Chapter 1

Galois Groups and Fundamental Groups

1.1 Galois Groups and Fundamental Groups

This begins a series of lectures on topics surrounding Galois groups, fundamental groups, étale fundamental groups, and étale cohomology groups. These underly a lot of deep relations between topics in topology and (algebraic) number theory, which in turn constitute an important part of modern arithmetic geometry.

Our motivating idea is this: two theories, one in algebra, the other in topology, look remarkably similar. These are the theories of Galois groups and field extensions and of fundamental groups and covering spaces. We begin by reviewing these similarities.

In the case of Galois groups, we have, given a Galois extension L/K of fields, a correspondence between subgroups of the Galois group $\mathrm{Gal}(L/K)$ and intermediate field extensions

$$L/M/K.$$

(In particular, if L is the [separable] algebraic closure $\overline{K}$, then the intermediate extensions correspond to *all* algebraic extensions of K, and the Galois group is the *absolute Galois group* of K.) One subgroup is contained within another iff there is an inclusion of fields going the other direction. The whole group corresponds to K, and the trivial subgroup corresponds to L. There is a notion of degree of an extension (it is the dimension of one field as a vector space over the other), and if the extension has finite degree over K, then the degree equals the index of the corresponding subgroup. Finally, the subgroup is normal iff the corresponding field extension is normal, and there is an isomorphism between the quotient of the Galois group by the corresponding subgroup and the automorphisms of the field extension. Finally, a field extension is separably closed (if you're not used to this, this is the same as algebraically closed in characteristic 0) iff it has no separable extensions, which is to say that its absolute Galois group is trivial.

In the case of fundamental groups, we have a correspondence between subgroups of the fundamental group $\pi_1(X)$ of a space X (I will always ignore basepoints and assume the space is connected) and connected covers

$$Y \to X.$$

(In this case, the universal cover is analogous to the separable algebraic closure of the field.) One subgroup is contained in another iff one cover dominates the other. The whole group corresponds to X, and the trivial subgroup corresponds to its universal cover $\tilde{X}$. There is a notion of degree of a cover (it is the number of preimages of any point), and if the cover has finite degree, then the degree equals the index of the corresponding subgroup. Finally the subgroup is normal iff the corresponding cover is normal, and there is an isomorphism between the quotient of the fundamental group by the corresponding subgroup and the deck transformations (i.e. automorphisms respecting the projection to X) of the cover. Finally, a space is simply connected iff it has no connected covers, which is to say that its fundamental group is trivial.

This is a nice analogy. But is it just an analogy? They clearly have the same formal properties. But more deeply, could we find some sort of function associating a group of some class of objects, such that fields and spaces are contained within that class of objects, and such that that function assigns to a space is fundamental group and to a field its (absolute) Galois group? Secondly, could we find some object in between a space and a field, so that Galois groups and fundamental groups are intertwined.

We shall give at least partial answers to both questions. As we shall see, it is very related to the following question. Suppose the space $X \subseteq \mathbb{C}^n$ is the solution set to a system of polynomial equations in n variables (or more generally, a complex algebraic variety, possibly projective). For example, consider surfaces in $\mathbb{C}^2$ cut out by the equations

$$xy - 1 = 0$$

and

$$y^2 = x^3 + ax + b.$$

The first is isomorphic to $\mathbb{C} \setminus \{0\}$, which has fundamental group $\mathbb{Z}$, and the second is a punctured torus. Then can we find the fundamental groups of this objects by purely algebraic means? The answer is partially yes, as we shall see in the next lecture. We shall also see that if such a space is defined by equations with coefficients in $\mathbb{Q}$ (or more generally some finite extension K of $\mathbb{Q}$), then the absolute Galois group of K is intertwined with the fundamental group of our space in a deep way that has important consequences for Diophantine solutions of such equations.

In this lecture, we will not get to all of these topics, but we will see how the fundamental group of a certain space relates to the Galois group of a related field of functions on that space.

1.2 Rings of Functions on Spaces and Primes as Points

Before proceeding, we mention two important general principles.

If X is some space (usually a manifold, or a subset of $\mathbb{R}^n$, or even just the real line $\mathbb{R}$ if you like), we often like to consider functions that associate a real number to each point of X. We often ask that such functions be continuous, or differentiable, or smooth, or infinitely differentiable. We might also consider functions associating a complex number to each point, and ask that they too be continuous, or even complex-differentiable.

If we have two functions on a space, we can multiply them, by multiplying their values at each point, and we can similarly add them. It is a basic fact that the sum and product of two continuous functions is again continuous, and the same is true for differentiable functions, and just about every other type of functions we've listed. One can see that the set of continuous real-valued functions on a space forms a ring. The same is true of the set of differentiable or smooth functions, of complex-valued continuous functions, of holomorphic functions, or just about anything you ask for. They all form rings under pointwise addition and multiplication.

Another important ring of functions that algebraic geometers often consider is the ring of functions on $\mathbb{C}^n$ given by polynomials in n variables. This ring is contained within the ring of continuous, differentiable, even holomorphic functions on $\mathbb{C}^n$.

Now suppose $r : X \to Y$ is a map of spaces. If we just care about the topological structure and are considering continuous functions, we want this map to be continuous. If we care about differentiability, we want this map to be differentiable, so on and so forth. Then if f is a function on Y, the composition $f \circ r$ is a function on X (this is called the *pullback* of f by r). In particular, this defines a *homomorphism* r^* from the ring of functions on Y to the ring of functions on X. Note that if r is merely continuous, we get a homomorphism of rings of continuous functions, and if r is differentiable, we get a homomorphism of rings of differentiable functions, etc. We have the following principle:

Principle 1.2.1. *A map of* spaces *going in one direction induces via pullback* a map of rings going in the other direction.

The second principle is this. Let P be a point of a space X, and suppose we are considering complex-valued functions (we could do real-valued is well, but I'm picking for the sake of example), either continuous or differentiable or holomorphic functions, whichever ring you wish. Then there is a homomorphism from the ring of functions on X to $\mathbb{C}$ send a function f to its value $f(P)$ at P. In general, this map will be surjective, and so the kernel will be a maximal ideal. This is the ideal of *functions that vanish at* P. More generally, if S is a subset of X, then the set of functions vanishing on S is an ideal, though not necessarily maximal.

Furthermore, suppose that $r : X \to Y$ is a map of spaces, $P \in X$, $Q \in Y$, and $r(P) = Q$. Then a function f on Y vanishes at Q iff $f \circ r$ vanishes at P. In particular, the maximal ideal associated to Q in the ring of functions on Y is the preimage of the maximal ideal associated to P in the ring of functions on X under the ring homomorphism induced by r. In particular, this gives a way to see that the point P maps to the point Q under r in terms of the ring homomorphism that r induces.

There is an important observation that in many contexts, every single maximal ideal of the ring of functions is the ideal of functions vanishing at some point. We therefore have the principle:

Principle 1.2.2. Points and maximal ideals are two ways of looking at the same thing.

