Étale Fundamental Groups

Aaron Lu

Advised by Professor Eugene Kushnirsky

A Thesis Submitted in Partial Fulfillment of the Requirements for Honors in Mathematics

Mathematics Department

Northwestern University

April 19th, 2024

This page is intentionally left blank.

Contents

1 Introduction.

This is meant to be a brief survey of some introductory ideas in algebraic geometry at an undergraduate level, with a focus on building up to the concept of an étale fundamental group. We will assume familiarity with the most common algebraic objects: groups, rings, fields—content which can be found in [4] Part One—as well as finite Galois theory, such as can be found in [4] Part Two, Chapters V and VI. We will also assume the reader is familiar with concepts which would be introduced in an undergraduate course on topology, or most of what can be found in [6]. In Sections 1 and 2, we motivate our discussion through relating Galois groups and fundamental groups, largely inspired by ideas found in [1] and [8]. In Section 3, supplemented by material found in [2] and [3], we introduce the prime spectrum of a ring and the concept of an affine scheme. These are fundamental objects in algebraic geometry which help frame the example in Section 4, and are necessary to both construct the étale fundamental group in Section 5, as well as understand finite étale morphisms, as seen in Section 6. Our treatment of algebraic varieties in Section 7 comes from the discussions on varieties found in [3] and [7]. Finally, the examples and exercises given in [5] form the basis of the examples seen in Section 8, and many more examples of étale fundamental groups can be found there.

1.1 Galois groups and fundamental groups.

Our discussion begins with two stories which look remarkably similar. On one hand, in Galois theory we study fields k and their extensions K/k. Under composition the set of automorphisms of K fixing k form the group Aut(K/k). If it happens that the field fixed by every automorphism in Aut(K/k) is exactly k, then K is Galois over k, and we denote Aut(K/k) by Gal(K/k), which we call the Galois group of K over k. Let us assume that K is a *finite* Galois extension. Then there is a correspondence between the subgroups of Gal(K/k) and the intermediate fields of K/k. Specifically, each subgroup H of Gal(K/k) fixes some subfield F_H of K, and to each intermediate field $K/F/k$ there is some subgroup of H_F of Gal(K/k) fixing F. Moreover, we have

$$F_{H_{F_0}} = F_0 \quad \text{and} \quad H_{F_{H_0}} = H_0$$

so that this correspondence is a bijection. This correspondence is also inclusion reversing, so that $H_1 \subset H_2$ if and only if $F_{H_1} \supset F_{H_2}$. Finally, we have that K is Galois over each intermediate field, and H_F is exactly (isomorphic to) Gal(K/F). In the case where H_F is a normal subgroup of Gal(K/k), then F is also Galois over the base field k and we have the isomorphism

$$\text{Gal}(F/k) \cong \frac{\text{Gal}(K/k)}{\text{Gal}(K/F)}.$$

If we take K to be k_s the separable closure of k, then every finite separable extension of k manifests as an intermediate field of k_s. Note that the above discussion on the correspondence of subgroups and intermediate fields only holds for finite extensions, while k_s/k is not necessarily finite. We will have more to say on infinite Galois extensions in Section 2. The extension k_s/k is, however, still

Galois, in the sense that the fixed field of $\mathrm{Aut}(k_s/k)$ is exactly k. We call $\mathrm{Gal}(k_s/k)$ the absolute Galois group of k.

On the other hand, in topology we study topological spaces X (to build the analogy, we will for now ignore properties of X and specifications of base points) and fundamental groups $\pi_1(X)$. There is a correspondence between the subgroups of $\pi_1(X)$ and the covers of X. Concretely, if $f : Y \to X$ is a covering then f induces an injective homomorphism $f_* : \pi_1(Y) \to \pi_1(X)$ and we identify f with the subgroup $f_*(\pi_1(Y))$. Moreover, if f_1, f_2 are two covering maps corresponding to subgroups H_1, H_2, then we have $H_1 \subset H_2$ if and only if f_1 dominates f_2, that is, there is some covering map $g : Y_1 \to Y_2$ so that

$$\begin{tikzcd} Y_1 \arrow[r, "g"] \arrow[dr, "f_1"'] & Y_2 \arrow[d, "f_2"] \\ & X \end{tikzcd}$$

commutes. Again, this exhibits some sort of order-reversing property. A "smaller" subgroup corresponds to a "larger" cover. Finally, if $f_*(\pi_1(Y))$ is normal in $\pi_1(Y)$, then f is a normal (or regular or Galois) covering and we have the isomorphism

$$\mathrm{Deck}(f) \cong \frac{\pi_1(X)}{f_*(\pi_1(Y))}$$

where $\mathrm{Deck}(f)$ is the group of deck transformations of f. Recall that a homeomorphism $d : Y \to Y$ is a deck transformation if

$$\begin{tikzcd} Y \arrow[r, "d"] \arrow[dr, "f"'] & Y \arrow[d, "f"] \\ & X \end{tikzcd}$$

commutes. If we take the universal cover $\tilde{f} : \tilde{X} \to X$ then $\tilde{f}$ dominates every other cover of X, and we have $\mathrm{Deck}(\tilde{f}) \cong \pi_1(X)$.

This is a remarkable list of similarities. In both cases, we are concerned with some object and a "larger object" which, in some sense, contains it. In both we are concerned with functions on the larger object which fix the one it contains, and these functions correspond to a group. The subgroups of this group correspond to intermediate objects under an inclusion-reversing correspondence, and in both cases the normal subgroups are of special improtance. The trivial subgroup is also of importance, corresponding to the absolute Galois group in Galois theory and the universal cover in topology.

Seemingly, there must be some fundamental connection between fields and topological spaces. Yet the way we define these objects seem on the surface unrelated. Fields are the natural setting where we are able to generalize the four basic operations of arithmetic, while topological spaces allow us to explore and formalize our intuitive notion of continuity.

Our goal is to pin down the connection between fields and topological spaces, where we imagine a wider class of objects under which fields and topological spaces naturally appear. Moreover, like the topological fundamental group, which gives us a powerful tool to study topological spaces through algebra, we would like some way to study this wider space through algebra. Specifically, we also imagine a map, analogous to the topological fundamental group, assigning to each object of this wider class a group, so that fields get mapped to their Galois groups and topological spaces to their fundamental groups. As we will see, this is not exactly what will play out, but we will get something close. The wider class of objects will be the category of *affine schemes* and the map will be the *étale fundamental group*. We set out to motivate and define both these ideas, and explore other connections between algebra and geometry along the way.

2 Infinite Galois extensions.

The separable closure of a field will have a large role to play in what follows, although as we have previously mentioned, the separable closure is not necessarily a finite extension. The problem with this is that if we drop the condition that a Galois extension E/k is finite, then the bijective correspondence between subgroups of Gal(E/k) and intermediate fields of E/k no longer holds in general. We can, however, bridge the gap between infinite Galois extensions and finite Galois extensions by identifying Galois groups with their finite quotients. For that we will need to introduce the concepts of inverse limits and profinite groups.

2.1 Inverse limits and profinite groups.

Definition 1. A *partially ordered set* is a set I and a relation $\leq$ on I such that for any $i, j, k \in I$, we have $i \leq i$; if $i \leq j$ and $j \leq i$ then $i = j$; and if $i \leq j$ and $j \leq k$ then $i \leq k$. A partially ordered set is *directed* if for each $i, j \in I$ there is some k so that $i \leq k$ and $j \leq k$.

Definition 2. An *inverse system* of groups is a family of groups $\{G_i\}_{i\in I}$ indexed by a directed partially ordered set I such that for each $i \leq j$ there is a homomorphism $f_i^j : G_j \to G_i$ satisfying $f_i^i = \text{id}$ and, if $i \leq j \leq k$, then

$$f_i^k = f_i^j \circ f_j^k.$$

We make $\prod_{i\in I} G_i$ a group by defining the group operation point-wise. The subgroup of $\prod_{i\in I} G_i$ consisting of elements (x_i) satisfying $f_i^j(x_j) = x_i$ for all $i \leq j$ is called the *inverse limit* of the family, which we denote $\varprojlim G_i$. This is a subgroup as if $(x_i), (y_i) \in \varprojlim G_i$ then

$$f_i^j(x_j y_j) = f_i^j(x_j) f_i^j(y_j) = x_i y_i.$$

Also,

$$f_i^j(x_j^{-1}) = (f_i^j(x_j))^{-1} = x_i^{-1}$$

so that $(x_i^{-1}) \in \varprojlim G_i$ if $(x_i) \in \varprojlim G_i$. The inverse limit is sometimes referred to as the *projective limit*.

Example. Suppose G is a group and consider all normal subgroups of finite index. We can establish a partial ordering by inclusion, that is, we think of "$N \leq M$" if $M \subset N$. Note that if N, M are normal subgroups of finite index, then so is $N \cap M$, and in this way our partial ordering becomes directed. If $N \leq M$ then there is a natural map $G/M \to G/N$ given by sending the equivalence class of an element x mod M to x mod N, and we can define the inverse limit $\varprojlim G/N$ taken over all normal subgroups of finite index.

Definition 3. A group which is the inverse limit of finite groups is called a *profinite* group.

