GALOIS GROUPS AND THE ETALE FUNDAMENTAL GROUP

ALEXANDRE PUTTICK

Abstract. The following texts consists of a first-year Masters student "memoire" on the subject of the deep link between two seemingly very different objects: Algebraic Extensions over an arbitrary base field and Galois theory on one side versus the topological fundamental group and it's covering spaces. We give a summary of both theories before building the first link in considering branched coverings of Riemann surfaces. This leads to an algebraic generalization of the fundamental group, the *étale fundamental group*, introduced by Grothendieck in [5], where we will also introduce the language of schemes. We conclude with a discussion of further topics and applications to the inverse Galois problem. As the writer intends this to be more as a demonstration of his own understanding, almost all of what follows was written with a little reference to the texts as possible. As such, details are lacking, and one should consult the reference material for rigorous treatment.

Contents

Date: June 2012.

1. Introduction

At the introduction of the fundamental group of a path-connected topological space and the classification of its covering spaces, the obvious aesthetic resemblance to the Galois theory of fields did not go unmarked, and it was immediately wondered if there was some deep connection between them. It was this very discernible correlation that caused the writer to ask himself the very same question as an undergraduate and to subsequently explore the answer in this paper. While the relation is easily expounded in the theory of branched coverings of a connected, compact Riemann surface and field extensions of its field of meromorphic functions, it was not until the 1960s, when Alexandre Grothendiek was able to find the proper generalization of a topology on algebraic objects and a corresponding algebraic notion of the fundamental group, that a full algebraic analogue of the topological situation and the direct relation to Galois theory was demonstrated. This text aims to explore this relation along quasi-historical lines, with a short word on modern applications. We assume certain knowledge in algebra, algebraic topology, commutative algebra and category theory, but will state all necessary results and give proofs when they are of interest. The chief text used was "Galois Groups and Fundamental Groups" by Tamas Szàmuely [13]. The outline here follows his almost exactly save for necessary details filled in from other sources and examples as well as results from particular exercises and diagrams completed or constructed by the myself during the duration of my study and, of course, many omissions. General references for algebra were [8] and [2], for algebraic topology [7], for commutative algebra [1] as well as the geometric interpretations given in [3], for sheaves and schemes [6], for Riemann surfaces [4] and [11] and for category theory, limits and colimits [9] and [12].

2. Preliminary Notions

The following is an ensemble of preliminary notions that will appear in various settings throughout the paper

2.1. **Commutative Algebra.**

This paper supposes a number of results from introductory commutative algebra, such as can be found in [1]. We record results significant to this paper below. However, many important details are omitted. We of course suppose all rings are commutative and unitary. The importance of each statement will eventually be made apparent.

2.1.1. *Facts and Definitions.*

1. *Localization*: Let A be a ring. A subset S of a ring is called *multiplicatively closed* if for all $s, t \in S$ $st \in S$ and it contains the identity element. We denote by $S^{-1}A$ the *localization of* A *with respect to* S, the set of equivalence classes (a, s) with $a \in A$ and $s \in S$ such that (a, s) (b, t) if there is a $r \in S$ such that $r(ta - sb) = 0$. There is a natural map, which we will denote by s from A to $S^{-1}A$ given by $a \to (a, 1)$ The localization satisfies the following universal property. If $\phi : A \to B$ is a ring homomorphism, and S a multiplicatively closed subset such that $\phi(s)$ is a unit for all $s \in S$, then there is a unique ring homomorphism $S^{-1}\phi : S^{-1}A \to B$ such that $\phi = S^{-1}\phi \circ s$. When A is a domain and $S = A - \{0\}$, S^{-1} is the *field of fractions.*

If $f \in A$ and $S =< f >$, we denote the localization by A_f. If $p \subset A$ is a prime ideal, $S = A - p$ is mult. closed and the localization is denoted by A_p. It is a local ring[1] given by the image of p and it's prime ideals are in one-to-one correspondence with those of A contained in p. The quotient of A_p by it's maximal ideal is called the *residue field at* p.

2. *Integrality*: Let $A \subset B$ be rings. An element $b \in B$ is called *integral* over A if it is a root of some polynomial with coefficients in A. B is said to be *integral* over A if every element of B is integral over A. One can show that the sum and product of two integral elements is again integral, thus we may consider the ring generated by A and all the elements integral over A. This is called the *integral closure of* A *in* B. If the integral closure in B is equal to A, A is said to be *integrally closed in* B A domain is said to be *integrally closed* if it is integrally closed in it's field of fractions. There are important correspondences between the prime (maximal) ideals in a ring and those of a ring integral over it. In the following we suppose $A \subset B$ with B integral over A. We denote prime ideals of A by p and those of B by q. q is said to *contract* to p if $q \cap A = p$, and p is said to *extend* to q if the ideal generated by p in B is equal to q.

3. *Primary Decomposition*[1, Chapter 4]: This is a generalization of factorization. An ideal q is called *primary* if for all $ab \in q$, either $a \in q$ or $b^n \in q$ for some n. This is equivalent to the *radical*, $r(q)$ of q, the set of all elements with a power contained in q, being prime. $p = r(q)$ is called the prime associated to q and q is called $p - primary$. An ideal α is said to be *decomposable* if it can be written as an intersection of finitely many primary ideals, with the ideals in the intersection called the *primary ideals assoiated to* α.

Proposition 2.1. *The contraction of every prime ideal in* B *is prime in* A. *If* q *is maximal, so is its contraction. Conversely, if* B *is integral over* A, *for* p *prime in* A, *there exists a prime ideal* q *in* B *contracting to* p, *which is maximal iff* p *is.*

This, and many other important statements relating a the prime ideals of a ring to those of in integral extension are essentially corollaries of Nakayama's Lemma, below.

2.1.2. *Some important lemmas and theorems.*

The following goes by the name of *Nakayama's Lemma*, which can be viewed as a generalization of the Cayley-Hamilton theorem, as pointed out in [1]. It is

[1] has a unique maximal ideal

useful in the study of local rings, which are themselves quite important in study of schemes[23].

Lemma 2.2. *Let $a \subset A$ be an ideal contained in the Jacobson radical of A, the intersection of all maximal ideals of A. If M is a finitely-generated A-module with $aM = 0$, then $M = 0$.*

The following is a very important theorem of Noether that allows one to define the *transcendental dimension* of a finitely-generated k-algebra for a given field k.

Theorem 2.3. *Let K be a finitely-generated k-algebra. If $(x_1, ..., x_n)$ denote the generators, up to reordering there exists a unique $0 \leq r \leq n$ such that K is integral over $k[x_1, ..., x_r]$. One defines r to be the transcendental dimension of K.*

Proof. See [1, Exercise 5.16]. □

We will also need a few facts concerning primary decomposition.

Definition 2.4. A ring is called *Noetherian* is every ascending chain of prime ideals stabilizes after finitely many steps.

Theorem 2.5. *Every ideal in a Noetherian ring has a primary decomposition.*

If there is a maximal length for the ascending ideals in a ring, one calls this length the dimension of the ring. Noetherian domains of dimension 1 are called *Dedekind*. A local Dedekind domain is called a *discretevaluationdomain*.

Now, recall that the intersection of two ideals is equal to their product iff they are relatively prime. Since every prime ideal of a Dedekind domain is maximal and distinct maximal ideals are relatively prime, and thus so are primary ideals belonging to distinct primes. One finds, in fact, that the primary ideals is a Dedekind domain are in fact powers of its prime ideals. Putting this all together, we have:

Corollary 2.6. *In a Dedekind domain every ideal can be uniquely written as a product of powers of prime ideals.*

This will prove fundamental in the discussion of proper normal curves.

2.1.3. *Prime Spectra .* Prime spectra will prove to be essential to the definition of schemes later in the paper. Their importance cannot be overstated. The exercises in [1] provide an excellent introduction to their properties and uses.

Definition 2.7. Let A be a ring. One considers the set of prime ideals, $Spec(A)$ of A and endows it with a topology whose closed sets are given by the set of prime ideals containing (the ideal generated by) a given subset in A, denoted by $V(I)$ with I a subset in A. One can show easily that these sets satisfy the axioms required of the closed sets of a topology, the *Zariski topology.* If $f \in A$, one denotes by $D(f)$ the compliment of $V(f)$. These sets form a basis for the Zariski topology. One verifies that $D(1) = Spec(A)$, $D(0) = \varnothing$ and that if (0) is prime, meaning A is integral, then every open set contains (0). In this case, (0) is called the *generic point* of $Spec(A)$. One can show that $Spec(A)$ is in fact quasi-compact, but Hausdorff iff it is totally disconnected, i.e. every prime ideal is maximal.

---

[2]Our stalks will always be local rings.

[3]Many properties, called local properties, held by the localization of a ring are shared by the ring itself [1, Chapter 3] ex. Flatness and projectivity. A sequence $0 \to M' \to M'' \to 0$ is exact iff the localized version is.

Given any ring homomorphism $A \to B$, the inverse image of any prime ideal is itself prime, and one attains an induced map $Spec(B) \to Spec(A)$. One can show that $Spec()$ is actually a contravariant functor.

2.2. **Category Theory.** Admittedly, one can easily be lost in the abstract nonsense ubiquitous in the theory of categories. However, one cannot ignore it's value as a universal language for drawing parallels between varying domains in mathematics nor the value in the mentality of not always considering mathematical objects with certain structure preserving relations between them, not to mention the guidance one gains in a new domain in comparing with understood categories, their properties, and which ones of those one would like to isolate or preserve in some new category. The usage in this memoire doesn't go far beyond the bare basics, which shall presented here, supposing the definition of category, objects, morphisms and functors as known and ignoring all notions of universes, "smallness" etc., except to say that all the categories with which we concern ourselves here are nice in the sense that the collection of morphisms between any two objects will be a set in the proper sense of the word.

Let $\mathcal{C}$ and $\mathcal{D}$ be two categories and $\mathcal{F}$ be a functor from $\mathcal{C} \to \mathcal{D}$. $\mathcal{F}$ is called *faithful* of the associated map $\mathrm{Hom}(\mathcal{F}(X), \mathcal{F}(Y)) \to \mathrm{Hom}(X, Y)$ is injective, *fully faithful* if it is bijective and an isomorphism if it is fully faithful and $\mathcal{F}$ yields a 1-1 correspondence between the objects of $\mathcal{C}$ and $\mathcal{D}$. This is in fact a rather constrictive notion and we prefer to look at functors that induce an *equivalance of categories* i.e. $\mathcal{F}$ is fully faithful and *essentially surjective*, meaning that every object in $\mathcal{D}$ is *isomorphic* to an object $\mathcal{F}(X)$ for some X.

$\mathcal{F}$ is called an *anti-isomorphism* if it is an isomorphism to the category $\mathcal{D}^{op}$ the *opposite category*, with the definition of *anti-equivalence* being an obvious generalization.

It will also be important to consider morphisms of functors $\Theta\mathcal{F} \to \mathcal{G}$ where $\mathcal{F}$ and $\mathcal{G}$ are functors between the same categories $\mathcal{C} \to \mathcal{D}$. Θ is given by a family of morphisms, one for every object in $\mathcal{C}$ such that all:

$$\begin{array}{ccc} \mathcal{F}(X) & \xrightarrow{\Theta_X} & \mathcal{G}(X) \\ {\scriptstyle \mathcal{F}(f)}\downarrow & & \downarrow{\scriptstyle \mathcal{G}(f)} \\ \mathcal{F}(Y) & \xrightarrow[\Theta_Y]{} & \mathcal{G}(Y) \end{array}$$

An essential definition for the length of this paper has to do with functors from either $\mathcal{C}$ or $\mathcal{C}^{op}$ to **Set**. In the first case, we call a covariant functor $\mathcal{F}$ *representable* if it as isomorphic, i.e. by an isomorphism in the category of functors from $\mathcal{C}$ to **Set** wherein morphisms are given by *natural transformations* [9], to the a functor $\mathrm{Hom}(X, \_)$ for some object X in $\mathcal{C}$. Such an X is called a *representation* of $\mathcal{F}$. The contravariant case is identical, replacing $\mathrm{Hom}(X, \_)$ with $\mathrm{Hom}(\_, X)$.

We now have all that is necessary to define limits and colimits, which will play a central role in the following presentation.

2.3. **Limits and Colimits.** The general categorical definition of a limit or colimit is very abstract, which is to be expected given that the concepts generalize a variety of very different looking objects. One may think of unions, disjoint unions, intersections, kernel, equalizers, direct product, direct sums, cokernels, fibre products, tensor products etc. as specific examples. For this paper we will be mainly concerned with inverse limits of directed systems of finite groups, fibre products of topological spaces, fibre products of schemes over a certain base scheme and stalks of sheaves, all to be defined below. For general discussion on limits see [9] and [12]. A useful way to look at these objects and see how they are all instances of the same thing is by thinking of limits (when they exist) as certain objects through which maps between an object and a certain *diagram* (defined below) functor.

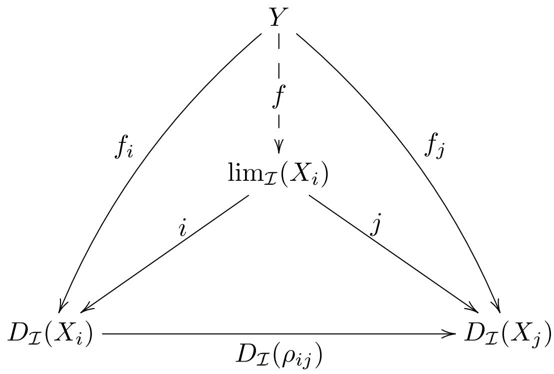
Definition 2.8. A *diagram* in $\mathcal{C}$ is a functor $\mathcal{D}_{\mathcal{I}}$ from a given category $\mathcal{I}$ whose objects form a set.

