# CIMPA SCHOOL ON SERRE'S BIG IMAGE THEOREM: BASIC NOTIONS

MATIAS ALVARADO

Abstract. In this mini-course, we present the prerequisites for the continuation of the program. In particular we remind some aspects of elliptic curves and study the classification of subgroups of $\mathrm{GL2}(\mathbb{F}_p)$.

## Introduction

The main goal of these notes is to remind the necessary background to understand the statement of Serre's theorem. This mini-course has three lectures of 2 hours each. The plan for the course is as follows

1. Some aspects of algebraic geometry.
2. Definition of elliptic curves
3. The arithmetic of elliptic curves I
4. The arithmetic of elliptic curves II
5. The arithmetic of elliptic curves III
6. Classification of subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$.

## 1. Lecture 1: Algebraic curves and elliptic curves

Let $k$ be a field, and $\bar{k}$ be a fixed algebraic closure of $k$. Generally in this school we are mostly interested when $k$ is a number field (for example $\mathbb{Q}$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt[5]{7})$, etc.), a finite field (for example $\mathbb{F}_2$, $\mathbb{F}_{47}$, $\mathbb{F}_{81}$, etc.), or an extension of the $p$-adic numbers (for example $\mathbb{Q}_3$, $\mathbb{Q}_{71}$, $\mathbb{Q}(i)_{(1+i)}$, etc.)

1.1. **Generalities on algebraic geometry.** In this section, we recall some concepts and facts on algebraic geometry, more concretely about algebraic curves. Since we need to cover several topics in this mini-course, we only deal with plane curves. For more details on algebraic geometry, you can see [SR94], [Ful08], or Chapter 1 in [Har13]. We start defining the ambient spaces, namely the affine and projective spaces over $k$. We define the affine and projective space of arbitrary dimension, but very soon, we focus on dimension 2.

**Definition 1.** *The affine space is the set*

$$\mathbb{A}^n = \mathbb{A}^n(\bar{k}) = \{p = (x_1, ..., x_n) : x_i \in \bar{k}\}.$$

*The $k$-rational points of $\mathbb{A}^n$ is defined as the set*

$$\mathbb{A}^n(k) = \{p = (x_1, ..., x_n) \in \mathbb{A}^n : x_i \in k\}.$$

*Date*: January 9, 2025.

**Definition 2.** *The projective space denoted by* $\mathbb{P}^n$ *or* $\mathbb{P}^n(\bar{k})$ *is the set of equivalence classes of elements*

$$(x_0, ..., x_n) \in \mathbb{A}^{n+1} \setminus \{(0, 0, ..., 0)\},$$

*where*

$$(x_0, ..., x_n) \sim (y_0, ..., y_n)$$

*if there is* $\lambda \in \bar{k}^\star$ *such that* $x_i = \lambda y_i$ *for all* $i \in \{0, 1, ..., n\}$.

*Remark* 1.1. The equivalence class of $(x_0, ..., x_n)$ is denoted by $[x_0 : ... : x_n]$.

Similarly to the case of the affine space, we define the set of $k$-rational points of $\mathbb{P}^n$ as

$$\mathbb{P}^n(k) = \{[x_0 : ... : x_n] \in \mathbb{P}^n : \exists y_0, ..., y_n \in k, \text{ and } (x_0, ..., x_n) \sim (y_0, ..., y_n)\}.$$

*Remark* 1.2. If $[x_0, ..., x_n] \in \mathbb{P}^1(k)$, then it does not implies that each $x_i \in k$. For example $[\sqrt{2} + 5 : \sqrt{8} + 10] \in \mathbb{P}^1(\mathbb{Q})$ (why?), but $(\sqrt{2} + 5) \notin \mathbb{Q}$.

Now we specialize to $n = 2$.

In $\mathbb{P}^2$, there are many copies of $\mathbb{A}^2$. We explore 3 of these. We define

$$U_0 = \{[x : y : z] \in \mathbb{P}^2 : x = 1\}$$
$$U_1 = \{[x : y : z] \in \mathbb{P}^2 : y = 1\}$$
$$U_2 = \{[x : y : z] \in \mathbb{P}^2 : z = 1\}$$

**Definition 3.** *The subsets* $U_0, U_1, U_2$ *of* $\mathbb{P}^2$ *are called the affine charts of* $\mathbb{P}^2$.

Let $\mathrm{Gal}(\bar{k}/k)$ be the absolute Galois group of $k$. There is an action of $\mathrm{Gal}(\bar{k}/k)$ on $\mathbb{A}^2$ and $\mathbb{P}^2$. If $\sigma \in \mathrm{Gal}(\bar{k}/k)$, and $(x_1, x_2) \in \mathbb{A}^2$, then

$$\sigma.(x_1, x_2) = (\sigma(x_1), \sigma(x_2)).$$

Similarly, if $[x_0 : x_1 : x_2] \in \mathbb{P}^2$, then

$$\sigma.[x_0 : x_1 : x_2] = [\sigma(x_0) : \sigma(x_1) : \sigma(x_2)].$$

The sets of $k$-rational points can be characterized as the set of the fixed points via the action of the Galois group, i.e.

$$\mathbb{A}^n(k) = (\mathbb{A}^n)^{\mathrm{Gal}(\bar{k}/k)} \text{ and } \mathbb{P}^n(k) = (\mathbb{P}^n)^{\mathrm{Gal}(\bar{k}/k)}$$

1.1.1. *Algebraic curves.* Let $f$ be a polynomial in $\bar{k}[x, y]$

**Definition 4.** *An affine algebraic curve is any set of the form*

$$V(f) = \{(x, y) \in \mathbb{A}^2 : f(x, y) = 0\}$$

**Definition 5.** *We say that an algebraic curve* $X$ *is defined over* $\bar{k}$ *if there is a polynomial* $f \in k[x, y]$*, such that* $X = V(f)$.

