a refinement of the wild inertia group, the so-called *higher ramification groups*. The natural setting for this definition is a finite extension of local fields, like L_w/K_v.

Definition 7.1. *Let L/K be a finite Galois extension of local fields, with valuations $w|v$, and denote by $v_L = ew$ the normalization of w, so that $v_L(L^\times) = \mathbb{Z}$. Then for each $i \in \mathbb{Z}_{\geq -1}$ we define the* i-th *ramification group as*

$$G_i(L/K) := \{\sigma \in \mathrm{Gal}(L/K) : v_L(\sigma(a) - a) \geq i + 1 \textit{ for all } a \in \mathcal{O}_L\}.$$

Note that the higher ramification groups form a descending sequence

$$\mathrm{Gal}(L/K) = G_{-1}(L/K) \supseteq G_0(L/K) \supseteq G_1(L/K) \supseteq \cdots$$

of normal subgroups of $\mathrm{Gal}(L/K)$.

Remark 7.2. *When L/K is a finite Galois extension of number fields, and $w|v$ are finite places, it holds that $G_{-1}(L_w/K_v) = D_w$, $G_0(L_w/K_v) = I_w$ and $G_1(L_w/K_v) = I_w^{\mathrm{wild}}$ (cf. [Neu99, (II.9.12)]).*

8 Compatible systems of Galois representations attached to the torsion of an elliptic curve

Let E be an elliptic curve defined over a number field K. For each prime ℓ, we have attached to E an ℓ-adic Galois representation $\rho_{E,\ell} : G_K \to \mathrm{GL}_2(\mathbb{Q}_\ell)$ We denote by

$$\rho_{E,\bullet} := \{\rho_{E,\ell} : G_K \to \mathrm{GL}_2(\mathbb{Q}_\ell)\}_{\ell \text{ prime number}}$$

the set of all these representations. Even though they are representations into different groups, they share many properties, since they all come from the elliptic curve E. In this section we formulate this relationship more precisely. The key observation is that, for each finite place v of K, the type of reduction of E at v carries information about the image of the decomposition group D_v by the representation $\rho_{E,\ell}$. The main result in this regard is the following, known as the Néron-Ogg-Shafarevich criterion (cf. [Sil92, (VII.7.1)]).

Theorem 8.1 (Néron-Ogg-Shafarevich)**.** *Let E be an elliptic curve defined over a number field K, v a finite place of K. The following are equivalent:*

1. *E has good reduction at v.*
2. *For all primes ℓ with $v \nmid \ell$, $\rho_{E,\ell} : G_K \to \mathrm{GL}(T_\ell(E))$ is unramified at v.*
3. *For some prime ℓ with $v \nmid \ell$, $\rho_{E,\ell} : G_K \to \mathrm{GL}(T_\ell(E))$ is unramified at v.*

In the setting of the above theorem, fix a prime ℓ, and choose a place $v \nmid \ell$ of good reduction for E. Denote by k_v the residue field of K at v, and pick an element $\mathrm{Frob}_v \in D_v$ projecting onto the Frobenius map in $\mathrm{Gal}(\overline{k}_v/k_v)$. Then by the Néron-Ogg-Shafarevich criterion, the image of I_v is trivial, thus the image of Frob_v is a well-defined element in $\mathrm{GL}(T_\ell(E))$ up to conjugacy, and the characteristic polyomial $\mathrm{charpoly}(\rho_{E,\ell}(\mathrm{Frob}_v))$ is well defined. We can give a precise description of this polynomial:

Proposition 8.2. *Let E be an elliptic curve defined over a number field K, ℓ a prime number and $v \nmid \ell$ a finite place of K of good reduction for E. Let $\mathrm{Frob}_v \in D_v$ be an element of G_K projecting onto the Frobenius map in $\mathrm{Gal}(\overline{k}_v/k_v)$. Then*

$$\mathrm{charpoly}(\rho_{E,\ell}(\mathrm{Frob}_v)) = T^2 - a_v T + \mathrm{N}v,$$

where

$$\begin{aligned} \mathrm{N}v &:= \mathrm{card}(k_v), \text{ and} \\ a_v &:= 1 + \mathrm{N}v - \mathrm{card}(\widetilde{E}(k_v)). \end{aligned} \tag{8.8}$$

Remark 8.3. *The quantity a_v can be interpreted as the deviation of the number of points of $\widetilde{E}$ over k_v from the "expected value" $1 + \mathrm{N}v$. Note that Proposition 8.2 shows, in particular, that $\mathrm{charpoly}(\rho_{E,\ell}(\mathrm{Frob}_v))$ depends only on the reduction $\widetilde{E}$ of E at the finite place v.*

Proof. First, we need to compare the Galois representations $\rho_{E,\ell}$ and $\rho_{\widetilde{E}_v,\ell}$, for a place $v \nmid \ell$ of good reduction for E. For all $\sigma \in D_v$, denote by $\widetilde{\sigma} \in \mathrm{Gal}(\overline{k}_v/k_v)$ its projection. Choosing compatible bases for $T_\ell(E) \simeq \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ and $T_\ell(\widetilde{E}_v) \simeq \mathbb{Z}_\ell \times \mathbb{Z}_\ell$, we obtain that, for all $\sigma \in D_v$, $\rho_{E,\ell}(\sigma) = \rho_{\widetilde{E}_v,\ell}(\widetilde{\sigma})$. In particular, if we denote by $\alpha : \overline{k}_v \to \overline{k}_v$ the morphism mapping $x \mapsto x^{Nv}$, we have that $\rho_{E,\ell}(\mathrm{Frob}_v) = \rho_{\widetilde{E}_v,\ell}(\alpha)$. Thus, it suffices to compute $\mathrm{charpoly}(\rho_{\widetilde{E}_v,\ell}(\alpha))$.

Since $\mathrm{char}(K) > 0$, we can define an *isogeny* $\psi : \widetilde{E}_v \to \widetilde{E}_v$ by $P = (x, y) \mapsto (x^{Nv}, y^{Nv})$; this isogeny is related to α as follows: if $(P_n)_n \in T_\ell(\widetilde{E})$,

$$\rho_{\widetilde{E}_v,\ell}(\alpha)((P_n)_n) = (\psi(P_n))_n.$$

Now we can apply Proposition 5.2 to the endomorphism ψ to conclude that $\det \alpha = \deg \psi$ and $\mathrm{trace}(\alpha) = 1 + \deg(\psi) - \deg(1 - \psi)$. But we know that $\deg \psi = \mathrm{card}(k_v) = N_v$ (cf. [Sil92, (II.2.11)]) and $\deg(1 - \psi) = \mathrm{card}(\ker(\mathrm{Id} - \psi)) = \mathrm{card}(\widetilde{E}_v(k_v))$ (cf. 3.3).

□

As a consequence of Proposition 8.2, the knowledge of the representation $\rho_{E,\ell}$ for a *single* prime ℓ of good reduction for E determines the representation $\rho_{E,\ell'}$ for any other prime ℓ', up to semi-simplification. Indeed, we know the characteristic polynomial of $\rho'_{E,\ell'}(\mathrm{Frob}_v)$ for all places v of good reduction for K, which do not lie above ℓ or ℓ', and this is enough, according to [Ser98, page I-10].