In our example above, since we are only taking normal subgroups of finite index, each G/N is a finite group, hence the resulting inverse limit will be a profinite group.

Example. If, in the above example, we take our group to be $\mathbb{Z}$ then the inverse limit is

$$\varprojlim \mathbb{Z}/n\mathbb{Z}.$$

This inverse limit is usually denoted $\hat{\mathbb{Z}}$ and is called the *profinite completion of* $\mathbb{Z}$.

2.2 The Galois group as a profinite group.

Proposition 4. *Let k be a field and K/k an algebraic extension. Then there is an embedding $K \hookrightarrow \overline{k}$ fixing k elementwise. Moreover, any such embedding $K \hookrightarrow \overline{k}$ can be extended to an isomorphism $\overline{K} \to \overline{k}$.*

Proof. See [4] Chapter V, Theorem 2.8. □

Consider a tower of finite extensions $M/N/k$ each Galois over k. Then Proposition 4 allows us to give a canonical surjection $\varphi_N^M : \mathrm{Gal}(M/k) \twoheadrightarrow \mathrm{Gal}(N/k)$ defined by sending an automorphism $\sigma \in \mathrm{Gal}(M/k)$ to $\sigma|_N$, its restriction to N. We verify that $\sigma|_N \in \mathrm{Gal}(N/k)$. First, the fact that $\sigma(N) \subset N$ follows as σ must send any $\alpha \in N$ to a root of the minimal polynomial of α. As N is Galois, hence normal, it contains all such roots. Then $\sigma|_N : N \to N$ is injective, as it is a map of fields, so that we must have $[N : \sigma(N)] = 1$, and it follows σ is actually bijective. So indeed $\sigma|_N \in \mathrm{Gal}(N/k)$. The fact that this map is actually a surjection requires Proposition 4. Here for some $\tau \in \mathrm{Gal}(N/k)$ we extend τ to an isomorphism $\overline{N} \mapsto \overline{k}$. Then $\overline{N}$ contains a copy of M, and if we restrict the extended map to M we produce some $\sigma \in \mathrm{Gal}(M/k)$ whose restriction to N is exactly τ.

If L/k is another Galois extension containing M, then we also have $\varphi_N^L = \varphi_N^M \circ \varphi_M^L$. In paticular let K/k be a (possibly infinite) Galois extension. We can impose a directed partial order on the finite Galois subextensions of K through inclusion. It is directed as above any two fields is their compositum. Then the family of Galois groups of finite Galois subextensions, together with the homomorphisms φ_N^M detailed above define an inverse system. In fact this inverse limit this inverse system defines is $\mathrm{Gal}(K/k)$.

Proposition 5. *Let K/k be a Galois extension. Then the Galois groups of all finite Galois subextensions of K form an inverse system, and the inverse limit is isomorphic to* $\mathrm{Gal}(K/k)$. *In particular* $\mathrm{Gal}(K/k)$ *is a profinite group.*

Proof. For each finite Galois extension F/k contained in K, let $\varprojlim \mathrm{Gal}(F/k)$ be the inverse limit compatible with the homomorphisms described above. We define the map $\varphi : \mathrm{Gal}(K/k) \to \varprojlim \mathrm{Gal}(F/k)$ by sending some $\sigma \in \mathrm{Gal}(K/k)$ to $(\sigma|_F)$, the tuple of its restriction onto each F. It is clear that the image of φ always lands inside the inverse limit, and that $\varphi(\sigma\tau) = \varphi(\sigma)\varphi(\tau)$ for any $\sigma, \tau \in \mathrm{Gal}(K/k)$. This map is injective, as if $\sigma \in \mathrm{Gal}(K/k)$ is non-trivial, then for some $\alpha \in K$ we have $\sigma(\alpha) \neq \alpha$. Thus the restriction of σ to the splitting field of α is non-trivial. As the splitting field of α is finite and Galois, it follows the kernel of φ is trivial, hence φ is injective. If $(\sigma_F) \in \varprojlim \mathrm{Gal}(F/k)$ then let $\sigma \in \mathrm{Gal}(K/k)$ be so that $\sigma(\alpha) = \sigma_F(\alpha)$ if $\alpha \in F$. This is a well-defined automorphism for if $\alpha \in F_1 \cap F_2$ where both F_1, F_2 are finite Galois extensions, then $F_1 \cap F_2$ is also a finite Galois extension and by construction of the inverse limit we have

$$\sigma_{F_1}(\alpha) = \sigma_{F_1 \cap F_2}(\alpha) = \sigma_{F_2}(\alpha).$$

Clearly $\varphi(\sigma) = (\sigma_F)$, so that φ is an isomorphism as claimed. □

2.3 The Galois group as a topological group.

Interestingly enough every profinite group (and thus, any Galois group) is equipped with a natural topology. First we must define a suitable way for the group and topological structures on a set to agree.

Definition 6. A *topological group* is a topological space G, along with a group structure $(G, \cdot)$ such that the group operation

$$\mu : G \times G \to G$$

and the inversion map

$$\iota : G \to G$$

are continuous.

We can trivially make any group into a topological group by simply endowing the underlying set with the discrete topology. Assume we have done this for a family of finite groups $\{G_i\}$, and let G be the profinite group $\varprojlim G_i$. Then we can give $\prod G_i$ the product topology, and G the subspace topology. This topology on profinite groups has many interesting properties, namely, that it is Hausdorff, compact, and totally disconnected. We will need a lemma.

Lemma 7. *Let $\{G_i\}_{i \in I}$ be an inverse system of groups with the discrete topology and endow $\prod G_i$ with the product topology. Then $\varprojlim G_i$ is a closed topological subgroup of $\prod G_i$.*

Proof. We shall show the complement is open. So assume $(x_i) \notin \varprojlim G_i$. Then there are fixed $j, k \in I$ where $f_j^k(x_k) \neq x_j$. Let $p_i : \prod G_i \to G_i$ be the canonical projection maps. Then by the definition of the product topology, $p_j^{-1}(x_j)$ and $p_k^{-1}(x_k)$ are open. Their intersection is also open, contains (x_i), and has empty intersection with $\varprojlim G_i$. We are done. $\square$

Proposition 8. *A profinite group G is Hausdorff, compact, and totally disconnected.*

Proof. Clearly G is Hausdorff, for if $(x_i) \neq (y_i)$ then there is a fixed j with $x_j \neq y_j$. In this case $p_j^{-1}(x_j)$ and $p_j^{-1}(y_j)$ are disjoint open sets containing $(x_i), (y_i)$, respectively. Finite discrete groups are compact, and by Tychonoff's theorem so is their product under the product topology. As closed sets of compact sets are compact, the compactness of G follows from Lemma 7. If C is a connected subset of G, consider $p_i(C)$. This is a continuous map of a connected subset, hence its image is connected. But the connected sets of a discrete space are the singletons, so that $p_i(C)$ is a singleton for every i. This must mean C is a singleton as well, since each entry of $(x_i) \in C$ is fixed (it must be the element in $p_i(C)$). This proves G is totally disconnected, and we are done. $\square$

3 An introduction to schemes.

In attempting to relate Galois groups and fundamental groups, our discussion is inextricably rooted in relating algebraic and topological phenomena. In this section, we take a step back from specifically examining relations between Galois groups and fundamental groups to turn our attention towards how algebraic objects naturally arise from topological spaces, and vice versa.

Our end goal of this section is to give a definition of an *affine scheme*. Our intuition here should be that affine schemes form a category which is opposite, or *anti-equivalent*, to the category of commutative rings. By this we mean we would like to associate to each ring A an affine scheme, which will be denoted Spec A, and for each morphism $A \to B$ in the category of rings we would like a morphism Spec $B \to$ Spec A going in the *opposite* direction. We will first have some motivating discussion with objects which may be more familiar to the reader.

3.1 Rings of functions on a space.

Let X be some topological space. One common object of interest is the set of continuous functions from X to a field, say $\mathbb{C}$. Let us denote this set $C(X, \mathbb{C})$. Then we can impose a ring structure on $C(X, \mathbb{C})$ by simply defining addition and multiplication point-wise. That is, for $f, g \in C(X, \mathbb{C})$, we define $f + g(x) = f(x) + g(x)$ and $fg(x) = f(x)g(x)$. The zero element is the constant function 0, and the unit element is the constant function 1. In this way we can associate to each topological space a ring.

The space X and its ring of functions $C(X, \mathbb{C})$ interact in an interesting way. Specifically, let Y be another topological space with $C(Y, \mathbb{C})$ its ring of functions, and suppose $\varphi : X \to Y$ is a continuous map. Now if $f : Y \to \mathbb{C}$ is a continuous function, then $f \circ \varphi : X \to \mathbb{C}$ is continuous as well. In this way, we can think of composition with φ as sending functions in $C(Y, \mathbb{C})$ to $C(X, \mathbb{C})$. We will denote this map $\varphi^* : C(Y, \mathbb{C}) \to C(X, \mathbb{C})$, which we call the *pullback* by φ. The important thing to note that is, while φ maps from X to Y, the pullback instead maps from the functions on Y to the functions on X. In other words, a map of spaces induces a map of functions going in the *opposite direction*.

