Fundamental group of a curve

Shishir Agrawal

Contents

1 Introduction

It is a foundational result of topology that the topological fundamental group of a reasonable topological space classifies its covering spaces. This result has an algebraic analogue: for any connected scheme X, there exists a profinite group $\pi(X)$ such that the category $\mathcal{F}\acute{\mathcal{E}}\mathrm{t}_X$ of finite étale coverings of X is equivalent to the category $\mathcal{FS}\mathrm{et}_{\pi(X)}$ of finite sets on which $\pi(X)$ acts continuously. In fact, the profinite group $\pi(X)$ is unique up to isomorphism, and is called the (étale) fundamental group of X [4, theorem 1.11].[1]

We will prove the existence assertion of this theorem when X is a *curve*, by which we mean it satisfies any of the following equivalent conditions [1, proposition 9.2 and theorem 9.3].

(a) The scheme X is one-dimensional, locally noetherian, normal and integral.

(b) The scheme X is connected, locally noetherian, and every local ring $\mathcal{O}_{X,x}$ is either a field or a discrete valuation ring.

(c) The scheme X is connected and has a covering by affine open subschemes of the form $\operatorname{Spec} A$, where A is Dedekind.

(d) Every nonempty affine open subscheme of X is of the form $\operatorname{Spec} A$, where A is Dedekind.

[1] More precisely, the profinite group $\pi(X)$ depends on the choice of a geometric point of X. See [4] for details.

In this case, we will construct the fundamental group of X as the Galois group of a particular field extension M of the function field K of X. We describe this field extension M and construct an equivalence of categories $Q : \mathcal{F}\acute{\mathcal{E}}\mathrm{t}_X \to \mathcal{FS}\mathrm{et}_{\mathrm{Gal}(M/K)}$ in section 3. The preceding sections define necessary notions and establish basic properties. To conclude, we demonstrate the arithmetic and geometric significance of the fundamental group by calculating some examples.

Essentially all results contained herein can be generalized, albeit with varying degrees of difficulty [4]. Nonetheless, we confine ourselves to the special case of curves for the sake of both brevity and concreteness. But before we begin, we briefly review some of the generalities regarding finite étale morphisms that permit us to legitimately consider only curves for the remainder of our discussion.

1.1 Finite étale morphisms

Let B be a finite and projective A-algebra. The trace $\mathrm{Tr}_{B/A}(b)$ of an element $b \in B$ is defined to be the trace of the A-linear map given by multiplication by b. Then $\mathrm{Tr}_{B/A} : B \to A$ is A-linear, and we define

$$\Phi_{B/A} : B \longrightarrow \mathrm{Hom}_A(B, A)$$

by $\Phi_{B/A}(b)(x) = \mathrm{Tr}_{B/A}(bx)$. If $\Phi_{B/A}$ is an isomorphism, then B is *separable* [4, section 4.8].

Proposition 1.1. *Let A be a ring and let B and C be a A-algebras.*

(a) If B is a finite, projective and separable A-algebra, then $B \otimes_A C$ is a finite, projective and separable C-algebra.

(b) Suppose that C is faithfully flat. Then $B \otimes_A C$ is a finite, projective and separable C-algebra if and only if B is a finite, projective and separable A-algebra.

Proof sketch. If B is a finite projective A-algebra, it is evident that $B \otimes_A C$ is a finite projective C algebra. If, in addition, C is faithfully flat, then it is clear that $- \otimes_A C$ will also reflect finite projectivity of B. For separability, we use the fact that B is finitely presented to obtain a natural identification

$$\mathrm{Hom}_A(B, A) \otimes_A C \xrightarrow{\sim} \mathrm{Hom}_C(B \otimes_A C, A \otimes_A C) \xrightarrow{\sim} \mathrm{Hom}_C(B \otimes_A C, C)$$

which makes the diagram

$$\begin{array}{ccc} B \otimes_A C & \xrightarrow{\mathrm{id}_{B \otimes_A C}} & B \otimes_A C \\ \downarrow{\scriptstyle \Phi_B \otimes \mathrm{id}_C} & & \downarrow{\scriptstyle \Phi_{B \otimes_A C}} \\ \mathrm{Hom}_A(B, A) \otimes_A C & \xrightarrow[\sim]{} & \mathrm{Hom}_C(B \otimes_A C, C) \end{array}$$

commute. Thus $\Phi_B \otimes \mathrm{id}_C$ is an isomorphism if and only if $\Phi_{B \otimes_A C}$ is an isomorphism. Both assertions now follow quickly. See [4, proposition 4.14] for details. □

Theorem 1.2. *Let K be a field with algebraic closure $\bar{K}$ and let B be a finite K-algebra. Further, let $\bar{B}$ be the finite $\bar{K}$-algebra $B \otimes_K \bar{K}$. Then the following are equivalent.*

(a) B is a finite separable K-algebra.

(b) $\bar{B}$ is a finite separable $\bar{K}$-algebra.

(c) $\bar{B}$ is isomorphic to $\bar{K}^n$ for some $n \geqslant 0$.

(d) B is isomorphic to $\prod_{i=1}^t B_i$ as K-algebras, where each B_i is a finite separable extension of K.

Proof reference. See [4, theorem 2.7]. □

A morphism $f : Y \to X$ of schemes is *flat at* $y \in Y$ if the local map $\mathcal{O}_{X,f(y)} \to \mathcal{O}_{Y,y}$ is a flat homomorphism. Then f is *flat* if it is flat at all $y \in Y$ (see proposition 2.2 for a reformulation in the case of curves). A morphism $f : Y \to X$ of schemes is *unramified at* $y \in Y$ if $\mathfrak{m}_{f(y)}\mathcal{O}_{Y,y} = \mathfrak{m}_y$ and the residue field $k(y)$ is a finite separable extension of $k(x)$. It is *unramified* if it is locally of finite type and unramified at all $y \in Y$ (see section 2.2 for the case of curves).

Finally, $f : Y \to X$ is *étale* if it is flat and unramified, and *finite étale* if it is finitely presented[2] and étale [4, section 6]. When X is locally noetherian, this is equivalent to being finite and étale.