The strong relationship between the representations in $\rho_{E,\bullet}$ can be formalized in the following definition:

Definition 8.4. *Let K be a number field. A strictly compatible system of Galois representations is a set $\{\rho_\ell : \ell \text{ prime}\}$ consisting of continuous representations $\rho_\ell : G_K \to \mathrm{GL}_n(\mathbb{Q}_\ell)$, such that there exist:*

1. *A finite set S of finite places of K (called* exceptional set of the system*);*
2. *For each $v \notin S$, a polynomial $P_v(x) \in \mathbb{Q}[x]$;*

satisfying that, for each $v \notin S$ and $v \nmid \ell$, then the representation ρ_ℓ is unramified at v, and

$$\mathrm{charpoly}(\rho_\ell(\mathrm{Frob}_v)) = P_v(x).$$

From the discussion above, we obtain the following proposition:

Proposition 8.5. *Let E be an elliptic curve defined over a number field K, and let S be the set of finite places of K where E has bad reduction. Then $\{\rho_{E,\ell} : \ell \text{ rational prime}\}$ is a compatible system of Galois representations, with exceptional set S.*

Now we turn to the mod ℓ representation $\overline{\rho}_{E,\ell} : G_K \to \mathrm{GL}_2(E[\ell]) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$. From the Néron-Ogg-Shafarevich criterion, it follows that, if E has good reduction at finite place $v \nmid \ell$, then $\overline{\rho}_{E,\ell}$ is unramified at v (in other words, the Galois extension $K(E[\ell])/K$ is unramified at v. However, the converse does not hold in general. You can find some examples in the Projects. Nevertheless, there is a result in this direction (cf. [Sil94, (IV.10.3)]).

Proposition 8.6. *Let K be a number field, E/K an elliptic curve with j-invariant j_E and v a place of K of good reduction for E such that $v(j_E) \geq 0$. Then the following are equivalent:*

1. *E has good reduction at v;*
2. *$K(E[m])/K$ is unramified at v for all m coprime to v;*
3. *There exists a prime $\ell \geq 3$ with $\ell \nmid v$ such that $K(E[\ell])/K$ is unramified at v.*

Remark 8.7. *From the proposition above, it follows that, given a prime ℓ, the only places $v \nmid \ell$ of K where E can fail to have good reduction while $K(E[\ell])/K$ is unramified are those appearing in the factorization of the denominator of j_E.*

9 Conductor of an elliptic curve

In this section, we fix an elliptic curve E defined over a number field K; we are going to define an invariant of E, the *conductor*, which contains information about the action of inertia groups I_v on the torsion of E at all finite places v of K. We follow closely the presentation of [Sil94, §10, Chapter IV].

First, for each finite place v of K we define an integer, the *exponent of the conductor at v*, which measures how complicated the action of I_v on the torsion of E is. Afterwards, we will combine all this information into a product (in principle over all places v of K, but, as we will see, only those of bad reduction contribute a non-trivial factor) of ideals of $\mathcal{O}_K$. The exponent of the conductor at v consists of two parts; the *tame* part, which is obtained from the action of I_v on the ℓ-adic Tate module $V_\ell(E) := \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell(E)$, and the *wild part*, which depends only on the ℓ-torsion points of E; as we will see below, it is defined in terms of the higher ramification groups of the Galois extension $K(E[\ell])/K$.

Definition 9.1. *Let K be a number field, v a finite place of K, and E/K be an elliptic curve. Choose a prime ℓ such that $v \nmid \ell$.*

1. *We define the* tame part of the conductor of E at v *as*

$$\varepsilon_v(E) = \dim_{\mathbb{Q}_\ell}(V_\ell(E)/V_\ell(E)^{I_v}) = 2 - \dim_{\mathbb{Q}_\ell}(V_\ell(E)^{I_v}).$$

2. *We define the* wild part of the conductor of E at v *as follows: if $L = K(E[\ell])$, then*

$$\delta_v(E) := \sum_{i=1}^{\infty} \frac{g_i(L/K)}{g_0(L/K)} \dim_{\mathbb{F}_\ell}(E[\ell]/E[\ell]^{G_i(L/K)}),$$

   where $g_i(L/K) = \mathrm{card}(G_i(L/K))$.

3. *We define the* exponent of the conductor of E at v *as the sum*

$$f_v(E) = \varepsilon_v(E) + \delta_v(E).$$

The first remark we should make is that, in order to define $\varepsilon_v(E)$ and $\delta_v(E)$, we chose a prime ℓ, so in principle this definition depends on this choice. However, we will see below that, in fact, we obtain the same quantities if we choose a different prime ℓ' with $\ell' \nmid v$.

Next, let us unravel the easiest case, namely the case when E has good reduction at v. In this case, I_v acts trivially on $V_\ell(E)$, thus $V_\ell(E)^{I_v} = V_\ell(E)$ has dimension 2, whence $\varepsilon_v(E) = 0$. Moreover, since $E[\ell]$ is a quotient of $T_\ell(E)$, it follows that I_v acts trivially on $E[\ell]$, thus the extension $K(E[\ell])/K$ is unramified at v. Therefore all $G_i(L/K)$ equal $\{\mathrm{Id}\}$, so $E[\ell]^{G_i(L/K)} = E[\ell]$ and the dimension of the quotient $E[\ell]/E[\ell]^{G_i(L/K)}$ is zero, whence $\delta_v(E) = 0$. We can conclude that $f_v(E) = 0$ whenever v is a place of good reduction for E. Conversely, if E has bad reduction at the place v, by the Néron-Ogg-Shafarevich criterion, the action of I_v on $T_\ell(E)$ is non-trivial. Thus $V_\ell(E)^{I_v} \neq V_\ell(E)$, which implies that $\varepsilon_v(E) > 0$, hence $f_v(E) > 0$.

The next remark we should make is that $f_v(E)$ is always a non-negative integer number. This is clear for the tame part of the conductor, but from the definition it is not immediate to conclude that $\delta_v(E) \in \mathbb{Z}_{\geq 0}$. For a proof, the reader can look at [Ser79, Cor. to Prop. 5, Chap. VI].

It turns out that the tame part of the conductor at v is completely determined by the type of reduction of E at v (good, multiplicative or additive) as follows (cf. [Sil94, (IV.10.2)]).

Theorem 9.2. *Let E be an elliptic curve defined over a number field K, v a finite place of K. Then*

$$\varepsilon_v(E) = \begin{cases} 0 \text{ if } E \text{ has good reduction at } v; \\ 1 \text{ if } E \text{ has (bad) multiplicative reduction at } v; \\ 2 \text{ if } E \text{ has (bad) additive reduction at } v. \end{cases}$$

Remark 9.3. *The main ingredient in the proof of the above theorem is the isomorphism*

$$V_\ell(E(\overline{K}_v))^{I_v} \simeq V_\ell(\widetilde{E}_{v,\mathrm{ns}}(\overline{k}_v)),$$

where $\widetilde{E}_{v,\mathrm{ns}}(\overline{k}_v)$ is the set of non-singular points of the reduced curve $\widetilde{E}_v/k_v$. When E has good reduction at v, $E_{v,\mathrm{ns}} = E_v$ is an elliptic curve and we know that $\widetilde{E}_v(\overline{k}_v)$ has a group structure. If the reduction is bad, we still can define a group structure on $\widetilde{E}_{v,\mathrm{ns}}(\overline{k}_v)$, which is isomorphic to the multiplicative group $\overline{k}_v^\times$ if E has multiplicative reduction at v, and to the additive group $\overline{k}_v$ if E has additive reduction at v (whence the terminology). The ℓ-adic Tate module of $\overline{k}_v^\times$ is a free rank 1 $\mathbb{Z}_\ell$-module, whereas the ℓ-adic Tate module of $\overline{k}_v$ is zero, since it does not have any ℓ-torsion points.