**Definition 6.** *If* $X$ *is an affine algebraic curve defined over* $k$*, then the set of* $k$*-rational points is defined as*

$$X(k) = X \cap \mathbb{A}^2(k)$$

Note that if $X$ is defined by the polynomial $f \in k[x, y]$, then $X(k)$ is the set of all solutions of $f$ in $k^2$.

*Remark* 1.3. We often write $X/k$ to denote that the algebraic curve $X$ is defined over the field $k$.

Now, we introduce the notion of projective algebraic curves.

**Definition 7.** *A polynomial* $f \in \bar{k}[x_0, ..., x_n]$ *is homogeneous of degree* $d$ *if*

$$f(\lambda x_0, ..., \lambda x_n) = \lambda^d f(x_0, ..., x_n).$$

**Definition 8.** *A projective algebraic curve is any set of the form* $V(f) \subset \mathbb{P}^2$ *for a homogenous polynomial* $f(x, y, z)$.

*Remark* 1.4. Note that the solutions of a homogeneous polynomial are well defined in $\mathbb{P}^2$.

1.1.2. *From an affine curve to a projective curve.* Let $f(x, y) \in \bar{k}[x, y]$ be a polynomial, and consider $V(f)$ the affine curve associated with $f$. We can associate a projective curve to $f$ via the *homogenezation* of $f$.

Let $d$ be the degree of $f$. Let $F(x, y, z)$ be the polynomial defined by

$$F(x, y, z) = z^d f(x/z, y/z).$$

$F(x, y, x)$ is a homogeneous polynomial of degree $d$.

In this way, we construct the projective variety associated with $F$. This projective curve is called the projectivization of $V$.

In general, we like working with projective curves (these curves have many good properties in contrast to the affine case). Often, projective curves are defined by non-homogeneous polynomials. In this case, we understand that it refers to the curve defined by the projectivization of the polynomial.

**Example 1.** *If we say, let* $E$ *be the projective curve defined by* $y^2 = x^3 - 1$, *we understand that the curve* $E$ *is the projective curve associated with the polynomial* $zy^2 - x^3 - z^3$.

1.1.3. *From a projective curve to an affine curve.* Let $X$ be a projective curve given by a polynomial $F(x, y, z)$; then we can get three different affine curves from $X$, which we call them the affine charts. Let $X \cap U_0 = \{F(1, y, z) = 0\}$, $X \cap U_1 = \{F(x, 1, z) = 0\}$, and $X \cap U_2 = \{F(x, y, 1) = 0\}$.

1.1.4. *Singular points and smooth curves.*

**Definition 9.** *Let* $X$ *be a planar curve defined by a polynomial* $f(x, y, z)$. *A point* $(x_0, y_0, z_0)$ *is said singular point of* $X$ *is* $(x_0, y_0, z_0)$ *is a simultaneous solution of the following equation system*

$$\begin{aligned} f(x_0, y_0, z_0) &= 0 \\ \frac{\partial f}{\partial x}(x_0, y_0, z_0) &= 0 \\ \frac{\partial f}{\partial y}(x_0, y_0, z_0) &= 0 \\ \frac{\partial f}{\partial z}(x_0, y_0, z_0) &= 0 \end{aligned}$$

**Definition 10.** *A curve* $X$ *with no singular points is called a smooth curve.*

Now, we introduce the function field of a curve. Let $f$ be an irreducible polynomial on $k[x,y]$, and $X$ be the curve over $k$ associated with $f$. We define the field of rational field as $k(X) = \text{Frac}\left(\dfrac{k[x,y]}{(f(x,y))}\right)$. At the same way, we define th field of rational function over $\bar{k}$ as $\bar{k}(X) = \text{Frac}\left(\dfrac{\bar{k}[x,y]}{(f(x,y))}\right)$.

1.1.5. *Morphisms between curves.* Let $X_1 = \{f = 0\}$, and $X_2 = \{g = 0\}$ be two curve defined over $k$.

**Definition 11.** *A regular map is a function $\phi\colon X_1 \to X_2$, with $\phi = [\varphi_0, \varphi_1, \varphi_2]$, where the functions $\varphi_0, \varphi_1$ and $\varphi_2 \in k(X_1)$, such that for any $p \in X_1$, $[\varphi_0(p) : \varphi_1(p) : \varphi_2(p)] \in X_2$*

Similarly, a morphism from $X_1$ to $\mathbb{P}^1$ is a tuple $[f,g]$ such that $f,g \in k(X_1)$, and for any $p \in X_1$, $[f(p) : g(p)] \in \mathbb{P}^1$. In this way, given $f \in k(X)$, it defines a morphism (that we also call $f$)

$$\begin{aligned} f\colon C &\longrightarrow \mathbb{P}^1 \\ p &\longmapsto [f(p):1], \end{aligned}$$

Conversly, let $\phi\colon X \to \mathbb{P}^1$, $\phi = [f,g]$, be a morphism $X_1 \to \mathbb{P}^1$. Then $f/g \in k(X)$.

Each morphism of curves has a field extension associated. Let's see this construction. Let $X_1/k$ and $X_2/k$ be curves defined over $k$, and let $\phi\colon X_1 \to X_2$ be a nonconstant morphism defined over $k$. Then, composition with $\phi$ induces a morphism of function fields

$$\phi^*\colon k(X_2) \to k(X_1)$$

defined as $\phi^*(f) = f \circ \phi$.

