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.

This survey is aimed at those with a basic background in (1) Galois theory and (2) fundamental groups and covering spaces. A little bit of algebraic geometry (such as the first two chapters of [SKKT00]) would be helpful, but we explain concepts as we go along. Now and then, we make references to algebraic number theory, but these are not necessary to follow the text.

For a more detailed resource on this topic, I suggest the book [Sza09], aptly titled "Galois Groups and Fundamental Groups."

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.

1.1.1 Galois Groups

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

$$L/M/K,$$

where $H = \mathrm{Gal}(L/M)$.

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* $G_K := \mathrm{Gal}(\overline{K}/K)$ of K. Then $H = G_M$.

If H_1, H_2 are subgroups corresponding to intermediate extensions M_1, M_2, then $H_1 \subseteq H_2$ iff

$$M_2 \subseteq M_1.$$

In other words, *a smaller subgroup corresponds to a larger extension.* The whole group $H = \mathrm{Gal}(L/K)$ corresponds to K, and the trivial subgroup $H = \{\mathrm{id}\}$ corresponds to L. There is a notion of degree $[M : K]$ 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 H in $\mathrm{Gal}(L/K)$. Finally, the subgroup H is normal iff the corresponding field extension M/K is normal. In that case, there is an isomorphism between $\mathrm{Gal}(L/K)/H$ and the group $\mathrm{Gal}(M/K)$ of automorphisms of the field extension M/K. Finally, a field 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.

1.1.2 Fundamental Groups

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

$$Y \to X.$$

Then our M before corresponds to Y, and $\overline{K}$ corresponds to the universal cover $\tilde{X}$. We have $H_1 \subseteq H_2$ iff Y_1 dominates Y_2, again meaning that *a smaller subgroup corresponds to a larger cover.* The whole group $H = \pi_1(X)$ corresponds to X, and the trivial subgroup $H = \{\mathrm{id}\}$ 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 (functor) associating a group to each of some class of objects, such that both 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, affine or 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 §1.3.

We will eventually see in §2.3 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. For now, 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. Much of the ideas in §1.2 can be learned in a basic course on algebraic geometry; we highly recommend [SKKT00], especially [SKKT00, §2.5-6]. See also [EH00, I.1].

First, 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 (holomorphic).

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 (commutative) 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, denoted $\mathbb{C}[x_1, \cdots, x_n]$. 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 (of the appropriate kind, i.e., differentiable or continuous or whatever), 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 between the corresponding 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 on X (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 $\mathbb{C}$, sending a function f to its value $f(P)$ at P. In general, this map will be surjective, and since $\mathbb{C}$ is a field, the kernel will be a maximal ideal. This is the ideal of *functions that vanish at* P and is denoted $\mathfrak{m}_P$. 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 (is in $\mathfrak{m}_Q$) iff $f \circ r$ vanishes at P (i.e., is in $\mathfrak{m}_P$). In particular, $\mathfrak{m}_Q$ is the preimage of $\mathfrak{m}_P$ under the ring homomorphism induced by r. In particular, if we didn't know the function r but only knew the ring homomorphism induced by r, we might be able to detect that $r(P) = Q$ by seeing what happens to maximal ideals under the ring homomorphism.

There is an important observation that, in many contexts (for example, the ring of continuous functions on a compact Hausdorff space, or the coordinate ring of an affine algebraic variety), 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 $\mathbb{Z}$; for example, they are both principal ideal domains. The maximal ideals of $\mathbb{Z}$ correspond to the prime numbers. Therefore, one might pretend that there is some space whose points are in bijection with the set of prime numbers. Under this analogy, the ring $\mathbb{Z}$ is the set of functions on that 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 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, the finite field of order p. In this bizarre world, the values of a single function at different points live in different fields. This is pointed out in 3.2.1 of `http://math.stanford.edu/~vakil/216blog/FOAGnov1817public.pdf`.

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 put this in analogy with $\mathbb{C}[\sqrt{z}]/\mathbb{C}[z]$; our geometric intuition from the latter case will then help us better understand extensions like $\mathbb{Z}[i]/\mathbb{Z}$. In particular, it will give us a geometric way to think about how primes of $\mathbb{Z}$ split in $\mathbb{Z}[i]$ (for example, 3 is prime in $\mathbb{Z}[i]$, $5 = (2+i)(2-i)$, and 2 is divisible by $(1+i)^2$). In the next section, we talk about the relationship between field extensions of $\mathbb{C}[z]$ and fundamental groups.

For more details on the analogy between number rings and ring of functions, see §2.6 of `http://www-math.mit.edu/~poonen/papers/curves.pdf`.

1.3 Fundamental Groups of Punctured Planes and Galois Groups

1.3.1 The Squaring Map

We now switch gears and talk about actual fundamental groups. We consider the simple covering map p from the complex plane $\mathbb{C}$ to itself given by sending a complex number to its square.

We recall some important terminology that applies to all covering maps: *If p is a covering map, then the domain of p is called the cover, and the range of p is called the base.*

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

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

We include a diagram on the next page. The w plane lies twisted above the z plane so that every point w_0 lies directly above $z_0 = p(w_0)$. The figure isn't really supposed to intersect itself; unfortunately, you would need four dimensions to draw it properly, and this is not a four-dimensional document.

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, you can show that this can't be a covering map because $\mathbb{C}$ is simply connected, so it has no connected coverings!)