The wild part of the conductor is more complicated, since in general it cannot be determined only by knowing if the reduction of E at v is good, multiplicative or additive. However, it vanishes most of the time (cf.[Sil92, (VI.102)]).

Proposition 9.4. *Let E be an elliptic curve defined over a number field K, v a finite place of K. Then $\delta_v(E) = 0$ if at least one of the following conditions hold:*

1. *E has good reduction or split multiplicative reduction at v.*

2. $p = \mathrm{char}(k_v) \geq 5$.

Remark 9.5. *The case of good reduction follows from the Néron-Ogg-Shafarevich criterion. In the case of multiplicative reduction, we will see later that the extension $K(E[\ell])/K$ is tamely ramified. The second part follows from (the proof of) Proposition 8.6. In Section 11 we will see a general formula for computing $f_v(E)$ for all residue characteristics.*

Finally, we can collect together the exponents introduced in Definition 9.1 as follows.

Definition 9.6. *Let K be a number field with ring of integers $\mathcal{O}_K$ and E/K be an elliptic curve. We define the* conductor *of E as the ideal*

$$\mathfrak{N}_E = \prod_{\substack{\mathfrak{p} \text{ maximal} \\ \text{ideal of } K}} \mathfrak{p}^{f_{v_\mathfrak{p}}(E)},$$

where $v_\mathfrak{p}$ is the (normalized) discrete valuation defined by the ideal $\mathfrak{p}$.

Note that the primes of $\mathcal{O}_K$ dividing $\mathfrak{N}_E$ are precisely those corresponding to the finite places $v_\mathfrak{p}$ satisfying that the valuation of the minimal discriminant of E with respecto to $v_\mathfrak{p}$ is nonzero.

10 p-adic uniformization of elliptic curves: Tate's Curve

In this section we take a closer look at elliptic curves, defined over a local field K, with (bad) multiplicative reduction. The key idea is that such curves admit (after possibly a quadratic base change) a p-adic uniformization, that is, an isomorphism $E(\overline{K}) \simeq \overline{K}^\times / q^\mathbb{Z}$ for a certain value of $q \in K^\times$. We proceed in two steps: first, we define a special class of elliptic curves, the so-called *Tate curves*, that admit this uniformization, and then we show that, if an elliptic curve has multiplicative reduction, then it is isomorphic to some Tate curve, possibly after a quadratic base change.

For the rest of the section, K is a finite extension of $\mathbb{Q}_p$, v is the valuation of K (which we can assume normalized), $\mathcal{O}_K$ the valuation ring, $\mathfrak{m}$ its maximal ideal, k_v is the residue field of K and $|\cdot|_v$ is the absolute value attached to v, defined by $|x|_v = \mathrm{card}(k_v)^{-v(x)}$ for all $x \in K^\times$.

For each $q \in K^\times$ with $|q|_v < 1$, consider the following power series:

$$a_4(q) = -5 \sum_{n \geq 1} \frac{n^3 q^n}{1 - q^n} \quad \text{and} \quad a_6(q) = -\frac{1}{12} \sum_{n \geq 1} \frac{(7n^5 + 5n^3) q^n}{1 - q^n}.$$

These series are convergent and define elements in $\mathcal{O}_K$. The Weierstrass equation

$$y^2 + xy = x^3 + a_4(q)x + a_6(q) \tag{10.9}$$

has discriminant

$$\Delta = q \prod_{n \geq 1} (1 - q^n)^{24};$$

since $|q|_n < 1$, this infinite product converges to a nonzero element. Thus, Equation (10.9) defines an elliptic curve. This elliptic curve will be denote by E_q/K, and is called a *Tate curve*.

Remark 10.1. *Clearly $\Delta \in \mathfrak{m}$. However, the invariant $c_4 = 1 - 48a_4(q) \notin \mathfrak{m}$, thus the curve E_q has multiplicative reduction at v (cf. Section 6).*

Now we give the p-adic uniformization (cf. [Sil94, (V.3.1)]). For each $q \in \mathfrak{m}$, we can define

$$x(u) = \frac{u}{(1-u)^2} + \sum_{n\geq 1}\left(\frac{q^n u}{(1-q^n u)^2} + \frac{q^{-n}u}{(1-q^{-n}u)^2} - 2\frac{q^n}{(1-q^n)^2}\right)$$
$$y(u) = \frac{u^2}{(1-u)^3} + \sum_{n\geq 1}\left(\frac{(q^n u)^2}{(1-q^n u)^3} + \frac{(q^{-n}u)^2}{(1-q^{-n}u)^3} + \frac{q^n}{(1-q^n)^2}\right)$$

These series converge for all $u \in \overline{K}^\times \setminus q^{\mathbb{Z}}$.

Theorem 10.2. *The map*

$$\phi : \overline{K}^\times \to E_q(\overline{K})$$
$$u \mapsto \begin{cases} (x(u), y(u)) \text{ if } u \notin \overline{K}^\times \setminus q^{\mathbb{Z}}; \\ O_{E_q} \text{ otherwise} \end{cases}$$

is a surjective homomorphism, compatible with the action of $\mathrm{Gal}(\overline{K}/K)$ *on both sides.*

As a consequence, we have a very explicit description of the action of G_K on the torsion points of E_q (cf. [Ser98, Apendix A.1.2]).

Corollary 10.3. *Let E_q/K be a Tate curve, and $\ell \neq p$ a prime number. Then we have the following exact sequence of* $\mathrm{Gal}(\overline{K}/K)$*-modules*

$$1 \to \mu_\ell(\overline{K}^\times) \to E_q[\ell] \to \mathbb{Z}/\ell\mathbb{Z} \to 0,$$

where the action of $\mathrm{Gal}(\overline{K}/K)$ *on $\mathbb{Z}/\ell\mathbb{Z}$ is trivial.*

In particular, the Galois representation $\rho_{E,\ell} : G_K \to \mathrm{GL}(E[\ell])$ is (at most) tamely ramified.

Given a Tate curve E_q/K, we can compute its j-invariant in terms of q by means of the formula

$$j \;=\; \frac{c_4^3}{\Delta} \;=\; \frac{(1-48a_4)^3}{\Delta} \;=\; \frac{\left(1 + 240\sum_{n\geq 1}\frac{n^3 q^n}{1-q^n}\right)}{q\prod_{n\geq 1}(1-q^n)^{24}} \;=\; \frac{1}{q} + 744 + 196884q + \cdots.$$

Thus, every element of K that can be expressed as $\frac{1}{q} + 744 + 196884q + \cdots = j(q)$ like in the formula above, for some value of q with $v(q) > 0$, is the j invariant of a Tate curve. An application of the Fixed Point Theorem allows one to prove that the map $q \mapsto j(q)$ is a bijection between the sets $\{q \in K : 0 < |q|_v < 1\}$ and $\{j \in K : |j|_v > 1\}$ (cf. [Hus04, Lemma 5.4, Chapter 10]). As a consequence, an elliptic curve is isomorphic to a Tate curve if and only if $v(j) < 0$. One can prove the following precise result (cf. [Sil92, Appendix C]).