Note that this discussion does not need to be confined to continuous complex-valued functions. We could have specified another field with a topological structure, for example $\mathbb{R}$, or have considered other classes of functions, for example polynomials, differentiable functions, or smooth functions.

3.2 Points and ideals.

Continuing with the scenario above, let X be a topological space and R_X some ring of complex-valued functions on the space. If we specify some point $a \in \mathbb{C}$ then we can define a ring homomorphism $\varphi_a : R_X \to \mathbb{C}$ by defining $f \mapsto f(a)$ for each $f \in R_X$. For most rings of functions we are interested in (polynomials, continuous, differentiable, etc.) this homomorphism will be surjective. (For example, the constant function at every point is in each of these classes of functions.) As the preimage of maximal ideals under surjective homomorphisms is again maximal, it follows that $\ker \varphi_a$ will be a maximal ideal in R_X. In this way we associate to each point $a \in \mathbb{C}$ a maximal ideal $\ker \varphi_a$.

Let us look at a specific example where we take our space to be $\mathbb{C}$ and the ring of functions to be the polynomial ring $\mathbb{C}[x]$. It is well known that, for any field k, its polynomial ring $k[x]$ is a PID. Thus the maximal ideals are simply those which are generated by irreducible elements. In the case where k is algebraically closed, we know that the irreducible elements are those of the form $x - a$ for each element $a \in k$. One can see then that the maximal ideals of $\mathbb{C}[x]$ correspond bijectively with the points of $\mathbb{C}$, and in fact the ideal $(x - a)$ is exactly $\ker \varphi_a$, the set of functions which vanish at a.

We have already observed above that a map of spaces induces a map on the ring of functions going in the opposite direction via the pullback. Can we go the other way around? That is, to start with a map of rings and induce a map of spaces? Suppose R_X and R_Y are two rings of functions, and let $\varphi : R_X \to R_Y$ be a surjective ring homomorphism. One way we can get a map going "in the opposite direction" is to take preimages of ideals of R_Y under φ to get ideals of R_X. In some way, this corresponds to a map of spaces going "in the opposite direction" because as we have shown, we can associate points of Y to maximal ideals of R_Y.

Say $\mathfrak{m} \subset R_Y$ is such a maximal ideal associated with a point. Then $\varphi^{-1}(\mathfrak{m})$ is a maximal ideal of R_X. Does $\varphi^{-1}(\mathfrak{m})$ always correspond to the functions vanishing at some point of X? In general this will not be true, but it is true for some important examples, such as we saw above with $\mathbb{C}$ and $\mathbb{C}[x]$. We will see another important class of spaces and rings for which this is true in section 7 when we talk of varieties and their affine coordinate rings.

There is something else which is quite bothersome about the current set up. Namely, that by considering maximal ideals we require the homomorphism φ to be surjective, while ideally we would like to drop the surjective condition. This problem can be rectified by expanding our scope to consider not just maximal, but all prime ideals. It is with this intuition that we introduce affine schemes.

3.3 Affine schemes.

The language of schemes allows us to formally associate to each ring a topological space. This is achieved through the following construction.

Definition 9. Suppose R is a commutative ring. The (prime) *spectrum* associated with R is the set

$$\{\mathfrak{p} \mid \mathfrak{p} \subset R \text{ a prime ideal}\}$$

and is denoted Spec R.

To each spectrum we associate a topology called the *Zariski* topology. For each $S \subset R$ we let $V(S) \subset$ Spec R be the set of prime ideals containing S. The set $\{V(S)\}_{S\subset R}$ form the closed sets in the Zariski topology. For this collection to be a suitable set of closed sets, it must contain both Spec R (consider when $S = \emptyset$) and the empty set (consider when $S = R$, recall that prime ideals are defined to be proper), closed under finite unions, and closed under arbitrary intersection. This is the case, as $V(S_1) \cup V(S_2) = V(S_1S_2)$, where the general case follows by induction, and

$$\bigcap_i V(S_i) = V\left(\bigcup S_i\right).$$

Open sets in the Zariski topology will simply be of the form Spec $R \setminus V(S)$ for some $S \subset R$. An equivalent definition of the Zariski topology can be given through a basis construction.

Definition 10. For each $f \in R$ we define the *distinguished* or *basic* open set associated with f to be the set of prime ideals not containing f. It is denoted (Spec $R)_f$.

Proposition 11. *The distinguished open sets form a basis for the Zariski topology.*

Proof. Let R be a commutative ring and Spec R its spectrum. First, we note that (Spec $R)_f$ is the complement of $V(\{f\})$, so open. Next, as by definition prime ideals are proper for each prime $\mathfrak{p}$ we can always find some $f \notin \mathfrak{p}$, so that $\mathfrak{p} \in$ (Spec $R)_f$. So the distinguished open sets cover. Then note that $f, g \notin \mathfrak{p}$ is equivalent to $fg \notin \mathfrak{p}$ for any prime ideal $\mathfrak{p}$. This exactly shows

(Spec $R)_f \cap$ (Spec $R)_g$ = (Spec $R)_{fg}$. In particular, if $\mathfrak{p}$ is in the intersection of (Spec $R)_f$ and (Spec $R)_g$ then

$$\mathfrak{p} \in (\text{Spec } R)_{fg} \subset (\text{Spec } R)_f \cap (\text{Spec } R)_g.$$

This shows the distinguished sets form a basis. To show it generates the Zariski topology, observe that for some U open in the Zariski topology we have

$$U = \text{Spec } R \setminus V(S) = \text{Spec } R \setminus \bigcap_{f \in S} V(\{f\}) = \bigcup (\text{Spec } R)_f$$

for some subset $S \subset R$, completing the proof. $\square$

The spectrum of a ring R, equipped with the Zariski topology is called the *affine scheme* associated with R.

Example. The prime ideals of $\mathbb{Z}$ are those generated by prime numbers, as well as the zero ideal. Thus as a set

$$\text{Spec } \mathbb{Z} = \{(p) \mid p \in \mathbb{Z} \text{ prime}\} \cup \{(0)\}.$$

Observe that for non-zero p, the point (p) is a closed set. Indeed, it is the set $V(\{p\})$. However, this is not true of the zero ideal. In fact, there is something even more peculiar about the zero ideal—as it does not contain any non-zero p, we have $(0) \in (\text{Spec } \mathbb{Z})_p$ for every p so that $\{(0)\}$ intersects with every non-trivial basis element, hence every open set. (Note that $(\text{Spec } \mathbb{Z})_0$ is empty.) In particular its closure is the entirety of Spec $\mathbb{Z}$ so that $\{(0)\}$ is actually a dense set! Such points have a special name.

Definition 12. A point of a topological $p \in X$ is a *generic point* if its closure is X, that is, if p is dense in X.

Example. From our discussion in section 3.2 we see that

$$\text{Spec } \mathbb{C}[z] = \{(x - a) \mid a \in \mathbb{C}\} \cup \{(0)\}.$$

The affine scheme associated to $\mathbb{C}[z]$ is called the *complex affine line*, and is denoted $\mathbb{A}^1$. It also has the zero ideal as its unique generic point.

We have given the definition of *affine* schemes, how do we define schemes in general? One can think of the relation of general schemes and affine schemes as analogous to manifolds and Euclidean space. That is, while manifolds are topological spaces which locally look like Euclidean space, schemes are topological spaces which locally look like affine schemes. We will only be working with affine schemes in these notes, but we give the definition of a general scheme.

Definition 13. A topological space X is a *scheme* if it is *locally affine*. That is, if there is an covering of X by open sets $\{U_i\}$ such that each U_i is isomorphic to Spec R_i for some ring R_i.

Remark. Schemes actually have more structure than what is presented here. The full definition of a scheme includes some algebraic information on each of its open sets, called a *sheaf of rings*, or the *strcuture sheaf* on the scheme. In these notes we will remain agnostic towards sheaves, but do note that it is through sheaves that we guarantee there is a unique ring associated with each affine scheme, and thereby making affine schemes a category anti-equivalent to the category of commutative rings. Of course, given a scheme and a covering by affine schemes, the sheaf of rings on the general scheme must somehow agree with the schemes on each of the covering sets. For more, see [3] Chapter II.

4 A motivating example: The punctured plane.

This section will focus on the fundamental group of the punctured plane $\mathbb{C} \setminus \{0\}$. Recall that the only non-trivial loops in the punctured plane are ones which loop around (at least in our case) the origin. Moreover, any two loops which loop around the origin the same number of times, and with the same orientation, are homotopically equivalent. So the loop which goes around the origin once (with either orientation) will generate the entire fundamental group. From here we get

$$\pi_1(\mathbb{C} \setminus \{0\}) \cong \mathbb{Z}.$$

We will see how covers of the punctured plane correspond naturally with a certain field extension, and how the Galois group which appears connects to $\pi_1(\mathbb{C} \setminus \{0\})$. First, we introduce the notion of a branched covering:

Definition 14. A map $f : Y \to X$ between topological spaces is a *branched* or *ramified* covering if it is a covering map everywhere except on some nowhere dense set, which we call the *branch set*. Elements of the branch set are called *branch points* and the preimage of a branch point under f is a *ramification point*.