**Definition 12.** *The degree of a morphism $\phi\colon X_1 \to X_2$ is defined as the degree of the extension $k(X_1)/k(X_2)$.*

**Definition 13.** *We say that a morphism $\phi\colon X_1 \to X_2$ is separable (resp. inseparable or purely inseparable) if the corresponding extension $k(X_1)/k(X_2)$ is separable (resp. inseparable or purely inseparable).*

**Example 2.** *Let $\text{char}(k) = p > 0$, and let $q = p^r$. Let $f(x,y,z) \in k[x,y,z]$ be a homogeneous polynomial. We define $f^{(q)}$ be the polynomial obtained from $f$ by raising each coefficient of $f$ to the $q^{th}$-power. If $X$ is the projective curve defined by $f$, then we define the curve $X^{(q)}$ defined by the polynomial $f^{(q)}$. The Frobenious map $X \to X^{(q)}$ is defined by $[x_0 : x_1 : x_2] \mapsto [x_0^q : x_1^q : x_2^q]$*

Each morphism $\phi\colon X_1 \to X_2$ facts as

$$X_1 \to X_1^{(q)} \to X_2.$$

Here the morphism $X_1 \to X_1^{(q)}$ is the $q$-Frobenious map, and $X_1^{(q)} \to X_2$ is a separable morphism.

**Definition 14.** *Let $\phi\colon X_1 \to X_2$ be a morphism which factos as*

$$X_1 \to X_1^{(q)} \to X_2,$$

*Then the separable degree is defined as* $\deg_s(\phi) = [k(X_1^{(q)}) : k(X_2]$*, the inseparable degree is defines as* $\deg_i(\phi) = [k(X_1) : k(X_1^{(q)})]$

*Remark* 1.5.
$$\deg(\phi) = \deg_i(\phi) \cdot \deg_s(\phi)$$

*Remark* 1.6. If $k$ is of characteristic zero, then any nonconstant morphism between curves is separable

1.1.6. *Divisors.* The divisor group of a curve $X$, denoted by $\mathrm{Div}(X)$ is the free abelian group generated by the points of $X$.

A divisor $D \in \mathrm{Div}(X)$ is a formal sum
$$D = \sum_{p \in X} n_p \cdot p$$
where $n_p \in \mathbb{Z}$, and for almost all $p \in C$, $n_p = 0$.

The Galois group $\mathrm{Gal}(\bar{k}/k)$ acts on $\mathrm{Div}(X)$. If $\sigma \in \mathrm{Gal}(\bar{k}/k)$, and $D = \sum n_p \cdot p \in \mathrm{Div}(X)$, then
$$\sigma(D) = \sum_{p \in X} n_p \sigma(p).$$

**Definition 15.** *Let* $D \in \mathrm{Div}(X)$*. We say that* $D$ *is defined over* $k$*, if*
$$D = \sigma(D), \text{ for all } \sigma \in \mathrm{Gal}(\bar{k}/k).$$
*The subgroup of divisors defined over* $k$ *is denoted by* $\mathrm{Div}_k(X)$*.*

*Remark* 1.7. If a divisor $D = \sum_{p \in C} n_p p$ is defined over $k$, then it is not true in general that for any $p$ with $n_p \neq 0, p \in X(k)$.

Now we assume that the curve $X$ is smooth, and let $f \in \bar{k}(X)^\times$, then there is a divisor associated to $f$. This divisor is denoted by $\mathrm{div}(f)$ and is given by
$$\mathrm{div}(f) = \sum_{p \in X} \mathrm{ord}_p(f) \cdot p.$$

In this way we get a morphism $\mathrm{div} \colon \bar{k}(X)^\star \to \mathrm{Div}(X)$

**Definition 16.** *We say that a divisor* $D \in \mathrm{Div}(X)$ *is principal if there is* $f \in k(X)^\times$ *such that* $D = \mathrm{div}(f)$*. The subgroup of all principal divisors is denoted by* $\mathrm{Prin}(X)$

In the group $\mathrm{Div}(X)$, we introduce an equivalence relation, called linear equivalence. $D_1 \sim D_2$ if there is a function $f \in k(X)$ such that $D_1 - D_2 = \mathrm{div}(f)$, i.e. $D_1 - D_2 \in \mathrm{Prin}(X)$.

The quotient group $\mathrm{Div}(X)/\mathrm{Prin}(X)$ is called the Picard group and denoted by $\mathrm{Pic}(X)$.

1.2. **Elliptic curves.** The approach we take to define elliptic curves is via Weierstrass equations.

**Definition 17.** *A Weierstrass equation over* $k$ *is a cubic polynomial equation in two variables that looks like*
$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

If, in addition, $a_1 = a_2 = a_3 = 0$, then we have an equation of the form

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

which are called short Weierstrass equations.

**Definition 18.** *An elliptic curve over $k$ is a smooth projective curve $E \subset \mathbb{P}^2$ defined by the homogenization of a Weierstrass equation.*

Note that the point $O = [0 : 1 : 0]$ always belong to $E(k)$. $O$ is the unique point outside the affine chart $U_2$.

1.2.1. *Group law.* The set of $k$-rational points in an elliptic curve $E$ has a group structure. Before defining the group structure, we recall a geometric result. Let $L$ be a line in $\mathbb{P}^2$. Then $E \cap L$ has 3 points (counting multiplicities) by Bezout's theorem.

Let $p, q \in E(K)$, let $L$ the line throught $p$ and $q$. If $p = q$, the line $L$ is the tangent line at $p$. Let $r$ be the third intersection point between $E$ and $L$ (possibly $r = p$ or $r = q$). now let $L'$ be the line through $r$ and $O$. The third point of intersection between $E$ and $L$ is denoted by $p \oplus q$.

**Proposition 1.8.** *The function*

$$\begin{aligned} \oplus \colon E(k) \times E(k) &\longrightarrow E(k) \\ (p, q) &\longmapsto p \oplus q \end{aligned}$$

*has the following properties*

(a) *If a line $L$ intersect $E$ at the points $p, q$ and $r$, then $(p \oplus q) \oplus r = O$*
(b) *$p \oplus O = p$ for all $p \in E(k)$*
(c) *$p \oplus q = q \oplus p$ for all $p, q \in E(k)$*
(d) *for all $p \in E(k)$, there is a point $\ominus p$, such that*

$$p \oplus (\ominus p) = O$$

(e) *Let $p, q, r \in E(k)$. Then*

$$(p \oplus q) \oplus r = p \oplus (q \oplus r)$$

*Proof.* See Proposition 2.2 in [Sil09] □

**Corollary 1.9.** *$E(k)$ with the operation $\oplus$ form an abelian group.*

The following theorem, known as the Mordell-Weil theorem, gives the structure of the group $(E(k), \oplus)$.