Let's illustrate this with the example of the ring $\mathbb{C}[z]$. Every polynomial in z is a function on the complex plane, i.e. associates a complex number to each point of the complex plane.

The maximal ideals in this ring are of the form $(z - a)$, where $a \in \mathbb{C}$. In particular, they correspond bijectively to the points of $\mathbb{C}$. It is easy to see that the ideal $(z - a)$ is the set of polynomials vanishing at a. Furthermore, the division algorithm tells us that for any polynomial $f(z)$, we can write

$$f(z) = q(z)(z - a) + r,$$

where r has degree 0 and is therefore a constant. Plugging in a for z, we see that

$$f(a) = q(a)(a - a) + r = r.$$

That is, the *remainder of $f(z)$ upon division by $z - a$ is the value of f at a.*

Mathematicians dating back to the 1800's noticed an analogy between the ring $\mathbb{C}[z]$ and the ring $\mathbb{Z}$. The maximal ideals of $\mathbb{Z}$ correspond to the prime numbers. Therefore, one might pretend that there is some space whose points correspond to the primes, and such that each element of $\mathbb{Z}$ is a function on this space. Carrying this analogy further, the value of an integer n, which we think of as a function on our space, at a prime number p, which we think of as a point in our space, should just be the reduction modulo p of the integer n, or the remainder of n upon division by p. In particular, its *value* at p lies in the field $\mathbb{Z}_p$ (this is the finite field of order p, following PROMYS notation). In this bizarre world, the values of a single function at different points live in different fields.

While this may seem very strange, the analogy becomes more fruitful when we consider extensions of $\mathbb{Z}$, the simplest of which is $\mathbb{Z}[i]$. We can then carry geometric intuition from extensions like $\mathbb{C}[z][\sqrt{z}]$ over $\mathbb{C}[z]$ to interesting analogies with the splitting of primes in extensions.

1.3 Fundamental Groups of Punctured Planes and Galois Groups

1.3.1 The Squaring Map

We now switch gears and actually talk about fundamental groups. We consider the simple map p from the complex plane $\mathbb{C}$ to itself given by sending a complex number z, to its square, z^2. We include the following picture:

To make things more clear later on, we suppose that the domain has coordinate z, and the range has coordinate w. In particular, this means

$$w = p(z) = z^2.$$

We include a diagram on the next page. The z plane lies twisted above the w plane so that every point z_0 lies directly above $p(z_0)$. The figure isn't really supposed to intersect itself; unfortunately, you would need four dimensions to draw it properly, and PROMYS doesn't have a four-dimensional yearbook.

For all $a \neq 0$ in $\mathbb{C}$, the preimage $p^{-1}(a)$ of a has two elements, the two square roots of a. But $p^{-1}(0)$ has only one element, namely 0. In particular, this map cannot be a covering map, since in a covering of a connected space, each point must have the same number of preimages. (Alternatively, $\mathbb{C}$ is simply connected, so it has no coverings!)

What we can do to mend the situation is to take out the point 0. That is, when restricted to $\mathbb{C} \setminus \{0\}$, p induces a map $\mathbb{C} \setminus \{0\} \to \mathbb{C} \setminus \{0\}$ sending a complex number to its square. One can in fact show that this map is a covering map. (To do this, one can note that the derivative, or Jacobian determinant if you don't like complex analysis, vanishes nowhere and then use the inverse function theorem.) Furthermore, this covering corresponds to the subgroup

$$2\mathbb{Z} \subseteq \mathbb{Z} \cong \pi_1(\mathbb{C} \setminus \{0\})$$

. This covering also has a nontrivial deck transformation, the automorphism of $\mathbb{C} \setminus \{0\}$ sending z to $-z$. This respects the covering p, as $p(z) = z^2 = (-z)^2 = p(-z)$. This corresponds to the nontrivial element of

