THE ÉTALE FUNDAMENTAL GROUP OF AN ELLIPTIC CURVE

ARNAB KUNDU

Abstract. We first look at the fundamental group, and try to find a suitable definition that can be simulated for algebraic varieties. In the next couple of sections we give a summary of the theory of Elliptic curves and étale maps. In the last section we define the finite étale site and define the étale fundamental group. Finally we compute the étale fundamental group of an Elliptic curve.

Contents

Introduction

The fundamental group is a topological invariant that measures how well connected a space is. For a well behaved topological space there is a space called the universal cover whose group of deck transformation gives the fundamental group. This nice topological construction can be used to classify all finite covers of the space; in fact there is a correspondence between finite quotients of the fundamental group and finite covers of the space. Varieties over complex numbers have a natural complex manifold structure and hence along with the algebraic structure they reveal topological structure as well. It is natural to ask if the fundamental group in the case of varieties over complex number can be computed algebraically. The answer is that the finite covers which can be defined algebraically reveal almost all of the fundamental group. The strength of this approach is in the fact that this could be generalized to other fields, whatever their characteristic may be.

The main aim of this article is to first motivate this approach, provide the framework of it and in the end explicitly compute the fundamental group of Elliptic curves. The first section is the motivation, the second and third are some background definitions and results. The fourth section states and proves most of the important results for the computations. The last section introduces the finite étale site and computes the fundamental groups.

1. Fundamental Group

Given any space there are algebraic invariants that can be used to measure certain geometric behavior, for example the fundamental group measures how well connected the space is, and the cohomology calculates how well local functions glue together to give global functions. Since varieties over $\mathbb{C}$ are naturally complex manifolds, we have access to all of these invariants when doing algebraic geometry over $\mathbb{C}$. But this approach does not work in positive characteristic.

In this section, we shall deal only with smooth connected real manifolds (in fact Riemann surfaces). The topological spaces are pointed without mention and continuous maps are based. The topological spaces shall be written as (X, x_0) to denote a space X with chosen base point $x_0 \in X$.

Definition 1.1. Given a real (or complex) manifold (X, x_0), we define the *fundamental group* to be $\left[S^1, (X, x_0)\right]_*$, that is pointed homotopy classes of pointed maps from S^1 to (X, x_0). Concatenation of paths gives the structure of a group. This will be denoted by $\pi_1(X, x_0)$ or simply $\pi_1(X)$.

Examples 1.2. Some computed values

(i) $\pi_1(\mathbb{C}^\times) = \mathbb{Z}$, a generator is given by the inclusion of the unit circle into $\mathbb{C}^*$.
(ii) $\pi_1(\mathrm{S}^1 \times \mathrm{S}^1) = \mathbb{Z}^2$, generators are given by the two inclusions $\theta \mapsto (\theta, 0)$ and $\theta \mapsto (0, \theta)$.

Definition 1.3. Let X be a real (or complex) manifold. Then a pair (Y, p) of a real (or complex) manifold Y with a surjective map $p : Y \to X$ is said to *cover* X if the following condition is satisfied. Given any point $x \in X$, there exists an open subset $U \subset X$, such that $p^{-1}(U)$ is a disjoint union of open subsets $U_\alpha \subset Y$ and the map restricted to each U_α, $p : U_\alpha \to U$ is a homeomorphism.

Example 1.4. Covers of $\mathbb{C}$ and $\mathbb{C}^\times$

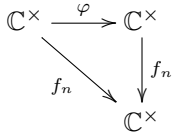
(i) Consider the pair $(\mathbb{C}^\times, f_n)$ with the map $f_n : \mathbb{C}^\times \longrightarrow \mathbb{C}^\times$ defined to be $z \mapsto z^n$. This is an example of an n-sheeted covering.
(ii) The universal covering of $\mathbb{C}^\times$ is $(\mathbb{C}, \pi)$ with the map $\pi : \mathbb{C} \to \mathbb{C}^\times$ defined to be $z \mapsto e^z$.

Observe that f_n is an isomorphism if and only if n equals 1.

Remark 1.5. We note that the covering maps f_n are actually polynomial maps and hence algebraic. However the universal covering π is an exponential map and cannot be realized as an algebraic map.

Now it is natural to ask if the finite covers of $\mathbb{C}^\times$, as given above, reveal the fundamental group. Although, as we shall see, it is not possible to completely recover the fundamental group of $\mathbb{C}^\times$; we may get its profinite completion as a limit of the automorphism group of these finite covers. In simple terms we can approximate the fundamental group by the finite covers and we are able to extract almost the fundamental group. The construction given below is a motivation for building the category defined in Section 5. Let $f_n : \mathbb{C}^\times \to \mathbb{C}^\times$ denote the same maps as in Example 1.4. We define the *automorphism group* $\mathrm{Aut}(\mathbb{C}^\times, f_n)$ to be the group of deck transformations of the cover, that is those maps $\varphi : (\mathbb{C}^\times, f_n) \to (\mathbb{C}^\times, f_n)$

that commute the following diagram:

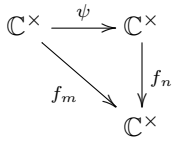


It is easy to see that $\mathrm{Aut}(\mathbb{C}^\times, f_n)$ equals $\mathbb{Z}/n\mathbb{Z}$. These are "*regular*", that is the action of the deck transformations on the fibers is free and transitive. It is worth noting that the action of the fundamental group, which factors through the above action, is also transitive.

Remark 1.6. Suppose X is a real manifold. We invoke from covering space theory the correspondence between quotients of the fundamental group $\pi_1(X)$ and coverings of the space X. Two facts from the theorem shall be relevant to us, and they are listed below.

- For every quotient G of $\pi_1(X)$, there exists a unique cover Y, up to isomorphism, of X with G as the group of deck transformations of Y over X.
- For every finite quotient G of $\pi_1(X)$, the above correspondence produces a finite regular cover of X.