If $f : Y \to X$ is a branched covering with S its branch set, then it is easy to see that (abusing notation)

$$f : Y \setminus f^{-1}(S) \to X \setminus S$$

is a covering map. In this section we will be concerned with branched coverings of the form $f_k : \mathbb{C} \to \mathbb{C}$, where $f_k(z) = z^k$ for some $k \in \mathbb{N}$. For each non-zero $z \in \mathbb{C}$ there are exactly k preimages under this map, while 0 only has a single preimage. It is then easy to see that the branch set is $\{0\}$ and that the set of ramification points is also $\{0\}$, thus there is a covering $f_k : \mathbb{C} \setminus \{0\} \to \mathbb{C} \setminus \{0\}$. Recall that the domain of a covering map is called the *cover* while the range is the *base*.

Let us look at the case $k = 2$. If we consider the unit circle as the generator of the fundamental group, then f_2 wraps the unit circle around itself twice. Thus the image under the induced homomorphism $f_{2*} : \pi_1(\mathbb{C} \setminus \{0\}) \to \pi_1(\mathbb{C} \setminus \{0\})$ is simply $2\mathbb{Z}$. As $\mathbb{Z}$ is an abelian group, and hence every subgroup is normal, we have that f_2 is a normal covering and would expect

$$\mathrm{Deck}(f_2) \cong \mathbb{Z}/2\mathbb{Z}.$$

Indeed this is the case, as the only non-trivial deck transformation $d : \mathbb{C} \setminus \{0\} \to \mathbb{C} \setminus \{0\}$ of f_2 is given by $d(z) = -z$ which is an element of order 2.

Now we introduce Galois theory into the picture, for which we consider the field of rational functions $\mathbb{C}(z)$ over $\mathbb{C} \setminus \{0\}$. Let $\mathbb{C}(z)$ be the functions over the cover of f_2 and $\mathbb{C}(w)$ the functions over the base. Then f_2 induces a map

$$f_2^* : \mathbb{C}(w) \to \mathbb{C}(z)$$

given by the *pullback* by f_2. That is, given by $a(w) \mapsto a \circ f_2(z)$ for each $a(w) \in \mathbb{C}(w)$. Observe that this is simply $a(w) \mapsto a(z^2)$. Hence we identify $\mathbb{C}(w)$ with the subfield $\mathbb{C}(z^2)$ of $\mathbb{C}(z)$, in other words, we can establish the relation $w = z^2$, or $\sqrt{w} = z$. Then it is natural to think of $\mathbb{C}(z)$ as a field extension of $\mathbb{C}(w)$ where we adjoin $\sqrt{w}$. Concretely,

$$\mathbb{C}(z) \cong \frac{\mathbb{C}(w)[z]}{(w - z^2)} \cong \mathbb{C}(\sqrt{w}).$$

Then $\mathbb{C}(z)/\mathbb{C}(w)$ is Galois (it is the splitting field of the separable polynomial $w - z^2$) with Galois group $\mathbb{Z}/2\mathbb{Z}$. Note how Gal$(\mathbb{C}(z)/\mathbb{C}(w))$ and Deck(f_2) are isomorphic! Moreover, the non-trivial element of Gal$(\mathbb{C}(z)/\mathbb{C}(w))$ is given by $z \mapsto -z$, which is exactly the pullback of $\mathbb{C}(z)$ by the deck transformation of f_2.

For an arbitrary $k \in \mathbb{N}$ the story for f_k is essentially the same. We now have a cover of degree k, and the image of $\pi_1(\mathbb{C} \setminus \{0\})$ under f_{k*} is the subgroup $k\mathbb{Z}$, and the group of deck transformations Deck$(f_k) \cong \mathbb{Z}/k\mathbb{Z}$. Here the group of deck transformations is generated by the map $z \mapsto \zeta z$ where ζ is a primitive k-th root of unity. Again f_k will induce a pullback on the field of rational functions

$$f_k^* : \mathbb{C}(w) \to \mathbb{C}(z)$$

identifying $\mathbb{C}(w)$ with the subfield $\mathbb{C}(z^k)$, and by a similar process we find

$$\mathbb{C}(z) \cong \frac{\mathbb{C}(w)[z]}{(w - z^k)} \cong \mathbb{C}(\sqrt[k]{w})$$

where the Galois group of this extension is $\mathbb{Z}/k\mathbb{Z}$.

Every cover of $\mathbb{C} \setminus \{0\}$ corresponds to some subgroup of its fundamental group, and this subgroup uniquely (up to an equivalence of covering maps) determines the covering map. Thus the collection of covers $\{f_k\}$ is an exhaustive list. Each cover corresponds to some field extension of $\mathbb{C}(w)$, and we now consider K the compositum of all such fields. All finite Galois subextensions of K are of the form $\mathbb{C}(w)[\sqrt[k]{w}]/\mathbb{C}(w)$ for some k, and by Proposition 5 we have

$$\text{Gal}(K/\mathbb{C}(w)) \cong \varprojlim \text{Gal}(\mathbb{C}(w)[\sqrt[k]{w}]/\mathbb{C}(w)) \cong \varprojlim \mathbb{Z}/k\mathbb{Z} \cong \hat{\mathbb{Z}}.$$

In particular

$$\text{Gal}(K/\mathbb{C}(w)) \cong \pi_1(\widehat{\mathbb{C} \setminus \{0\}}\}$$

and we have related Galois groups and fundamental groups!

5 Constructing the étale fundamental group.

Here is one way to tell the story of $\pi_1(\mathbb{C} \setminus \{0\})$: To each covering space $\mathbb{C} \setminus \{0\}$ we associated a field of functions $\mathbb{C}(z)$, and to the base $\mathbb{C} \setminus \{0\}$ we associated the field of functions $\mathbb{C}(w)$. Each cover $f : \mathbb{C} \setminus \{0\} \to \mathbb{C} \setminus \{0\}$ induced a map on the associated fields

$$f^* : \mathbb{C}(w) \to \mathbb{C}(z)$$

going in the *opposite direction*. By this, we mean to observe that f^* maps functions associated with the base to functions associated with the cover. Each normal subgroup N of $\pi_1(\mathbb{C} \setminus \{0\})$ (every subgroup in our example was normal, but this will not be the case when we attempt to generalize) corresponded with such an f, and we had that

$$\pi_1(\mathbb{C} \setminus \{0\})/N \cong \text{Deck}(f).$$

Moreover, through the pullback each $\varphi \in \text{Deck}(f)$ induced an automorphism on $\mathbb{C}(z)$ which, when restricted to the image of $\mathbb{C}(w)$, acted as the identity. Through this, we found

$$\text{Deck}(f) \cong \text{Gal}(\mathbb{C}(z)/\mathbb{C}(w)).$$

Finally, by taking the inverse limits over each $\text{Gal}(\mathbb{C}(z)/\mathbb{C}(w))$ we recovered the profinite completion of $\pi_1(\mathbb{C} \setminus \{0\})$.

With the above serving as our intuition, we now attempt to construct the étale fundamental group for an affine scheme Spec A, denoted $\pi_1^{\text{ét}}(\text{Spec } A)$. Essentially, we will try to construct the étale fundamental group in such a way so that it exhibits all the similarities we outlined in section 1.1. It will also closely mirror the story above, where our first step is to consider (normal) covering maps Spec $B \to$ Spec A. Such maps correspond to a specific type of ring homomorphism.

Definition 15. A map Spec $B \to$ Spec A is a covering map if the corresponding map of rings $A \to B$ is *finite étale*.

The topic of finite étale morphisms will be discussed in section 6. For now, it suffices to understand finite étale as the algebraic condition corresponding to the topological idea of a covering map. For our definition of $\pi_1^{\text{ét}}(\text{Spec } A)$ to be consistent with what we know of Galois groups and fundamental groups, we would want each finite étale map $A \to B$ inducing a covering of Spec A to correspond with a normal subgroup N of $\pi_1^{\text{ét}}(\text{Spec } A)$. Moreover, we would want the quotient of $\pi_1^{\text{ét}}(\text{Spec } A)$ by N to be isomorphic to the deck transformations of the map $A \to B$.

Definition 16. A *deck transformation* of the ring homomorphism $\varphi : A \to B$ is an automorphism on B which acts as the identity on $\varphi(A)$. In other words, an automorphism of B as an A-algebra.

Thus we would want

$$\pi_1^{\text{ét}}(\text{Spec } A)/N \cong \text{Aut}_A(B).$$

In fact, we should expect every normal subgroup (of finite index) of the étale fundamental group to correspond with some finite étale homomorphism, and that we should have the the same isomorphism in that case. In this way, we know what every finite quotient of $\pi_1^{\text{ét}}(\text{Spec } A)$ should look like, and we simply need to force this to be the case in our definition.

Definition 17. Consider an affine scheme Spec A and its corresponding ring A. Let $\{B_i\}_{i\in I}$ be the collection of all rings such that there is a finite étale homomorphism $A \to B_i$. Then the *étale fundamental group* of Spec A is defined to be

$$\pi_1^{\text{ét}}(\text{Spec } A) := \varprojlim_{i\in I} \text{Aut}_A(B_i).$$

6 Finite étale morphisms.

6.1 Ramification.

The first condition we require for a ring homomorphism to be étale is that it must be *unramified*. One may recall from section 4 that a branched covering is also called a *ramified* cover, and indeed this is where our intuition stems from—ramified covers are explicitly not covers. Let us recall our example of

$$f_2 : \mathbb{C} \to \mathbb{C}$$

sending $z \mapsto z^2$. Here we were able to discern that f_2 was not a cover by considering preimages of points, where we noted that each point has exactly 2 preimages, while 0 has only 1. Thus we called 0 (in the domain) a *ramification point*.