Examples 2.9.

1. If $\mathcal{I} = *$, a one-point set, then a diagram is just a choice of object in $\mathcal{C}$. In general, if $\mathcal{I}$ is any *discrete category* (no morphisms), then a diagram is a set of objects in $\mathcal{C}$.
2. If $\mathcal{I} = i \to j$, a diagram is of the form $X \to Y$ with X, Y in $\mathcal{C}$. In general, a connected, oriented graph with vertices thought of objects and edges thought of as morphisms yields a corresponding diagram by replacing vertices with objects of $\mathcal{C}$ and edges with morphisms in $\mathcal{C}$.
3. Any other example can be thought of as a disjoint union of the above two examples, intuitively "connected components" of a diagram.
4. $\mathcal{I}$ is called *directed* if it can be given a partial ordering $\leq$, given by $i \leq j$ iff there is a morphism going from i to j, such that for all $i, j \in \mathcal{I}\ \exists k \in \mathcal{I}\ st\ i \leq k, j \leq k$.

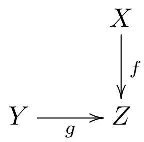
Remark: One should keep in mind that in any given category, every object is at least attached to the identity morphism and, since a functor take the identity morphisms to identity morphisms, every vertex in the diagram has a "loop" corresponding to the identity.

With this in mind, one my think of a limit as an object, denoted $\lim_{\mathcal{I}}(X_i)_{i\in\mathcal{I}}$, such that given an object Y and a set of morphisms $f_i : Y \to X_i$, one for each $i \in \mathcal{I}$ such that the diagram resulting from adding Y and all the f_i is commutative. We call this a *cone* over the diagram. One may also think of a cone a natural transformation from the "diagonal" diagram to $\mathcal{D}_{\mathcal{I}}$ [9]. Then, if $\lim_{\mathcal{I}}(X_i)_{i\in\mathcal{I}}$ exists, there is a unique $f : Y \to \lim_{\mathcal{I}}(X_i)_{i\in\mathcal{I}}$ with morphisms $i : \lim_{\mathcal{I}}(X_i)_{i\in\mathcal{I}} \to X_i$ such that $f_i = i \circ f$. These i are naturally associated to the limit and don't depend on Y. Such objects don't always exist and it's not immediately clear how the i are defined. In **Set** one can always define such objects and the general existence comes down to the representability of a certain set-valued functor. This is reflected in the statement that the limit is the final object in the category of cones over our given diagram. This can be seen pictorially as:

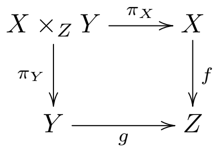


The colimit case is exactly dual to this, namely the colimit is an *initial object* in the category of cones pointing *towards* Y, also called a *cocone* over the diagram. With this in mind, we give the general definition of limit, first in **Set**, then in the general case.

Definitions 2.10. 1. *Limits in Set*: We define first the notion of *fibre products* in the category of sets. Suppose we are given the situation in the diagram below.



We define the fibre product , denoted $X \times_Z Y$ as the subset of $X \times Y$ such that $f(x) = g(y)$. Pictorially, we have:



Here π_X and π_Y are the restriction of the standard projection maps from the product. Clearly, we can preform the exact same construction over any diagram as a subset of $\amalg_{i\in\mathcal{I}} X_i$ in an identical manner. This is called the *limit* (or projective or inverse limit) of the X_i and is often denoted $\varprojlim(X_i)$. There are several things to note. Firstly, we don't necessarily have that given X_i and X_j there will be a common target space in which to compare their image. One takes $\mathcal{I}$-tuples $(x_i)_{i\in\mathcal{I}}$ s.t. whenever one has $f_i : X_i \to X_k$ and $f_j : X_j \to X_k$, bearing in mind identity morphisms, one has $x_k = f_i(x_i) = f_j(x_j)$. Secondly, note that had we started with a discrete diagram, the limit would've been the ordinary product. With this in mind, one may think of the limit as the disjoint union of the limits of the "connected components" of the diagram. This limit comes with natural "projections" to the X_i just as in the case of the fibre product.

Dually, given a diagram:

$$\begin{array}{ccc} Z & \xrightarrow{f} & X \\ {\scriptstyle g}\downarrow & & \\ Y & & \end{array}$$

we define the amalgamated sum $X \wedge_Z Y$ as $X \amalg Y$ quotiented identifying $f(z)$ with $g(z)$ for all $z \in Z$, which will be the *colimit* (or direct or inductive limit) of the above diagram. As in the case of limits, the general definition over set is a logical generalization of this, namely we start with $\amalg X_i$ and identify points who share a preimage. As in the remark following the definition of a limit, the spaces are not necessarily comparable, which comes down to the statement that the relation $x_i \ x_j$ iff $\exists \ x_k \in X_k$ and morphisms in the diagram sending x_k to x_i an x_j is not in general an equivalence relation, though it is clearly symmetric and reflexive. One takes the *equivalence relation generated by the above relation.* Note that this has general injections given by the standard injections into the disjoint union, followed by the quotient map. One may denote the limit $\varinjlim(X_i)$.

Note that the condition that the diagram be *directed* is exactly that which allows us to compare any two elements in the $\mathcal{I}$-tuples is the case of limits and makes the relation stated above an equivalence relation (in this case a directed diagram comes from a *contravariant* functor) in the case of colimits.

2. *The general case*: Now let $\mathcal{C}$ be an arbitrary category. Given a diagram as above, we may consider the set valued functors $X \to \varprojlim(\mathrm{Hom}(X, X_i))$ and $X \to \varprojlim(\mathrm{Hom}(X_i, X))$ where X is an object in $\mathcal{C}$. In the first case, if the functor is representable, we denote the representative $\varprojlim(X_i)$, the projective limit, and, in the second case, $\varinjlim(X_i)$, the inductive limit. One may check over **Set** that the two definitions coincide.

Examples 2.11. As stated above, we care mostly about limits of directed diagrams, also known as *directed systems.*

1. For sufficiently algebraic objects (rings, modules, groups), or generally belonging to what one calls an *Abelian Category*, limits and colimits are relatively easy to describe. We give some examples for modules over a commutative, unitary ring A.

a) Let M and N be A-modules. Consider the diagram:

$$\begin{array}{ccc} A & \xrightarrow{f} & M \\ {\scriptstyle g}\downarrow & & \\ N & & \end{array}$$

Where $f(a) = a \cdot 1_M$ and $g(a) = a \cdot 1_N$. Then the inductive limit is given exactly by $M \otimes_A N$.

b) Let (M_i, ρ_{ij}) be a (co)directed diagram. Then the inductive limit is the direct sum of the M_i quotiented by $m_i \ m_j$ iff they share a preimage in some (and therefore all) X_k where $i, j \leq k$.

c) Let (M_i, ρ_{ij}) be a directed diagram. The inverse limit is just the subset of the direct product given by $\mathcal{I}$-tuples s.t. $\rho_{ik}(x_i) = \rho_{jk}(x_j) = x_k$ for $i, j \leq k$.

d) The situations for groups, rings, fields etc. are all analogous. For discrete diagrams, the inverse limit is just the direct sum and the direct limit is just the direct sum.

2. Let X be a topological space and consider the direct system corresponding to its open sets, ordered by inclusion. In this case, $(U_{i,ij})$ admits *finite projective limits* in the form of intersections, but does not in general admit infinite projective limits. However, one has infinite direct limits, namely unions.

3. Suppose now that we are in the category of topological groups. Let (G_i, ρ_{ij}) be a directed system of *finite* groups given the discrete topology. Then $\varprojlim(G_i)$ is a class of topological group known as a *profinite* group. It is a closed subgroup of $\prod G_i$ such that $\rho_{ik}(x_i) = \rho_{jk}(x_j) = x_k$ for $i, j \leq k$. By Tychonoff's theorem, the product, and therefore any closed subgroup, is compact. Furthermore, one can show that the limit is *totally disconnected*, the only connected subsets are singletons. A typical example is $\mathbb{Z}_p$, the *p-adic integers*. Such groups will play a very important role in what follows. A particular example comes from taking all subgroups G_i of finite-index of a given group G and creating a direct system out of the finite quotient groups and natural projections. The resulting limit is called the *profinite completion* of G and is typically denoted $\hat{G}$. Such groups will be fundamental in what follows.

2.4. **Presheaves and Sheaves .**

Definition 2.12. Let X be a topological spaces. A *presheaf of sets* $\mathcal{F}$ on X associates to each nonempty open subset $U \subset X$ a set $\mathcal{F}(U)$ and for each inclusion of open sets $V \subset U$ a "restriction" map $\rho_{UV} : \mathcal{F}(U) \to \mathcal{F}(V)$ such that the maps ρ_{UU} are identity maps and satisfying the identity $\rho_{UW} = \rho_{VW} \circ \rho_{UV}$ when $W \subset V \subset U$ The elements of $\mathcal{F}(U)$ are called *sections* of $\mathcal{F}$ over U. Sections over the whole space are called *global sections*.

Presheaves are very general objects that appear in many domains in mathematics. One can similarly define *presheaves of groups* in which every element of $\mathcal{F}(U)$ is additionally a group and the ρ_{UV} are group homomorphisms.

In the language of Category Theory, we may take as a category X_{Top} associated to a topological space X with objects being the nonempty open subsets of X and morphisms being defined by natural inclusions [4]. Then a *presheaf* of sets (groups, abelian groups etc.) is a set (group, abelian group...)-valued, contravariant functor on the category X_{Top}[5].

In this way the presheaves of a certain type associated to X themselves form a category with morphisms being morphisms of contravariant functors.[6]

By their definition, one can see that (pre)sheaves are tailored to make local statements easy. Typically one formulates the question of what local properties are preserved globally to the study of global sections. Oftentimes, however, we are more interested in local analysis. Let $x \in X$ and let $\mathcal{F}$ be a sheaf on X. Then if we consider only the $\mathcal{F}(U)$ with $x \in U$. We may order the neighborhoods of x in X by reverse inclusion i.e. $U \leq V$ iff $V \subset U$. We then have a directed set indexed

[4] Note that there are no parallel morphisms.

[5] Of interest is the fact that in this category limits are given by unions and colimits are given by intersections. In particular X_{Top} admits finite colimits and arbitrary limits.

[6] Alternatively, a morphism of presheaves is a family of maps, one for each open set in X, that commute with the restriction maps.

by the neighborhoods of x since if U and V are both neighborhoods of x, then $U, V \leq U \cap V$. For $U \leq V$ we have maps $\rho_{UV} : \mathcal{F} \to \mathcal{V}$ defined by the restriction maps, equal to the identity when $U = V$. Thus we may consider the direct limit of this direct system.

Definition 2.13. The direct limit defined above is called the *the stalk of $\mathcal{F}$ at x* and is denoted $\mathcal{F}_x$.

Examples 2.14. Sheaves are designed to make local statements easy, so it's not surprising that one finds many examples for objects that one tends to study locally. 1. *Vector Fields on a Smooth Manifold*: Let M be a manifold. One defines the *presheaf of smooth vector fields* by $T(U) = smoothvectorfields$, i.e. the tangent bundle over U. Clearly $T(M)$ is the tangent bundle of M and global sections are exactly smooth vector fields. The stalk at a point is none other than the tangent space at that point. 2. Let A be a ring. There is a naturally defined presheaf of rings associated to $Spec(A)$. We give the definition, keeping in mind that it is enough to define a presheaf over basis sets.

Definition 2.15. The *structure sheaf* of $Spec(A)$ is defined by $\mathcal{O}_{Spec(A)}(D(f)) = A_f$, the localization at f. Since $D(f) \cap D(g) = D(fg)$, one has well-defined restriction maps induced by corresponding ring homomorphisms. For a given $p \in A$, one finds the stalk of the structure sheaf is given by none-other than the local ring A_p.

Definition 2.16. A prime-spectrum combined with it's structure sheaf is called an *affine scheme*.

The examples above share a particular property that will be generalized in the following definition:

Definition 2.17. A presheaf $\mathcal{F}$ is a *sheaf* if it satisfies the following:

1. Given a non-empty open set U and an open covering $\{U_i : i \in I\}$ of U by nonempty sets, if two sections $s, t \in \mathcal{F}(U)$ agree on every U_i i.e. $\rho_{UU_i}(s) = \rho_{UU_i}(t) \forall U_i$ then $s = t$.

2. For an open covering of U like the one above, if there exist sections s_i on each U_i such that $s_i = s_j$ on $U_i \cap U_j$ whenever the intersection is not empty, then there exists a section s on U such that $s = s_i$ on each U_i

Remark 2.18. Intuitively, sheaves are just presheaves that satisfy nice properties i.e. sections agreeing on intersections can be glued to form sections of the union and the glueing is unique.

The collections of sheaves on a space X also form a category by taking the full subcategory whose objects are sheaves of the category of presheaves. The morphisms automatically respect sheaf structure since they were originally supposed to commute with restriction maps.