Given the facts, we may consider the directed set $I = \mathbb{Z}_{>0}$ with the ordering $n \leq m \iff n \mid m$, and the system of covers $\{(\mathbb{C}^\times, f_n)\}_{n\in I}$. We apply the correspondence stated above to $X = \mathbb{C}^\times$. We know that $\pi_1(\mathbb{C}^\times) = \mathbb{Z}$. A finite quotient of $\mathbb{Z}$ is of the form $\mathbb{Z}/n\mathbb{Z}$ for some integer n, and thus the above system forms the complete set of finite regular covers of $\mathbb{C}^\times$. Moreover, if $n \mid m$ then the cover $(\mathbb{C}^\times, f_n)$ "dominates" the cover $(\mathbb{C}^\times, f_m)$, or in other words there is a map ψ such that the following digram commutes:



Thus they form an inverse system of finite regular covers of $\mathbb{C}^\times$. We could check that $\mathrm{Aut}(\mathbb{C}^\times, f_n) = \mathbb{Z}/n\mathbb{Z}$ and the limit of inverse system of automorphism groups is $\varprojlim_n \mathrm{Aut}(\mathbb{C}^\times, f_n) = \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}$. This is the profinite completion of the topological fundamental group, which is $\mathbb{Z}$. Therefore we have extracted almost the fundamental group by using only the finite regular covers. This shall serve as motivation for defining the "fundamental group" itself to be the limit of the inverse system of the finite regular covers, which we do in the last section.

2. Curves

In this section we shall define curves and state some of the fundamental properties of them. Before that we need to recall some basic definitions.

Fix an algebraically closed field K. We denote the projective n-scheme over K by $\mathbb{P}^n_K \coloneqq \operatorname{Proj} K[x_0, \ldots, x_n]$.

Definition 2.1. We define a *variety* over K to be an integral, separated scheme of finite-type over K. The dimension of a variety is its dimension as a noetherian

topological space. A variety is called *complete* if it is proper over K. A *curve* is defined to be a complete variety of dimension 1 over K.

Examples 2.2. Suppose char$K$ is different from 2 or 3. Consider the equation $y^2 = x^3+Ax+B$ where A and B are elements of K satisfying that $\Delta = -16(4A^3+27B^2)$ is nonzero. Then $\operatorname{Spec} K[x,y]/(y^2 - x^3 - Ax - B)$ is an affine smooth scheme of dimension 1. The nonsingular completion of the above is the non-singular projective curve $\operatorname{Proj} K[x,y,z]/(y^2z - x^3 - Axz^2 - Bz^3)$.

Let C be a curve with structure sheaf $\mathcal{O}_C$. At any point $P \in C$ we denote the local ring at P by $\mathcal{O}_{P,C}$ and maximal ideal of the local ring by $m_{P,C}$. When there is no risk of confusion, the notation shall be simplified to $\mathcal{O}_P$ and m_P respectively. The residue field $\mathcal{O}_P/m_P$ at P shall be denoted by $\kappa(P)$.

Definition 2.3. Let C be a curve over a field K. The curve is said to be non-singular at a closed point $P \in C$ if $\dim_{\kappa(P)} \left(m_P/m_P^2\right) = 1$. The curve C is said to be *non-singular* if it is non-singular at every closed point $P \in C$.

The $\kappa(P)$-vector space m_P/m_P^2 is the Zariski cotangent space and hence asking the vector space to be dimension 1 is a natural definition for non-singularity. It can be checked that the projective curve given in Example 2.2 is non-singular.

Definition 2.4. Given a curve C over K, its *function field* is defined to be the local ring $\mathcal{O}_\eta$ at its generic point $\eta \in C$. It shall be denoted by $K(C)$. Suppose P is any closed point of the curve. The *valuation* of a non-zero element $f \in \mathcal{O}_P$ is the largest integer n such that $f \in m_P^n$. This integer shall be denoted by $v_P(f)$. This valuation can be extended to $K(C)^\times$ by defining the valuation of f/g by $v_P(f/g) = v_P(f) - v_p(g)$, where f and g are non-zero rational functions. An element is said to have a *zero, pole* or is *non-vanishing* at P if $v_P(f)$ is positive, negative or zero respectively.

Definition 2.5. Let $\varphi : C_1 \to C_2$ be a *finite* map of curves, or a non-constant map. The *degree* of φ is defined to be the degree of the extension of $K(C_1)$ over $\varphi^*(K(C_2))$. This shall be denoted by $\deg(\varphi)$.

Definition 2.6. Let $\varphi : C_1 \to C_2$ be a non-constant map of curves. Then the *ramification index* of φ at a closed point $P \in C_1$, is the largest integer n such that $\varphi^*(m_{\varphi(P)}) \subset m_P^n$. This number shall be denoted by $e_\varphi(P)$. The point $P \in C_1$ is called *ramified* or *unramified* in the case when $e_\varphi(P)$ is 1 or bigger than 1 respectively. The map φ is said to be *unramified* if it is unramified at every closed point $P \in C_1$.

Now we shall state a celebrated theorem that shall prove to be instrumental in our case.

Theorem 2.7. *(Riemann-Hurwitz) Let $\varphi : C_1 \to C_2$ be non-constant separable map of non-singular curves over K. Suppose g_1 and g_2 are the genera of the curves C_1 and C_2 respectively.*

(1) If $char(K) = 0$ or $char(K)$ is prime to e_P for all $P \in C_1$, then

$$2g_1 - 2 = \deg(\varphi)(2g_2 - 2) + \sum_{P \in C_1} (e_\varphi(P) - 1)$$

(2) More generally

$$2g_1 - 2 \geq \deg(\varphi)(2g_2 - 2) + \sum_{P \in C_1} (e_\varphi(P) - 1)$$

For proof check Hartshorne[3, IV.2.4].

3. Elliptic Curves

First we need to define the objects called Elliptic curves. Like the previous section we assume that the base field K is algebraically closed.

Given a scheme S over K, a K-point of the scheme is a map $\operatorname{Spec} K \to S$, such that composition with the structure map $S \to \operatorname{Spec} K$ is the identity map of $\operatorname{Spec} K$. This is called a *geometric point* of the scheme. The set of all geometric points of the scheme shall be denoted by $S(K)$. Note that for varieties there is a one-to-one correspondence between the K-points and the closed points.