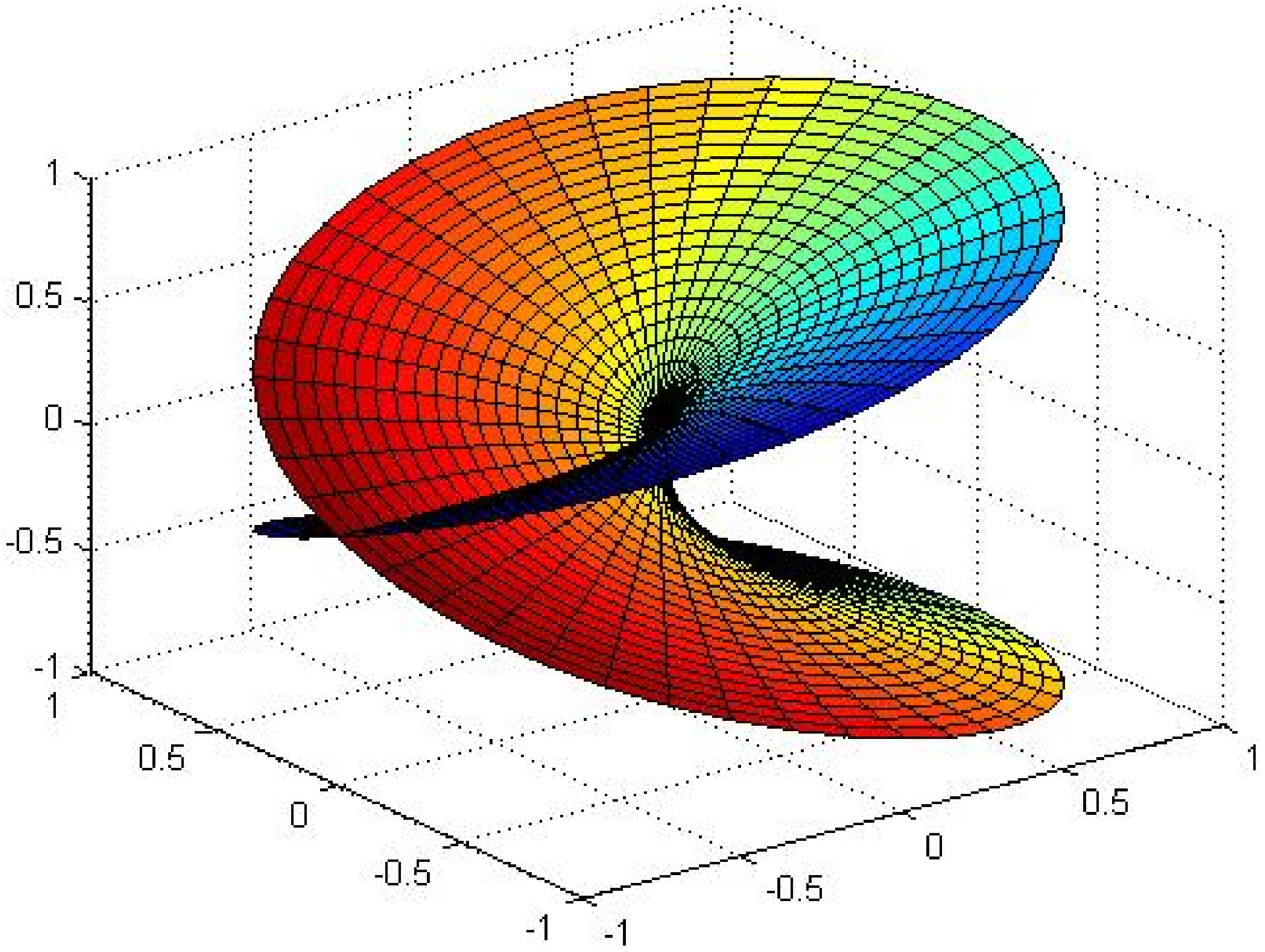

Figure 1.1: http://upload.wikimedia.org/wikipedia/commons/b/b5/Riemann_sqrt.jpg

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 nonzero complex number to its square. One can in fact show that this map (the one from $\mathbb{C} \setminus \{0\}$ to $\mathbb{C} \setminus \{0\}$) is a covering map. (To prove that it is a covering map, one can note that the complex derivative, or Jacobian determinant if you don't like complex analysis, vanishes nowhere, and then use the inverse function theorem to show the map is a local homeomorphism.) 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 automorphism, σ, sending w to $-w$. Then σ respects the covering p because $p(w) = w^2 = (-w)^2 = p(-w) = p(\sigma(w))$; in other words, σ is a *deck transformation.*[1] This nontrivial deck transformation corresponds to the nontrivial element of

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

in that for any w and a path γ from w to $\sigma(w)$, the path $p(\gamma)$ is a loop based at $p(w) = p(\sigma(w))$ representing this element of $\pi_1(\mathbb{C} \setminus \{0\})/2\pi_1(\mathbb{C} \setminus \{0\})$.

Caveat: *σ is a map from the cover to itself. It does not involve the base.*

We know that this is the cover of $\mathbb{C} \setminus \{0\}$ of degree 2 simply because every point has two preimages. But if you want to think about fundamental groups in terms of actual loops, note that squaring in the complex plane wraps the unit circle around itself twice, meaning it corresponds to doubling in the fundamental group. Therefore, p gives the multiplication-by-2 map on $\pi_1(\mathbb{C} \setminus \{0\})$.

Next, consider the ring $\mathbb{C}(z)$ of rational functions in z. 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 other words, *we may think of the ring $\mathbb{C}(z)$ as a ring of functions on the base of p.* Similarly, we may think of $\mathbb{C}(w)$ as a ring of functions on the cover associated to p.

Under the map p, the function assigning to each point of $\mathbb{C} \setminus \{0\}$ its coordinate z pulls back to the function w^2 on the w-plane. This map p corresponds therefore to an inclusion

$$p^* : \mathbb{C}(z) \hookrightarrow \mathbb{C}(w)$$

of fields sending z to w^2.

The relation $z = w^2$ is essentially the same as $w = \sqrt{z}$, and we can view $\mathbb{C}(w)$ as the field extension $\mathbb{C}(z)[\sqrt{z}]$. More formally, we have

$$\mathbb{C}(w) = \mathbb{C}(z)[w]/(w - z^2).$$

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 $\sqrt{z}$ to $-\sqrt{z}$, or w to $-w$. In particular, *it is the ring homomorphism induced by σ* under Principle 1.2.1.

[1] Recall that if $p\colon Y \to X$ is a covering map, then a deck transformation is a map σ from Y *to itself* such that $p = p \circ \sigma$.

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

More generally, consider the map $p_k \colon w \mapsto z = w^k$, for $k \in \mathbb{N}$. Then the preimage of $z = a \in \mathbb{C}$ consists of all kth roots of a. What are the kth roots of a? Well if $w = \sqrt[k]{a}$ denotes one of them, then all of them are of the form

$$\{\zeta_k^n w\}_{n \in \mathbb{Z}},$$

where ζ_k is a primitive kth root of unity. Since the expression $zeta_k^n w$ depends only on n modulo k, there are exactly k kth roots of a. On the other hand, if a is 0, then it has only one preimage, and as before, the map p_k is a covering only when restricted to a map $\mathbb{C} \setminus \{0\} \to \mathbb{C} \setminus \{0\}$. In fact, p_k is the unique degree k connected cover of $\mathbb{C} \setminus \{0\}$, and it corresponds[2] to the subgroup

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

Pullback of rational functions along this map is none other than the inclusion of fields

$$\mathbb{C}(z) \hookrightarrow \mathbb{C}(w = \sqrt[k]{z}),$$

or in other words the field extension $\mathbb{C}(w)/\mathbb{C}(z)$. Its Galois group $\mathrm{Gal}(\mathbb{C}(w)/\mathbb{C}(z))$ is generated by the automorphism

$$w \mapsto \zeta_k w.$$

But this is precisely the formula for a deck transformation of the cover

$$p_k \colon \mathbb{C} \setminus \{0\} \to \mathbb{C} \setminus \{0\};$$

more specifically, we get a natural isomorphism

$$\pi_1(\mathbb{C} \setminus \{0\})/k\pi_1(\mathbb{C} \setminus \{0\}) \cong \mathrm{Gal}(\mathbb{C}(w)/\mathbb{C}(z)) \cong \mu_k := \{\zeta_k^j : \ 0 \le j \le k-1\},$$

where μ_k denotes the group of kth roots of unity in $\mathbb{C}$. In this way, all finite covers of $\mathbb{C} \setminus \{0\}$ correspond to certain Galois extensions of the field $\mathbb{C}(z)$, and the groups of deck transformations can be recovered as the Galois groups of these field extensions.