3. Galois Theory

When Grothendieck formalized the theory of schemes and étale coverings, he demonstrated, as we will see, that the étale fundamental group is a generalization of the absolute Galois group of a field (defined below). Later we will see very specifically how Galois theory and coverings intersect as morphisms of a certain "fibre" functor to finite sets, an understanding that was already very concrete in Galois theory and permutations of the roots the minimal polynomial of a generator of a Galois extension over the base field, and in the domain of the fundamental group and the corresponding monodromy action on the fibres. We assume full knowledge of the Galois theory of finite, Galois extensions, which can be found an any standard textbook on Abstract Algebra, see [2], for example. We cite here, without proof, the most important results for our purposes, and then give the generalization to infinite, Galois extensions, which will be fundamental in the later portions of the paper. For the following we will denote by K our base field and denote field extensions by $L|K$.

3.1. **Galois Theory of Finite Field Extensions.**

Facts

1. Every finite algebraic extension of K is a *simple* extension, i.e. equal to $K(\alpha)$ for some α algebraic over K.

2. Every irreducible polynomial over a perfect or finite field is separable. If $P \in K[X]$ splits, factors into linear factors, over some field L, then every polynomial in K with a root in L splits in L. Such an L is called a *splitting field* or *decomposition field* for P. A field finite extension $L|K$ is called *separable* if the minimal polynomial of the generating element is separable iff the minimal polynomial of every element of L over K is separable.

3. Let $L|K$ be a finite, algebraic extension. The following are equivalent:

a) L is Galois

b) L is separable and the splitting field of the minimal polynomial m_α of it's generating element

c) The fixed field of the group of field automorphisms of L is exactly equal to K. In this case one denotes the group of automorphisms by $\mathrm{Gal}(L|K)$ and calls it the *Galois group* of $L|K$. One should note that such an automorphism permutes the roots of m_α and is in fact uniquely determined by it's action on the roots. Moreover, this is true for general automorphisms of an algebraic extensions of K, but the action is transitive iff the extension is Galois. Moreover, the order of $\mathrm{Gal}(L|K)$ is exactly the degree of the field extension.

Theorem 3.1 (Fundamental Theorem of Galois Theory)**.** *Let $L|K$ be a finite, Galois field extension. There is a one-to-one contravariant correspondence between subgroups of $G = \mathrm{Gal}(L|K)$ and finite, algebraic extensions of K contained in L. Namely, if $H \leq G$ then the set of elements fixed by H, denoted L^H is a finite algebraic extension of K contained in L of degree $[G : H]$, $L|L^H$ is Galois with Galois group equal to H. $L^H|K$ is Galois iff H is normal is G, with Galois group isomorphic to G/H*

Remark 3.2. This last follows exactly from the fact that H is the kernel of the natural map from $\mathrm{Gal}(L|K) \to \mathrm{Gal}(L^H|K)$ obtained by restriction. Such a map can be attained to the automorphism group of any subextension over K and is *always* surjective by the theory of extending field morphisms.

3.2. **Infinite Galois Theory.**

The generalization of Galois theory to infinite field extensions is very similar, and can also be found in most foundational textbooks on the subject. Here limits and topology will come into play, and we will see that the analogue of the Fundamental Theorem will take on a very similar form with the exception that the fixed fields corresponding to *closed* subgroups of our Galois group will be those corresponding to field extensions of our base field, which we still denote by K.

First, we should observe that the characterization of a Galois extension as the splitting field for an irreducible, separable polynomial is no longer valid as we are no longer dealing with simple extensions. We can still, however, define Galois extensions as those separable, algebraic field extensions whose groups of field automorphisms over K has fixed field exactly equal to K.

As we see in the case of finite extensions, given a Galois extension, we have all the information of the extensions it contains. With this in mind, we begin by characterizing the Galois group of the *separable closure* of K, denoted K_s, which is simply the composite field of all separable extensions of K. Note that by definition, this must be contain every Galois extension of K. Clearly, K_s is an algebraic closure iff K is perfect. K_s is in fact itself a Galois extension of K. Indeed, if α is a separable element over K, not contained in K, then there exists a finite Galois extension, L containing α and an automorphism over K taking α to one of the other roots of it's minimal polynomial. By the theory of field extensions, we may extend this automorphism to $K_s|K$.

Now, in a manner similar to 3.2, we expect to obtain the Galois groups of finite subextensions of K as the normal subgroups of finite index in $\mathrm{Gal}(K_s|K)$. This is the case and works exactly as in 3.2.

In 2.11 we gave an example of a topological group given by a limit of finite groups endowed with the discrete topology, itself endowed with a generally non-trivial topology whose basic open sets, where exactly inverse images of the projection maps onto each of the finite components, and in particular we stated how one can attain such a group starting from any arbitrary group in taking the *profinite completion*. Are goal is to show that $\mathrm{Gal}(K_s|K)$ is such a group, equal to it's profinite completion, bearing in mind the above fact that normal subgroups of finite index are exactly the Galois groups of finite, Galois subextensions.

Proposition 3.3. *The Galois group $G = \mathrm{Gal}(K_s|K)$ is isomorphic to the inverse limit, $\varprojlim(G_i)$ of the direct system (G_i, ρ_{ij}) formed by the Galois groups of all finite, Galois subextensions of K_s and the natural projections induced by projection of groups/inclusion of fields.*

Remark 3.4. The above discussion shows that this is exactly the profinite completion

Proof. We easily attain a map from $G \to \varprojlim(G_i)$ by constructing the natural map from $G \to \prod G_i$ obtained by restriction an element $\sigma \in G$ to the subfield defined by G_i, denoted by σ_i. Now $(\sigma_i)_{i\in\mathcal{I}}$ clearly defines an element of the limit. Since, by the theory of field extensions, an automorphism of some field extends *uniquely* to a given field containing it, it's not hard to see that any element of the limit defines an element of G by extending all the way to K_s, giving surjectivity, while the uniqueness of such extensions gives injectivity, since if $\sigma \neq \tau \in G$ then there is an $\alpha \in K_s$ such that $\sigma(\alpha) \neq \tau(\alpha)$. Since α is contained in some finite, Galois extension, we conclude. □

Examples 3.5.

1. Let p be a prime number and consider the extension $\mathbb{Q}_p$ denote the extension attained from $\mathbb{Q}$ by adjoining all p^n roots of unity for all $n \in \mathbb{N}$. Denote by μ_n a primitive p^n-th root of unity. Then $\mathrm{Gal}(\mathbb{Q}(\mu_n|\mathbb{Q})$ is isomorphic to $\varprojlim(\mathbb{Z}/p^r\mathbb{Z})^\times = (\mathbb{Z}_p)^\times$, the groups of units of $\mathbb{Z}_p$, the p-adic integers.

2. Let $\mathbb{F}$ be a finite field. Then every finite field extension of $\mathbb{F}$ is essentially unique with cyclic Galois group whose order is equal to the degree of the extension on $\text{Gal}(\mathbb{F}_s|\mathbb{F}) \simeq \hat{\mathbb{Z}}$, the profinite completion.

We thus endow G with natural limit topology, which in this case is known as the *Krull* topology. We've seen now that the *finite* field extensions appear very naturally as fixed fields of finite index, resulting easily from what's known in the Galois theory of finite extensions. The gap that remains is in identifying subgroups corresponding to infinite field extensions and describing which among them is Galois. This is the content of *Krull's Theorem*, which we state here.

Theorem 3.6 (Krull)**.** *Let L be a possibly infinite Galois extension of K. There is an anti-isomorphism of categories between subextensions of K with inclusion and closed subgroups of $G = \text{Gal}(L|K)$ given by fixed fields on one hand and automorphism groups over K on the other. The degree of the corresponding extensions is given by the index of the subgroup in G. Galois subextensions correspond to normal subgroups.*

Remarks 3.7. We provide a non-detailed discussion and refer the reader to [13, Thm. 1.3.11] for a more detailed proof. It's clear that when L is finite, this exactly the content of 3.1. We already showed that the Galois groups of finite, Galois extensions correspond to the basic open sets, and since open subgroups, being the complement of the union of their disjoint,open cosets, are automatically closed in a topological group, the case for finite, Galois subextensions is already done, and the case for an arbitrary finite extension F is handled by first embedding the extension in a Galois extension M, taking the inverse image of $\text{Gal}(M|F) \leq \text{Gal}(M|K)$ by the natural projection from the limit, and showing this it's open and equal to $\text{Gal}(L|F)$.

For the infinite case, we observe that F is the composite of the finite extensions it contains and thus $\text{Gal}(L|F)$ is the intersection of the open subgroups corresponding to these finite subextensions.

Conversely, given an arbitrary closed subgroup, $H \leq G$, we take the fixed field L^H. We may take any basic open set of the identity in $\text{Gal}(L|L^H)$, denoted by U_M, which corresponds to a finite, Galois subextension M, we have H surjects onto $\text{Gal}(M|L^H)$ by finite Galois theory and the fact that H moves every element in M not contained in L^H. Now, if $\sigma \in \text{Gal}(L|L^H)$, we project to $\text{Gal}(M|L^H)$ and find that $\bar{\sigma} = \bar{h}$ for some $h \in H$. Therefore σU_L is contained in H. Since we can take U_M arbitrarily small, σ must be in the closure of H.

3.3. **Grothendieck's Formulation of Galois Theory.** We arrive now at a slight reformulation of the above whose significance will not be readily apparent until later. Fixing a base field k, we may consider the category of finite, algebraic extensions over k and the field morphisms between them. Since each of these extensions is simple, we may define a functor, denoted Fib_k to **Set** taking a field extension L to the set of roots of the minimal polynomial of a generator, which we will call *fibres*. This set has a natural, transitive, left $\text{Gal}(k_s|k)$ action since there always exists are field automorphism from L to k_s taking one root to another. Note that we can identify this set with $\text{Hom}(L, k_s)$ with $\text{Gal}(k_s|k)$ acting by left composition, and that morphisms of fields induce morphisms of fibres in the opposite direction. One sees easily that morphisms of fibres are compatible with the group action, so that Fib_k is actually a *G-equivariant* functor. The Galois action is in fact *continuous* in the following sense:

Definition 3.8. An action of a topological group on a topological space is *continuous* if the map $G \times X \to X$ is continuous. If X is discrete, this is equivalent to the stabilizer of any point being open [13, ??].

If X is a finite set of roots described above and $\alpha \in X$, then the stabilizer $G_\alpha \leq G$ is exactly the subgroup fixing $k(\alpha)$, so our action is indeed continuous. We thus see that the extension is Galois iff the stabilizer is normal.

Conversely, given a finite set X with a continuous, transitive, left $\mathrm{Gal}(k_s|k)$ action, we may associate a field extension by taking the stabilizer of a given point, which will have finite index by the orbit-stabilizer theorem. The corresponding field extension will have X as its fibre with the orginial $\mathrm{Gal}(k_s|k)$-action.

We introduce one more object, which will also become very important despite the simplicity of its definition.

Definition 3.9. An *étale k-algebra* is a k-algebra isomorphic to a finite direct sum of separable, algebraic extensions of k.

Because it will be important later, we explicitly demonstrate the structure of the tensor product of two finite, algebraic extensions of k.

Proposition 3.10. *If L_1 and L_2 are two finite, separable, algebraic extensions of k, then $L_1 \otimes_k L_2$ is an étale k-algebra.*

Proof. We have $L_1 \simeq k[x]/(x-a_1)...(x-a_2) \simeq k(a_i)$ for some i. where $\prod(x-a_i)$ is irreducible. Then:
(3.11)

$$L_1 \otimes_k L_2 \simeq (k[x]/\prod(x-a_i)) \otimes L_2 \simeq L_2[x]/\prod(x-a_i) = L_2[x]\prod p_j(x) \simeq \oplus(L_2/p_j)$$

Where $p_j(x)$ are the irreducible factors of $\prod(x-a_i)$ over L_2, and the last isomorphism comes from the Chinese remainder theorem. This last is clearly an étale k-algebra. □

Remark 3.12. In particular, one of these summands contains a_i and corresponds to the composite field L_1L_2. If $L_1 \cap L_2 = k$, the tensor product is exactly equal to the composite field.

Now with the above definitions we may provide Grothendieck's reformulation of Galois theory, which will eventually be a special case of the theory of étale coverings.

Theorem 3.13 (Grothendieck's reformulation of Galois Theory)**.** *There is an anti-equivalence of categories between finite sets with a continuous, left* $\mathrm{Gal}(k_s|k)$*-action and étale k-algebras. In this correspondence, orbits correspond to finite, separable extensions of k, with orbits having normal stabilizers corresponding to Galois extensions.*

3.4. **Inertia Groups.** We introduce one last tool combining commutative algebra and Galois theory that will be needed later: Inertia Groups

Suppose we are given an integrally closed domain A with field of fractions K. Now suppose L is a Galois extension of K and consider the group $G = \mathrm{Gal}(L|K)$. If B is the integral closure of A in L and P is a fixed maximal ideal of A, one finds that G acts transitively on $S = \{Q \in Spec(B) | Q \cap A = P\}$, the set of maximal ideals, noting that integrality of B over A implies maximality of extended ideals, in B contracting to P [1, Proposition 5.7]. This transitivity is interesting and rather useful, both in general and in defining *inertia groups* below, which will be important when we consider the meaning of "unramified" in the context of morphisms of proper normal curves. The general idea is to note that if Q_1 and Q_2 are two ideals contracting to P then if we suppose by contradiction that $\sigma(Q_1) \neq \tau(Q_2) \forall \sigma, \tau \in \mathrm{Gal}(L|K)$. We can apply the Chinese remainder theorem, using the fact that distinct maximal ideals are pairwise relatively prime to choose an element $x \in B$ such that $x \equiv 1$ modulo the product of all the ideals in the orbit of Q_1 under the Galois action and $x \equiv 0$ modulo the product of all ideals in the orbit of Q_2. Taking the norm of such an element over K gives an element of A because x is integral over A and in fact an element of P, being an element of $Q_2 \cap A$. However, x was chosen such that $x \notin \sigma(Q1) \forall \sigma$ This is a contradiction since the norm is contained in Q_1, but is written as a product of elements not in Q_1.