Definition 3.1. Given a pair (E, O) of a smooth curve E over a field K and a prescribed base point $O \in E(K)$, we say it is an *Elliptic curve* over K if E has genus $g = 1$. To denote the curve we shall write E/K, that is the curve is defined over K.

Note that here we assume O to be a closed point of the curve E. This point shall be identified with the identity of the group of K-points of the curve.

There is another definition that some of the readers might be familiar with, which calls an Elliptic Curve to be the curve of zero locus of the equation $y^2 = x^3 + Ax + B$ in the plane. The equivalence of our definition with the above follows from Proposition 3.2 which shall be assumed as a fact in this article to simplify the proofs. Wherever necessary we might also assume $\operatorname{char}(K)$ to be prime to 2 and 3 for simplification, although the results shall still remain true otherwise.

Proposition 3.2. *Let (E, O) be an Elliptic curve defined over K. Then there exist functions $x, y \in K(E)$ such that the map*

$$\varphi : E \to \mathbb{P}^2_K$$
$$\varphi = [x : y : 1]$$

gives an isomorphism of E/K onto a curve given by a Weierstrass equation

$$C : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{3.3}$$

with coefficients $a_1, \ldots, a_6 \in K$; and such that $\varphi(O) = [0 : 1 : 0]$.

For the proof check Silverman[4, III.3.1]. The image of the curve in $\mathbb{P}^2_K$ is in fact a non-singular curve, and the equation so obtained is a non-singular Weierstrass Equation. To simplify our computations we fix the point $[0 : 1 : 0]$, called the point at infinity on the curve, to be our chosen base point of the image of E.

It is a fact that we could introduce a group structure on the K-points of the Elliptic curve with the chosen base geometric point as the identity of the group. There are "translation" maps which could be used to change the identity point. The introduced group law is, in fact, of an abelian group. From this point on we shall view the Elliptic curve with its additional group structure. Now let us consider a map between two Elliptic curves. It is natural to ask if and when it preserves the group structure. As it turns out the answer is very simple. If the base point of one

curve is sent to the base point of the other one, then the map is, in fact, a group homomorphism as well. These shall be termed as isogenies.

Definition 3.4. Let (E_1, O_1) and (E_2, O_2) be two Elliptic curves. A morphism $\varphi : E_1 \to E_2$ is said to be an *isogeny* if $\varphi(O_1) = O_2$.

Proposition 3.5. *Let $\varphi : E_1 \to E_2$ be an isogeny between two Elliptic curves over K. Then it is a homomorphism of the underlying abelian groups.*

For the proof check Silverman[4, III.4.8]. Now given any abelian group there are multiplication by n maps, which reveal a lot of the structure of the group. The same is true in the case of Elliptic curves.

Definition 3.6. By $[m] : E \to E$ we shall denote the multiplication by m map, that is $[m] : P \mapsto mP$.

Proposition 3.7. *The multiplication by m map of any Elliptic curve over K, is a non-constant isogeny.*

For the proof check Silverman[4, III.3.6] and Silverman[4, III.4.2].

Proposition 3.8. *Let $\varphi : E_1 \to E_2$ be a non-constant isogeny of degree m. Then there exists an isogeny $\hat{\varphi} : E_2 \to E_1$ such that $\hat{\varphi} \circ \varphi = [m]$ as a map $E_1 \to E_1$ and $\varphi \circ \hat{\varphi} = [m]$ as a map $E_2 \to E_2$.*

For the proof check Silverman[4, III.6.1]. In the above case $\hat{\varphi}$ is said to be the *dual isogeny* of φ.

Definition 3.9. Let E be an Elliptic curve given by equation (3.3). The *Frobenius twist* of E, denoted $E^{(p)}$ is the elliptic curve whose Weierstrass coefficients are given by a_i^p. Alternatively, $E^{(p)}$ is defined by the following fiber diagram

$$\begin{array}{ccc} E^{(p)} & \longrightarrow & E \\ \downarrow & & \downarrow \\ \operatorname{Spec} K & \xrightarrow{x \mapsto x^p} & \operatorname{Spec} K \end{array}$$

Note that the map $E \to E^{(p)}$ is not a map of K-schemes (i.e., it is nontrivial on the coefficients). The r-th iterated Frobenius twist will be denoted $E^{(p^r)}$.

The *Frobenius morphism* is the map (of K-schemes) $Fr \colon E \to E^{(p)}$ given by $[x : y : z] \mapsto [x^p : y^p : z^p]$. Composition gives a map $Fr^r \colon E \to E^{(p^r)}$.

Remark 3.10. It is easy to see that the Frobenius morphism is non-constant. It can be shown that the morphism is purely inseparable. Also since the identity $[0 : 1 : 0]$ is mapped to itself, it is an isogeny of Elliptic curves.

The Elliptic curves over fields of characteristic $p > 0$ can be classified according to the behavior of the dual of the Frobenius morphism.

(1) If the dual $\hat{Fr} : E^{(p)} \to E$ is purely inseparable then $\ker([p] : E(K) \to E(K)) = 0$. In this case the Elliptic curve is said to be *supersingular*. Supersingular Elliptic curves have no p-torsion geometric points.
(2) If the dual $\hat{Fr} : E^{(p)} \to E$ is separable then $\ker([p] : E(K) \to E(K)) = \mathbb{Z}/p\mathbb{Z}$. In this case the Elliptic curve is said to be *ordinary*. Notice that there is a unique subgroup of $E(K)$ of order p^r for every $r \geq 1$, and $\ker[p^r]$ is this subgroup. It must also be noted that the dual of the Frobenius commutes with multiplication by n maps, that is if $p \nmid n$ then $\hat{Fr} \circ [n] = [n] \circ \hat{Fr}$.

4. Étale Maps

By a scheme in this section we shall mean a scheme of finite type over a field, unless otherwise mentioned.