Proposition 1.3. *Let $f : Y \to X$ be a morphism of schemes. Then the following are equivalent.*

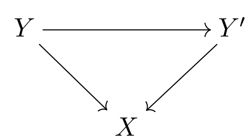
(a) *f is finite étale.*

(b) *There is an affine open cover* $\{\operatorname{Spec} A_i \subset X\}$ *such that* $f^{-1}(\operatorname{Spec} A_i) = \operatorname{Spec} B_i$ *for B_i a finite, free and separable A_i-algebra.*

(c) *For every affine open subscheme* $\operatorname{Spec} A \subset X$, $f^{-1}(\operatorname{Spec} A) = \operatorname{Spec} B$ *for a finite, projective and separable A-algebra B.*

Proof sketch. Using the fact that finitely presented and flat is the same as finitely generated and projective, which is the same as locally free of finite rank [4, theorem 4.6 and lemma 6.5], we reduce to proving the following statement. If A is a ring and B is a finite and free A-algebra, then B is seperable over A if and only if $\operatorname{Spec} B \to \operatorname{Spec} A$ is unramified. By base changing to fibers $k(\mathfrak{p})$ for prime ideals $\mathfrak{p} \subset A$, we further reduce to the case when A is a field. In this case, B is artinian so we may write $B = \prod_{i=1}^{t} B_i$, where B_i is the localization of B at a prime ideal $\mathfrak{q} \subset B$. Thus $\operatorname{Spec} B \to \operatorname{Spec} A$ is unramified if and only if B_i is a finite separable field extension of A. We now apply theorem 1.2. See [4, proposition 6.9] for details. □

A finite étale map $f : Y \to X$ is also called a *finite étale covering* of X. We denote by $\mathcal{F}\acute{\mathcal{E}}\mathrm{t}_X$ the category of finite étale coverings of X, with a morphism between coverings $Y \to X$ and $Y' \to X$ being a morphism $Y \to Y'$ forming a commuting triangle.



A priori, no restrictions are imposed on the morphism $Y \to Y'$, but it turns out that this morphism is also guaranteed to be finite étale [4, proposition 5.15]. We will prove this in the case of curves in proposition 2.6.

1.2 Finite étale coverings of curves

Suppose X is an integral scheme with function field K, and let L be a field extension of E. Then for every affine open subscheme $\operatorname{Spec} A \subset X$, A is a subring of L, and if B is the integral closure of A in L, then $\operatorname{Spec} A \mapsto B$ defines a $\mathcal{O}_X$-algebra $\mathcal{B}$ which is quasi-coherent because integral closure is stable under localization [1, proposition 5.12]. Thus, by setting $Y = \operatorname{Spec}_X \mathcal{B}$, we obtain an affine morphism $f : Y \to X$ called the *normalization* of X in L.

All finite étale coverings of a normal integral scheme arise as normalizations. To prove this, we will use the criterion of proposition 1.3, so we begin with the following characterization of finite, projective and separable algebras over an entire ring integrally closed in its field of fractions.

Lemma 1.4. *Let A be an entire ring integrally closed in its field of fractions K, and let B be a finite, projective and separable A-algebra. Then there are finite separable field extensions $L_1, \ldots, L_t$ of K such that*

[2] We follow [4] in the definition of a finitely presented morphism: the map $f : Y \to X$ is finitely presented if for every affine open subscheme $\operatorname{Spec} A \subset X$, we have $f^{-1}(\operatorname{Spec} A) = \operatorname{Spec} B$ for B a finitely presented A-module.

$B \otimes_A K$ is isomorphic to $\prod_{i=1}^t L_i$, and this isomorphism induces an isomorphism of B with $\prod_{i=1}^t B_i$, where B_i is the integral closure of A in L_i.

Proof. The isomorphism of $B \otimes_A K$ with $\prod_{i=1}^t L_i$ results from proposition 1.1 and theorem 1.2. Thus we regard $B \subset \prod_{i=1}^t L_i$, and it is clear that $B \subset \prod_{i=1}^t B_i$ since B is a finite A-algebra. Conversely, suppose $x \in \prod_{i=1}^t B_i$. Set $\mathrm{Tr} = \mathrm{Tr}_{B\otimes_A K/K}$, and observe that for any $y \in B$, we have $\mathrm{Tr}(xy)$ is given (up to sign) by the next-leading coefficient of the characteristic polynomial over K corresponding to multiplication by xy. It is well-known that the characteristic polynomial is a power of the minimal polynomial over K. Since $xy \in B$ is integral over A, which is integrally closed in K, its minimal polynomial over K must have coefficients in A. Thus $\mathrm{Tr}(xy) \in A$.

In other words, $y \mapsto \mathrm{Tr}(xy)$ defines an A-linear map $B \to A$, so since B is a finite, projective and separable A-algebra, there exists an $x' \in B$ such that $\mathrm{Tr}(xy) = \mathrm{Tr}_{B/A}(x'y)$ for all $y \in B$. It follows from basic properties of the trace that $\mathrm{Tr}(xy) = \mathrm{Tr}(x'y)$ for all $y \in B \otimes_A K$. Since $B \otimes_A K$ is separable over K, we conclude that that $x = x' \in B$, so $B = \prod_{i=1}^t B_i$. □

Proposition 1.5. *Let X be a normal integral scheme and $f : Y \to X$ a finite étale morphism, and suppose further that Y is connected. Then Y is integral, and if L is the function field of Y, then f is the normalization of X in L.*

Proof. Let $\operatorname{Spec} A \subset X$ be an affine open subscheme. Then A is an entire ring integrally closed in its field of fractions, so if $f^{-1}(\operatorname{Spec} A) = \operatorname{Spec} B$, proposition 1.3 shows that B is a finite, projective and separable A-algebra, so lemma 1.4 states that B is a product of entire rings. Thus $\operatorname{Spec} B$ is a disjoint union of open irreducible subsets and all of its local rings are entire. Letting $\operatorname{Spec} A \subset X$ vary, we see that Y must also be a disjoint union of open irreducible subsets with all local rings entire. Since Y is connected, we conclude that Y must be irreducible and therefore integral. Moreover, now lemma 1.4 also shows that Y is precisely the normalization of X in the function field L of Y. □

Proposition 1.6. *Let X be a curve with function field K and let L be a finite separable field extension of K. If $Y \to X$ is the normalization of X in L, then Y is a curve.*