What if we wanted to write down the universal cover? The universal cover is given by the exponential map from $\mathbb{C}$ to $\mathbb{C} \setminus \{0\}$. The fundamental group $\pi_1(\mathbb{C} \setminus \{0\})$ acts on this universal cover by sending $n \in \pi_1(\mathbb{C} \setminus \{0\})$ to the automorphism of $\mathbb{C}$ given by $z \mapsto z + 2\pi i n$. The preimage of $1 \in \mathbb{C} \setminus \{0\}$ under the exponential map is the subgroup $2\pi i\mathbb{Z} \subseteq \mathbb{C}$. Choosing the point $0 \in \mathbb{C}$, we have a natural identification between $\pi_1(\mathbb{C} \setminus \{0\})$ and $2\pi i\mathbb{Z} \subseteq \mathbb{C}$.

However, we wish to do algebraic geometry; and for that reason, we cannot consider the universal cover, because the exponential map is not a polynomial map. One 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 $\mathbb{C}(z)$. For any group G, there is a topological group,

[2] under the standard one-to-one correspondence between connected covering spaces and subgroups of the fundamental group. If $Y \to X$ is a connected cover, then Y corresponds to the image of the induced map $\pi_1(Y) \to \pi_1(X)$.

$\widehat{G}$, 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. There 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 $\widehat{\mathbb{Z}}$, which we describe in more detail in the next section. In this case, $\widehat{\mathbb{Z}}$ is the (infinite) Galois group of the extension of the field $\mathbb{C}(z)$ attained by adjoining all kth roots of z. I won't say precisely what this means now, but this implies that the étale fundamental group

$$\pi_1^{\text{ét}}(\mathbb{C} \setminus \{0\}) \cong \widehat{\mathbb{Z}}.$$

1.3.3 Ramified Covers of the Complex Plane

Now, I'd like to go back for a second to the map $p : \mathbb{C} \to \mathbb{C}$ (sending $w \in \mathbb{C}$ to $z = w^2 \in \mathbb{C}$) which is manifestly *not* a covering. It is, however, something more general, known as a *ramified cover*. The point $z = 0$ over which the map is not a cover is called a *branch point*, and its preimage $w = 0$ 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 z-plane) is associated the ideal $(z - a)$ in the ring $\mathbb{C}[w]$. Consider the image of $z - a$ in the ring $\mathbb{C}[z]$. It maps to $w^2 - a \in \mathbb{C}[w]$. If $a \neq 0$, it splits as a product of two distinct irreducibles in $\mathbb{C}[w]$, namely, $w - \sqrt{a}$ and $w + \sqrt{a}$. If $a = 0$, then it is simply a nontrivial power of a single irreducible polynomial, namely w^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 $\mathbb{C}[w]$, and the ideal associated to $z = 0$ 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 $(1 + i)^2$. This phenomenon is known as *ramification* in algebraic number theory; to learn more about it, consult a standard book on algebraic number theory, such as [Mar18] or [Sam70]. For the case of quadratic extensions, see Chapter 13 of Michael Artin's book Algebra.

Remark 1.3.1. The reader may object that *none* of the irreducibles of $\mathbb{C}[z]$ remain irreducible in $\mathbb{C}[w]$, whereas some prime numbers remain prime in $\mathbb{Z}[i]$ (more specifically, it is the set of primes congruent to 3 modulo 4, such as $3, 7, 11, 19, \cdots$). For this, we could consider the extension $\mathbb{R}[w = \sqrt{z}]/\mathbb{R}[z]$. Here, ideals $z - a$ for a positive or zero work exactly as before, while $z - a$ for a negative are just like the prime 3 in $\mathbb{Z}[i]$.

More generally, suppose we have a map $f : \mathbb{C} \to \mathbb{C}$ given by a polynomial $z = f(w)$. Then the map is ramified precisely at those points w_0 for which $f'(w_0) = 0$ (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 $\mathbb{C}(w)$ of $\mathbb{C}(z)$ obtained by sending z to $f(w)$. 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 1.3.2. Consider the polynomial $f(w) = w^3 - 6w^2 + 9w + 1$, so that $\mathbb{C}(w) = \mathbb{C}(z)[w]/(w^3 - 6w^2 + 9w + 1 - z)$. We have $f'(w) = 3w^2 - 12w + 9$, which factors as $3(w-1)(w-3)$, 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 $\pi_1(\mathbb{C} \setminus \{1, 5\})$. Let K be the Galois closure of $\mathbb{C}(w)$ over $\mathbb{C}(z)$; then K corresponds to a normal cover of $\mathbb{C} \setminus \{1, 5\}$, and the Galois group $\mathrm{Gal}(K/\mathbb{C}(z))$ 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 $w^3 - 9w^2 + 18w - z$, a root of which gives a Galois cubic extension over $\mathbb{C}(z)$.) 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.

1.3.4 The Correspondence Between Galois Groups and Fundamental Groups

More generally, any finite field extension $K/\mathbb{C}(z)$ 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 $w \in K$ such that $g(w, z) = 0$ for some $g(x, z) \in \mathbb{C}[x, z]$,[3] then consider the set $\{X := (w, z) \in \mathbb{C}^2 \mid g(w, z) = 0\}$. This set X maps onto $\mathbb{C}$ by sending (w, z) to z. One can show that this is a ramified cover and that it corresponds to the field extension K in the same way as before. If its set of branch points (the images under the map of the ramification points, i.e. the points at which the derivative vanishes) is S, then it gives a topological covering[4] of $\mathbb{C} \setminus S$, hence corresponds to a subgroup of $\pi_1(\mathbb{C} \setminus S)$. In particular, if $K/\mathbb{C}(z)$ is chosen to be Galois, then there is a natural map

$$\pi_1(\mathbb{C} \setminus S) \to \mathrm{Gal}(K/\mathbb{C}(z))$$

whose kernel is $\pi_1(X)$.

Remark 1.3.3. 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 $L/K/\mathbb{C}(z)$, 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.

We've now explained how every finite field extension of $\mathbb{C}(z)$ gives rise to some finite topological cover of an open subset of $\mathbb{C}$. Conversely, suppose we have a topological covering of $\mathbb{C} \setminus S$ for some finite set S. Then the famous *Riemann Existence Theorem* 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 $\mathbb{C}(z)$. This has an interesting application. Let G be an

[3] In other words, for some polynomial g in one variable x with coefficients in the ring $\mathbb{C}[z]$.

[4] Technically it could be an open subset of a topological covering, but we will not worry about this point here. The reader with a background in algebraic geometry will note that this does not matter because we are considering function fields rather than coordinate rings.

arbitrary finite group. Then it can be generated by some number of elements, say n. Let S be a set of n complex numbers. Then $\pi_1(\mathbb{C} \setminus S)$ is the free group on n generators, which has G as one of its quotients. Thus there is a finite covering X of $\mathbb{C} \setminus S$ with covering group G. It then corresponds to a field extension $K/\mathbb{C}(z)$ with Galois group G. In particular, *every finite group is the Galois group of an extension of* $\mathbb{C}(z)$. What's amazing is that we proved this using topology.