Proposition 10.4. *Let E/K be an elliptic curve such that $v(j) < 0$ (in particular, it has bad reduction). Let $q \in \mathfrak{m}$ be such that $j_E = j(q)$. Then:*

1. *If E has split multiplicative reduction, then E and E_q are isomorphic.*

2. *If E has non-split multiplicative reduction, then there exists an unramified quadratic extension K'/K such that E and E' are isomorphic over K'.*

3. *If E has bad additive reduction,then there is a ramified quadratic extension K'/K such that E and E' are isomorphic over K'.*

11 Ogg's formula for the conductor

The aim of this section is to provide a formula for computing the exponent of the conductor $f_v(E)$ of an elliptic curve E defined over a number field K, at any finite place of K, in terms of the reduction of E at v. This purpose leads us the issue of reduction of curves defined over local fields, which, in turn, brings us to the theory of models of curves, which requires scheme theory to be formulated properly. Following the spirit of these notes, we try to keep as little technical as possible, at the cost of ommiting most of the details. A rigorous and complete treatment can be found in [Liu02, Chapter 10, Section 10.1].

We already discussed the reduction theory of elliptic curves defined over local fields in Section 6, where we encountered the first difficulty, namely that not every Weierstrass equation (1.1) defining an elliptic curve can be reduced modulo a finite place v (since there could be denominators in the coefficients $a_1, \ldots, a_6 \in K$ with positive v-adic valuation), and even when this was the case, we could obtain different reduced Weierstrass equations for the same elliptic curve E. In Section 6 we addressed this question in an elementary way by introducing the concept of minimal discriminant. For the purposes of this section, this solution will not be enough.

We recall briefly some key concepts from arithmetic geometry. The appropriate setting for studying models of curves is that of arithmetic surfaces, that is to say, schemes $X \to S$ over a discrete valuation ring S (or, more generally, a Dedekind domain) of dimension 2. In particular, we will work with *fibered surfaces*, which are integral, projective, flat S-schemes of dimension 2 (cf. [Liu02, Definition 8.3.1]). A fibered surface X/S satisfies that both the generic fibre X_η/K_S and the special fibre X_s/k_S are curves (where by K_S we denote the field of fractions of S and k_S the residue field of S).

Definition 11.1. *Let K be a local field, with ring of integers $\mathcal{O}_K$; denote by $S = \operatorname{Spec} \mathcal{O}_K$. Let C be a smooth projective curve defined over K. A* model of C over S *is a normal fibered surface $\mathcal{C} \to S$, together with an isomorphism f from the generic fibre of $\mathcal{C}$ to C.*

We will be interested in the *regular models* of a curve C. If the genus of C is at least 1, then there exists a (unique) *minimal regular model* $\mathcal{C}_{\min}$ (cf. [Liu02, (9.3.21)]). If the curve C has good reduction (which, in general, means that there exists some model of C over $\mathcal{O}_K$ which is smooth), then the minimal regular model $\mathcal{C}_{\min}$ is smooth.

When E/K is an elliptic curve, we have two (different in general) models of E over $\mathcal{O}_K$; one is provided by a minimal Weierstrass equation, and the other one is the minimal regular model $\mathcal{C}_{\min}$.

If E/K has good reduction at the (unique) maximal ideal $\mathfrak{m}_K$, then they coincide, and the special fibre of $\mathcal{C}_{\min}$ coincides with the projective curve defined by the reduction of the minimal Weierstrass equation. However, when E/K has bad reduction, the two models are different. The reason why we are interested in the minimal regular model of E/K is because there is a formula that relates the valuation of the minimal discriminant of E, the number of components of the special fibre of $\mathcal{C}_{\min}$, and the exponent of the conductor of E/K (cf. [Sil94, (IV.11.1)]).

Theorem 11.2 (Ogg's Formula)**.** *Let $K/\mathbb{Q}_p$ be a finite extension, E/K an elliptic curve. We denote by*

- *$v(\Delta_{E/K})$ the valuation of the minimal discriminant of E/K,*
- *$m(E/K)$ the number of components, defined over $\overline{\mathbb{F}}_p$, of the special fibre of the minimal regular model $\mathcal{C}_{\min}$ of E/K, (where each component is counted once, even if they occur with higher multiplicity).*

Then

$$f(E/K) = v(\Delta_{E/K}) - m(E/K) + 1.$$

There is a classification, due to Néron and Kodaira, of the special fibre of the minimal regular model of an elliptic curve defined over a p-adic field K. They distinguish 10 types, denoted by I_0, I_n, II, III, IV, I_0^*, I_n^*, IV^*, III^*, II^*. The type I_0 corresponds to good reduction (thus the special fibre is an elliptic curve), and the rest correspond to different configurations of intersecting curves (cf. [Sil94, (IV.8.2)]). Given an elliptic curve E defined over a p-adic field K by means of a Weierstrass equation, there is an algorithm, due to Tate, that computes the special fibre of the minimal regular model of E. This algorithm is presented in detail in [Sil94, Chapter IV, §9], and is implemented e.g. in SageMath. Combining this algorithm with Theorem 11.2, we can compute the conductor of an elliptic curve E defined over a number field K.

12 Project work

The summer school *Explicit and computational approaches to Galois representations* included three sessions for project work, where several exercises are proposed to the participants, to solve with the help of the computer algebra system SageMath, and the database of L-functions, modular forms and related objetcts (LMFDB). Here are the three projects corresponding to the course *Elliptic curves*.

12.1 First Project: Computing images of mod ℓ Galois representations attached to elliptic curves

In this project we consider elliptic curves E defined over the field of rational numbers, which we assume defined by an affine Weierstrass equation of the general shape

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{12.10}$$

for some coefficients $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q}$.

Given a prime number ℓ, the action of $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the group of ℓ-torsion points of E induces a Galois representation

$$\overline{\rho}_{E,\ell} : G_{\mathbb{Q}} \to \mathrm{GL}_2(E[\ell]) \simeq \mathrm{GL}_2(\mathbb{F}_\ell).$$

Let $K = \mathbb{Q}(E[\ell])$ be the extension of $\mathbb{Q}$ obtained by adjoining the coordinates of the points of ℓ-torsion of E; in other words, K is the fixed field of $\overline{\mathbb{Q}}$ by $\ker \overline{\rho}_{E,\ell}$. The extension $K/\mathbb{Q}$ is finite and Galois, satisfying that $\mathrm{Im}\overline{\rho}_{E,\ell} \simeq \mathrm{Gal}(K/\mathbb{Q})$. In this project, we want to compute this Galois group in some examples.