Let G_i denote the stabilizer of $Q_i \in S$. Since G fixes P by definition, we attain a group homomorphism from $\phi : G_i \to \mathrm{Aut}(\kappa(Q_i)|\kappa(P))$ where $\kappa(Q_i)$ and $\kappa(P)$ denote the residue fields B/Q_i and A/P respectively. By [1, Proposition 5.6], $\kappa(Q_i)$ is always algebraic over $\kappa(P)$. If it is in fact a Galois extension then ϕ is surjective and it's kernel, denoted by I_i is called the *inertial subgroup* related to Q_i.

4. Covering Spaces and The Fundamental Group

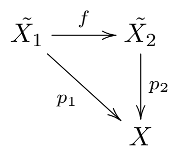
4.1. **The Classification of Covering Spaces.** The theory of covering spaces and the fundamental group is a rich and beautiful one, that we unfortunately must skip here for the most part. Rigorous treatment may be found in [7]. We cite some facts from [7], reformulated so as to more closely resemble the later results for étale coverings, where such formulations are necessary because we can no longer describe covering and fibres by inverse images of continuous maps, since points and open sets will be "attached" to algebraic information in addition to their topology. Note that we place ourselves in either **Top** or **Top$_\bullet$**, pointed topological spaces.

Definition 4.1. Let X be a topological space. A map $p : \tilde{X} \to X$ is a *covering map* if it is surjective and for all $x \in X$, there is a neighborhood U of x such that $p^{-1}(U)$ is the disjoint union of homeomorphic copies of U. $\tilde{X}$ is called a *covering space*. It is called *trivial* if we can take $U = X$. A *section*[7] is a map $s : X \to \tilde{X}$ such that $ps = id$.

Remarks 4.2.

1) A covering is called $finite$ if the pre-image of p over a trivial neighborhood U is homeomorphic to $U \times F$ with F finite, discrete. If $\tilde{X}$ is connected, F is fixed, and then if $|F| = n$, $\tilde{X}$ is called an $n-$*sheeted* covering.

2) We call a *morphism of covering spaces* a continuous map between covering spaces of a shared base space that commutes with the covering maps:



[7]It is no coincidence that the terminology overlaps with that of sheaf theory. We will see that sections in the sense of covering spaces correspond exactly to sections of a corresponding sheaf. In general, one may think of sections of a sheaf over a topological space as lifts in the topological sense to the corresponding *Etale space*.

This category admits finite products. We will denote the set of morphisms between two objects by $Hom_X(\tilde{X_1}, \tilde{X_2})$.

Note, in terms of fibre products we have that every point has a neighborhood U such that if $i : U \to X$ is the inclusion, then $\tilde{X} \times_X U$ is a disjoint union of copies of X.

Definition 4.3. The *topological fundamental group* is the group of loop classes up to base-point preserving homotopy and is denoted $\pi_1(X, x)$, where x is a specified base-point. π_1 is functorial from $\mathbf{Top_\bullet}$ to $\mathbf{Gp}$, by composing loops with maps. If f is a map in $\mathbf{Top_\bullet}$, then we denote the induced map by f_*.

Definition 4.4. A topological space is called *simply-connected* if it has trivial fundamental group. A covering space is called *universal* if it is simply-connected.

Fact. for p a covering map, p_* is injective and we may thus naturally identify the fundamental group of the covering with a subgroup of the fundamental group of the base space. Changing base-point in the covering space is equivalent to conjugating by an element in $\pi_1(X, x)$.

Definition 4.5. Let $f : Y \to X$ be a map. A $lift$ of f to $\tilde{X}$ is a map $\tilde{f} : Y \to \tilde{X}$ such that $p\tilde{f} = f$.

Note that for such a Y, the fibre product $\tilde{X} \times_X Y$ is a covering space of Y.

Fact *Unique Lifting Property*: $f : (Y, y) \to (X, x)$ has a lift to $(\tilde{X}, \tilde{x})$ iff $f_*(\pi_1(Y, y)) \subset p_*(\pi(\tilde{X}, \tilde{x}))$ iff there is a section of Y into the fibre product $\tilde{X} \times_X Y$. Such a lift is uniquely determined by the image of y in $p^{-1}(x)$, i.e. choice of $\tilde{x}$. In particular, since $[0, 1]$ is simply-connected, then every loop at x can be lifted and this lift is uniquely decided by the choice of starting point in $p^{-1}(x)$ and always lifts to a path between points in the fibre. The resulting $pi_1(X, x)$-action on the fibre p^{-1} is called the *monodromy action*.

The lifting property tells us that every element of $Aut_X(Y)$, the group of covering space automorphisms, which are merely lifts of the covering map, called the *group of deck transformations* and denoted $G(Y)$, is decided by its action on $p^{-1}(x)$. We may thus construct a functor Fib_X from the category of covering spaces over X to the category of sets with a continuous $\pi_1(X, x)$-action.

Definition 4.6. A covering is called *normal* or *Galois* when the $G(Y)$-action in $p^{-1}(x)$ is transitive.

Facts

1) If X is path-connected, locally path-connected (spaces where path-connectedness is equivalent to connectedness) and *semi-locally simply-connected*, meaning that every point is contained in a neighborhood such that every loop contained in the neighborhood is contractible *in* X, then the fibre functor described above is representable, by a Galois cover $\tilde{X}$, called the *universal cover*. It is in fact the unique, up to isomorphism, simply-connected cover of X and satisfies $G(\tilde{X}) = \pi_1(X, x)$. Connected Riemann surfaces are such spaces, so in the following theory, we restrict our attention spaces with these properties.

2) Given any subgroup $H \leq \pi_1(X, x)$, one can construct a covering space $p_H : (X^H, x_H) \to (X, x)$ such that the image of p_* is equal to H. Namely, we quotient $\tilde{X}$ by the action induced by H, seen as a subgroup of $G(\tilde{X})$. Note that such a space

is also covered by $\tilde{X}$. Moreover, if $H_1 \subset H_2$ then there is a natural covering map $X^{H_1} \to X^{H_2}$.

3) If $Y \to X$ is a morphism, than the pullback[8] of a cover, not necessarily connected, of Y. This fact won't be useful for this section, but will be in what follows.

With that, we may present the theorem of interest.

Theorem 4.7 (Classification of Covering Spaces)**.** *Let X be a path-connected, locally path-connected, semi-locally simply-connected topological space. Let $\tilde{X}$ be its universal covering. Then:*

1) There is a one-to-one, contravariant correspondence between subgroups of $G = \pi_1(X, x)$ and connected coverings of X. In this correspondence, conjugate subgroups correspond to isomorphic coverings and normal subgroups correspond to Galois coverings.

2) The group of covering automorphisms of X^H is isomorphic to $N_G(H)/H$.

See [7, Chapter 1.3] for a detailed proof.

Thus we have what, asthetically, very closely resembles the fundamental theorem of Galois theory, but applying to a group-functor on topological spaces. It shouldn't be clear why there should be any link between the theories, but we will see in the following that given a category of "topological" (the quotations to be explained later) spaces simultaneously endowed with sufficiently compatible algebraic structure, namely a field corresponding to every connected space and such that covering maps respect this structure (such that covering spaces equate to field extensions), we will make explicit the relation between the two theories. Riemann surfaces will be the first example.

4.2. **The Equivalence of Locally Constant Sheaves and Covering Spaces.**

We quickly demonstrate of handy equivalence of categories that will aid in the coming generalizations of covering spaces, in addition to creating a nice way to apply covering space theory to other problems.[9]

Definition 4.8. The sheaf defined $\mathcal{F}(U)$ being the set of all continuous functions from U to some fixed discrete space S. The terminology comes from the fact that the sections over a connected, open set in such a sheaf are exactly constant functions.

Definition 4.9. A sheaf $\mathcal{F}$ is called *locally constant* if every point $x \in X$ has an open neighborhood U such that the restriction of $\mathcal{F}$ to U is isomorphic to a constant sheaf (in the category of sheaves of U)

In particular, given a covering over X $p : Y \to X$, define a presheaf $\mathcal{F}_Y$ by letting $\mathcal{F}(U)$ for U open in X be the set of *sections*, continuous functions $s : U \to Y$ such that $p \circ s = id_u$. The restriction maps are simply restrictions of each section s from U to $V \subset U$. This is clearly locally constant by the definition of a covering space. A section is merely a lift of U to an isomorphic copy in X.

The fact that this presheaf actually defines a sheaf is an easy consequence of the fact that the sections are just locally defined continuous functions.

[8]The fibre product and the corresponding map to Y

[9]See for example the discussion in [7, Chapter 3] on Poincaré duality and the *orientation* covering space.

Definition 4.10. The sheaf $\mathcal{F}_Y$ defined above is called the *the sheaf of local sections* of X.

The more interesting statement is that given a locally-constant sheaf, we may associate a covering in a naturally way, in the sense that morphisms of shaves yield morphisms of the corresponding coverings.

We begin in the most naive way possible, by letting $X_{\mathcal{F}}$. be the disjoint union of the $\mathcal{F}_x$ and defining a preliminary covering map as $p : X_{\mathcal{F}}. \to X$ sending $\mathcal{F}_x$ to x. Now we may view the stalk as the disjoint union of $\mathcal{F}(U)$ with $x \in U$ modulo the equivalence relation $s\ t$ if either s or t is a restriction of the other. There are therefore canonical maps from $\mathcal{F}(U)$ to $X_{\mathcal{F}}$ sending each section s in $\mathcal{F}(U)$ the map $i_s : U \to X_{\mathcal{F}}$ sending s to it's image in $X_{\mathcal{F}}$. We can therefore endow $X_{\mathcal{F}}$ with the coarsest topology rendering every $i_s(U)$ open for every s and U.[10]

The two following statements are simple definition manipulations and can be viewed in [13, Chapter 2]

Proposition 4.11. *With $X_{\mathcal{F}}$ endowed with the above topology and p as defined above, if $\mathcal{F}$ is locally constant, then $X_{\mathcal{F}}$ is a covering space of X.*

Theorem 4.12. *The category of covering spaces of X is equivalent to the category of locally constant sheaves of X.*

5. Riemann Surfaces

Riemann surfaces are wonderful meeting ground of topology, algebra, analysis and differential geometry and it's perhaps not surprising that this is where we most directly see the relation between Galois theory and the topological fundamental group. In the following, we will consider *compact*, *connected* Riemann surfaces, which we define as complex manifolds of dimension 1, with morphisms being continuous functions whose local representations are holomorphic. As usual, we begin with some basic facts. See [11] or [4] for a more detailed treatment.

5.1. **Branched Coverings of Riemann Surfaces.**

Let X be a connected, compact Riemann surface.

We now demonstrate the following proposition:

Proposition 5.1. *Let $p : Y \to X$ be a connected covering. Then Y is itself a Riemann surface, naturally endowed with a complex structure such that p is holomorphic.*

Proof. Let $y \in Y$. Consider the image $x = p(y)$ in X. Let (U, ϕ) be a chart around x. By taking smaller charts if necessary, we may assume that there is an open neighborhood U of x that lifts to an isomorphic copy V in Y. Then $(V, \phi \circ p)$ define a chart. These charts form an atlas because intersections of open sets subordinate to the covering are also subordinate to the covering, where p has a local inverse and we may write $(\phi_i \circ p) \circ (\phi_j \circ p)^{-1} = (\phi_i \circ p) \circ (p^{-1} \circ \phi_j^{-1}) = \phi_i \circ \phi_j^{-1}$, which is assumed holomorphic. Thus p is represented locally by the identity, and therefore a morphism of Riemann surfaces. □

Now, a fundamental observation is that the converse is almost true.

---

[10]Note that this is done for an arbitrary presheaf, and we attain what is called the *Etale Space of a Presheaf.* One may understand the sheaf associated to a presheaf as $\bar{\mathcal{F}}(U)$ being the set of *sections* of $X_{\mathcal{F}}$ over U. See [6, Exercise 2.1.13].

Proposition 5.2. *Given X as above, and $p : Y \to X$ a non-constant holomorphic map with finite fibres*[11] *There exists a discrete, and therefore finite, set of points $S \subset X$ such that $p_{\ Y-p^{-1}(S)}$ defines a $finite$ covering-map from $Y - p^{-1}(S) \to X - S$.*

Remark 5.3. Such a covering is called a *branched covering.*

Proof. First, one can show that any holmorphic map to compact surface is automatically surjective. One may then write any non-constant holomorphic function locally as $z \to z^n$ with $n > 0$ and independent of choice of chart. Let S be the set of points where $n \neq 0$. That S is discrete follows from the theorem of isolated zeroes of holomorphic functions. Outside of these points, p is clearly a local isomorphism, and thus a covering since our spaces are Hausdorff. □

Remarks 5.4. The points of S are called *ramification points.* Their pre-images are called *branch points.*

Using the two above results, we may extend any branched covering, which is already a holomorphic map by above, $p' : Y' \to X' = X - S$ to a Riemann surface $Y \to X$. If $x \in X$ is a ramification point, one looks at a sufficiently small neighborhood U of x such that $U - x$ is holomorphic to the punctured disc D^* and lifts to biholomorphic copies, V' of itself in Y. Thus, in the local charts over $U - x$ we have a finite covering of the punctured disc, which is known to be of the form $z \to z^n$ for some $n\, 0$, where n might vary depending on the lift of $U - x$. Thus, we add abstract points to each of these lifts in Y and extend holomorphically the map,

$D^* \to V' \to U - x \to D^*$, to a map from $D \to V' \cup y \to U \to D$, sending $z \to z^n$, which is allowed by an application of Riemann's removable singularity theorem. Doing this extends the complex structure of Y' to the added points, thus rendering a compact Riemann surface Y and a holomorphism from Y to X.