As we would like to shift the focus from talking about covering maps explicitly to considering covering maps through their corresponding ring homomorphisms, our aim is to find an algebraic condition corresponding to a ramification point. Towards this end, let us first reintroduce our example through our new language of schemes. We start with the ring homomorphism

$$f_2^* : \mathbb{C}[w] \to \mathbb{C}[z]$$

defined by $w \mapsto z^2$. This corresponds to the map on schemes

$$f_2 : \text{Spec } \mathbb{C}[z] \to \text{Spec } \mathbb{C}[w]$$

by mapping prime ideals of $\mathbb{C}[z]$ to their preimages in $\mathbb{C}[w]$. Observe that every non-zero prime ideal $(w-a)$ is mapped under f_2^* to the ideal (z^2-a), which is contained in the prime ideals $(z-\sqrt{a})$ and $(z+\sqrt{a})$. Thus in the corresponding map on schemes, f_2 maps the "point" $(z-a)$ to $(w-a^2)$. If we recall the correspondence in section 3.2 between points of $\mathbb{C}$ and the maximal ideals of its polynomial ring, we see that f_2 is exactly the squaring map, sending a to a^2. Now observe that for $a \neq 0$ the ideals $(z-\sqrt{a})$ and $(z+\sqrt{a})$ are distinct, so that $(w-a)$ "splits" into the product of two prime ideals. However, the ideal (w) is sent the non-trivial power of a prime ideal, (z^2). It is this difference which motivates our algebraic definition of ramification.

Definition 18. Let $\varphi : A \to B$ be a map of rings. For some prime $\mathfrak{p} \subset B$ let $\mathfrak{q} \subset A$ be its preimage under φ, and define

$$\varphi^\sharp : A_\mathfrak{q} \to B_\mathfrak{p}$$

to be the map on local rings induced by φ. Suppose $\mathfrak{m}_\mathfrak{q}, \mathfrak{m}_\mathfrak{p}$ are the maximal ideals of $A_\mathfrak{q}, B_\mathfrak{p}$, respectively. Then we say φ *ramifies* at the prime $\mathfrak{p}$ if $\varphi^\sharp(\mathfrak{m}_\mathfrak{q})B_\mathfrak{p} \neq \mathfrak{m}_\mathfrak{q}$. A map *unramified* if it does not ramify at any prime, and if the residue field of $B_\mathfrak{p}$ is a finite separable extension of the residue field of $A_\mathfrak{q}$.

Let us see how this plays out with the squaring map, where we would expect f_2^* to ramify at the ideal (z), and nowhere else. Note that, with notation as in Definition 18, if $\mathfrak{m}_A$ is a principal ideal generated by α, then $\varphi^\sharp(\mathfrak{m}_A)B_\mathfrak{p}$ is simply the ideal generated by $\varphi^\sharp(\alpha)$. So at the prime (z), whose preimage under f_2 is (w), we have that

$$f_2^{*\sharp}((w))\mathbb{C}[z]_{(z)} = (z^2) \neq (z)$$

so indeed f_2 ramifies at (z). However, at a prime $(z-a)$ for $a \neq 0$, whose preimage is $(w - a^2)$, we instead get

$$f_2^{*\sharp}((w-a^2))\mathbb{C}[z]_{(z-a)} = (z^2 - a^2) = (z-a)$$

since $z + a$ is a unit in $\mathbb{C}[z]_{(z-a)}$, and thus f_2^* is unramified away from (z) as expected.

Our "solution" to the fact that the squaring map was unramified, and hence not a covering map, was to simply remove the ramification point, thereby giving a cover $\mathbb{C} \setminus \{0\} \to \mathbb{C} \setminus \{0\}$. In our algebraic analogue, our map ramifies at (z) in $\mathbb{C}[z]$. Is there a way we can "get rid of the ramification point"? It turns out there is, and the trick is to invert z! That is, to consider the ring $\mathbb{C}[z][1/z]$. Indeed, once z is inverted, the ideal (z) becomes the unit ideal, and we no longer consider it in the prime spectrum. We have essentially "gotten rid" of the problematic point (z). And indeed, once can see that the prime ideals of $\mathbb{C}[z][1/z]$ are still of the form $(z - a)$, but now only for $a \neq 0$. Thus the map $\mathbb{C} \setminus \{0\} \to \mathbb{C} \setminus \{0\}$ corresponds to the map

$$\mathbb{C}[w]\left[\frac{1}{w}\right] \to \mathbb{C}[z]\left[\frac{1}{z}\right]$$

which one can check is unramified, essentially with the same argument which showed the map $\mathbb{C}[w] \to \mathbb{C}[z]$ is unramified away from (z).

6.2 Flatness.

The second condition we need for being étale is the notion of flatness.

Definition 19. Let R be a commutative ring. The *Krull dimension* of R is the length n of the longest chain of prime ideals

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n.$$

For an affine scheme $X = \text{Spec } R$, its dimension is the Krull dimension of R. For each closed point $x \in X$, there is also a notion of the *dimension at* x, denoted $\dim_x X$. Each point of X corresponds to a prime ideal $\mathfrak{p}$ of R, and $\dim_x X$ is defined similarly to the Krull dimension only instead, with notation as in Definition 19, we take $\mathfrak{p}_n = \mathfrak{p}$.

Definition 20. Let $f : X \to Y$ be a map of schemes. Then f is *flat* if for all $x \in X$ and $y = f(x)$, we have

$$\dim_x X = \dim_y Y + \dim_x f^{-1}(y).$$

A ring homomorphism $A \to B$ is flat if its corresponding map on affine schemes is flat.

Remark. This is not the general definition of flatness, but it is equivalent in every case we will be considering here.

Here is an example of why flatness is needed. Consider the canonical projection map $\mathbb{C}[x] \to \mathbb{C}[x]/(x)$. Note that Spec $\mathbb{C}[x]/(x)$ has a single point, corresponding to the zero ideal, so the corresponding map is simply $\{(0)\} \to \mathbb{A}^1$, which is certainly not a map we would want to consider a covering. But it is clear to see that this map is unramified—the maximal ideal when $\mathbb{C}[x]/(x)$ is localized at (0) is again the zero ideal, which evidently will be mapped onto. However, this map is not flat. To see this, observe that the preimage of (0) under the projection map is (x). So we would need

$$\dim_{(0)}\text{Spec } \mathbb{C}[x]/(x) = \dim_{(x)}\mathbb{A}^1 + \dim_{(0)}(0)$$

but $\dim_{(0)}\text{Spec } \mathbb{C}[x]/(x) = 0$ while $\dim_{(x)}\mathbb{A}^1 = 1$.

Another example to consider is the map $\mathbb{C}[x, y] \to \mathbb{C}[x]$ where we send a polynomial $p(x, y) \mapsto p(x, 0)$. Note that the preimage of the ideal generated by $x - a$ in $\mathbb{C}[x]$ is still the ideal generated by $x - a$ in $\mathbb{C}[x, y]$, we can think about this map as the inclusion $\mathbb{A}^1 \hookrightarrow \mathbb{A}^2$. Again, this map is unramified yet we would not want to consider it a covering. We see this fails the flatness condition as $\dim_{(x-a)}(\mathbb{A}^1) = 1$, while $\dim_{(x-a)}(\mathbb{A}^2) + \dim_{(x-a)}(x - a) = 2$.

Definition 21. A map of rings is *étale* if it is unramified and flat.

6.3 Finiteness.

We have tackled the étale condition of a finite étale morphism, and we now introduce the condition of being *finite*.

Definition 22. A map of rings $\varphi : A \to B$ is *finite* if φ makes B a finitely generated A-module.

It is really this finiteness condition which guarantees that the corresponding map on schemes is actually a covering. We will illustrate through an example. Consider the canonical inclusion map

$$\mathbb{A}^1 \setminus \{(z)\} \hookrightarrow \mathbb{A}^1.$$

As we have previously showed, the left corresponds to Spec $\mathbb{C}[z][1/z]$ while the right is defined to be Spec $\mathbb{C}[z]$. So this corresponds to the ring homomorphism

$$\mathbb{C}[z] \hookrightarrow \mathbb{C}[z]\left[\frac{1}{z}\right]$$

which is an étale map, yet clearly the inclusion $\mathbb{A}^1 \setminus \{(z)\} \hookrightarrow \mathbb{A}^1$ is not a covering, it is not even surjective. This is precisely because $\mathbb{C}[z][1/z]$ is not a finitely generated $\mathbb{C}[z]$ module. To see this, take any finite set $f_1, \ldots, f_n \in \mathbb{C}[z][1/z]$. Each f_i will have some power of z in its denominator, and we can choose an n that is larger than any of those powers. Then the f_i cannot possibly generate the element $1/z^n$, which shows that no finite set can generate all of $\mathbb{C}[z][1/z]$.