Our main tool will be to consider the Frobenius elements at primes different from ℓ. Given a prime $p \neq \ell$, which is unramified in the extension $K/\mathbb{Q}$, choose a prime $\mathfrak{p}$ of the ring of integers $\mathcal{O}_K$ of K which lies above p, and set $D_{\mathfrak{p}} := \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) : \sigma\mathfrak{p} = \mathfrak{p}\}$. This is the *decomposition group at* p. Denoting by k_p the residue field $\mathcal{O}_K/\mathfrak{p}$, the reduction map

$$D_{\mathfrak{p}} \to \mathrm{Gal}(k_p/\mathbb{F}_p)$$

is an isomorphism. Let $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(K/\mathbb{Q})$ be the element in $D_{\mathfrak{p}}$ projecting onto the map $x \mapsto x^p$ (the Frobenius element in $\mathrm{Gal}(k_p/\mathbb{F}_p)$). This element depends on the choice of $\mathfrak{p}|p$, but if we choose a different prime of $\mathcal{O}_K$ above p, we obtain an element conjugate to $\mathrm{Frob}_{\mathfrak{p}}$. Thus, abusing notation, we will denote it by Frob_p. The next proposition (cf. [Ser72, §4]) tells us what is the characteristic polynomial of the image of Frob_p by $\overline{\rho}_{E,\ell}$ (which is well-defined, since it is invariant by conjugation).

We will see in the morning lectures that those primes p such that the elliptic curve has good reduction mod p are unramified in the extension $K/\mathbb{Q}$ (this follows from the so-called Néron-Ogg-Shafarevich criterion).

Proposition 12.1. *Let $E/\mathbb{Q}$ be an elliptic curve, ℓ a prime number, $\overline{\rho}_{E,\ell}$ the Galois representation attached to the ℓ-torsion points of E, and $p \neq \ell$ a prime number such that E has good reduction at p. Then*

$$\begin{cases} \mathrm{trace}(\overline{\rho}_{E,\ell}(\mathrm{Frob}_p)) = 1 + p - \mathrm{card}(\widetilde{E}_p(\mathbb{F}_p)) \mod \ell \\ \det(\overline{\rho}_{E,\ell}(\mathrm{Frob}_p)) = p \mod \ell \end{cases}$$

where $\widetilde{E}_p$ denotes the reduction of E at p.

The above proposition provides us with the characteristic polynomials of many elements in $\mathrm{Im}\overline{\rho}_{E,\ell}$. In fact, Chebotarev's Density Theorem tells us that, if we computed $\overline{\rho}_{E,\ell}(\mathrm{Frob}_p)$ for *all* primes p of good reduction for E (with possibly finitely many exceptions), we would obtain elements belonging to each conjugacy class of $\mathrm{Im}\overline{\rho}_{E,\ell}$.

Theorem 12.2 (Chebotarev)**.** *Let L/K be a finite Galois extension of number fields, let $X \subset \mathrm{Gal}(L/K)$ be a subset that is fixed by conjugation. Then the set S of primes $\mathfrak{p}$ of $\mathcal{O}_K$ such that $\mathrm{Frob}_{\mathfrak{p}} \in X$ has a density, equal to*

$$\mathrm{card}\, X/\,\mathrm{card}(\mathrm{Gal}(L/K)).$$

For more details regarding density of sets of primes in number fields, as well as references for a proof, see [Ser98, Chapter 1].

Remark 12.3. *In particular, it follows from Theorem 12.2 that* $\det \overline{\rho}_{E,\ell} : \mathrm{Gal}(K/\mathbb{Q}) \to \mathbb{F}_\ell^\times$ *coincides with the mod* ℓ *cyclotomic character, which is surjective.*

Our aim is to determine $\mathrm{Gal}(K/\mathbb{Q})$ by computing the image of enough Frobenius elements. We know that $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathrm{Im}\overline{\rho}_{E,\ell}$ is a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, such that the restriction of the determinant to this subgroup is surjective. A result of Serre (cf. [Ser72, Proposition 19]) shows that, when $\ell \geq 5$, the information provided by the characteristic polynomial of the image of Frob_p *for all* p is enough to determine if $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell)$ or not.

Proposition 12.4. *Let* $\ell \geq 5$ *be a prime,* $H \subset \mathrm{GL}_2(\mathbb{F}_\ell)$ *be a subgroup such that:*

1. *There exists* $s_1 \in H$ *with* $\mathrm{trace}(s_1)^2 - 4\det(s_1)$ *a nonzero square in* $\mathbb{F}_\ell$ *and* $\mathrm{trace}(s_1) \neq 0$.
2. *There exists* $s_2 \in H$ *with* $\mathrm{trace}(s_2)^2 - 4\det(s_2)$ *a non-square in* $\mathbb{F}_\ell$ *and* $\mathrm{trace}(s_2) \neq 0$.
3. *There exists* $s_3 \in H$ *with* $u = \mathrm{trace}(s_3)^2/\det(s_3)$ *satisfying:* $u \neq 0, 1, 2, 4$ *and* $u^2 - 3u + 1 \neq 0$.

Then H *contains* $\mathrm{SL}_2(\mathbb{F}_\ell)$. *If* $\det|_H$ *is surjective, then* $H = \mathrm{GL}_2(\mathbb{F}_\ell)$.

In particular, if $\ell \geq 5$, it suffices to show that, for any pair $(a, b) \in \mathbb{F}_\ell \times \mathbb{F}_\ell^\times$, there exists $s \in H$ such that $\mathrm{charpoly}(s) = T^2 + aT + b$.

Note that, while Proposition 12.4 allows you to prove that $\mathrm{Im}\overline{\rho}_{E,\ell} \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$, it does not allow you to prove anything if the image is smaller. Using explicit versions of Chebotarev's Density Theorem, one can determine a bound, depending on E, such that, if some polynomial $T^2 + aT + b$ does not appear as the characteristic polynomial of Frob_p for some prime p strictly smaller than this bound, then it will not appear as the characteristic polynomial of the Frobenius element for any p. As a consequence, a finite computation will provide a proof that the image is *not* surjective. For more details, see [Sut16].

If $\ell = 2$ or 3, the situation is more complicated, since only the characteristic polynomials of Frobenius elements are not enough to determine if $\mathrm{Im}\overline{\rho}_{E,\ell}$ is the whole group $\mathrm{GL}_2(\mathbb{F}_\ell)$. Luckily, in these cases the equations that define the ℓ-torsion points of E are still simple enough to be manipulated.

For $\ell = 2$, we have that $\mathrm{GL}_2(\mathbb{F}_2) \simeq S_3$, and it has only three proper subgroups up to conjugation, namely

$$H_1 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}, H_2 \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}, H_3 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}.$$

The coordinates of the points of order exactly 2 of $E(\overline{\mathbb{Q}})$ are the roots of the polynomial

$$P(x) = 4x^3 + b_2x^2 + 2b_4x + b_6.$$

Using the group of points of 2-torsion which are defined over $\mathbb{Q}$ and the discriminant of E, we can determine $\mathrm{Im}\overline{\rho}_{E,\ell}$ completely, as shown in the next proposition (cf. [RV01, Proposition 2.1]).

Proposition 12.5. *Let $E(\mathbb{Q})[2]$ the group of 2-torsion points defined over $\mathbb{Q}$, and let Δ_E be the discriminant of E. Then it holds:*

$$\mathrm{Im}\overline{\rho}_{E,\ell} = \begin{cases} H_1 \text{ if } E(\mathbb{Q})[2] \neq \{O\} \text{ and } \Delta_E \in \mathbb{Q}^2 \\ H_2 \text{ if } E(\mathbb{Q})[2] \neq \{O\} \text{ and } \Delta_E \notin \mathbb{Q}^2 \\ H_3 \text{ if } E(\mathbb{Q})[2] = \{O\} \text{ and } \Delta_E \in \mathbb{Q}^2 \\ \mathrm{GL}_2(\mathbb{F}_\ell) \text{ if } E(\mathbb{Q})[2] = \{O\} \text{ and } \Delta_E \notin \mathbb{Q}^2 \end{cases}$$

For $\ell = 3$, recall that the 3-division polynomial

$$\psi_3(x) = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8$$

satisfies that its roots are precisely the x-coordinates of the 3-torsion points of E (cf. [Sil92, Exercise 3.7, Chapter III]). We can complete this information with the discriminant of E to obtain a surjectivity criterion (cf. [RV01, Theorem 2.3]).