5.2. **Relation to Field Theory.** We begin with some facts which are not at all trivial, but will be assumed in what follows.

1) The meromorphic functions $X \to \mathbb{C} \cup \{\infty\}$ form a field, which we will denote by $\mathcal{M}(X)$.

2) Meromorphic functions are equivalent to holomorphic functions to the Riemann Sphere, which we denote by $\mathbb{CP}_1$.

3) $\mathcal{M}(\mathbb{CP}_1) = \mathbb{C}(t)$, the field of rational functions in $\mathbb{C}$.

Our aim is to construct a functor from the category of holomorphic maps from compact surfaces to a base surface X to the category of field extensions of $\mathcal{M}(X)$. Given such a map $\phi : Y \to X$ holomorphic, with Y connected, we attain a natural map of fields $\phi^* : \mathcal{M}(X) \to \mathcal{M}(Y)$ taking $g \to g \circ \phi$. That this is functorial is clear, as is faithfulness. We of can of course identify $\mathcal{M}(X)$ with $\phi^*(\mathcal{M}(X))$. The fundamental result will be the following.

[11]It is not normally assumed that branched coverings are finite, but this will be essential in forming the correspondence with Galois theory, wherein all groups concerned are profinite. Infinite-sheeted coverings are in general not algebraic in nature. Take, for example, the simply-connected coverings of S^1 by $\mathbb{R}$ given by the exponential. This means that the fibre functor will no longer be representable.

Theorem 5.5. *Let X be a connected, compact Riemann surface and $\mathcal{M}(X)$ its field of meromorphic functions. There is an anti-equivalence of categories between branched coverings of X and finite field extensions of $\mathcal{M}(X)$.*

Lemma 5.6. *Let $Y' \to X'$ be an n-sheeted covering of X' and extend to a holomorphic map $\phi Y \to X$. Then $\mathcal{M}(Y)$ is an algebraic extension of $\phi * (\mathcal{M}(X))$ of degree n.*

Proof. Let $f \in \mathcal{M}(Y)$. By assumption, X' is covered by finitely many U_i' subordinate to the covering. Thus, over each U_i' we have n sections $\{s_{ij}\}$ with $j = 1, ..., n$. Letting $f_i j = f \circ s_{ij}$, we attain n elements of $\mathcal{M}(U_i)$[12]

By construction, provided we choose a consistent ordering of the sections over each U_i, the f_{ij} agree on intersections, and we may use the sheaf axiom to find global sections f_j, $j = 1, ..., n$, and consider the polynomial $P(T) = \prod_{j=1,...,n}(T - f_j)$. To show that the coeffecients of this polynomial extend to the branch points, one applies again Riemann's removable singlarity theorem [13, Section 3.3]. To show that f satisfies $\phi{*}(P)$, we demonstrate that evaluating the polynomial at any $y \in Y$ yields 0. Since y is in the image of s_{ij} for some (i, j),

$$f(y) - \phi^*(f_j)(y) = f(s_{ij}(\phi(y))) - f_j(\phi(y)) = 0 \tag{5.7}$$

. □

Remark 5.8. To show that the extension if exactly of degree n requires Riemann's Existence theorem, which states that if $(a_i)_{i=1,...n}$ is a sequence of distinct, complex numbers and $(y_i)_{i=1,...,n}$ a sequence of distinct points of a Riemann surface Y, then there exists $f \in \mathcal{M}(Y)$ such that $f(y_i) = a_i$ for all i. Taking a the points over an unramified fibre in a branched covering of X and choosing a function taking distinct values on the points of this fibre allows us to ensure that the roots of P are distinct.

This shows that the functor above indeed lands in the category of *algebraic* extensions of $\mathcal{M}(X)$. We now need essential surjectivity.

Lemma 5.9. *Let $L|\mathcal{M}(X)$ be a finite, algebraic extension. Then there exists a compact, Riemann surface X_L such that $\mathcal{M}(X_L) \simeq L$.*

We present the idea of the proof. For details, see [13, 3.3.8]. Let α be a primitive element of L and let F be it's minimal polynomial. By the irreducibility of F, we have $AF + BF' = 1$ for some $A, B \in \mathcal{M}(X)$. Letting S be the set of poles the coeffecients of A, B and F, then we construct a sheaf on $X' = X - S$ by letting $\mathcal{F}(U)$ be the set of holomorphic functions on U satisfying $F(f) = 0$. Or condition on S allows us to demonstrate that $\mathcal{F}$ is locally constant, thus yielding a branched covering of X, X_L'. One shows that the resulting Riemann surface, X_L is connected and finds a function on it such that $F(f) = 0$. By mapping $f \to \alpha$, we find that $\mathcal{M}(X_L) \simeq L$.

For a proof that the functor is fully faithful see [13, 3.3.9].

Putting the above results together proves the theorem.

Moreover, the functor above induced an equivalence between *Galois* branched coverings of X and Galois extensions of $\mathcal{M}(X)$. This comes from the fully faithfulness. If $Y \to X$ is a branched covering, then $\mathrm{Aut}(Y|X) \simeq \mathrm{Aut}(\mathcal{M}(Y)|\mathcal{M}(X)$.

[12]One defines the *sheaf of meromorphic functions*, $\mathcal{M}$ in a logical manner. It's global sections are, of course, the field of meromorphic functions.

With the above results from Galois theory, we attain:

Corollary 5.10. *Let X be as above. The category of compact Riemann surfaces with holomorphic map onto X is equivalent to the category of finite sets with a continuous left $Gal(\overline{\mathcal{M}(X)}|\mathcal{M}(X))$-action.*

5.3. **Relation to the Fundamental Group.** We have just seen the relation between *finite* branched coverings of X and field extensions of $\mathcal{M}(X)$. We now expect a relation between the fundamental group of the base space, and the Galois group of it's field of meromorphic functions. Indeed we have the following theorem. We expect, analogous to Galois theory, that if $X' = X - S$ for some discrete subset S, then $\pi_1\widehat{(X', x)}$ should be isomorphic to some quotient of $\mathrm{Gal}(\overline{\mathcal{M}(X)}|\mathcal{M}(X))$. Indeed we have the following theorem [13, 3.4.1].

Theorem 5.11. *Consider the composite field $K_{X'}$ of field extensions of $\mathcal{M}(X)$ coming from coverings of X' in a fixed algebraic closure $\overline{\mathcal{M}(X)}$. Then $K_{X'}|\mathcal{M}(X)$ is Galois with Galois group equal to $\pi_1\widehat{(X', x)}$.*

For this, we observe first that:

Lemma 5.12. *Every finite subextension of $K_{X'}$ comes from a surface restricting to a cover over X'.*

Proof. We first show that given subextensions L_1 and L_2 coming from covers over X', the composite field L_1L_2 also comes from a cover of X'. Denote by X_1 and X_2 the surfaces corresponding to L_1 and L_2 respectively. Since an anti-equivalence of categories takes limits to colimits and vice-versa, we find that the functor takes the fibre product $X_1 \times_X X_2$, which restricts to a cover of X', to the tensor product $L_1 \otimes_{\mathcal{M}(X)} L_2$ (2.11) . We saw in 3.10 that the tensor product is a direct sum of field extensions of $\mathcal{M}(X)$, corresponding to the connected components of the fibre product. L_1L_2 is among the summands and we have thus found a connected covering of X' corresponding to L_1L_2. This shows that we may construct a tower of field extensions corresponding to coverings of X' contained in $K_{X'}$. Now given $L = \mathcal{M}(Y)$ coming from a branched covering of X' and $L|M|\mathcal{M}(X)$. By above, $M = \mathcal{M}(Z)$ for some Riemann surface Z between Y and X. An counting argument relating the degrees of corresponding field extensions and the number of points over a point $x' \in X'$ in Z shows that Z also restricts to a branched covering over X'. □

5.11. By above, every Galois conjugate of $L \subset K_{X'}$ results from a covering space automorphism of the covering corresponding to L. Thus $K_{X'}$ is Galois. By definition, every finite quotient of $\pi_1\widehat{(X', x')}$ corresponds to a finite, branched covering of X', which by above, corresponds to a finite quotient of $\mathrm{Gal}(K_{X'}|\mathcal{M}(X))$. we thus have a 1-1, functorial correspondence between the finite quotients of the two groups. Thus the limit of the two systems is isomorphic and we conclude. □

5.4. **The Absolute Galois Group of $\mathbb{CP}_1$ and the inverse Galois problem.** We now have all the tools necessary to demonstrate that *all* finite groups are realizable as Galois groups of field extensions of $\mathbb{C}(t)$, which is the field of meromorphic functions of $\mathbb{CP}_1$ [4], using the fact that the fundamental group of S^2 minus a finite number of points is well-known.

Proposition 5.13. *Let A be a finite subset of $X = S^2$ of cardinality n. Then $\pi_1(X,x) \simeq < \gamma_1, ..., \gamma_n | \prod_{i=1,...,n} \gamma_i = 1 >$, where γ_i denotes a loop going once around $i \in A$, and no other points of A.*

Remark 5.14. This group is in fact isomorphic to the *free group on n-1 generators*, namely, send γ_i to a_i for $i < n$ and γ_n to $(a_1....a_{n-1})^{-1}$.

Theorem 5.15. *Let G be a finite group. There exists a finite, Galois extension of $\mathbb{C}(t)$ with Galois group G.*

Proof. Let $< g_1, ..., g_n | r >$ be a presentation of G. Let $X' = \mathbb{CP}_1$ with $n + 1$ points removed. Then $\pi_1\widehat{(X', x')}$ is isomorphic to $\hat{F}_n$. Since G may be written as a finite quotient of F_n, we find a normal, finite-index subgroup of $\mathrm{Gal}(K_{X'}|\mathbb{C}(t))$ whose quotient is G and thus a finite, Galois, branched covering of X'. The resulting Galois group is exactly G.[13] □

6. The Etale Fundamental Group

We've seen the compatibility of the topology and algebra of compact Riemann surfaces leads to a simple and fruitful correspondence between Galois theory and covering space theory. Now, one can show that every compact Riemann surface is isomorphic to a smooth, projective curve. Curves over arbitrary rings[14], come endowed with a natural topology resulting directly from their algebraic structure, the Zariski topology (2.1.3). For Riemann surfaces, the Zariski topology is a subtopology of the complex topology. We'll see later that the Zariski topology is insufficient for our purposes, thus leading to the construction of the étale topology and étale coverings.

Observe that, since every compact Riemann surface has morphisms to the Riemann sphere, that we were dealing with curves whose function fields were $\mathbb{C}$-algebras of transcendental dimension 1. The logical next step is to consider *proper normal curves*, which can be thought of as compactified curves over a domain with transcendental degree 1 and integrally closed local rings. We choose, however, to present the general theory followed by proper normal curves as an elucidative example.

6.1. Schemes.

Schemes are central objects in algebraic geometry and in some manner generalize all the other algebraic objects thus far presented[15]. They are topological spaces along with certain sheaves, which as we saw in many of the given examples, are locally easy to analyse, but capable of any manner of global structure. To draw an analogy with differential geometry, in which manifolds consist of pieces resembling open subsets of Euclidean space, glued pairwise along homeomorphic subsets, one can think of a scheme as glued together out of simple components isomorphic to *prime spectra of commutative rings* (2.1.3) endowed with the Zariski topology. This is done by a general process for sheaves called *glueing* [6, Exercise 1.22].

---

[13] From the above, it's easy to show that the absolute Galois group of $\mathbb{C}(t)$ is in fact $\hat{F}(\mathbb{C})$, *the free profinite group over* $\mathbb{C}$, the profinite completion of the free group with basis $\mathbb{C}$. One can see that any free profinite with an infinite basis containes every finite group.

[14] Bear in mind our convention on rings, noted in section 1

[15] More precisely every algebraic variety is almost a scheme in the sense that one attains a scheme from a variety by adding a certain number of generic points, points contained in every open set [6, Chp. 2]

Definition 6.1. A *scheme* is a topological space X endowed with a sheaf of rings, called its *structure sheaf*, denoted by $\mathcal{O}_X$, whose stalks are local rings, admitting an open-covering $\{U_i\}$ such that each U_i with the induced restriction sheaf is isomorphic, in a sense to be described below, to the spectrum of some ring. Such an open set is called an *affine open set*. We will assume that the affine coverings can always be taken to be finite.

Example 6.2.
1. It is a general property that the map of spectra induced by the natural localization map is an open immersion. Thus the affine scheme $Spec(A)$ is itself built out of smaller affine schemes given by its basic open sets.

A *morphism of schemes* $\phi : X \to Y$ will be exactly those continuous maps of the underlying topological spaces combined with a family of ring homomorphisms $\phi^\sharp : \mathcal{O}_Y(U) \to \mathcal{O}_X(\phi^{-1}(U))$ that commute with restriction maps.