Let's fix a particular finite set $S \subseteq \mathbb{C}$ and try to understand $\pi_1(\mathbb{C} \setminus S)$ in terms of Galois theory. Luckily, the compositum of two fields unramified above a point is again unramified above that point. Therefore, for a given set of points S, we can take the compositum K_S of all finite extensions $K/\mathbb{C}(z)$, whose branch points are contained in S. Then K_S is a Galois algebraic (but not necessarily finite) extension of $\mathbb{C}(z)$, and there is a natural map

$$\pi_1(\mathbb{C} \setminus S) \to \mathrm{Gal}(K_S/\mathbb{C}(z)).$$

Riemann's existence theorem would seem to suggest that this is an isomorphism; that is almost true, but not quite. Let's think about the case $S = \{0\}$. Then $\pi_1(\mathbb{C} \setminus S) = \mathbb{Z}$, while

$$K_S = \mathbb{C}(z)[\{\sqrt[k]{z}\}_{k \in \mathbb{N}}].$$

In Galois theory, everything comes from finite extensions; in particular, the infinite Galois group $\mathrm{Gal}(K_S/\mathbb{C}(z))$ is not $\mathbb{Z}$, but rather the inverse limit $\varprojlim_k \mathbb{Z}/k\mathbb{Z}$ known as $\widehat{\mathbb{Z}}$. This is the group of all compatible systems of elements of $\mathbb{Z}/k\mathbb{Z}$, i.e.

$$\widehat{\mathbb{Z}} = \left\{ (n_k)_k \in \prod_k \mathbb{Z}/k\mathbb{Z} \,\middle|\, n_k \equiv n_{k'} \pmod{k} \text{ if } k \mid k' \right\}$$

Thus the map

$$\pi_1(\mathbb{C} \setminus S) \to \mathrm{Gal}(K_S/\mathbb{C}(z)).$$

is not an isomorphism, but it does induce a bijection between all *finite quotients* of the left- and right-hand sides. In particular, this map realizes $\mathrm{Gal}(K_S/\mathbb{C}(z))$ as the profinite completion $\widehat{\pi_1(\mathbb{C} \setminus S)}$ of $\pi_1(\mathbb{C} \setminus S)$.

We now have an isomorphism

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

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 1.3.4. In a very technical sense, there is really a canonical *anti-isomorphism* between the Galois group and the fundamental group, 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 $\mathbb{C}(z)$ 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. The étale fundamental group was first introduced in the massive work [SGA03]. We refer to [Sza09, Chapter 5] for a gentle modern treatment.

We will greatly use the two principles from last time. Before we begin, we review affine varieties.

2.1 Affine Varieties

A very good reference is once again [SKKT00]. We also recommend [Sil09, Chapter I].

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 P. 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

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

This is explained on p.24-25 of [SKKT00].

2.1.1 Fundamental Groups of Affine Varieties

Let's bring topology back into the picture. $\mathbb{C}^m$ 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. One reason for wanting such a ring-theoretic criterion 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.

Such a criterion exists, and it is the notion of a *(finite) étale* map of rings. This is precisely why the word “étale” pops up so often in things like étale fundamental groups, étale cohomology, and so on.

Thus 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. However, *what's most important to know is simply that there exists an abstract ring-theoretic condition corresponding to a covering map.*

2.1.2 Sketch of the Definition of Etale

In Terms of Ramification

Let's recall some notation from §1.3.3. Recall that the map $p_k \colon \mathbb{C} \to \mathbb{C}$ is not a covering map because of the existence of branch points. Our intuition is therefore that a covering map is simply a map without branch points. We would therefore like an algebraic criterion for determining whether a map of rings has branch points (equivalently, ramification points).

Remark 2.1.1. Technically, as we'll see, the notion of being a covering map is a little more restrictive than just not having branch points. A map without branch points is always *an open subset of a covering map*,[1] and is known as a *local homeomorphism* (more on what that means below). A standard example of a local homeomorphism that is not a covering map would be the map

$$p_k \colon \mathbb{C} \setminus \{0, 1\} \to \mathbb{C} \setminus \{0\}.$$

This difference corresponds to the difference between étale and finite étale (the former corresponding to local homeomorphisms). A finite étale map is essentially an étale map such that every point on the base has "enough preimages," while an étale map is the composition of a finite étale map with the inclusion of an open set.

Recall furthermore from §1.3.3 a ring-theoretic avatar of the fact that 0 is a branch point of p_k. This was the fact that the irreducible polynomial z splits in $\mathbb{C}[w]$ as a nontrivial power w^k, where $k > 1$. Therefore, as an approximate definition, we might say that a map $f \colon A \to B$ of rings is étale if for every prime ideal $\mathfrak{p}$ of A, the ideal $\mathfrak{p}B$ does not have any repeated factors (in a sense, is "square-free").

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 $S_{\mathfrak{p}}$ (rather than onto a power of it, say). Then a map is étale if it is flat, locally of finite presentation, and unramified.

In Terms of Local Homeomorphisms

First, let's say a little bit more about what "local homeomorphism" means. Obviously, a nontrivial cover is not a homeomorphism, for any point $x \in X$ has multiple preimages. But you might not

[1] In algebraic geometry, the fact that any étale map may be factored by an open immersion followed by a finite étale map is nontrivial and follows from Zariski's Main Theorem.

object that it's not even locally a homeomorphism, because no matter how small a neighborhood you take of X, the map is not a homeomorphism on that neighborhood. The key is that it is locally *on* Y a homeomorphism. In other words, "local homeomorphism" means that it is a homeomorphism when we restrict to an open neighborhood of some preimage y of X. And indeed, for any $y \in Y$, there exists a neighborhood of h such that the restriction of the covering map to that neighborhood is a homeomorphism onto its image.

Our motivation now comes from differential geometry. If we're considering maps of smooth 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.

This already seems somewhat more algebraic, because we can define derivatives of polynomials in a purely formal and algebraic way. However, we would like something even 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 to the variety at P 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, and it is the definition of étale in that case.

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. This is equivalent to the other definition of étale for rings satisfying reasonable conditions.

More on Etale vs. Finite Etale

This subsection is already getting quite technical. But feel free to read it if you're bugged by the adjective "finite" always appearing before "étale."

As we've said, not every local homeomorphism is a covering. For an even simpler example than in Remark 2.1.1, the inclusion of an open subset U into a space X (also known as an *open immersion*) is locally a homeomorphism, but it is clearly not a covering.

What condition on a local homoeomorphism ensures that it's a covering map? We might, as a first approximation, 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.

Let's explain why the word "finite" appears. 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 in algebraic geometry to the ring homomorphism $\mathbb{C}[z] \to \mathbb{C}[z]\left[\frac{1}{z}\right]$ (because when we restrict to $\mathbb{C} \setminus \{0\}$, z becomes invertible). Since we can consider arbitrarily high powers of $\frac{1}{z}$, the ring $\mathbb{C}[z]\left[\frac{1}{z}\right]$ 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.