There is a slightly stronger condition to being finite, and that is a map which is *finitely presented*. Now, for any finitely generated A-module B (say B is generated by n elements) there is a surjective morphism $A[x_1, \ldots, x_n] \to B$, where each x_i is sent to a generator of B. The kernel of this morphism is an ideal, and we say that B is *finitely presented* over A if this ideal is finitely generated. It should be evident that finitely presented maps are also finite. This distinction will not be too important for our purposes, as we will mainly be looking at cases where A, hence any finite polynomial ring over it, is a Noetherian ring, so that this condition is trivially satisfied.

7 Varieties.

7.1 Varieties and ideals.

Definition 23. A *complex affine variety* is the common zero set in $\mathbb{C}^n$ of a collection of complex polynomials $\{f_i\}_{i\in I}$. Here each $f_i \in \mathbb{C}[x_1, \ldots, x_n]$. For the set of polynomials $\{f_i\}$ we denote the associated affine variety by

$$\mathbb{V}(\{f_i\}) \subset \mathbb{C}^n.$$

If V is an affine variety, then a subset $V' \subset V$ is a *subvariety* if there exists an affine variety W such that $V' = V \cap W$.

Definition 24. Let $F : \mathbb{C}^n \to \mathbb{C}^m$ be a *polynomial map*, by which we mean a map

$$F(x) = (f_1(x), \ldots, f_m(x))$$

where each f_i is a polynomial in n variables. If $V \subset \mathbb{C}^n$ and $W \subset \mathbb{C}^m$ are affine varieties, then $f : V \to W$ is a *morphism of affine varieties* if it is the restriction of a polynomial map $F : \mathbb{C}^n \to \mathbb{C}^m$ to V.

Each variety $V \subset \mathbb{C}^n$ associates to an ideal of $\mathbb{C}[x_1, \ldots, x_n]$ in a natural way, constructed by defining

$$\mathbb{I}(V) = \{f \in \mathbb{C}[x_1, \ldots, x_n] \mid f(x) = 0, \forall x \in V\}.$$

Note that if two polynomials f, g vanish on a set $S \subset \mathbb{C}^n$, and h an arbitrary polynomial, then $h(f+g)$ vanishes on S also, establishing that $\mathbb{I}(V)$ is an ideal.

What is interesting to observe about the ideal $\mathbb{I}(V)$ is when we take $\mathbb{V}(\mathbb{I}(V))$. Now by definition, every polynomial in $\mathbb{I}(V)$ vanishes on V, hence $V \subset \mathbb{V}(\mathbb{I}(V))$. On the other hand, V is defined by a set of polynomials, say $V = \mathbb{V}(\{f_i\})$. Then $\{f_i\} \subset \mathbb{I}(V)$, which gives $\mathbb{V}(\mathbb{I}(V)) \subset V$, and we conclude

$$\mathbb{V}(\mathbb{I}(V)) = V.$$

One upshot of considering ideals associated with an affine variety comes from the fact that $\mathbb{C}[x_1, \ldots, x_n]$ is Noetherian, that is, its ideals are finitely generated. Hence for a variety V, there are polynomials $f_1, \ldots, f_k \in \mathbb{C}[x_1, \ldots, x_n]$ with

$$\mathbb{I}(V) = (f_1, \ldots, f_k).$$

In particular

$$V = \mathbb{V}(\mathbb{I}(V)) = \mathbb{V}(\{f_1, \ldots, f_k\})$$

so that we only need to consider the zero sets of a finite number of polynomials to define any variety.

Now we observe that an ideal $I \subset \mathbb{C}[x_1, \ldots, x_n]$ is a set of functions, so we can consider $\mathbb{V}(I)$. Given that we already have $\mathbb{V}(\mathbb{I}(V)) = V$, we naturally ask ourselves, do we also have $\mathbb{I}(\mathbb{V}(I)) = I$? This is not true in general. For example, take the ideal $I = (x^2)$ in $\mathbb{C}[x]$. Then $\mathbb{V}(I) = \{0\}$, but $\mathbb{I}(\mathbb{V}(I))$ is the ideal (x), not (x^2). We can, however, get something pretty close, due to the ideals $\mathbb{I}(V)$ being of a special type.

Definition 25. Let R be a commutative ring. For an ideal $\mathfrak{a} \subset R$, the *radical* of $\mathfrak{a}$, denoted $\sqrt{\mathfrak{a}}$, is the set of all $r \in R$ such that $r^n \in \mathfrak{a}$ for some $n \in \mathbb{N}$. If $\mathfrak{a} = \sqrt{\mathfrak{a}}$ we say $\mathfrak{a}$ is a *radical ideal*.

Proposition 26. *The radical of an ideal is an ideal.*

Proof. Let notation be as in Definition 25. Then recall that an element $r \in R$ is *nilpotent* if $r^n = 0$ for some n. The set of all nilpotent elements is denoted nil R and is called the *nilradical* of a ring R. Now nil R is an ideal, for suppose $r, s \in$ nil R with $r^n = 0$ and $s^m = 0$. Then $(r+s)^{n+m} = 0$ (expand with the binomial theorem) and for some arbitrary $a \in R$ we have $(ar)^n = 0$.

Now $r \in \sqrt{\mathfrak{a}}$ means that $r^n \in \mathfrak{a}$ for some n, equivalently $r^n + \mathfrak{a} = \mathfrak{a}$. We can rewrite

$$r^n + \mathfrak{a} = (r + \mathfrak{a})^n.$$

But then, letting $\pi : R \to R/\mathfrak{a}$ being the canonical projection map, this means $\pi(r) \in$ nil $R/\mathfrak{a}$. In fact, from the above it is clear to see that if $\pi(r) \in$ nil $R/\mathfrak{a}$ then $r \in \sqrt{\mathfrak{a}}$. Thus $\mathfrak{a}$ is the preimage of the ideal nil $R/\mathfrak{a}$ under the ring homomorphism π, so it too is an ideal. $\square$

The ideal $\mathbb{I}(V)$ is a radical ideal. Indeed, suppose $f^n \in \mathbb{I}(V)$ for some $n \in \mathbb{N}$, i.e., that f^n vanishes at every point of V. Then we must also have that f vanishes at every point of V, for $\mathbb{C}$ is integral and thus the power of a non-zero element is never zero. The important observation is that every radical ideal I is also of the form $\mathbb{I}(V)$ for some variety V. This is presented as follows.

Theorem 27 (Hilbert's Nullstellensatz)**.** *For an ideal $I \subset \mathbb{C}[x_1, \ldots, x_n]$, we have*

$$\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}.$$

In particular, if I is radical then

$$\mathbb{I}(\mathbb{V}(I)) = I.$$

First, we prove a lemma.

Lemma 28 (Weak Nullstellensatz)**.** *Let I be an ideal of $\mathbb{C}[x_1, \ldots, x_n]$. Then $\mathbb{V}(I) = \emptyset$ if and only if $I = (1)$.*

Proof. Clearly $\mathbb{V}((1)) = \emptyset$. Suppose $I \neq (1)$. As $\mathbb{C}[x_1, \ldots, x_n]$ is Noetherian, I is finitely generated, say by $f_1, \ldots, f_n$. Then $\gcd(f_1, \ldots, f_n) \neq 1$ by assumption, so there is some polynomial dividing each of them. This polynomial has a root as $\mathbb{C}$ is algebraically closed, so that $\mathbb{V}(I) \neq \emptyset$. □

Proof of Hilbert's Nullstellensatz. The discussion above shows $\sqrt{I} \subset \mathbb{I}(\mathbb{V}(I))$. (One can also see this by observing the radical of I is always the smallest radical ideal containing I.) So suppose $f \in \mathbb{I}(\mathbb{V}(I))$. We use a trick that is due to Rabinowitsch, where we consider a new variable y and the ring $\mathbb{C}[x_1, \ldots, x_n, y]$. Note $1 - fy$ cannot possibly share a zero with any element of I (considered as an ideal in $\mathbb{C}[x_1, \ldots, x_n, y]$) so that the ideal J generated by $1 - fy$ and I must be the unit ideal by the Weak Nullstellensatz. Supposing I were generated by $h_1, \ldots, h_m$, then there are polynomials $g_i \in \mathbb{C}[x_1, \ldots, x_n, y]$ with

$$1 = g_0(1 - yf) + g_1 h_1 + \cdots g_m h_m.$$

This equality still holds if we were to substitute y with f^{-1}, where we may now have powers of f in the denominator on the right hand side. Multiplying by a sufficiently large power of f to clear these denominators shows that $f^k \in I$ for some power, hence $f \in \sqrt{I}$, completing the proof. □

7.2 The Zariski topology.

We observe that the union of two subvarieties of $\mathbb{A}^n$ is again a variety. Indeed, if $\{f_i\}_{i \in I}$ and $\{f_j\}_{j \in J}$ are two collections of polynomials then we have

$$\mathbb{V}(\{f_i\}_{i \in I}) \cup \mathbb{V}(\{f_j\}_{j \in J}) = \mathbb{V}(\{f_i f_j\}_{(i,j) \in I \times J}).$$

By induction, the union of finitely many varieties is also a variety. Next, the arbitrary intersection of varieties is also a variety. Indeed suppose $\{I_\alpha\}$ is a collection of indexing sets and I their union. Then

$$\bigcap_\alpha \mathbb{V}(\{f_i\}_{i\in I_\alpha}) = \mathbb{V}(\{f_i\}_{i\in I}).$$

Finally, we note that all of $\mathbb{C}^n$ is a variety (consider the variety defined by the constant zero function) and the empty set is also a variety (consider the variety defined by any non-zero constant function). In particular, if we take the set of all complements of varieties, then this set would contain $\mathbb{C}^n$ and the empty set, be closed under arbitrary unions, and closed under finite intersections. This proves the following.