Proof. The statement is local, so it suffices to consider the case $X = \operatorname{Spec} A$ for A a Dedekind ring. Then $Y = \operatorname{Spec} B$ for B the integral closure of A in L. Since A is noetherian, B is finitely generated as an A-module [1, proposition 5.17], so is noetherian. Also, since B is integral over A, $\dim B = \dim A = 1$. The field of fractions of B is L, so B is integrally closed in its field of fractions. Thus B is Dedekind [1, theorem 9.3]. Letting $\operatorname{Spec} A \subset X$ vary, we obtain a cover of Y of the form $\operatorname{Spec} B$ for Dedekind rings B, and therefore conclude that Y is a curve. □

Corollary 1.7. *Let X be a curve and $Y \to X$ a finite étale covering of X. Then $Y = \coprod Y_i$ and each Y_i is a curve.*

Proof. Since $Y \to X$ is finite étale, if Y_i is a connected component of Y, the map $Y_i \to X$ is also clearly finite étale. Thus Y_i is the normalization of X in the function field of Y_i, so Y_i is a curve. □

2 Morphisms of curves

In this section, we characterize what it means for morphisms of curves to be flat and unramified. We then establish some useful properties of normalizations that will be used in subsequent sections.

2.1 Finite and flat morphisms

Lemma 2.1. *Let A be a discrete valuation ring with uniformizer π and let M an A-module. Then M is flat if and only if π is not a zero-divisor on M. Moreover, if M is finitely generated, then M is flat if and only if it is free.*

Proof. Since A is a discrete valuation ring, the set of ideals (π^i) as i varies is all ideals of A [1, proposition 9.2]. Thus M is flat if and only if the multiplication map $(\pi^i) \otimes M \to M$ is injective for all i [3, chapter XVI, proposition 3.7]. In other words, M is flat if and only if π^i is not a zero-divisor on M for all i. Furthermore, if π is not a zero-divisor on M, then neither is π^i for any other i. This proves the first statement, so now suppose M is finitely generated. The above shows that M is flat if and only if it is torsion-free, and since A is a principal entire ring, we conclude that M is torsion-free if and only if it is free [3, theorem 7.3]. $\square$

Proposition 2.2. *A morphism $f : Y \to X$ of curves is flat if and only if it maps the generic point of Y to the generic point of X.*

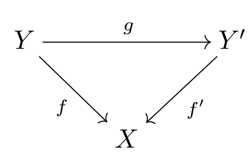
Proof. Suppose first that f is flat and suppose $y \in Y$ maps to a closed point $x = f(y) \in X$. Let π_x be a uniformizer for the discrete valuation ring $\mathcal{O}_{X,x}$. The local homomorphism $f^\sharp : \mathcal{O}_{X,x} \to \mathcal{O}_{Y,y}$ must map π_x into $\mathfrak{m}_y$, but since f is flat, $f^\sharp(\pi_x)$ cannot be a zero-divisor in $\mathcal{O}_{Y,y}$ by lemma 2.1. Thus $f^\sharp(\pi_x)$ is a nonzero element of $\mathfrak{m}_y$, so $\mathcal{O}_{Y,y}$ is not a field and y cannot be the generic point of Y.

Conversely, suppose f maps the generic point $y \in Y$ to a closed point $x = f(y) \in X$. Then $\mathcal{O}_{X,x}$ is a discrete valuation ring, so letting π_x be a uniformizer, we see that $f^\sharp : \mathcal{O}_{X,x} \to \mathcal{O}_{Y,y}$ must map π_x into $\mathfrak{m}_y = 0$. Therefore π_x is a zero-divisor on $\mathcal{O}_{Y,y}$, so $\mathcal{O}_{Y,y}$ cannot be flat over $\mathcal{O}_{X,x}$ by lemma 2.1. $\square$

Corollary 2.3. *A finite morphism $f : Y \to X$ of curves is flat if and only if it is surjective. Moreover, if the finite morphism f is not flat, its image consists of a single closed point of X.*

Proof. The image of a finite morphism must be closed. Therefore f is flat if and only if its the image is a closed set containing the generic point, if and only if it is surjective. Moreover, since Y is irreducible, its image must be irreducible, so if f is not flat, its image is a nonempty, proper, closed and irreducible subset of X. Since X is one-dimensional, this implies that the image of f is a single closed point of X. $\square$

Lemma 2.4. *Suppose that*



is a commutative diagram of morphisms of curves, and that f and f' are finite. Then g is finite. Moreover, f is flat if and only if g and f' are flat.

Proof. Let $\operatorname{Spec} A \subset X$ be an affine open subscheme. Then $g^{-1}(\operatorname{Spec} A) = \operatorname{Spec} B$ for B a finitely generated A-module. Also, $f'^{-1}(\operatorname{Spec} A) = \operatorname{Spec} B'$ for B' a finitely generated A-module. Thus

$$g^{-1}(\operatorname{Spec} B') = (f' \circ g)^{-1}(\operatorname{Spec} A) = f^{-1}(\operatorname{Spec} A) = \operatorname{Spec} B$$

and B is finitely generated over A, so it is also certainly finitely generated over B'. As $\operatorname{Spec} A \subset X$ varies, the sets $\operatorname{Spec} B' \subset Y'$ form an open cover, so we conclude that g is finite.

If g and f' are flat, then they are both surjective. Then f is surjective and therefore flat as well. Conversely, suppose f is flat. Then it is surjective, so f' is surjective and therefore flat as well. Moreover, if g is not flat, then its image is a single closed point of Y', so the image of the composite $f' \circ g$ is also a single closed point of X, which contradicts the fact that $f' \circ g = f$ is surjective. $\square$

Let $Y \to X$ be a finite and flat morphism of curves. Then the generic point of Y maps to the generic point of X, so if K and L are the function fields of X and Y, respectively, the finite morphism $Y \to X$ induces a finite field extension $K \to L$. We define the *degree* of Y over X to be

$$[Y : X] = [L : K].$$

2.2 Ramification

Let $Y \to X$ be a finite and flat morphism of curves, and let K and L be the function fields of X and Y, respectively. Let L^{sep} denote the separable closure of K inside L. Then we define the *separable degree* of Y over X by

$$[Y : X]_{\text{sep}} = [L : K]_{\text{sep}} = [L^{\text{sep}} : K]$$

and the *inseparable degree* of Y over X by

$$[Y : X]_{\text{ins}} = [L : K]_{\text{ins}} = [L : L^{\text{sep}}].$$

We say that $Y \to X$ is *separable*, or *inseparable*, or *purely inseparable* if L is a separable, or inseparable, or purely inseparable field extension of K, respectively. The following are easily seen to be equivalent.