**Theorem 1.10.** *Let $k$ be a number field, then $E(k)$ is finitely generated*

**Corollary 1.11.** *there exist a natural number $r$, and a finite subgroup $T$ of $E(k)$, such that*

$$E(k) \simeq \mathbb{Z}^r \oplus T$$

The number $r$ in the previous corollary is called the (algebraic) rank of $E$, and $T$ corresponds to torsion points.

## 2. Lecture 2: The arithmetic of elliptic curves

**Definition 19.** *Let $E_1$ and $E_2$ be elliptic curves. An isogeny from $E_1$ to $E_2$ is a nonzero morphism*

$$\phi\colon E_1 \to E_2$$

*such that $\phi(O_{E_1}) = O_{E_2}$*

We visit some neccesary results on isogenies in order to understand the structure of the set of $m$-torsion points of an elliptic curve.

**Theorem 2.1.** *Let $\phi\colon E_1 \to E_2$ be a nonzero isogeny, then*

(a) *For every $Q \in E_2$*

$$\#\phi^{-1}(Q) = \deg_s(\phi).$$

*In particular if $\phi$ is separable, then*

$$\#\ker(\phi) = \deg(\phi)$$

*Proof.* See Theorem 4.10 in [Sil09]. □

In particular if $E = E_1 = E_2$, then an isogeny $E \to E$ is called an endomorphism. The set of endomorphisms (denoted by $\mathrm{End}(E)$) is endowed with a ring structure. Let $\phi, \psi \in \mathrm{End}(E)$, then the sum is as functions, and the product is defined by the composition. The ring $\mathrm{End}(E)$ is a free $\mathbb{Z}$-algebra. For curves over fields of charcateristic zero, $\mathrm{End}(E)$ is either $\mathbb{Z}$ or an order $\mathcal{O}$ in a quadratic imaginary extension of $\mathbb{Q}$.

**Definition 20.** *Let $k$ be a field of characteristic zero. If $E/k$ is an elliptic curve. We say that $E$ has real multiplication if $\mathrm{End}(E) \simeq \mathbb{Z}$. On the other hand, if $\mathrm{End}(E)$ is isomorphic to an order in a quadratic imaginary extension of $\mathbb{Q}$, then we say that $E$ has complex multiplication, or simply we say that $E$ is a CM curve.*

If $k$ has positive charcateristic, then $\mathrm{End}(E)$ can be also isomorphic to an order in a quaternion algebra.

Given $E$ an elliptic curve, and a integer $m$, there is a dintinguished isogeny.

$$\begin{aligned}[m]\colon E(k) &\longrightarrow E(k)\\ p &\longmapsto \underbrace{p \oplus p \oplus \cdots \oplus p}_{m\text{-times}}\end{aligned}$$

If $\phi\colon E_1 \to E_2$ is an isogeny of degree $m$, then there exists an isogeny in the other direction $\hat{\phi}\colon E_2 \to E_1$, which is called the dual isogeny and such that $\hat{\phi} \circ \phi = [m]$. Some of the properties of the dual isogenies are summarized in the following proposition

**Proposition 2.2.** *Let $\phi, \psi\colon E_1 \to E_2$ be two isogenies from $E_1$ to $E_2$, and $\lambda$ an isogeny from $E_2 \to E_3$, then*

(i) *let $m = \deg(\phi)$, then $\hat{\phi} \circ \phi = [m]$*
(ii) $\widehat{\lambda \circ \phi} = \hat{\lambda} \circ \hat{\phi}$
(iii) $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$
(iv) $\widehat{[m]} = [m]$
(v) $\deg(\phi) = \deg(\hat{\phi})$

(vi) $\hat{\hat{\phi}} = \phi$

*Proof.* See for example Theorem 6.2 in [Sil09] □

Now we study the points of $m$-torsion. The subgroup of $m$-torsion is defined as $\ker([m])$ and we denote it by $E[m]$. In other words $E[m] = \{p \in E : [m]p = 0\}$. Similarly, the $k$-rational points $E[m](k) = \{p \in E(k) : [m]p = 0\}$.

As the isogenies $[m]$ are defined over $k$, we have that for any $\sigma \in \mathrm{Gal}(\bar{k}/k)$, $\sigma([m]p) = [m]\sigma(p)$. We conclude that $\mathrm{Gal}(\bar{k}/k)$ acts on $E[m]$ for all $m$.

Now we explore the structure of the set $E[m]$.

**Proposition 2.3.** *Let $E$ be an elliptic curve and let $m \in \mathbb{Z}$.*

(a) $\deg([m]) = m^2$

(b) *If* $\mathrm{char}(k) = 0$ *or* $p = \mathrm{char}(k) > 0$ *and* $p \nmid m$, *then*

$$E[m] \simeq \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}$$

(c) *If* $\mathrm{char}(k) = p$, *then one of the following hold*

(i) $E[p^e] = \{O\}$ *for all* $e \in \mathbb{N}$

(ii) $E[p^e] = \dfrac{\mathbb{Z}}{p^e\mathbb{Z}}$ *for all* $e \in \mathbb{N}$.

*Proof.*

(a) As we saw previously, $\widehat{[m]} = [m]$. Then if $d = \deg([m])$, we have

$$[d] = [m] \circ \widehat{[m]} = [m] \circ [m] = [m^2].$$

We know that the ring of endomorphisms is torsion free $\mathbb{Z}$-module. The we conclude $d = m^2$.