$$\pi_1(\mathbb{C} \setminus \{0\})/2\pi_1(\mathbb{C} \setminus \{0\}).$$

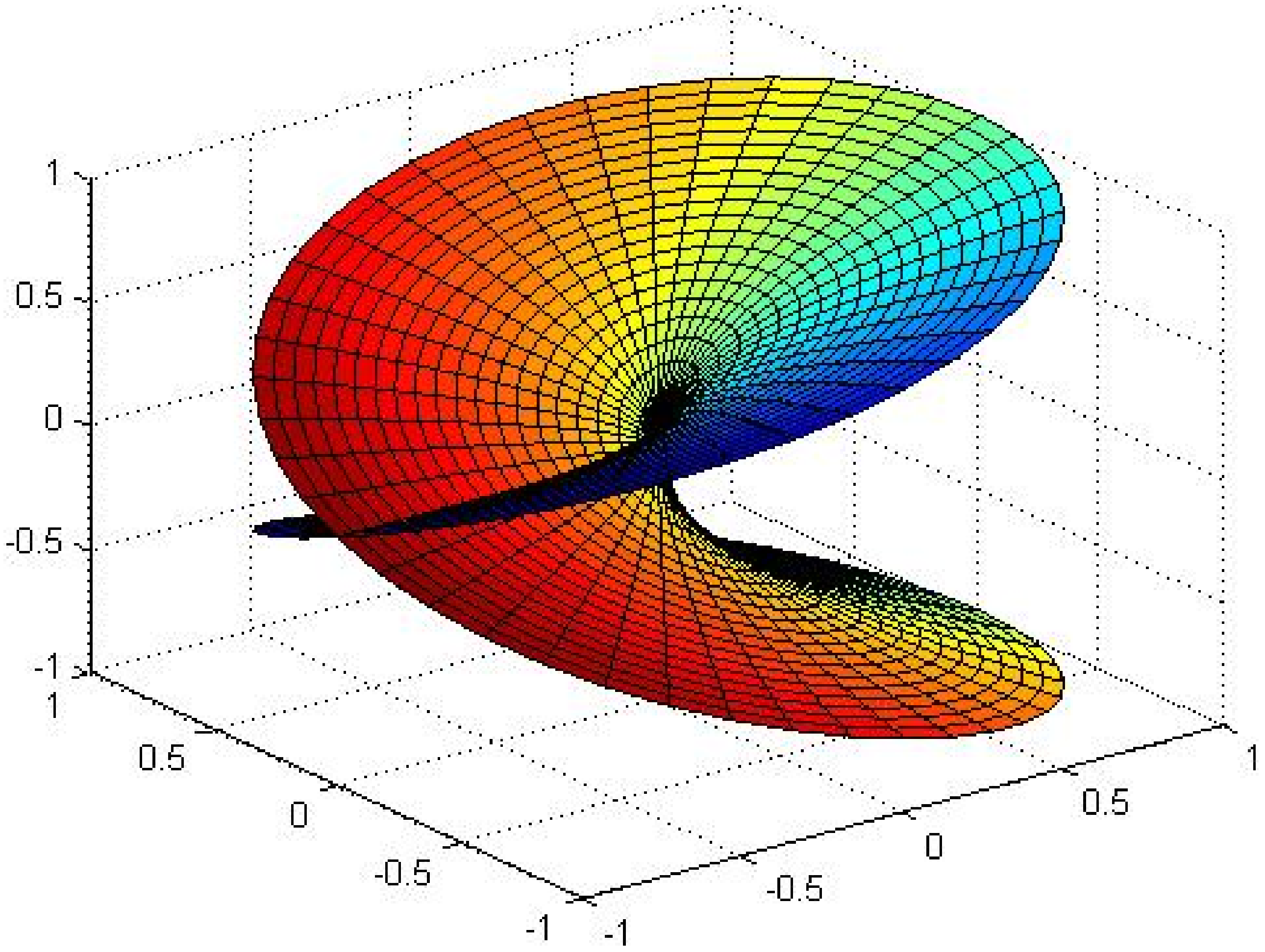

Figure 1.1: http://upload.wikimedia.org/wikipedia/commons/b/b5/Riemann_sqrt.jpg

While we know that this is the cover of $\mathbb{C} \setminus \{0\}$ of degree 2 simply because every point has two preimages, we note that squaring in the complex plane wraps the unit circle around itself twice, meaning it corresponds to doubling in the fundamental group.

Next, consider the ring $\mathbb{C}(w)$ of rational functions in w. While an arbitrary rational function does not define a function on all of $\mathbb{C}$ (as it is undefined wherever its denominator vanishes), it at least defines a function on most of $\mathbb{C}$. In particular, we can still add and multiply rational functions, and we can pull them back by maps. In particular, the function assigning to each point of $\mathbb{C} \setminus \{0\}$ its coordinate w pulls back under p to the function z^2 on the z-plane. This map p corresponds therefore to an inclusion $p^* : \mathbb{C}(w) \hookrightarrow \mathbb{C}(z)$ of fields sending w to z^2.

The relation $w = z^2$ is essentially the same as $z = \sqrt{w}$, and we can view $\mathbb{C}(z)$ as the field extension $\mathbb{C}(w)[\sqrt{w}]$ (or more formally, $\mathbb{C}(w)[z]/(z - w^2)$). This is a field extension of $\mathbb{C}(z)$ of degree 2, and its Galois group has order 2. The nontrivial element of this Galois group sends $\sqrt{w}$ to $-\sqrt{w}$, or z to $-z$. In particular, *it is ring homomorphism induced by the nontrivial deck transformation of the cover.*

1.3.2 Finite Covers of $\mathbb{C} \setminus \{0\}$

More generally, consider the map $p_k : z \mapsto w = z^k$, for $k \in \mathbb{N}$. Then the preimage of $w = a \in \mathbb{C}$ consists of all kth roots of a, and if $\sqrt[k]{a}$ denotes one of them, then the others are of the form $\zeta_k^n \sqrt[k]{a}$, where ζ_k is a kth root of unity. If a is 0, then it only has one preimage, and as before, the map is a covering when restricted to a map $\mathbb{C} \setminus \{0\} \to \mathbb{C} \setminus \{0\}$. This is the unique degree k connected cover of $\mathbb{C} \setminus \{0\}$, and it corresponds to the subgroup

$$k\pi_1(\mathbb{C} \setminus \{0\}) \subseteq \pi_1(\mathbb{C} \setminus \{0\}).$$

In a similar way, this map corresponds to the field extension

$$\mathbb{C}(z = \sqrt[k]{w})/\mathbb{C}(w).$$

Its Galois group is generated by the automorphism $z \mapsto \zeta_k z$, which corresponds to a generator of the group of deck transformations of the cover p_k! In this way, all finite covers of $\mathbb{C} \setminus \{0\}$ correspond to certain Galois extensions of the field $\mathbb{C}(w)$, and the groups of deck transformations can be recovered as the Galois groups of these field extensions!

Notice that the universal cover is given by the exponential map from $\mathbb{C}$ to $\mathbb{C} \setminus \{0\}$, and we do not consider it, for we would like to restrict to polynomial maps (as these give algebraic field extensions). Another way to see why the universal covering map cannot be given by polynomials is that a polynomial has finitely many roots, while every point of $\mathbb{C} \setminus \{0\}$ has infinitely many preimages in the universal cover.

In some sense, we can recover all finite quotients of the fundamental group $\pi_1(\mathbb{C} \setminus \{0\})$ from the Galois groups of field extensions of the field $\mathbb{C}(w)$. For any group G, there is a topological group, $\widehat{G}$, known as the *profinite completion* of G, which has the same set of finite quotients as G, and is in fact uniquely determined by those finite quotients. This is a natural homomorphism $G \to \widehat{G}$, and in many cases this map is injective. In particular, the profinite completion of $\mathbb{Z}$ is a group known as $\widehat{\mathbb{Z}}$. In this case, $\widehat{\mathbb{Z}}$ is the (infinite) Galois group of the extension of the field $\mathbb{C}(w)$ attained by adjoining all kth roots of w. I won't say what this means now, but this implies that the étale fundamental group

$$\pi_1^{\acute{e}t}(\mathbb{C} \setminus \{0\}) \cong \widehat{\mathbb{Z}}.$$

1.3.3 Ramified Covers of the Complex Plane

Now, I'd like to go back for a second to the map $p : \mathbb{C} \to \mathbb{C}$ which is manifestly *not* a covering. It is, however, something more general, known as a *ramified cover.* The point $w = 0$ over which the map is not a cover is called a *branch point*, and its preimage $z = 0$ is called a *ramification point.* In particular, a map is *unramified* and therefore a *covering map* if it has no ramification points.

Now, recall that to each point $a \in \mathbb{C}$ (in the w-plane) is associated the ideal $(w - a)$ in the ring $\mathbb{C}[w]$. Consider the image of $w - a$ in the ring $\mathbb{C}[z]$. It maps to $z^2 - a \in \mathbb{C}[z]$. If $a \neq 0$, it splits as a product of two distinct primes, $z - \sqrt{a}$ and $z + \sqrt{a}$. If $a = 0$, then it is simply a power of a prime ideal, namely z^2. More generally, if we consider the kth power map p_k, the same holds. That is, the ideal associated to a non-branch-point splits as a product of k distinct primes when viewed in $\mathbb{C}[z]$, and the ideal associated to $w = 0$ equals a power of a prime. This is analogous to the fact that most primes of $\mathbb{Z}$ either remain prime or split as a product of two distinct prime ideals in $\mathbb{Z}[i]$, whereas the prime 2 generates the power of a prime ideal, namely $(1 + i)^2$.

More generally, suppose we have a map $f : \mathbb{C} \to \mathbb{C}$ given by a polynomial $w = f(z)$. Then the map is ramified precisely at those points z_0 for which $f'(z_0) = 0$ (we can see this either by using the inverse function theorem, or at least prove it's not a cover by using the derivative to describe numbers of preimages). The branch points are their images under f. Let S be the set of branch points in $\mathbb{C}$. Then f is a covering of $\mathbb{C} \setminus S$. In particular, it corresponds to some subgroup of $\pi_1(\mathbb{C} \setminus S)$.