Definition 4.1. A non-constant map of non-singular curves $\varphi : C_1 \to C_2$ is said to be unramified at a closed point $P \in C_1$, if we have $\varphi^* m_{\varphi(P)} = m_P$ and $\mathcal{O}_P/m_P$ is a finite separable extension of $\mathcal{O}_{\varphi(P)}/m_{\varphi(P)}$. The above map is said to be unramified if the map is unramified at all closed points $P \in C_1$.

Remark 4.2. For curves it is enough to check that $\#\varphi^{-1}(Q) = \deg \varphi$ for every closed point $Q \in C_2$, for the map to be unramified. For Elliptic curves C_1 and C_2 and an isogeny φ, these fibers $\varphi^{-1}(Q)$ have the cardinality when Q varies over closed points of C_2. Therefore, in this case φ is unramified if and only if $\deg \varphi = \# \ker \varphi$

Remark 4.3. Let $\varphi : C_1 \to C_2$ be an unramified map. Then $K(C_1)$ is a finite separable extension of $\varphi^*(K(C_2))$, that is the map is separable.

We shall try to motivate the above definition. Suppose that a branched covering of real manifolds $\varphi : X \to Y$ is given. Intuitively we may think of X as a collection sheets homeomorphic to Y pasted together at the ramified points. Following that idea, we see that around a ramified point $P \in X$ the map branches into multiple sheets. Thus a point $p \in X$ is unramified if and only if the pull-backs of coordinate functions at $f(P) \in Y$ gives us coordinate functions at P. If we look at the definition above, we notice the similarity with this intuition.

Definition 4.4. Let $\varphi : X \to Y$ be a morphism of schemes. Then φ is said to be étale if it is flat and unramified.

For a discussion on flat and étale maps see Milne[5, I].

Remark 4.5. A non-constant map of non-singular curves $\varphi : C_1 \to C_2$ is automatically flat. Therefore for curves the terms étale and unramified are interchangeable. If the reader wishes so, it is possible to replace all the statements below containing the adjective étale with unramified, provided the map is between nonsingular curves.

Let us try to indicate as to why étale maps capture the notion of local homeomorphisms. First of all, the étale maps being flat forces the fibers to be of the same dimension. Moreover, these maps being unramified forces the fibers to be of dimension 0. Proposition 4.10 shall show that the fibers are in fact disjoint union of spectrum of residue fields, which means that the fibers are, in particular, discrete. This and the fact that étale maps are unramified, motivates us to think of étale maps as local homeomorphisms.

Proposition 4.6. *Let $\varphi : X \to Y$ and $\psi : Y \to Z$ be morphisms of schemes along with their composition $\psi \circ \varphi : X \to Z$.*
(1) If φ and ψ are étale, then so is $\psi \circ \varphi$.
(2) If ψ and $\psi \circ \varphi$ are étale, then so is φ.
Let $\varphi : X \to Y$ be an étale morphism of schemes over a scheme S. Then the base changed map $f_{S'} : X \times S' \to Y \times S'$ is an étale morphism, for any base change $S' \to S$.

For the proof check Murre[6, 3.3.3].

Remark 4.7. The point (1) enables us to create a category with objects being schemes and morphisms being étale maps between them. The point (2) enables us to fix a base scheme and build a category with objects beings schemes with morphisms to the base scheme. These two properties will enable us to produce a nice étale site which we shall define in the next section. The last part of the proposition is sort of a lemma, which shall make our lives easier as we need to change bases to simplify our proofs.

We have only defined what it means for a map to be finite when the domain and target are curves. We define it in a general setting now.

Definitions 4.8. Let $\varphi : X \to Y$ be a morphism of schemes over a base field K. Then φ is called affine if for every open affine subscheme $\operatorname{Spec}(A) = U \subset Y$ the pre-image $f^{-1}(U) \subset X$ is an affine open subscheme, $f^{-1}(U) = \operatorname{Spec} B$. The above map φ is said to be a finite map if it is affine and for every open affine sub-scheme $\operatorname{Spec}(A) = U \subset Y$ and its pre-image $\operatorname{Spec}(B) = f^{-1}(U) \subset Y$, the corresponding map $A \to B$ makes B into a finitely generated A-module.

An important class of finite maps for us shall be the non-constant maps of curves.

Remark 4.9. The degree of a finite map is defined to be the degree of the corresponding extension of the function fields. It can be shown that finite maps are closed. On the other hand étale maps are open. Thus finite étale maps are surjective morphisms onto connected schemes.

We already know that étale maps are analogs of local homeomorphisms. Finite maps are proper. Thus finite étale maps can be thought of as proper local homeomorphisms, which are finite surjective coverings. To get a better feel of them we shall look at an example.

Proposition 4.10. *Let k be a field. The following are equivalent:*

1. *X is finite étale over $\operatorname{Spec} k$, and*
2. *X is a disjoint union $\sqcup \operatorname{Spec}(K)$, where each K is a finite separable extension of k.*

Proof. (1) $\implies$ (2) Let us first assume that X is connected. Since X is finite over k, by the affiness we get that $X = \operatorname{Spec} A$ is an affine scheme. Also by finiteness we get that A has finite dimension as a vector space over k. If A is not a field, then it has a non-zero prime ideal $\mathfrak{P}$. After localizing we get a ring $A_{\mathfrak{P}}$ whose maximal ideal satisfies $m_{\mathfrak{P}} = 0$. This is true since the maximal ideal of k shall generate the maximal ideal of $A_{\mathfrak{P}}$, by the unramifiedness of the algebra A. This is a contradiction to our assumption and hence $A = K$ is a field. Also the unramifiedness enforces K to be finite separable over k. Thus each connected component is a field, and by the finiteness there are finite many connected components.