(b) Since $\mathrm{char}(k) \nmid m$, we have that the isogeny $[m]$ is separable. Then by Theorem Theorem 2.1(b), we have

$$\#E[m] = \deg[m] = m^2.$$

Additionally, for any prime divisor $p$ of $m$, we have

$$E[p] = \frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}},$$

by the classification of abelian groups of order $p^2$. This is now an exercide of group theory to prove that this implies that

$$E[m] \simeq \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

(c) Let $\phi$ be the Frobenious morphism

$$\begin{aligned} \#E[p^e] &= \deg_s[p^e] \\ &= (\deg_s(\hat{\phi} \circ \phi))^e \\ &= (\deg_s \hat{\phi})^e \end{aligned}$$

If $\hat{\phi}$ is inseparable, then $E[p^e] = 1$. On the other hand, if $\hat{\phi}$ is separable, then

$$E[p^e] \simeq \mathbb{Z}/p^e\mathbb{Z}.$$

□

**Theorem 2.4** (Serre's Theorem). *Let $E$ be an elliptic curve over a number field $k$ and suppose that for an infinite set of primes $p$ the image of $\mathrm{Gal}(\bar{k}/k)$ acting on the $p$-torsion points of $E$ is strictly smaller than $\mathrm{GL}_2(\mathbb{F}_p)$. Then $E$ has CM.*

2.0.1. *Tate module.* Let $k$ be a field such that $\mathrm{char}(k)$ or $\mathrm{char}(k) \nmid m$. As we saw in previous sections, $\mathrm{Gal}(\bar{k}/k)$ acts on $E[m]$. Equivalently, there exists a map $\mathrm{Gal}(\bar{k}/k) \to \mathrm{Aut}(E[m]) \simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. In this way we construct a Galois representation associated to $E$. In order to construct a Galois reprepresentation over a ring of characteritic zero, we introduce the Tate module. Let $\ell$ be a prime number. Multiplication by $\ell$ define a group morphism between $E[\ell^{n+1}]$ and $E[\ell^n]$. In this way $(E[\ell^n], [\ell])$ form an inverse system. We define the $\ell$-adic Tate module of $E$ as the inverse limit

$$T_\ell(E) = \varprojlim E[\ell^n]$$

*Remark* 2.5. As each $E[\ell^n]$ is a $\mathbb{Z}/\ell^n\mathbb{Z}$-module, we conclude that $T_\ell(E)$ is a $\mathbb{Z}_p$-module

**Proposition 2.6.** *As a $\mathbb{Z}_\ell$, the Tate module has the following structure*

(i) $T_\ell(E) \simeq \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ *if* $\ell \neq \mathrm{char}(k)$
(ii) $T_\ell(E) \simeq \{0\}$ *or* $\mathbb{Z}_\ell$ *is* $\ell = \mathrm{char}(k) > 0$.

*Proof.* This is consequence of Proposition 2.3. □

The action of $\mathrm{Gal}(\bar{k}/k)$ on $E[\ell^n]$ commute with the multiplication by $\ell$, then $\mathrm{Gal}(\bar{k}/k)$ acts on $T_\ell(E)$. Moreover, since $\mathrm{Gal}(\bar{k}/k)$ acts continuosly on each finite group $E[\ell^n]$, then the action on $T_\ell(E)$ is continuos.

Now we can define the $\ell$-adic representation associated to $E$.

**Definition 21.** *The $\ell$-adic representation of $\mathrm{Gal}(\bar{k}/k)$ associated to $E$ is the homomorphism*

$$\rho_{E,\ell} \colon \mathrm{Gal}(\bar{k}/k) \to \mathrm{Aut}(T_\ell(E))$$

*induced by the action of $\mathrm{Gal}(\bar{k}/k)$ on the $\ell^n$-torsion points of $E$.*

If $\mathrm{char}(k)$ is zero or $\ell \nmid \mathrm{char}(k)$, then $T_\ell(E)$ is a free $\mathbb{Z}_\ell$-module of rank 2. If we take a $\mathbb{Z}_\ell$-basis for $T_\ell(E)$, then the $\ell$-adic representation look like

$$\mathrm{Gal}(\bar{k}/k) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$$

In particular, since $\mathbb{Z}_p \subset \mathbb{Q}_\ell$, then we can see the $\ell$-adic representation as the morphism

$$\mathrm{Gal}(\bar{k}/k) \to \mathrm{GL}_2(\mathbb{Q}_\ell).$$

2.0.2. *Functiorality of Tate module.* Let $E_1$, $E_2$ be elliptic curves, and $\phi \colon E_1 \to E_2$ be an isogeny. The isogeny $\phi$ induce a group homomorphism (also called $\phi$)

$$\phi \colon E_1[\ell^n] \to E_2[\ell^n].$$

Moreover, this induce a $\mathbb{Z}_\ell$-linear map

$$\phi_\ell \colon T_\ell(E_1) \to T_\ell(E_2).$$

In this way we obatain a group homomorphism

$$\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}(T_\ell(E_1), T_\ell(E_2))$$

2.0.3. *Weil pairing.* Let $k$ be a field of charateristic not dividing a fixed integer $m$. Let $\mu_m$ be the set of $m^{\text{th}}$-root of unities. The idea is construct a bilinear, alternating, not degenerate and Galois invariant pairing

$$e_m\colon E[m] \times E[m] \to \mu_m.$$

For the construction we need 2 lemmas.

**Lemma 2.7.** *Let $X_1, X_2$ be two projective algebraic curves. Then any non-constant morphism $\phi\colon X_1 \to X_2$ is surjective*

*Proof.* See theorem II.2.3 in [Sil09] □

**Lemma 2.8.** *Let $E$ be an elliptic curve and let $D = \sum n_p p \in \operatorname{Div}(E)$. Then $D$ is a principal divisor if and only if*

$$\sum_{p\in E} n_p = 0 \text{ and } \sum_{p\in E} [n_p]p = O.$$

*Proof.* See Corollary III.3.5 in [Sil09] □

Next, we construct the Weil pairing.