On the field-theoretic side, this corresponds to a field extension $\mathbb{C}(z)$ of $\mathbb{C}(w)$ obtained by sending w to $f(z)$. In particular, the degree of this extension equals the degree of the polynomial f. If this field extension is Galois, then the corresponding subgroup of $\pi_1(\mathbb{C} \setminus S)$ is normal, and the quotient by this subgroup is the Galois group of the extension.

Example 1.3.1. Consider the polynomial $f(z) = z^3 - 6z^2 + 9z + 1$. Its derivative is $3z^2 - 12z + 9$, which factors as $3(z - 1)(z - 3)$, so the ramification points are 1 and 3. The corresponding branch points are $w = f(1) = 1$ and $w = f(3) = 5$, so 1 and 5 are the branch points of this map. In particular, this map is a covering of $\mathbb{C} \setminus \{1, 5\}$, and it corresponds to a finite index subgroup of $\pi_1(\mathbb{C} \setminus \{1, 5\})$. We can take its Galois closure to get a normal cover of $\mathbb{C} \setminus \{1, 5\}$, and the Galois group is isomorphic to a quotient of the fundamental group of $\pi_1(\mathbb{C} \setminus \{1, 5\})$. (We could have also considered a polynomial like $z^3 - 9z^2 + 18z - w$, a root of which gives a Galois cubic extension over $\mathbb{C}(w)$.) Now $\mathbb{C} \setminus \{1, 5\}$ is a twice-punctured plane and hence homotopy equivalent to a figure-eight, which has fundamental group isomorphic to the free group on two generators. In particular, the Galois group of this extension can be generated by two elements. Of course, all groups of order ≤ 6 can be generated by two elements, but there are certain situations where this fact is nontrivial.

1.3.4 The Correspondence Between Galois Groups and Fundamental Groups

More generally, any field extension of $K/\mathbb{C}(w)$ corresponds to a connected cover of the complex plane punctured at some finite number of points. To see this, we can take a primitive element $z \in K$ such that $g(z, w) = 0$ for some $g(z, w) \in \mathbb{C}[z, w]$, then consider the subset $\{(z, w) \mid g(z, w) = 0\} \subseteq \mathbb{C}^2$. This maps onto $\mathbb{C}$ by sending (z, w) to w. One can show that this is a ramified cover and that it in some sense corresponds to the field extension K. If its set of branch points (the images under the map of the ramification points, i.e. the points at which it is not a cover) is S, then it gives a topological covering of $\mathbb{C} \backslash S$, hence corresponds to a subgroup of $\pi_1(\mathbb{C} \backslash S)$. In particular, if $K/\mathbb{C}(w)$ is Galois, then the Galois group is the quotient of the fundamental group by this subgroup.

Remark 1.3.2. In fact, a field extension gives a *unique* ramified cover, and its branch points (which are the points over which the map is not a cover) are are determined by the cover. Furthermore, if $L/K/\mathbb{C}(w)$, then every branch point of K is a branch point of L, so that we have to puncture in at least as many places to get a covering for L as we do for K. In fact, the compositum of two fields unramified above a point is again unramified above that point.

Conversely, suppose we have a topological covering of $\mathbb{C} \setminus S$ for some finite set S. Then the famous existence theorem of Riemann says that there is a field extension of $\mathbb{C}(w)$ giving rise to it.

In particular, *all* finite quotients of the fundamental groups of puncturings of the complex plane arise as Galois groups of field extensions of $\mathbb{C}(w)$. This has an interesting application. Let G be an arbitrary finite group. Then it can be generated by some number of elements, say n. Let X be the space obtained by puncturing the complex plane at n points. Then its fundamental group is the free group on n generators, which therefore has G as one of its quotients. Thus there is a covering of X whose group of deck transformations is isomorphic to $\mathbb{C}(w)$

It is a corollary of the remark above that for a finite subset $S \subseteq \mathbb{C}$, we can consider the compositum K_S of all field extensions of $\mathbb{C}(w)$ corresponding to ramified covers with no branch points outside of S (equivalent, which correspond to actual topological coverings of $\mathbb{C} \setminus S$). Then we have an isomorphism

$$\mathrm{Gal}(K_S/\mathbb{C}(w)) \cong \pi_1\widehat{(\mathbb{C} \setminus S)}$$

between the Galois group of this extension and the fundamental group of $\mathbb{C} \setminus S$. This is the "free profinite group on $|S|$ generators," also the free product of $\widehat{\mathbb{Z}}$ with itself n times, if you know what either of those terms mean.

Remark 1.3.3. In a very technical sense, there is really a canonical *anti-isomorphism* between the two because maps of spaces go the opposite direction as maps of rings or fields. So left actions of one correspond to right actions of the other. (On the *é*-tale site ;).) But every group is isomorphic to its opposite via the inverse map.

More generally, Riemann's theorem works with $\mathbb{C}$ replaced by any compact Riemann surface (in the case of $\mathbb{C}$, it is the Riemann sphere), and $\mathbb{C}(w)$ replaced by the field of meromorphic functions on that Riemann surface. Then we can find profinite completions of fundamental groups in terms of Galois groups of function fields.

In conclusion, we have seen a concrete situation where certain Galois groups correspond to certain fundamental groups, and we can (partially) recover the fundamental group from the Galois group of a certain extension. Next time we will come at the problem from a different (but related) angle and answer some of the questions posed at the beginning.

Chapter 2

Etale Fundamental Groups

We will now talk about Grothendieck's approach to fundamental groups of varieties, building upon others before him. We will greatly use the two principles from last time. Before we begin, we review affine varieties.

2.1 Affine Varieties

A good reference is the first chapter of Silverman's book *Arithmetic of Elliptic Curves* or most introductory texts on algebraic geometry.

A (complex) affine variety X is the subset of $\mathbb{C}^m$ consisting of the solutions to a system of polynomial equations

$$f_1(x_1, \cdots, x_m) = f_2(\cdots) = \cdots = f_s(x_1, \cdots, x_m) = 0$$

in m variables. To the variety, we associate its *affine coordinate ring*

$$A(X) := \mathbb{C}[x_1, \cdots, x_m]/I(X),$$

where $I(X)$ is the set of polynomials vanishing on X. Hilbert Nullstellensatz states that this is the radical of the ideal generated by $f_1, \cdots, f_s$. Conversely, X is the set of points at which every element of $I(X)$ vanishes. Since every element of $I(X)$ vanishes on X, the elements of $A(X)$ are well-defined complex-valued functions on X, and an element of $A(X)$ is determined by its value at each point.

To every point $P \in X$ we associate the ideal $\mathfrak{m}_P \subseteq A(X)$ of functions that vanish at X. It is a maximal ideal, and Hilbert's Nullstellensatz implies that every maximal ideal corresponds to a unique point.