Proposition 29. *The set of all complements of varieties defines a topology on* $\mathbb{C}^n$.

As we will see in section 7.3, it turns out that this topology is the Zariski topology. To distinguish between $\mathbb{C}^n$ with its usual topology, we denote the set $\mathbb{C}^n$ with the Zariski topology by $\mathbb{A}^n$, the *affine n-space*. Recall that Spec $\mathbb{C}[z]$ is also denoted $\mathbb{A}^1$. This is no coincidence, and will also be explained in the section 7.2.

We now introduce a notion of dimension for varieties.

Definition 30. A variety V is *irreducible* if it cannot be written as the union of two non-empty subvarieties.

Definition 31. The *dimension* of a variety V is the length n of the longest chain of irreducible subvarieties

$$V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_n.$$

For some $x \in V$ the *dimension at x* is the longest chain of irreducible subvarieties where $V_0 = \{x\}$. These are denoted dim V and dim$_x V$, respectively.

One may notice that this formulation of dimension is similar to the definition of the Krull dimension. In fact, it is essentially equivalent, as there is a bijective correspondence between irreducible varieties and prime ideals of $\mathbb{C}[x_1, \ldots, x_n]$.

Proposition 32. *For an irreducible variety V, the ideal $\mathbb{I}(V)$ is prime. Conversely, a variety $\mathbb{V}(I)$ defined by a prime ideal I is irreducible.*

Proof. Suppose $\mathbb{I}(V)$ is not prime, that is, there are $f, g \notin \mathbb{I}(V)$ but $fg \in \mathbb{I}(V)$. Then consider the ideals $(f) + \mathbb{I}(V)$ and $(g) + \mathbb{I}(V)$. By our choice of f, there must be a point of V on which f does not vanish, and thus this point will not be in the common zero set of $(f) + \mathbb{I}(V)$. We conclude $\mathbb{V}((f) + \mathbb{I}(V))$ is a proper non-trivial subvariety of V, and similarly for $\mathbb{V}((g) + \mathbb{I}(V))$. But now

$$\mathbb{V}((f) + \mathbb{I}(V)) \cup \mathbb{V}((g) + \mathbb{I}(V)) = \mathbb{V}(\mathbb{I}(V) + (fg)) = \mathbb{V}(\mathbb{I}(V)) = V$$

so that V is reducible, and the first statement follows by the contrapositive.

Now assume $\mathbb{V}(I)$ is reducible. Then write $\mathbb{V}(I) = V_1 \cup V_2$ for proper non-trivial subvarieties V_1, V_2. Choosing $f \in \mathbb{I}(V_1) \setminus \mathbb{I}(V_2)$ and $g \in \mathbb{I}(V_2) \setminus \mathbb{I}(V_1)$ we see that fg vanishes on $\mathbb{V}(I)$, hence is in $\mathbb{V}(I)$. But neither f nor g vanishes on both V_1, V_2, hence $f, g \notin \mathbb{I}(V)$. Thus $\mathbb{V}(I)$ is not prime, and the proof is complete. □

Remark. Just as we do not normally consider the unit ideal to be prime, we do not usually consider the empty set to be an irreducible set.

7.3 Affine coordinate rings.

At this point, it should come as no surprise that we are interested in considering rings of functions over varieties. So let $V \subset \mathbb{C}^n$ be a variety and $f \in \mathbb{C}[x_1, \ldots, x_n]$. Then the restriction of f to V defines a function $V \to \mathbb{C}$, and through defining addition and multiplication pointwise (as in section 3.1), this set of functions defines a ring $\mathbb{C}[x_1, \ldots, x_n]|_V$. We denote this ring $A(V)$, and call it the *affine coordinate ring* of V.

Now consider some $f \in \mathbb{C}[x_1, \ldots, x_n]$ and $g \in \mathbb{I}(V)$. Then we observe that $f|_V = (f+g)|_V$. In particular, the kernel of the natural surjection

$$\mathbb{C}[x_1, \ldots, x_n] \twoheadrightarrow A(V)$$

is exactly $\mathbb{I}(V)$ and we obtain the isomorphism

$$A(V) \cong \mathbb{C}[x_1, \ldots, x_n]/\mathbb{I}(V).$$

The affine coordinate ring allows us to explain why we use $\mathbb{A}^1$ to both denote the variety defined by the constant 0 function, as well as the scheme associated with $\mathbb{C}[z]$. From the definition of affine coordinate ring, we see that $A(\mathbb{A}^1)$ is exactly $\mathbb{C}[z]$. There is, however, one small difference between $\mathbb{A}^1$ the variety and Spec $\mathbb{C}[z]$—when we consider $\mathbb{A}^1$ as a variety, we do not consider the generic point of Spec $\mathbb{C}[z]$. Recall from our discussion in Section 3.3 on how every point in Spec $\mathbb{C}[z]$ is closed except for the generic point. More generally, for some point in an affine scheme $\mathfrak{p} \in$ Spec R its closure consists of all $\mathfrak{q}$ where, as ideals, $\mathfrak{p} \subset \mathfrak{q}$. Thus it follows that a point is closed if and only if it is maximal. This is exactly the link between the scheme associated to an affine coordinate ring and the associated variety. As maximal ideals of the coordinate rings correspond to the points of the variety, what we have shown is the following.

Proposition 33. *Let V be a variety and $A(V)$ its affine coordinate ring. Then the points of V exactly correspond to the closed points of* Spec $A(V)$.

Let us take a closer look at the structure of an affine coordinate ring $A(V)$. First, we observe that affine coordinate rings have a $\mathbb{C}$-algebra structure, given by composing the inclusion map $\mathbb{C} \to \mathbb{C}[x_1, \ldots, x_n]$ and the projection map $\mathbb{C}[x_1, \ldots, x_n] \to A(V)$. It is also clear to see that the images of $x_1, \ldots, x_n$ under the projection to $A(V)$ generate $A(V)$ as a $\mathbb{C}$-algebra, so that affine coordinate rings are finitely generated. Finally, affine coordinate rings are *reduced*, that is, they have no nilpotent elements. This comes from the fact that $A(V)$ is isomorphic to $\mathbb{C}[x_1, \ldots, x_n]/\mathbb{I}(V)$ and $\mathbb{I}(V)$ is radical. Thus, if $f^n = 0$ for some $f \in A(V)$ this must mean $f^n \in \mathbb{I}(V)$, hence $f \in \mathbb{I}(V)$ and $f = 0$ in $A(V)$. (Here we abuse notation, identifying some $f \in \mathbb{C}[x_1, \ldots, x_n]$ with its image in $A(V)$.) In fact, these three properties fully characterize affine coordinate rings.

Proposition 34. *Any finitely-generated reduced $\mathbb{C}$-algebra R is isomorphic to the affine coordinate ring of some variety.*

Proof. Let $r_1, \ldots, r_n$ be the generators of R as a $\mathbb{C}$-algebra. Then the map

$$\varphi : \mathbb{C}[x_1, \ldots, x_n] \to R$$

defined by $x_i \mapsto r_i$ is a surjection. As R is reduced, then by a similar argument presented above, it follows that ker φ is radical. Thus ker φ defines a variety whose affine coordinate ring is exactly

$$\mathbb{C}[x_1, \ldots, x_n]/\text{ker } \varphi \cong R$$

as desired. □

Up until now, we have abstractly hinted at the fact that a map of rings $A \to B$ corresponds to a map Spec $B \to$ Spec A. We will now explicitly see how maps of coordinate rings induce maps on their associated varieties. We first note that the way maps on varieties induce a map on their coordinate rings is similar to what has been previously discussed—through the pullback. Explicitly, given a morphism of varieties $f : V \to W$, we define a map of coordinate rings $A(W) \to A(V)$ defined by $g \mapsto g \circ f$. It is easy to check this map is a $\mathbb{C}$-algebra homomorphism.