More specifically, a map $A \to B$ of rings is *finite étale* if it is finite and étale. It is this ring-theoretic criterion that corresponds precisely to covering maps in topology.

2.2 Grothendieck's Approach and Etale Fundamental Groups

2.2.1 Spaces and Rings

We recommend [SKKT00, §2.5-6] and [EH00, I.1] as companion reading to this section.

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. In other words, we have an *anti-equivalence of categories* between affine algebraic varieties over $\mathbb{C}$ and reduced finitely-generated $\mathbb{C}$-algebras (see [SKKT00, §2.5] or [EH00, p.8]).

Grothendieck's 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." Put another way, he simply *defined* the category of affine schemes to be the opposite of the category of rings.

Taking this (imagined) analogy further, the "points" of this "space" $\operatorname{Spec} A$ 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 $\operatorname{Spec} B \to \operatorname{Spec} A$ 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:

Definition 2.2.1. We define a covering of an affine scheme A to be a map $\operatorname{Spec} B \to \operatorname{Spec} A$ such that the map of rings $A \to B$ is finite étale.

Note that once we know what 'finite étale' means, this definition is nothing more than a formality.

A deck transformation of such a covering is just an automorphism of B that restricts to the identity on the image of A.

2.2.2 Etale Fundamental Groups

Now let's suppose we have a ring A and we want to compute the fundamental group of $\operatorname{Spec} A$. Then we should consider each connected $\operatorname{Spec} B \to \operatorname{Spec} A$ and its group of deck transformations.

Note that we have defined "covering" but not "connected." But the idea is 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 product 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 product of two other rings. Therefore, we say $\operatorname{Spec} B$ is connected if B is not the direct sum of two other rings. In general, we should require $\operatorname{Spec} A$ to be connected from the start, as we should consider fundamental groups only of connected spaces.

Now we want to construct a group $\pi_1^{\text{ét}}(\operatorname{Spec} A)$ whose subgroups correspond to the covers of $\operatorname{Spec} A$. For this, we focus on its normal subgroups. If N is a normal subgroup of $\pi_1^{\text{ét}}(\operatorname{Spec} A)$, then N corresponds to a covering $\operatorname{Spec} B \to \operatorname{Spec} A$ for which $\pi_1^{\text{ét}}(\operatorname{Spec} A)/N$ is isomorphic to the group of deck transformations of this covering. (If N is not normal, then the corresponding covering will not have enough deck transformations, just as non-Galois field extensions don't have enough automorphisms.) As mentioned above, the set of deck transformations is the set of automorphisms of B that act as the identity on A, aka the automorphisms of B as an A-algebra.[2] We thus should

[2] Again, as mentioned in an earlier footnote, the group structure is the *opposite* because of contravariance.

have

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

We can thus define the *étale fundamental group*

$$\pi_1^{\text{ét}}(\operatorname{Spec} A) := \varprojlim \operatorname{Aut}_A(B)$$

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"!

Spoiler (more details below): The étale fundamental group of an affine variety is just the profinite completion of the ordinary topological fundamental group. On the other hand, if $A = K$ is a field, then $\pi_1^{\text{ét}}(\operatorname{Spec} A)$ is just $G_K = \operatorname{Gal}(\overline{K}/K)$, the absolute Galois group of K!

In more detail, 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

$$\pi_1^{\text{ét}}(\operatorname{Spec} A(X)) \cong \pi_1\widehat{(X(\mathbb{C})}),$$

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

We thus have a purely algebraic way to define the fundamental group of a complex algebraic variety; no loops or continuous maps involved! One might ask whether we can recover the fundamental group of a variety, not only its profinite completion, in a purely algebraic manner; i.e. solely from the ring $A(X)$. This method doesn't seem to work, but you might wonder if there is a different way. As it turns out, Serre provided an example that proves there is no different way. (I sometimes refer to this as "Theorem: Too Bad"; that even made it onto a t-shirt.)

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 ([Ser64]). 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 recover only its finite quotients.

2.2.3 Galois Groups as Fundamental Groups

We have recovered the fundamental group of a variety, or at least its finite quotients, in a purely algebraic way, thus answering one of the original questions. But we have done something even deeper: we've found a construction (étale fundamental group of a(n affine) scheme) such that when we input a space, we get its fundamental group, and when we input a field, we get its (absolute) Galois group.

As mentioned above, if K is a field, then

$$\pi_1^{\text{ét}}(\operatorname{Spec} K) \cong \operatorname{Gal}(\overline{K}/K).$$

(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 saying that the derivative of the polynomial defining the extension doesn't vanish identically. But if the derivative were to vanish identically, then *every* point would be a ramification point.

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 $\operatorname{Spec} B \to \operatorname{Spec} A$ of spaces should induce a homomorphism $\pi_1^{\text{ét}}(\operatorname{Spec} B) \to \pi_1^{\text{ét}}(\operatorname{Spec} A)$, and it in fact does. In the case of a separable algebraic extension $K \hookrightarrow L$, the map $\operatorname{Spec} L \to \operatorname{Spec} K$ induces the natural inclusion $\operatorname{Gal}(\overline{L}/L) \hookrightarrow \operatorname{Gal}(\overline{K}/\overline{L})$.

In particular, a K is separably closed iff $\operatorname{Spec} K$ 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 $\operatorname{Spec} A$ 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 $\operatorname{Spec} K$ 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 $\operatorname{Spec} K$ tells us very little about the actual "geometry" of $\operatorname{Spec} K$. In modern language, one would say that the Zariski site of $\operatorname{Spec} K$ is trivial, but the étale site is very interesting.

Let's go back to our discussion in §1.3.4 about the fundamental group of $X = \mathbb{C} \setminus S$, where $S = \{a_1, \cdots, a_n\}$. You may convince yourself that X is the set of solutions to the equation

$$(x - a_1)(x - a_2) \cdots (x - a_n)y = 1,$$

so its coordinate ring is

$$A(X) = \mathbb{C}[x]\left[\frac{1}{(x - a_1)(x - a_2) \cdots (x - a_n)}\right].$$

As mentioned above, we must have $\pi_1^{\text{ét}}(\operatorname{Spec} A(X)) = \widehat{\pi_1(\mathbb{C} \setminus S)}$. We also recall our definition of K_S as the compositum of all extensions of $\mathbb{C}(z)$ coming from covers with branch points in S. Then if you unravel the definition of étale, it turns out that, almost by definition, we have

$$\pi_1^{\text{ét}}(\operatorname{Spec} A(X)) = \operatorname{Gal}(K_s/\mathbb{C}(z)).$$

Furthermore, there is a natural inclusion $A(X) \to \mathbb{C}(X)$, which induces a map $\operatorname{Spec} \mathbb{C}(X) \to \operatorname{Spec} A(X)$. As we've stated, this should induce, by functoriality of $\pi_1^{\text{ét}}$, a map

$$\pi_1^{\text{ét}}(\operatorname{Spec} \mathbb{C}(X)) \to \pi_1^{\text{ét}}(\operatorname{Spec} A(X)).$$

As it turns out, this map is just the quotient map from $\operatorname{Gal}(\overline{\mathbb{C}(X)}/\mathbb{C}(X))$ to $\operatorname{Gal}(K_S/\mathbb{C}(X))$.