(2) $\implies$ (1) Each connected component is finite étale over k. Thus the result follows. □

The above gives us a reasonable description of the fibers of finite étale maps. We know by Proposition 4.6 that finiteness and being étale is preserved under base change. Thus given a finite étale map $\varphi : X \to Y$ we can take the fiber $\varphi_s : X_s \to \operatorname{Spec} k$, where $s : \operatorname{Spec} k \to Y$ is a point and $X_s = X \times_Y \operatorname{Spec} k$ is the fiber over that point. The produced map f_s is finite étale over a field k, and thus Proposition 4.10 forces X_s to be discrete.

Lemma 4.11. *Let $\varphi : X \to C$ be a finite étale map of schemes. If C is a non-singular curve, and X is connected then X is a non-singular curve.*

Proof. We need to check that X is a complete non-singular variety over K of dimension 1. A variety is a reduced, irreducible, separated scheme of finite type over K. Finiteness shall imply shall it is complete, separated, finite-type of dimension 1. The former condition along with unramifiedness shall imply the rest. Let us sketch the proof below.

Consider an induced map of local rings $\mathcal{O}_{P,C} \to \mathcal{O}_{Q,X}$. The local ring $\mathcal{O}_{P,C}$ is a discrete valuation ring, being a local ring of a non-singular curve, and $\mathcal{O}_{Q,X}$ is a flat unramified extension. This shall imply that $\mathcal{O}_{Q,X}$ is a discrete valuation ring, in particular an integral domain. Since being reduced is a local property, X is reduced. We now need to show that X is irreducible. Now X, being Noetherian, has finitely many irreducible components; $X = C_1 \cup \cdots \cup C_n$ be the irreducible decomposition. Since X is connected, two of them shall intersect, say C_1 and C_2. Take some closed point $Q \in C_1 \cap C_2$. We may show that the local ring at Q is not an integral domain (by passing into some affine neighborhood), contradicting the statement made above about local rings. Thus X is irreducible, and also reduced; hence integral. Moreover, non-singularity of X follows from the fact that the local rings $\mathcal{O}_{Q,X}$ are discrete valuation rings, for every closed point $Q \in X$. This also forces X to be of dimension 1, and we are done. □

Lemma 4.12. *Assume that C is $\mathbb{P}^1_K$. Let $\varphi : X \to C$ be a finite étale map. Then φ is an isomorphism.*

Proof. Firstly by Lemma 4.11 the scheme X is a non-singular curve. We may apply the equality case of Riemann Hurwitz formula (Theorem 2.7). Let g be the genus of X and d be the degree of the map φ. Then $2g - 2 = -2d$ which implies $g = 0$ and $d = 1$. Thus X is a smooth curve of genus 0, the map φ is of degree 1 between non-singular curves. Thus the result follows. □

This just confirms our intuition derived from the study of Riemann Surfaces. We know that there are no unbranched covers of the Riemann Sphere, because it is simply connected. The above shows that the same is true over other algebraically closed fields.

Proposition 4.13. *Let $\varphi : X \to E$ be a finite étale map of schemes over K. If E is an Elliptic curve, and X is connected then X is an Elliptic curve.*

Proof. Following the same line of reasoning as the proof of Lemma 4.12 we get that X is a non-singular curve. After that we may similarly apply the equality case of Riemann Hurwitz formula (Theorem 2.7). Let g be the genus of X and d be the degree of the map φ. Then $2g - 2 = d \cdot 0$ which implies $g = 1$. Thus X is a smooth curve of genus 1, and if a suitable base point is chosen it becomes an Elliptic curve. □

The above shall let us restrict our attention to maps between Elliptic curves.

Proposition 4.14. *Let $[n] : E \to E$ be the multiplication by n map of Elliptic curves over a field K. If $\operatorname{char}(K)$ is 0 or relatively prime to n then the map is a finite étale map. However if $\operatorname{char}(K) \mid n$ then the map is ramified.*

Proof. If $\text{char}(K) = 0$ or relatively prime to n, we know that $\ker([n] : E(K) \to E(K))$ equals $(\mathbb{Z}/n\mathbb{Z})^2$. Thus, the fiber over O has size n^2, implying that $[n]$ is unramified (Remark 4.2).

Conversely, if $\text{char}(K) \mid n$ then $\ker([n] : E(K) \to E(K))$ is strictly contained in $(\mathbb{Z}/n\mathbb{Z})^2$. On the other hand $\deg[n] = n^2$, thus it is unramified precisely when $\text{char}(K) = 0$ or is prime to n. Additionally, $[n]$ is non-constant map of curves and hence finite. □

Proposition 4.15. *Suppose* $\text{char}(K) = p > 0$*, and let* E *be a supersingular Elliptic curve defined over* K*. Then any map* $\varphi : F \to E$ *of Elliptic curves of degree* n $(p \mid n)$*, is ramified.*

Proof. Suppose that $n = qm$ where $q = p^r$ is a power of p and m is coprime to p. Let $\hat{\varphi} : E \to F$ be the dual of φ. Then we know that $\varphi \circ \hat{\varphi} = [n] = [q] \circ [m]$. Now $[q] = Fr^r \circ \hat{Fr}^r$, and since E is supersingular both maps are ramified. In particular $\ker[q] = 0$, and thus the size of $\ker \varphi$ does not have any factor of p. Thus the size of $\ker \varphi$ cannot equal n and φ is ramified by Remark 4.2. □

Proposition 4.16. *Suppose* $\text{char}(K) = p > 0$*, and let* E *be an ordinary Elliptic curve defined on* K*. Then any separable map* $\varphi : F \to E$ *of Elliptic curves of degree* $p^r m$ $(p \nmid m)$*, can be written as* $\varphi = \phi \circ \hat{Fr}^r$ *for some separable isogeny* $\phi \colon F \to E^{(p^r)}$ *of degree* m*.*

Proof. Since φ is separable and $\varphi \circ \hat{\varphi} = [p^r m]$, $\hat{\varphi}$ has inseparable degree p^r. By Silverman II.2.12, we can write $\hat{\varphi} = Fr^r \circ \hat{\phi}$ for some isogeny $\hat{\phi}$ of degree m. In particular, $\varphi = \phi \circ \hat{Fr}^r$, with ϕ of degree m. □

5. Étale Fundamental Group

Like in the previous section a scheme is always finite type over an algebraically closed field. We would build the Galois category of the étale covers of a scheme, and will try to motivate the construction via examples. The proofs in the general setting can be found in Murre[6]. Milne[5, I.5] has a concise introduction to the concept. We shall assume the reader to be reasonably familiar with the idea of fundamental group and universal cover, although their knowledge is not necessary. Here we leave the realm of algebraic topology and forget the definition of fundamental group using the closed loops. Instead, the relevant result to us from algebraic topology is that the fundamental group is isomorphic to the group of deck transformation of the universal cover. The fundamental group has a natural action on the fiber over the base point and the action is termed as the monodromy action. The monodromy action is transitive. All these properties can be algebraically simulated, although not directly. The universal covering of the space does not necessarily exist in our category, however, there is an inverse system whose limit is the object of our interest.