We thus attain a well-defined category of schemes. We will be mostly concerned with certain sub-categories, namely schemes over a certain fixed scheme S. An important property of both is the existence of finite limits, particularly fibre products.

Definition 6.3. A *scheme over* S is a scheme X along with a morphism of schemes $\phi : X \to S$. A *morphism of schemes over* S is a morphism of schemes $\rho : X \to Y$ such that the following diagram commutes.

$$\begin{array}{ccc} X & \xrightarrow{\rho} & Y \\ & \searrow^{\phi_X} & \downarrow{\scriptstyle \phi_Y} \\ & & S \end{array}$$

We denote the set of morphisms between two objects X and Y in the category of schemes over S by $Hom_S(X, Y)$, whose elements will be called S-morphisms.

Proposition 6.4. *In the category of schemes, the set-valued functor taking values in the subset of* $Hom_S(\_, X) \times Hom_S(\_, Y)$ *taking the same value in* S *is representable i.e. one can take fibre products (2.10) of schemes over* S*. As before, we denote the fibre product by* $X \times_S Y$*.*

6.1.1. *Étale morphisms of schemes.* Etale morphisms play a central role in algebraic geometry and the theory of schemes. They are what we will use to define the scheme-theoretic analogue of covering spaces. Historically their invention goes back to the birth of étale cohomology and the eventually successful tools created in order to solve the Weil conjectures. We try to justify its usage in the following section, but for now, the reader will have to go somewhat on faith. The definitions should seem more reasonable after the discussion of proper normal curves. The condition that a morphism of schemes be étale is exactly what makes the theory a direct generalization of Galois theory. Namely, when K is a field, an étale covering of $Spec(K)$ will be exactly of the form $Spec(A)$ where A is an étale K-algebra.

Definition 6.5. *Sheaves of* $\mathcal{O}_X$*-modules*: Let (X,$\mathcal{O}_X$) be scheme. A sheaf of $\mathcal{O}_X$-modules, $\mathcal{M}$, is a sheaf of modules s.t. each $\mathcal{M}(U)$ is an $\mathcal{O}_X(U)$-module.

1. $\mathcal{M}$ is called *quasi-coherent* if there is an affine covering $\{Spec(A_i)\}$ of X and corresponding A_i-modules, M_i such that $\mathcal{M}(D(f)_i)$ is isomorphic to the $(A_i)_f$-module $(M_i)_f$, where $D(f)_i$ denotes a basic open set in $Spec(A_i)$.

2. $\mathcal{M}$ is called *coherent* if it is quasi-coherent and each M_i is a finitely generated A_i module.
3. $\mathcal{M}$ is called *locally-free* if the M_i are free A_i-modules.

Coherent sheaves are particularly nice because they satisfy certain good properties. If a stalk at a point is zero, then there is an open neighbourhood of the point where the sheaf is zero. If the stalk is free, then the sheaf is free on a neighbourhood. This allows us to check local freeness at stalks instead of points.

Proof. Suppose we have $\mathcal{M}_x = 0$ for $x \in X$. Let $U = Spec(A)$ be an affine neighbourhood of x with an A-module M corresponding to $\mathcal{M}(U)$. We want to show that $M_f = 0$ for some $f \in A$. Let $\{m_i\}_{i=1,\ldots,n}$ be generators of M over A. Since $M_p = 0$, there are $f_i \in A - p$ such that $f_i m_i = 0$. Letting $f = \prod_i f_i$ does the job.

From the fact that $M_p \simeq A_p \otimes M$ [1, Chapter 3], we determine immediately the if $\mathcal{M}_X$ is free, so are the stalks. Conversely, suppose the stalk is free. In particular, it is projective, then by [1, 3.9], so is M. As we supposed A Noetherian, projectiveness is equivalent to local freeness [1, Exercises Chp. 7].

□

Definition 6.6. A morphism $\phi : Y \to X$ is *affine* if there is an affine covering of Y, $\{Spec(A_i)\}$, such that $\phi^{-1}(U_i) = Spec(B_i)$ is affine. It is *finite* if, moreover, $\phi^*\mathcal{O}_Y$ is a finite $\mathcal{O}_X$-module. This is equivalent to saying that $\phi^*\mathcal{O}_Y$ is a coherent $\mathcal{O}_X$-module. If it is locally free, we call ϕ locally free [CONVERSE].

An important difference between the case of morphisms of topological spaces and morphisms of schemes is that the points of a scheme come with an "attached" stalk. Thus we can't define a fibre as simply the inverse image of a point. This forces us to consider a more abstract definition of a point, namely a map of schemes $p : Spec(K(p)) \to S$, where topologically we have a map from a one-point set to some point $p \in S$, where $K(p)$ is the residue field at that point.

Definition 6.7. For S a scheme and $p \in S$, let $K(p)$ denote the residue field of $(\mathcal{O}_S)_p$. We have an *inclusion* map $Spec(K(p)) \to S$ whose image is p coming from the quotient map. Now, if $X \to S$, we define the fibre over p, denoted X_p to be the fibre product $X \times_S Spec(K(p))$.

We now have all the definitions necessary for defining an étale morphism.

Definition 6.8. A morphism of schemes $X \to Y$ is étale if it is finite, locally free and if for every $p \in X$, the fibre over p is the spectrum of a $K(p)$ étale algebra.

Note that what we define here is really what is called a *finite* étale morphism. There is a non-finite version, but we don't need it here. In the literature, one usually says that a morphism is étale if it is *flat*, *smooth* and *unramified*. Loosely speaking, flatness corresponds to local freeness with smooth and unramified corresponding to étale fibres.

Flatness is the easiest to explain. In commutative algebra, one sees that a finitely generated module over a local ring is flat[16] iff it is free. One defines tensor products of $\mathcal{O}_X$-modules locally in a logical manner, creating tensor sheaf. Short exact sequences of sheaves in an Abelian category are also defined logically. One finds

[16] Tensoring with it presevers left-exactness.

that a finite morphism $\phi : X \to S$ is locally free iff $\phi^* \mathcal{O}_X$ is a flat $\mathcal{O}_S$-module. This explains the equivalence of flatness and local freeness in defining an étale morphism.

We will discuss the remaining terminology later.

6.2. **Etale Coverings.**

Definition 6.9. A *finite étale cover* is a surjective finite étale morphism.

This definition is sufficiently obtuse, but from above we see that defining a finite, locally free morphism is equivalent to defining a coherent $\mathcal{O}_X$-algebra that is locally free of finite rank as an $\mathcal{O}_X$-module whose stalks are étale algebras over the residue field. This should, at least aesthetically, resemble the definition of topological covering spaces in terms of locally constant sheaves. In fact, with the sufficient generalized notion of topology, this is exactly the definition.

We now take a short detour to explain the constant references to a generalized notion of topology. This will serve to make more apparent the direct analogies between the theory of étale coverings and that of topological coverings.

6.2.1. *The Etale Topology.*

In 2.4 we introduced the category X_{Top} of open sets over a given space X with the natural restrictions and defined a presheaf as no more than a functor from this category. Grothendieck's key observation was that there was no need to restrict one's attention to open sets. One can instead look at categories associated to our objects interest that "look like" topologies, i.e. satisfying analogues of being closed under finite intersection and arbitrary union. We've already seen that the general categorical analogues of these are finite colimits/fibre products and infinite limits. Such categories are called *Grothendieck topologies* or *sites*.[17]

In [13, Chapter 5] it is shown that all maps in the cocartesian square formed by a fibre product (2.10) are again étale. The composition of two finite, étale morphisms is also étale, and the infinite limit property is also satisfied. We thus find that both the category of étale morphisms over a fixed base scheme defines a *site*, called the *étale topology* of a scheme.[18]

With this in mind, one may think of etale coverings as being surjective morphisms that are locally trivial in the étale topology.

We first need some definitions and a fact.

Fact: As in the case of topological covering spaces, given an etale covering $X \to S$ and a morphism $Y \to S$, the resulting fibre product is an etale covering of Y. In particular, the fibre product of two étale coverings is again étale.

Definition 6.10. An etale covering $\phi : X \to S$ is called trivial if X is isomorphic to a disjoint union of copies of S and ϕ restricts to the identity on each copy.

Proposition 6.11. *Let $\phi : X \to S$ be a surjective affine morphism. Then ϕ is an étale covering iff there is an étale morphism $U \to S$, such that $U \times_S X$ is a trivial covering of U.*

Proof. □

[17] The actual theory is not so simple. For example, while one can always construct X_{Top}, there are topologies, such as the discrete topology, that can't be recovered from the corresponding site. While the objects in a site look a lot like open sets it's not generally isomorphic to some X_{Top}.

[18] We may then generalize the notion of a presheaf over a space X as a contravariant functor from a site associated to X. It is this construction for étale morphisms over a base scheme that leads to the defintion of étale cohomology [10].

Given an étale covering $X \to S$ and a morphism $Y \to S$, the fibre product $X \times_S Y$ is an étale covering of Y. In particular, the fibre product of two étale coverings is again an étale covering of S, with the projections also being étale coverings, i.e. intermediary covers. This is called the *base-change property* of étale coverings.

We'll need the following definition as well.

Definition 6.12. Let $p : Spec(K(p)) \to S$ be a point. We define the corresponding *geometric point* $\bar{p} : Spec(\Omega) \to S$ where Ω is an algebraic closure of $K(p)$. One defines the *geometric fibre* with respect to a map $X \to S$, denoted by $X_{\bar{p}}$, as the fibre product $X \times_S Spec(\Omega)$.

Geometric fibres will play the role of ordinary fibres in the topological case, and geometric points will play the role of base points.

Etale coverings also satisfy an analogue of unique lifting. This again requires a slightly different formulation than before as a result of our more abstract notion of a point.

Proposition 6.13 (Unique Lifting)**.** [13, 5.3.3] *If $Z \to S$ is a connected scheme and ϕ_1, ϕ_2 are two S-morphisms to a finite étale S-scheme X*[19] *and let $\bar{z}$ be a geometric point of Z. If $\phi_1 \circ \bar{z} = \phi_2 \bar{z}$, then $\phi_1 = \phi_2$.*

This follows from [13, Proposition 5.3.1], another property telling us that our topological intuition is valid.

Lemma 6.14. *Let $\phi : X \to S$ be an étale covering. A section $s : S \to X$ is an étale morphism and an isomorphism onto an open and closed subscheme of X. Thus if S is connected, s is an isomorphism onto a connected component of X.*

Proof of 6.13. Replacing $X \to S$ with the étale covering $Z \times_S X \to Z$, we reduce to the case where ϕ_1 and ϕ_2 are sections. Since there are then isomorphisms onto connected components of X, it's clear that $\phi_1 = \phi_2$ iff they map agree at a (geometric) point. □

6.3. **The Galois Theory of Étale Coverings.** We may now reconstruct the Galois theory of topological covers for étale coverings.

Proposition 6.15. *Let $\phi : X \to S$ be a finite, étale covering. The non-trivial elements of the group of deck transformations* $\mathrm{Aut}(X|S)$ *act without fixed points on each geometric fibre.* $\mathrm{Aut}(X|S)$ *is thus finite.*

Proof. One may see the result as a direct corollary of [13, Corollary 5.3.3]. More directly, if π_X and $\pi_{\bar{s}}$ denote the projections from the geometric fibre and let $\sigma \in \mathrm{Aut}(X|S)$, we have the following square:

$$\begin{array}{ccc} X_{\bar{s}} & \xrightarrow{\pi_{\bar{s}}} & \bar{s} \\ {\scriptstyle \sigma\circ\pi_X}\downarrow & & \downarrow{\scriptstyle \bar{s}} \\ X & \xrightarrow[\phi]{} & S \end{array}$$

Since $\phi\sigma = \phi$, the square is cocartesian and one attains an induced automorphism of $X_{\bar{s}}$.[20]

[19] In other words, lifts of ϕ.

[20] This is known as the morphism induced by base change.

Now, by the unique lifting property, any automorphism fixing a geometric point must be the identity.

Since the stabilizers are trivial, we have that $\mathrm{Aut}(X|S)$ has the same cardinality as an orbit, and is thus finite.

□

We thus associate a finite group to each etale covering. As is the case for topological coverings, one can take any subgroup $G \subset Aut(X|S)$ and define a quotient scheme X/G whose underlying topological space is the quotient space by the action of G. Every element of G induces an automorphism of each $\mathcal{O}_X(U)$ by the definition of a morphism of schemes. Thus using the continuous projection π, which we define $\mathcal{O}_{X/G}(U) = (\mathcal{O}(\pi^{-1}(U))^G$, denoting the G-invariant elements. This immediately gives us a ringed space, but we must show 1) that X/G is a scheme and 2) that $X \to X/G$ and $X/G \to S$ are etale coverings.

Proposition 6.16. [13, Prop. 5.3.6] *X/G is a scheme, π is affine and surjective, and ϕ factors as $\phi = \psi \circ \pi$, where ψ is affine $X\,\mathrm{Gal} \to S$.*

Proof. Since the elements of the automorphism group are affine maps, and there are only finitely many of them, we may take an affine covering simultaneously subordinate to all the maps in G. Thus we may assume $X = Spec(B)$, $S = Spec(A)$ and we just want to show that X^G is isomorphic to B^G the set of G-invariant elements of B. This automatically gives π affine and surjective since B is integral over B^G, as $b \in B$ a root of the polynomial whose roots are all the G-conjugates of B, which is clearly G-invariant. Since every prime ideal of a ring can be written as the contraction of a some prime ideal in some fixed integral extension, we have surjectivity.