Proposition 12.6. *Let $E/\mathbb{Q}$ be an elliptic curve. The following conditions are equivalent:*

- *ψ_3 does not have any rational roots and $\Delta_E \notin \mathbb{Q}^3$;*
- $\mathrm{Im}\overline{\rho}_{E,\ell} \simeq \mathrm{GL}_2(\mathbb{F}_3)$.

Exercise 12.1. *For the following elliptic curves, check whether the image of $\overline{\rho}_{E,\ell} \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$, for the primes $\ell = 2, 3, 5, 7, 11$:*

1. $E_1 : y^2 + y = x^3 - x^2$
2. $E_2 : y^2 + xy + y = x^3 - x$
3. $E_3 : y^2 + y = x^3 - x$

Exercise 12.2. *Consider the elliptic curve E defined over $\mathbb{Q}$ by the Weierstrass equation $E : y^2+xy = x^3 - x^2 - 107x + 552$. Can you find a single prime ℓ such that $\overline{\rho}_{E,\ell} \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$?*

The previous exercise shows an example of an elliptic curve $E/\mathbb{Q}$ with *complex multiplication*, that is to say, such that the ring of endomorphisms $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$ is strictly bigger than $\mathbb{Z}$. There are only 13 j-invariants in $\mathbb{Q}$ corresponding to elliptic curves with complex multiplication.

Assume $E/\mathbb{Q}$ has complex multiplication; then $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$ is an order in an imaginary quadratic field (cf. [Sil92, Cor. 9.4, Chap. III]), say K. Then any $\phi \in \mathrm{End}_{\overline{\mathbb{Q}}}(E)$ is in fact defined over K (cf. [Sil94, Theorem 2.2.b, Chap. II]). Thus, if we take any $\phi \in \mathrm{End}_{\overline{\mathbb{Q}}}(E)$, and consider its restriction

to $E[\ell]$, we obtain a morphism of $\mathbb{F}_\ell$-vector spaces that commutes with the image of any $\sigma \in G_K$ by the representation $\overline{\rho}_{E,\ell}$. In particular, we conclude that $\overline{\rho}_{E,\ell}(G_K)$ is isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ whose commutator is strictly greater than $\mathbb{Z}$. It can be shown that such a subgroup is abelian (cf. [Sil94, Ex 2.6, Chap. II]). Therefore, $\mathrm{Im}\overline{\rho}_{E,\ell}$ is either an abelian group or has an abelian group of index 2; in both cases, it is strictly smaller than $\mathrm{GL}_2(\mathbb{F}_\ell)$ if $\ell > 2$.

For the computational part of this project, we will rely on the data collected in the **database of L-functions, modular forms and related objetcts (LMFDB)**, which can be found at

`http://www.lmfdb.org/`

Here you can find lists of elliptic curves, together with many data related to them, including the images of $\overline{\rho}_{E,\ell}$ in many cases. You can check whether your computations in Exercise 1.1 were correct.

The elliptic curves are usually ordered according to their *conductor*. This is an integer number which contains information about the *reduction* of the elliptic curve at different primes, via the action of the inertia group at all rational primes on the ℓ-adic Tate module. We will tackle it in the morning lectures; for the moment, it suffices to know that the conductor of an elliptic curve $E/\mathbb{Q}$ is a number, whose prime factors are those primes where E has bad reduction.

Each curve is uniquely determined by a label. The label consists of two parts: a number, which equals the conductor or the elliptic curve, a letter, which identifies the isogeny class, and a number, which distinguishes the curves inside each isogeny class. For example, the labels of the elliptic curves in the exercise above are (11.a3), (14.a5) and (37.a1).

Remark 12.7. *To compute the characteristic polynomial of $\overline{\rho}_{E,\ell}(\mathrm{Frob}_p)$, you needed to compute the number of points of the reduction $\widetilde{E}_p$ for many primes p. In fact, this information is also contained in the LMFDB. For each elliptic curve, there appears a modular form in the database. For example, for the curve E_3 above the modular form is*

$$f(q) = q - 2q^2 - 3q^3 + 2q^4 - 2q^5 + 6q^6 - q^7 + 6q^9 + 4q^{10} \\ - 5q^{11} - 6q^{12} - 2q^{13} + 2q^{14} + 6q^{15} - 4q^{16} - 12q^{18} + O(q^{20})$$

For each prime $p \neq \ell$ of good reduction of E (that is, not dividing the conductor of E), the coefficient a_p of q^p coincides with $p + 1 - \mathrm{card}(\widetilde{E}_p(\mathbb{F}_p))$. The existence of a modular form which encodes information about the number of points of the reduction of E modulo p is precisely the statement of the Shimura-Taniyama conjecture. You can check this fact in the examples you computed.

Serre conjectured that the largest prime ℓ such that there exists some elliptic curve $E/\mathbb{Q}$, without complex multiplication, with $\mathrm{Im}\overline{\rho}_{E,\ell} \neq \mathrm{GL}_2(\mathbb{F}_\ell)$ is $\ell = 37$. D. Zywina refines this conjecture as follows (cf. [Zyw15a, Conjecture 1.12]):

Conjecture 12.8. *If E is an elliptic curve over $\mathbb{Q}$, without complex multiplication, and $\ell \geq 17$ is a prime such that the pair $(\ell, j_E) \notin \{(17, -17\cdot 373^3/2^{17}), (17, -17^2\cdot 101^3/2), (37, -7\cdot 11^3), (37, -7\cdot 137^3\cdot 2083^3)\}$. Then $\mathrm{Im}\overline{\rho}_{E,\ell} \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$.*

Zywina has verified this conjecture for all elliptic curves $E/\mathbb{Q}$ with conductor at most 360000 (cf. [Zyw15b]).

12.2 Second Project: Elliptic curves with isomorphic ℓ-torsion modules

In this project, we fix an elliptic curve $E/\mathbb{Q}$, and a prime ℓ such that $\overline{\rho}_{E,\ell}$ is surjective onto $\mathrm{GL}_2(\mathbb{F}_\ell)$. Let $K = \mathbb{Q}(E[\ell])$. Then we know that $K/\mathbb{Q}$ is a finite Galois extension with Galois group isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell)$. We ask the following question:

Question 1: Is there some other elliptic curve $E'/\mathbb{Q}$ such that the field $K' = \mathbb{Q}(E'[\ell])$ coincides with K?

Actually, we can also consider a more restrictive question, namely:

Question 2: Is there some other elliptic curve $E'/\mathbb{Q}$ such that the representations $\overline{\rho}_{E,\ell}$ and $\overline{\rho}_{E',\ell}$ are isomorphic?