Let $T \in E[m]$. Then there is a function $f \in \bar{k}(E)$ satisfying

$$\operatorname{div}(f) = m(T) - m(O).$$

Take $T' \in E$ a point such that $[m]T' = T$. Similarly, there is function $g \in \bar{k}(E)$ satisfying

$$\operatorname{div}(g) = \sum_{R\in E[m]} (T' + R) - (R).$$

We note $f \circ [m] = g^m$ have the same divisor. Up to multiplying by a constant from $\bar{k}^\times$, we have

$$f \circ [m] = g^m.$$

Let $S \in E[m]$, and $X \in E$. Then

$$g(X + S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m.$$

For any $X$, $g(X + S)/g(X)$ is a $m^{\text{th}}$-root of unity. Then the morphism $E \to \mathbb{P}^1$ such that $X \mapsto g(X + S)/g(X)$ is not surjective. Then we conclude that it is constant.

**Definition 22.** *The Weil pairing is the function*

$$e_m\colon E[m] \times E[m] \to \mu_m$$

*defined by*

$$e_m(S, T) = \frac{g(X + S)}{g(X)}$$

**Proposition 2.9.** *The Weil pairing satifies the following properties:*

(a) *Bilinear*

$$e_m(S_1 + S_2, T) = e_m(S_1, T)E_m(S_2, T)$$
$$e_m(S, T_1 + T_2) = E_m(S, T_1)e_m(S, T_2).$$

(b) *Alternating*

$$e_m(T,T).$$

*In particular* $e_m(S,T) = e_m(T,S)$.

(c) *Nondegenerate: if* $e_m(S,T) = 1$ *for all* $S \in E[m]$*, then* $T = O$

(d) $e_m$ *and* $e_{mm'}$ *are compatible. This means*

$$e_{mm'}(S,T) = e_m([m']S,T)$$

*for all* $S \in E[mm']$ *and* $T \in E[m]$

(e) *Galois invariant. Let* $\sigma \in \mathrm{Gal}(\bar{k}/k)$*, then*

$$\sigma(e_m(S,T)) = e_m(\sigma(S),\sigma(T)).$$

*Proof.* See Proposition III.8.1 in [Sil09]. □

In particular if $m = \ell^n$, then we have the $\ell^n$-Weil pairing

$$e_{\ell^n} \colon E[\ell^n] \times E[\ell^n] \to \mu_{\ell^n}.$$

Note that $\mu_{\ell^n}$ with the morphisms $\mu_{\ell^{n+1}} \to \mu_{\ell^n}$ with send $\zeta \to \zeta^\ell$ is a compatible inverse system. We define the Tate module of $\mu$ as

$$T_\ell(\mu) = \varprojlim \mu_{\ell^n}.$$

Then taking inverse limit in the $e_{\ell^n}$-Weil pairing, we get the $\ell$-adic Weil pairing

$$e \colon T_\ell(E) \times T_\ell(E) \to T_\ell(\mu).$$

2.0.4. *Cyclotomic character.* Let $k$ be a number field. Let $\ell$ be a prime number, and $\mu_{\ell^n}$ the set of $\ell^{\mathrm{n}}$-root of unity. Then $\mathrm{Gal}(\bar{k}/k)$ acts on $\mu_{\ell^n}$. If $\zeta$ is a primitive root of unity, then for any $\sigma \in \mathrm{Gal}(\bar{k}/k)$, then there is an element $a(\sigma,n) \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times$ such that

$$\sigma(\zeta) = \zeta^{a(\sigma,n)}.$$

This define a Galois representation

$$\mathrm{Gal}(\bar{k}/k) \to \mathrm{Aut}(\mu_{\ell^n}) \simeq (\mathbb{Z}/\ell^n\mathbb{Z})^\times$$

that is called the cyclotomic character.

Using the Weil pairing, we can see that the determinant character of the Galois representation coincide with the cyclotomic character.

Let $\sigma \in \mathrm{Gal}(\bar{k}/k)$. Taking a basis $\{S,T\}$ of $E[\ell^n]$ as a $\mathbb{Z}\ell^n\mathbb{Z}$-module, then $\sigma$ acts as matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then $\sigma S = aS + cT$, and $\sigma T = bS + dT$.

$$\begin{aligned}
\sigma(\zeta) &= \sigma(e(S,T)) \\
&= e(\sigma(S),\sigma(T)) \\
&= e(aS+cT, bS+dT) \\
&= e(aS,bS)e(aS,dT)e(cT,bS)e(cT,dT) \\
&= e(S,S)^{ab}e(S,T)^{ad}e(T,S)^{cb}e(T,T)^{cd} \\
&= e(S,T)^{ad}e(TS)^{cd} \\
&= e(S,T)^{ad-bc} \\
&= \zeta^{ad-bc}.
\end{aligned}$$

## 3. Lecture 3:Subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$

We recall that a Galois representation mod $p$ coming from an elliptic curve is a group homomorphism

$$\rho\colon \mathrm{Gal}(\bar{k}/k) \to \mathrm{GL}_2(\mathbb{F}_p).$$

The image of $\rho$ is a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. In this lecture we study and classify the subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. We begin recalling to basic definitions of group theory. First, we recall the notion of maximal subgroup. Let $G$ be a group, and $H \subset G$ be a subgroup. $H$ is said maximal if for any other subgroup $K$ of $G$ with $H \subset K \subset G$, we have $K = H$ or $K = G$.

Let $G$ be a group and $H \subset G$ be a subgroup. The normalizer of $H$ in $G$ is defined by

$$N_G(H) = \left\{ g \in G | gHg^{-1} = H \right\}.$$

Now we introduce some kind of subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$.