If $X \subseteq \mathbb{C}^m$ and $Y \subseteq \mathbb{C}^n$ are affine varieties, then a map (or morphism) between the varieties is a map from the set Y to the set X given by m polynomials $h_1, \cdots, h_m$ each in n variables. The map defined by a sequence of polynomials sends the point $(y_1, \cdots, y_n) \in Y$ to

$$(h_1(y_1, \cdots, y_n), h_2(\cdots), \cdots, h_m(\cdots)) \in X \subseteq \mathbb{C}^m.$$

If $r : Y \to X$ is a map between varieties, then the pullback of any polynomial function on X (i.e. an element of the ring $A(X)$) is a polynomial function on Y, and this defines a ring homomorphism

$r^* : A(X) \to A(Y)$. The key observation is that this actually gives a bijection between maps from Y to X and $\mathbb{C}$-algebra homomorphisms from $A(X)$ to $A(Y)$. Another way to say this is that the category of affine varieties is anti-equivalent to the category of affine coordinate rings (with $\mathbb{C}$-algebra homomorphisms as morphisms).

To see why, first consider the case $X = \mathbb{C}^m$,$Y = \mathbb{C}^n$. Then a map from Y to X is the same as a collection of m polynomials in n variables. But this is the same as a $\mathbb{C}$-algebra homomorphism $\mathbb{C}[x_1, \cdots, x_m] \to \mathbb{C}[y_1, \cdots, y_n]$, since such a map is determined uniquely by a choice of where each x_i goes. Now, suppose that X and Y are cut out by polynomials $f_1, \cdots, f_s$ and $g_1, \cdots, g_r$, respectively. Then a map $Y \to X$ is uniquely determined by a collection of m polynomial functions on Y, i.e. m elements of $A(Y)$, which is the same as a $\mathbb{C}$-algebra homomorphism $\mathbb{C}[x_1, \cdots, x_m] \to A(Y)$. This map is a map to X iff the image is contained within X, which is to say that every polynomial in $I(X)$ vanishes on the image. But this exactly corresponds to the condition that the map $\mathbb{C}[x_1, \cdots, x_m] \to A(Y)$ factor through the quotient

$$\mathbb{C}[x_1, \cdots, x_m] \to \mathbb{C}[x_1, \cdots, x_m]/I(X) \cong A(X).$$

Now $\mathbb{C}^m$ has a topology, being homeomorphic to $\mathbb{R}^{2m}$, and X has a topology as a closed subspace of $\mathbb{C}^m$. Furthermore, polynomial maps are continuous, and so we can talk about what it means for a map between varieties to be a *covering map.*

Since maps between varieties correspond bijectively to maps between their affine coordinate rings, we can single out those ring homomorphisms between affine coordinate rings that correspond to covering maps of varieties and call them *covering ring homomorphisms.* We would like to now find an intrinsically ring-theoretic criterion for a map between rings to be a covering ring homomorphism.

The notion of being locally a homeomorphism corresponds to being a finite *étale* homomorphism of rings. That is, a map between varieties is a covering iff the corresponding map on affine coordinate rings is finite étale. We give a sketch of how you might define such a notion, but the reader may wish to skip this sketch. What's most important is to know that there is an abstract ring-theoretic condition corresponding to a local homeomorphism. One reason for wanting this is that we would like to give a purely algebraic construction of the fundamental group, and giving an algebraic definition of covering space is one step in that direction. The other reason is in order to make a vast generalization that we will see in the next section.

2.1.1 Sketch of the Definition of Etale

It's related to the idea that a covering $Y \to X$ is locally a homeomorphism. You might object that this could not be the case, for any point in X has multiple preimages (assuming it's a nontrivial cover), so no matter how small a neighborhood you take of that point, the map is not a homeomorphism. The key is that it is locally *on* Y a homeomorphism. And indeed, for any point in Y, there exists a neighborhood of that point such that the restriction of the covering map to that neighborhood is a homeomorphism onto its image.

If we're considering maps of manifolds, then the map is locally a homeomorphism at a point iff its map on tangent spaces is an isomorphism, or equivalently its Jacobian determinant does not vanish. This follows from the inverse function theorem. You might remark that we can define derivatives of polynomials in a purely formal and algebraic way, but we would like something more ring-theoretic. If P is a point of X, then $\mathfrak{m}_P$ is the ideal of functions vanishing at X. Each function has a gradient at P, which is a cotangent vector at P. The functions with vanishing gradient are those in $\mathfrak{m}_P^2$. In particular, the cotangent space is isomorphic to $\mathfrak{m}_P/\mathfrak{m}_P^2$. This gives us a ring-theoretic way to consider the cotangent space. We might then say that $r : Y \to X$ is a covering iff for all $P, Q \in X, Y$ such that $r(Q) = P$, the induced homomorphism $A(X)/\mathfrak{m}_P^2 \to A(Y)/\mathfrak{m}_Q^2$ is an isomorphism. This definition turns out to be satisfactory when the varieties are nonsingular, but when the varieties are singular, we need higher order information. It turns out that the right definition is that the map is étale if $A(X)/\mathfrak{m}_P^k \to A(Y)/\mathfrak{m}_Q^k$ is an isomorphism for all $k \in \mathbb{N}$. More generally, we say that a homomorphism $q : R \to S$ of rings is étale if for all maximal ideals $\mathfrak{m}$ of S, the induced homomorphism

$$R/q^{-1}(\mathfrak{m})^k \to S/\mathfrak{m}^k$$

is an isomorphism.

There is an alternative definition that banks on something we remarked last time. That is, the fact that the map $z \mapsto w = z^k$ has a branch point at $w = 0$ corresponds to the fact that the ideal $(w - a) \subseteq \mathbb{C}[w]$ factors into a prime ideal with nontrivial multiplicity in $\mathbb{C}[w][\sqrt{w}]$ iff $a = 0$. The technical definition is that a map of rings $q : R \to S$ is unramified if for every prime ideal $\mathfrak{p}$ of S, the corresponding map on local rings $R_{q^{-1}(\mathfrak{p})} \to S_{\mathfrak{p}}$ sends $q^{-1}(\mathfrak{p})$ onto the maximal ideal of $S_{\mathfrak{p}}$. Then a map is étale if it is flat, locally of finite presentation, and unramified.

Note that not every local homeomorphism is a covering. Consider, for example, the inclusion of an open subset U into a space X (also known as an *open immersion*). Then this is locally a homeomorphism, but it is clearly not a covering. To remedy this, we might require that our map be surjective. But consider the map from $\mathbb{C} \setminus \{0, 1\}$ to $\mathbb{C} \setminus \{0\}$ given by sending z to z^2. Then this map is a local homeomorphism and is surjective, but it is not a covering. In particular, the point 1 is missing an element of its fiber. This is because the map is obtained by the composition

$$\mathbb{C} \setminus \{0, 1\} \to \mathbb{C} \setminus \{0\} \to \mathbb{C} \setminus \{0\}$$

of an open immersion with a covering.