The above paragraph summarizes the salient features. Let $f : X \to Y$ be a covering map of pointed topological spaces, with both the spaces path-connected. Then again the fundamental group $\pi_1(Y)$ has an action on the fiber over the base point, however it might not be free or transitive. We have the group the of deck transformations of the cover, called the automorphism group of the cover X over Y. This group $\text{Aut}_Y(X)$ acts freely on the fiber. When the action is transitive it is said to be a normal or regular. In our case we shall restrict our attention to finite covers. In some sense the finite regular covers could be used to approximate the

fundamental group. For a complete discussion of fundamental groups we encourage the readers to check Hatcher[1, 1.3].

Definition 5.1. By an étale covering of a scheme S, we mean a finite étale morphisms of schemes $\varphi : X \to S$.

Finite étale maps are surjective and this the "covering" terminology is justified.

Let us first construct the *Galois category* over S, which is the finite étale site.

Definition 5.2. Given any category $\mathscr{C}$, by $\mathrm{Obj}(\mathscr{C})$ we mean the class of objects of the category. Given two objects $X, Y \in \mathrm{Obj}(\mathscr{C})$, by $\mathrm{Hom}_{\mathscr{C}}(X, Y)$ we mean the set of morphisms from X to Y. When the category is clearly understood the subscript is dropped and $\mathrm{Hom}(X, Y)$ denotes the set of morphisms from X to Y. Also in most cases $X \in \mathscr{C}$ is denotes that X is an object in $\mathscr{C}$.

Let $Sets$ denote the category of sets. Let us fix a field K, and a separable closure Ω of K. From this point on, all schemes shall be over this field K.

Definition 5.3. Given a scheme S over the field K, by a *geometric point* $\bar{s}_0$ of the scheme we mean a morphism $\bar{s}_0 : \operatorname{Spec} \Omega \to S$.

Note that for a curve over an algebraically closed field, the geometric points are in one to one correspondence with the closed points.

Definition 5.4. Consider the base scheme S with a fixed base geometric point $\bar{s}_0 \in S$. We construct a category called the *finite étale site* over S, which is denoted as FEt/S.

(1) The objects of this category are the schemes $\varphi : X \to S$ over S, with φ being finite and étale.
(2) Morphisms in this category are maps that commute with the maps to S, that is for $X, Y \in \mathrm{FEt/S}$ the morphisms from X to Y are the morphisms of schemes that makes the diagram commutative:

(5.5)
$$\begin{array}{ccc} X & \longrightarrow & Y \\ & \searrow & \downarrow \\ & & S \end{array}$$

Remark 5.6. Consider $X, Y \in \mathrm{FEt/S}$ as above. Any morphism $\varphi : X \to Y$ that commutes the diagram (5.5) above is, in fact, finite and étale. This is implied by Proposition 4.6 point (2).

The above is called the Finite Étale site over S, or the Grothendieck Category of étale coverings of S. Some remarks are in order.

Remark 5.7. There exists a functor $F : \mathrm{FEt/S} \to Sets$ called the fundamental functor. It is defined as $F(X) \coloneqq \{\varphi : \operatorname{Spec} \Omega \to X_s\}$, that is for each X, $F(X)$ is the set of all $\varphi : \operatorname{Spec} \Omega \to X_s$ maps that commute the diagram below:

$$\begin{array}{ccc} \operatorname{Spec} \Omega & \xrightarrow{\varphi} & X \\ & \searrow^{\bar{s}_0} & \downarrow \\ & & S \end{array}$$

This functor could also be thought of as taking values in the fiber over the base geometric point of S. Notice that this is a covariant functor from FEt/S to the

category of sets. There is a (right) action of $\mathrm{Aut}(X)$ on $F(X)$, given by $x \cdot g = g \circ x$, for $g \in \mathrm{Aut}(X)$ and $x \in F(X)$. If we take a connected scheme X, then the action is, in fact, *free*. If for some connected object X the action is transitive, then the object X is said to be *regular* or *Galois* over S. A covariant functor F from the category $\mathscr{C}$ to *Sets* is said to be representable if there exists an object X such that $F(Z) = \mathrm{Hom}(X, Z)$ for all $Z \in \mathscr{C}$ in the category. The fundamental functor is "represented" by the universal cover, provided it exists. In any case this functor is "prorepresented" by the system of *Galois covers* in this category. In other words consider the collection of Galois covers $X \in \mathrm{FEt/S}$ ordered by the relation $X \leq Y$ if the map $X \to S$ is "dominated" by the map $Y \to S$, that is, there exists a map $\varphi : X \to Y$ such that the diagram (5.5) commutes with the top map being φ. Let the collection of connected covers be indexed by I, and the collection be $\{X_\alpha\}_{\alpha \in I}$. Then for any $Z \in \mathrm{FEt/S}$, we have that $F(Z) = \varprojlim_{\alpha} \mathrm{Hom}(X_\alpha, Z)$, and hence the functor is *prorepresented*.

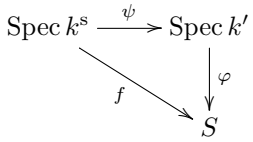
Definition 5.8. We shall assume the notation of the above discussion (remark 5.7). The *étale fundamental group* is defined as the limit $\pi_1^{\text{ét}}(S) \coloneqq \varprojlim_{\alpha \in I} \mathrm{Aut}(X_\alpha)$, where $\{X_\alpha\}_{\alpha \in I}$ is the collection of Galois covers of S.