(a) The morphism $Y \to X$ is separable.

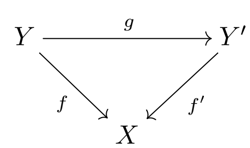
(b) The separable degree $[Y : X]_{\text{sep}}$ coincides with the degree $[Y : X]$.

(c) The morphism $Y \to X$ is unramified at the generic point of Y.

For a closed point $y \in Y$, set $x \in X$ be its image. Since $Y \to X$ is finite, it is a closed map, so x must be a closed point and $\mathcal{O}_{X,x}$ a discrete valuation ring. The *ramification index* $e(y)$ of y is defined to be the valuation of the image of a uniformizer $\pi_x \in \mathcal{O}_{X,x}$ under the map $\mathcal{O}_{X,x} \to \mathcal{O}_{Y,y}$. Thus, $e(y) = 1$ if and only if $\mathfrak{m}_x \cdot \mathcal{O}_{Y,y} = \mathfrak{m}_y$. When it is ambiguous, we will also write $e(y/x)$ for the ramification index of y over x.

Using this terminology, $Y \to X$ is unramified at y if and only if $e(y) = 1$ and the residue field $k(y)$ is a finite and separable field extension of $k(x)$. The degree $[k(y) : k(x)]$ of the field extension of residue fields is called the *residue class degree* of y.

Lemma 2.5. *Suppose that*



is a commutative diagram of finite and flat morphisms of curves. Then f is unramified if and only if g and f' are unramified.

Proof. Consider any set of points $y \in Y$, $y' \in Y'$, and $x \in X$ such that $g(y) = y'$ and $f'(y') = x$. A uniformizer $\pi_x \in \mathcal{O}_{X,x}$ maps to an element of valuation $e(y'/x)$ in $\mathcal{O}_{Y',y'}$, which then maps to an element of valuation $e(y'/x)e(y/y')$ in $\mathcal{O}_{Y,y}$. Since the diagram commutes, we obtain

$$e(y'/x)e(y/y') = e(y/x).$$

Moreover, the extension $k(y)$ over $k(x)$ can be decomposed as the composite of the extensions of $k(y')$ over $k(x)$ and then $k(y)$ over $k(y')$.

If g and f' are unramified, then $e(y'/x) = e(y/y') = 1$, so $e(y/x) = 1$, and then $k(y)$ over $k(x)$ is finite and separable since $k(y')$ over $k(x)$ and $k(y)$ over $k(y')$ are. Letting y, y', and x vary shows that f is unramified. Conversely, if f is unramified, then $1 = e(y/x) = e(y'/x)e(y/y')$ forces $e(y'/x) = e(y'/y) = 1$, and then since $k(y)$ is a finite separable extension of $k(x)$, it follows that both $k(y')$ over $k(x)$ and $k(y)$ over $k(y')$ are as well. Again letting x, y and y' vary, we conclude that g and f' are both unramified. □

We can now easily show that a morphism between finite étale coverings of a curve must itself be finite étale as well.

Proposition 2.6. *Let X be a curve and suppose $Y \to X$ and $Y' \to X$ are finite étale coverings of X. If*

$$\begin{array}{ccc} Y & \longrightarrow & Y' \\ & \searrow \quad \swarrow & \\ & X & \end{array}$$

is any morphism in $\mathcal{F\acute{E}t}_X$, then $Y \to Y'$ is a finite étale morphism.

Proof. We know from proposition 1.6 that Y and Y' are curves. By lemma 2.4, it follows that $Y \to Y'$ is finite and flat, and by lemma 2.5, it is unramified. □

We conclude our discussion of ramification for morphisms of curves with the following formula relating the degree of a finite and flat morphism of curves with ramification indices and residue class degrees. We will not need this for proving the existence of the fundamental group of a curve, but we will use it in the subsequent calculations.

Proposition 2.7. *Let $f : Y \to X$ be a finite and flat morphism of curves. Then for every closed point $x \in X$,*

$$\sum_{y \in f^{-1}(x)} e(y)[k(y) : k(x)] = [Y : X].$$

Proof. We first claim that, for any closed point $x \in X$, the preimage $f^{-1}(x)$ is a nonempty and finite set of closed points $y_1, \ldots, y_r$, and

$$(f_* \mathcal{O}_Y)_x = \bigoplus_{i=1}^{r} \mathcal{O}_{Y,y_i}.$$

To see this, observe that since f is finite, it is quasi-finite, and since it is flat, it is surjective, so the preimage of x must be a nonempty, finite set of closed points $y_1, \ldots, y_r \in Y$. Now observe that

$$(f_* \mathcal{O}_Y)_x = \operatorname*{colim}_{U \ni x} f_* \mathcal{O}_Y(U) = \operatorname*{colim}_{U \ni x} \mathcal{O}_Y(f^{-1}(U))$$

so by taking the limit over the cofinal set of all open neighborhoods U of x such that $f^{-1}(U)$ is a collection of disjoint neighborhoods $V_1, \ldots, V_r$ of $y_1, \ldots, y_r$, respectively, it follows that

$$(f_* \mathcal{O}_Y)_x = \operatorname*{colim}_{U \ni x} \mathcal{O}_Y \left(\bigcup_{i=1}^{r} V_i \right) = \operatorname*{colim}_{U \ni x} \bigoplus_{i=1}^{r} \mathcal{O}_Y(V_i) = \bigoplus_{i=1}^{r} \mathcal{O}_{Y,y_i},$$

where the second isomorphism is a result of the sheaf axiom for $\mathcal{O}_Y$.

Next, we claim that $f_* \mathcal{O}_Y$ is locally free of rank $[Y : X]$ on X. To see this, fix any point $x \in X$. Since f is finite and flat, we know that $(f_* \mathcal{O}_Y)_x$ is finitely generated and flat over $\mathcal{O}_{X,x}$ since it is a direct sum of the stalks $\mathcal{O}_{Y,y_i}$ which are flat over $\mathcal{O}_{X,x}$. By lemma 2.1, it must be free of some finite rank r. Thus there exists some open neighborhood U of x such that $(f_* \mathcal{O}_X)|_U$ is free of rank r [4, theorem 4.6]. Then U also contains the generic point, so we must have $r = [Y : X]$. Letting $x \in X$ vary, we conclude that $f_* \mathcal{O}_Y$ is locally free of rank $[Y : X]$.