What is more interesting is considering a map $\varphi : A(W) \to A(V)$ and producing a map on varieties. Suppose $V \subset \mathbb{A}^n$ and $W \subset \mathbb{A}^m$, then our goal is to produce a polynomial map $\mathbb{A}^n \to \mathbb{A}^m$ whose restriction to V lands in W and whose pullback is φ. Let us look at our map as

$$\varphi : \frac{\mathbb{C}[y_1, \ldots, y_m]}{\mathbb{I}(W)} \to \frac{\mathbb{C}[x_1, \ldots, x_n]}{\mathbb{I}(V)}.$$

Then for each i, the image $\varphi(y_i)$ is represented by some polynomial f_i in n variables. Then consider the polynomial map $F : \mathbb{A}^n \to \mathbb{A}^m$ defined by $x \mapsto (f_1(x), \ldots, f_m(x))$. We claim that $F(v) \in W$ for all $v \in V$. Indeed, consider any polynomial $p \in \mathbb{I}(W)$. Then

$$p(F(v)) = p(f_1(v), f_2(v), \ldots, f_m(v)) = p(\varphi(y_1)(v), \varphi(y_2)(v), \ldots, \varphi(y_m)(v)) = \varphi(p)(v).$$

This line of equalities is a bit hard to digest, so lets take the explicit example $p = y_1 + y_2$ to see it play out. Then $\varphi(p) = \varphi(y_1) + \varphi(y_2)$ so that

$$\varphi(p)(v) = \varphi(y_1)(v) + \varphi(y_2)(v) = f_1(v) + f_2(v).$$

But then we see the latter-most expression is just $p(f_1(v), f_2(v)) = p(F(v))$. Now, as $p \in \mathbb{I}(w)$, then $p \equiv 0 \bmod \mathbb{I}(W)$, and as φ is a homomorphism we must have $\varphi(p) \equiv 0 \bmod \mathbb{I}(V)$. Thus we have $p(F(v)) = \varphi(p)(v) = 0$. What we have shown is that $F(v)$ is in the common zero set of $\mathbb{I}(W)$ for every $v \in V$. In other words, $F(v) \in \mathbb{V}(\mathbb{I}(W)) = W$. Note that $p(F(v)) = \varphi(p)(v)$ is also saying the pullback by F is φ, thus F is exactly the polynomial map we are looking for.

8 Some étale fundamental groups.

In this section we will give some explicit examples of étale fundamental groups, including seeing how they relate to Galois groups and topological fundamental groups. The task of computing étale fundamental groups is a difficult one, and many of even the simplest examples require number theory and other machinery that is neither covered here, nor would be normally seen in an undergraduate curriculum. However, outside of those methods and theorems which we will cite here without proof, the reader should be at this point comfortable enough with the general ideas to see how the étale fundamental group appears in each of the following examples.

Example. For a field k, suppose Spec $K \to$ Spec k is a covering. Then this corresponds to a finite étale map $k \to K$. If K were not a field, then it has some non-zero maximal ideal $\mathfrak{m}$, whose preimage is some proper ideal in k, hence to zero ideal. But then in the corresponding map on local rings $k \to K_{\mathfrak{m}}$ the image of the zero ideal generates the zero ideal, and not the maximal ideal of $K_{\mathfrak{m}}$ so this map ramifies, contradicting the fact that $k \to K$ is finite étale. We conclude K is a field as well. The fact that $k \to K$ is unramified further means that the map on residue fields gives a finite separable extension. But the residue field of a field is just the field itself, thus a morphism $k \to K$ is finite étale only when K is a finite separable extension of k. Then K is Galois over k and the automorphisms on K which fix k are exactly the elements of Gal(K/k), thus we have

$$\pi^{\text{ét}}(\text{Spec } k) = \varprojlim \text{Gal}(K/k)$$

where the inverse limit is taken over all finite separable extensions. This shows that the étale fundamental group of Spec k for any field k is simply the absolute Galois group of k. For a more explicit example, suppose k were $\mathbb{F}_q$, the finite field with q elements. Then the finite separable extensions of $\mathbb{F}_q$ are of the form $\mathbb{F}_{q^n}$, and each Gal$(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is cyclic of order n, generated by the Frobenius automorphism. Thus for finite fields,

$$\pi^{\text{ét}}(\text{Spec } \mathbb{F}_q) = \hat{\mathbb{Z}}.$$

Example. The link between topological fundamental groups and étale fundamental groups is given through the *Riemann Existence Theorem*. In section 4 we saw how covers of $\mathbb{C} \setminus \{0\}$ correspond to certain Galois extensions of $\mathbb{C}(z)$. The Riemann Existence Theorem tells us that these covers also correspond to the finite étale maps out of $\mathbb{C}[z][1/z]$, which corresponds to $\mathbb{C} \setminus \{0\}$ as we saw in section 6.1. In particular, if K is the composite of all fields above $\mathbb{C}(w)$ corresponding to a cover of $\mathbb{C} \setminus \{0\}$, then

$$\text{Gal}(K/\mathbb{C}(w)) \cong \pi^{\text{ét}}(\text{Spec } \mathbb{C}[z][1/z]).$$

We saw in section 4 that Gal$(K/\mathbb{C}(w)) \cong \pi_1(\widehat{\mathbb{C} \setminus \{0\}})$, so that the étale fundamental group is just the profinite completion of the ordinary topological fundamental group.

In fact, in a more general setting, if S is any finite subset of $\mathbb{C}$, then Riemann's Existence Theorem says that a topological covering of $\mathbb{C} \setminus S$ corresponds to some field extension of $\mathbb{C}(w)$, and again the étale fundamental group arises as the profinite completion of the ordinary topological fundamental group. From here, we get that

$$\pi^{\text{ét}}(\mathbb{C} \setminus S) \cong \widehat{\mathbb{Z}^n}$$

where $|S| = n$. Note that the coordinate ring of $\mathbb{C} \setminus S$ would be

$$\mathbb{C}[z]\left[\frac{1}{(z-a_1)(z-a_2)\cdots(z-a_n)}\right]$$

where $S = \{a_i\}_{i=1}^n$. One can see this by the same logic presented in section 6.1, where by inverting the element $(z - a_1)$ we are essentially "getting rid of the point" a_1.

In its fullest generality, we do not just consider the complex plane punctured at a number of points, but any affine variety. Here Riemann's Existence Theorem tells us that, given a variety V and its affine coordinate ring $A(V)$, then all topological covers of V correspond to finite étale maps $A(V) \to B$, giving us the isomorphism

$$\pi^{\text{ét}}(\text{Spec } A(X)) \cong \widehat{\pi_1(V)}.$$

Example. We call a finite separable extension K of $\mathbb{Q}$ a *number field*. An element of a number field which is the root of a monic polynomial with integer coefficients is called an *algebraic integer*. The set of all algebraic integers in a number field form a ring, called the *ring of integers*, and is usually denoted $\mathcal{O}_K$. For example, the ring of integers in $\mathbb{Q}$ is simply $\mathbb{Z}$. The ring of integers in $\mathbb{Q}(i)$ is $\mathbb{Z}[i]$, since i satisfies the polynomial $x^2 + 1$. It happens that if $\mathbb{Z} \to A$ is a finite étale morphism, then A is isomorphic to the ring of integers of some number field. This fact, combined with the following theorem, gives an interesting result.

Theorem 35 (Minkowski)**.** *Any non-trivial finite extension of $\mathbb{Q}$ ramifies at some prime $p \in \mathbb{Z}$.*

What this theorem from Minkowski implies is that there are no non-trivial unramified extensions of $\mathbb{Z}$, i.e., if $\mathbb{Z} \to A$ is a finite étale map, then $A = \mathbb{Z}$. It follows that $\pi^{\text{ét}}(\text{Spec } \mathbb{Z})$ is trivial.

Example. Consider the rings $A = \mathbb{Z}[\sqrt{-3}]$ and $B = \mathbb{Z}[x]/(x^4 + x^2 + 1)$. Let α be the image of x in B, and consider B as an A-algebra through the ring homomorphism $A \to B$ defined by $\sqrt{-3} \mapsto \alpha - \alpha^{-1}$. This is a finite étale map, and note that $\alpha^{-1} = -x^3 - x$ so that

$$\alpha - \alpha^{-1} = x^3 + 2x.$$

Also,

$$(x^3 + 2x)^2 = x^6 + 4x^4 + 4x^2 \equiv -3 \text{ mod } (x^4 + x^2 + 1)$$

so that our homomorphism is well-defined. There is a non-trivial automorphsim on B as an A-algebra defined by sending $\alpha \mapsto -\alpha^{-1}$ so that $\text{Aut}_A(B)$ is non-trivial, and in particular this implies that the étale fundamental group of Spec A is non-trivial. We do not have the tools to explicitly calculate this group, although it turns out that we have

$$\pi^{\text{ét}}(\text{Spec } \mathbb{Z}[\sqrt{-3}]) \cong \mathbb{Z}/2\mathbb{Z}.$$

References

[1] D. Corwin. *Galois Groups and Fundamental Groups*. University of Berkeley, 2020.

[2] D. Eisenbud and J. Harris. *The Geometry of Schemes*. Springer-Verlag New York, Inc., 2000.

[3] R. Hartshorne. *Algebraic Geometry*. Springer Science+Business Media, Inc., 1977.

[4] S. Lang. *Algebra 3rd ed.* Addison-Wesley Publishing Company, 1993.

[5] H.W. Lenstra. *Galois Theory for Schemes*. Universiteit Leiden, 2008.

[6] J. Munkres. *Topology 2nd ed.* Pearson Education Limited, 2014.

[7] K.E. Smith et al. *An Invitation to Algebraic Geometry*. Springer Science+Business Media New York, 2000.

[8] T. Szamuely. *Galois Groups and Fundamental Groups*. Cambridge University Press, 2009.