We thus have to show that the map $Spec(B) \to Spec(B^G)$ has the G-orbits of B for fibres. This is done by contradiction in assuming two orbits lie above a single point using an argument exactly like that used to prove 3.4. □

Proposition 6.17. *$X/G \to S$ and $X \to X/G$ are finite etale coverings.*

Proof. See [13, Proposition 5.3.7]. □

We again say an etale covering is *Galois* if the action of its automorphism group on a geometric fibre is transitive. Since etale coverings satisfy all the same properties as topological coverings that were required for the topological case, one deduces a Galois theory of etale coverings in a manner exactly analogous to the topological case.

We will also need to following analogue of the fact that every finite, separable field extension can be embedded in a finite Galois extension and that there is a minimal such extension.

Proposition 6.18. *Let $\phi : X \to S$ be a finite, etale cover. There finite, Galois cover P with $\pi : P \to X$ such that $\phi \circ \pi$ is a Galois cover of S.*

For a nice and interesting proof by Serre, see [13, Proposition 5.3.9]. Essentially, if n is the cardinality of the geometric fibre, one takes the n-fold fibre product, which has a canonical geometric point given by the point mapping to the geometric point in S, which one can write as an n-tuple $(\bar{x_i})_{i=1,\ldots,n})$. P will be the connected component of the product containing this point. One finds that its geometric fibre is represented by permutations of $\{1,...,n\}$ and every permutation induces a covering automorphism, therefore transitive on the fibre.

6.4. **The Etale Fundamental Group.** In each of the preceding sections we constructed a fibre functor from our category of interest to finite sets with a continuous action of some profinite group. We may reformulate our results in the following two theorems:

Theorem 6.19. *(Galois) Let k be a field and k_s a fixed separable extension. Then the absolute Galois group $\mathrm{Gal}(k_s|k)$ is exactly the group of automorphisms of the fibre functor.*[21]

Theorem 6.20. *Let X be a connected topological space with base point x. Then $\pi_1(X,x)$ is also the group of automorphisms of the fibre functor.*

For the first, we saw that every element of the Galois group induces a morphism on every finite subextension, all compatible in the sense that they commute with restriction. Thus the resulting morphisms are also all compatible and thus defines a automorphism of functors (2.2). Conversely, an automorphism of the fibre functor commutes with the morphisms in the image of the fibre functor, which are exactly the actions of $\mathrm{Gal}(k_s|k)$. Thus morphisms of functors are $\mathrm{Gal}(k_s|k)$-equivariant. It follows that the family of morphisms defining the automorphism of functors defines an element of the inverse limit, $\mathrm{Gal}(k_s|k)$.

The case for the fundamental group is similar. We saw that every element of $\pi_1(X,x)$ induces monodromy on fibres. The monodromy is equivalent to a morphism of the fibre functor.[22]

This motivates the following definitions:

Definition 6.21. Let $\bar{s}$ be a geometric point. Define a functor $Fib_{(S,\bar{s})}$ from finite étale coverings of S to finite sets by sending $X \to S$ to the corresponding geometric fibre. The *Etale Fundamental Group*, denoted by $\pi_1(S,\bar{s})$ is the group of automorphisms of $Fib_{(S,\bar{s})}$.

Remark 6.22. We showed in the preceding section that any automorphism of a finite étale cover induces an action in the geometric fibre. Thus we again can see automorphisms of the fibre functor as being equivalent to compatible families of étale deck transformations.

Example 6.23. Let $S = Spec(k)$ where k is a field. An étale covering is then of the form $Spec(A) \to Spec(k)$, where A is an étale k-algebra.[23]

Then a geometric fibre is just $Spec(A \otimes \bar{k})$ [24]. Since the spectrum of a sum is the disjoint union of the spectra of the components, we may suppose A is a finite

[21] Of course here we mean functors from the category defined by the image of the fibre functor to itself with two-sided inverses.

[22] The major difference here is that the universal covering is itself a part of the category of covering spaces over X, and we thus saw that the fibre functor was in fact representable. $Fib_X(Y) = \mathrm{Hom}_X(\tilde{X}, Y)$ where $\tilde{X}$ denotes the universal covering. k_s is NOT in general a finite algebraic extension of k, and thus we can't say the fibre functor is representable.

[23] The étale condition on the fibres forces this, the residue field at the one point of $Spec(k)$ of course being k itself.

[24] In [1, Exercises, Chp. 1], one shows that $Spec()$ is in fact a contravariant functor to the category of affine schemes. It is in fact an isomorphism of categories. Thus tensor products correspond to fibre products.

algebraic extension of k, L. The fibre is thus one point for each root of the minimal polynomial of a defining element of L. The automorphisms of the fibre functor are exactly the absolute Galois group of k and one sees that the étale fundamental group generalizes Galois theory!

6.4.1. *Properties of the Etale Fundamental Group.* We will make precise the statement above that an automorphism of the fibre functor comes compatible families of automorphisms of étale coverings. Since every étale covering X can be associated to a minimal Galois covering over it and every other Galois covering over X factors through it, "compatible families" of automorphisms will be exactly those automorphisms defining an automorphism of the direct limit of Galois covers.[25].

The following theorem is due (of course) to Grothendieck.

Theorem 6.24. *Let S be a connected scheme with $\bar{s}$ a geometric point.*

1) $\pi_1(S, \bar{s})$ is profinite and it's action on each $Fib_{\bar{s}}(X)$ is continuous.

2) $Fib_{\bar{s}}$ induces an equivalence of categories between Fet_S[26] and finite sets with a continuous $\pi_1(S, \bar{s})$-action. Transitive action corresponds to connected covers and Galois covers correspond to normal subgroups of finite index.

As before, the fibre functor isn't representable, because the inverse limit is not necessarily itself a finite, étale cover. It's not far from being representable though.

Definition 6.25. A set-valued functor F is called *pro-representable* if there is a direct system $(P_\alpha, \phi_{\alpha\beta})$ such that

$$\varinjlim \operatorname{Hom}(P_\alpha, X) \simeq F(X). \tag{6.26}$$

We just need to show that the Galois covers over a fixed base scheme form an inverse system. We say $\alpha \leq \beta$ if there exists a morphism $P_\beta \to P_\alpha$. The fibre product of two Galois coverings in a covering with each of the components as intermediary coverings. The same is true for any of it's connected components. Choosing one and taking the associated minimal Galois extension above it shows that the system is indeed directed. However, we must define the $\phi_{\alpha\beta}$ which exist by definition, but are not necessarily uniquely defined. We circumvent this by choosing a *distinguished point*, p_α in each fibre and using the unique lifting property to define a $\phi_{\alpha\beta}$ as the unique morphism from $P_\beta \to P_\alpha$ sending p_β to p_α. Then (p_α) define an element of $\varprojlim P_\alpha$.

Details on showing that the fibre functor is pro-representable by this system can be found in [13, Proposition 5.4.6].

This allows us to characterize automorphisms of the fibre functor as morphisms of the directed system $(P_\alpha, \phi_{\alpha\beta})$, which are nothing but new choices of a set of distinguished points p'_α. Since these also define an element of the direct limit, we may construct a morphism of direct systems by taking the collection of uniquely defined automorphisms of each P_α taking p_α to $p\alpha'$.

Corollary 6.27. *The automorphism groups $\operatorname{Aut}(P_\alpha)^{op}$ form a direct system whose inverse limit is isomorphic to $\pi_1(S, \bar{s})$.*

Proof. Since intermediate coverings correspond to subgroups of the automorphism group by the Galois theory of étale coverings, one has a surjective morphism $\operatorname{Aut}(P_\beta|S) \to \operatorname{Aut}(P_\alpha|S)$, and the system is directed by the above.

[25] Compare to the section on Galois theory

[26] The category of finite, etale coverings of S

Each element of the inverse limit is equivalent to an automorphism of the P_α direct system, which is equivalent to an automorphism of the fibre functor.

□

We thus have that $\pi_1(S, \bar{s})$ in indeed profinite and one demonstrates the rest of 6.24 in a manner analogous to the situation in Grothendieck's formulation of Galois theory. Details are in [13, Theorem 5.4.3].

6.5. **Integral Proper Normal Curves.** We now return to proper normal curves for a slightly more concrete formulation of the preceding theory. Let A be an integrally closed, finitely generated of transcendence degree 1 over k, analogous to the section on Riemann surfaces[27]. While this may seem quite restrictive, such rings are quite important. They go by another name: Dedekind domains.

6.5.1. *Construction: Building an integral proper normal curve from A.* We construct and define below a *integral proper normal curve* built from glueing two affine schemes isomorphic to $Spec(A)$ in a manner analogous to the gluing of two complex planes to form the Riemann sphere. Note that for A as above, $Spec(A)$ is also known as scheme-theoretically as an *integral normal affine curve.*

We begin with the assumption that $A = k[x]$ for x an indiscriminate over k and then generalize the following construction. A has a field of fractions given by $k(x)$ which is also the field of fractions of $A' = k[x^{-1}]$. We thus attain two affine schemes, $Spec(A)$ and $Spec(A')$. Note the $Spec(A)$ is also called the affine line over k and denoted by $\mathbb{A}^1_k$..

Now, if $B = k[x, x^{-1}]$, we have natural inclusions:

$$\begin{array}{ccc} & & A \\ & & \big\downarrow{\scriptstyle i} \\ A' & \xhookrightarrow[i']{} & B \end{array}$$

Applying the contravariant functor $Spec()$ gives us a new diagram with reversed arrows. We take the limit of the resulting diagram to define a integral proper normal curve which we denote by $\mathbb{P}^1_A$.

We may describe concretely the resulting object in a manner curtailing the above usage of abstract nonsense. The following is adapted from [13].

Lemma 6.28. *Let $X = Spec(A)$ be an integral normal affine curve and denote $\mathcal{O}(X) = A$ with fraction field $K(X)$ are exactly the discrete valuation rings R with fraction field $K(X)$ containing $\mathcal{O}(X)$.*

Proof. First, it's a property of localizations of domains that all share the same field of fractions. Intuitively, this comes from the fact that localizing can be viewed as giving inverses to certain elements and thus in intermediary step towards constructing the field of fractions. More concretely, if S is multiplicatively closed subset of A and T is another, then of we denote by T_S the image of T under the canonical application $A \to S^{-1}A$, then $S_T^{-1}T^{-1}A = T_S^{-1}S^{-1} = (ST)^{-1}$ where ST denotes the multiplicative set generated by S and T.

Now, let R be a dvr as described in the statement. The intersection of its maximal ideal M with $\mathcal{O}(X)$ is non-zero since otherwise the restriction to $\mathcal{O}(X)$ of

[27]To Zariski and his followers, the curves we consider were known as abstract Riemann Surfaces.

the projection $R \to R/M$ would be injective. Thus the field R/M would contain the field $K(X)$, which isn't possible. [WHY?]

Thus $M \cap \mathcal{O}(X)$ is a prime ideal P in $\mathcal{O}(X)$ and thus contains the local ring $\mathcal{O}(X)_P$. But since a dvr contained in another with the same fraction field must be the entire dvr, R=$O(X)_P$ for some $P \in Spec(A)$.

□

Thus the integral proper normal curve contained above we see that there is only one local ring with fraction field $K(X)$ that isn't a local ring of $O(X)$, corresponding to the localization of A' by the ideal (x^{-1}). This can be thought of as the "point at infinity". Thus $\mathbb{P}^1_A$ is exactly $Spec(A)$ plus this extra point, exactly parallel to the complex situation.

Now for a general integral affine normal curve, we again use the notation $\mathcal{O}(X)$ and denote it's field of fractions by $L(X)$, which is a finite algebraic extension of $K(X)$. By assumption, there exists a transcendental generator x such that $\mathcal{O}(X)$ is integral over $k[x]$. We again consider $k[x^{-1}]$ and let $O(X_-)$ be the integral closure of $k[x^-1]$ in $K(X)$ with X_- denoting $Spec(O(X_-))$. Considering the integral closure of $k[x, x^{-1}]$ in $K(X)$, we obtain an identical diagram as the one above. Concretely, we add finitely many points to X corresponding to the finitely many local rings R with fraction field $K(X)$ namely by the finitely many ideals in $O(X_-)$ lying above $(x^{-1}) \in k[x^{-1}]$ enumerated by the primes appearing factorization of it's image under the injection $k[x^{-1}] \hookrightarrow O(X_-)$ into prime powers, see below.

The above constructions show that our objects are indeed schemes, whose structure sheaves are inherited directly from the spectra of the corresponding Dedekind domains.

Moreover, given A finitely-generated of transcendence degree 1 over $k[x]$, any finite integral extension B of A, we may first construct the two copies of the affine curves corresponding to each and the inclusion induced homomorphisms between them. The gluing above also allows us to extend this morphism to the whole integral proper normal curve.

By [13, 4.4.7] every surjective morphism of integral proper normal curves is finite and in fact comes from such a morphism as described in the last paragraph. This means, for example, that our maps are always affine. We write $Y^L \to X^K$, where superscripts correspond to function fields. The end result is:

Proposition 6.29. *The contravariant functor from the category of integral proper normal curves with a surjective morphism to a fixed base curve X^K to the corresponding finite field extension of K in the category of finite field extensions of K is an anti-equivalence of categories.*

6.5.2. *Etale morphism and coverings for proper normal curves.* We present the theory in the last section in the case of integral proper normal curves. This will be equivalent to the definitions given above [13, Chapter 5]. Note the structure of such morphisms as always associated to a morphism of field extensions.