Now clearly it suffices to prove that, if $x \in X$ is a closed point, for any $y \in f^{-1}(x)$, the local ring $\mathcal{O}_{Y,y}$ is free of rank $e(y)[k(y) : k(x)]$ over $\mathcal{O}_{X,x}$. Since tensoring up to $k(x)$ preserves rank, it further suffices to prove that

$$\mathcal{O}_{Y,y} \otimes_{\mathcal{O}_{X,x}} k(x) = \mathcal{O}_{Y,y} / (\mathfrak{m}_x \cdot \mathcal{O}_{Y,y})$$

is of dimension $e(y)[k(y) : k(x)]$ over $k(x)$. Let π_y be a uniformizer for $\mathcal{O}_{Y,y}$ such that a uniformizer of $\mathcal{O}_{X,x}$ is mapped to $\pi_y^{e(y)}$, so

$$\mathcal{O}_{Y,y} / (\mathfrak{m}_x \cdot \mathcal{O}_{Y,y}) = \mathcal{O}_{Y,y} / (\pi_y^{e(y)}).$$

Now consider the filtration

$$\mathcal{O}_{Y,y} \supset (\pi_y) \supset (\pi_y^2) \supset \cdots \supset (\pi_y^e(y)).$$

The successive quotients of this filtration are

$$(\pi_y^i)/(\pi_y^{i+1}) = (\pi_y^i) \otimes k(y)$$

which is clearly one-dimensional over $k(y)$ by Nakayama's lemma, and therefore has dimension $[k(y) : k(x)]$ over $k(x)$. Since there are $e(y)$ steps in the filtration, we conclude that $\mathcal{O}_{Y,y} \otimes_{\mathcal{O}_{X,x}} k(x)$ has dimension $e(y)[k(y) : k(x)]$ over $k(x)$. □

2.3 Normalizations

We saw in proposition 1.5 that finite étale morphisms into a curve arise as normalizations. Here we prove the converse statement.

Proposition 2.8. *Let X be a curve with function field K and let $f : Y \to X$ be the normalization of X in a finite separable field extension L of K. Then f is a finite and flat morphism of curves of degree $[L : K]$.*

Proof. We know that Y is a curve by proposition 1.6. To see that $Y \to X$ is finite and flat, we may assume that $X = \operatorname{Spec} A$ is affine. Then $Y = \operatorname{Spec} B$ for B the integral closure of A in L. Since A is noetherian, B is finitely generated as an A-module [1, proposition 5.17], so f is finite. Moreover, f is surjective by the lying-over theorem, so by corollary 2.3, we conclude that f is finite and flat. Finally, the field of fractions of B is L, so f is of degree $[L : K]$. □

Suppose X is a curve with function field K, and suppose L is a finite separable extension of K. If the normalization $Y \to X$ of X in L is an unramified morphism, then we say that X is *unramified in L*. By proposition 2.8, this is precisely the condition necessary for the normalization to be a finite étale morphism. Using the terminology of [3, chapter V, section 1], we now show that the class of field extensions of K in which X is unramified is distinguished.

Proposition 2.9. *Let X be a curve with function field K. Suppose L is a finite separable field extension of K and $L' \subset L$ is a subfield. Let $Y' \to X$ be the normalization of X in L'. Then X is unramified in L if and only if it is unramified in L' and Y' is unramified in L.*

Proof. Let $Y \to X$ be the normalization of X in L and let $Y \to Y'$ to the normalization of Y' in L. Then evidently the diagram

$$\begin{array}{ccc} Y & \longrightarrow & Y' \\ & \searrow \quad \swarrow & \\ & X & \end{array}$$

commutes, and all maps are finite and flat by proposition 2.8. Now apply lemma 2.5. □

Proposition 2.10. *Let X be a curve with function field K. Suppose L is a finite separable extension of K with X unramified in L. Let K' be a finite separable extension of X and let $X' \to X$ be the normalization of X in K'. Then X' is unramified in any compositum L' of L and K'.*

Proof. Since $Y \to X$ is finite étale, it follows from propositions 1.1 and 1.3 that $X' \times_X Y \to X'$ is finite étale. By proposition 1.6, we know that X' is a curve, so by proposition 1.7, we see that we can write $X' \times_X Y = \coprod Y_i'$ where each connected component Y_i' is a curve. This gives us the following cartesian diagram.

$$\begin{array}{ccc} \coprod Y_i' & \longrightarrow & Y \\ \downarrow & & \downarrow \\ X' & \longrightarrow & X \end{array}$$

By proposition 2.2, the fiber of $\coprod Y_i'$ over the generic point $\operatorname{Spec} K' \to X'$ consists precisely of the generic points of the connected components of $\coprod Y_i'$. But also, the fiber of $\coprod Y_i' = X' \times_X Y' \to X'$ over $\operatorname{Spec} K' \to X'$ is $\operatorname{Spec} K' \otimes_K L$. Consider the surjective map $K' \otimes_K L \to L'$ given by multiplication. The kernel of this homomorphism is a point of $\operatorname{Spec} K' \otimes_K L$ whose stalk is L'. In other words, the kernel corresponds to the generic point of some connected component Y_i' of $\coprod Y_i'$, and then Y_i' has function field L'.

Since the map $\coprod Y_i' \to X'$ is finite étale, so is $Y_i' \to X'$. Thus, by proposition 1.3, $Y_i' \to X'$ is the normalization of X' in L'. In fact, since $Y_i' \to X'$ is finite étale, we conclude that X' is unramified in L'. □

A formal consequence of the previous two results is the following.