It is clear that if $E'/\mathbb{Q}$ is an elliptic curve such that $\overline{\rho}_{E',\ell}$ is isomorphic to $\overline{\rho}_{E,\ell}$ (meaning that the $G_\mathbb{Q}$-modules $E[\ell]$ and $E'[\ell]$ are isomorphic), then $K = K'$. However, it is not immediate to determine whether the other implication holds (can you say something about it?)

Note that, if we have an isogeny $\varphi : E \to E'$ defined over $\mathbb{Q}$, then φ induces an isomorphism of $G_\mathbb{Q}$-modules between $E[\ell]$ and $E'[\ell]$. Thus, isogenous elliptic curves provide us with a trivial answer to Question 2. In the rest of the project, we will look for *non-isogenous* elliptic curves providing a positive answer to the questions.

To address the second question, we need to recall some facts from the representation theory of groups. First of all, we state the following classical result (cf. [CR62, (30.16)]).

Theorem 12.9 (Brauer-Nesbitt)**.** *Let ℓ be a prime and V a finite dimensional $\mathbb{F}_\ell$-vector space. Let $\overline{\rho}, \overline{\rho}' : G \to \mathrm{GL}_n(V)$ be two irreducible representations. Then $\overline{\rho}$ and $\overline{\rho}'$ are isomorphic if and only if for all $g \in G$, the characteristic polynomials of $\rho(g)$ and $\rho'(g)$ coincide.*

Combining this result with Chebotarev's Density Theorem, we obtain the following result:

Proposition 12.10. *Let $E/\mathbb{Q}$, $E'/\mathbb{Q}$ be two elliptic curves. Assume that, for all primes p of good reduction for E and E', we have the equality*

$$\mathrm{charpoly}(\overline{\rho}_{E,\ell}(\mathrm{Frob}_p)) = \mathrm{charpoly}(\overline{\rho}_{E',\ell}(\mathrm{Frob}_p)). \tag{12.11}$$

Then $\overline{\rho}_{E,\ell}$ and $\overline{\rho}_{E',\ell}$ are isomorphic.

Note that, since $\det \overline{\rho}_{E,\ell}(\mathrm{Frob_p}) = p = \det \overline{\rho}_{E',\ell}(\mathrm{Frob}_p)$, condition (12.11) is equivalent to $a_p \equiv a'_p \mod \ell$, where $a_p = p + 1 - \mathrm{card}(\widetilde{E}_p(\mathbb{F}_\ell))$ and $a'_p = p + 1 - \mathrm{card}(\widetilde{E'}_p(\mathbb{F}_\ell))$.

However, in finite time we can only check finitely many of the congruences above. Luckily for us, if the first few congruences hold, then one can prove that all congruences will hold as well. This result makes use of the theory of modular forms and the proof of the Shimura-Taniyama conjecture.

The bound C up to which one needs to check the congruences depends on the conductors N and N' of E and E' respectively. This invariant carries information about the reduction of the elliptic curve at each prime p. For example, the exponent of p in N is 1 if and only if the reduction of E at p is multiplicative.

The next proposition is taken from [KO92, Proposition 4]:

Proposition 12.11. *Let E, E' be two elliptic curves defined over $\mathbb{Q}$, with conductors N and N' respectively. Let S be the set of prime numbers where E has split multiplicative reduction and E' has non-split multiplicative reduction. Define the quantities:*

$$M = \operatorname{lcm}(N, N') \prod_{p \in S} p$$

$$\mu(M) = M \prod_{\substack{p|M \\ p \text{ prime}}} \left(1 + \frac{1}{p}\right)$$

Then the following conditions are equivalent:

1. *$\overline{\rho}_{E,\ell}$ and $\overline{\rho}_{E',\ell}$ are isomorphic.*
2. *For all $p < \mu(M)/6$ not dividing NN', we have $a_p \equiv a'_p \pmod{\ell}$, and for all $p < \mu(M)/6$ with $p|NN'$ but $p^2 \nmid NN'$, we have $a_p a'_p \equiv p + 1 \pmod{\ell}$.*

Before starting to compare representations coming from different elliptic curves, some further considerations about the conductor are in order. The conductor N of an elliptic curve $E/\mathbb{Q}$ is a number defined in terms of the ramification of the *ℓ-adic* representations $\rho_{E,\ell} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Q}_\ell)$. If $E'/\mathbb{Q}$ is another elliptic curve, a necessary condition for $\rho_{E,\ell}$ and $\rho_{E',\ell}$ to be isomorphic is that, for all primes $p \neq \ell$, the exponent of p in N coincides with the exponent of p in N'.

Since $\overline{\rho}_{E,\ell}$ is the mod ℓ reduction of $\rho_{E,\ell}$, it turns out that $\overline{\rho}_{E,\ell}$ can only be ramified at p if $\rho_{E,\ell}$ is ramified at p. However, in the process of reducing mod ℓ, some ramification can be lost. Thus, in order for $\overline{\rho}_{E,\ell}$ and $\overline{\rho}_{E',\ell}$ are isomorphic is no longer necessary that the conductors of E and E' coincide (away from the prime ℓ). But, the loss of ramification is a relatively rare phenomenon, so we can expect that the conductors of E and E' should not be too different.

Exercise 12.3. *Compare the mod ℓ representations attached to the following pair of elliptic curves (this example is taken from [KO92]):*

$$\ell = 7, \begin{cases} (26.a2) & E : y^2 + xy + y = x^3 - 5x - 8 \\ (182.a1) & E' : y^2 + xy + \text{`}y = x^3 - 4609x + 120244 \end{cases}$$

Exercise 12.4. *Can you find an example of a prime ℓ and a couple of non-isogenous elliptic curves $E, E'/\mathbb{Q}$, with the same conductor, such that $\overline{\rho}_{E,\ell} \simeq \overline{\rho}_{E',\ell}$?*

Exercise 12.5. *Does it always happen that, whenever $\overline{\rho}_{E,\ell} \simeq \overline{\rho}_{E',\ell}$, then E and E' have either the same conductor, or the same conductor outside of ℓ? Check the following example (this example is taken from [FK17]).*

$$\ell = 7, \begin{cases} (52.a1) & E : y^2 = x^3 - 4x - 3 \\ (988.c1) & E' : y^2 = x^3 - 362249x + 165197113 \end{cases}$$

What do you observe? Can you make a conjecture about a necessary condition on the conductors of E and E' in order for $\overline{\rho}_{E,\ell} \simeq \overline{\rho}_{E',\ell}$ to be isomorphic?

Exercise 12.6. *Compare the mod ℓ representations attached to the following pair of elliptic curves (this example is taken from [KO92]):*

$$\ell = 3, \begin{cases} (11.a3) & E : y^2 + y = x^3 - x^2; \\ (121.c2) & E' : y^2 + xy = x^3 + x^2 - 2x - 7; \end{cases}$$

12.3 Third Project: $\mathrm{GL}_2(\mathbb{F}_\ell)$-extensions of $\mathbb{Q}$ coming from the mod ℓ-torsion of elliptic curves

Fix a prime ℓ, and consider a fixed Galois extension $K/\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$. In the second project, we considered the question of determining if there can be two "essentially different" elliptic curves such that $K = \mathbb{Q}(E[\ell]) = \mathbb{Q}(E'[\ell])$. In this project, we address the question of the existence of *at least* one elliptic curve with $K \simeq \mathbb{Q}(E[\ell])$, once we have fixed K.