The *finite* condition on finite étale homomorphisms of rings ensures that the map is actually a cover. A ring homomorphism $R \to S$ is finite if S is a finitely-generated module over R. Note that this does *not* have to do with the fact that every point has finitely-many preimages - for the same is true of any open immersion! Rather, it has to do with the fact that an open immersion is the roughly same thing as localization, or formally inverting elements. For example, the inclusion $\mathbb{C} \setminus \{0\} \hookrightarrow \mathbb{C}$ corresponds to the ring homomorphism $\mathbb{C}[z] \to \mathbb{C}[z][\frac{1}{z}]$, as when we restrict to $\mathbb{C} \setminus \{0\}$, z becomes invertible. Since we can consider arbitrarily high powers of $\frac{1}{z}$, the ring $\mathbb{C}[z][\frac{1}{z}]$ is not finitely-generated as a module over $\mathbb{C}[z]$. It is this finiteness condition that ensures an étale map is actually a covering.

2.2 Grothendieck's Approach and Etale Fundamental Groups

2.2.1 Spaces and Rings

We now outline Grothendieck's point of view on all of this. He noted that affine varieties correspond bijectively to affine coordinate rings, which can be characterized as finitely-generated reduced $\mathbb{C}$-algebras. The "finitely-generated" condition just says that the ring is the quotient of a polynomial ring, and the "reduced" (also known as "nilpotent-free") condition comes from the fact that $I(X)$ is the radical of another ideal by the Nullstellensatz. Furthermore, $\mathbb{C}$-algebra maps correspond bijectively to maps of varieties going in the other direction. His important contribution was to ask why we restrict ourselves to such a specific class of rings, namely finitely-generated reduced $\mathbb{C}$-algebras, and not instead consider *all* commutative rings. He imagined that every ring is the ring of functions on some space, and if A is a ring, he called this imagined space "Spec(A)." This space would correspond to A in the same way that an affine variety corresponds to its affine coordinate ring. He referred to this space as an "affine scheme."

Taking this (imagined) analogy further, the "points" of this "space" Spec(A) should correspond to the maximal ideals $\mathfrak{m}$ of A, and if $q : A \to B$ was a ring homomorphism, then the point (or maximal ideal) $\mathfrak{m} \subseteq B$ should map to the maximal ideal $q^{-1}(\mathfrak{m})$ in A. He further noted that the preimage of a maximal ideal was not always maximal (consider the preimage of $(0) \subseteq \mathbb{Q}$ under the inclusion of $\mathbb{Z}$ into $\mathbb{Q}$) and therefore suggested that *all* prime ideals of A should count as points of this space.

Armed with this point of view, we should say that the map of spaces $\text{Spec}(B) \to \text{Spec}(A)$ is a covering iff the corresponding map of rings $A \to B$ is finite étale (we say that B is a "finite étale extension" of A). We don't actually know what these spaces are or mean or if they exist (or what that would mean!); they are imagined. But whatever they are, we are *defining* a map between these spaces to be a covering if the corresponding map on rings is étale.

2.2.2 Etale Fundamental Groups

Now let's suppose we have a ring A and we want to compute the fundamental group of Spec(A), whatever that means. Then the idea is that subgroups of this group should correspond to connected covers $\text{Spec}(B) \to \text{Spec}(A)$.

We almost have defined what we mean by a connected cover of Spec(A). We just need to specify what "connected" means for a space Spec(B). The idea is actually quite simple. If a space X is disconnected, say it is a disjoint union $X_1 \sqcup X_2$, then a specifying a function on X is the same as independently specifying a function on X_1 and a function on X_2. In particular, the ring of functions on X is just the direct sum of the ring of functions on X_1 with the ring of functions on X_2. In particular, a space is connected if its ring of functions is not the direct sum of two rings. Therefore, we say Spec(B) is connected if B is not the direct sum of two other rings. In general, we should require Spec(A) to be connected from the start, as we should only consider fundamental groups of connected spaces.

Now we want to construct a group $\pi_1^{\acute{e}t}(\text{Spec}(A))$ whose subgroups correspond to the covers of Spec(A). How do we get the group structure. The key is to note that if a subgroup of the fundamental group is normal, then its corresponding cover has a group of transformations isomorphic to the quotient of the fundamental group by this normal subgroup. We can therefore recover all the (finite) quotients of this fundamental group, which we have yet to define, as the automorphism groups of finite connected covers $\text{Spec}(B) \to \text{Spec}(A)$ that are "normal." Recall that maps of spaces correspond to maps of rings going in the other direction, so this is the same as looking at automorphisms of B as an A-algebra. (Oh wait this is starting to look like Galois theory...)

It turns out that any covering $\text{Spec}(B) \to \text{Spec}(A)$ (a fact we can prove in commutative algebra). This is the same problem as we had before, that we cannot express infinite-degree covers in algebraic geometry. Nonetheless, we can define its *étale fundamental group*

$$\pi_1^{\acute{e}t}(\mathrm{Spec}(A)) := \varprojlim \mathrm{Aut}_A(B)$$

as an inverse limit over all finite étale homomorphisms from A to connected rings B. This is the profinite completion of what the fundamental group should be, but it serves our purposes for the moment. We have given a meaning to "the fundamental group of Spec(A)"!

We should first note that this answers one of our questions from before, namely that of finding an algebraic way to recover the fundamental group of a complex variety. Namely, if we have an affine variety X, we can consider its affine coordinate ring $A(X)$ and then consider all finite étale homomorphisms $A(X) \to B$. It turns out that B will always be an affine coordinate ring, with a $\mathbb{C}$-algebra structure inherited from A (so the map will be a $\mathbb{C}$-algebra homomorphism!). The important fact is that a more general form of Riemann's existence theorem than the one we used last time ensures that *any* finite topological covering of a complex algebraic variety arises as a polynomial map between varieties, and the deck transformations are maps of varieties. This means that finite topological covers of X correspond bijectively to finite étale maps $A(X) \to B$. In particular, we have an isomorphism

$$\pi_1^{\acute{e}t}(\mathrm{Spec}(A(X))) \cong \pi_1\widehat{(X(\mathbb{C})}),$$

where $X(\mathbb{C})$ denotes the points of X in the complex topology.

One might ask whether we can recover the fundamental group of a variety, not just its profinite completion, in a purely algebraic manner, i.e. solely from the ring $A(X)$. This method doesn't seem to work, but maybe there is a completely different way. As it turns out, Serre provided an example that proves we cannot do this. If you see the quote "Theorem: Too Bad" on the t-shirt, that refers to this.