Corollary 2.11. *Let X be a curve with function field K and suppose L and L' are finite separable extensions of K. If X is unramified in L and L', then X is unramified in any compositum E of L and L'.*

3 Fundamental group

Notation will remain fixed throughout this section. Let X be a curve with function field K. Let $\bar{K}$ be an algebraic closure of K and let I denote the set of all finite and separable field extensions L of K contained in $\bar{K}$ such that X is unramified in L. Then let M be the compositum of all such field extensions. We will call M the *maximal unramified extension* of K in $\bar{K}$. Observe that

$$M = \bigcup_{L \in I} L.$$

To see this, suppose $\alpha \in L$ and $\beta \in L'$ for some $L, L' \in I$. Then $\alpha \pm \beta$ and $\alpha\beta^{-1}$ (when β is nonzero) are elements of the compositum $L \cdot L'$ in M, which is in I by corollary 2.11. Thus $\alpha \pm \beta$ and $\alpha\beta^{-1}$ are also contained in $\bigcup_{L \in I} M$.

Lemma 3.1. *Let L be a subfield of M containing K. If L is finite over K, then $L \in I$.*

Proof. Since L is a subfield of the separable extension M, it is itself separable. Thus, by the theorem of the primitive element, we write $L = K(\alpha)$ for some $\alpha \in L \subset M$. But $M = \bigcup_{L' \in I} L'$, so there exists some $L' \in I$ such that $\alpha \in L'$, hence $L \subset L'$. Proposition 2.9 now states that X is unramified in L. □

Lemma 3.2. *M is a Galois extension of K.*

Proof. Suppose $L \in I$. By the theorem of the primitive element, we may write $L = K(\alpha)$, and then let $\alpha_1, \dots, \alpha_r$ be the Galois conjugates of α in $\bar{K}$. The fields $K(\alpha_i)$ are isomorphic to $K(\alpha)$ as field extensions of K. Thus, clearly X is unramified in $K(\alpha_i)$ for all i. Corollary 2.11 now implies that X is unramified in the compositum of all $K(\alpha_i)$, which is precisely the Galois closure of $K(\alpha) = L$. It follows that M is a Galois extension of K [4, theorem 2.2]. □

Define $G = \operatorname{Gal}(M/K)$ and let $\mathcal{FS}\text{et}_G$ denote the category of finite sets on which G acts continuously, together with G-equivariant maps. This is a non-full subcategory of the category $\mathcal{S}\text{et}$ of sets.

The generic point of X defines a morphism $\operatorname{Spec} K \to X$. Consider the functor $Q : \mathcal{F\acute{E}}\text{t}_X \to \mathcal{S}\text{et}$ given by

$$Q(Y \to X) = \operatorname{Hom}_{\operatorname{Spec} K}(\operatorname{Spec} M, \operatorname{Spec} K \times_X Y).$$

This definition is somewhat opaque, but makes functoriality of Q evident. In the process of showing that Q induces an equivalence with $\mathcal{FS}\text{et}_G$, the proof of theorem 3.3 below will unwind this definition.

Theorem 3.3. *The functor Q is an equivalence of categories $\mathcal{F\acute{E}}\text{t}_X \to \mathcal{FS}\text{et}_G$.*

Proof. Define a right action of G on the set $Q(Y \to X)$ by precomposition, so that if $\varphi \in Q(Y \to X)$ and $\sigma \in G$, then $\varphi \cdot \sigma = \varphi \circ \operatorname{Spec}(\sigma)$. If

$$\begin{array}{ccc} Y & \xrightarrow{\quad g \quad} & Y' \\ & \searrow \quad \swarrow & \\ & X & \end{array}$$

is a morphism in $\mathcal{F}\acute{\mathcal{E}}\mathrm{t}_X$, it is evident that the induced map

$$Q(Y \to X) \xrightarrow{Q(g)} Q(Y' \to X)$$

is G-equivariant.

Fix a finite étale cover $Y \to X$. We now show that $Q(Y \to X)$ is a finite set on which G acts continuously. Notice that $\operatorname{Spec} K \times_X Y$ is precisely the fiber of $Y \to X$ over the generic point $\operatorname{Spec} K \to X$, so consists of the generic points of the connected components of Y by proposition 2.2. If we write $Y = \coprod Y_i$ and each integral subscheme Y_i has function field L_i, we see that

$$\operatorname{Spec} K \times_X Y = \coprod \operatorname{Spec} L_i.$$

Thus

$$Q(Y \to X) = \operatorname{Hom}_{\operatorname{Spec} K}\left(\operatorname{Spec} M, \coprod \operatorname{Spec} L_i\right) = \coprod \operatorname{Hom}_K(L_i, M)$$

where passing across the final identification, the right action of G on $\coprod \operatorname{Hom}_{\operatorname{Spec} K}(\operatorname{Spec} M, \operatorname{Spec} L_i)$ given by precomposition becomes a left action on $\coprod \operatorname{Hom}_K(L_i, M)$ given by postcomposition. But it is well-known that

$$\operatorname{Hom}_K(L_i, M) = G/H_i$$

as G-sets, where $H_i = \operatorname{Gal}(M/L_i)$. Since L_i is of finite degree over K, the fundamental theorem of Galois theory states that $H_i \subset G$ is an open subgroup, which must have finite index in G. Thus we conclude that each G/H_i and therefore $Q(Y \to X)$ is finite. Moreover the kernel of the action of G on $Q(Y \to X)$ is the open subgroup $\bigcap H_i \subset G$, so the action is continuous. Thus, the image of the functor Q is indeed contained in $\mathcal{FS}\mathrm{et}_G$.

Observe that any E in $\mathcal{FS}\mathrm{et}_G$ can be decomposed into orbits and written as $E = \coprod G/H_i$ for open subgroups $H_i \subset G$, since the kernel of a continuous action of G on a finite set must be open. By the fundamental theorem of Galois theory, $L_i = M^{H_i}$ is finite separable extension of K, and X is unramified in L_i by lemma 3.1. Thus the normalization $Y_i \to X$ of X in L_i is a finite étale morphism, and if we set $Y = \coprod Y_i$, then $Y \to X$ is also a finite étale morphism. Moreover, using the same sequence of identifications as above,

$$Q(Y \to X) = \operatorname{Hom}_{\operatorname{Spec} K}(\operatorname{Spec} M, \operatorname{Spec} K \times_X Y) = \coprod G/\operatorname{Gal}(M/L_i),$$

but by the fundamental theorem of Galois theory, we also know that $\operatorname{Gal}(M/L_i) = H_i$. Thus

$$Q(Y \to X) = \coprod G/H_i$$

and we conclude that Q is essentially surjective.