Exercise 12.7. *Knowing that $\det \overline{\rho}_{E,\ell} = \chi_\ell$, can you give a necessary condition for a number field K to satisfy $K = \mathbb{Q}(E[\ell])$?*

Given a Galois extension $K/\mathbb{Q}$ with Galois group $\mathrm{GL}_2(\mathbb{F}_\ell)$, its discriminant Δ_K gives us information about the primes that ramify in $K/\mathbb{Q}$. We give here a precise formulation (cf. Theorem 3.12.11 of [Koc00])

Theorem 12.12 (Dedekind's Discriminant Theorem)**.** *Let $K/\mathbb{Q}$ be a finite extension, Δ_K its discriminant and p a prime number. Suppose that*

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdot \cdots \cdot \mathfrak{p}_g^{e_g}$$

is the decomposition of the ideal $p\mathcal{O}_K$ into prime ideals of $\mathcal{O}_K$, and let f_i be the inertia degree $[\mathcal{O}_K/\mathfrak{p}_i : \mathbb{F}_p]$.

Then the exponent of p in Δ_K satisfies

$$v_p(\Delta_K) \geq (e_1 - 1)f_1 + \cdots + (e_g - 1)f_g,$$

with equality if and only if $p \nmid e_i$ for all $i = 1, \ldots g$.

In our case, $K/\mathbb{Q}$ is a Galois extension, hence denoting by e the ramification index at p, f the inertia degree at p, and g the number of primes of $\mathcal{O}_K$ above p, we have $v_p(\Delta_K) \geq (e-1)fg$, with equality if and only if p is tamely ramified in $K/\mathbb{Q}$.

Can you find a necessary condition for a number field K to be equal to $\mathbb{Q}(E[\ell])$, in terms of the discriminant Δ_K and the conductor of E?

In the database of L-functions, modular forms, and related objects (LMFDB), we can find lists of polynomials whose decomposition fields have prescribed Galois groups.

Exercise 12.8. *For $\ell = 2$, go through the list of Galois extensions $K/\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_2) \simeq S_3$ (label 6T2), and try to find elliptic curves $E/\mathbb{Q}$ satisfying that $K = \mathbb{Q}(E[\ell])$. Can you find some number field $K/\mathbb{Q}$ which (conjecturally) does not correspond to any elliptic curve?*

Exercise 12.9. *Prove that, for any Galois extension $K/\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_2) \simeq S_3$, there exists an elliptic curve $E/\mathbb{Q}$ such that $\mathbb{Q}(E[2]) \simeq K$ (Hint: Look at the equations that give the coordinates of the 2-torsion points of an elliptic curve).*

For $\ell \geq 3$, the situation is more complicated because the degree $[K : \mathbb{Q}]$ is too big to make explicit computations! In the LMFDB you can find polynomials $P(X) \in \mathbb{Q}[X]$ of degree 8 whose splitting field K is $\mathrm{GL}_2(\mathbb{F}_3)$. However, you only have information about the number field $F := \mathbb{Q}[X]/(F(X))$. If we have a tower of fields $\mathbb{Q} \subset F \subset K$, we have the following relationship between the discriminants Δ_K, Δ_F and $\delta_{K/F}$ (which is an ideal of $\mathcal{O}_F$):

$$\Delta_K = \mathrm{Norm}_{F/\mathbb{Q}}(\delta_{K/F})\Delta_F^{[K:F]}$$

Exercise 12.10. *Fix $\ell = 3$. The LMFDB includes a list of polynomials $P(X)$ of degree 8 whose Galois group is isomorphic to $\mathrm{GL}_2(\mathbb{F}_3)$ (label 8T23). Go through the list of elliptic curves $E/\mathbb{Q}$, ordered by conductor, and take those with $\mathrm{Im}\rho_{E,\ell} \simeq \mathrm{GL}_2(\mathbb{F}_3)$. For each such curve, there exists a degree-8 polynomial $P(x) \in \mathbb{Q}[X]$ whose splitting field coincides with $\mathbb{Q}(E[\ell])$ (prove it!). Try to match up the polynomials $P(x)$ and the elliptic curves $E/\mathbb{Q}$. Is there some polynomial which (conjecturally) does not correspond to any elliptic curve?*

In fact, it can be proven that, if $\ell = 3, 5$, given a Galois extension $K/\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$, there exist (infinitely many) elliptic curves $E/\mathbb{Q}$ such that $\mathbb{Q}(E[\ell]) = K$, cf. [Rub97, Theorem 3]. The situation changes drastically when we consider primes $\ell \geq 7$: There exist Galois extensions $K/\mathbb{Q}$ with Galois group $\mathrm{GL}_2(\mathbb{F}_\ell)$ which do not come from elliptic curves defined over $\mathbb{Q}$, that is, there is no elliptic curve $E/\mathbb{Q}$ such that $\mathbb{Q}(E[\ell]) = K$. You can find a proof in [Cal06, §3]. The different behaviour for small values of ℓ and large values of ℓ is due to the fact that the modular curves $X(\ell)$, $\ell = 2, 3, 5$, have genus 0, whereas $X(\ell)$ has genus $g \geq 1$ for all primes $\ell \geq 7$.

References

[Cal06] Frank Calegari. Mod p representations on elliptic curves. *Pacific J. Math.*, 225(1):1–11, 2006.

[CR62] Charles W. Curtis and Irving Reiner. *Representation theory of finite groups and associative algebras*. Pure and Applied Mathematics, Vol. XI. Interscience Publishers, a division of John Wiley & Sons, New York-London, 1962.

[FK17] N. Freitas and A. Kraus. On the symplectic type of isomorphims of the p-torsion of elliptic curves. *arXiv:1607.01218*, pages 1–75, 2017.

[Har77] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[Hus04] Dale Husemöller. *Elliptic curves*, volume 111 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2004. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen.

[KO92] A. Kraus and J. Oesterlé. Sur une question de B. Mazur. *Math. Ann.*, 293(2):259–275, 1992.

[Koc00] Helmut Koch. *Number theory*, volume 24 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2000. Algebraic numbers and functions, Translated from the 1997 German original by David Kramer.

[Liu02] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Rub97] Karl Rubin. Modularity of mod 5 representations. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 463–474. Springer, New York, 1997.

[RV01] Amadeu Reverter and Núria Vila. Images of mod p Galois representations associated to elliptic curves. *Canad. Math. Bull.*, 44(3):313–322, 2001.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

[Ser98] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves*, volume 7 of *Research Notes in Mathematics*. A K Peters, Ltd., Wellesley, MA, 1998. With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original.

[Sil92] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Sut16] Andrew V. Sutherland. Computing images of Galois representations attached to elliptic curves. *Forum Math. Sigma*, 4:e4, 79, 2016.

[SZ14] Renata Scognamillo and Umberto Zannier. *Introductory notes on valuation rings and function fields in one variable*, volume 14 of *Appunti. Scuola Normale Superiore di Pisa (Nuova Serie) [Lecture Notes. Scuola Normale Superiore di Pisa (New Series)]*. Edizioni della Normale, Pisa, 2014.

[Zyw15a] David J. Zywina. On the possible images of the mod ℓ representations assoicated to elliptic curves over $\mathbb{Q}$. *arXiv:1508.07660*, 2015.

[Zyw15b] David J. Zywina. On the surjectivity of mod ell representations associated to elliptic curves. *arXiv:1508.07661*, 2015.