**Definition 23.** *Any subgroup of* $\mathrm{GL}_2(\mathbb{F}_p)$*, which up to conjugation is of the form*

$$\left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}; a,b,d \in \mathbb{F}_p \right\}$$

*is called a Borel subgroup.*

**Definition 24.** *Let* $\epsilon \in \mathbb{F}_p^\times$ *be a non-square. We define to kind of subgroups*

(i) *Any subgroup of* $\mathrm{GL}_2(\mathbb{F}_p)$*, which up to conjugation is of the form*

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}; a,d \in \mathbb{F}_p \right\}$$

*is called a* ***split Cartan*** *subgroup.*

(ii) *Any subgroup of* $\mathrm{GL}_2(\mathbb{F}_p)$*, which up to conjugation is of the form*

$$\left\{ \begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix}; a,b \in \mathbb{F}_p \right\}$$

*is called a* ***nonsplit Cartan*** *subgroup.*

Finally we define the probably the most famous subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$, namely the special linear subgroup and the scalar matrices.

**Definition 25.** *The **special linear group** denoted by $\mathrm{SL}_2(\mathbb{F}_p)$ is defined as*

$$\mathrm{SL}_2(\mathbb{F}_p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}; ad - bc = 1 \right\}.$$

**Definition 26.** *The subgroup of scalar matrices is defined by*

$$Z = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}; a \in \mathbb{F}_p \right\}.$$

Additionally we introduce a quotient of $\mathrm{GL}_2(\mathbb{F}_p)$ which is called the **projective linear group** over $\mathbb{F}_p$. This group is

$$\mathrm{PGL}_2(\mathbb{F}_p) = \mathrm{GL}_2(\mathbb{F}_p)/Z.$$

We are now in a position to state the classification theorem of the subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$.

**Theorem 3.1** (Classification of maximal subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$)**.** *Let $G$ be a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ be a maximal subgroup (respect to inclusion order). Then one of the following hold*

(i) $\mathrm{SL}_2(\mathbb{F}_p)$ *is contained in $G$.*
(ii) *$G$ is a Borel subgroup*
(iii) *$G$ is the normalizer of a Cartan subgroup*
(iv) *The image of $G$ in $\mathrm{PGL}_2(\mathbb{F}_p)$ via the quotient map $\mathrm{GL}_2(\mathbb{F}_p) \twoheadrightarrow \mathrm{PGL}_2(\mathbb{F}_p)$ is isomorphic to $A_4, S_4$ or $A_5$.*

If $p = 2$, then the group $\mathrm{GL}_2(\mathbb{F}_2)$ is not difficult to understand. In the following exercise we explore this group.

**Exercise 1.** (i) *Show that $GL_2(\mathbb{F}_2)$ has 6 elements*
(ii) *Prove that $\mathrm{GL}_2(\mathbb{F}_2)$ is a non-abelian group.*
(iii) *conclude that $\mathrm{GL}_2(\mathbb{F}_2) \simeq S_3$.*

### 3.1. **Subgroup of order divisible by $p$.**

**Lemma 3.2.** *Let $A$ be a matrix in $\mathrm{GL}_2(\mathbb{F}_p)$ of order p, i.e. $A^p = I$. Then $A$ is contained in a Borel subgroup.*

*Proof.* Let $A$ be a matrix of order $p$. Let $\{L_1, ..., L_{p+1}\}$ the set of all lines in $\mathbb{F}_p^2$ passing through $(0, 0)$. The matrix $A$ sends a line $L_i$ to another line $L_j$. As the set of lines has cardinality $p + 1$ and the order of $A$ is $p$, we conclude that there exists a line fixed by the action of $A$.

Let $L$ be the line fixed by $A$, and $v$ be a vector in the line $L$. Since $A$ fixes $L$, there is $\lambda \in \mathbb{F}_p^\times$ such that $Av = \lambda v$. We conclude that $v$ is an eigenvector of $A$. On the other hand, there is not another eigenvector $u$ lineraly independent to $v$. If $u, v$ l.i. eigenvector of $A$. Then $A$ is diagonalizable, which implies that up to conjugation, it is a diagonal matrix. It is a contradiction, because the diagonal matrix has order $p - 1$. On the other hand, $A$ has to $\lambda$ as its unique eigenvalue, otherwise if $\mu$ is an eigenvalue, then $Aw = \mu w$. As $\mu \neq \lambda$, then $w$ is l.i. to $v$. So, the characteristic polynomial of $A$ is $(x - \lambda)^2$.

Equivalently, we have $\mathrm{im}(A - \lambda I) = \langle v \rangle$ which is of dimension 1. We conclude that up conjugacy, $A$ has the form $\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$. As $A$ has order $p$, we conclude that up to conjugation, $A$ has the form $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. In this way we conclude that any element of order $p$ belong to a Borel subgroup. □

**Lemma 3.3.** *Suppose that a subgroup $G \subset \mathrm{GL}_2(\mathbb{F}_p)$ contains two order $p$ elements, such that neither of which is a power of the other. Then $G$ contains $\mathrm{SL}_2(\mathbb{F}_p)$.*

*Proof.* We begin recalling the group $\mathrm{SL}_2(\mathbb{Z})$. This group is defined as the group 2x2 matrix with entries in $\mathbb{Z}$ and determinant 1. We define two distinguished elemts in $\mathrm{SL}_2(\mathbb{Z})$.

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

It is well-known that $T$ and $S$ generate $\mathrm{SL}_2(\mathbb{Z})$. We define also the matrix

$$U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

We can check $T = S^{-1}US$. Then $U$ and $S$ generate $\mathrm{SL}_2(\mathbb{Z})$. We take now the projection $\mathrm{SL}_2(\mathbb{Z}) \twoheadrightarrow \mathrm{SL}_2(\mathbb{F}_p)$, which send each matrix to its reduction module $p$. Since this morphism is surjective, the image of $U$ and $S$ generate $\mathrm{SL}_2(\mathbb{F}_p)$.