2.2.4 Etale Fundamental Groups of Arithmetic Schemes

If we apply the idea of schemes to the ring $\mathbb{Z}$ of integers, then $\operatorname{Spec} \mathbb{Z}$ is some sort of space with a point for each prime number p. For a picture, see [EH00, II.4.1]. Similarly, $\operatorname{Spec} \mathbb{Z}[i]$ has points for prime elements such as $1 + i$, 3, and $1 + 2i$.

The map $\operatorname{Spec} \mathbb{Z}[i] \to \operatorname{Spec} \mathbb{Z}$ coming from the inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}[i]$ sends $1 + i$ to 2, 3 to 3, and $1 + 2i$ to 5. Because $(2) = (1 + i)^2$ (as ideals, not elements), the prime (or "point") (2) ramifies in the extension. This means that the map is not a covering.

We can, however, localize to get rid of the prime 2, forming instead hte ring homomorphism $\mathbb{Z}[1/2] \hookrightarrow \mathbb{Z}[i][1/(1 + i)]$. This is in fact a finite étale homormophism of rings. In particular, $\operatorname{Spec} \mathbb{Z}[1/2]$ is not simply connected. Because this cover goes away when we include the point (2), we can think of there being a nontrivial "loop" running around the point (2).

See [EH00, II.4.2] for what happens in the case of the map $\operatorname{Spec} \mathbb{Z}[\sqrt{3}] \to \operatorname{Spec} \mathbb{Z}$, including a picture!

More generally, if you know algebraic number theory, let $\mathcal{O}_K$ be the integer ring of a number field K, S a finite set of primes, and $\mathcal{O}_{K,S}$ the ring of S-integers, i.e., with primes in S inverted. Then $\pi_1^{\text{ét}}(\operatorname{Spec} \mathcal{O}_{K,S})$ is the Galois group of the maximal extension of K unramified outside S.

There's a theorem of Minkowski that $\mathbb{Q}$ has no unramified extensions; in other words, this says that $\operatorname{Spec} \mathbb{Z}$ is simply connected! Going even further, the theory of the Hilbert class field tells that the (narrow) class group of $\mathcal{O}_K$ is isomorphic to the Galois group of the maximal unramified abelian extension of K. In other words,

$$\operatorname{Cl}^+(\mathcal{O}_K) \cong \pi_1^{\text{ét}}(\operatorname{Spec} \mathcal{O}_K)^{\text{ab}}.$$

One deficiency of the étale theory is that it does not detect "ramification" at the infinite places and so does not see the full class group $\operatorname{Cl}(\mathcal{O}_K)$. There are some more sophisticated approaches to this, such as the Artin-Verdier étale topos (see [Mor11]).

On the other hand, note that $\pi_1^{\text{ét}}(\operatorname{Spec} \mathbb{Z}[1/p])$ is already very large. It contains a quotient isomorphic to $\mathbb{Z}_p^\times$, coming from the p-power cyclotomic extensions of $\mathbb{Q}$.

Knots and Primes

In this direction of considering fundamental groups in arithmetic, note that for a finite field $\mathbb{F}_q$, we have $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \cong \widehat{\mathbb{Z}}$. This is the same as the étale fundamental group of $\mathbb{C} \setminus \{0\}$, so we might think that $\operatorname{Spec} \mathbb{F}_q$ is homotopically a circle. In more topological terms, we say that $\operatorname{Spec} \mathbb{F}_q$ is a $K(\widehat{\mathbb{Z}}, 1)$.

What about $\operatorname{Spec} \mathbb{Z}_p$? What is its étale fundamental group? First, let's recall what happens for $\operatorname{Spec} \mathbb{Q}_p$; as $\mathbb{Q}_p$ is a field, a covering is just a map $\operatorname{Spec} K \to \operatorname{Spec} \mathbb{Q}_p$ for a finite field extension $K/\mathbb{Q}_p$, and $\pi_1^{\text{ét}}(\operatorname{Spec} \mathbb{Q}_p) = \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$.

Now, $\mathbb{Q}_p$ is the fraction field of $\mathbb{Z}_p$. As we discussed at the end of §2.2.3, if A is the coordinate ring of $\mathbb{C} \setminus S$ (whose fraction field is $\mathbb{C}(z)$), then the set of finite étale covers of A corresponds to only *some* of the finite étale covers of $\mathbb{C}(z)$, and we have a quotient map $\pi_1^{\text{ét}}(\operatorname{Spec} \mathbb{C}(z)) \to \pi_1^{\text{ét}}(\operatorname{Spec} A)$. Similarly, only *some* finite field extensions K of $\mathbb{Q}_p$ should give finite étale covers of $\operatorname{Spec} \mathbb{Z}_p$ (and when they do, the corresponding finite étale covering is $\operatorname{Spec} \mathcal{O}_K \to \operatorname{Spec} \mathbb{Z}_p$). Which ones? Based on our discussion of ramification, the following answer should make sense to you: $\operatorname{Spec} \mathcal{O}_K \to \operatorname{Spec} \mathbb{Z}_p$ is étale precisely when $p\mathcal{O}_K$ is not a nontrivial power of a prime ideal. In other words, this is étale precisely when $K/\mathbb{Q}_p$ is an *unramified* extension of $\mathbb{Q}_p$.

This tells us that $\pi_1^{\text{ét}}(\operatorname{Spec} \mathbb{Z}_p) = \mathrm{Gal}(\mathbb{Q}_p^{unr}/\mathbb{Q}_p)$, where $\mathbb{Q}_p^{unr}$ is the maximal unramified extension of $\mathbb{Q}_p$. From the basic theory of extensions of $\mathbb{Q}_p$, we know that this Galois group is naturally isomorphic to $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \cong \widehat{\mathbb{Z}}$ and has a natural generator known as Frobenius. In fact, this isomorphism comes from the fact that the natural inclusion of schemes $\operatorname{Spec} \mathbb{F}_p \to \operatorname{Spec} \mathbb{Z}_p$ induces an isomorphism on étale fundamental groups.

Taking this further, since $\operatorname{Spec} \mathbb{F}_p$ is like a circle, we might think of an embedding of $\operatorname{Spec} \mathbb{F}_p$ into another scheme as being a knot in that scheme. In fact, for each prime number p, we have a natural embedding of schemes $\operatorname{Spec} \mathbb{F}_p \hookrightarrow \operatorname{Spec} \mathbb{Z}$. For reasons that are too complicated to explain here (they involve étale *cohomology*; see [Maz73]), it is appropriate to think of $\operatorname{Spec} \mathbb{Z}$ as a 3-manifold, and so a prime number is like a knot in a 3-manifold. This analogy was originated by Mumford and Mazur, who showed that the analogy goes fairly deep: quadratic residues are an arithmetic analogue of linking number, and the Alexander polynomial has an arithmetic analogue in Iwasawa theory! For a survey of these ideas, see [Mor10], or see [Mor12] for a more detailed introduction.