Remarks 5.9.
(i) It can be proved that for a finite étale cover, the set $\mathrm{Aut}(X)$ is finite. This group could be given the discrete topology. Then the fundamental group $\pi_1^{\text{ét}}(S, \bar{s}_0)$ inherits the limit topology. For each object $X \in \mathrm{FEt/S}$, there is an (right) action of $\pi_1^{\text{ét}}(S, \bar{s}_0)$ on the finite set $F(X)$. Thus if $F(X)$ is given the discrete topology, this action can be viewed as continuous. A subcollection $\{Y_\beta\}_{\beta \in J}$ indexed by $J \subset I$ is said to be *cofinal* if any X_α is dominated by some Y_β with $\alpha \in I$ and $\beta \in J$. It can be shown that limits are preserved if a cofinal collection is taken. Thus the fundamental functor shall be prorepresented as well as the fundamental group could be computed by taking the cofinal subcollection. Our goal in this article is to produce a cofinal collection of Galois covers over the base Elliptic curve.
(ii) We also need to remark about the choice of the base geometric point $\bar{s}_0$. It is indeed true that the fundamental group so obtained is independent of the choice of the base geometric point, provided that the base scheme is connected. To prove that we need to follow the following steps. We can show that the category FEt/S is equivalent to the category of finite $\pi_1^{\text{ét}}(S, \bar{s}_0)$-sets, which is the category of finite sets with continuous $\pi_1^{\text{ét}}(S, \bar{s}_0)$ action and the morphisms commuting with the group action. The functor from FEt/S to $\pi_1^{\text{ét}}(S, \bar{s}_0)$-sets could be taken as F, which maps X to a finite set $F(X)$ with $\pi_1^{\text{ét}}(S, \bar{s}_0)$ action on it. The equivalence of the two categories shall enforce the uniqueness of the fundamental group of the category, upto isomorphism of groups. Hence chosen any base geometric point, the fundamental group obtained is isomorphic, provided that the base scheme is connected.

Before we move onto Elliptic curves we compute the fundamental group of a field and the projective line.

Examples 5.10. (i) Let k be a field, and $S = \operatorname{Spec} k$. By Proposition 4.10 we know that $X \to S$ is étale if and only if $X = \sqcup \operatorname{Spec} K$ where each K is a finite separable extension of k. Thus any connected covering is just $\operatorname{Spec} k'$, where

k' is a finite separable extension of k. Let k^s be a separable closure of k, and $f : \operatorname{Spec} k^s \to \operatorname{Spec} k$ be a covering. Then for any map $\varphi : \operatorname{Spec} k' \to S$ there is a map $\psi : \operatorname{Spec} k^s \to \operatorname{Spec} k'$ such that the following diagram commutes.



If $\operatorname{Spec} k^s$ exists in the category, it is the universal cover of the space. In that case, this object represents the fundamental functor and the group of automorphisms of this cover is the étale fundamental group. Unfortunately, sometimes it does not exist in the category, for example when $k = \mathbb{Q}$. However, as we know, the separable closure can be obtained by taking the union of all finite separable extensions of the field k. Speaking in more categorical terms, the collection of finite separable extensions form a direct system whose limit is the separable closure. Thus the spectrum of these finite separable extensions form an inverse system whose limit is the spectrum of the separable closure. The Galois covers in this case is the collection of finite Galois extensions of the field k. We can take the automorphism group of each cover $\varphi : \operatorname{Spec} k' \to \operatorname{Spec} k$, where k' is a finite Galois extension of k. The automorphism group can be checked to equal $\operatorname{Aut}(\operatorname{Spec} k', \varphi)$ is $\operatorname{Gal}(k'/k)$. Notice that in this case the fundamental functor $F(\operatorname{Spec} k')$ equals the set of embeddings of k' in Ω fixing k. Also the limit $\varprojlim \operatorname{Gal}(k'/k)$ equals $\operatorname{Gal}(k^s/k)$, where the limit has been taken over finite Galois extensions of k. This means that the étale fundamental group of $\operatorname{Spec} k$ is the absolute Galois group of k.

(ii) Consider any cover $\varphi : C \to \mathbb{P}^1$. Then by Lemma 4.12 we know that φ is an isomorphism. Thus $\operatorname{Aut}_{\mathbb{P}^1}(C)$ is the trivial group, and hence the fundamental group $\pi_1^{\text{ét}}(\mathbb{P}^1)$ is trivial.

Given an Elliptic curve E over K, we will show there exists a simple cofinal inverse system of Galois covers of the curve. This shall enable us to compute the fundamental group easily. First we show that unramified isogenies of Elliptic curves indeed Galois.

Lemma 5.11. *Let E, F be Elliptic curves over K. Suppose $\varphi : F \to E$ is a finite étale cover. Then (F, φ) is a Galois cover.*

Proof. Suppose $P \in \ker \varphi$. Consider the translation by P morphism $\tau_P : F \to F$ which takes $Q \mapsto Q + P$. This is not an isogeny as the identity O is taken to P; nonetheless it is a map of curves. We have $\varphi \circ \tau_P = \varphi$ by the definition, which implies that $\tau_P \in \operatorname{Aut}(F, \varphi)$. Notice that $\tau_Q \circ \tau_P = \tau_{P+Q}$ and thus choosing the map $\ker \varphi \to \operatorname{Aut}(F, \varphi)$ given by $P \mapsto \tau_P$ is an injective group homomorphism. Thus it identifies $\ker \varphi$ with a subgroup of $\operatorname{Aut}(F, \varphi)$. On the other hand by Proposition 3.5 we know that any map between Elliptic curves is a composition of a translation and an isogeny. Any isogeny from (F, φ) to itself fixes the identity, and thus is an isomorphism of covers. Therefore $\operatorname{Aut}(F, \varphi) \cong \ker \varphi$. It is also clear from the above discussion that $\operatorname{Aut}(F, \varphi)$ acts transitively on the fibers, that is $\ker \varphi$. Connectedness of the cover is clear as F is curve, and thus (F, φ) is a Galois cover of E. □

Now we shall compute the fundamental group of the Elliptic curve over a characteristic zero field.