If one has a set of polynomial equations in $\mathbb{C}$ that cut out a variety, one can apply an automorphism of $\mathbb{C}$ to all of the coefficients. Assuming the coefficients are not all rational, this can change the variety and actually change the topology of the variety. However, because the algebra of both varieties is exactly the same, their affine coordinates rings are isomorphic (note that they are *not* isomorphic as $\mathbb{C}$-algebras, for the varieties are not isomorphic). In particular, this means that their étale fundamental groups are isomorphic. Serre found an example of two varieties with isomorphic affine coordinate rings but whose fundamental groups were different. By everything we've said, the profinite completions of these different fundamental groups had to be the same, for they are both the étale fundamental group of the underlying coordinate ring. But this means that we cannot recover the fundamental group of a variety from its affine coordinate ring; we can only recover its finite quotients.

2.2.3 Galois Groups as Fundamental Groups

We have, at least partially, answered one of the questions from the first lecture. We have recovered the fundamental group of a variety, or at least its finite quotients, in a purely algebraic way. But we can now answer a more important dream: To find a function such that when we input a space, we get its fundamental group, and when we input a field, we get its (absolute) Galois group.

It turns out that if K is a field, then

$$\pi_1^{\acute{e}t}(\mathrm{Spec}(K)) \cong \mathrm{Gal}(\overline{K}/K).$$

(Note that $\overline{K}$ denotes the *separable* closure of K.)

This follows from the fact, which one can prove in commutative algebra, that the finite connected étale homomorphisms out of K are precisely the finite separable field extensions of K. It follows immediately from our definitions that the above statement is true (and again, there is a canonical *anti*-equivalence between the two, as a map of rings corresponds to a map of spaces going in the other direction). To see why separable might come into the étale picture, recall that separability can be defined by a condition on the derivative of a polynomial. This differential condition then corresponds to the differential condition implicit in the definition of étale.

Furthermore, the correspondence between finite-index subgroups of the étale fundamental group and connected finite étale covers is exactly the same as the correspondence between subgroups of the Galois group and separable finite extensions of K. Furthermore, a map $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ of spaces should induce a homomorphism $\pi_1^{\acute{e}t}(\mathrm{Spec}(B)) \to \pi_1^{\acute{e}t}(\mathrm{Spec}(A))$, and it in fact does. In the case of a separable algebraic extension $K \hookrightarrow L$, the map $\mathrm{Spec}(L) \to \mathrm{Spec}(K)$ induces the natural inclusion $\mathrm{Gal}(\overline{L}/L) \hookrightarrow \mathrm{Gal}(\overline{K}/\overline{L})$.

In particular, a K is separably closed iff $\mathrm{Spec}(K)$ has no nontrivial finite separable extensions, which is to say that its étale fundamental group is trivial and that it is *simply connected*. More generally, we say that $\mathrm{Spec}(A)$ is simply connected if it has no nontrivial connected coverings.

The funny thing to note is that if K is not separably closed (e.g. $\mathbb{Q}$), then it is not simply connected, yet $\mathrm{Spec}(K)$ consists of only a point, since K has only one prime ideal. In some bizarre sense, there are nontrivial loops in this one-point space! At the very least, this demonstrates that the point-set of $\mathrm{Spec}(K)$ tells us very little about the actual "geometry" of $\mathrm{Spec}(K)$.

If $A(X)$ is an affine coordinate ring, then we recall from last time (at least in the case that X is $\mathbb{C}$ punctured at finitely many points; more generally this is true if X is a normal variety) that the profinite completion of the fundamental group of X is isomorphic to the Galois group of a certain extension of the function field $\mathbb{C}(X)$ of X. This extension is the compositum of those field extensions that correspond to covers of X. There is a natural inclusion $A(X) \to \mathbb{C}(X)$, which induces a map $\mathrm{Spec}(\mathbb{C}(X)) \to \mathrm{Spec}(A(X))$. As we've stated, this should induce by functoriality of $\pi_1^{\acute{e}t}$ a map

$$\pi_1^{\acute{e}t}(\mathrm{Spec}(\mathbb{C}(X))) \to \pi_1^{\acute{e}t}(\mathrm{Spec}(A(X))).$$

As it turns out, this map is just the quotient map from $\mathrm{Gal}(\overline{\mathbb{C}(X)}/\mathbb{C}(X))$ to the Galois group of the intermediate extension.

In a similar way, the map $\mathrm{Spec}(\mathbb{Z}[i]) \to \mathrm{Spec}(\mathbb{Z})$ coming from the inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}[i]$ is not a covering because $(2) = (1+i)^2$, i.e. the prime (or "point") (2) ramifies in the extension. We can, however, localize to get rid of the prime 2, and it turns out that the induced map $\mathbb{Z}[1/2] \to \mathbb{Z}[i][1/(1+i)]$ is a finite étale homormophism of rings. In particular, it is not simply connected, and it has a nontrivial "loop" running around the point (2). More generally,if you know algebraic number theory, then if $\mathcal{O}_K$ is the integer ring of a number field K, and S is a finite set of primes, then $\pi_1^{\acute{e}t}(\mathrm{Spec}(\mathcal{O}_{K,S}))$, where $\mathcal{O}_{K,S}$ denotes the localization of $\mathcal{O}_K$ outside the primes in S, is the Galois group of the maximal extension of K unramified outside S.

2.3 Galois Groups and Fundamental Groups, Intertwined

We've so far considered covers of $\mathrm{Spec}(A)$ when A is an affine coordinate ring and when A is a field. These give us topological covers of some space and extensions of some field, respectively. Can we find a ring A that combines both worlds?

The reason affine coordinate rings of complex varieties reflect *geometric* phenomena is that the base field is algebraically closed. Let us consider a variety over $\mathbb{Q}$. That is, let us consider a system of polynomials $f_1, \cdots, f_s$ in m variables with rational coefficients. We then consider the ring $\mathbb{Q}[x_1, \cdots, x_m]/(f_1, \cdots, f_s)$. Note that we could replace $\mathbb{Q}$ by any number field, but we omit this generality for simplicity.

This ring has various étale extensions. Some correspond to algebraic extensions of $\mathbb{Q}$, the simplest being $\mathbb{Q}(\sqrt{2})[x_1, \cdots, x_m]/(f_1, \cdots, f_s)$. Others correspond to actual geometric maps of varieties. Some are a combination of the two. We can formalize this by considering the string of homomorphisms

$$\mathbb{Q} \to \mathbb{Q}[x_1, \cdots, x_m]/(f_1, \cdots, f_s) \to \mathbb{C}[x_1, \cdots, x_m]/(f_1, \cdots, f_s).$$

We should note that we want the polynomials to be such that $\mathbb{C}[x_1, \cdots, x_m]/(f_1, \cdots, f_s)$ is an integral domain, i.e. the variety X it corresponds to is irreducible over $\mathbb{C}$ (we say *geometrically irreducible*). These maps of rings give rise to maps

$$\mathrm{Spec}(\mathbb{C}[x_1, \cdots, x_m]/(f_1, \cdots, f_s)) \to \mathrm{Spec}(\mathbb{Q}[x_1, \cdots, x_m]/(f_1, \cdots, f_s)) \to \mathrm{Spec}(\mathbb{Q}).$$