Since $G$ cointains two matrices or order $p$, which is not a power of each other, up to conjugation we can assume that theses matrices have the form

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Since these matrices generate $\mathrm{SL}_2(\mathbb{F}_p)$, we conclude $\mathrm{SL}_2(\mathbb{F}_p) \subset G$. □

3.2. **Elements of order prime to $p$.** We Study some geometric properties of Cartan subgroups. Let $G$ be a split Cartan subgroup, and let $D$ be the subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ defined by $\left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}; a, d \in \mathbb{F}_p \right\}$. There is an invertible matrix $B$, such that $G = BDB^{-1}$

Since the matrices in $D$ fix the lines $\ell_1 = \left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\rangle$, and $\ell_2 = \left\langle \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\rangle$, then the group $G$ fixed the lines $L_1 = B\ell_1$ and $L_2 = B\ell_2$. We conclude that any split Cartan subgroup fix two lines in $\mathbb{F}_p^2$. Conversly, given two lines, there is a unique split Cartan subgroup such that fix each line.

Now we explore the geometric characterization of the non-split Cartan subgroup. Let $\sigma \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ such that $\sigma^2 = \epsilon \in \mathbb{F}_p^\times$. Let $C$ be a nonsplit Cartan subgroup which is conjugate to the group

$$\left\{ \begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix} \right\}$$

Let $A = B \begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix} B^{-1}$ for some matrix $B$. be a matrix in $G$. A direct computation give us that $a + b\sigma$ and $a - b\sigma$ are the eigenvalues of $A$, $\begin{pmatrix} 1 \\ \sigma \end{pmatrix}$, and $\begin{pmatrix} -1 \\ \sigma \end{pmatrix}$ its corresponding eigenvectors. We conclude that the group $G$ fix two lines over $\mathbb{F}_{p^2}$. Then we conclude that any nonsplit Cartan subgroup is the stabilizer of two lines defined over $\mathbb{F}_{p^2}$ but not over $\mathbb{F}_p$.

**Lemma 3.4.** *Let $A$ be a non-scalar matrix with order prime to $p$ belongs to a unique Cartan subgroup.*

*Proof.* Let $A \in \mathrm{GL2}(\mathbb{F}_p)$ be a matrix of order coprime to $p$ nad non-scalar. We have that $A$ has two distinct eigenvalues over $\mathbb{F}_{p^2}$ (Check!). If this eigenvalues are defined over $\mathbb{F}_p$, then $A$ stabilize two lines in $\mathbb{F}_p^2$. In this case $A$ belong to a split-Cartan group. On the other hand, if the eigenvalues are in $\mathbb{F}_{p^2}$, then $A$ has 2 eigenvector in $\mathbb{F}_{p^2}^2$. We conclude that $A$ fixes two lines defined over $\mathbb{F}_{p^2}$. In this way we conclude that any matrix with order coprime to $p$ belong to a Cartan subgroup. □

3.3. **Subgroup of $\mathrm{PGL}_2(\mathbb{F}_p)$.** Next, we state a classification theorem of subgroups of $\mathrm{PGL}_2(\mathbb{F}_p)$, whose proof it is tedious. The proof of this theorem will be added as an appendix.

**Theorem 3.5.** *Let $H \subset \mathrm{PGL}_2(\mathbb{F}_p)$ be a subgroup of order prime to $p$. If $H$ is not cyclic or dihedral, then $H$ is either isomorphic to $A_4$, $S_4$ or $A_5$.*

*Proof.* See section 2.5 in [Ser72]. □

Now we only need to deal with the case of cyclic and dihedral subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$.
The content of the following 2 theorems is precisely that.

**Theorem 3.6.** *Let $G$ be a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ such that the image of $G$ in $\mathrm{PGL}_2(\mathbb{F}_p)$ is cyclic and $|G|$ coprime to $p$. Then $G$ is contained in a Cartan subgroup.*

*Proof.* Let $g \in G$ such that its image $\bar{g}$ in $\mathrm{PGL}_2(\mathbb{F}_p)$ is a generator of the image of $G$. We observe that $G = \langle Z, g\rangle$. As we saw before, $g$ should be belong in a Cartan subgroup, since $g$ has order coprime to $p$. □

**Theorem 3.7.** *Let $G$ be a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ such that the image of $G$ in $\mathrm{PGL}_2(\mathbb{F}_p)$ is a dihedral group with $|G|$ coprime to $p$. Then $G$ is contained in the normalizer of a Cartan subgroup*

*Proof.* Since $G \subset \pi^{-1} \circ \pi(G)$, it is enough to show the last one is contained in the normalizer of a Cartan subgroup. Let $H$ be the cyclic subgroup of $\pi(G)$ or order $\#\phi(G)/2$. $\phi(G)$ is the normalizer of $H$ in $\phi(G)$. Then $\phi^{-1}(H)$ is the normalizer of $\phi^{-1}(H)$ in $\phi^{-1}(\phi(G))$. since $\phi^{-1}(H)$ is cyclic coprime to $p$, then it is contained in a Cartan. Then $\phi^{-1}(\phi(G))$ is contained in the normalizer of a Cartan. □

In this way we conclude the classification of maximal subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$.

## References


[Ful08] William Fulton, *Algebraic curves*, An Introduction to Algebraic Geom **54** (2008).

[Har13] Robin Hartshorne, *Algebraic geometry*, vol. 52, Springer Science & Business Media, 2013.

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

[Sil09] Joseph H Silverman, *The arithmetic of elliptic curves*, vol. 106, Springer, 2009.

[SR94] Igor Rostislavovich Shafarevich and Miles Reid, *Basic algebraic geometry*, vol. 2, Springer, 1994.



Departamento de Matemáticas, Pontificia Universidad Católica de Chile. Facultad de Matemáticas, 4860 Av. Vicuña Mackenna, Macul, RM, Chile

*Email address*, M. Alvarado: mnalvarado1@uc.cl