Proposition 5.12. *Let K be an algebraically closed field of characteristic 0, and suppose E is an Elliptic curve over K. Then the étale fundamental group $\pi_1^{\text{ét}}(E, \bar{s}_0)$ equals $\hat{\mathbb{Z}}^2$, chosen any base geometric point $\bar{s}_0$.*

Proof. Consider the étale covers $[n] : E \to E$, for each n. The fact that they are Galois follows from Lemma 5.11. Given the fact that $[n] \circ [m] = [nm]$, it implies that they form an inverse system with the indexing set $\mathbb{Z}_{>0}$ with order $n \leq m$ if $n \mid m$. Proposition 3.8 could be used to prove that this system is indeed cofinal. Given an étale covering $\varphi : F \to E$, there is a dual isogeny $\hat{\varphi} : E \to F$ such that $\hat{\varphi} \circ \varphi = [\deg \varphi]$ as a map $E \to E$. We know that $[\deg \varphi]$ is an étale covering from Proposition 4.14. Thus the étale coveing $[\deg \varphi] : E \to E$ dominates the map $\varphi : F \to E$, and this is true for any φ. Also we know that $\text{Aut}(E, [n]) = (\mathbb{Z}/n\mathbb{Z})^2$ from the proof of Lemma 5.11. Additionally, $\varprojlim_n (\mathbb{Z}/n\mathbb{Z})^2 = \hat{\mathbb{Z}}^2$. Thus the result follows. □

Let $\mathbb{Z} \setminus p\mathbb{Z}$ denote the set of integers coprime to p. The following two propositions compute the fundamental group of the Elliptic curves over fields of positive characteristic.

Proposition 5.13. *Let K be an algebraically closed field of characteristic p, and suppose E is a supersingular Elliptic curve over K. Then the étale fundamental group $\pi_1^{\text{ét}}(E, \bar{s}_0)$ equals $\prod_{q \neq p} (\mathbb{Z}_q)^2$, chosen any base geometric point $\bar{s}_0$.*

Proof. Consider the directed set $\mathbb{Z} \setminus p\mathbb{Z}$, with the ordering $n \leq m$ if $n \mid m$. For each $n \in \mathbb{Z} \setminus p\mathbb{Z}$ take the cover $[n] : E \to E$. These covers form an inverse system of Galois étale covers. Any map whose degree is divisible by p is ramified , from Proposition 4.15. Proposition 3.8 shows that the above forms a cofinal collection. We know that $\text{Aut}(E, [n]) = (\mathbb{Z}/n\mathbb{Z})^2$ from the proof of Lemma 5.11. In this case the limit is $\varprojlim_{n \in \mathbb{Z} \setminus p\mathbb{Z}} \text{Aut}(E, [n]) = \prod_{q \neq p} \mathbb{Z}_q$. Thus the result follows. □

Proposition 5.14. *Let K be an algebraically closed field of characteristic p, and suppose E is an ordinary Elliptic curve over K. Then the étale fundamental group $\pi_1^{\text{ét}}(E, \bar{s}_0)$ equals $\prod_{q \neq p} (\mathbb{Z}_q)^2 \times \mathbb{Z}_p$, chosen any base geometric point $\bar{s}_0$.*

Proof. We know by Proposition 4.16 that any separable map $\varphi : F \to E$ factors as $\varphi = \phi \circ \hat{Fr}^r$ where ϕ has degree coprime to p. Thus given any connected étale cover $\varphi : F \to E$, we may take $\hat{\phi} : E^{(p^r)} \to F$ and produce a map $\hat{\phi} \circ \phi \circ \hat{Fr}^r = [\deg \phi] \circ \hat{Fr}^r$. Consider the directed set $I = (\mathbb{Z} \setminus p\mathbb{Z}) \times \mathbb{Z}_{\geq 0}$ with the ordering $(n, i) \leq (m, j)$ if $n \mid m$ and $i \leq j$. For each (n, i) with $i > 0$ take the cover $[n] \circ \hat{Fr}^i : E^{(p^r)} \to E$, and for each $(n, 0)$ take the cover $[n] : E \to E$. Using the fact that the dual of the Frobenius commutes with $[n]$, we get that they form an inverse system. We know that $\text{Aut}(E, [n] \circ \hat{Fr}^i) = (\mathbb{Z}/n\mathbb{Z})^2 \times \mathbb{Z}/p^i\mathbb{Z}$ from the proof of Lemma 5.11. Additionally, the limit is $\varprojlim_{(n,i) \in I} (\mathbb{Z}/n\mathbb{Z})^2 \times \mathbb{Z}/p^i\mathbb{Z} = \prod_{q \neq p} (\mathbb{Z}_q)^2 \times \mathbb{Z}_p$. Thus the result follows. □

Acknowledgments. I would like to thank my mentor Drew Moore for guiding me throughout this project, without whose constant support and encouragement this would have been impossible. I express my gratitude to Prof. Peter May for making it possible for me to be a part of this memorable experience. I also thank my friends for their warmth and hospitality.

References

[1] A. Hatcher. Algebriac Topology. https://www.math.cornell.edu/ hatcher/AT/ATpage.html
[2] J. P. May. A Concise Course in Algebraic Topology. University of Chicago Press. 1999.
[3] R. Hartshorne. Algebraic Geometry. Springer. 1977.
[4] J. H. Silverman. Arithmetic of Elliptic Curves. Springer. 2009.
[5] J. Milne. Étale Cohomology. Princeton Mathematical Series, Volume 33.
[6] J. P. Murre. Lectures on An Introduction to Grothendiecks Theory of the Fundamental Group. http://www.math.tifr.res.in/ publ/ln/tifr40.pdf