As per functoriality of $\pi_1^{\acute{e}t}$, we should have a sequence of group homomorphisms

$$\pi_1^{\acute{e}t}(\mathrm{Spec}(\mathbb{C}[x_1, \cdots, x_m]/(f_1, \cdots, f_s))) \to \pi_1^{\acute{e}t}(\mathrm{Spec}(\mathbb{Q}[x_1, \cdots, x_m]/(f_1, \cdots, f_s))) \to \pi_1^{\acute{e}t}(\mathrm{Spec}(\mathbb{Q})).$$

Assuming the variety is nonsingular, it turns out that this sequence is exact, with the last map surjective. The idea behind this is that $\mathrm{Spec}(\mathbb{Q}[x_1, \cdots, x_m]/(f_1, \cdots, f_s))$ is somehow like a fiber bundle (or fibration) over $\mathrm{Spec}(\mathbb{Q})$ with fiber $\mathrm{Spec}(\mathbb{C}[x_1, \cdots, x_m]/(f_1, \cdots, f_s)))$. This idea might seem strange, given that $\mathrm{Spec}(\mathbb{Q})$ is just a point. But recall that it is a point with nontrivial loops, with nontrivial *monodromy.* In particular, it can have nontrivial fiber bundles over it. To talk about the fiber over a point, we want to talk about the fiber over a *simply connected point.* To that end, we look at the fiber over $\mathrm{Spec}(\mathbb{C}) \to \mathrm{Spec}(\mathbb{Q})$, and this is where it all comes from.

It turns out, furthermore, that the first map is injective. Equating $\pi_1^{\acute{e}t}(\mathrm{Spec}(\mathbb{C}[x_1, \cdots, x_m]/(f_1, \cdots, f_s)))$ with $\pi_1\widehat{(X(\mathbb{C})})$ and $\pi_1^{\acute{e}t}(\mathrm{Spec}(\mathbb{Q}))$ with $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, we have a short exact sequence

$$0 \to \pi_1\widehat{(X(\mathbb{C})}) \to \pi_1^{\acute{e}t}(\mathrm{Spec}(\mathbb{Q}[x_1, \cdots, x_m]/(f_1, \cdots, f_s))) \to \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to 0.$$

As it turns out, this exact sequence was known to Zariski, who came up with the notion of ”algebraic fundamental group” of a variety, a precursor to the notion of étale fundamental group. We call this exact sequence the *fundamental exact sequence.*

We now note an interesting connection with Diophantine equations, namely the study of rational solutions to polynomial equations. A solution $(x_1, \cdots, x_m)$ to the equations

$$f_1(x_1, \cdots, x_m) = f_2(x_1, \cdots, x_m) = \cdots = f_s(x_1, \cdots, x_m) = 0$$

with *rational* coordinates $x_1, \cdots, x_m$ is the same as a $\mathbb{Q}$-algebra homomorphism

$$\mathbb{Q}[x_1, \cdots, x_m]/(f_1, \cdots, f_s) \to \mathbb{Q}.$$

This is therefore the same as a map $\mathrm{Spec}(\mathbb{Q}) \to \mathrm{Spec}(\mathbb{Q}[x_1, \cdots, x_m]/(f_1, \cdots, f_s))$ such that the composition

$$\mathrm{Spec}(\mathbb{Q}) \to \mathrm{Spec}(\mathbb{Q}[x_1, \cdots, x_m]/(f_1, \cdots, f_s)) \to \mathrm{Spec}(\mathbb{Q})$$

is the identity. In particular, by functoriality of $\pi_1^{\acute{e}t}$, this gives a splitting of the fundamental exact sequence. This means, for example, that if one could compute the fundamental exact sequence of a particular variety and then show that it does not split, one would have proven that the equations have no rational solutions. More specifically, Grothendieck showed that if X is a hyperbolic curve (an algebraic curve of genus $g \geq 2$), then each rational point corresponds to a unique section. In particular, if he could prove that the fundamental exact sequence has finitely many splittings, then he could prove Mordell's famous conjecture that such a curve has finitely many rational points! Unfortunately, no one has been able to make good on this approach, and Faltings later proved the Mordell conjecture using different methods.

Furthermore, Grothendieck conjectured that for hyperbolic curves, *every splitting comes from a rational point.* This is the famous section conjecture in anabelian geometry. The term "anabelian" refers to the marked lack of abelian-ness of the fundamental groups of hyperbolic curves and the fact that this might limit the number of splittings of the fundamental exact sequence.

We note one more consequence of the fundamental exact sequence. The group

$$\pi_1^{\acute{e}t}(\mathrm{Spec}(\mathbb{Q}[x_1, \cdots, x_m]/(f_1, \cdots, f_s)))$$

acts on itself by conjugation, and since $\pi_1\widehat{(X(\mathbb{C}))}$ is a normal subgroup, this action restricts to $\pi_1\widehat{(X(\mathbb{C}))}$. We therefore have a homomorphism

$$\pi_1^{\acute{e}t}(\mathrm{Spec}(\mathbb{Q}[x_1, \cdots, x_m]/(f_1, \cdots, f_s))) \to \mathrm{Aut}(\pi_1\widehat{(X(\mathbb{C}))})$$

, which we compose with the quotient map

$$\mathrm{Aut}(\pi_1\widehat{(X(\mathbb{C}))}) \to \mathrm{Out}(\pi_1\widehat{(X(\mathbb{C}))})$$

to the group of *outer automorphisms* of $\pi_1\widehat{(X(\mathbb{C}))}$, the quotient of the group of all automorphisms by the group of inner automorphisms. Since $\pi_1\widehat{(X(\mathbb{C}))} \subseteq \pi_1^{\acute{e}t}(\mathrm{Spec}(\mathbb{Q}[x_1, \cdots, x_m]/(f_1, \cdots, f_s)))$ acts by inner automorphisms on itself, it maps to the identity in the group of outer automorphisms. This induces a homomorphism

$$Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Out}(\pi_1\widehat{(X(\mathbb{C}))}),$$

known as the outer action of the Galois group on the étale fundamental group. More concretely, a cover of a variety over $\mathbb{Q}$ is defined over some extension of $\mathbb{Q}$, and we can apply any element of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ to the defining equations of the cover to get a new topological cover, and this defines the outer action. A famous theorem of Belyi shows that this outer action is faithful (i.e. the homomorphism is injective) when X is $\mathbb{C} \setminus \{0, 1\}$. In particular, this means that we can understand $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ through its action on something slightly more concrete, namely the outer automorphisms of the profinite completion of the free group on two generators. This can be built into something combinatorial, which is known as the theory of *Dessins d'enfant.*

The existence of a homomorphism to $\mathrm{Out}(\pi_1\widehat{(X(\mathbb{C}))})$ is vaguely reminiscent of the mapping class group in Teichmuller theory. In fact, this has given rise to a field known as Grothendieck-Teichmuller theory.