Minhyong Kim has recently tried to find arithmetic analogues of gauge theory and TQFT as applied to knots; for a survey, see [Kim18].

2.3 Galois Groups and Fundamental Groups, Intertwined

We've so far considered covers of $\operatorname{Spec} A$ 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. So let us consider varieties over a non-algebraically closed field. In fact, 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

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

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. That would suggest that $\pi_1^{\text{ét}}(\operatorname{Spec} A)$ is a combination of $\pi_1^{\text{ét}}(\operatorname{Spec} \mathbb{Q}) = G_{\mathbb{Q}}$ and $\pi_1^{\text{ét}}(\operatorname{Spec} A_{\mathbb{C}})$, where

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

Notice that $A_{\mathbb{C}}$ is the coordinate ring of a complex variety, a kind of ring we've considered before.

We can formalize this by considering the string of homomorphisms

$$\mathbb{Q} \to A \to A_{\mathbb{C}}.$$

Remark 2.3.1. As a technical point, we want the polynomials to be such that $A_{\mathbb{C}}$ is an integral domain, i.e. the variety X it corresponds to is irreducible over $\mathbb{C}$ (we say *geometrically irreducible*). For example, we would not consider $f_1(x, y) = f(x, y) = x^2 + y^2$, even though A in this case would be an integral domain.

These maps of rings give rise to maps

$$\operatorname{Spec} A_{\mathbb{C}} \to \operatorname{Spec} A \to \operatorname{Spec} \mathbb{Q}.$$

As per functoriality of $\pi_1^{\text{ét}}$, we should have a sequence of group homomorphisms

$$\pi_1^{\text{ét}}(\operatorname{Spec} A_{\mathbb{C}})) \to \pi_1^{\text{ét}}(\operatorname{Spec} A) \to \pi_1^{\text{ét}}(\operatorname{Spec} \mathbb{Q}).$$

Assuming the variety is nonsingular, it turns out that this sequence is exact, with the last map surjective. The idea behind this is that $\operatorname{Spec} A$ is somehow like a fiber bundle (or fibration) over $\operatorname{Spec} \mathbb{Q}$ with fiber $\operatorname{Spec} A_{\mathbb{C}}$). This idea might seem strange, given that $\operatorname{Spec} \mathbb{Q}$ 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 $\operatorname{Spec} \mathbb{C} \to \operatorname{Spec} \mathbb{Q}$; and that is where it all comes from!

It turns out, furthermore, that the first map is injective. Equating $\pi_1^{\text{ét}}(\operatorname{Spec} A_{\mathbb{C}})$ with $\pi_1\widehat{(X(\mathbb{C})})$ and $\pi_1^{\text{ét}}(\operatorname{Spec} \mathbb{Q})$ with $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, we have a short exact sequence

$$0 \to \pi_1\widehat{(X(\mathbb{C})}) \to \pi_1^{\text{ét}}(\operatorname{Spec} A) \to \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to 0.$$

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.*

2.3.1 Sections and Rational Points

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

$$A \to \mathbb{Q}.$$

This is therefore the same as a map $\operatorname{Spec}\mathbb{Q} \to \operatorname{Spec} A$ such that the composition

$$\operatorname{Spec}\mathbb{Q} \to \operatorname{Spec} A \to \operatorname{Spec}\mathbb{Q}$$

is the identity. By functoriality of $\pi_1^{\text{ét}}$, this gives us a map $\pi_1^{\text{ét}}(\operatorname{Spec}\mathbb{Q}) \to \pi_1^{\text{ét}}(\operatorname{Spec} A)$ that splits 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 ([Gro97a]) 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. For a modern survey of results related to the section conjecture, see [Sti13].

2.3.2 Geometric Galois Actions

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

$$\pi_1^{\text{ét}}(\operatorname{Spec} A)$$

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

$$\pi_1^{\text{ét}}(\operatorname{Spec} A) \to \operatorname{Aut}(\pi_1\widehat{(X(\mathbb{C}))}),$$

which we compose with the quotient map

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

to the group of *outer automorphisms* of $\widehat{\pi_1(X(\mathbb{C}))}$, the quotient of the group of all automorphisms by the group of inner automorphisms. Since $\widehat{\pi_1(X(\mathbb{C}))} \subseteq \pi_1^{\text{ét}}(\operatorname{Spec} A)$ acts by inner automorphisms on itself, it maps to the identity in the group of outer automorphisms. This induces a homomorphism

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

known as the outer action of the Galois group on the étale fundamental group.

We can now explain another important part of the "anabelian geometry" alluded to earlier, also from [Gro97a]. Grothendieck was inspired by a theorem in hyperbolic geometry known as Mostow Rigidity, which states that a hyperbolic manifold is determined by its fundamental group (even the hyperbolic structure!). Grothendieck conjectured that if X is a hyperbolic curve over a number field K, then this outer action (as encoded in the group $\pi_1^{\text{ét}}(X)$) should determine X as an algebro-geometric object! This conjecture was eventually settled by Shinichi Mochizuki; for a survey, see [NTM01].

We've left open one important question: what does this action look like in concrete terms? Let's consider $A = \mathbb{Q}[x, 1/x]$, so that $\operatorname{Spec} A_{\mathbb{C}}$ is geometrically $\mathbb{C} \setminus \{0\}$. Then $\pi_1^{\text{ét}}(\operatorname{Spec} A_{\mathbb{C}}) \cong \widehat{\mathbb{Z}}$. This has a degree k quotient $\mathbb{Z}/k\mathbb{Z}$. Recall from §1.3.2 that we identified this $\mathbb{Z}/k\mathbb{Z}$ with the group μ_k of kth roots of unity. The Galois action, in this case, is simply induced by the natural action of $G_{\mathbb{Q}}$ on μ_k, which factors through $\operatorname{Gal}(\mathbb{Q}(\mu_k)/\mathbb{Q})$. Taking the limit over all natural numbers k, the action corresponds to a map

$$G_{\mathbb{Q}} = \operatorname{Aut}(\widehat{\mathbb{Z}}) = \widehat{\mathbb{Z}}^{\times}$$

known as the cyclotomic character.

More generally, if X is a variety over $\mathbb{Q}$, we choose a basepoint $b \in X(\mathbb{Q})$ (whose role was played by $1 \in \mathbb{C} \setminus \{0\}$ above). We consider covers defined over $\mathbb{Q}$ for which there exists a rational point over b (why we can do this is beyond us, but I'll just say it comes from the theory of twisting torsors). We may then identify the set of all $\overline{\mathbb{Q}}$-points of the cover above b with the group of deck transformations. Then the $G_{\mathbb{Q}}$-action on these points determines an action on this group of deck transformations. Taking a limit over all sufficiently large covers, we get an action of $G_{\mathbb{Q}}$ on $\widehat{\pi_1(X(\mathbb{C}))}$.[3]

This action of $G_{\mathbb{Q}}$ on the (profinite completion of the) fundamental group of a variety is the subject of much research. For example, if X is a configuration space, then its fundamental group is a braid group, so we get a Galois action on braid groups.