Definition 6.30. A morphism $\phi : Y \to X$ of integral proper normal curves is called *separated* if $K(Y)|K(X)$ is separable. If we let $A \subset B$ be the corresponding Dedekind rings, ϕ is called *étale* if over a closed point[28] $P \in X$, B/PB is a finite étale algebra over $K(P) = A/P$, the residue field at P.

[28] Not the unique generic point.

Remark 6.31. From the discussion on Dedekind rings in section 1, it follows that

$$PB = \prod_{i=1\dots n} Q_i^{e_i} \tag{6.32}$$

Where each $Q_i \cap A = P$ is distinct. Since distinct maximal ideals are relatively prime, we apply the Chinese remainder theorem to find that

$$B/PB = \prod_{i=1,\dots,n} B/(Q_i)^{e_i} \tag{6.33}$$

From this, one can see the ϕ is étale iff all the e_i are equal to one and the $K(Q_i)|K(P)$ are separable.

Regarding the curves as schemes, we have $B/PB \simeq (\phi^*\mathcal{O}_Y)_P \otimes_{\mathcal{O}_{X,P}} K(P)$. It's spectrum is exactly the fibre of the map over P as defined in the last section.

We thus would like to know about the e_i, which are called the *ramification indices* of ϕ.

Proposition 6.34. [13, Proposition 4.1.6] *Let A be a Dedekind ring with fraction field K, and let B be the integral closure of A in a finite separable extension $L|K$. For a nonzero prime ideal $P \subset A$ with primary decomposition $\prod_{i=1\dots n} Q_i^{e_i}$ in B. Then*

$$\sum_{i}^{n} e_i[K(Q_i) : K(P)] = [L : K] \tag{6.35}$$

Corollary 6.36. *For A and B as above such that $L|K$ is Galois, with group G, and let P be prime in A. If all the $K(Q_i)|K(P)$ are separable, then the ramification indices are all the same and equal to the order of the inertia subgroups at any of the Q_i.*

Remark 6.37. This allows us to speak of *the ramification index* of an ϕ at a point.

Example 6.38. With A being the field of meromorphic functions of a Riemann surface, the e_i correspond to the ramification indices of a branched covering. Thus morphisms of integral proper normal curves whose fields are finite extensions of $\mathbb{C}(t)$ are the same as holomorphic maps between compact Riemann surfaces.

Proof. Recall that D_Q denotes the stabilizer in G of Q by its action on the prime ideals corresponding to P. Let K_1 denote the fixed field of D_{Q_1}, A_1 the integral closure of A in K_1, and $P_1 = A_1 \cap Q_1$. By construction, Q_1 is the only ideal lying above P_1. Since $Gal(K(Q_1)|K(P_1) \simeq D_{Q_1}/I_{Q_1}$, we have

$$|D_{Q_1}| = |I_{Q_1}| \cdot [K(Q_1)|K(P_1)] = e_i[K(Q_1)|K(P_1)] \tag{6.39}$$

by the above proposition. Since all the D_Q and I_Q are conjugate, and thus all have the same order, in G, the result follows. □

Regarding the properties of the Zariski topology, one sees that finding that given a separable map of integral proper normal curves, finding an open set over which the map is étale as saying the morphism is étale over all but a discrete set. In fact, one can always do this [13, Proposition 4.5.9]. Thus we are in a situation exactly to analogous to the Riemann surface case, wherein every non-constant morphism is a *branched covering.*

Definition 6.40. Whenever $\phi : Y \to X$ induces a Galois extension $K(Y)|K(X)$, we say Y is a *branched Galois cover* of X. The Galois group act transitively on the fibre over a point P by the transitivity on the ideals contracting to P.

Thus a Galois cover is unramified iff the inertia subgroups have order 1.

6.5.3. *The Etale Fundamental Group of a Proper Normal Curve.* We proceed to describe the étale fundamental group in this setting. We begin with a fact that's proved in a way exactly to the corresponding fact for Riemann surfaces demonstrated above.

Definition 6.41. A integral proper normal curve, whose ring of functions in integral over $k[x]$ is a *k-curve.*

Proposition 6.42. [13, 4.6.1] *Let X be a proper normal k-curve with k perfect*[29]*. Let K denote the function field of X, K_s denote a fixed separable closure, and let $U \subset X$ denote a non-empty open set. Then the composite K_U of all finite subextensions $L|K$ so that the corresponding morphism of proper normal curves is étale over all $P \in U$ is a a Galois extension of K, and each finite subextension of K_U comes from a curve étale over U.*

Definition 6.43. The *algebraic fundamental group* $\pi_1(U)$ of U is the group $\mathrm{Gal}(K_U|K)$.

Note that here we make no reference to base points. We are free to do this because, as discussed in the section on inertia subgroups, given a curve étale over U, the Galois groups $\mathrm{Gal}(K(Q)|K(P))$ are naturally identified with subgroups of finite quotients of $Gal(K_U|K)$, since there is no ramification. Thus, the action on any geometric fibre is completely determined by $\pi_1(U)$.

We now consider disjoint unions of integral proper normal curves, whose function fields are just direct sums of the components. Such objects are called *proper normal curves.*

We thus have, as always, the following theorem:

Theorem 6.44. *Let X be an integral proper normal curve over a perfect field k, and let $U \subset X$ be open. The category of proper normal curves over X, $\phi : Y \to X$ étale over U is equivalent to the category of finite continuous left $\pi_1(U)$-sets.*

Example 6.45. For the case of X a compact, connected Riemann surface, $\pi_1(U)$ is none other than the profinite completion of $\pi_1(X, x)$.

7. Applications and Comments

7.1. **The Homotopy Exact Sequence, Outer Galois Action and the Inverse Galois Problem.**

We present an application of the above discussion on proper normal curves to the inverse Galois problem.

Definition 7.1. An integral proper normal curve X with function field K is called *geometrically integral* if for every $L|k$ separable and algebraic in some fixed separable closure, $\mathcal{O}_X \otimes_k L$ is integral, equivalent to $K \otimes_k L$ being a field for all such L, equivalent to $K \otimes_k k_s$ being a field. We denote by X_L the fibre product $X \times_{Spec(k)} L$, itself a proper normal curve, integral if X is geometrically integral. X_L is called the *base change* of X. Base change is easily seen to be functorial. Note that the

[29]This way we don't need to worry about separability, and the cases of interest for us will always be perfect.

resulting morphism $X_L \to X$ is in fact finite étale when X is geometrically integral since the fibres are just the spectra of $K(P) \otimes_k L$.

The following theorem is demonstrated in [13, 5.7.8].

Theorem 7.2. *Let k be of characteristic 0, X be an integral proper normal k-curve, and* $U \subset X$ *open. The base change functor* $Y \to Y_L$ *induces an equivalence between the finite covers of X étale over U and those of* X_L *over* U_L*. Thus, there is an isomorphism* $\pi_1(U_L) \to \pi_1(U)$*.*

Remark 7.3. This tells us, for example, that given any integral proper normal curve defined over $\bar{\mathbb{Q}}$, we may take the base change to $\mathbb{C}$ and the fundamental group of the (open subset of) the curve will be equal to that of the base change.

Now let be X as above and $\bar{k}$ some algebraic closure[30]. We assume X is geometrically integral. Now, suppose K_s is a separable closure of K containing $\bar{k}$. One finds that $K \otimes_k \bar{k} \simeq K\bar{k}$, the composite field in K_s. In particular, since $X_L \to X$ is always étale, in particular over every restriction $U_L \to U$, we find that $K\bar{k} \subset K_U$ for all U. We there is a canonical isomorphism $\mathrm{Gal}(K(X_L)|K) \simeq \mathrm{Gal}(L|k)$ and thus $\mathrm{Gal}(K\bar{k}|K) \simeq \mathrm{Gal}(\bar{k}|k)$. This implies that $\mathrm{Gal}(\bar{k}|k)$ arises as a quotient $\pi_1(U)$ for all U.

In fact, we have the following short exact sequence of profinite groups, a specific instance of the *homotopy exact sequence of the étale fundamental group* [13, Chp. 5]:

$$0 \to \pi_1(U_{\bar{k}}) \to \pi_1(U) \to \mathrm{Gal}(\bar{k}|k) \to 0 \tag{7.4}$$

Proof. [13, 4.7.1] □

Definition 7.5. $\pi_1(U_{\bar{k}})$ is called the *geometric fundamental group* of U.

When one has an exact sequence of profinite groups, $0 \to N \to G \to \Gamma \to 0$, one can always identify N with a normal subgroup of G and consider the action of G on N by conjugation, described by a continuous group homomorphism $G \to \mathrm{Aut}(N)$. Restricting to conjugation by elements of N gives the group of inner automorphisms $\mathrm{Inn}(N)$.

Definition 7.6. The *group of outer automorphisms* is given by the quotient

$$\mathrm{Aut}(N)/\mathrm{Inn}(N).$$

Thus, since $\Gamma \simeq G/N$, and we have a natural map $G/N \to \mathrm{Out}(N)$, one attains a natural map

$$\Gamma \to Out(N).$$

We thus attain a continuous homomorphism:

$$\rho_U : \mathrm{Gal}(\bar{k}|k) \to Out(\pi_1(U_{\bar{k}}))$$

This is called the *outer Galois action of the geometric fundamental group.*

The interest in the inverse Galois problem, which asks what finite groups can be realized as Galois groups of finite extensions of $\mathbb{Q}$ lies in the fact, demonstrated by Belyi, that when $k = \mathbb{Q}$, and $U = \mathbb{P}_1 - \{0, 1, \infty\}$, the above morphism has trivial kernel, i.e. the outer representation is *faithful.*

[30]Since k is assumed perfect, $\bar{k}$ is also a separable closure.

Proof. This actually comes from the well-known "Belyi's" Theorem, for which one direction can be proved elementarily [4], while the other is more difficult [13, 4.7.6].

Theorem 7.7. *Let X be a compact, connected Riemann surface. Then there exists a holomorphic map $X \to \mathbb{P}_1$ unramified over $\mathbb{P}_1 - \{0, 1, \infty\}$ iff X can be defined over $\overline{\mathbb{Q}}$* [31]

Thus we now consider the projective spaces $\mathbb{QP}_1$ and $\bar{\mathbb{Q}}\mathbb{P}_1$.

If $U = \mathbb{QP}_1 - \{0, 1, \infty\}$ and $\bar{U}$ denotes the base change to $\bar{\mathbb{Q}}$, and ρ_U has non-trivial kernel, then we may take the fixed field of the kernel, L. By construction ρ_{U_L} has trivial kernel. This means that every automorphism on $\pi_1(\bar{U})$ induced by conjugating by an element $x \in \pi_1(U_L)$ is also induced by conjugation by some $y \in \pi_1(\bar{U})$. Thus $y^{-1}x$ is in the centralizer, C of $\pi_1(\bar{U})$ in $\pi_1(U_L)$.

Thus any element of $\pi_1(U_L)$ can be written as the product of an element in the centralizer and an element of $\pi_1(\bar{U})$. By 7.3, we know that $\pi_1(\bar{U})$ is isomorphic to the free group on two generators, and thus has trivial center. This means that $\pi_1(U_L) = \pi_1(\bar{U}) \oplus C$. We may thus write $\pi_1(\bar{U})$ as a quotient of $\pi_1(U_L)$. Thus, by the Galois correspondence established for étale coverings, we see that every étale covering of $\bar{U}$ comes by base change from a cover of U_L. By Belyi's theorem, this means that every proper normal curve defined over $\bar{\mathbb{Q}}$ can in fact be defined over L, but there are counterexamples. See [13, Facts 4.7.8].

□

Acknowledgments. It is a pleasure to thank professor Jean-Francois Dat for guiding me through the project and answering numerous questions. I would like to further thank professor Pierre Schapira for his Category Theory explanations, the TER board at Jussieu and the several fellow students who listened to me trying to explain stuff and helped me understand in turn.

References

[1] Michael Atiyah. I.G. McDonald. *Introduction to Commutative Algebra.* Westview Press. 1969.
[2] David Dummit. Richard M. Foote. *Abstract Algebra.*
[3] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry.* Springer. 2004.
[4] Elisha Falbel. *Riemann Surfaces.* Unpublished course notes. 2009
[5] Alexandre Grothendieck. *Revêtements Étales et Groupe Fondamental (SGA 1).* Société Mathématique de France. 2003.
[6] Robin Hartshorne. *Algebraic Geometry.* Springer. 2010.
[7] Allen Hatcher. *Algebraic Topology.* Cambridge University Press. 2001.
[8] Serge Lang. *Algebra.* Springer.
[9] Saunders MacLane. *Category Theory for the Working Mathematician.* Springer.
[10] J.P. Milne. *Etale Cohomology.* Unpublished course notes. 2012.
[11] Rick Miranda. *Algebraic Curves and Riemann Surfaces.*
[12] Pierre Schapira. *Algebraic Topology and Homological Algebra.* Unpublished course notes. 2011.
[13] Tamás Szamuely. *Galois Groups and Fundamental Groups.* Cambridge Studies in Advanced Mathematics. 2010.

[31] This of course means that X is isomorphic to a Riemann surface defined by a polynomial whose coefficients lie in $\overline{\mathbb{Q}}$.