We now show that it is fully faithful. Suppose $Y \to X$ and $Y' \to X$ are both finite étale morphisms. We wish to show that the map

$$\operatorname{Hom}_X(Y \to X, Y' \to X) \longrightarrow \operatorname{Hom}_G(Q(Y \to X), Q(Y' \to X))$$

is a bijection. We write $Y = \coprod_{i \in I} Y_i$ and $Y' = \coprod_{j \in J} Y_j$ and then, as above, we make the identifications

$$Q(Y \to X) = \coprod_{i \in I} G/H_i$$

and

$$Q(Y' \to X) = \coprod_{j \in J} G/H'_j$$

for open subgroups $H_i = \mathrm{Gal}(M/L_i)$, where L_i is the function field of Y_i, and $H'_j = \mathrm{Gal}(M/L'_j)$ for L'_j the function field of Y'_j. It is clear that a G-equivariant map

$$h : \coprod_{i \in I} G/H_i \to \coprod_{j \in J} G/H'_j$$

must correspond uniquely to a set map $\delta : I \to J$ such that h restricts to a G-equivariant map of G/H_i into $G/H'_{\delta(i)}$. This induces an inclusion $H_i \subset H'_{\delta(i)}$ and therefore a field extension $L_i \supset L'_{\delta(i)}$. Thus Y_i is the normalization of $Y'_{\delta(i)}$ in L_i and there is an induced map $Y_i \to Y'_{\delta(i)}$. Piecing together these maps gives a morphism $g : Y \to Y'$ in $\mathcal{F\acute{E}t}_X$. Chasing through the sequence of identifications made above shows that we must have $Q(g) = h$, so Q is full. Now suppose

$$g' : \coprod_{i \in I} Y_i \to \coprod_{j \in J} Y'_j$$

is another map in $\mathcal{F\acute{E}t}_X$ such that $Q(g') = h$. Since each Y_i is connected, there must exist a $\delta' : I \to J$ such that g' restricts to a map of Y_i into $Y'_{\delta'(i)}$ and the diagram

$$\begin{array}{ccc} Y_i & \longrightarrow & Y'_{\delta'(i)} \\ & \searrow \quad \swarrow & \\ & X & \end{array}$$

commutes. We know from proposition 2.6 that $Y_i \to Y'_{\delta'(i)}$ is a finite étale morphism, so by proposition 1.5, Y_i must be the normalization of $Y'_{\delta'(i)}$ in L_i. Moreover, since $Q(g') = h$, clearly we must have $\delta' = \delta$. Thus g' exactly matches our construction of g above, so $g = g'$, and we conclude that Q is fully faithful and therefore an equivalence.[3] □

Henceforth, we will write $\pi(X)$ for $G = \mathrm{Gal}(M/K)$. This is the *(étale) fundamental group* of X.

4 Examples

4.1 Fundamental group of the integers

Consider the curve $X = \mathrm{Spec}\,\mathbf{Z}$. Minkowski's theorem [6, theorem 5.4.10] states that, in any finite separable extension L of $\mathbf{Q}$, some prime in the ring of integers of L is ramified. Therefore the maximal unramified extension of $\mathbf{Q}$ is $\mathbf{Q}$ itself, and then

$$\pi(\mathrm{Spec}\,\mathbf{Z}) = \mathrm{Gal}(\mathbf{Q}/\mathbf{Q}) = 1.$$

Thus the only finite étale coverings of $\mathrm{Spec}\,\mathbf{Z}$ are trivial.

[3]This proof avoided the construction of an explicit inverse functor $\mathcal{FS}\mathrm{et}_G \to \mathcal{F\acute{E}t}_X$ to Q, but the proof of essential surjectivity of Q effectively describes the action of the inverse functor $\mathcal{FS}\mathrm{et}_G \to \mathcal{F\acute{E}t}_X$ on objects.

4.2 Fundamental group of the projective line

Suppose K is an algebraically closed field. Then $\mathbf{P}^1$ is proper over K, and if $Y \to \mathbf{P}^1$ is any finite étale morphism, the composite $Y \to \operatorname{Spec} K$ is proper as well, so Y is a proper curve over K.

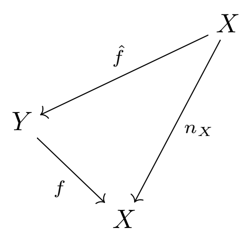
Let E denote the function field of $\mathbf{P}^1$ and suppose L is a finite separable extension of E of degree n with $\mathbf{P}^1$ unramified in L. Let $f : Y \to \mathbf{P}^1$ be the normalization of $\mathbf{P}^1$ in L. Then Y is a curve, and by Hurwitz's formula [2, chapter IV, corollary 2.4], we see that Y has genus $g' = 1 - n$. This is impossible unless $n = 1$, in which case $L = E$. Therefore the maximal unramified extension M of E is precisely E, and

$$\pi(X) = \operatorname{Gal}(E/E) = 1.$$

In other words, as with $\operatorname{Spec} \mathbf{Z}$, the only coverings of $\mathbf{P}^1$ are trivial. We remark here that, when $K = \mathbf{C}$, the analytification of $\mathbf{P}^1$ is a sphere, and the ordinary topological fundamental group of the sphere is also known to be trivial.

4.3 Fundamental groups of elliptic curves

Let K be an algebraically closed field of characteristic $p \geqslant 0$. Suppose X is a proper curve of genus 1 over K. Let E be the function field of X and L a finite separable field extension of degree n with X unramified in L. Then let $f : Y \to X$ be the normalization of X in L. As before, Y is a proper curve over K and Hurwitz's formula implies that Y is of genus 1 as well. In other words, choosing a closed point $0 \in X$ and then a closed point $0 \in f^{-1}(0)$, f becomes a surjective isogeny of elliptic curves of degree n. If $\hat{f} : X \to Y$ is the dual isogeny, we obtain a commutative diagram



where $n_X : X \to X$ is multiplication by n. Thus L is contained as a subfield of the extension field E_n of E corresponding to $n_X : X \to X$. Let E_n^{sep} denote the separable closure of E inside E_n and observe that we still have $L \subset E_n^{\text{sep}}$.