This is reminiscent of Teichmuller theory, where one studies the mapping class group $\operatorname{MCG}(\Sigma)$ of a surface Σ and the natural map

$$\operatorname{MCG}(X(\mathbb{C})) \to \operatorname{Out}(\pi_1(X(\mathbb{C}))).$$

The mapping class group is the fundamental group of a Teichmuller space, which is analytically the complex manifold associated to a moduli space of algebraic curves M_g. In fact, we may combine braid groups and mapping class groups by considering $M_{g,n}$, the moduli space of genus g algebraic

[3] Notice that we got an actual action, not just an outer action. This is because we chose a rational basepoint b. More generally, the outer action does not depend on the choice of basepoint.

curves with n marked points. This has a structure of an algebraic variety over $\mathbb{Q}$, so there is an action of $G_{\mathbb{Q}}$ on its profinite fundamental group, and the action of the mapping class group is Galois-equivariant.

For more on this and related topics, see the volumes "Geometric Galois Actions" ([SL97a], [SL97b]). See also the ICM address of Ihara [Iha91].

In fact, this has given rise to a field known as Grothendieck-Teichmuller theory. Grothendieck gave a lot of thought to this in his gigantic collection of writings "La Longue Marche à Travers La Théorie de Galois" ([Gro95]), as well as a much shorter survey [Gro97b], which is reproduced in [SL97a].

Finally, we end by considering the case $X = \mathbb{C}\backslash\{0,1\}$, also commonly referred to as $\mathbb{P}^1\backslash\{0,1,\infty\}$ or $M_{0,4}$. A famous theorem of Belyi shows that the outer action on $\widehat{\pi_1(X)}$ in this case is faithful (i.e. the homomorphism is injective). In particular, this means that we can understand $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ 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* (see [Zap]). Grothendieck found a combinatorially-defined subgroup $\widehat{\mathrm{GT}}$, known as the *Grothendieck-Teichmuller group*, of $\mathrm{Out}(\pi_1(\widehat{\mathbb{C} \setminus \{0,1\}}))$ that contains the image of $G_{\mathbb{Q}}$. Some even wonder whether this combinatorially-defined group might be isomorphic to $G_{\mathbb{Q}}$; for more, see [Sch97].

Bibliography

[EH00] David Eisenbud and Joe Harris. *The geometry of schemes*, volume 197 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[Gro95] Alexandre Grothendieck. *La longue marche à travers la théorie de Galois. Tome 1*. Université Montpellier II, Département des Sciences Mathématiques, Montpellier, 1995. Transcription d'un manuscrit inédit. [Transcription of an unpublished manuscript], Edited and with a foreword by Jean Malgoire.

[Gro97a] Alexander Grothendieck. Brief an G. Faltings. In *Geometric Galois actions, 1*, volume 242 of *London Math. Soc. Lecture Note Ser.*, pages 49–58. Cambridge Univ. Press, Cambridge, 1997. With an English translation on pp. 285–293.

[Gro97b] Alexandre Grothendieck. Esquisse d'un programme. In *Geometric Galois actions, 1*, volume 242 of *London Math. Soc. Lecture Note Ser.*, pages 5–48. Cambridge Univ. Press, Cambridge, 1997. With an English translation on pp. 243–283.

[Iha91] Yasutaka Ihara. Braids, Galois groups, and some arithmetic functions. In *Proceedings of the International Congress of Mathematicians, Vol. I, II (Kyoto, 1990)*, pages 99–120. Math. Soc. Japan, Tokyo, 1991.

[Kim18] Minhyong Kim. Arithmetic gauge theory: a brief introduction. *Modern Phys. Lett. A*, 33(29):1830012, 26, 2018.

[Mar18] Daniel A. Marcus. *Number fields*. Universitext. Springer, Cham, 2018. Second edition of [MR0457396], With a foreword by Barry Mazur.

[Maz73] Barry Mazur. Notes on étale cohomology of number fields. *Ann. Sci. École Norm. Sup. (4)*, 6:521–552 (1974), 1973.

[Mor10] Masanori Morishita. Analogies between knots and primes, 3-manifolds and number rings [translation of mr2208305]. volume 23, pages 1–30. 2010. Sugaku expositions.

[Mor11] Baptiste Morin. On the Weil-étale cohomology of number fields. *Trans. Amer. Math. Soc.*, 363(9):4877–4927, 2011.

[Mor12] Masanori Morishita. *Knots and primes*. Universitext. Springer, London, 2012. An introduction to arithmetic topology.

[NTM01] Hiroaki Nakamura, Akio Tamagawa, and Shinichi Mochizuki. The Grothendieck conjecture on the fundamental groups of algebraic curves [translation of Sūgaku **50** (1998), no. 2, 113–129; MR1648427 (2000e:14038)]. volume 14, pages 31–53. 2001. Sugaku Expositions.

[Sam70] Pierre Samuel. *Algebraic theory of numbers*. Translated from the French by Allan J. Silberger. Houghton Mifflin Co., Boston, Mass., 1970.

[Sch97] Leila Schneps. The Grothendieck-Teichmüller group $\widehat{\mathrm{GT}}$: a survey. In *Geometric Galois actions, 1*, volume 242 of *London Math. Soc. Lecture Note Ser.*, pages 183–203. Cambridge Univ. Press, Cambridge, 1997.

[Ser64] Jean-Pierre Serre. Exemples de variétés projectives conjuguées non homéomorphes. *C. R. Acad. Sci. Paris*, 258:4194–4196, 1964.

[SGA03] *Revêtements étales et groupe fondamental (SGA 1)*, volume 3 of *Documents Mathématiques (Paris) [Mathematical Documents (Paris)]*. Société Mathématique de France, Paris, 2003. Séminaire de géométrie algébrique du Bois Marie 1960–61. [Algebraic Geometry Seminar of Bois Marie 1960-61], Directed by A. Grothendieck, With two papers by M. Raynaud, Updated and annotated reprint of the 1971 original [Lecture Notes in Math., 224, Springer, Berlin; MR0354651 (50 #7129)].

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[SKKT00] Karen E. Smith, Lauri Kahanpää, Pekka Kekäläinen, and William Traves. *An invitation to algebraic geometry*. Universitext. Springer-Verlag, New York, 2000.

[SL97a] Leila Schneps and Pierre Lochak, editors. *Geometric Galois actions. 1*, volume 242 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1997. Around Grothendieck's "Esquisse d'un programme".

[SL97b] Leila Schneps and Pierre Lochak, editors. *Geometric Galois actions. 2*, volume 243 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1997. The inverse Galois problem, moduli spaces and mapping class groups.

[Sti13] Jakob Stix. *Rational points and arithmetic of fundamental groups*, volume 2054 of *Lecture Notes in Mathematics*. Springer, Heidelberg, 2013. Evidence for the section conjecture.

[Sza09] Tamás Szamuely. *Galois groups and fundamental groups*, volume 117 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2009.

[Zap] Leonardo Zapponi. What is...a dessin d'enfant? *Notices of the AMS*, 50(7).