Let $n_X^{\text{sep}} : X' \to X$ the normalization of X in E_n^{sep}. As above, n_X^{sep} is a surjective isogeny of elliptic curves. Then n_X^{sep} is a separable morphism, so the locus of points at which n_X^{sep} is unramified contains the generic point, so there must exist an unramified closed point of X.[4] Using the translation maps of X shows that every other closed point is also unramified, so n_X^{sep} is unramified. In other words, the maximal unramified extension M of E is the union of all E_n^{sep} as n varies.

The preimage of the closed point $0 \in X$ is precisely $\operatorname{Ker} n_X^{\text{sep}}$. Since K is algebraically closed, the residue class degrees in the formula of proposition 2.7 are all 1, and since n_X^{sep} is unramified, all ramification indices are also 1, so the left hand side of the formula counts points in the preimage of 0. Thus,

$$[E_n^{\text{sep}} : E] = [X' : X] = \# \operatorname{Ker} n_X^{\text{sep}} = \# \operatorname{Aut}(E_n^{\text{sep}}/E),$$

where the last equality is a result of the bijection of [5, chapter III, theorem 4.10(b)], which takes a closed point $x \in \operatorname{Ker} n_X^{\text{sep}}$ to the field automorphism induced by the translation map by x at the generic point. This

[4] One way of seeing this is to use the fact that n_X^{sep} is unramified at $x \in X'$ if and only if $(\Omega_{X'/X})_x = 0$. Thus, the set of ramified points corresponds to the support of the coherent sheaf $\Omega_{Y/X}$, which is necessarily closed.

shows that E_n^{sep} is a finite Galois extension of E. Therefore,

$$\pi(X) = \mathrm{Gal}(M/E) = \lim_n \mathrm{Gal}(E_n^{\mathrm{sep}}/E)$$

where the limit is over positive integers partially ordered by divisibility. Since the prime powers are cofinal in this set, in fact we have

$$\pi(X) = \prod_\ell \lim_r \mathrm{Gal}(E_{\ell^r}^{\mathrm{sep}}/E),$$

where ℓ varies over primes.

When $\ell \neq p$, the field extension E_{ℓ^r} is of degree ℓ^{2r} over E and therefore cannot be inseparable. Thus we have $E_{\ell^r} = E_{\ell^r}^{\mathrm{sep}}$, and

$$\mathrm{Gal}(E_{\ell^r}^{\mathrm{sep}}/E) = \mathrm{Gal}(E_{\ell^r}/E) = \mathrm{Ker}\,\ell_X^r = (\mathbf{Z}/\ell^r\mathbf{Z} \times \mathbf{Z}/\ell^r\mathbf{Z}),$$

whence

$$\lim_r \mathrm{Gal}(E_{\ell^r}^{\mathrm{sep}}/E) = \lim_r (\mathbf{Z}/\ell^r\mathbf{Z} \times \mathbf{Z}/\ell^r\mathbf{Z}) = \mathbf{Z}_\ell \times \mathbf{Z}_\ell.$$

When $p = 0$, this is the whole story and we can conclude that

$$\pi(X) = \prod_\ell \mathbf{Z}_\ell \times \mathbf{Z}_\ell.$$

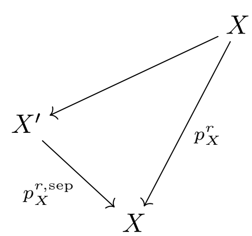
Now suppose $p > 0$. If X is supersingular, then p_X^r is purely inseparable for all r, so $E_{p^r}^{\mathrm{sep}} = E$. Hence

$$\lim_r \mathrm{Gal}(E_{p^r}^{\mathrm{sep}}/E) = 1$$

and we conclude that

$$\pi(X) = \prod_{\ell \neq p} \mathbf{Z}_\ell \times \mathbf{Z}_\ell.$$

Now suppose X is ordinary. Observe that we have the following commutative diagram



where $X \to X'$ is the normalization of X' in the purely inseparable field extension $E_{p^r}^{\mathrm{sep}} \subset E_{p^r}$. Then

$$\#\,\mathrm{Ker}(X \to X') = [E_{p^r} : E_{p^r}^{\mathrm{sep}}]_{\mathrm{sep}} = 1,$$

where the first equality is [5, chapter III, theorem 4.10(a)]. This gives us the middle identification in

$$\mathrm{Gal}(E_{p^r}^{\mathrm{sep}}/E) = \mathrm{Ker}\,p_X^{r,\mathrm{sep}} = \mathrm{Ker}\,p_X^r = \mathbf{Z}/p^r\mathbf{Z},$$

so

$$\pi(X) = \left(\lim_r \mathbf{Z}/p^r\mathbf{Z}\right) \times \prod_{\ell \neq p} \mathbf{Z}_\ell \times \mathbf{Z}_\ell = \mathbf{Z}_p \times \prod_{\ell \neq p} \mathbf{Z}_\ell \times \mathbf{Z}_\ell.$$

We conclude with a remark about comparisons with topological fundamental group. Suppose $K = \mathbf{C}$ and recall that the analytification of X is a torus, whose topological fundamental group is $\mathbf{Z} \times \mathbf{Z}$. Notice that we can rewrite

$$\pi(X) = \prod_{\ell} \mathbf{Z}_\ell \times \mathbf{Z}_\ell = \hat{\mathbf{Z}} \times \hat{\mathbf{Z}}$$

and this is precisely the profinite completion of $\mathbf{Z} \times \mathbf{Z}$. This phenomenon is what we observed for $\mathbf{P}^1$ as well, and in fact, it is no accident: for a scheme X of finite type over $\mathbf{C}$, the étale fundamental group $\pi(X)$ is known to be the profinite completion of the topological fundamental group of the analytification of X.

References

[1] Michael F. Atiyah and Ian G. Macdonald. *Introduction to commutative algebra.* Addison-Wesley Publishing Company, Inc., London, 1969.

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

[3] Serge Lang. *Algebra.* Springer-Verlag, New York, 2002. Graduate Texts in Mathematics, No. 211.

[4] Hendrick W. Lenstra. Galois theory for schemes. Course notes available from the Universiteit Leiden Mathematics Department, `http://websites.math.leidenuniv.nl/algebra/GSchemes.pdf`.

[5] Joseph H. Silverman. *The arithmetic of elliptic curves.* Springer-Verlag, New York, 2009. Graduate Texts in Mathematics, No. 106.

[6] Edwin Weiss. *Algebraic number theory.* Dover Publications Inc., Mineola, 1998. Reprint of the 1963 original.